# TABLE OF CONTENTS

## Introduction .................................................................................................................. 4

### 1. Benefits of NFV as a Concept ................................................................................. 8
   1.1 Improved Capital Efficiency .................................................................................. 8
   1.2 Operational Efficiencies ....................................................................................... 9
   1.3 Service Agility, Innovation and Differentiation ..................................................... 10

## 2. Considerations for Planning and Deployment of NFV-Based Solutions ............... 11

### 2.1 Cost Transformation – Investments, Savings and Redistribution ..................... 11
   2.1.1 Case for Opex Savings ..................................................................................... 12
   2.1.2 Case for Capex Savings ................................................................................... 12
   2.1.3 Other Cost Implications .................................................................................. 14
   2.1.4 Plan to Invest ................................................................................................ 14

### 2.2 Triggers for NFV Planning .................................................................................... 15

### 2.3 Managing a Legacy-to-NFV Evolution ................................................................. 16

### 2.4 Timeline to a Positive ROI .................................................................................. 16

### 2.5 Commercial Deployment Considerations ............................................................ 17

## 3. Architectures and Ecosystems .................................................................................... 18

### 3.1 Major Architectural Considerations Around NFV ............................................... 18

### 3.2 Agile Service Introduction and Evolution .............................................................. 20

### 3.3 Architectural Challenges and Opportunities in Multi-Vendor NFV Ecosystems .... 20

   3.3.1 Scaling Services ............................................................................................. 21
   3.3.2 Intra-Service Dependency ............................................................................. 21
   3.3.3 Session Data Sharing ..................................................................................... 22
   3.3.4 Virtualization Technology Dependencies ....................................................... 22
   3.3.5 Interoperability ............................................................................................. 22

### 3.4 Reliability and Stability Guarantees ...................................................................... 23

### 3.5 Performance on Virtualized Deployments ............................................................. 24
3.6 Scale-Up vs. Scale-Out / Small vs. Large Distribution ................................................................. 25
3.7 Shared Network Infrastructure......................................................................................................... 27
3.8. Key Considerations for Implementing NFV Architecture ............................................................ 29
3.9 NFV Roadmap Strategies .............................................................................................................. 29
3.10 Which Nodes Benefit the Most From a Completely Virtualized Environment? .............................. 31
3.11 Software Design Considerations in NFV Evolution ....................................................................... 32
3.12 Ecosystem of Solutions and Services Complementing and Supporting NFV Architecture .................. 32
3.13 Operator NFV Strategies ............................................................................................................. 33
  3.13.1 Telefónica Unica ....................................................................................................................... 33
  3.13.2 AT&T UDNC ............................................................................................................................ 34
3.14 Standard and Open Source Activities ........................................................................................... 36

4. Use Cases ........................................................................................................................................ 38
  4.1 Virtualizing IMS and VoLTE ......................................................................................................... 38
  4.2 Virtualized EPC (VEPC) .............................................................................................................. 40
  4.3 New Offerings with VEPC and SGI Services ................................................................................. 42
  4.4 C-RAN .................................................................................................................................. 43

5. Next Steps and Recommendations - Architecting the NFV Journey ................................................. 45
  5.1 Managing the Architectural Strategy ............................................................................................ 46
    5.1.1 Set Responsibility for Architecture and Standards ............................................................... 46
    5.1.2 Build an Evolution Plan ....................................................................................................... 46
  5.2 Role of Vendors and Operators in the 4G LTE NFV Ecosystem ...................................................... 47
  5.3 Utilize Proof of Concepts and Move Towards Devops ................................................................... 48

Conclusion .......................................................................................................................................... 49

References ......................................................................................................................................... 50

Appendix ........................................................................................................................................... 51
  Cloud Definitions ............................................................................................................................... 51
  ETSI ISG PoC List ............................................................................................................................. 52
  Definition of IaaS/PaaS/SaaS ........................................................................................................... 53

4G Americas Brining Network Function Virtualization to LTE November 2014 2
Acronyms

Acknowledgements
INTRODUCTION

The mobile telecommunications industry is at the verge of a unique business crossroads. The growing gap between capacity and demand is an urgent call for new approaches and alternative network technologies to enable mobile operators to achieve more with less.

Today, mobile broadband data is growing at an annual rate of 40-50 percent per year in the U.S. and other regions globally. Mobile service providers address these rapidly expanding traffic volumes through deployment of additional network functions, which will be a significant capital expenditure (CAPEX) challenge. The nature of that mobile broadband data traffic is also evolving with new services including new video applications, connected cars and the Internet of Things (IoT). This rapid capacity growth and increasing traffic diversity in LTE networks stresses the assumptions of existing network architectures and operational paradigms.

Network Functions Virtualization (NFV) provides a new path that can increase the flexibility required by mobile service providers and network operators to adapt and accommodate this dynamic market environment. NFV is a new operational approach applying well-known virtualization technologies to create a physical Commercial Off-the-Shelf (COTS) distributed platform for the delivery of end-to-end services in the context of the demanding environment of telecom network infrastructure and applications. Much of the terminology of NFV used today originated from the initial European Telecom Standards Institute (ETSI) white paper titled, *Network Functions Virtualisation – Introductory White Paper* [1].

Mobile telecom operators today are managing and running complex physical networks with a wide variety of network nodes, technologies and geographical span. These network functions are deployed using a mix of COTS and single-purpose built hardware dedicated to individual network functions. This approach to building and operating mobile networks is almost unsustainable moving forward, as outlined in the problem statement by the ETSI NFV Industry Specification Group (ISG) [1]:

- Complex carrier networks with a large variety of proprietary nodes and hardware appliances are negatively impacting efficiency.

- Launching services is difficult, takes too much time and requires another variety of box which needs to be integrated.

- Operation is slow and expensive due to the traditional standardize-procure-design-integrate-deploy cycle.

Figure 1 summarizes these problems and compares them to the ETSI vision as described in [1].
The NFV ISG’s mission is to facilitate the industry transformation and development of an open, interoperable ecosystem through specification, implementation and deployment experience. Figure 2 illustrates the ETSI NFV architectural framework which provides guidance for a NFV approach that can be deployed in multivendor environments. The framework includes new management and orchestration functions which can impact existing operational procedures and service models, rearrange the responsibility/administrative domains of operators and reduce Operating Expenses (OPEX). Another important transformation is to introduce a much higher level of automation in the control, provisioning and management of the NFV applications, infrastructure and resources.
As the virtualization technology has been used in the IT industry for many years, the mobile operators and vendors have decided to endorse the ETSI ISG work to provide the building blocks for standardization as opposed to proprietary and non-standard solutions.

In the context of NFV, Virtualized Network Functions (VNFs) are used by mobile operators to realize the network nodes/applications required to construct end-to-end services using NFV. The virtualized network functions are deployed and operated over physical COTS or more standard compute, networking and storage resources. This complex of infrastructure resources is described by ETSI as Network Functions Virtualization Infrastructure (NFVI). A VNF is a software implementation of a network function capable of running on the NFVI. The NFVI includes a virtualization layer that abstracts the hardware to support decoupling of the VNFs from the hardware. The virtualization layer provides the execution environment (e.g., virtualized compute, storage and networking) required by the VNFs, allowing them to be dynamically instantiated on physical resources. One common solution is to implement the virtualization layer with a hypervisor and a guest Operating System (OS) to support the VNFs. The ISG also envisions a framework emphasizing end-state functions deployed in a distributed cloud infrastructure allowing for more dynamic deployment of network functions in the location where they can maximize their efficiency.

The NFV management architecture supports the management and orchestration of the NFVI resources together with the VNFs. The orchestration of these resources can be combined into NFV forwarding graphs (a chain of existing network functions) or service chains that define how a set of VNFs work together. These chains can then be additionally optimized per user, traffic flow, profile or another defined policy within the network. Very often services such as Network Address Translation (NAT), firewall and Deep Packet Inspection (DPI) are applied to a data session in sequence. To orchestrate this capability in the context of an NFV implementation, a management and orchestration system can create a “blueprint” of this sequence of services, then provision and start up the

---

1 In this paper, the term “cloud” is used in the generic sense without implying the implementation of a specific type of cloud for NFV.
NFVI infrastructure and VNFs comprising of the service sequence as well as the networking connections are needed to start up and connect the service flows (forwarding graphs) together. This automation and ability to automatically add capacity or new sequences is a distinct operational advantage made possible by NFV.

Software Defined Networking (SDN) is a new networking technology approach that can provide a new way of controlling, switching and routing the connections between the VNFs. Similar to how NFV decouples hardware and software in network functions, SDN decouples control and switching in the networking domain. Together NFV and SDN provide a highly configurable and flexible networking and network function. NFV can also be implemented with current and evolved routing, switching and service control. NFV and SDN are two independent architectural approaches that complement each other, but NFV does not require SDN implementation to realize the benefits. With this paper, SDN as a standalone technology is not discussed; rather it is described as a complement to NFV used to deliver a complete virtualized solution.

Multiple architectural, operational and organizational challenges may need to be addressed in the transition toward an architecture using NFV platforms. There are practical and economic reasons why network functions that become virtualized cannot happen overnight. Some network functions may never be virtualized, and some of the key challenges are addressed later in this paper.

The high-level objectives driving the initial use cases for NFV include:

- Rapid service innovation through automated deployment and operationalization of software-based network functions and end-to-end services
- Improved operational efficiencies resulting from common automation and operating procedures
- Reduced power usage achieved by migrating workloads and powering down unused hardware
- Standardized and open interfaces between functions and their management entities so that decoupled network elements can be provided by different vendors
- Greater flexibility in assigning VNFs to hardware
- Improved capital efficiencies compared with dedicated hardware implementations

In particular, mobile operators can take the advantages of NFV as new services are introduced. Evolved Packet Core (EPC), Voice over LTE (VoLTE), IP Multimedia System (IMS) and enhanced messaging services among others are examples of opportunities to use virtualized solutions. In addition, this paper discusses how mobile operators will gain the agility to dynamically deploy new services on top of a common NFVI infrastructure.
1. BENEFITS OF NFV AS A CONCEPT

While virtualization has been applied in many different contexts, the virtualization of network functions is an emerging paradigm for 4G LTE networks. NFV’s key concept is not the technology of the hypervisor, but rather the transformation of the network infrastructure and associated operational and business models. The ability to dynamically instantiate VNFs, compose end-to-end services and independently scale the network infrastructure capacity to support emerging service demands frees the service provider from the lengthy procurement and deployment timeframes associated with proprietary hardware. The following sections outline the expected benefits and opportunities in the network investment as a business case.

1.1 IMPROVED CAPITAL EFFICIENCY

With NFV, the operator will be able to deploy and operate VNFs in a COTS hardware-based infrastructure platform. This COTS infrastructure is expected to support VNFs from multiple vendors and the VNFs deployed on a given processor may support different services. This creates a new paradigm for capacity of the COTS infrastructure where scaling of the infrastructure takes into consideration demand aggregated across all of the tenant VNFs planned to operate on a given infrastructure instance. In contrast, existing proprietary network elements have the hardware and software component tightly bound together so that both must be incremented together, typically in coarse capacity increments. NFV infrastructure is expected to generate CAPEX savings by:

- Provisioning capacity for all functions versus each individual function
- Providing more granular capacity increments (e.g., another core on a processor rather than another chassis or blade)
- Exploiting the larger economies of scale associated with COTS hardware
- Centralizing VNFs in data centers where latency requirements allow
- Separately and dynamically scaling VNFs residing in the user (or data or forwarding) plane designed for execution in the cloud, control and user-plane functions as needed

Some operators even consider the NFVI implementation as ‘Internal Infrastructure as a Service’ (IaaS) or a ‘Platform as a Service’ (PaaS) style resource deployed by the operator’s Chief Information Officer (CIO) or Chief Technology Officer (CTO to serve a large category of applications or “workloads”. Treating this as an internal service platform helps speed up provisioning and reduces long lead times for installation of new custom hardware. This treatment also makes it much faster and easier to upgrade and supports increasing capacity needed without continually deploying CAPEX for each implementation. The mobile operator can consistently repurpose the underlying resources through the cloud manager platform, making them available to other VNFs as needed. This also reduces the risk of stranded hardware assets that may be left from a service that did not reach its forecasted utilization.

Functions that are non-real-time and reside on the control plane can run on highly scalable distributed NFVI hardware wherever capacity is available. Functions that depend upon deterministic, real-time performance and high availability can also benefit from NFV; however, these functions put much greater demand on an NFVI and need special consideration. There are also specific performance and architectural considerations that need to be taken into account when deploying control and data plane VNFs. These are outlined in the architecture discussion in Section 3.

Consolidation from an infrastructure point of view can also increase utilization of computing and storage resources and eliminate the low computing/storage utilization rates for existing dedicated platforms. The computational load of VNFs supporting different services may or may not be entirely synchronized. As a result,
the aggregate computational load seen by the “common” infrastructure may be less than the sum of the peak loads of all the individual VNFs when workloads are notably different. When VNF capacity is underutilized, the NFVI resources manager may reallocate the resources to other VNFs or to the processing of non-VNF workloads (e.g., OSS/BSS functions).

Finally operating network functions on homogenous COTS hardware allows for interface connections over virtual “links” and when capacity requirements permits, to be placed on virtual machines (VMs) of the same physical hardware. This reduces both physical ports and networking equipment required, resulting in CAPEX savings.

1.2 OPERATIONAL EFFICIENCIES

The potential for OPEX savings from a well-planned and designed VNF deployment is arguably an area with the biggest potential. The deployment of VNFs as software using cloud management techniques enables scalable automation at the click of an operator’s (or customer’s) mouse or in response to stimulus from network analytics. Maximizing automated service actions is one of the core promises of NFV. Mobile network and service architectures are significantly diverse, complex and sophisticated. The ability to automate onboarding, provisioning and in-service activation of new virtualized network functions can yield significant savings. Obtaining the VNF from a VNF provider in a standard software format enables automation in regression testing and configuration of new and existing services. The efficiency of automation not only saves money but enables significant reduction in the time to revenue for new orders or reconfigurations of existing service types. Finally, the NFV framework enables automation to self-correct problems in end-to-end services (e.g., rerouting traffic out of congested paths dynamically, killing VNFs’ VMs that are “stuck” and transferring the VNF’s workload to newly instantiated VMs).

Another area for operational savings is reducing manual intervention for installation, operations, administration and maintenance of proprietary hardware. As the network functions are virtualized and deployed onto a “common” NFVI hardware platform, the variety of disparate proprietary systems is reduced. This provides operational efficiency through reductions in both the spare inventory of equipment, maintenance, lifecycle management of separate platforms and in training of personnel.

As an example, Voice Over LTE (VoLTE) has several products/nodes elements in the network and are required to deploy an end-to-end VoLTE solution. In a VoLTE deployment with single-purpose, proprietary hardware, it could require multiple racks’ worth of independently deployed equipment. With NFV, the same scenario could require as little as a single server or blade. The operator can in principle take multiple vendor’s software applications and deploy them to interoperate from a common NFV infrastructure platform and orchestrate their utilization accordingly, thus demonstrating significant savings from the NFV framework.

Another deployment example is to provide a multi-tenant hosted solution. A mobile operator can collocate VNFs that are on a common platform in a single hosted data center that is shared by multiple entities or markets (e.g., mobile operating companies from different countries). Performance and economic evaluations of such collocation may need to consider studies covering aspects such as transport networks costs, latency dependencies of the hosted network functions and traffic-shaping needs.
1.3 SERVICE AGILITY, INNOVATION AND DIFFERENTIATION

The ability to easily deploy new types of VNFs on a cloud-like NFVI creates a new degree of flexibility for service providers. These new VNFs can be efficiently connected and deployed as new service packages without standing up an entirely new, proprietary-hardware network consisting of multiple boxes for routing and other network services appliances. Through automation and agility in deploying these new VNFs, time-to-market for new network services can be significantly reduced, increasing the operator’s ability to capture market share and develop market-differentiating services.

New revenue opportunities may also come from virtualization of network functions that today are deployed in areas like customer premises equipment. Once decoupled from the underlying hardware platform, they can be delivered as a service from a service provider’s NFVI or operated by the mobile provider in a virtualized environment on a customer's NFVI node [5]. These applications can include virtualized home or enterprise gateways, mobile enterprise services and a broad range of operator and end-user oriented services such as virtual desktop applications, collaboration services and more.

The new delivery model also enables an increased agility in serving new customer use cases and addressing new industry sectors. Consumers and enterprises increasingly expect mobile services to be immediately available as soon as they or their employees sign up. NFV enables mobile operators to meet those expectations even when those services are highly customized for a specific vertical or a specific customer. For example:

- Scalability for massive sports events such as the Super Bowl or World Cup. The leagues and other sports organizations could work with mobile operators to deliver streaming video of the games to millions of smartphones, tablets and other devices within a country or around the world.

- Use of wireless IoT sensors in verticals such as manufacturing, retail and transportation. These applications’ bandwidth requirements may vary by season, hours of the day and/or local events. In such instances, network capacity and configuration can be optimized on demand (and charged as such on usage basis) without static over-investment in capacity.

Networks of the future must be able to scale effectively, respond to varied and unpredictable traffic models, compete with and support over-the-top (OTT) providers and accelerate the introduction of new mobile services. Traditionally, these new services take mobile operators one to two years or more to implement in their network. In a NFV operational model, because the operators are now deploying software, it is possible to accelerate the introduction of new services into the network and deploy them flexibility to meet the varying demand. NFV also enables greater agility in how those new services are introduced.

Functions, typically those that are non-real-time and reside on the control plane, can run on highly scalable distributed NFVI hardware wherever capacity is available. This can yield significant cost and operational efficiencies, analogous to those of Web-scale solutions today. Today’s networks are also becoming widely distributed to provide a variety of functions close to the user for improved customer experience. The same NFV technologies enabling efficiencies in centralized locations can also be deployed in distributed locations and managed in the same fashion.

In order to realize the breadth of new and sophisticated deployment possibilities, mobile operators must take advantage of automation and delivery tools to deploy new network elements into the network. The automated configuration of all of the routing, IP addressing and logical interfaces, as well as verification that those functions behave correctly in the network before they are active, enables more efficient service creation using modern software operations approaches such as those commonly used in the IT space. One such approach form the IT
space is known as DevOps. With DevOps, service creation (development) is closely aligned with the operational deployment requirements through automated configuration testing and validation. With continuous integration, the baseline build is incrementally adjusted as new resources are deployed, services defined and applications integrated. DevOps strategy is particularly powerful when deploying “as a service” style applications in the IaaS, Platform as a Service (PaaS) or Software as a Service (SaaS) models where the operator owns and manages the whole stack and the can continuously update the running software applications with incrementally features and capabilities.

To demonstrate the concept of increased agility, let’s say an enterprise wants a simple, private voice network. Without NFV, this would involve deploying separate physical network elements, network configurations and network bandwidth allocations. With an NFV network, all of the logical applications can be instantiated in the operator’s core and access networks to deliver a private, end-to-end VoLTE solution for that enterprise. With NFV, this can be instantiated as new software deployed on available NFVI hardware using policy rules to build out this new suite of services dedicated to that specific customer. Configuration changes to the VoLTE service in response to customer requests can automatically be deployed across multiple sites once the first site configuration is validated.

As easy as this may sound, in the next section we will address the planning and considerations that need to be taken into considerations before deploying a NFV solution.

2. CONSIDERATIONS FOR PLANNING AND DEPLOYMENT OF NFV-BASED SOLUTIONS

The promises of the NFV model to realize significant OPEX and CAPEX savings will take careful consideration. There are operator specific impacts on the business case that make the details of the savings and the roadmap to achieve these savings different for every operator. The realization of the OPEX and CAPEX benefits will be dependent on the rates at which a common architectural approach can be agreed, the operational transformation and automation can be implemented and underutilized hardware capacity can be minimized. There is also a very complex transformation and migration required to go from running and operating a large existing complex set of networking infrastructure and applications that must continue to function as the newer infrastructure and frameworks are put in place for the next generation of NFV infrastructure and applications. This transformation phase may even take extra investment in order to operate both network generations during the transformational time frame.

2.1 COST TRANSFORMATION – INVESTMENTS, SAVINGS AND REDISTRIBUTION

A common question is whether there are net savings from the NFV transformation or whether it is simply a redistribution of how and where budget is consumed. The reality is that in the early stages of the transformation, there could be as much redistribution as there is savings, but in the long term, the savings become the dominant factor. If the cost savings are based on an assumption of a multitentant infrastructure, then CAPEX savings may not accrue until the second tenant (VNF or service) is deployed. Degree of impact in deployment of an NFV strategy also depends upon several key strategic factors that can affect the overall success in reducing costs over the long term:

- New commercial terms in software, hardware and services in a more complex multi-vendor and open-source environment

- How many applications are transitioned to NFV and over what time period
• Leveraging infrastructure and operational synergies as multiple functions are virtualized
• Commitment to broad operational transformation and automation
• Competence transformation vs. overall operational staff reductions to support the operational optimization

2.1.1. CASE FOR OPEX SAVINGS

On the OPEX side, the key to significant savings rests on automation of operational procedures and the associated changes in staffing levels and skills. The NFV orchestration function (NFVO) provides a network automation function based on the information models for the virtualized and real resources. Once implemented this can drive significant OPEX savings over time as costly manual processes are replaced. Initially the NFVO function is new to the operator environment, and that in general will create one-time startup costs as each VNF area is transformed. The speed to achieve savings is gated by the ability to impact the most costly activities. OPEX saving are tied to a well-designed carrier grade automation of operational processes that span from onboarding and instantiation of new VNFs to the design and deployment of new services.

As the NFV architecture becomes a reality in operator networks, the innovation process leading up to deployment of new services can be optimized as well. Testing and trials of new services can happen much more rapidly and at much lower cost. This can ultimately lead towards a DevOps style deployment process, as discussed earlier, increasing the speed and agility in delivering new services to the market. This ultimately saves costs and improves time for revenue.

2.1.2. CASE FOR CAPEX SAVINGS

CAPEX reductions are driven by the migration from proprietary hardware platforms to a unified set of hardware for the network supporting the NFVI framework and the optimization of software utilization based more on demand as opposed to peak planning.

Some savings are achieved immediately through the simple replacement of telecom-specific hardware with COTS platforms. The larger, long-term business benefit is in the concentration of the hardware CAPEX on a much narrower set of suppliers, configurations and components that can benefit from scale in procurement. Facilities optimize from higher density deployments using the latest power optimization and HVAC strategies can also create cost savings.

Virtualization of network functions transforms proprietary systems of tightly coupled hardware and software into proprietary software running on COTS hardware. The proportional costs of the software and hardware components of the proprietary system may be different from those in the NFV environment. Through virtualization of the software assets, the scaling characteristics of the VNF licensing costs in the NFV environment may become much more adapted to the traffic/services utilization as opposed to today’s licensing “step functions” associated with deploying tightly coupled proprietary systems. In addition, the metrics underlying the VNF licensing may be more aligned with business needs (e.g., effective throughput) rather than capacity of proprietary boxes.

For example, when providing services in the context of a mobile core, network DPI and policy controls are used to invoke specific services for specific user groups, profiles or traffic types. Services such as security, anti-virus, parental controls, URL filtering and optimization services may be deployed at a specific, relatively fixed scale to accommodate the anticipated traffic levels. This means both the hardware footprint and software licensing are fixed to support the expected levels. When deployed with NFV framework, these services (software applications) become VNFs and can be scaled according to the actual service utilization levels managed by manual or
automatic scaling. This transformation brings forward some important considerations regarding software licensing models to accommodate fixed vs. dynamic licensing of the applications. Implications also reach into the common infrastructure platform elements, such as databases and middleware required to support new deployment models for the VNFs. Both operators and vendors need to fully analyze the requirements of the software applications to be sure the underlying software platforms, databases and services have licensing that can support virtualization and dynamic scaling and pricing to match the agility and flexibility of the NFV framework.

CAPEX reductions may also be achieved through conversion of capital expenses to operational expenses (e.g., software licenses). When software is purchased (often together with hardware and installation services), these expenses are typically capitalized and depreciated. When software is purchased on a pay-per-use or other non-perpetual licensing of software, it becomes an operational expense and is accounted for in a month-to-month, quarterly or other recurring fee. OPEX also can imply that the operator no longer owns the software asset. This can be defined as a CAPEX-to-OPEX cost transformation. This also affects the balance sheet and other supply chain and accounting practices.

In PaaS and SaaS, vendors bundle the solution into an “as-a-service” model and can deploy this in the operators’ network or provide turnkey services and capabilities from vendor-operated solutions. This is more common today in areas of Machine-to-Machine (M2M), managed core networks or solutions targeted at specific industries. Securing services this way also falls on the side of an OPEX cost.

OPEX savings should consider the operational lifecycle (Figure 3) for the VNFs as software components. This is a different lifecycle compared to architectures based on relatively static proprietary hardware. The total cost of ownership should consider all phases of the lifecycle, as well as the improvement in flexibility and agility capabilities for service modifications or evolutions. The transition to software based infrastructure may require different staff skill mixes, but provide other advantages such as increased testing automation.

![Figure 3. A VNF Life Cycle.](image)

Source: AT&T
2.1.3 OTHER COST IMPLICATIONS

There are some areas where costs may vary or could be affected by strategic decisions. NFV elements that have not been tested, previously deployed, certified in commercial operation and are designed from scratch for the NFV framework, may need extra integration and SLA (Service Level Agreement) verification before being ready for commercial operations. VNF and NFVI layers may now consist of an increasingly diverse set of vendors, open-source software and operator-developed components. Unless sourced as a verified solution from one vendor or solution provider, an increased burden is put on development and verification of the integration points, functional requirements, performance and throughput verification, as well as software/hardware lifecycle management that may have traditionally been done by a single vendor or system integrator. Strategies that involved more highly distributed VNF create additional demands on new software to manage, maintain and monitor the distributed environment.

There are some areas that are likely to result in increased CAPEX and OPEX costs. Introduction of the basic underlying NFVI and virtual infrastructure and management software, regardless of the platform environment decision, introduces costs associated with the operation of this platform. As the operator stands up the first instance, it will also require a period of time to work through a different combination of hardware and software to meet the specific operator’s needs and expectations. There will likely be phases of proof-of-concepts, lab trials, vendor trials, pre-commercial trials to prove out the NFV framework and even specific 4G LTE functional areas independently. These costs must be included in the NFV business case. This can be evaluated as internally or externally outsourced if the mobile operators have no desire, time or budget to add this expertise in house.

“Solution in a box” versus component or node based purchasing can create new options. There are varying levels of integration possible in the context of integrated VNF+NFVI solutions. For example, an IMS node could be an integrated solution sold as one node but internally use all of the aspects of NFV framework for its own operations, scaling, management, and so on. Another extreme could be all of the VNF, NFVI and management elements needed for a complete IMS VoLTE solution be pre-integrated, packaged and implemented in one hardware-software package, even scaled down to the smallest possible hardware footprint for smaller implementations.

2.1.4 PLAN TO INVEST

New software elements used for NFV management and orchestration software will be an additional cost. This serves many different functions, but a key aspect of this piece of the solution is to bridge the end-to-end network view across the NFV orchestrator, various VNF managers, and the virtualized infrastructure manager for NFVI and Operation Support Systems/Business Support Systems (OSS/BSS) between cloud-based and traditional network elements and systems. Systems integration, verification, support, lifecycle management and upgrades of the various NFV framework layers in multi-vendor VNFs/NFVI and the NFV management and orchestration software all are needed. The level of system integration services and support needed will vary by degree of pre-integrated elements.

Establishing reliable and controllable levels of automation in software provisioning, capacity/scaling and workflow processes across network operations will need extensive, operator specific implementation verification. Some operators are concerned about the risks involved with highly or “fully” automated provisioning and scaling. If a fully automated process were to be faulty, it could create cascading effects that may spin out of control without some manual intervention points.

Another aspect to consider is additional sets of management and troubleshooting tools, techniques and competencies needed to deal with the additional complexity of the network in two contexts: physical and logical. As the NFV frameworks are realized, there is now a complex translation and myriad of combinations of physical to
logical (or virtualized) instances of nodes, layers, appliances, ports, connections and so on. The entire network domain needs to be addressed at both the physical and logical levels as well as a legacy and NFV context. In addition, for highly distributed VNFs, the physical and logical layers can be spread across multiple physical data center instances. This increased complexity will require additional investment in competence, resources, tools, techniques, training, operational skills and processes that may not even exist today. Old troubleshooting and isolation techniques may not be applicable or may need to be completely changed in the new context of NFV since issues may arise in both the physical and virtual solution domain.

Lastly, different procurement models are now possible. Operators’ supply chain, procurement models and processes also need to adapt to the change to take advantage of the new business models. No longer is a function or service defined and procured in isolation. When planning a purchase where scaling is critical, this may become a more complex task due to the increasingly independent connection between the hardware and software purchasing strategies. Additionally, old dimensioning models setup for traditional network equipment and software purchasing may no longer be valid.

### 2.2 TRIGGERS FOR NFV PLANNING

In addition to the changes and transformations in operations and business model described in previous sections, such as market conditions, internal business policy decisions, business strategy considerations, operational procedure improvements, etc; in this section the technical triggers are analyzed. For operators working with growth and evolution of LTE networks, there are a variety of planning triggers that can be used to implement the move to NFV:

- EPC expansion to accommodate ever increasing data traffic
- VoLTE introductions
- New mobile enterprise services
- IP provider edge services
- Introduction or expansion of M2M networks and services

Capacity of mobile core networks continues to grow in and around the EPC (Enhanced Packet Core). This creates both a need and an opportunity to deploy capacity in an innovative way to create dynamic network segments for “tenants” such as Mobile Virtual Network Operators (MVNOs), cost-sensitive services such as M2M or major enterprise customers. NFV can define the network “slices” or by effectively creating a virtualized core (essentially a virtualized EPC) for each service, with each virtualized EPC engineered for requirements of the specific service. This can involve a few or many components of the core, such as Mobility Management Entity (MME), Policy and Charging Rules Function (PCRF), Authentication, Authorization and Accounting (AAA) and Home Subscriber System (HSS), as well as user plane-components such as Serving Gateway in an LTE core network (S-GW) and Packet Data Network Gateway in an LTE core network (P-GW). Because the user plane often presents a bottleneck or limitation on traffic control, the S-GW and P-GWs can be virtualized and run separately for each service providing independent control and scaling per end customer.

VoLTE has started deployment in North America for both voice and rich services. Because many of the IMS components are primarily software-based control functions, nodes such as Call Session and Control Function (CSCF), Media Gateway Control Function (MGCF) and SGWs and messaging and telephony apps are software components and become good candidates for virtualization. As VoLTE demand grows, operators can use NFV frameworks to flexibly grow VNFs capacity to meet that demand.
For mobile enterprise services, operators can leverage NFV to accelerate time to market for services to support the increasing demand for access to enterprise applications from a diverse set of nomadic and mobile devices. It’s key to have a flexible, efficient and automated way to configure and deploy new services to manage the increasing mobile workforce. One example could be deployment of a specific enterprise VPN security package to connect a mobile workforce through a commercial mobile operator network. This requires some capacity and capability in the mobile core network, as well as the specific applications and virtualized appliances that can also be configured and deployed using a NFV framework. This could range from virtualized security services all the way to enterprise-dedicated Access Point Name (APN) and P-GW instances.

2.3 MANAGING A LEGACY-TO-NFV EVOLUTION

The adoption of the NFV framework is a transformational journey for each operator that will take time to adopt across the network infrastructure, personnel and processes. The transformation speed may be limited by training and other personnel matters rather than technology or capital. This can result in a hybrid network with cloud and legacy elements coexisting and interacting over a long period, if not within operators, then certainly between them. This hybrid nature can impact the operator’s cost-benefit analysis and should be taken into account very carefully when planning for resources and capital as well as setting expectations for Return on Investment (ROI).

Interoperability of the NFV and legacy elements is not expected to be a significant impact as the 3rd Generation Partnership Project (3GPP) interfaces remain untouched. In that sense, NFV is an underlay, where the 3GPP functions can be deployed as tenant application VNFs. The more significant impact is on the operational side in aligning the legacy and NFV environments. Troubleshooting and issue resolution of a NFV element versus a traditional element will be very different, and care has to be taken in designing the new hybrid workflow.

The adoption of NFV is also a transformational journey for infrastructure vendors. A direct approach of migrating an appliance into an equivalent VNF may seem attractive for some deployments, such as to minimize the impact on related OSS systems. The history of virtualizing functions as experienced by other industries suggests that this is an initial step of product migration that many equipment providers will take. The ecosystem of VNF providers is not, however, limited to existing equipment providers. New market entrants familiar with the enhanced capabilities of cloud infrastructures to support scaling and resiliency may choose to design their VNFs differently [13].

More discussion on managing transition from legacy to NFV implementation is covered in later sections of this paper.

2.4 TIMELINE TO A POSITIVE ROI

The identification and sequencing of functions to virtualize is a significant factor in the time to a positive ROI. The virtualization of network functions is analogous to the migration of existing IT functions onto a cloud infrastructure. Although there are many technical considerations in such migrations, the business strategies underlying the migration determine the ROI. Business strategies are generally developed considering both profit opportunities and risk mitigation. The flexibility afforded by NFV architectures in trialing potential new services can be reflected in the Total Cost of Ownership (TCO).

\[2\] Considerations such as those in ODCA’s Master Usage Model: Business Strategy Enabled by Cloud Rev1.0 (2014) may be relevant.
When looking at the cost-benefit ratio of introducing the NFV architecture, it is important to have a comprehensive view of the timeline for adoption in order to maximize the commercial benefits of the operational transformation to cloud-enabled automation. Careful analysis of the PMO costs is very helpful. This will provide the unique roadmap to long-term benefit to the operator by targeting the largest budget items in the present mode of operation.

Certainly at the functional level, immediate benefits of migrating to the NFV architecture can be realized, but higher-level network benefits have to be prioritized and considered carefully when developing the expected/required ROI view.

2.5 COMMERCIAL DEPLOYMENT CONSIDERATIONS

From a commercial perspective, NFV poses both opportunities and challenges. Although a complete equipment replacement is a clean technical solution for NFV implementation, it is not necessarily a viable approach from a business point of view. A green field NFV deployment may definitely be a solution to envision, but it may not be a viable case for an established operator with legacy networks. The cost for large-scale equipment replacement is probably too high, not to mention the service interruption potential for customers. Waiting to deploy NFV elements until legacy platforms’ end of life is not necessarily the best approach either as it leads to a long, drawn-out transition period to NFV, but it is more manageable than a complex total rip and replace.

A “cap and grow” scenario may by another option and can also allow some smaller amounts of traffic to pass through the new platform as the technology and operational processes become established.

Finally, consider cases of local coverage solutions for specific customers. As this is a kind of network-in-a-box solution, it may be worthwhile to use NFV for a more cost-efficient implementation, as there are fewer interactions with the operator networks’ nodes.

As there is pressure on the carriers to reduce CAPEX and OPEX costs immediately, this may become a higher priority driver than the ability to support new service applications as a means to generate new revenue streams. To ensure maximum cost optimization and optimal transition towards NFV, it is important to architect the transition with careful planning.
This section outlines the key characteristics of an NFV architecture based on the collaborative work carried out within ETSI and key industry players. It focuses on the key considerations of a service provider when laying out and implementing a NFV roadmap in a multi-vendor, open-source ecosystem where new implementations exist alongside transforming legacy implementations. Key considerations are interoperability, reliability and performance, as well as scaling and sharing of resources in a cloud environment.

3. MAJOR ARCHITECTURAL CONSIDERATIONS AROUND NFV

One of the ETSI’s NFV goals is to create a structure where key network capabilities can be decoupled as VNFs from the infrastructure (NFVI) on which the VNFs execute, enabling the VNFs to scale when necessary. ETSI describes a VNF as a network function capable of running on an NFVI and orchestrated by a NFV orchestrator (NFVO) and VNF manager. It has well-defined interfaces to other network functions, the VNF manager, its element management system (EMS) and the NFVI, as well a well-defined functional behavior.

A VNF may:

- Implement a single network entity with interfaces and behavior defined by standardization organizations such as 3GPP or IETF
- Be deployed as a set of virtual machines, in which case internal interfaces between VMs do not need to be standardized
- Be structured into components called VNF components (VNFC)
When it comes to managing and automating this new and complex environment, integration with a versatile and operator-friendly cloud-management solution is critical. ETSI distinguishes between three main management functions in its NFV architecture for management and orchestration as shown Figure 5.

Figure 5. ETSI NFV Management and Orchestration.

The Virtual Infrastructure Manager (VIM) includes the NFV orchestrator and the VNF manager (VNFM). A VIM controls and manages the NFVI compute, storage and network resources. It exposes the underlying physical infrastructure as IaaS. OpenStack is one example of the role of a VIM that many operators are exploring.

The NFV orchestrator orchestrates NFVI resources across multiple VIMs and is responsible for the lifecycle management of network services. Service catalogs and inventories are held here.

A VNF manager should be as generic as possible, handling lifecycle management of the VNF under the control of the NFVO. Each VNF instance is assumed to have an associated VNF manager, which may be assigned for the management of a single VNF instance, or the management of multiple VNF instances of the same type or of different types. Most of the VNF Manager functions are assumed to be generic common functions applicable to any type of VNF. However, the NFV-MANO³ architectural framework needs to also support cases where VNF instances need specific functionality for their lifecycle management in particular when it comes to the deployment and scaling of complex VNFs. In these cases, the VNF manager has to understand the particulars of the VNF and is tightly coupled with it. Consequently, in many cases there will be a VNF manager per VNF provided by the VNF vendor. In a real-world scenario, this will lead to a multitude of VNF managers from different vendors (depending

³ NFV_MANO refers to the Management and Orchestration specification from ETSI NFV ISG.)
on the operator’s VNF choice) that need to integrate with different VIMs and orchestrators. Clearly defined interfaces between these functional blocks are important to avoid integration complexity.

3.2 AGILE SERVICE INTRODUCTION AND EVOLUTION

In recent years, people have come to expect anytime, anywhere access to business and consumer applications and services. That expectation is changing mobile operators’ service models. They need to incorporate business applications, video streaming, user-generated content and Internet video across a variety of fixed and mobile platforms requiring higher data speed. Today’s powerful and feature-rich mobile devices serve as e-commerce and entertainment platforms in addition to their traditional role as communication devices. This evolution necessitates deployment of new applications such as mobile TV, online gaming and personalized video. NFV can be very effective in supporting these scenarios, where operators are rapidly introducing new services in the network to meet emerging demands from consumers and businesses. The network architecture can be defined, and necessary integration work required to realize the service feature can be done more quickly. Hence, the services can be launched in multiple markets simultaneously.

NFV can assist in an easier evolution of an operator’s network though new ways to introduce software upgrades, corrections, testing and new service introductions. NFV will enable more effective rollouts of software supporting new services in the network. Software release upgrades can be done in the network more frequently, with the ability to support multiple version of software in the production and pre-production environments across multiple server instances. The integration testing with different network elements can also be done in multiple environments.

Major and minor software corrections can be tested and deployed in the network much easily in a controlled manner. Operators could manage more frequent network software upgrades in the network for adding new features and services. Testing and deployment of new services could be done using smaller, controlled DevOps-style NFV environment so that necessary changes can be migrated easily in the network.

3.3 ARCHITECTURAL CHALLENGES AND OPPORTUNITIES IN MULTI-VENDOR NFV ECOSYSTEMS

The benefits of NFV will likely be realized in a more “open ecosystem”, which is the ability to integrate VNFs from multiple vendors with other third-party NFV orchestrators and NFV VIM/NFVI. In addition, some common software functions may be taken from the open source community or open source distribution suppliers. Furthermore, different vendors VNFs shall be able to be deployed on the same NFVI. This increasingly diverse multivendor architecture has many implications.

For example, this architecture may add complexity to well-defined 3GPP interfaces which is why published interfaces and vendor interoperability partnerships are essential to achieving cost reduction in deployment. Common Representational State Transfer (REST) APIs, such as those provided via open source, can be key for mitigating this issue.

Also, when considering a multi-vendor approach for hardware, hypervisors and virtual appliances, operators need to consider the system integration efforts and node level performance, reliability and resiliency implications.

Integrated nodes with open platforms still need to comply with typical requirements around Service Level Agreement (SLA), performance and reliability through certified hardware-software combinations. A more diverse multivendor approach to the hardware, software and virtualization layers will leave these types of commitments up to operators, their solution supplier or their system integrator.
From the design perspective of a new mobile network service utilizing the NFVI capabilities under an open ecosystem, the high-level functional principles must be carefully assessed and monitored:

- **Scaling service** – Do the combination of functions that compose the service limit the service chain’s scalability and flexibility?
- **Intra-service dependencies** – Are there interface and functionality dependencies within the chain?
- **Session data sharing** – Do all functions in the service chain have the same view of session information and traffic data? For example, can all the functions access the user’s identity or data consumption limits?
- **Virtualization technology dependencies** – Are there specific dependencies on the virtualization technology?
- **Interoperability** – As software is changed, patched and upgraded, it must be certified as working together not just functionally but also to a degree of scalability that makes the service chain workable.

### 3.3.1 SCALING SERVICES

The definition of a service chain or forwarding graph is fundamental to taking full benefit of network virtualization. As services scale, each function in a chain may scale linearly or be integrated in a loosely coupled design principle. In any case a single function in a chain must not become a performance bottleneck or a single point of failure, and this requirement must be addressed at design time. Service scale must also consider the aggregated latency of the service chain. Physical traffic flows have to be designed carefully in the elastic deployment of service chains, and the design process must remember that some services in the chain may require flow affinity \(^4\).

### 3.3.2 INTRA-SERVICE DEPENDENCY

By definition, a chain provides a composite discrete overall function. In the past, if the composite functions within a chain are interdependent in terms of version, then this can negate the future evolution of services. Today, loosely coupled designs can prevent this limitation and thus add a new level of agility to the designs of network service chains. One of NFV’s key aspects is faster time to market for new services. If services are interdependent by version then, potentially, multiple vendor roadmaps will be interlocked, and this is a complexity that requires proper management, communication and cooperation.

The development of loosely coupled interfaces then becomes an important priority to enable independent evolution and scaling by advance planning of proper vendor-interoperability scenarios. Responsibility for this interoperability and verification needs to be identified early on. Other challenges include service chaining and the development of service chains in multi-vendor environments. Examples include the demands on the physical layer, the management of service chains, the processing of both data plane and control plane information and the development of new expertise in the operation of dynamic cross-domain operational environments.

---

\(^4\) Flow affinity refers to assign a data packet flow to a specific CPU, NIC or resource (hash distribution) instead of a default flow distribution based on round-robin, for example.
3.3.3 SESSION DATA SHARING

The application of individual service functions in a chain can also be dependent on the policy or other related control information. Ideally each function in the chain should not need to access control/session information separately. Instead, a common mechanism needs to be defined to share data between virtualized functions in a chain to avoid control plane overload or unnecessary latency. In addition, the definition and purpose of functions within a service chain and the chain itself needs to be considered carefully in the design (service granularity principle). Defining these at a too-granular level will lead to a number of integrations and/or interfaces potentially established (and torn down) between service nodes. That can affect the service chain’s orchestration and have a ripple effect on the reliability or performance issue of the platform as a whole.

3.3.4 VIRTUALIZATION TECHNOLOGY DEPENDENCIES

The development of low-latency services using virtualization as an abstraction layer to take advantage of COTS hardware is one of the key challenges in architecting solid NFV platform architectures. Interdependencies to mitigate this impact can lead to dependencies on specific technology implementations of virtualization. More details are provided in the “Performance on Virtualized Deployments” section below.

3.3.5 INTEROPERABILITY

In a multi-vendor service chain, adherence to open standard interfaces from a data sharing and management capability is key to driving open interoperability. However, ultimately vendors in a service chain need to establish interoperability with real implementations.

Managing the evolution and operation of legacy network integration together with VNF and IT cloud applications is important. Multiple virtual infrastructure managers and orchestrators might exist in parallel for the different domains (IT, telco, and public cloud) even though this is not the desired state and will require cross-domain orchestration. Cross-domain orchestration currently is common in the OSS above the orchestration layer.

As operators consider putting together multi-vendor layering inside network nodes, verification and certification responsibility moves to the operator or system integrator partner, or it will lead to a smaller number of verified and certified stacks. These “multi-vendor inside” nodes then must be integrated according to the 3GPP multivendor node-to-node integration specifications/standards. With the introduction of multi-vendor layers that also spans NFVI, VNFs and MANO elements, a multitude of combination and configurations needs careful management. Continuing the analogy between VNF migration and migration of existing IT applications to clouds, it may be relevant to consider best practices [13] in the design of applications for cloud environments. More details are provided in the “Software Design Considerations in NFV Evolution” section below.

Planning for demanding VNF application performance may require agile but optimized infrastructure (or even PaaS) designs for different levels of performance, throughput and storage (types and speed) requirements.

Some multivendor PoC projects are experimenting across open-source players working with Linux, KVM and OpenStack. Trials also include integrating some of the latest Intel advances in Intel® Data Plane Development Kit (Intel® DPDK) and the standard Single Root I/O virtualization (SR-IOV) capabilities that help optimize throughput and performance together with the x86 architectures. Figure 6 illustrates an example architecture that has been used to demonstrate feasibility.
3.4 RELIABILITY AND STABILITY GUARANTEES

VNF’s key objective is to ensure service continuity rather than focusing on platform availability, whereas the service-continuity level required will be below the recognizable level, and service recovery is performed automatically. Here the expectations differ from those on typical applications in the IT domain, where outages lasting seconds are tolerable and the customer typically initiates retries. However, not every VNF has the same requirements for resiliency.

Due the nature of VNFs being deployed in virtual environments, the focus does not have to be on hardware availability. Instead, software availability and network functions shall be designed to handle failure rather than focusing on uptime. This depends on a large extend on the nature of the VNF being deployed and the particular vendor’s implementation of that function relative to awareness of the underlying hardware or NFVI infrastructure capability or redundancy design.

Top-level design criteria that need to be fulfilled by VNFs include service continuity and failure containment, automated recovery, preventing a single point of failure in the underlying architecture and supporting a multi-vendor environment and hybrid infrastructure. When deploying complex sets of VNFs in a common NFVI, considerations must be made on how many and which VNFs are deployed across common or separate physical hardware elements. The concept of creating “affinity” and “anti-affinity” rules when orchestrating the deployment of VNFs across the virtual and physical infrastructure is important to reduce the potential of an outage if a single piece of hardware or virtualization software fails. Affinity rules and anti-affinity rules are used to keep virtual entities together or separated. Affinity rules can help reduce traffic across networks and keep the virtual workload balanced on available hosts. If two virtual machines communicate frequently and should share a host, they can be kept together. Conversely, if two resource-hungry VMs would over-tax a host, an anti-affinity rule will keep those VMs from sharing a host. Anti-affinity rules are also important to secure availability of a virtual machine in a redundant setup and not have them executed on a single host or even rack.
In a virtualized environment, service resilience is a key factor. This provides the ability to maintain an acceptable level of service at times of faults and challenges comparable to traditional network operation.

The same mechanism to achieve service resiliency and availability in physical deployments such as distributed processing, geo-redundancy or replicated network storage can be used for VNF. In the virtual domain, deployment is automatically controlled through orchestration and management. Orchestrator, VNF manager and infrastructure management coordinate deployment of VNF based on resource availability, requested SLA and can optimize resource consumption, service performance and availability based on a current as-is situation. A higher degree of flexibility is possible at the expense of management complexity.

3.5 PERFORMANCE ON VIRTUALIZED DEPLOYMENTS

Performance and networking capabilities supported by the virtualization environment play a critical role in supporting the real-time requirements of many of the VNFs found in mobile networks’ control and bearer elements. The NFV platform of choice must be ready to interoperate smoothly with a hybrid hypervisor environment because a large NFV adoption is unlikely be uniform in hypervisor support. Choice must always be available in open-standards platforms.

The industry is moving to address the challenges of determinism and latencies in the virtualized environment; most, if not all, are targeting NFV. A few initiatives to mention are related to improving VM-to-VM performance and reduced latency due to interruption. There are also offerings that enable different hypervisors to work with different controllers and VIMs. Not all the challenges are believed solved, such as interoperability and real-time scaling. Performance requirements are necessary to drive the industry, but it is not clear what the target for real time should be.

Performance and throughput are quite different between control planes and data planes and require different levels of deterministic performance. In an LTE network, signaling nodes such as a Mobility Management Entity (MME), a PCRF and CSCF might accept a “small” performance degradation, which can be resolved by scaling up the number of control plane instances for these nodes. On the other hand, nodes requiring a high packet-processing rate and/or media transcoding, such as a P-GW or an SBC (Session Border Controller), require innovative solutions to reduce the virtualization impact when deploying these applications on generic COTS servers.

When it comes to varying degrees of binding the application software to the OS or the hardware layer, there are still multiple approaches. These vary from fully virtualized VNF/NFVI to combinations of virtualization with bare metal OS/networking all the way to specialized appliance type implementations. Each alternative comes with a different cost/performance expectation. In certain cases specialized hardware/software solutions can often significantly outperform COTS based solutions, but only for a specific service or application, but can come at a higher cost and reduced flexibility.
According to the Heavy Reading analyst report “Bringing Network Function Virtualization to LTE,” operators are willing and even desire to use COTS servers for the data plane. Where the issue is simply raw throughput, operators generally think COTS’ cost advantages make it feasible to grow by adding more servers. When it comes to deterministic packet processing, such as in an EPC S/P-GW, operators are somewhat less confident in using general-purpose CPUs in combination with hypervisor. Figure 8 illustrates this operator feedback.

3.6 SCALE-UP VS. SCALE-OUT / SMALL VS. LARGE DISTRIBUTION

During a VNF’s lifecycle, different Key Performance Indicators (KPIs) can be monitored and evaluated within the execution environment or by the VNF or its related VNF manager. Scaling operations can be triggered based on the measured KPI or criteria such as time of day. Trigger criteria can be very simple and directly relate to used virtual machine resources such as CPU load and memory consumption. In this case, generic functionality in the cloud management and execution environment can initiate scaling.
In general, two types of scaling can be distinguished: vertical scaling (scale up/down) and horizontal scaling (scale out/in). In the case of a VNF scaling up or down (vertical scaling), configuration of the virtualized resources are changed, and either capacity such as the Central Processing Unit (CPU), memory and networking is added or removed from the virtual machines executing the VNF. When scaling out or in (horizontal scaling), new virtualized machines are added or removed from a VNF. Here new virtual machine instances are started or shut down and released from the pool of instances executing a VNF.

Both types of scaling are possible within a single VNF where parts might benefit more from additional resources while others can share load better when being replicated. VNFs must be carefully designed [13] to support removal of resources from operational instances. Consequently, VNF needs to be architected in a way that allows scaling components individually using either scaling type.

Both types of scaling have advantages and disadvantages:

- Vertical scaling (scaling up) is often easily implemented and requires no changes to the application architecture. In particular, when state needs to be managed, vertical scaling has advantages in order to avoid a more complex application architecture and management. No or very little impact is seen on OSS and BSS. Adding or removing resources from a node might require changes to the configuration and mechanism to make this effective while running. Vertical scaling is limited to the capacity of the underlying hardware, and scaling beyond that capacity often involves downtime and comes with an upper limit. In case of failure, the impact might be higher compared to one node of a horizontally scaled application failing.

- Horizontal scaling (scaling out) enables dynamic scaling by adding more machines into the existing resource pool. It enables Web-scale deployment and distribution of nodes across the network closer to where the load is. It also minimizes the impact of individual node failure and can speed up recovery. Management complexity can increase depending on the characteristics of the application both inside the application and towards OSS and BSS. In cases where state needs to be managed and kept, logic needs to be implemented that distributes state when scaling out and evacuates it when scaling in to ensure session continuity. State distribution among the nodes needs to be managed for high availability and resiliency. As a consequence, VNFs need to be architected for horizontal scaling to fully benefit from the potential advantages. This includes avoiding state where possible and moving toward smaller VNF components that can be scaled and potentially distributed individually. VNF management also has to ensure that OSS are aware of scaling activities. New virtual machines need to be monitored, and in case of scaling in and removal of virtual machines, no alarms need to be triggered on the OSS side.

From an operation point of view, any mobile operator would like to run its business at scale by allocating and optimizing resources to drive the greatest results and volume of traffic across the different integrated platforms. One use case related to operations could be to deploy NFV-based architecture to scale the mobile network resources up and/or down based on the network’s needs rather than planning for the worst-case scenario. This would address temporary increased customer demand for products and services, such as a retailer during the holiday season or for a promotional campaign. It would be similar to using Amazon Web Services to enable increased server capacity (scale up) when network use demand is high without having to invest in new hardware. Operators could then reduce server capacity (scale down) when returning to normal operating periods. This ability to offer products and services would let operators pay only for what they need and only when they need it. At times when resources are scaled down, the extra NFVI resources can be utilized for other purposes. The scaling up and scaling down could possibly be automated based on the various services’ demand.

Another NFV implementation example is the deployment of smaller scale network nodes. Often an operator has limitations in improving services to its customers because of the lack of scalability of its vendors’ products. Use of
high-cost, high-capacity network platforms may not be workable in low-traffic areas, which would nevertheless be better served by deploying local network nodes. NFV may provide the required flexibility when deployed over a COTS-based platform. The improved scalability due to the use of COTS, coupled with NFV, could allow the operator to offer improved services in a cost-effective way.

With virtualization and transformation of network functions, consolidation is taking place, and the number of data centers is significantly reduced. Still, some network functions benefit from being distributed in the network. Here horizontal scaling can mean not only more virtual machines in a single data center but also distribution of these across the network to where the workload is best processed. Examples are distributed analytics, IoT use cases or applications that have peaks in different geographies at different times of the day and “follow” the workload.

### 3.7 SHARED NETWORK INFRASTRUCTURE

NFV can provide a different layer of “ownership” where “tenants” can own their virtual nodes and virtual network. This can be realized by creating an internal IaaS/PaaS that supports VNF multi-tenancy and interconnect. This multi-tenancy can refer to different internal VNF domains that are tenants on the NFVI or could refer to literal external users who are tenants on a shared NFVI infrastructure. A Mobile Virtual Network Operator (MVNO) is an example of a tenant.

An operator network can be described as a set of solutions, such as an EPC or IMS/VoLTE, split over multiple organizational domains. In turn, these domains consist of sets of telco applications that interconnect using site NFVI (and legacy) infrastructure, such as switches, routers, firewalls and transport networks.

When a network is described virtually, each organizational domain within the operator becomes a tenant of the shared cloud infrastructure, which provides Virtual Data Centers (VDCs) that serve as resource containers and zones of isolation for the tenants. The VDC concept can be articulated as a managed collection of computational, storage and networking slices provided to a tenant by the cloud infrastructure from its pool of resources, which may be distributed across a set of data centers. Resources assigned to a given tenant are isolated from other tenants, but they can be interconnected through external networks and other VDCs. The tenant determines how this interconnection takes place on the basis of their security policies.

The cloud infrastructure fulfills the interconnect capability, along with other infrastructure requirements that are provided by site infrastructure and transport networks in non-virtualized environments. Interconnectivity needs to be maintained between virtualized and non-virtualized networks, and the domain managers (OSS) for operator solutions need to be able to manage dedicated infrastructure as well as virtual resources. These systems and applications place tough demands on the networking capabilities of cloud infrastructure. This is because telco system requirements are much more stringent and varied than generic IT applications. Typical telco systems need support for:

- Multiple routing contexts and routing protocols
- Multiple VPN connections to external networks
- Packet load balancers to manage heavy payload applications that cannot be managed by application delivery controllers (ADCs)
- Support for virtual network interface cards (NICs) to trunk large numbers of VLANs and interconnect to external networks
- Path diversity
• Service chaining for transparent bump-in-the-wire applications
• Security zoning
• Complex routing between tenant networks
• Geo-redundancy mechanisms.
• Latency/QoS control

In traditional networks, these features are provided by the site infrastructure. In the NFV context, these features need to be replicated by the cloud infrastructure (NFVI) in such a way that they can be orchestrated. That is because orchestrated features can be exposed through appropriate abstractions, as well as being coupled with advanced support for discoverability and traceability.

An IMS core network is based on standardized interconnected logical functions whose operation in a virtual data center would be supported by additional infrastructure-related functions such as firewalling and load balancing. Cloud deployment creates the possibility to implement multiple instances of IMS core networks to serve different tenants by utilizing the cloud infrastructure’s multitenant capability. The set of telco VNFs that implements a given tenant’s IMS core network is deployed in the VDC dedicated to the tenant. An example of such deployment is illustrated in Figure 9.

![Figure 9. Multitenant, Multi-Instance IMS Network in VDC.](source: Ericsson [6])

Tenants are deployed over a shared cloud infrastructure in which the networking solution guarantees tenant separation, thus fulfilling security requirements and fair use of resources.

As Figure 9 illustrates, the requirements placed on the cloud infrastructure are complex. Advanced Virtual Local Area Network (VLAN) handling for telco VNFs is required, as is path redundancy, the ability to cope with large numbers of VLANs for SBG access, interconnect for multiple enterprises and routing and complex interconnect with legacy networks/VPNs. All of these requirements not only need to be implemented; they also need to be automated. The functionality provided by the virtual data center needs to cover all of these aspects, on top of providing true tenant separation, real-time performance, geographical distribution and telecom-grade availability.
Automation and dynamic management are key elements of providing a cloud offering as a service based on an IMS core.

### 3.8. KEY CONSIDERATIONS FOR IMPLEMENTING NFV ARCHITECTURE

NFV and related SDN transformation also introduces some unique challenges that need to be considered. There will be a competence and complexity shift from physical to logical complexity in both technology and operations. Network functions that were once based upon physical appliances installed in physical network topologies will become virtual applications tied to physical assets that may be located in different areas of the network depending upon capacity demand, functionality and frequency of use.

The realities of telco-grade performance, SLA, reliability, high availability, geo-redundancy and legacy regulatory and compliance requirements are still valid and will not be sacrificed with NFV even though the mechanisms used to deliver these services may be quite different. However, a few open questions remain to be addressed, such as:

- What (if any) are the performance differences between the NFV technologies as applied to traditional IT applications verses telephony/wireless applications?
- Are all virtualized telco/wireless network element functions subject to the same level of performance requirements? For instance the virtualized subscriber data (HSS) function may need a much higher level of availability than a virtualized switching function (S-GW) because the HSS function supports a large number of virtualized functions and users. By comparison, the inability of accessing a virtualized S-GW instance would impact only a single user.

Maintaining and complying with these kinds of requirements will not be solved by open platforms and virtualization alone. Performance indicators will be more measured on the service and end-user levels rather than inside the different underlying technology layers that provide the service. That puts higher demand on management, orchestration and OSS. Each operator’s network will have unique topologies, deployment models and operating environments that drive unique architectural and operational requirements. Being able to achieve real-time performance with flexibility and scale is a significant challenge.

### 3.9 NFV ROADMAP STRATEGIES

NFV roadmap strategies can span many areas of 4G networks depending upon each operator’s evolution and modernization strategies. LTE operators currently are early stages of NFV implementations from many different starting points:

- EPC (P/S gateway, MME).
- IMS core, VoLTE IP core routing, switching.
- SGi services (e.g., DPI, policy control and enforcement).
- Scale and agility in IP access (router, gateway, IP services).
- Enterprise services modernization (e.g., mobile VPN).
- OSS and BSS.
- CPE (mobile broadband routers, enterprise gateways).
- M2M networks.
Each of these areas demonstrates different characteristics that might drive motivations to move to an NFV architecture. Different strategies are being explored by different operators:

- Start with Greenfield network elements, regardless of whether they are centralized or distributed. Examples include VoLTE or M2M network infrastructure builds.
- Areas in need of immediate modernization or optimization. Examples include IP access and network-edge services or mobile enterprise VPN services that currently require long time to market.
- Areas of the network that will be severely impacted by rapid mobile broadband data growth and can benefit from early maturity in VNF areas. Examples include virtualized appliances, load balancers, routers and firewalls.

The availability, location and capacity of NFV infrastructure must also be considered. Mobile operators must decide when to make the investment and commitment to the hardware and software infrastructure required to support a common telco network/IT platform for deploying the next generation of VNFs. This investment will increase the NFV initiatives’ initial costs and must be taken into account as part of the initial investment for the first set of functions. Benefits such as reduced CAPEX and operational efficiencies will outweigh initial costs when a critical mass of network functions are virtualized and share a common execution and management environment. Benefits can significantly increase when the focus goes beyond just NFV toward one environment that also supports IT.

Improved service agility, time to market and differentiation for new services also need to be considered when outlining the NFV roadmap. For example, the enterprise service roadmap can provide input and motivation to the virtualization technology roadmap. New offerings should be based on virtualized network functions and should also help identify services or components that can be re-used in different offerings. The components can establish the foundation of a service platform (PaaS) for future offerings. Openness of these services and platforms through APIs is also key to rapid applications development and deployment.
Financial aspects such as TCO, new revenues and net present value will be key in operators’ decisions to move to a cloud deployment model. Avoiding double OPEX connected to initial deployments will be as important as minimizing risk. It will be crucial to ensure that gains through platform consolidation, higher utilization and increased automation will not be offset by increased software, system integration and verification costs.

3.10 WHICH NODES BENEFIT THE MOST FROM A COMPLETELY VIRTUALIZED ENVIRONMENT?

Assessing the benefits from virtualizing a particular node, network function or application requires calculating TCO. This analysis needs to consider the cost or complexity to virtualize and the expected gains and benefits, which is not an easy exercise. Many factors can play a role and cost and benefits rise with the ambition level when virtualizing. Cost and complexity come from the effort needed to decouple and virtualize and to maintain and guarantee required performance characteristics on top of a virtualized infrastructure. Cost can also increase when requiring additional application characteristics that impact application and infrastructure management and ultimately the organization and needed skillset of the individual in the organization. The operator’s strategy to incorporate multiple vendors in the layers of a network element also create new skills and capabilities to verify and certify node level performance and SLA once the various vendor elements are integrated.

Benefits depend on cost savings due to resource sharing, reduced infrastructure CAPEX, rapid deployment and additional characteristics that can come through virtualization, such as automated scaling or that enable business agility and shorter time to market for new offerings.

Typically applications already running on standard x86 platforms can be virtualized easily and be deployed on a virtualized infrastructure. The less business-critical they are and the lower their performance requirements the lower is the cost of virtualization making them natural first choices. OSS and BSS, as well as non-real-time media applications, are in this category as shown in Figure 11.

![Figure 11. Risk vs. Value in NFV Virtualization.](source: Ericsson Review, July 2014 [7])
With increasing application complexity, required performance guarantees and ultimately hardware dependencies, these elements are more of a challenge. Core and edge routers and the access network elements tend to be in this category. These elements are generally much more involved in the data plane where high data throughput and very low latency are required. However, the ETSI NFV, and other Forums are looking to address these challenges. For instance, over the air C-RAN virtualization ETSI PoC has been demonstrated at MWC 2014. Value of virtualization increases as shown by the announcement of ETSI Mobile Edge Computing [14] for services in the Wireless network.

3.11 SOFTWARE DESIGN CONSIDERATIONS IN NFV EVOLUTION

When assessing how virtualization of network functions is accomplished, operators can benefit from experiences in migrating other software applications on a cloud infrastructure. Speed of telecom network virtualization is still in the early stages relative to segments such as IT applications and media/CDN services. Some systems have already started to large degree and are moving very fast, whereas others will take a very long time. Telecom’s NFV transformation will be a long, evolutionary process with some revolutionary steps along the way. Learning from transformation in IT, OSS/BSS and media solutions will all benefit the telecom NFV transformation. Along the way, it is important to assess the alternatives in evolution and migration of VNF applications to the NFVI. The applications themselves must also be sourced from existing or new vendors and be deployed based upon an understanding of how these applications are designed against the new generation of NFVI.

For most there are three basic approaches: porting, redesign and design from scratch. Porting is a natural first step for existing applications. They get virtualized and can be deployed as a virtual machine image on top of the now virtual infrastructure. Porting is difficult for applications that have a very tight dependency on the underlying hardware to guarantee performance and availability characteristics. In many cases, porting of complex applications requires significant additional effort to enable wanted behavior such as easy or automatic deployment and scaling.

Industry best practices [13] suggest application redesign to provide for scalability, reliability and so on, and to deliver more configurable and optimized solutions. In this case, different design patterns and guidelines would be implemented and applications architected for this new environment. These applications benefit from maintaining their features and requirements as a network function, but wherever possible, they take advantage of the new capabilities of the NFVI and MANO evolution.

New applications designed from the beginning for cloud-based infrastructure can maximize the new capabilities of the NFVI. However, these new applications must also go through rigorous feature, requirement and interoperability certification and testing required of any network function going into a mission critical role in an operator’s network.

3.12 ECOSYSTEM OF SOLUTIONS AND SERVICES COMPLEMENTING AND SUPPORTING NFV ARCHITECTURE

Multiple operators, vendors and services companies are engaged in proof-of-concept testing to verify and validate NFV’s various aspects. ESTI ISG has identified a set of proof-of-concept activities supporting the general NFV ecosystem. A number of these proof-of-concept activities are relevant to various mobile operator considerations and use cases. This paper’s appendix lists proof-of-concept use cases as of September 2014.

OPNFV is a new open-source collaborative project in the inception phase aimed at achieving the ETSI ISG NFV architecture and use cases. It is established based on the intention of the ETSI NVF Phase 2 work to have an open-source realization of the reference architecture. OPNFV’s main goal is to create reference solutions based
on standard high-volume platforms that demonstrate and validate key components of the NFV reference architecture to support one or more NFV use cases. Initially, the focus will be on NFVI. Other groups and vendors also support their own ecosystems and NFV/SDN labs activities and proof-of-concept/demo cases showcasing different early-stage use cases.

3.13 OPERATOR NFV STRATEGIES

3.13.1 TELEFÓNICA UNICA

As reported in Telecoms.com [10] “Telefónica believes NFV is an important and transformative technology,” said Enrique Algaba, Network Innovation and Virtualization Director at Telefónica’s I+D-Global CTO Unit. “We believe that the deterministic allocation of CPU, memory, I/O, and storage relative to a particular type of VNF is critical to delivering the predictable performance needed for telco-grade network functions. This new deterministic architecture transforms a generic cloud computing data center into a Telco Data Center capable of supporting NFV.” Figure 12 summarizes these and other benefits.

UNICA promises to offer real and permanent change for Telefónica’s network, transforming the company into a true digital telco. All this will reduce the time to market and accelerate the deployment of a new generation of services in the coming years, characterized by an overwhelmingly improved level of quality and personalization given that critical mass will no longer be necessary for implementation.

Telefónica has led the charge toward standardization for virtualization since its inception, participating alongside operators such as AT&T or Verizon in key international forums on two of the most important standards: SDN and NFV. In addition, the company has worked with all equipment manufacturers to standardize interfaces with existing legacy networks and interfaces between data and control layers.

Among the many capabilities offered by UNICA is the idea of multi-tenancy (where the same basic solution works for multiple organizations) or network as a service (NaaS), using pre-installed templates to deploy virtualized equipment in real time and with integrated resource management.
3.13.2 AT&T UDNC

The user-defined network cloud is a transformative initiative for AT&T. Integrated through AT&T’s wide-area network (WAN) and using NFV and SDN, as well as modern architectural and operational approaches, AT&T plans to simplify and scale its network by:

- Separating hardware and software functionality.
- Separating network control plane and forwarding planes.
- Improving management of functionality in the software layer.

Some highlights from AT&T’s Domain 2.0 white paper outline the important aspects of the company’s approach to the NFV landscape. Migrating AT&T businesses to a multi-service, multi-tenant platform implies replacing or augmenting existing network elements, which today are typically integrated to perform a single function. The replacement technology consists of a substrate of networking capability, often called NFVI, or simply infrastructure that is capable of being directed with software and SDN protocols to perform a broad variety of network functions and services.

This infrastructure is expected to be comprised of several types of substrate. The most typical type is servers that support NFV, followed by packet-forwarding capabilities based on merchant silicon or “white boxes.” However, it’s envisioned that other specialized network technologies also will be brought to bear when general-purpose processors or merchant silicon are not appropriate.

AT&T services will increasingly become cloud-centric workloads. Starting in data centers and at the network edges, networking services, capabilities and business policies will be instantiated as needed over the aforementioned common infrastructure. This will be embodied by orchestrating software instances that can be composed to perform similar tasks at various scale and reliability using techniques typical of cloud software architecture.
NFV infrastructure might differ from a commercial cloud or an enterprise IT cloud. AT&T expects a high degree of reuse of the same software components and footprint with commercial cloud offers. It also expects that there will be functional or engineering tradeoffs that are different in the NFVI and wants to think of these as separate. AT&T identified the top likely differentiators: footprint/distribution, separation of data, control and management, and throughput intensity. Other differences include software and software architecture maturity, latency, support for some specialized hardware and the overall range of workloads supported. Despite these and other potential differences, there remains a strong need to leverage common infrastructure across a broad variety of VNFs, as well as a desire to get to the point where this infrastructure is provisioned in pods rather than the traditional methods of racking and cabling equipment individually.

SDN can act as an enabler for NFV because the separation of control and data planes enables the virtualization of the separated control plane software. NFV can also act as an enabler for SDN because the separation between data-plane and control-plane implementations is simplified when one or both of them are implemented in software running on top of standard hardware.

Table 1 identifies several significant operational shifts to consider [11]:

![Figure 13. AT&T's High-Level Cloud Networking Architecture.](image)

Table 1. SDN and NFV Operational Transitions.

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Centric</td>
<td>Software Centric</td>
</tr>
<tr>
<td>Separate IT/data center &amp; Network/CO</td>
<td>Common technology &amp; technical plant</td>
</tr>
<tr>
<td>Quarterly software releases</td>
<td>Continuous software process - “sandbox.”</td>
</tr>
<tr>
<td>Geographically fixed, single purpose equipment</td>
<td>Highly dynamic &amp; configurable topology &amp; roles.</td>
</tr>
<tr>
<td>Tight coupling of NE, generic, EMS &amp; NMS/OSS</td>
<td>Separation of physical &amp; logical components.</td>
</tr>
<tr>
<td>Separation of service elements &amp; support systems</td>
<td>Integrated orchestration, automation &amp; virtualization.</td>
</tr>
<tr>
<td>Faults as service failures</td>
<td>Faults as capacity reduction events</td>
</tr>
<tr>
<td>Hardware monitoring appliances</td>
<td>Software based monitoring.</td>
</tr>
<tr>
<td>Service specific resource combinations</td>
<td>Profiles, templates &amp; reusable resource combinations.</td>
</tr>
<tr>
<td>Special design and provisioning processes</td>
<td>Configurable catalog/rule-driven delivery frameworks.</td>
</tr>
<tr>
<td>Optimized provider network &amp; ops process</td>
<td>Optimized customer experience.</td>
</tr>
<tr>
<td>Highly constrained, independent &amp; disaggregated control planes</td>
<td>Highly integrated &amp; automated control planes driven by customer &amp; operator policies.</td>
</tr>
<tr>
<td>Limited service dimensions</td>
<td>Multifaceted service dimensioning.</td>
</tr>
<tr>
<td>Highly constrained data translation &amp; synchronization solutions for shared management knowledge between network &amp; systems</td>
<td>Shared management “Data Bus” technology between network &amp; systems.</td>
</tr>
<tr>
<td>Slow tooling changes requiring coding</td>
<td>Rapid tooling changes using polices/rules</td>
</tr>
<tr>
<td>Network management</td>
<td>Customer experience management</td>
</tr>
<tr>
<td>Long lead provisioning times – often hardware and process constrained</td>
<td>Real-time provisioning</td>
</tr>
<tr>
<td>Static billing and charging</td>
<td>Granular and dynamic usage-based charging, billing, financial management, subscription</td>
</tr>
</tbody>
</table>

3.14 STANDARD AND OPEN SOURCE ACTIVITIES

To enable and accelerate the commercialization of NFV architectures requires industry activities in both specification and open source development [14]. Among several of the industry fora and standards bodies, the notable ones relevant for this paper are ETSI, 3GPP, the Open Networking Foundation (ONF), OpenStack, Open DayLight, and OPNFV.

The ETSI NFV ISG is probably the world’s largest with over 220 companies participating in the development and standardization of NFV: www.etsi.org/technologies-clusters/technologies/nfv. In its first phase, the ETSI NFV ISG published six specifications in October 2013 in and will finalize and publish another 11 by the end of 2014. This NFV ISG is continuing for another two years to further develop the NFV ecosystem. ETSI has also recently initiated a second ISG to build Mobile Edge Computing applications on the NFV architecture [15].
The 3GPP standards work on virtualization is about to be started in Release 12. The initial focus will be turned towards O&M aspects. Work on core network and radio architecture is expected to follow later in Release 13.

The ONF focuses on improving networking through SDN through the standardization of the OpenFlow protocol and related technologies. (For more information, visit https://www.opennetworking.org.) It was born out of the recognition that cloud computing blurs the distinction between computing and networking, resulting in software playing the most dominant role to bring innovations quickly into the telecom networks. In addition to several white papers, the ONF’s key output includes the OpenFlow Standard, which enables remote programming of the forwarding plane. OpenFlow is at the core of the SDN technology and is an essential component of NFV.

OpenStack project is a collaborative effort on delivering free and open-source ubiquitous software cloud computing platform for public and private clouds, which can be deployed as an IaaS solution. It relies on pooling of resources from storage and networking throughout the data center and is accessed by the users through a Web-based dashboard, CLI or a RESTful API. For more details, see www.openstack.org.

The OpenDaylight Project is a collaborative open source project among 41 participating organizations that aims to accelerate SDN and NFV adoption by facilitating interworking between them. The project has released the first open source software called “Hydrogen” in three different editions: Base Edition, Virtualization Edition and Service Provider Edition. The software is a combination of components including a fully pluggable controller, interfaces, protocol plug-ins and applications. The northbound (programmatic) and southbound (implementation) interfaces are clearly defined and documented APIs. For more details, see www.opendaylight.org.

A new organization has been formed called Open Network Function Virtualization (OPNFV) under the Linux Foundation. This new organization seeks to create integration projects that combine upstream code from projects such as OpenStack, OpenDaylight and the Linux Kernel and combine them with extensive testing, custom configuration and possibly upstream code patches. OPNFV is aimed at realization of the ETSI ISG NFV architecture and use cases. It is established based on the intention of the ETSI NVF Phase 2 work to have an open-source realization of the reference architecture. OPNFV’s main goal will be to create reference solutions based on standard high-volume platforms that demonstrate and validate key components of the NFV reference architecture to support one or more NFV use cases. Initially, the focus will be on NFVI.
4. USE CASES

The primary NFV use cases are driven by the operator and vendor communities. The ETSI NFV initiative was originally established by a core group of operators looking to guide the industry on how to capitalize on the innovation happening in the IT industry relative to virtualization and cloud technologies, business models and ecosystems. This section outlines a few example use cases to demonstrate how NFV can be used to fundamentally change the way new services are designed and deployed into a 4G LTE network. These use cases enable operators to respond with agility and speed when traffic and service demands change over time or instantaneously. Additionally, they highlight the agility and efficiency in deployment of new revenue generating services through cost improvement and accelerated time-to-market.

Figure 14 identifies the key areas of mobile networks that can most benefit from the NFV transformation.

![Figure 14. Where NFV Has the Most Benefit.](source)

The following sections explore examples of LTE core network elements and how virtualization changes the way capabilities are deployed and how new services can be realized.

4.1 VIRTUALIZING IMS AND VOLTE

3GPP’s IMS has been considered to be a complicated and costly solution based on its complex, standards-defined architecture, where multiple functions and interfaces allow the required functional interoperability among all of them. This architecture inhibits scaling components and interface capacities independently. As mobile operators deploy IMS, there are dozens of functions that are instantiated into many traditional proprietary network elements. With a virtualized IMS solution, it is possible to instantiate these network functions or products into a very small COTS NFVI node to enable trials of new services or tests of new configurations. Mobile operators deploying IMS for the first time may evaluate several configurations to understand how the functionality will actually be implemented. NFV is not a departure from the established 3GPP standards but a profound optimization of the how-to of the physical deployment of its conceptual and logical architectures as software VNFs on COTS infrastructure.

With more and more mobile operators launching LTE networks and committing to RCS, demand for IMS looks set to rise to unprecedented levels. The IMS has matured into quite a versatile framework that is now proving to be a powerful ally for operators as they look to secure market share and protect revenues. Perhaps most relevant to
the current climate, IMS also provides the architectural framework to deliver VoLTE and RCS. As this scenario unfolds, it facilitates the rapid growth of a broad and diverse ecosystem, which in turn drives innovation up and price down.

Ultimately, IMS will most likely move to the cloud. IMS’ modularity and layered architecture lends itself to be centralized and instantiated in a virtualized environment, with perhaps virtualized SBCs remaining at the edge. The opportunity to build the 4G core network in the cloud promises the mobile operator potentially huge savings by fundamentally changing the cost structure for building and managing data centers. More reasons for virtual IMS include:

- Diminishing cost and complexity.
- Mobile IMS is just the beginning.
- IMS is an enabler, not a service.
- IMS complements WebRTC.

One of the big new drivers for IMS in LTE is the introduction of VoLTE. With VoLTE, domain network virtualization will allow the operator to adapt to the increasing demand in traffic, provide more optimal resource utilization (both applications and infrastructure), enable flexible network management, provide easier multi-tenancy support and allow faster configuration of new services. E2E deployment of VoLTE also impacts many of the E2E elements of the mobile network. NFV can also be used to provide an efficient common production environment, which can be used by different applications supporting the coexistence of several versions of network service software. Pre-production and test environment support can also be achieved for deploying new services.
IMS deployment is a good example to articulate how affinity/anti-affinity rules are important. Anti-affinity rules can be used in the case of using for 1+1 redundant pairs where you don’t want both of the VMs to be on the same host and thus both fail when the host fails. This would be applicable to any of the functions within IMS or VoLTE that are in a 1+1 redundant configuration. Affinity rules are mainly used when you want to place VMs close together for performance or to reduce cross-network traffic. This would be applicable in IMS/VoLTE if there are any fault-tolerant clusters with a lot of replication or between network elements that have a lot of signaling traffic between them.

4.2 VIRTUALIZED EPC (VEPC)

Because the EPC is critical to the realization and management of all LTE traffic, it is important to consider use cases related to virtualization of the EPC elements. Each individual EPC element also has specific considerations that determine whether to deploy with NFV. vEPC is a good example: Multiple VNFs can be deployed and managed on a NFVI but must cater to performance scalability in the signaling and control plane, each potentially demanding different levels of NFVI resources.

vEPC elements can benefit from more agile deployment and scalability. However, virtual resource monitoring and orchestration, along with service awareness, are essential for implementing elasticity effectively. Due to the nature of telecom networks, SLAs will be a key issue for a virtualized mobile core network. Because virtualization usually leads to a performance trade-off, equipment vendors must optimize data-plane processing to satisfy carrier-grade bandwidth and latency requirements and sufficient control-plane performance for SLAs needed to ensure availability of regulatory services, such as emergency calls.
Some virtualized EPC deployments target enterprise customers for VPNs or private network services. A promising approach is to introduce specific virtualized functions within the operator’s network. For example, it may be desirable to use NFV for enterprise customers with specific APN. By doing so, the operator could reduce time to market by faster APN development (better orchestration) at a lower cost by using COTS rather than proprietary platforms. In the case of customers with specific SLA, development of a separate NFV-based service platform could reduce the level of coordination required on the overall operator’s network. Therefore, it would facilitate scheduling of networks’ improvements without impacting SLAs.

Deployment of a virtualized MME (virtual Mobility Management Entity) has some interesting characteristics. Once the deployed vMME has achieved feature and functionality parity with the existing MME in the network, the operator can add the vMME to a MME pool and assign a relative low capacity to the vMME such that the eNBs will steer a low percentage of traffic to the assigned vMME. This vMME can be considered “under test” to allow the operation team to become familiar with the new operation model. Over time, S1 interface relative capacity in EPC can be set to value to steer the desired traffic to the vMME.

Similar use case can be defined to the core nodes. SGWs can be added to the network and use DNS to control the amount and route of traffic into the network by using test APNs that are then migrated to production APNs.

The EPC flexibility provides room for operators to create and redefine deployments by combining 3GPP nodes on a reduced numbers of VNFs compared to the traditional deployments. One example is EPC nodes on a single VNF with only S1 and SGi as the external interfaces. Another example is the opportunity to converge the SGW, PGW and SBC plane functions into a one logical element with a single control-plane function and multiple,
separate media-plane functions. The objective is to allow mobile operators to optimize the EPC/IMS network for VoLTE.

The investment cycle is a critical driver of the industry schedule. Many advanced operators – the ones most likely to be interested in virtual EPC – have only recently deployed new EPCs and do not expect to revisit that investment in the next few years.

Finally, NFV implementation of these mission-critical core network elements also takes careful network and resiliency planning to ensure proper performance, capacity, resiliency and overall SLA requirements in an LTE network.

### 4.3 NEW OFFERINGS WITH VEPC AND SGI SERVICES

Bringing NFV to mobile core networks allows operators to define separate network capabilities, capacity and services that realize new, more targeted offerings in areas such as SGI value-added services (e.g., DPI, firewall, optimization, CDN). NFV also enables capability sets to launch MVNOs or specialized/optimized services for M2M or other vertical industry applications.

As mobile operators require more control over services being offered on the SGI interface, the use of APN, P-GW and SGI-based applications could become a fundamental framework for realizing new service suites around EPC as Figure 18 shows. SGI services can also benefit from NFV implementation. When combined with the ability to direct service flows with technologies such as SDN forwarding and control, the VNFs can be instantiated on a per-flow or per-use-case basis. This eliminates the need to stack up fixed amounts of hardware and software to accommodate worst-case scenarios. Also, new flow-based sessions can be created dynamically based on the user profile or traffic profile.

As described in the Signals Research Group’s Signals Ahead Report [12], NFV can define separate network slices by effectively creating a virtualized core (essentially a virtualized EPC) for each service, with each virtualized EPC engineered for requirements of the specific service. Applying NFV to mobile core networks requires virtualizing key control plane components such as the MME, PCRF, AAA and HSS, as well as user plane components such as S-GW and P-GW.
It may not be necessary for operators to create completely separated core networks for each service. Operators can control the extent to which the core network is virtualized and shared among different services. For example, there may not be much to be gained from creating unique virtualized MME pools for many services. Most services may be able to share the same virtualized MME pool. Because the user plane presents the bottleneck, the S-GW and P-GWs can be virtualized and run separately for each service.

Figure 19 shows this hybrid architecture. In this case, the S-GW and P-GWs are run as separate virtualized instances for each service, whereas the MME and PCRFs may or may not be shared among services.

![Figure 19](image)

**Figure 19. Realization of New M2M and MVNO Services Using NFV in the EPC.**

Source: Signals Research Group [12]

In any case, the introduction of the ePC and SGi services as virtualized solution in the cloud opens the door to novel approaches to redefine and re-design the network functions and node boundaries to deliver customized versions of ePC and SGi services to better fit the operator deployment models.

### 4.4 C-RAN

Virtualization and pooling of radio access networks is sometimes termed cloud-RAN (C-RAN), but this does not necessarily involve any of the NFV concepts. Today there are non-NFV approaches to C-RAN that involve centralization and pooling of RAN baseband resources that yield significant savings by providing both OPEX and CAPEX relief.

Centralizing BBUs can save money from a lease-fee perspective and can reduce time to market by avoiding zoning delays for new cell sites. Pooling further reduces costs and time to market by enable sharing of site loads. With the deployment of Coordinated Multi-Point (CoMP) transmission/reception technology, there are additional benefits to having co-located baseband processing, especially when looking at the most sophisticated CoMP models.

One of the bigger challenges of non-NFV C-RAN is the requirement for fiber connectivity to cell sites to supply the required high throughput rates. Cost and availability of dark fiber for front haul to remote radios can make adoption of centralized RAN somewhat challenging, especially in the North American market.
By leveraging NFV concepts, there is the potential to overcome the difficulties identified in the basic C-RAN concept and make the model much more practical and applicable in North America.

The pooled baseband units can take advantage of the NFV concept of COTS hardware to reduce cost and add the flexibility of NFV elasticity to the pool to enable additional CAPEX optimization. There are challenges to overcome, such as some of the real-time and near-real-time requirements of baseband processing. But these are being addressed by enhancements to the cloud model and ongoing advancements in x86 processing capabilities.

In addition, the more advanced NFV concept of redefining traditional nodes into smaller software functions called Virtual Network Function Components (VNFCs) may lead to a redefinition of the baseband and radio unit functional split that will further enhance the ability of NFV to support RAN requirements. Finally, the current versions of the protocols running between the radio units and the baseband require dark fiber transport, which can be a significant cost barrier. But with the potential to redefine the functional split while leveraging NFV software architectures, there is the strong potential to packetize the connection and leverage switched or even SDN-based transport.

In addition, other uses of virtualization in the access network include deploying services (e.g., caching, analytics, location applications, advertisements), reducing the time to deliver services and backhaul costs while improving customer experiences. The ability to manage, change or move these services based on time, events or profiles is a benefit of NFV infrastructure.

Because of the additional complexities of the RAN, the realization of NFV-based C-RAN will probably not be one of the first NFV use cases ready for deployment. However, the benefits of centralizing baseband will ultimately
drive resolution of these complexities and lead to a NFV-enabled C-RAN solution set for North American mobile operators.

5. NEXT STEPS AND RECOMMENDATIONS - ARCHITECTING THE NFV JOURNEY

While NFV has many technology components, the application to the mobile operator’s core network is as much about adopting a new operational model as it is about adopting new technology. NFV brings many aspects of the IT environment to the telecom world, and this affects the operator’s business operations. It’s also important to develop and manage a long-term transformation strategy across the network at a different level and at stages of maturity and dependence on legacy integration Key areas that must be carefully considered include:

- **Internal Operational Model** – Who will build the fundamental data center infrastructure and maintain it? This is traditionally a CIO team function, but now that this infrastructure is supporting core network functions directly, this creates a new CTO-CIO team relationship. This may be handled by reorganization or by the adoption of internal SLAs between functional teams. Either model can work, but this must be well-defined before taking the NFV model into live service.

- **Procurement Model** – Traditional telecom solutions have been fully integrated with hardware and software. The new model is horizontal, with the procurement of the hardware and software potentially being completely separate. This affects things such as contractual terms, SLAs, warranties, support agreements. Potential shifts in CAPEX to OPEX also need to be considered and addressed.

- **Operational Model** – Mobile operators have complex existing support and operational models to maintain the traditional physical deployment model. With the selective introduction of cloud in the network, work will need to be done to quickly introduce a hybrid support model across traditional and NFV-based network elements as the action model under different situations will be quite different.

- **Competence Shift** – Competence and skills geared today for physical equipment and manual configuration/management/control/upgrades need to be transformed. Existing competencies in mobile network design, deployment and operations need to transform with new skills in completely new areas. For example:
  - Physical data center compute/network/storage deployment.
  - Logical software-based deployment of virtualized equipment.
  - Virtualization software configuration, VNF and NFVI orchestration/management.
  - New ways of auditing and fault isolation (physical and virtual).
  - Understanding the role and performance of new layers of software in the NFV stack.

Whether a mobile operator has already embarked in NFV tests and trials, or is just starting to look into the world of NFV, the following sections outline a set of recommendations to operators planning a deeper journey into the NFV evolution of their networks.
5.1 MANAGING THE ARCHITECTURAL STRATEGY

From an architectural and design perspective there are some key areas that fundamentally change the way CIO and CTO teams approach NFV design and deployment. The following suggestions may provide insights into important areas to consider when assessing how to approach this next generation of architectural choices and strategies.

**Establish Architectural Domains**

Separation of concerns is a critical principle in all complex architecture endeavors, and NFV must not be different. As such, the first step for an operator to embark in the NFV journey is to assess itself and start developing a program towards addressing its capabilities, needs and preparedness for each of these areas. For example:

- **VNFs** – Mapping of legacy network functions to virtualized network functions.
- **NFV Orchestrator** – Orchestration use cases for the infrastructure and network functions.
- **NFVI Platform** – Compute, storage, networking and automation and enabling, and chaining of services (i.e. SDN).

### 5.1.1 SET RESPONSIBILITY FOR ARCHITECTURE AND STANDARDS

Another critical step is to define an NFV “common services” organization to tackle the aspects that involve strategic direction on architecture and standards:

- An NFV architecture office should be in charge of the architecture qualities that are common to the three architecture layers that must be consistent to avoid technology silos. The areas to cover here are mainly integration, performance, availability and security.

- This group should dictate integration standards, performance KPI and thresholds in the form of architectural qualities requirements that all implementations must comply with.

- Address the inclusion of any open-source ecosystem (when applicable to the operator strategy). Furthermore, the organization may decide to actively participate as a contributor to an open-source project to expedite the target architecture deployment model.

### 5.1.2 BUILD AN EVOLUTION PLAN

Such deployment enables evolution toward an NFV-based network in three critical dimensions:

1. Existing applications eventually become compatible and optimized for NFV infrastructure, and can therefore be moved or deployed on the infrastructure as they become available.
2. New applications designed for NFV can rapidly be introduced and scaled or retired depending on market success, leading to an accelerating TTM for new services and capabilities.
3. The infrastructure itself will evolve with the pace of the IT industry, enabling an ever-increasing class of applications, including bearer plane applications. This, in line with evolution of the necessary operational models, will lead to acceleration of 1 and 2.
5.2 ROLE OF VENDORS AND OPERATORS IN THE 4G LTE NFV ECOSYSTEM

It is important to understand and determine which roles and tasks are managed by the operator versus the role the vendors and integrators play in the architecture and deployment plan for the NFV strategy. NFV solutions in the vendor ecosystem can range from individual products and components to complete NFV solutions for any segment or element of the framework.

The NFV ecosystem consists of many vendors, with some vendors taking on several roles to meet each operator’s needs. As the market matures, there are some key core roles that evolve over time:

- **Network Infrastructure Providers** – Companies that can deliver the core compute, storage and network capabilities that are at the core of the NFVI. These companies will also take on the challenge of how to enable more demanding applications by introducing new types of resources (such as digital signal processing capabilities) into this “elastic” infrastructure. The providers in this category include both hardware and virtualization software that supports the realization of the NFVI.
- **Infrastructure Orchestration Providers** – Companies that enable the orchestration of the underlying core platform to enable the virtualization and orchestration of the infrastructure. While typical IT cloud capabilities are very well developed, these players will focus on enabling this layer to deliver on the often more stringent requirements of telecommunications.
- **Application Providers** – Both the providers of the critical applications that today are delivered in the traditional model and new innovative providers will enter the market. The primary challenge of the providers of critical applications will be to evolve existing network functions to take advantage of the new infrastructure as it evolves. New innovative application providers should enter the market as the availability of an open infrastructure should boost the strength of this ecosystem.
- **System Integrators** – These organizations will take ownership for the end-to-end implementation of systems incorporating applications and NFV infrastructure.

Vendors currently take on a combination of the above roles and will continue to do so as the market transitions to NFV. For example, the traditional vendors will in some cases continue to play the roles of application provider and system integrator. NFV will allow them to deliver applications in more of an ISV model as NFV standardizes on the shared, open infrastructure. Operators need to decide which components they will build themselves or acquire from vendors and what level of system integration and certification responsibilities are done in-house versus with a services partner.

As Figure 21 shows, there is also a maturity evolution in how players and users of the NFV ecosystem will evolve as the NFV features and capabilities evolve over time. Different areas of the LTE network may require more or less feature sophistication, so it is appropriate to start the journey at the level that suits the evolution maturity of the 4G LTE network area being transformed. Scope and level of feature sophistication can also help to manage the level of uncertainty and risk an operator is willing to accept as the NFV journey evolves.
5.3 UTILIZE PROOF OF CONCEPTS AND MOVE TOWARDS DEVOPS

Critical for this stage is to measure and document all the architecture scenarios, which can then be extrapolated later to address capacity decisions for the production environments.

It is important to understand that NFV is a framework that consists of discrete components. There is typically a VNF 1:1 mapping with the physical network elements that exist in the network today. As a result, it is possible to start deploying VNFs as soon as possible. Conceptually, it’s possible to replace a single element in the network today with a VNF. When planning the transformation into the NFV framework, starting with a well-defined single VNF or a closely connected set of VNFs is key to working through all of the transitional steps needed both operationally and architecturally. It also gives the key stakeholders a chance to understand the organizational impact of the evolution. To minimize NFV operational model challenges, the operations team must take fundamental steps to gain the knowledge and experience necessary to build and operate NFV in the future, by carefully planning the steps to introduce NFV into the network.
CONCLUSION

After exploring these areas, there is no single, universal answer to when an operator may choose to proceed with implementing the NFV model. There are many compelling advantages, as have been outlined in this document, but ultimately the decision must be carefully considered and timing and resourcing of the commitment to the change must be understood and planned in detail. Pursuing an NFV deployment strategy needs to take into account all of the implications of technology, architecture, operational and business transformation required to realize the return on investment in time and resources required to execute this long-term transformation.

In conclusion, NFV evolution is real and it is happening now; therefore, it is up to the LTE operator community to consider leveraging this opportunity to start down the migration path to NFV and start reaping the benefits. It may take some investment of time, resources, education and operational transformation, but it may be the most efficient strategy going forward to keep pace with the rapid growth of the LTE networks of tomorrow.
REFERENCES


APPENDIX

CLOUD DEFINITIONS

Cloud-based services vary based on how the cloud is accessed. A public cloud implies use of the public Internet, so its name, and therefore services relying on it, are based on best effort without any guaranteed QoS for the end user. A private cloud uses managed resources, allowing provision for some service-level guarantee to the end user, which could even involve service level agreement (SLA). A hybrid cloud is a combination of both private and public clouds, looking to take advantages of each. However, it cannot achieve the same guaranteed level of service that private cloud provides. In this paper, the term “cloud” is used in the generic sense without implying the implementation of a specific type of cloud for network function virtualization.

When discussing cloud implementations within a telecom operator environment, there are four potential cloud models that can be considered. As shown in Figure 22, two of the models would be considered in the public access domain, and two would be considered in the private access domain.

![Type of Operator Clouds](image)

*Figure 22. Four Potential Cloud Models for Telecom Operators.*

The key differentiators of the models are use case, security, privacy and connectivity. The public-access clouds are intended to provide direct end user services (i.e., IaaS, PaaS and/or SaaS) to enterprises and consumers. To accomplish this, the end user must have federated access to the cloud API and control mechanisms. This requires appropriate security and privacy controls. Such implementations are outside the scope of this document.

The private-access cloud APIs and control systems are only intended to be directly accessed by operator- or partner-owned resources. However, the applications running in these private instances are providing service to external customers (e.g., IMS core, S-GW, MME).

Although these four distinct cloud models may imply completely separate instances, the implementation selected will be Operator specific. The pros and cons of different implementations are outside of the scope of this document.
### ETSI ISG POC List

| PoC#1: | CloudNFV Open NFV Framework |
| PoC#2: | Service Chaining for NW Function Selection in Carrier Networks |
| PoC#3: | Virtual Function State Migration and Interoperability |
| PoC#4: | Multi-vendor Distributed NFV |
| PoC#5: | E2E vEPC Orchestration in a multi-vendor open NFVI environment |
| PoC#6: | Virtualised Mobile Network with Integrated DPI |
| PoC#7: | C-RAN virtualization with dedicated hardware accelerator |
| PoC#8: | Automated Network Orchestration |
| PoC#9: | VNF Router Performance with DDoS Functionality |
| PoC#10: | NFV Ecosystem |
| PoC#11: | Multi-Vendor on-boarding of vIMS on a cloud management framework |
| PoC#12: | Demonstration of multi-location, scalable, stateful Virtual Network Function |
| PoC#14: | ForCES Applicability for NFV and integrated SDN |
| PoC#15: | Subscriber Aware SGi/Gi-LAN Virtualization |
| PoC#16: | NFVIaaS with Secure, SDN-controlled WAN Gateway |
| PoC#17: | Operational Efficiency in NFV Capacity Planning, Provisioning and Billing |
| PoC#18: | VNF Router Performance with Hierarchical Quality of Service Functionality |
| PoC#19: | Service Acceleration of NW Functions in Carrier Networks |
| PoC#20: | Virality based content caching in NFV framework |
| PoC#21: | Network Intensive and Compute Intensive Hardware Acceleration |
| PoC#22: | Demonstration of High Reliability and Availability aspects in a Multivendor NFV Environment |
| PoC#23: | Demonstration E2E orchestration of virtualized LTE core-network functions and SDN-based dynamic service chaining of VNFs using VNF FG |
| POC#24: | Constraint based Placement and Scheduling for NFV/Cloud Systems |
| POC#25: | Demonstration of Virtual EPC (vEPC) Applications and Enhanced Resource Management |
DEFINITION OF IAAS/PAAS/SAAS

**IaaS** – The operator gets access to the computer/server. Therefore, IaaS is essentially a physical server box. The vendor manages the networking, storage, hardware of the box and virtualization O/S. The operator manages the VMs.

**PaaS** – PaaS is a hosted application/framework/tools that allows the operator to provide a service to build something on. For example, the operator accesses the platform in the form of an SDK.

**SaaS** – The service vendor provides a complete business functionality. There is practically no management by the operator. The operator gets access to the service by APIs.

![Separation of Responsibilities](image-url)

*Figure 23. Responsibility of IaaS/PaaS/SaaS Services [8]. Source: Cisco*
<table>
<thead>
<tr>
<th>ACRONYMS</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>3GPP</td>
<td>3rd Generation Partnership Project</td>
</tr>
<tr>
<td>AAA</td>
<td>Authentication, Authorization, and Accounting</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>APN</td>
<td>Access Point Name</td>
</tr>
<tr>
<td>BBU</td>
<td>Base Band Unit</td>
</tr>
<tr>
<td>BSS</td>
<td>Business Support Systems</td>
</tr>
<tr>
<td>CapEx</td>
<td>Capital Expenditure</td>
</tr>
<tr>
<td>CDN</td>
<td>Content Distribution Network</td>
</tr>
<tr>
<td>CGNAT</td>
<td>Carrier-Grade Network Address Translator</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>CoMP</td>
<td>Coordinated Multi-Point</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial-off-the-shelf</td>
</tr>
<tr>
<td>CPE</td>
<td>Customer Premises Equipment</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>CSCF</td>
<td>Call Session and Control Function</td>
</tr>
<tr>
<td>CTO</td>
<td>Chief Technology Officer</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host control Protocol</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Server</td>
</tr>
<tr>
<td>DPI</td>
<td>Deep Packet Inspection</td>
</tr>
<tr>
<td>EMS</td>
<td>Element Management System</td>
</tr>
<tr>
<td>EPC</td>
<td>Evolved Packet Core</td>
</tr>
<tr>
<td>ETSI</td>
<td>European Telecom Standards Institute</td>
</tr>
<tr>
<td>HSS</td>
<td>Home Subscriber System</td>
</tr>
<tr>
<td>IaaS</td>
<td>Infrastructure as a Service</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IMS</td>
<td>IP Multimedia System</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ISG</td>
<td>Industry Specification Group</td>
</tr>
<tr>
<td>ISV</td>
<td>Independent Software Vendor</td>
</tr>
<tr>
<td>KPI</td>
<td>Key Performance Indicator</td>
</tr>
<tr>
<td>LB</td>
<td>Load Balancer</td>
</tr>
<tr>
<td>MANO</td>
<td>Management and Orchestration</td>
</tr>
<tr>
<td>MME</td>
<td>Mobility Management Entity</td>
</tr>
<tr>
<td>M2M</td>
<td>Machine-to-Machine</td>
</tr>
<tr>
<td>MGCF</td>
<td>Media Gateway Control Function</td>
</tr>
<tr>
<td>MRFP</td>
<td>Multimedia Resource Function Processor</td>
</tr>
<tr>
<td>MTAS</td>
<td>Multimedia Telephony Application Server</td>
</tr>
<tr>
<td>MVNO</td>
<td>Mobile Virtual Network Operator</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>NFV</td>
<td>Network Function Virtualization</td>
</tr>
<tr>
<td>NFVI</td>
<td>Network Function Virtualization Infrastructure</td>
</tr>
<tr>
<td>NMS</td>
<td>Network Management System</td>
</tr>
<tr>
<td>NOC</td>
<td>Network Operations Center</td>
</tr>
<tr>
<td>OpEx</td>
<td>Operational Expenses</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OSS</td>
<td>Operation Support System</td>
</tr>
<tr>
<td>PaaS</td>
<td>Platform as a Service</td>
</tr>
<tr>
<td>PCRF</td>
<td>Policy and Charging Rules Function</td>
</tr>
<tr>
<td>PE</td>
<td>Provider Edge</td>
</tr>
<tr>
<td>PGW (or P-GW)</td>
<td>Packet Data Network Gateway in an LTE core network</td>
</tr>
<tr>
<td>PoC</td>
<td>Proof-of-Concept</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RAN</td>
<td>Radio Access Network</td>
</tr>
<tr>
<td>RCS</td>
<td>Rich Communication Services</td>
</tr>
<tr>
<td>REST</td>
<td>Representational State Transfer</td>
</tr>
<tr>
<td>RNC</td>
<td>Radio Network Controller</td>
</tr>
<tr>
<td>ROI</td>
<td>Return on Investment</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
<tr>
<td>SBC</td>
<td>Session Border Controller</td>
</tr>
<tr>
<td>SDN</td>
<td>Software Defined Networking</td>
</tr>
<tr>
<td>SGSN</td>
<td>Serving GPRS Support Node</td>
</tr>
<tr>
<td>SGW (or S-GW)</td>
<td>Serving Gateway in an LTE core network</td>
</tr>
<tr>
<td>SHV</td>
<td>Standard High Volume</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SR-IOV</td>
<td>Single Root I/O virtualization</td>
</tr>
<tr>
<td>TAS</td>
<td>Telephony Application Server</td>
</tr>
<tr>
<td>TCO</td>
<td>Total Cost of Ownership</td>
</tr>
<tr>
<td>vEPC</td>
<td>Virtualized Enhanced Packet Controller</td>
</tr>
<tr>
<td>VIM</td>
<td>Virtual Infrastructure Manager</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>VNF</td>
<td>Virtual Network Function</td>
</tr>
<tr>
<td>VNFC</td>
<td>Virtual Network Function Components</td>
</tr>
<tr>
<td>VNFaaS</td>
<td>VNF as a Service</td>
</tr>
<tr>
<td>VoLTE</td>
<td>Voice Over LTE</td>
</tr>
<tr>
<td>VR</td>
<td>Virtual Router</td>
</tr>
<tr>
<td>vSwitch</td>
<td>Virtual Switch</td>
</tr>
<tr>
<td>x86</td>
<td>Intel x86 reference compute reference architecture</td>
</tr>
</tbody>
</table>
ACKNOWLEDGEMENTS

The mission of 4G Americas is to advocate for and foster the advancement and full capabilities of the 3GPP family of mobile broadband technologies, including LTE-Advanced, throughout the ecosystem's networks, services, applications and wirelessly connected devices in the Americas. 4G Americas' Board of Governors members include Alcatel-Lucent, América Móvil, AT&T, Cable & Wireless, Cisco, CommScope, Entel, Ericsson, HP, Intel, Mavenir Systems, Nokia, Openwave Mobility, Qualcomm, Rogers, Sprint, T-Mobile USA and Telefónica.

4G Americas would like to recognize the significant project leadership and important contributions of Bob Gessel of Ericsson and Carlos Molina of Mavenir Systems, as well as representatives from the other member companies on 4G Americas’ Board of Governors who participated in the development of this white paper.

The contents of this document reflect the research, analysis, and conclusions of 4G Americas and may not necessarily represent the comprehensive opinions and individual viewpoints of each particular 4G Americas member company.

4G Americas provides this document and the information contained herein to you for informational purposes only, for use at your sole risk. 4G Americas assumes no responsibility for errors or omissions in this document. This document is subject to revision or removal at any time without notice.

No representations or warranties (whether expressed or implied) are made by 4G Americas and 4G Americas is not liable for and hereby disclaims any direct, indirect, punitive, special, incidental, consequential, or exemplary damages arising out of or in connection with the use of this document and any information contained in this document.

© Copyright 2014 4G Americas