DEPLOYING VNFS EFFICIENTLY IN NFV

Network Functions Virtualization (NFV) is gaining momentum in the network service provider community, and it will transform the way networks are built and operated. NFV transformation introduces new challenges to service providers, and the right decisions must be made to reap the benefits of NFV architecture. This report describes various deployment models for Virtual Network Functions (VNFs), so that service providers can get insights into the NFV transformation journey to help them make right decisions during the implementation of NFV.

1. Introduction

Service provider networks are populated with proprietary hardware that delivers specific network functionality. The cost to acquire and maintain this proprietary hardware is very high. Introducing new services requires planning for space, energy, new equipment, and so on. These steps mean it takes a lot of time to bring a service to the market. Furthermore, the equipment is statically assigned to a service and cannot be shared with other services. All this results in increased capex and opex.

NFV[1] architecture addresses these shortcomings by decoupling the hardware from the software stack by leveraging the virtualization technology. In the NFV architecture, legacy network functions are virtualized and deployed on a virtualization layer running on top of industry standard servers. The decoupling of the hardware from the software enables flexible and faster deployment of network services.

As a first step toward the NFV transformation journey, network functions must be virtualized without compromising the functionality, performance and reliability offered by legacy network functions. The virtualized variants of the network functions are referred to as VNFs. The performance and efficiency of the VNFs depend on the combination of hardware, virtualization layers used in the NFV implementation, and the VNF itself. There are several models available to deploy VNFs. Service providers can start the NFV transformation journey with one of these models, and evolve toward implementing a completely vendor neutral network.

Network services are often made up of one or more network functions. Deploying individual network functions one at a time and configuring them manually increases the service creation times and is a method that is prone to errors. An orchestrator is needed to provision and configure the VNFs, and to interconnect them to bring down the service creation times and satisfy the immediacy needs of the service providers' customers in time.

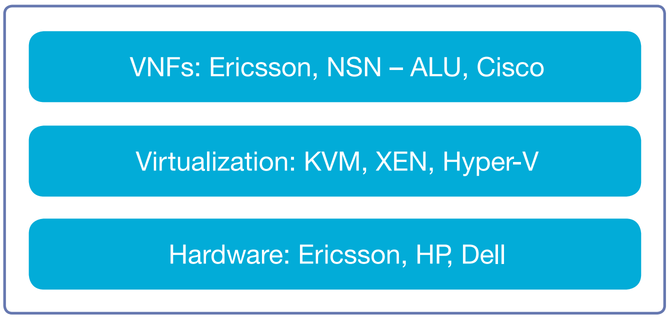
Network services can be created from VNFs from a single vendor or from multiple vendors. In an environment made up of VNFs from multiple vendors, multi-vendor verification becomes crucial, and standardized software must be used to reduce the pain points in integrating and deploying multi-vendor products and to avoid the unnecessary vendor lock-in.

As a first step toward the NFV transformation journey, network functions must be virtualized without compromising the functionality, performance and reliability offered by legacy network functions.

The transformation to NFV is complex, and service providers are faced with critical decisions to manage the complexity of this transformation. This report describes in detail the VNF deployment models, orchestration of network services, multi-vendor verification, and multi-cloud aspects involved in efficient deployment of VNFs as part of the NFV transformation journey.

2. VNF deployment models

NFV consists of several layers of technology – the hardware platform, the virtualization platform, and the VNFs themselves. These underlying technologies can be sourced from various vendors in each category, as shown below.



VNFs: Ericsson, NSN – ALU, Cisco

Virtualization: KVM, XEN, Hyper-V

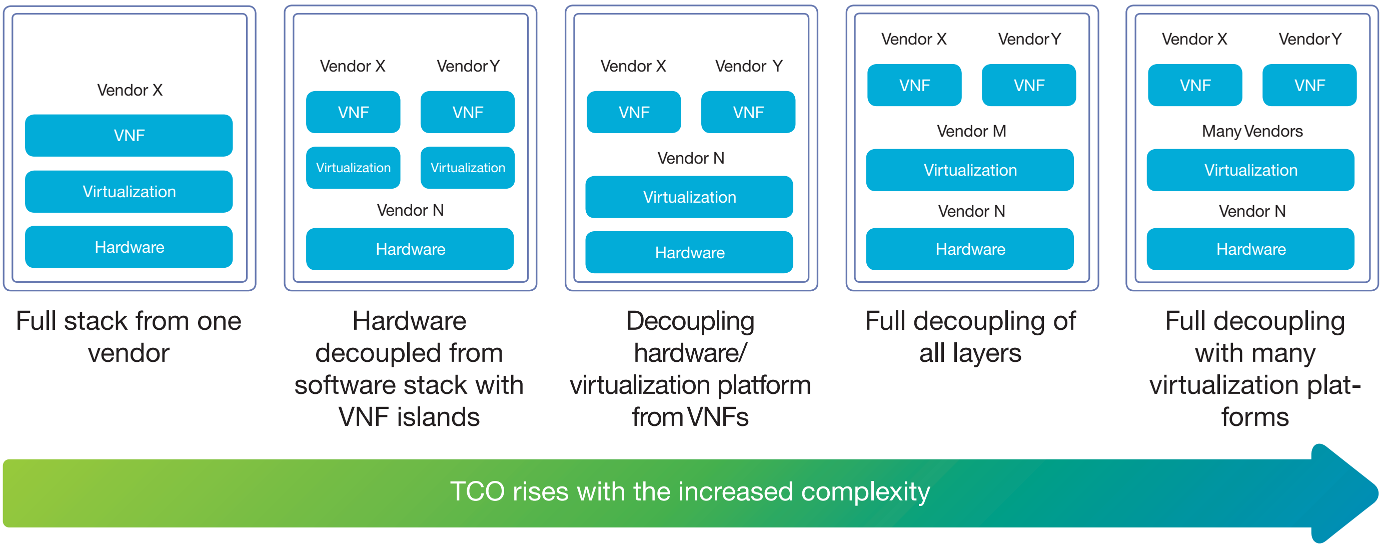
Hardware: Ericsson, HP, Dell

All these layers can impact the functionality, performance and reliability of a VNF. The selection of these technologies impacts the NFV transformation journey on several dimensions, such as system integration costs, performance, operational complexity, and life cycle management, resulting in various levels of total cost of ownership (TCO) benefits.

A VNF may be CPU, memory, network or storage intensive. Selecting hardware best suited for the VNF placement is essential in guaranteeing the performance characteristic. Ericsson HDS 8000 provides building blocks to deliver high CPU, memory, network or storage performance using a single system based on Intel Rack Scale Architecture. It is well suited to run VNFs in modern data centers. For central offices, Ericsson BSP 8100 is suitable. It is NEBS3 compliant in order to operate in demanding conditions, e.g. from a temperature perspective. It is built on Intel x86 runs native and virtual network functions.

The virtualization layer introduces a performance penalty for network and storage input/output. For example, virtualization could increase network latency and add jitter. Service providers can keep the performance penalty within the acceptable limits to make sure that voice quality is not impacted by the virtualization overhead. Ericsson provides a virtualization layer with enhanced vSwitch to meet the carrier-grade demands of the network services.

Legacy network services are typically run on a high capacity monolithic system. The systems are selected based on the peak load conditions, and most of the time they are underutilized. To utilize the hardware resources efficiently, the VNFs need to be auto scalable. As the load increases, new VNF instances are created to meet the demand, and as the load decreases, VNF instances are terminated. VNFs need to work



Full stack from one vendor

Hardware decoupled from software stack with VNF islands

Decoupling hardware/ virtualization platform from VNFs

Full decoupling of all layers

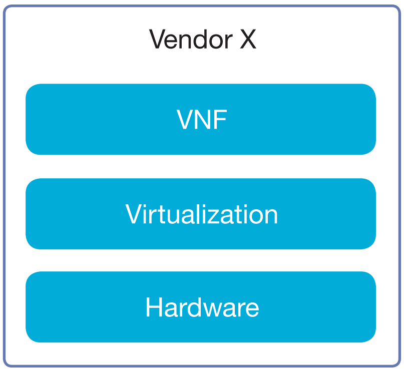
Full decoupling with many virtualization platforms

in conjunction with an orchestrator for auto-scaling features.

The availability of a wide variety of products from a wide variety of vendors at each level in the architecture results in several deployment models. The above diagram shows some of those models.

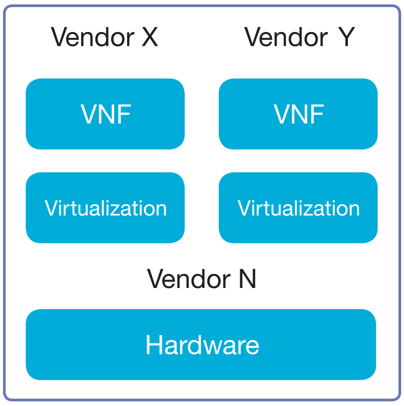
Each model has its own advantages and disadvantages and is described in detail below.

Model 1 – Full stack from one vendor



In this model, a single vendor supplies all the components in the architecture – the hardware and the software. The advantage with this model is that the solution is pre-validated and results in very low system integration costs. In this model, the architecture works like a well-oiled machine and provides deterministic performance demanded by the service provider networks. If there is a technical issue, the operator just needs to work with one vendor to quickly resolve it. Life cycle management is easier in this model, as the vendor can perform end-to-end testing before delivering the software updates to the service provider. In this model, the vendor can standardize the hardware elements using industry standard components, so that the same hardware elements can be used across several different VNFs, resulting in economies of scale and reduced capex and opex. A good level of flexibility can be achieved with this model with features like elasticity and orchestration, while the workloads supported can be limited based on the virtualization platforms supported by the vendor. This model would be a great option for service providers as they start their journey toward realizing the NFV benefits quickly. This model also has the lowest TCO compared with other models.

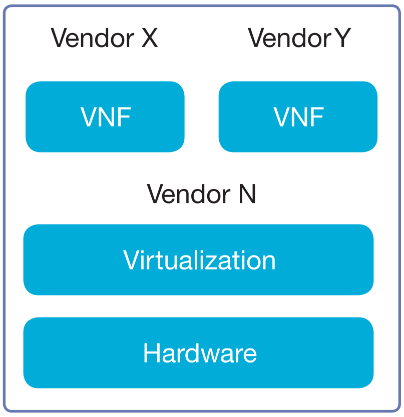
Model 2 – Hardware decoupled from software stack with VNF islands



In this model, one vendor supplies the hardware. The system can have VNFs from multiple vendors, and each vendor supplies a virtualization layer along with the VNF. This model involves moderate system integration costs, as the VNF vendors need to perform end-to-end testing with the hardware chosen by the service provider. VNFs can have a deterministic performance to a large extent. Care must be taken when placing the VNF on the server hardware to guarantee the performance of the VNF. This model would be a good option if the virtualization layer requires customizations to meet the functionality and performance demands of the VNFs. If there is an issue with a VNF, the service provider would need to work with both the hardware vendor and the VNF vendor to resolve it, resulting in a low to medium level of complexity. For life cycle management, care must be taken to make sure that a change in the hardware does not impact the VNF and vice versa. This results in moderate complexity for the life cycle management. A better level of flexibility can be achieved with this model with features like elasticity, orchestration and the freedom of workloads. This model is a great option if hardware and software decoupling is a must for the NFV implementation. This model does not have the lowest TCO, although it is low compared with some of the other models.

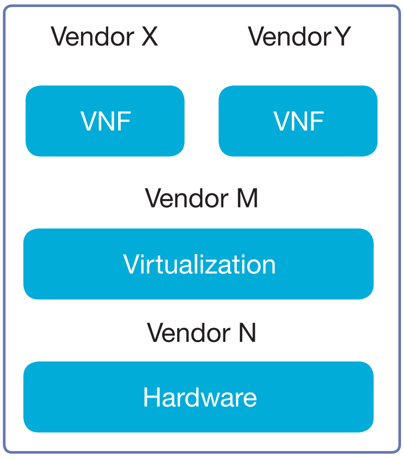
Model 3 – Decoupling hardware/virtualization platform from VNFs

In this model, a single vendor provides hardware and virtualization platforms, and the VNFs come from several vendors. The hardware and virtualization layers are tightly coupled for faster server deployments and



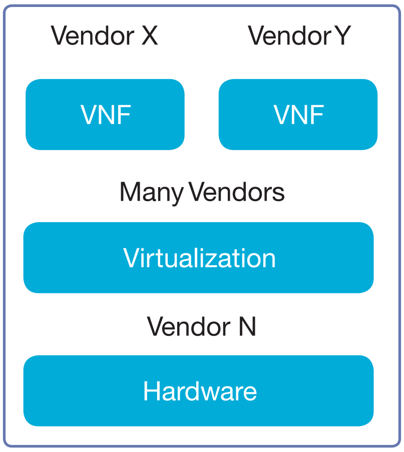
health monitoring. This model involves moderate system integration costs, as the VNF vendors need to perform end-to-end testing with the hardware and virtualization chosen by the service provider. In this model, some VNF features may not work because of the lack of required functionality in the virtualization layer. Furthermore, the performance of the VNF may not be deterministic, as the hypervisor layer may not have carrier-grade extensions. If there is an issue with a VNF, the service provider would need to work with both the hardware and virtualization vendor and the VNF vendor to resolve it, resulting in medium complexity. For life cycle management, care must be taken to make sure that a change in the hardware and virtualization layer does not impact the VNF and vice versa. This results in moderate complexity regarding the life cycle management. A good level of flexibility can be achieved with this model with features like elasticity and orchestration, while the workloads supported can be limited based on the virtualization platforms supported by the vendor. The TCO is medium compared with some of the other models.

Model 4 – Full decoupling of all layers



In this model, hardware is procured from one vendor, the virtualization layer from another vendor, and VNFs from several vendors. This model involves high system integration costs, as the VNF vendors need to perform end-to-end testing with the hardware and virtualization chosen by the service provider. In this model, some VNF features may not work because of the lack of required functionality in the virtualization layer. Furthermore, the performance of the VNF may not be deterministic, as the virtualization layer may not have carrier-grade extensions, and the underlying hardware may not have the needed hardware acceleration capabilities. If there is an issue with a VNF, the service provider would need to work with all the vendors involved – the hardware vendor, the virtualization vendor and the VNF vendor – to resolve the issue, resulting in high complexity. For life cycle management, care must be taken to make sure that a change in any of the hardware or virtualization layers does not impact the VNF. This results in high complexity for the life cycle management. A better level of flexibility can be achieved with this model with features like hardware selection, elasticity and orchestration, while the workloads supported can be limited based on the virtualization platforms supported by the vendor. In this model, the TCO is high compared with some of the other models.

Model 5 – Full decoupling with many virtualization platforms



In this model, each layer is procured from one or more vendors. This model has the most moving parts and the highest system integration cost, as each VNF vendor needs to perform end-to-end testing with the several hardware and virtualization layers selected by the service provider. In this model, some VNF features may not work because of the lack of required functionality in the virtualization layer. Furthermore, the performance of the VNF may not be deterministic, as the hypervisor layer may not have carrier-grade extensions, and the underlying hardware may not have the needed hardware acceleration capabilities. The dynamic selection of the hardware and virtualization layer to run the VNF will play a role in the functionality and performance of the VNF. If there is an issue with a VNF, the service provider would need to work with all the vendors involved – the hardware vendor, the virtualization vendor and the VNF vendor – to resolve the issue, resulting in very high complexity. For life cycle management, care must be taken to make sure that a change in any of the hardware or virtualization layers does not impact the VNF. This results in the highest level of complexity regarding the life cycle management. The best level of flexibility can be achieved with this model with features like elasticity, orchestration and the freedom of workloads. This model has the highest TCO compared with the other models.

Table 1 summarizes the complexities involved in each of these models. A pre-integrated stack from a single vendor will be a great starting point for the service providers, as they can quickly start realizing the benefits of the NFV transformations like capex and opex reductions and faster time to market products. This is a very efficient solution for deploying the VNFs, and it does not have the system level integration issues that are common in other deployment models.

At present, a pre-integrated stack from a single vendor provides the lowest TCO. As the technology matures and capabilities are added to the cloud software, service providers can move toward selecting independent vendors for each technology layer.

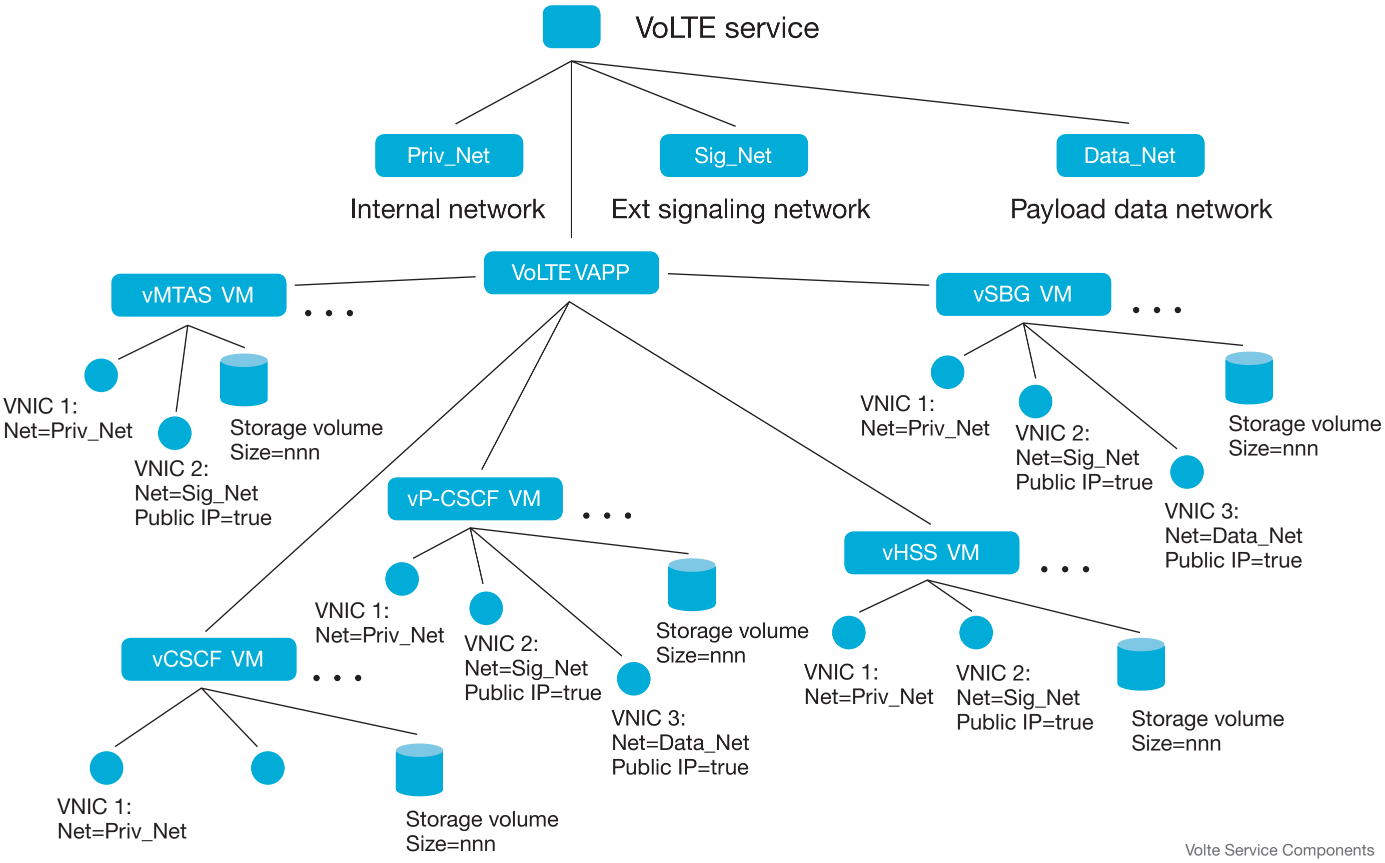
	Model 1	Model 2	Model 3	Model 4	Model 5
System Integration Costs	Lowest	Low	Medium	High	Highest
Functionality & Performance	Deterministic	Deterministic to large extent	Non-deterministic	Non-deterministic	Non-deterministic
Operational complexity	Lowest	Low – Medium	Medium	High	High
Life Cycle Management	Lowest	Medium	Medium	High	Highest
Flexibility	Medium	High	Medium	High	Highest
TCO	Lowest	Low	Medium	High	Highest

Table 1: comparison of VNF deployment models

3. Orchestration

Typical network services are composed of more than one network function. For example, a VoLTE service is made up of several virtual appliances like a virtual Multimedia Telephony Application Server (vMTAS), a virtual proxy call session control function (vP-CSCF), a virtual Session Border Gateway (vSBG), a virtual Home Subscriber Server (vHSS), and a virtual Call Session Control Function (vCSCF). It also comprises virtual networks such as an internal network, a signaling network, a payload network, and one or more virtual network interface controllers (NICs) for the virtual machines. If the service is deployed manually, it could take several hours and will be highly error prone.

Creating a network service typically requires provisioning the VNFs, configuring them, and interconnecting them with the virtual networks. As part of the life cycle management of these VNFs, tremendous care must be taken to make sure that VNF versions are compatible with each other. If done manually, all these steps are very time consuming and error prone. An automated mechanism is required that can orchestrate all these steps with a single click of a button or through programmatic application programming interfaces (APIs). A software module that provides this kind of functionality is referred to as an orchestrator. The orchestrator allows the composition of a network service with several VNFs with required configuration and the connectivity information, and makes it available for consumption through a catalog. Customers with access to the catalog can create the service with a single click of a button or through a programmatic API. Additional rules can be specified



Volte Service Components

on the order in which the VNFs of the network service are started and stopped as part of the life cycle of the network service.

The orchestrator is critical for efficient and faster deployment of network services. Ericsson Cloud Manager (ECM) is an orchestrator specifically designed for service provider environments. ECM provides an integrated platform for managing NFV infrastructure that may be geographically distributed by enabling the creation, orchestration, activation and monitoring of services running on virtualized resources.

> The OPNFV platform enables service providers to efficiently deploy the VNFs and bring network services faster to the market to meet immediacy needs of their customers.

4. Multi-vendor environment

Over the course of the NFV transformation journey, the NFV implementations will consist of products from several vendors. Care must be taken to make sure that all these different products work in synergy to meet the functionality and performance demands of the carrier-grade networks. Cloud software plays a key role in achieving the required interoperability, functionality and performance. By avoiding proprietary cloud software in the NFV implementation, service providers are able to bypass unnecessary vendor lock-in and system integration costs associated with validating VNFs on top of proprietary cloud software. Service providers can adopt open technologies like Open Platform for NFV (OPNFV) instead as a reference platform for the efficient deployment of VNFs.

OPNFV[2] is an open source project created to increase the adoption of NFV in the service provider community. It is cloud software based on the OpenStack[3] industry standard, but with several carrier-grade enhancements to meet the stringent requirements of the operator networks. Several tier 1 service providers, network vendors and software vendors support OPNFV. With OPNFV as a reference platform, service providers can minimize the interoperability, functionality and performance issues stemming from the underlying cloud software. With OPNFV as a standardized platform for service providers, network vendors can start validating the VNFs from day one on the OPNFV reference platform and reduce the system integration time and costs associated with running their VNFs in the service provider environments. The OPNFV platform enables service providers to efficiently deploy the VNFs and bring network services faster to the market to meet immediacy needs of their customers.

5. Multi-cloud environments

A typical service provider environment has three types of clouds – a network cloud, an IT cloud, and a commercial cloud. These clouds have different characteristics. Network clouds need to be highly available and resilient with 99.999 uptime guarantees. IT clouds need to be versatile and support several types of workloads including legacy applications. Commercial clouds have to be highly secure and cost-efficient. At present, service providers are using different technologies for these different clouds. Service providers want to merge these different clouds into a single converged cloud without compromising their qualities. This allows the efficient use of hardware and software resources, as well as the operational benefits of managing a single cloud.

By using standardized hardware elements like Ericsson HDS 8000 platforms based on Intel RSA[4], service providers can implement the converged cloud efficiently and reap the benefits of economies of scale. The Ericsson HDS 8000 platform provides six axes of scalability in hardware design – CPU count, memory, storage capacity, storage performance (read/write operations), network capacity (bandwidth), and network performance (speed and latency). By utilizing the HDS 8000 platform, service providers can greatly reduce the capex for building the converged clouds.

Security and governance become critical for the converged cloud to protect the internal data as well as the customer data. Security needs to be built into the architecture instead of bolting on top of the existing infrastructure. Service providers can use cutting-edge platform as a service technologies like Apcera Continuum to meet the security and governance needs.

6. Conclusion

NFV transforms the way networks are built and operated. Choosing the right VNF deployment model enables service providers to realize the capex, opex and time to market benefits envisioned in the NFV. Without the right VNF deployment model, service providers will spend time and money on system integration efforts and troubleshooting reliability and performance issues stemming from the interoperability of underlying technology layers. With a pre-integrated deployment model from a single vendor as an initial deployment model, service providers can efficiently deploy the VNFs and reduce the TCO.

As more and more network functions become virtualized, NFV implementation will include products from multiple vendors, and interoperability, functionality and performance will become key issues. Service providers can transition from a single vendor full stack model to the complex deployment models using an open platform like OPNFV as the technology matures. With open platforms, service providers can address the interoperability and performance issues efficiently, and minimize system integration costs, while improving the operational efficiency of the service provider networks, and converging their multiple clouds into a single cloud.

GLOSSARY

API	application programming interface
CPU	central processing unit
ECM	Ericsson Cloud Manager
NFV	Network Functions Virtualization
OPNFV	Open Platform for Network Function Virtualization
RSA	Rack Scale Architecture
TCO	total cost of ownership
vCSCF	virtual call session control function
vHSS	virtual Home Subscriber Server
vMTAS	virtual Multimedia Telephony Application Server
VNF	Virtual Network Function
vP-CSCF	virtual proxy call session control function
vSBG	virtual Session Border Gateway

REFERENCES

1. ETSI, October 2014, Network Functions Virtualisation – White Paper #3, available at: http://portal.etsi.org/NFV/NFV_White_Paper3.pdf
2. OPNFV, available at: https://www.opnfv.org
3. OpenStack, available at: http://www.openstack.org
4. Intel Rack Scale Architecture, available at: http://www.intel.com/content/www/us/en/architecture-and-technology/intel-rack-scale-architecture.html

We are a world leader in the rapidly changing environment of communications technology – providing equipment, software and services to enable transformation through mobility.

Some 40 percent of global mobile traffic runs through networks we have supplied. More than 1 billion subscribers around the world rely every day on networks that we manage. With more than 37,000 granted patents, we have one of the industry's strongest intellectual property rights portfolios.

Our leadership in technology and services has been a driving force behind the expansion and improvement of connectivity worldwide. We believe that through mobility, our society can be transformed for the better. New innovations and forms of expression are finding a greater audience, industries and hierarchies are being revolutionized, and we are seeing a fundamental change in the way we communicate, socialize and make decisions together.

These exciting changes represent the realization of our vision: a Networked Society, where every person and every industry is empowered to reach their full potential.

Ericsson AB
SE-126 25 Stockholm, Sweden
Telephone +46 10 719 0000
www.ericsson.com