Considerations, Best Practices and Requirements for a Virtualised Mobile Network

About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with almost 300 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series of conferences.

For more information, please visit the GSMA corporate website at www.gsma.com. Follow the GSMA on Twitter: @GSMA.

Network 2020

The GSMA's Future Networks Programme is designed to help operators and the wider mobile industry to deliver all-IP networks so that everyone benefits regardless of where their starting point might be on the journey.

The programme has three key work-streams focused on: The development and deployment of IP services, The evolution of the 4G networks in widespread use today, The 5G Journey developing the next generation of mobile technologies and service.

For more information, please visit the Network 2020 website at: www.gsma.com/network2020

With thanks to contributors:
AT&T
China Mobile
China Telecom
China Unicom
KDDI
KT
LG Uplus
NTT DoCoMo
Orange
Proximus
America Movil
SK Telecom
Telecom Italia
Telefónica
Telekom Austria
Telenor Group
TeliaSonera
T-Mobile US
United States Cellular
Vodafone
Ascom Network Testing
Cisco
Ericsson
Gemalto
HP
Huawei
Nokia
Oracle America
Samsung Electronics
ZTE

Contents

CONSIDERATIONS, BEST PRACTICES AND REQUIREMENTS FOR A VIRTUALISED MOBILE NETWORK

1

Introduction

1.1 Scope

This document outlines the key considerations in the deployment of network virtualisation in a mobile network environment. The topics covered within represent solutions to the potential obstacles mobile operators may face when wishing to capitalize on network virtualisation (covering both Network Functions Virtualisation and Software-Defined Networking).

This document provides an overview of the steps mobile operators should take to adopt this technology and where appropriate, provide an indication of what they will need to complete the work and which external organisations are best placed to deliver it.

The document also outlines a number of examples and approaches that have been taken by operators to identify and address the gaps. These best practice examples are provided as guidance and do not represent the consensus of the GSMA members participating to this activity.

1.2 Those are Definitions

Term	Description
Lifecycle management	Set of functions required to manage the instantiation, maintenance and termination of a Virtualised Network Function or Network Service
Network controller	Functional block that centralizes some or all of the control and management functionality of a network domain and may provide an abstract view of its domain to other functional blocks via well-defined interfaces
Network Function	Functional block within a network infrastructure that has well-defined external interfaces and well-defined functional behaviour
Network Functions Virtualisation	Principle of separating Network Functions from the hardware they run on by using virtual hardware abstraction
Network Functions Virtualisation Orchestrator	Functional block that manages the Network Service lifecycle and coordinates the management of Network Service lifecycle, Virtualised Network Function lifecycle and NFV infrastructure to ensure an optimized allocation of the necessary resources and connectivity
Network Functions Virtualisation Infrastructure	Totality of all hardware and software components that build up the environment in which Virtualised Network Functions are deployed
Network service orchestration	Subset of Network Functions Virtualisation Orchestrator functions that are responsible for Network Service lifecycle management
Network service descriptor	Template that describes the deployment of a Network Service including service topology as well as Network Service characteristics such as Service Layer Agreements for the Network Service on-boarding and lifecycle management of its instances
Network Service	Composition of Network Functions and defined by its functional and behavioural specification
Orchestration	Type of composition where one particular element is used by the composition to oversee and direct the other elements
Quota	Upper limit on specific types of resources
Resource orchestration	Subset of Network Functions Virtualisation Orchestrator functions that are responsible for global resource management governance
Service lifecycle	Set of phases for realizing a service from conception and identification to instantiation and retirement
Software-Defined Networking	A set of techniques that enables to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner
SDN Orchestration	A process that oversees and directs a set of software-defined networking activities and interactions with the objective of carrying out certain work in an automated manner.
Virtualised Infrastructure Manager	Functional block that is responsible for controlling and managing the Network Functions Virtualisation Infrastructure compute, storage and network resources, usually within one operator's Infrastructure Domain
Virtualised Network Function	Implementation of an Network Function that can be deployed on a Network Function Virtualisation Infrastructure
Virtualised Network Function Component	Internal component of a Virtualised Network Function providing a defined sub-set of that Virtualised Network Function's functionality.

1.3 Abbreviations

Term	Description
API	Application Programming Interface
ATIS	The Alliance for Telecommunication Industry Solutions
BSS	Business Support Systems
CAPEX	Capital Expenditure
CNI	Critical Network Infrastructure
CPU	Central Processing Unit
DPDK	Data Plane Development Kit
DUT	Device Under Test
ECOMP	Enhanced Control, Orchestration, Management & Policy
EOSL	End of Service Life
EPC	Evolved Packet Core
EM	Element Management
ETSI	European Telecommunications Standards Institute
ETSI GS	ETSI Group Specification
FCAPS	Fault, Configuration, Accounting, Performance and Security
GS-O	Global Service Orchestration
ICT	Information and Communications Technology
IoT	Internet of Things
IPC	Instructions Per Cycle
iTLB/dTLB	instruction Translation Lookaside Buffer / data Translation Lookaside Buffer
ISB	Industry Standard Benchmarking
ISG	Industry Specification Group
KPI	Key Performance Indicator
KVM	Kernel-Based Virtual Machine
L1/L2/LLC	Level 1/Level 2/ Last Level Cache
Open-O	Open Orchestrator Project
OPEX	Operating Expense
OPNFV	Open Platform for NFV
OS	Operating System
OSM	Open Source MANO project
OSS	Operations Support Systems
OVS	Open vSwitch
PGW	Packet Data Network Gateway
PNF	Physical Network Function
RAN	Radio Access Node
RFC	Request For Comments
MANO	Management and Orchestration
MME	Mobility Management Entity
MVNO	Mobile Virtual Network Operator
NextGen	Next Generation
NF	Network Function
NFV	Network Functions Virtualisation
NFV-O	Network Functions Virtualisation Orchestrator
NFVI	Network Functions Virtualisation Infrastructure
NOC	Network Operations Centre
NS	Network Service
SDN	Software Defined Networking
SDN-O	Software Defined Networking Orchestration
SHV	Standard High Volume
SGW	Serving Gateway
UMO	Unified Management and Orchestration
vACL	virtual Local Area Network Access Lists

vCG-NAPT	virtual Concatenation Group Network Address Port Translation
vEPC	virtual Evolved Packet Core
vFW	virtual Fire Wall
vMME	virtualised Mobility Management Entity
vPE	virtual Provider Edge
vSwitch	virtual Switch
VIM	Virtualised Infrastructure Manager
VM	Virtual Machine
VNF	Virtualised Network Function
VNFC	Virtualised Network Function Component

1.4 References

Ref	Doc Number	Title
[1]	GS ETSI NFV 002	Network Functions Virtualization (NFV); Architectural Framework
[2]	GS ETSI NFV-MAN 001	Network Functions Virtualisation (NFV); Management and Orchestration
[3]	GS ETSI NFV-IFA 009	Network Functions Virtualisation (NFV); Management and Orchestration; Report on Architectural Options
[4]	GS ETSI NFV-IFA 010	Network Functions Virtualisation (NFV); Management and Orchestration; Functional requirements specification
[5]	ITU-T Y.3300	Framework of software-defined networking
[6]	ISO/IEC 18384-1	Reference Architecture for Service Oriented Architecture (SOA RA) Part 1: Terminology and Concepts for SOA
[7]	NGMN	5G white paper
[8]	AT&T Ecomp	Enhanced Control, Orchestration, Management & Policy Architecture; http://about.att.com/content/dam/snrdocs/ecomp.pdf
[9]	Open-O	Open-O architecture; www.open-o.org
[10]	OSM	Open Source MANO; http://osm.etsis.org/
[11]	ETSI GS NFV-REL006 V0.0.3 (2016-07)	Network Function Virtualisation (NFV); Reliability; Specification on Software Update Process
[12]	Yardstick	https://wiki.opnfv.org/display/yardstick
[13]	Bottlenecks	https://wiki.opnfv.org/display/bottlenecks
[14]	StorPerf	https://wiki.opnfv.org/display/storperf
[15]	VSPerf	https://wiki.opnfv.org/display/vsperf/VSperf+Home
[16]	CPerf	https://wiki.opnfv.org/display/cperf
[17]	GS ETSI NFV 001	ETSI GS NFV 001: “Network Function Virtualisation (NFV); Use Cases”
[18]	GS ETSI TST 001	ETSI GS NFV-TST 001: “pre-deployment testing, report on validation of NFV environments and services”
[19]	GS ETSI TST 002	ETSI GS NFV-TST 002: “Testing Methodology; Report on NFV Interoperability Testing Methodology”
[20]	GS ETSI PER 001	ETSI GS NFV-PER 001: “NFV performance and portability best practices”
[21]	GS ETSI IFA 003	ETSI GS NFV-IFA 003 V2.1.1: “Network Functions Virtualisation (NFV); Acceleration Technologies; vSwitch benchmarking and acceleration specification”
[22]	draft-ietf-bmwg-virtual-net-04	https://datatracker.ietf.org/doc/draft-ietf-bmwg-virtual-net/
[23]	draft-ietf-bmwg-ipsec-term-12	IETF: draft-ietf-bmwg-ipsec-term-12.txt, “Terminology for Benchmarking IPsec Devices”.
[24]	draft-ietf-bmwg-ipsec-meth-05	IETF: draft-ietf-bmwg-ipsec-meth-05.txt, “Methodology for Benchmarking IPsec Devices”.
[25]	draft-ietf-bmwg-vswitch-opnfv-01	IETF: draft-vsperf-bmwg-vswitch-opnfv-01.txt, “Benchmarking Virtual Switches in OPNFV”.
[26]	draft-kim-bmwg-ha-nfvi-01	IETF: draft-kim-bmwg-ha-nfvi-01.txt, “Considerations for Benchmarking High Availability of NFV Infrastructure”.
[27]	GS ETSI NFV-REL001	ETSI GS NFV-REL001 “Network Functions Virtualisation (NFV); Resiliency Requirements”
[28]	ETSI NFV-SEC 007	ETSI GS NFV-SEC 007 “Network Functions Virtualisation (NFV); Trust; Report on Attestation Technologies and Practices for Secure Deployments”
[29]	ETSI GS NFV-SEC 013	ETSI GS NFV-SEC 013 “Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification”
[30]	ETSI GS NFV-SEC 012	ETSI GS NFV-SEC 012 “Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components”
[31]	ETSI TS 103 308	ETSI TS 103 308 “CYBER; Security baseline regarding LI and RD for NFV and related platforms”

2

NFV reference architecture

Figure 1 shows the NFV reference architectural and functional blocks [1]. The functional blocks are:

- Operations Support Systems (OSS) and Business Support Systems (BSS).
- Element Management (EM);
- Virtualised Network Function (VNF);
- Service, VNF and Infrastructure Description;
- VNF Manager(s);
- NFV Orchestrator;
- Virtualised Infrastructure Manager(s) (VIM);
- NFV Infrastructure (NFVI), including hardware and virtual compute, storage and network resources

A VNF is an implementation of a Network Function that can be deployed in an NFV Infrastructure. Examples of mobile network functions are Mobility Management Entity (MME), Serving Gateway (SGW), Radio Access Node (RAN) and Packet Data Network Gateway (PGW).

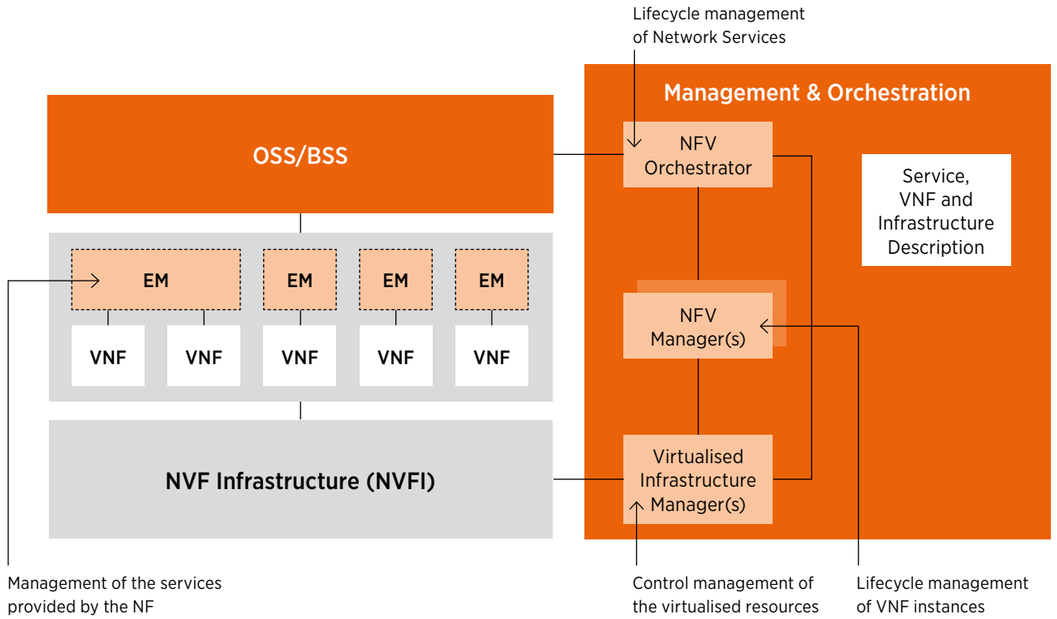
The NFV Orchestrator is responsible for the management and orchestration of NFV infrastructure, as well as the software resources and delivering the network services on the NFV infrastructure. The ISG ETSI NFV [3] identifies the following management and orchestration data repositories:

- VNF Catalogue;
- NS Catalogue;
- NFV Instances repository;
- NFVI Resources repository

The NFV Orchestrator has two main responsibilities:

- Network Service Orchestration: managing the lifecycle of network services. This includes the management of the Network Services templates and VNF Packages. The Network Service Orchestration provides the management of the instantiation of VNFs, in coordination with VNF Managers;
- Resource Orchestration: providing an overall view of the resources to which it provides access and hides the interfaces of the VIMs present below it

Figure 1: NFV architecture



Source: GS ETSI NFV-002 Network Function Virtualization (NFV); Architecture Framework

3

Requirements for Network Orchestrator

3.1 Introduction

Network Functions Virtualisation requires a new set of management and orchestration functions to be added to the current model of operations, administration, maintenance and provisioning. The Network Functions Virtualisation Management and Orchestration has the role of managing the NFVI and control the allocation of resources needed by the NSs and VNFs.

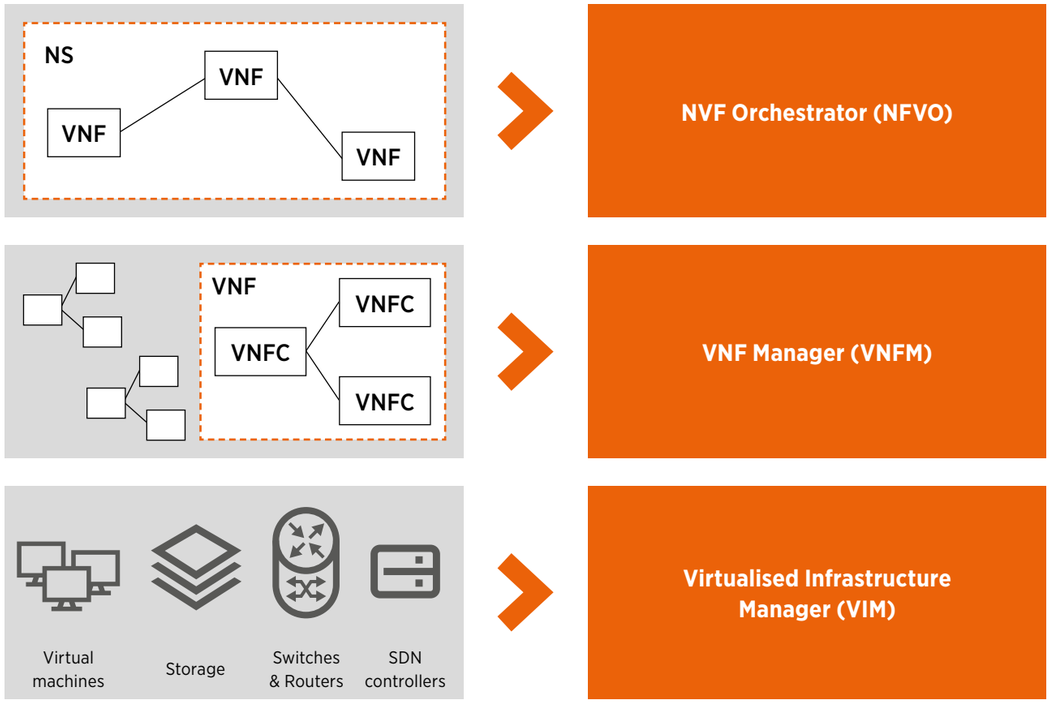
The management and orchestration takes place at three different levels as depicted in Figure 2.

3.1.1 Network Services

The Network Service Orchestration is responsible for the Network Service lifecycle management including operations such as:

- On-board and management of Network Service Descriptors;
- Instantiate Network Service;
- Scale Network Service;
- Update Network Service;
- Terminate Network Service

Figure 2: Management & Orchestration at different abstraction levels



Source: Orange

3.1.2 Virtualised Network Functions

The management and orchestration elements of a VNF include fulfilment, assurance and security management, however, the focus in NFV is the decoupling of the VNF software from the hardware. The decoupling of Network Functions from the physical infrastructure results in a new set of management functions that are focused on the creation and lifecycle management of virtualised resources for the VNF, referred to as VNF Management. VNF Management functions are responsible for the VNF's lifecycle management including operations such as:

- Instantiate VNF (create a VNF instance using the VNF on-boarding artefacts);
- Scale VNF (increase or reduce the capacity of the VNF);
- Update and/or Upgrade VNF (support VNF software and/or configuration changes of various complexity);
- Terminate VNF (release VNF-associated NFVI resources and return it to NFVI resource pool)

3.1.3 Network Functions Virtualisation Infrastructure

Network Functions Virtualisation Infrastructure (NFVI) resources under consideration are both virtualised and non-virtualised resources, supporting virtualised network functions and partially virtualised network functions.

Virtualised resources are offered for use through abstracted services, for example:

- Network, including: networks, subnets, ports, addresses, links and forwarding rules, for the purpose of ensuring intra- and inter-VNF connectivity;
- Compute including machines, and virtual machines, as resources that comprise both CPU and memory;
- Storage, including: volumes of storage at either block or file-system level

3.2 NFV Orchestrator functional requirements

The Network Orchestrator shall fulfil all requirements specified in clause 6 of ETSI NFV-IFA 010 [5] applicable to an NFVO. These requirements include functional requirements for VNF lifecycle, Network Service lifecycle and virtual resource management summarized as follows:

- Network Service:
- lifecycle management (instantiation, scaling, updating, termination);
- information management (NS descriptor);
- performance management;
- fault management

VNF:

- lifecycle management (instantiation, scaling, termination);
- information (VNF package) management;
- configuration management (initial configuration and update);
- performance management;
- Indicator management
- fault management

Virtualised resource management:

- direct/indirect, reservation;
- capacity, fault, performance;
- network forwarding path;
- information;
- quota, allowance

Other requirements are also considered for:

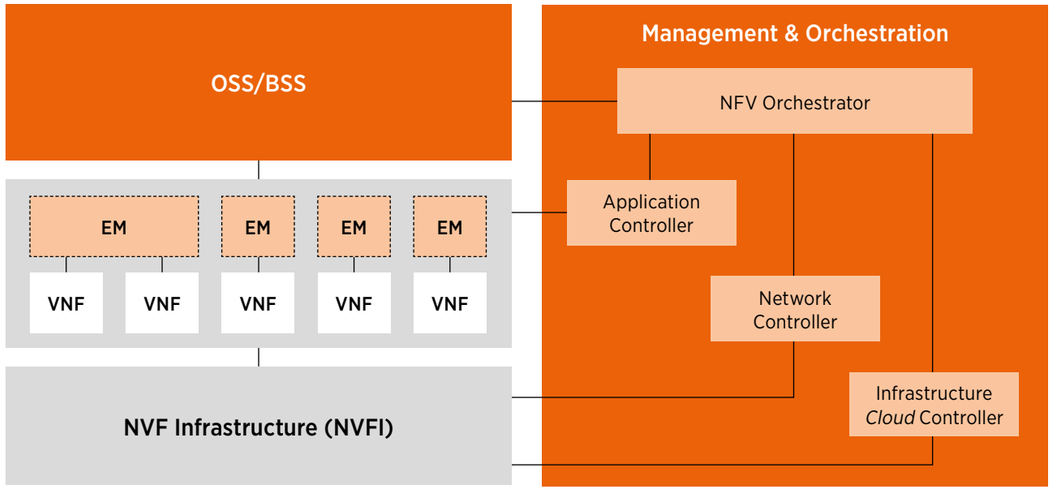
- Multi-Tenancy (Tenant management);
- Infrastructure resource management;
- Software image management;
- NFV acceleration management;
- Security consideration;
- Policy administration

3.3 Other NFV related architectures

In NFV reference architecture, the VIM can play the role of an SDN application, sitting on top of the northbound interfaces of the SDN controller. The VIM delegates to the SDN controller the connectivity management of virtualised network resources that are required by network services and their constituent network functions. This architecture does not propose a direct interface between the NFV-O and SDN controllers. However, in some architecture (e.g. AT&T ECOMP architecture), a Master Orchestrator for NFV and SDN acts as an NFV-O and as a direct consumer of the APIs exposed by an SDN controller.

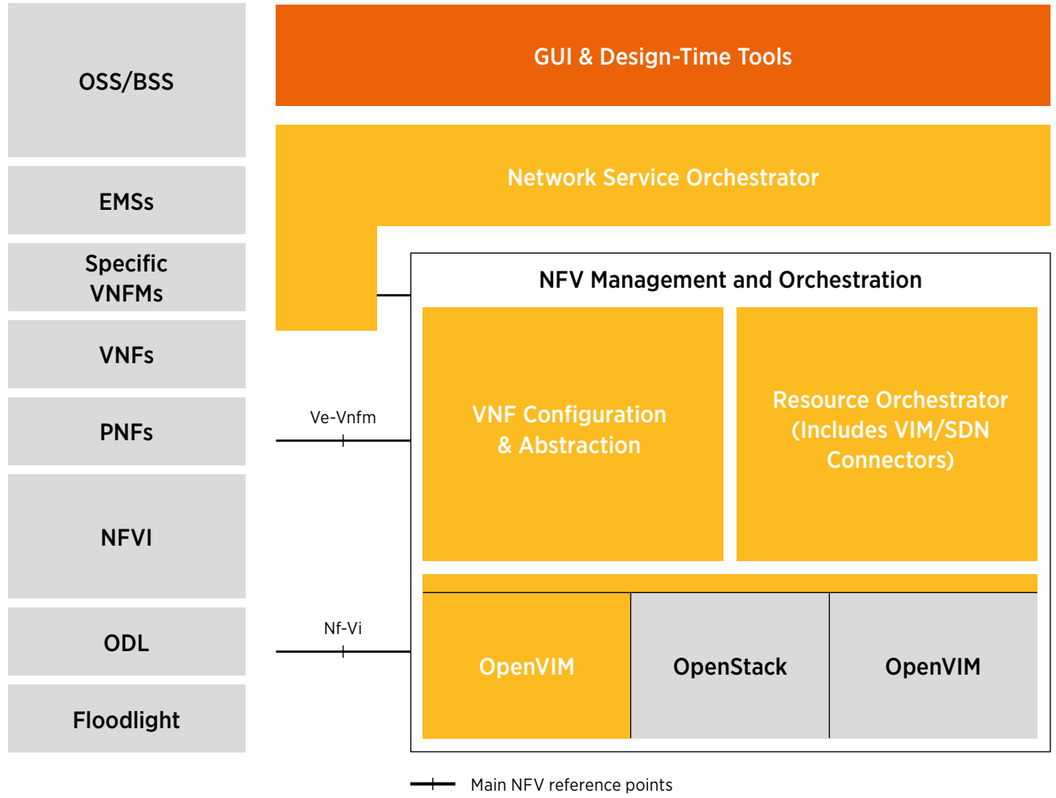
In the case of the OSM project, as shown in Figure 4, the SDN controller is a well-defined part of the resources managed by the Resource Orchestrator, rather than accessing it exclusively through the VIM interface. This provides finer control of network configuration, decouples resource and cloud-native lifecycle management and supports multi-VIM services at the Resource Orchestrator level.

Figure 3: ECOMP orchestration architecture



Source: ECOMP www.openecomp.org

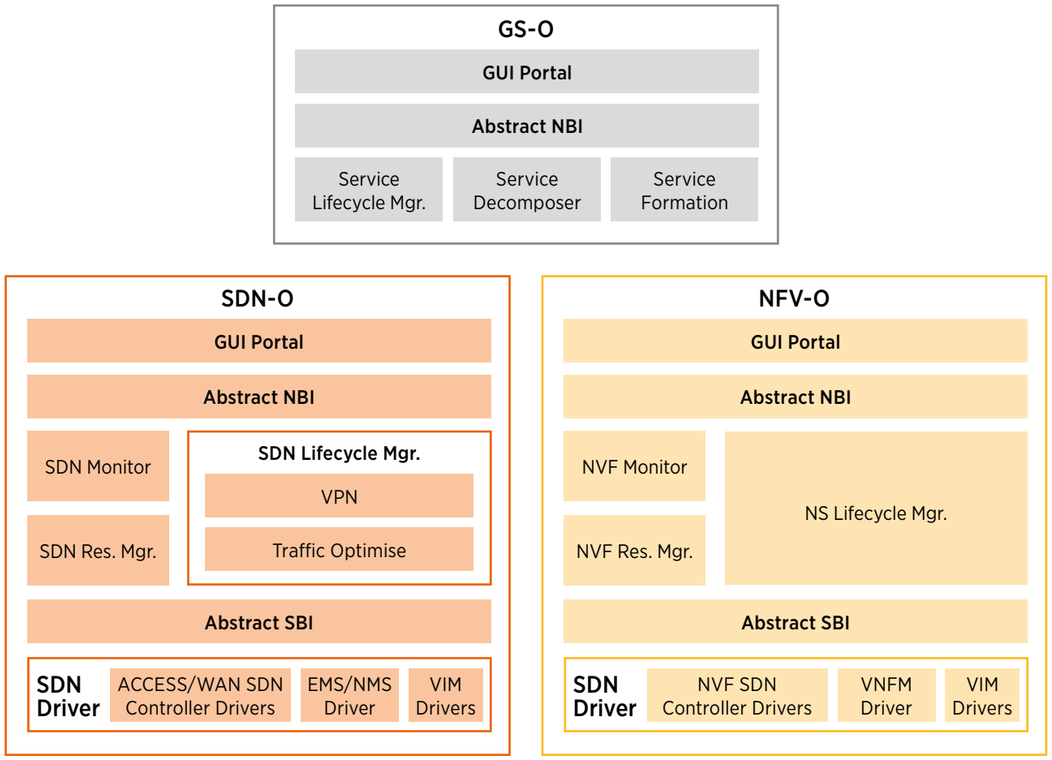
Figure 4: OSM architecture mapping onto ETSI NFV framework elements



Source: OSM Project

In another architectural approach, the SDN Orchestrator can be separated from the NFV Orchestrator (e.g. Open-O architecture) to manage the SDN service connectivity independently from NFV (e.g. for VPN on Demand use case). In this approach, a Global Service Orchestrator GS-O is placed on the top of the SDN-O and NFV-O orchestrators.

Figure 5: Open-O orchestration architecture



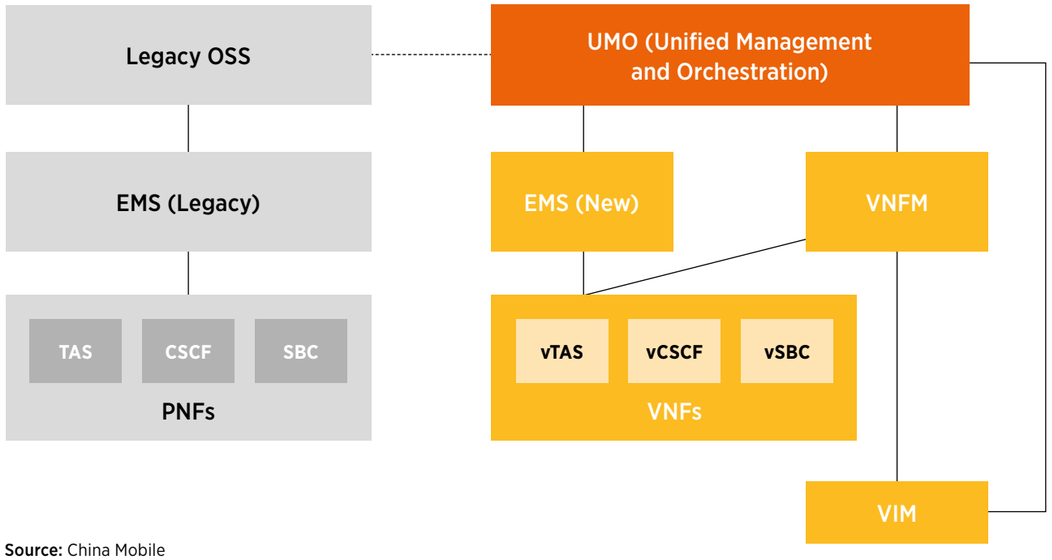
Source: Open-O www.open-o.org

3.4 Best Practices

3.4.1 Planning an NFV based network management and orchestration architecture

Figure 6 shows an example of an architecture for a future NFV based network management strucuture from an implementation based on China Mobile's network. In this architecture, the complete network management system can be divided into two parts. The right section is a sub-system managing VNFs under UMO (Unified Management and Orchestration). The UMO is China Mobile's NFV based network management and orchestration system. The left section shows the legacy OSS: in order to avoid having to reconstruct the existing sub-system, the legacy OSS will stay unchanged and will continue to manage existing PNFs. An interface between legacy OSS and UMO is not precluded and could be a proprietary interface, based on operators' requirements.

Figure 6: possible NFV based network management and orchestration architecture



Source: China Mobile

The UMO is a combination system that has the capability of network orchestration, VNF and NS lifecycle management. It also covers policy design and management, resource management and VNF FCAPS management.

The benefit of this architecture is that the role and responsibilities of legacy OSS and UMO are clear, separate and defined. The UMO can be considered a unified system designed to manage the whole virtualised network. All the information needed for a mobile network service, VNF and NS resource management will be handled by the UMO only, which has no impact on the legacy network.

3.4.2 Example of 5G Telco-MANO architecture

ETSI's Network Functions Virtualisation (NFV) Industry Specification Group (ISG) is defining NFV-MANO architecture. This is a framework for the management and orchestration of all resources in the cloud computing infrastructure as well as NS and VNF lifecycle management.

Some network functions are hard to transform to virtualised network functions (VNFs) and will remain as physical network functions (PNFs).

These hybrid physical and virtual network environments should be considered for a 5G Telco management and orchestration architecture. 5G Telco-MANO is required to provide end-to-end network provisioning for 5G network slicing on demand and one-view network monitoring instead of monitoring physical and virtual network(s) separately. 5G Telco-MANO should also be easy to implement.

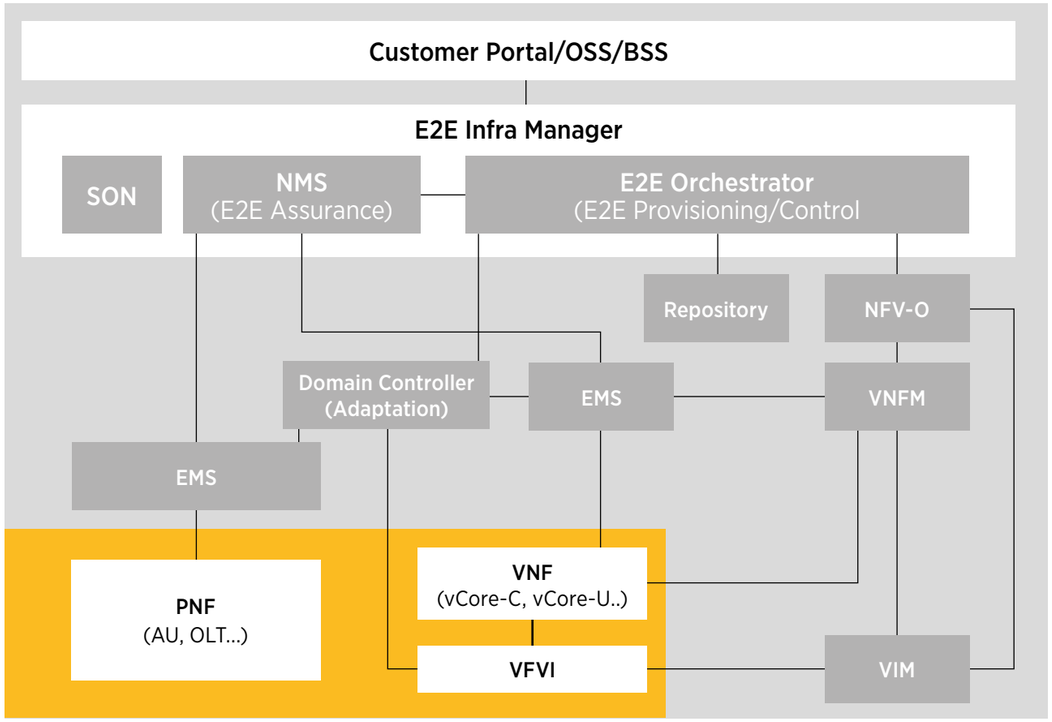
Figure 7 shows an example of a 5G Telco-MANO architecture.

In this architecture, NMS-Assurance is used for end-to- end network assurance. NMS-Assurance is the most widely used network assurance system in PNF networks and can be extended as a virtual networks assurance system with the help of EMS and VNF. Thanks to the reuse of NMS- Assurance, end-to-end network assurance can be easily implemented to avoid the complexity of reconstructing a system from scratch. E2E orchestrator and domain controllers are new elements designed to support end-to-to-end network provisioning and configuration. In each network domain, a network controller (for example, Transport-SDN, Cloud SDN) will provision and configure the network function with an open interface regardless of whether they are physical or virtualised network functions, with the interfacing of an E2E orchestrator. In this way, an E2E orchestrator can provision a 5G network slice using both PNFs and VNFs end-to-end.

In addition to NFV-MANO defined interfaces, Figure 6 shows interfaces between an E2E orchestrator and domain controllers as well as between domain controllers and EMS that are necessary for the 5G Telco MANO architecture to work.

By following this approach, a 5G Telco-MANO, end-to-end on-demand network provisioning and one-view network assurance in physical and virtual hybrid networks can be achieved.

Figure 7: Possible end-to-end management and orchestration architecture for 5G



Source: KT

4

Virtualised network security

4.1 Introduction

NFV can greatly amplify existing security problems in terms of impact. The vulnerabilities are similar to those of today, but instead iNFV concentrates them in one place and increases the likelihood of a common mode failure. In many ways, it puts all our “security eggs in one basket”. In traditional telecommunications equipment, a number of factors helped to frustrate would be attackers such as physical security, proprietary software, hardware, installation and configuration and reduced the ability to exploit vulnerabilities.

4.1.1 Maturity

No vendor is at an advanced stage when it comes to compliance with national security regulations regarding NFV. A number of interested parties are working hard with standardisation bodies to include and embed security from the ground up. We do not anticipate seeing mature NFV products/ solutions implementing the latest security standards (e.g. ETSI NFV SEC) in the near future. Therefore, any product currently available today is highly unlikely to have the required security built in. Indeed, many NFV vendors are new to telecommunications security concepts. The cloud technologies being used to underpin NFV are not of the maturity required to underpin Critical Network Infrastructure (CNI) and iits related obligations.

The main threat vectors for a virtual network remain fundamentally unchanged:

- **Loss of availability:** Attacks that result in crashing a virtual network element or rendering it unusable through flooding/denial of service;
- **Loss of confidentiality:** Either caused by eavesdropping or leakage of sensitive data;
- **Loss of integrity:** Resulting from a modification of data during transit (man-in-the-middle-attack) or in the virtual network element, as well as from unauthorised access to a virtualised network function;
- **Loss of control:** Loss of control can take place at the network level where the attacker controls the network exploiting a protocol or implementation flaw or at virtual function level

Another threat that needs to be considered in virtualised networks is the possible absence of a single entity overseeing the whole network. This is because a virtual network (Figure 1) can be easily subdivided in to different administrative domains each with different elements requiring the establishment of secure interaction between themselves.

4.2 Architectural Challenges

This section lists the security aspects that operators deploying a virtualised network need to take into account.

- Integrity of infrastructure and VNF
- Several Trust Domains:
  - A Trust Domain is a collection of entities that share security policies
  - Even in the context of a single CSP:
    - a dedicated trust domain for LI in addition to an admin trust domain
  - Regulation geographical constraints with location attestation ensuring that LI can only take place on known POI/IAP
- Separation of LI function executions from other VNF and Hypervisor is considered a requirement
  - Segregation of Lawful Interception information/ flows. Monitoring behaviour of infrastructure should not decrease the confidentiality of a Lawful Interception solution
  - Encrypted targets DB in a separate/secured context
  - Secure Encryption
    - a location to store “properly” keys ensuring that they can’t be compromised by e.g. a privileged hypervisor manager or other process.
  - Secure execution

4.3 Best practices

The GSMA Fraud and Security Group’s (FASG) preliminary discussions on NFV security highlighted 5 key security risks operators need to take into account:

- **Legal and Regulatory Compliance failure:** Core risks are about geographic deployment and security of solutions, particularly in heterogeneous environments;
- **Isolation Failure:** Core risk is around functions “escaping” from allocated resources, enabling prejudicial data access to extensive areas of information (at rest, in motion or in memory);
- **Denial of Service:** Risks include flooding of public interface or resource exhaustion (e.g. on internal network or memory);
- **Topology Validation and Enforcement:** Risk is around malicious configuration (e.g. VM layer misconfiguration);
- **Security Logging and Incident Management:** Risks arise from failures to log or manage issues from complex interactions across domains

FASG also elaborated on mitigation strategies for the above risks highlighting the importance of a strong cooperation between operators, manufacturer and where appropriate regulators. Three recommendations are made:

- Vendors shall be required to adopt best-of-breed security features as specified by ETSI NFV SEC and operators:
  - Location attestation means
  - Root of Trust (NFV SEC 007 [27]).
  - Multiple Trust Domains (NFV SEC 013 [28]).
  - Execution Enclaves for Sensitive Applications (NFV SEC 012 [29])
- The open-source community needs to be motivated to include basic security measures. A “fixing as we go along” approach is not suitable for this environment;
- Everyone needs to develop a secure architecture with separate zones of trust

4.4 Conclusions

- Security for NFV is still a work in progress
- Security involves all NFV architecture components (VNF level, NFVI, MANO)
- LI community requires the strongest requirements
- LI Requirements / Security for LI Function will depend on National Regulations / Countries
- Still quite difficult to establish the right level of requirements for RFI/RFP

4.5 Actions

- All vendors must be able to credibly answer (with evidence) a set of basic questions around the security of their NFV products in accordance with ETSI TS 103 308 [30]
- Operators should consider a delay in the use of NFV where sensitive functions are involved, unless appropriate mitigations are available
- Government regulatory advice should provide greater clarity, now, on the potential security risks around NFV, and be able to legally and competently deal with this topic

CONSIDERATIONS, BEST PRACTICES AND REQUIREMENTS FOR A VIRTUALISED MOBILE NETWORK

5

Carrier grade NFV/ Reliability

5.1 Introduction

5.1.1 Carrier-grade

In telecommunications, "carrier-grade" refers to a system, or hardware or software component that is extremely reliable, well tested and proven. Carrier grade systems are tested and engineered to meet or exceed the "five-9s" (99.999%) availability standards, that provide resiliency and fast fault recovery.

Product or service development within the telecommunications industry has traditionally followed rigorous standards for stability, protocol adherence and quality, reflected by the use of the term 'carrier-grade' to designate equipment demonstrating this reliability. Over time, telecom service providers have engineered an extensive range of sophisticated features into their networks, to the point where they can guarantee their high reliability.

However, it is difficult to achieve the same grade of high reliability in each component of the NFV network. What is important for service providers is to be able to offer carrier grade services that meet the required availability, reliability and performance requirements for end-to-end voice, video, data or converged-services.

5.1.2 The essential value of carrier-grade reliability

Telecom networks must be always-on and guarantee a level of service because society, business and industries increasingly depend on reliable connections for both routine and critical communications.

Always-on reliability is mandatory and telecom service providers have built their networks, reputations and revenue streams on a foundation of carrier-grade reliability. A carrier-grade network guarantees a 'five-9s' availability standard, that allows for no more than 5.27 minutes of downtime per year per service. If there is just one failure in the system, the NOC (Network Operations Centre) will be notified and proceed with remediation in less than 5 minutes so that the five-9s target can still be met. Hence there is an overwhelming need to automate the entire process, including quick service recovery processes and to provide a seamless transfer from the failing element to healthy elements.

This level of service is typically required by high-value enterprise customers who often will pay a premium for Service Level Agreements that specify high availability.

Figure 8: The benefits of Carrier-grade NFV for Operators

5.1.3 NFV carrier-grade reliability challenges

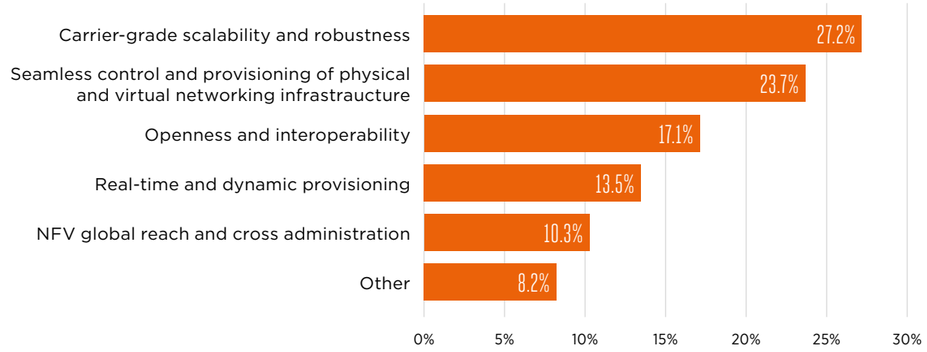
With all the industry initiatives around NFV, network reliability has become a hot topic, as shown in a survey published by Heavy Reading in Jan 2015, as well as some challenges experienced by the industry when implementing NFV:

- Service recovery in a multi-layer or multi-vendor environment
- Carrier-grade reliability when NFV has components with a lower grade of reliability
- New skills and process requirements
- Multi-component interoperability management
- Security concerns
- Complexity in E2E problem demarcation

When service providers refine their plans to introduce NFV into their networks, they are also reviewing the implications for high reliability on a network infrastructure that incorporates virtualised functions.

There are numerous initiatives underway currently to specify, align and promote NFV carrier-grade capabilities for achieving efficient carrier-grade NFV solutions. These include ETSI NFV Proof of Concept, Open-Platform for NFV project, Carrier Network Virtualisation Awards, ATIS (The Alliance for Telecommunication Industry Solutions) and various supplier ecosystems.

Figure 9: Challenges faced by the NFV Testing Market

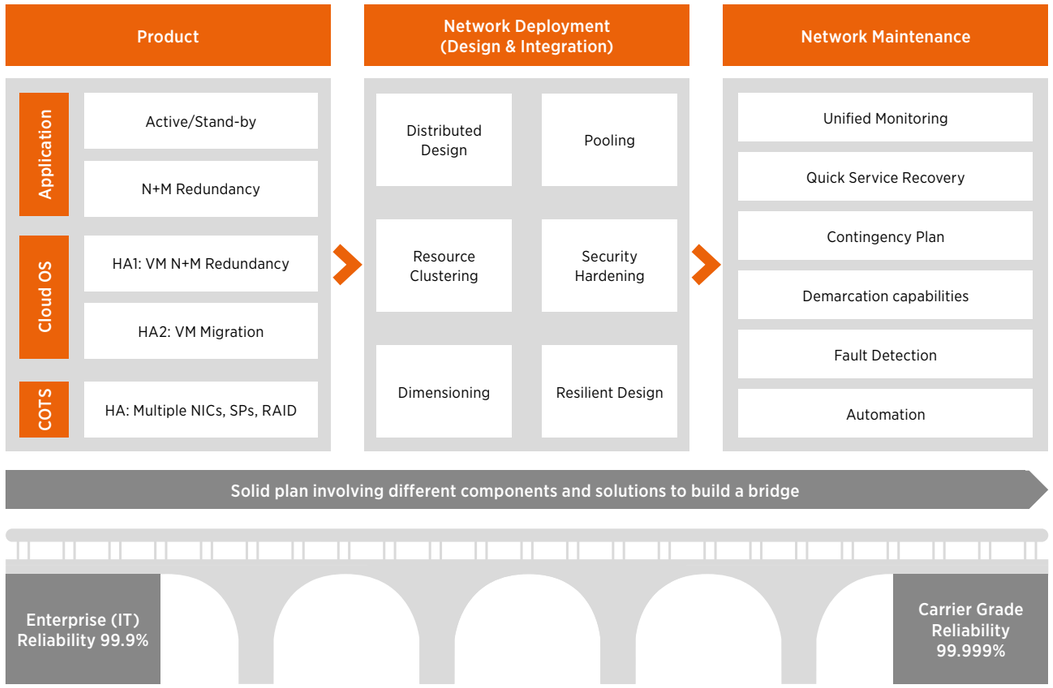


Source: Heavy Reading Mobile Networks Insider

5.1.4 NFV carrier-grade reliability scope

Practically, there are 3 key areas in achieving NFV-driven carrier-grade reliability: product, network deployment (design and integration) and network maintenance.

Figure 10: End-to-End Carrier-grade Reliability Scope



Source: Huawei

1. Each product should be highly reliable and fault resilient. Different types of resiliency can be applied such as “1+1” or “N+M” (simple 1+1 redundancy is deprecated as a recommended strategy for resilience). For stateful applications, data synchronization and restoration mechanisms should be in place for state continuity in case of component failure. Furthermore, to respond to a failure of a physical or virtual element within an NFV platform, the management software must be able to detect failed components, hosts, or virtualisation solutions (e.g. VMs) immediately and recover automatically, if possible through an autonomous response mechanism (example: virtual machine migration).

2. Networks should be deployed in a way so that failure in a node will not impact service continuity. This can be achieved with distributed design across multiple sites, deploying additional resources and proper dimensioning. Also, it is important to consider a feature deployment and system configuration that can protect a network from different threats. It is desirable that the network is able to identify events or drivers in the network as well as external to the network that could degrade or otherwise impair the quality or availability of the supplied services. For example, if a network received a significant increase in traffic beyond the level it was engineered to expect.

NOTE: ETSI NFV ISG (Industry Specification Group) has provided some guidelines and best practices on product reliability and resilient network design [27].

3. Most of the challenges are in network maintenance. Even if a redundant network is deployed, failures can happen. Therefore, it is critical to follow a proactive, predictive and pre-emptive approach that identifies incidents before they impact users. This can be achieved using extensive telemetry to monitor the different components in the NFV network. Moreover, this complexity and scale requires fault conditions to be identified by network probes with management tools in place that should be responded to by pre-programmed event responders (autonomics – big data analytics. This allows the creation of algorithms to perform tasks within seconds that may otherwise take operations engineers hours or days to resolve.
    1. When large scale failure does occur, emergency handling capabilities are needed to recover the services quickly and minimize impact.
    2. Organizations must ensure staff have the right skills as well as the appropriate tools and right processes in place. They must also ensure network management capabilities meet the same dependable level of carrier-grade reliability expected by customers.

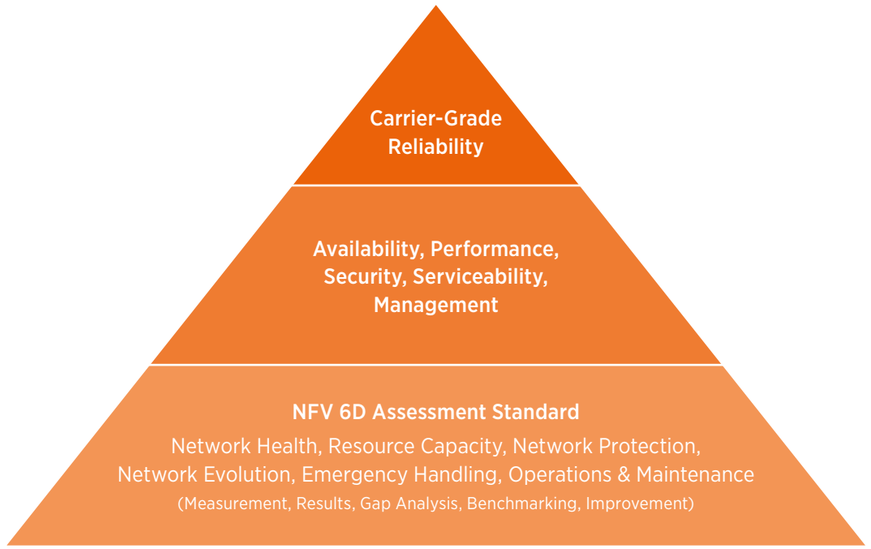
5.2 Carrier Grade Service – Requirements for NFV Reliability

As illustrated in the diagram below, there is a daunting list of requirements for achieving carrier-grade reliability and deliver the always-on connectivity expected by service providers and their customers. Such reliability is attained by complying with a very stringent criteria of availability, security, performance, serviceability and management requirements, which fall into six primary dimensions (6D) for a NFV-driven carrier-grade system.

5.3 NFV Reliability Assessment Standard

In order to provide an ultra-reliable, highly secure and fully connected network, an in-depth and comprehensive NFV network assessment framework has been developed.

Figure 11: Requirements for Carrier-Grade NFV Reliability



Source: Huawei

Figure 12: Carrier-Grade NFV Reliability Assessment Framework

6 Dimensions	Network Health	Resource Capacity	Network Protection	Network Evolution	Network Handling	Operations & Maintenance
360° Assessment Elements/ Formulas	Hardware Health	Software Licensing	Overload Protection	Inter-operability	Network Information (Example: Design and Topology)	Staff / Organisation Skills
	Virtualisation Layer Health	Physical Resources	Autonomous Response Mechanism (Example: Virtual Machine Migration)	Zero downtime Software Upgrade	Emergency Case Processes	Tools/ Platforms (Example: Network Telemetry)
	VNF Health	Link Utilisation	Security	Deployment of new function, feature, technology	Disaster Recovery Capabilities	Processes
	Connectivity	Scaling	Resiliency	Hardware upgrade and expansion		
	Grey Failure	Load Balancing				
	MANO					
Input	Design	Alarms/ Log-files	Statistics	Configuration	Topology	Processes	Features

Source: Huawei

1. **Network Health**
   NFV brings a lot of new challenges to operators due to its architecture. With regards to network health, operators need to consider several new elements when compared to PNF (physical network function) that should be in a healthy status, otherwise they may impact a network's reliability. Also, if there is deterioration in a basic service KPI then it should be treated quickly and automatically, to minimize the downtime or eliminate the impact on users. Some of the critical elements which should be monitored regularly and proactively include hardware and software components, the virtualisation layer as well as connectivity and network performance. Predictive fault detection becomes more important in NFV, because applications use infrastructure delivered by other vendors. For example, operators should identify grey failures in advance, such as a memory leak or CPU overutilization (based on a traffic model) that have not yet affected the service performance and end users.

2. **Resource Capacity**
   How efficiently and effectively resources are utilised (e.g. software, hardware, links) is critical for NFV network reliability. Operators need to monitor and avoid overloading resources above the network's designed thresholds and maintain load-balance between the resources. NFV introduces scaling capabilities in order to enhance a network's agility and reliability.

3. **Network Protection**
   Networks should be protected from all possible threats which can impact services. NFV brings a number of new challenges such as cloud computing, component scalability and resiliency, information, cyber security and network access provisioning. A network should be protected from known threats, such as signalling storms (overload protection), denial of service attacks and hardware or software failures. A network should be designed properly for its resilience (no single point of failure) and should be able to recover automatically when possible (migration, reconstruction etc.). A robust network shouldn't be vulnerable to any of these threats.

4. Network Evolution

A network is always evolving with the introduction of new features, functions, services, technologies, software upgrades and hardware equipment etc. NFV increases the complexity further with a larger number of components and vendors. A reliable, high-performance network might be impacted after a change in one of the layers. For example, when a vendor's hardware is incompatible with some of the components for a server capacity expansion which creates interoperability issues impacting network reliability. As a result, openness is critical in driving innovation and enhancing reliability. Open interfaces (APIs) play a vital role in building carrier-grade services. Additionally, it is important to introduce software upgrade procedures with zero downtime in order to minimize the impact to end users.

5. Emergency Handling

Failures may happen any time in the network. Quick recovery and service continuity are very important, so emergency handling capabilities, including skills, processes, information (network topology) and automation, are essential. That is important for physical networks, but in NFV we need to consider recovery in this more complex, multi-layer environment.

6. Operations & Maintenance

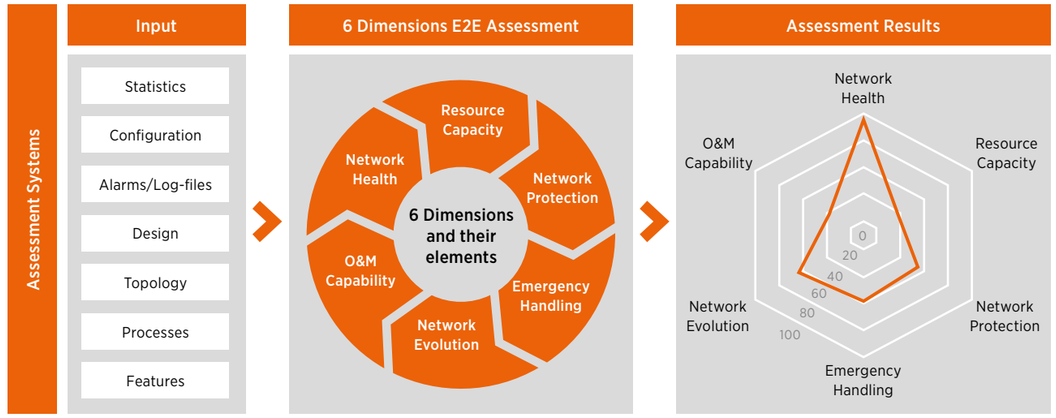
In order to maintain high reliability, operational efficiency is critical. ICT operational transformation is taking place in operator organizations to adopt NFV technology. Service providers need to build teams with skilled staff for new technologies and products, efficient tools for monitoring (e.g. telemetry), fault (e.g. root cause analysis) and performance management, processes for routine maintenance considering the dynamic environment of NFV networks. For example, an added complexity in NFV is driven by the implementation on an as needed basis. Historically once an application was put into the network it stayed in the network. Going forward applications will be applied to the network as needed then all or a part of them will be removed. In this situation, the configurations of the network will be changing on an ongoing basis.

5.4 Best Practices

5.4.1 Use case scenarios

All actors in the industry are invited to use the above framework to build use cases to get carrier-grade reliability results, to maintain openness, and to avoid vendor or technology lock-in. At this juncture, China Mobile and Huawei have announced partnerships to carry out the laboratory testing on top of live systems.

Figure 13: Carrier-Grade NFV Reliability Assessment Methodology



Source: Huawei

5.5 Conclusion

Carrier-grade is demanding, but it is an essential feature of today's telecom networks to maintain strict reliability requirements as both the enterprise customers or consumers have been conditioned to expect extreme reliability in our networks. However, with careful planning and the assistance of telecom-system engineering experts, NFV network and service designers (new versions of service software will be necessary to fully utilise the new opportunities of virtualisation), service providers can build this capability into their NFV deployments and then, with carrier-grade systems to confidently commercialize their NFV services, knowing that they will meet business and technology objectives while satisfying their customers.

Service providers know that they need to continue to meet those expectations as they transition to NFV. Without this assurance for NFV, they run the risk of losing their high-value customers and seeing increased subscriber churn which could offset the many business benefits provided by NFV. No new technology is worth that risk, regardless of the potential saving in CAPEX and OPEX. So, in order to provide an ultra-reliable, highly secure and full connected network, a robust, 360 degree, in-depth analytical NFV network assessment framework is required.

CONSIDERATIONS, BEST PRACTICES AND REQUIREMENTS FOR A VIRTUALISED MOBILE NETWORK

6

Migration

6.1 Introduction

This section describes migrations and software upgrades from both a deployment and software upgrade aspect after the l aunch of a virtualised network launch. Operators should consider interoperability between entities comprised of PNF and VNF. Not all network functions are well-suited to be virtualised and in this section, we examine three categories from an operator perspective.

6.1.1 Migration from physical network to virtualised network

This category considers several migration paths from physical to virtualised, e.g., single functionality level virtualisation, PNF/VNF-mixed operation in the unique functionality (e.g., the operation which includes vMME and existing MME in the same pool), operation without utilizing NFV orchestrator etc.

6.1.2 Software upgrades

Several aspects should be considered in this category, for example, VNF application software upgrade, NFVI (e.g., host OS/hypervisor) upgrade and VIM upgrade (e.g., OpenStack). There are also some other important differences in software upgrade procedures between NFV and traditional networks.

1 – Process

The software architecture is different for each VNF, and so consequently, the software procedure should be adjusted accordingly. It is recommended that the VNF structure and number of VNFCs be considered, before upgrading the VNF. Another difference between NFV and a traditional network is that in the NFV it is possible to access a shared pool of resources (i.e. servers) that can be used when a process needs them. This provides flexibility to operators or vendors who could apply a different strategy based on their needs.

2 – Zero downtime

Each VNF/VNFC may be composed of several instances and this could provide more flexibility to operators in order to perform a zero-downtime software upgrade.

3 – Vertical Interoperability Verification

In NFV, there are multiple components provided usually by different vendors. Each layer's software has to be upgraded or updated periodically. Any change to any layer may impact the interoperability and therefore the service performance. Before implementing a sotfware upgrade in the network, it is important to verify it in an operator's test bed (or any other external LAB), mirroring the exact environment with the same components end-to-end. Once it is verified, the software release could then be safely rolled-out in the live environment.

4 – Software upgrade/update frequency

Vertical layout may be composed by different vendors and each vendor may provide software releases (patches or versions) in different time periods. Some vendors may release software packages once a month, some quarterly or semi-annually etc. Each time, a multi-vendor verification process may be needed, which is time consuming and requires additional resources. Operators should plan accordingly and consider how to optimize the process per case.

6.1.3 Interoperability

This category considers the interoperability between the physical entity and the virtualised entity or network connection using virtualised networking i.e., SDN in the NFV configuration.

6.2 Best practices

6.2.1 Migration

Two possible approaches to introduce virtualised products in an operator network following the launch of commercial LTE services are discussed below.

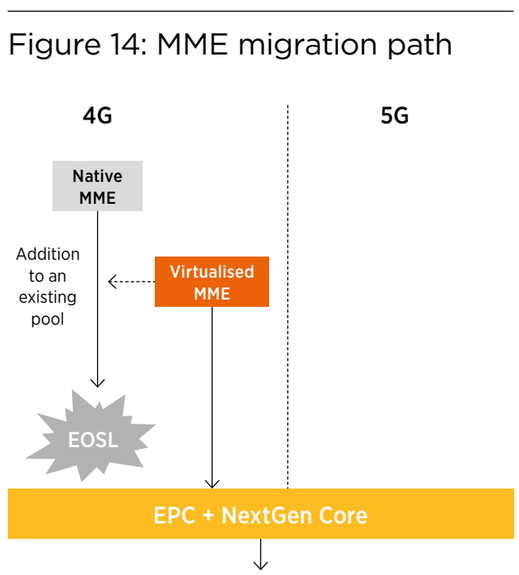
1. Introduction of a new system for newly developed services (e.g., IoT services, facilities for MVNOs and services for the enterprise customers);
2. Expansion to existing facilities

As the introduction of new systems for newly developed services is not necessarily a migration, the rest of this section will focus on area of expansion.

As an example the case of MME deployment is discussed here. In this example, the operator who has launched commercial LTE services is going to migrate its native MME to a virtualised one. In general, the operator has to keep the existing native MMEs operating so that it can continue to serve existing users, therefore the operator would initially introduce the virtualised MMEs as additional facilities. In this example, newly added vMMEs are added to an existing MME pool.

After a certain period of time, the EOSL (End of Service Life) of the existing native MMEs is reached, the operator may want to introduce the Next Generation core network (NGCN) to access one of its unique functions e.g. network slicing. In this example, the deployment approach is described as a combo-node deployment of both EPC and NextGen core.

Figure 14: MME migration path



Source: KDDI

6.2.2 Software upgrades

The types of NFV software to be upgraded are identified in [11]. These are as follows;

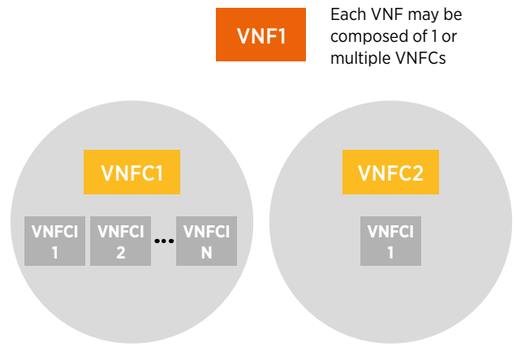
- VNF domain software
- MANO domain software
- NFVI software

From those components, the most critical one is the VNF, since it provides the services. The process should ensure a zero-downtime software upgrade in order to provide high availability (including planned and unplanned downtime) and improve a user's experience. The NFVI software upgrade process is not as complex as VNFs, but the process should protect service continuity. Finally, the MANO software upgrade process can not impact the service, but only operations (e.g. commands, auto-scaling may not work etc.).

There are several different processes to be followed for software upgrades based on industry best practice. For each component, the same or different strategy may be executed and this depends on:

- Software architecture
- Availability of Additional resources
- Traffic migration capabilities
- Network Design

Figure 15: VNF Architecture



Source: Huawei

1. Using VNF in Pool, so it is easier to migrate traffic from one VNF to another one. Then upgrade the "empty" (not loaded) VNF without risk.

2. Rolling SW Upgrade (instance by instance), it is applicable when there are multiple instances. It is used for Active-Active or Active Stand-By mode, to isolate an instance, upgrade it and then put it back to the traffic.

3. Scale-out/Scale-In process, when deployment of VNFC instances with the new SW (in the same VNF), migrate traffic to them and kill old instances (scale-in). Additional resources are needed.

4. New VNF deployment, initially instantiate a new VNF, migrate traffic to that one and then terminate the "old" VNF. Traffic migration may require configuration from external nodes.

5. NFVI SW Upgrade (i.e. host OS, KVM, Open V switch or DPDK) uses live VM migration to minimize the impact. VMs are migrated from NFVI (old SW) to the upgraded NFVI area and continue upgrading all the resources.

6. MANO SW Upgrade process is not as critical as other components, since there is usually no service impact. Any method highlighted above could be used based on the SW architecture.

6.3 Requirements

6.3.1 Migration

The following aspects should be considered for the migration from physical to virtualised:

- It should be possible to share PNF and VNF resources for the same network function

  NOTE: The "resources" are not the resources which are provided by the NFVI, such as compute, storage or network resources
- In a mixed environment consisting of both physical and virtualised network functions, it should be possible to maintain the same interfaces between network functions

6.3.2 Software upgrades

The following elements should be considered for software upgrades;

- The traffic should be switched seamlessly for all the methods of SW upgrade described above
- Migration of active VNFs (live migration) from the compute node in operation to the maintenance zone should be executed without interruption when VIM software or NFVI software will be upgraded. If the interruption occurs, it should be minimized
- Required hardware acceleration functionality should be available for the destination of the migration
- Due to complexity, automated software upgrade / update process is preferred
- Quick roll-back process in case of failure
- Ensure zero downtime for the services during VNF upgrade

7

Performance benchmark for NFV infrastructure

7.1 Performance benchmark scope

When NFV was brought to the industry, it was claimed to help operators shorten their service time to market and offer agility in system expansion, while simplifying network operation through the use of common servers. However, since NFV is built on common x86 servers, service level performance is often questioned. Given the circumstances, vendors and operators should team up to provide some performance metrics and carry out tests.

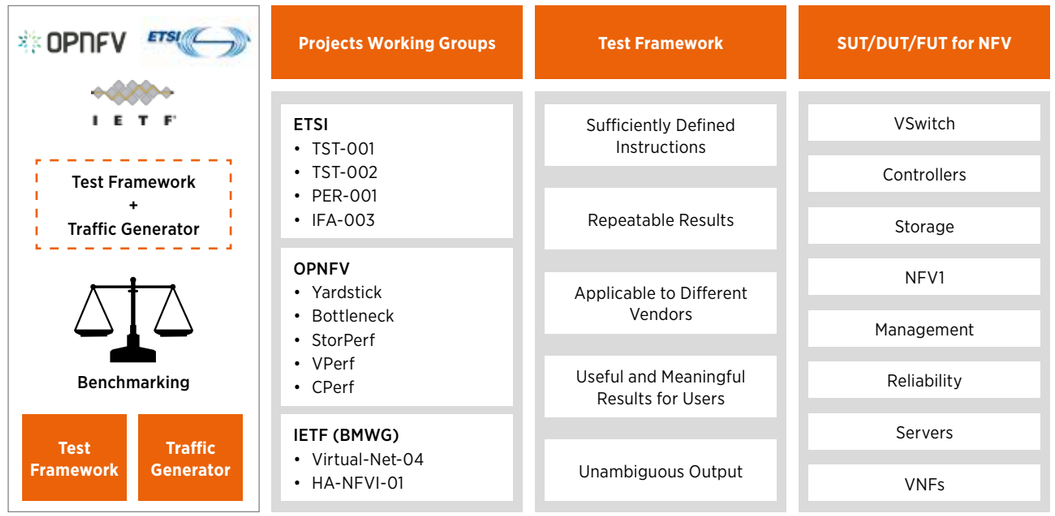
Each single portion of the NFV system can be benchmarked, for example, VNF performance, NFVI performance, storage performance, virtual switch performance etc. Each level of these performance benchmarks will help operators to decide which product will fit into their NFV systems. From the end-to-end service perspective, it is possible to benchmark service deployment. For example, how quickly a NFVI could be set up, how long it would take to upload a VNF package and how long to instantiate a VNF or a Network Service etc. Based on these benchmarks, operators can tell if it is feasible to deliver a low cost, high performance solution based on NFV.

In addition to the vendors and operators' own tests, many standard organizations and open source communities are very supportive of NFV performance benchmarking experiments. Usually this work will involve test framework and traffic generators, as benchmarking could not be performed in live networks. Other common characteristics of performance benchmarking work are as follows:

- Include testing instructions that are sufficiently specified (prerequisites, procedures, output)
- Results are repeatable
- Test cases can be performed on different vendor's device/system
- The produced results are useful and meaningful for the users

In this chapter, state of the art NFV performance benchmarking is outlined. Performance metrics, test methodologies and use cases that have been defined will be helpful for vendors and operators who want to carry out the tests in their own labs.

Figure 16: NFV performance benchmark scope



Source: Huawei

7.2 State of the art in NFV performance benchmarking

In OPNFV, there are several test projects which have been initialized to benchmark the performance of a NFV system and its components. Yardstick and Bottlenecks are the names given to projects used to benchmark system level performance, while StorPerf, VSPerf and CPerf define methodology in benchmarking storage, virtual switch and SDN controller performance respectively.

Yardstick [12] is a project that aims to verify the infrastructure compliance from the perspective of a VNF. Based on the uses cases that have been defined in ETSI GS NFV 001 [17], each use case implies specific requirements and complex configuration on the underlying infrastructure and test tools. In order to find a system level benchmark, in Yardstick, every single VNF work-load performance metric is broken down into a number of characteristics/performance vectors and each performance vector is then represented by a test case.

In the OPNFV Colorado release, test cases covering Performance/Speed and Capacity/Scale are available, Reliability/Availability part will be finished in the coming releases.

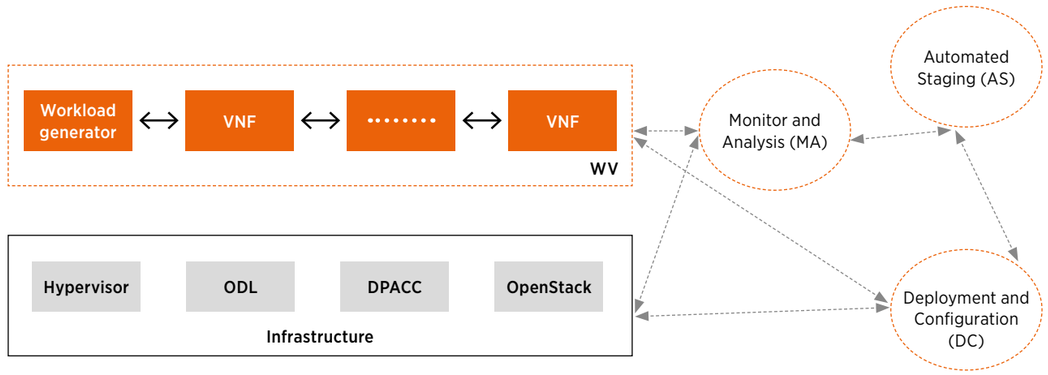
The scope of Yardstick is the development of a test framework as well as test cases and test stimuli to enable NFVI verification. This methodology is aligned with ETSI TST 001 [18].

The Bottlenecks [13] project aims to find system bottlenecks by testing and verifying the OPNFV infrastructure in a staging environment before committing it to a production environment. It defines an automatic method for executing benchmarks to validate the deployment during the staging phase. The framework has four components: Workload generator and VNFs (WV), Monitor and Analysis (MA), Deployment and Configuration (DC), Automated Staging (AS). The architecture is shown as follows:

Figure 17: YardStick performance metrics and test suite

	Performance/Speed	Capacity/Scale	Reliability/Availability
Compute	• Latency for random memory access • Latency for cache read/write operations • Processing speed (instructions per second) • Throughput for random memory access (bytes per second)	• Number of cores and threads • Available memory size • Cache size • Processor utilisation (max, average, standard deviation) • Memory utilisation (max, average, standard deviation) • Cache utilisation (max, average, standard deviation)	• Processor availability (error free processing time) • Memory availability (error free memory time) • Processor mean-time-to-failure • Memory mean-time-to-failure • Number of processing faults per second
Network	• Throughput per NFVI mode (frames/byte per second) • Throughput provided to a VM (frames/byte per second) • Latency per traffic flow • Latency between VMs • Latency between NFVI nodes • Packet delay variation (jitter) between VMs • Packet delay variation (jitter) between NFVI nodes	• Number of connections • Number of frames sent/received • Maximum throughput between VMs (frames/byte per second) • Maximum throughput between NFVI nodes (frames/byte per second) • Network utilisation (max, average, standard deviation) • Number of traffic flows	• NIC availability (error free connection time) • Link availability (error free transmission time) • NIC mean-time-to-failure • Network timeout duration due to link failure • Frame loss rate
Storage	• Sequential read/write IOPS • Random read/write IOPS • Latency for storage read/write operations • Throughput for storage read/write operations	• Storage / Disk Size • Capacity allocation (block-based, object-based) • Block size • Maximum sequential read/write IOPS • Maximum random read/write IOPS • Disk utilisation (max, average, standard deviation)	• Disk availability (error free disk access time) • Disk mean-time-to-failure • Number of failed storage read/write operations per second

Figure 18: Bottlenecks test framework



Source: OPNFV Bottlenecks project

The workload generator generates workloads which go through VNFs, and then analysis units will monitor the infrastructure and VNF status. Test results will then be analysed to find out the system bottleneck. Therefore, a wide range of different hardware resources and software configurations will be used to locate a system's bottleneck.

The Storage Performance Benchmarking for NFVI (StorPerf) [14] is a project that aims to provide a tool to measure block and object storage performance in an NFVI. The project will define a test suite, including test cases, metrics and test process to find the benchmarks, which can provide a good preview of expected storage performance behaviour for any type of VNF workload.

The vSwitch Performance (VSPerf) [15] project will develop a generic and architecture agnostic vSwitch testing framework and associated tests, which will serve as the basis for validating the suitability of different vSwitch implementations in a Telco NFV deployment environment.

The Controller Performance Testing (CPerf) [16] project will serve as a performance testing environment for the SDN controller portion of the large, realistic, automated deployments required by OPNFV. The initial focus of CPerf is OpenDaylight, but later-on the project tends to leave the controller part of the test matrix open and will welcome collaboration with other controller communities.

The Network Service Benchmarking (NSB) is an open source framework that allows benchmarking and characterization of VNFs by testing with real-life traffic scenarios on Bare Metal, Standalone Virtualised, and Managed Virtualised environments. The NSB test harness is inherited from the OPNFV Yardstick open source solution (also upstream the patches back to Yardstick community developed in test harness), and incorporates a benchmarking methodology that facilitates deterministic and repeatable benchmarking on Industry Standard High Volume (SHV) servers. It provides several VNFs: vCG-NAPT, vACL, vFW, vPE, vEPC as the samples for demonstration, and it also can integrate 3rd-party VNF as the benchmarking tool for operators, which can help in characterizing VNFs by measuring Network, VNF and NFVI KPIs:

- Network KPIs: e.g. Traffic Generator KPIs like packets in, packets out, throughput, latency as per RFC 2544 etc.
- VNF KPIs: e.g. packets in, packets out, packets dropped, etc.
- NFVI KPIs: e.g. CPU utilisation, IPC, L1/L2/LLC cache hit/misses, iTLB/dTLB hit/misses, OVS stats, memory bandwidth & latency, etc.

In ETSI, ETSI GS NFV-TST 001 [18], TST 002 [19], PER 001 [20] and IFA 003 [21] have been produced by ETSI Industry Specification Group (ISG) to benchmark the NFV-related performance and test methods.

TST 001 provides an informative report on methods for pre-deployment testing of the functional components of an NFV environment, including VNFs, NFVI and MANO. The recommendations focus on lab testing and the following aspects of pre-deployment testing:

- Assessing the performance of the NFVI and its ability to fulfil the performance and reliability requirements of the VNFs executing on the NFVI
- Data and control plane testing of VNFs and their interactions with the NFV Infrastructure and the NFV MANO
- Validating the performance, reliability and scaling capabilities of Network Services

TST 002 provides interoperability test methodology that is applied to NFV by analysing some of the core NFV capabilities and the interactions between the functional blocks defined within the NFV architectural framework required to enable them. It describes two types of testing: Conformance Testing and Interoperability Testing.

PER 001 provides a list of minimal features which the VM Descriptor and Compute Host Descriptor should contain for the appropriate deployment of VM Images over an NFVI, in order to guarantee high and predictable performance of data plane workloads while assuring their portability. In addition, the document provides a set of recommendations on the minimum requirements which hardware and hypervisor should have for a NFVI suitable for different workloads (data-plane, control-plane, etc.) present in VNFs. According to the workload analysis in clause 6, clause 7, it provides a recommendation on the minimum requirements that a Compute Host should have for a NFVI suitable for data-plane workloads, and, clause 8 gathers the list of features which the Compute Node Descriptor and the VM Descriptor templates should contain for the appropriate deployment of VM Images over an NFVI, in order to guarantee high and predictable performance while preserving portability across different servers.

IFA 003 specifies performance benchmarking metrics for virtual switching, with the goal that the metrics will adequately quantify performance gains achieved through virtual switch acceleration conforming to the associated requirements specified herein. It defines the critical aspects of vSwitch performance by treating the vSwitch as a Device Under Test (DUT), with specific configurations that are consistent across instantiations of a vSwitch on a computing platform. It also uses the existing testing and benchmarks specifications (see [22], [23], [24] and [26]) to measure the performance of the DUT under specific configurations and conditions, such as vSwitch physical to physical, vSwitch virtual to virtual, etc.

In IETF, the draft-ietf-bmwg-virtual-net-04 [22] document researched by Benchmarking Methodology Working Group (BMWG) has defined the considerations for benchmarking virtual network functions and their infrastructure. This document investigates additional methodological considerations necessary when benchmarking VNFs instantiated and hosted in general-purpose hardware, using bare-metal hypervisors or other isolation environments such as Linux containers. It lists several new benchmarks and related metrics, such as time to deploy VNFs, time to migrate VNFs, time to create a virtual network in the general-purpose infrastructure, etc. it also defines several new considerations which must be addressed to benchmark VNF and their supporting infrastructure, like hardware configuration parameters (shelf occupation, CPUs, caches, memory), etc.

Another document, "Considerations for Benchmarking High Availability of NFV Infrastructure" [27] lists additional considerations and strategies for benchmarking high availability of NFV infrastructure when network functions are virtualised and performed in NFV infrastructure. With VNFs and NFVI replacing the legacy network devices, operators have several issues to cope with such as availability, resiliency and non-measurable failures. Above all, they want to ensure the availability of the VNF products and their infrastructures. From the operator point of view, the availability is the most important feature and the benchmarking tests for the high availability of NFV infrastructure are also important. This document investigates considerations for high availability of NFV Infrastructure benchmarking tests.

CONSIDERATIONS, BEST PRACTICES AND REQUIREMENTS FOR A VIRTUALISED MOBILE NETWORK

8

Vertical interoperability

8.1 Introduction

Physical mobile networks are made up by equipment provided by multiple vendors in general. This is made possible by the clear definition of open interfaces between the network nodes specified by 3GPP. Such a multi-vendor environment fosters innovation and competition, resulting in advantages both for operators and subscribers.

It will be beneficial for virtual networks to be made by equipment provided by multiple sources.

8.2 Requirements for vertical interoperability

Figure 18 highlights an example of a virtual network where individual components are procured from a number of different vendors.

For networks to operate correctly it is important that the interfaces between the individual blocks of the architecture are tightly specified and implemented.

Failing to define interoperable interfaces is expected to result in a higher total cost of ownership as well as a slower time to market. Operators will need to ensure that the open source community developing the architecture understand the importance of vertical interoperability.

8.3 Challenges and potential risks

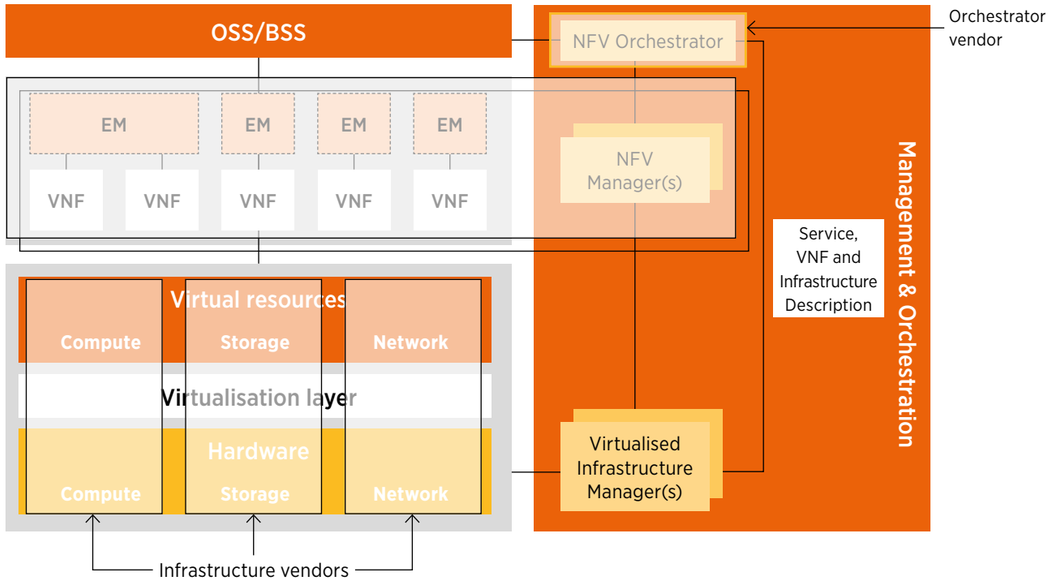
When vendors use non-standardised non-standardised interfaces there could be potential risks in the network. Some of the potential impacted areas are described below:

1. Vertical Integration
With characteristics such as hardware-software decoupling and hardware generalization, NFV further opens up carriers' network architecture. NFV is one huge complex ICT systems integration project, involving multiple technologies, interfaces and multiple vendors.

It is important that vertical cloud platform integration is performed smoothly and quickly. Interoperability plays a key role in vertical integration, especially in a multi-vendor ecosystem.

2. Network Service Deployment
Interoperability can cause problems in Network Service deployment, since multiple components provided by different vendors are involved during this process. This includes from OSS/BSS and Portals up to NFVO, VNFM, VIM, Cloud OS and COTS. Descriptors, such as NSD, VNFD should also follow the standardised format for a successful service instantiation.

Figure 19: example of multivendor virtual network



3. Service Assurance
Service performance and high availability are also dependent on interoperability. When there is a failure in the network, the information should be propagated quickly to the upper layers, based on the standard interfaces so that each component can use this information effectively. For example, a hardware failure should trigger an alarm to users allowing them to act immediately.

Automation also plays an important role in NFV lifecycle management and different components have in-built self-healing mechanisms (i.e. VM migration in case of host failure). These mechanisms are triggered under specific conditions, such as notifications that have been received from the network. If this kind of information is not received then the system will not recover automatically, and cause network outage.

4. Software Upgrade
Any change in the software of a component, in any layer, could cause problems to the other layers. Consequently, this could impact existing services and their users. Vertical verification is recommended in order to test interoperability. Horizontal verification challenges remain the same as in traditional network, so there is no real difference.

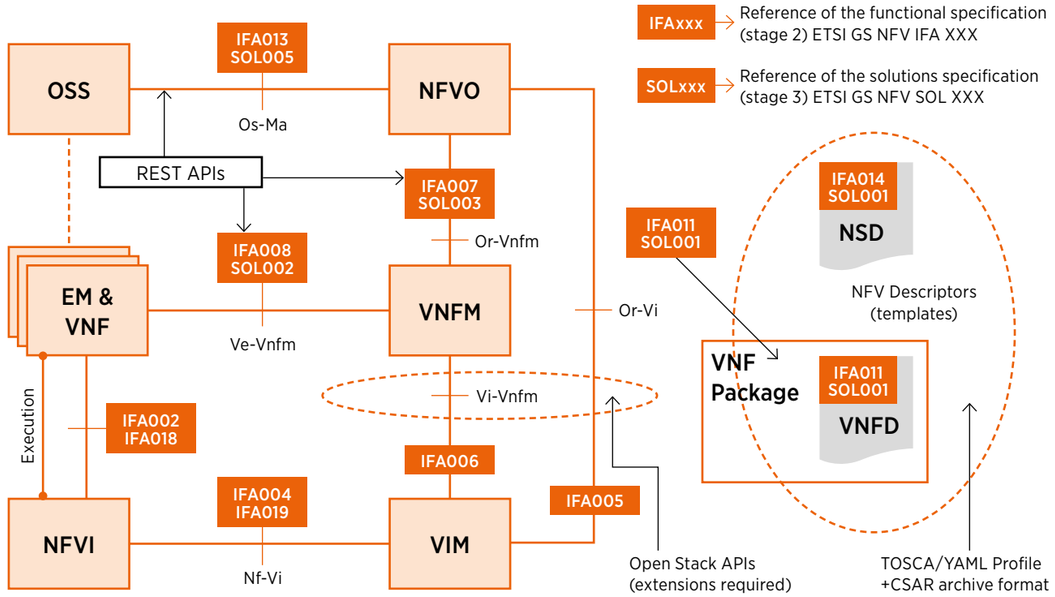
8.4 Best Practices

Incompatible systems elements or software versions can cause further network faults, and require compatibility management. The key elements are to use standardised interfaces and proper compatibility validation processes.

1. Standardised Interfaces
NFV solutions should be based on interoperable multi-vendor ecosystems with open source technologies or standardised protocols and interfaces. ETSI's IFA Workgroup focus on interface standardisation and several open source projects have developed platforms based on this, such as OPNFV, OPEN-O, OSM etc. There have also been several documents released by ETSI. Figure 20 shows some of the important work done by the ETSI IFA and SOL Working Groups.

2. ETSI Plugtests
ETSI identified the need for thorough industry interoperability testing and took on the initiative to start organizing NFV Plugtests. They will offer test sessions where vendors and Open Source projects will be able to assess the level of interoperability of their implementations and verify the correct interpretation of the ETSI NFV specifications.

Figure 20: MANO to IFA Mapping – reference points



Source: ETSI NFV

The component for the test sessions are Virtual Network Functions (VNFs), Management and Orchestration (MANO) solutions and NFV Infrastructure (NFVI) with pre-integrated Virtual Infrastructure Manager (VIM).

3. Integration and Verification

Most of the interoperability issues appear during the integration phase. Multiple vendors are involved in this phase, so cooperation and coordination are important. Either operators or one of the assigned services suppliers should lead this complex project and act as a prime system integrator, having extensive IT and CT experience, in order to deliver an integrated E2E solution.

A proper verification plan is required for interface compatibility and service validation. For this purpose, an operator's test bed could be used, using the same multi-vendor ecosystem. Alternatively, a vendor's NFV Lab could be used for solution validation or pre-packaged, pre-integrated and pre-tested solutions. The same process applies for a software upgrade process.

Find out more at
www.gsma.com/network2020

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601