QoE in Virtualized Networks (NFV)

Angelo Baccarani
Product Manager – NFV Service Assurance

May 20, 2019

EMPIRIX

About the Author

- Angelo Baccarani is currently Product Manager at Empirix (www.empirix.com) for NFV Service Assurance solutions
- He works in the Telecom sector since 1991, covering various roles in Software Development, Product Management and Strategic Marketing mainly focused on probes-based passive monitoring systems for Communications Service Providers (CSP)
- He holds a Bachelor's Degree in Computer Science at the University of Modena and Reggio Emilia (Italy) since 2014, following his first level degree obtained in 1988 at the same college
- He can be reached on LinkedIn and at abaccarani@yahoo.com

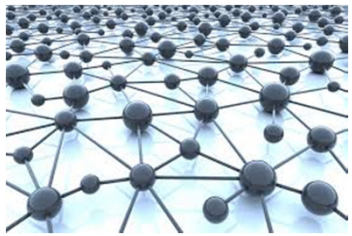
Presentation Summary

- QoE Definition
- Introduction to NFV
- Passive Probing of NFV

QoE in Virtualized Networks
Definition

Telecom Operators Challenge

Many Network Technologies



What is the Quality of Experience of my users ?

Many Devices

Many Subscribers Profiles

Many Applications

Problem: Thousands of KPI but…no QoE !

Mobile Network

- Packet Switch - Core
- Packet Switch - Access
- Circuit Switch - Core
- Circuit Switch - Access

Voice/Text Services



…the reality today….

…too many uncorrelated indicators !

Data Services

Fixed Network

- NGN Core
- IMS Core
- SS#7 Core

QoE is not QoS !

➢ QoS: very well known concept

- ✓ *The ability of a network to provide a service with an assured service level*

- Defined by means of set of technical metrics (a.k.a. Key Performance Indicators, KPI) such as Packet Loss, Delay, Throughput

➢ Quality of Experience: various definitions…

- ✓ *The overall acceptability of an application or a service, as perceived subjectively by the end-user (by ITU)*
- ✓ *How a user perceives the usability of a service when in use, how satisfied is with the service*
- ✓ *The degree of delight of the user of a service, influenced by content, network, device, application, user expectations and goals, and context of use*

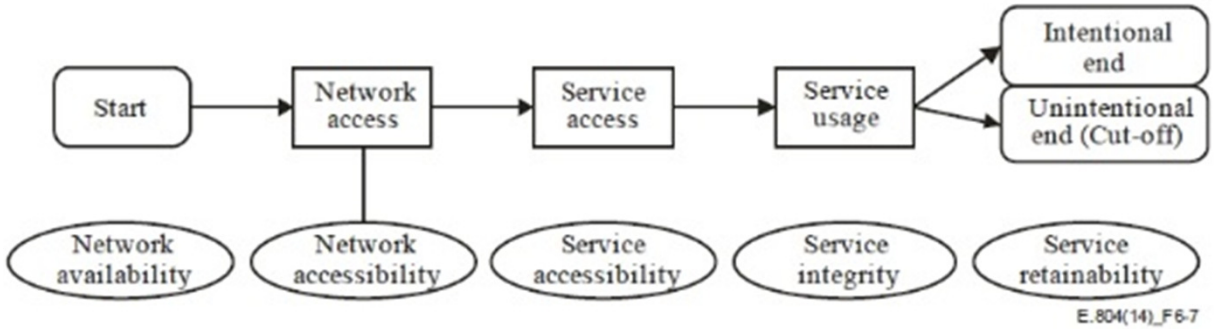
- Defined by indicators like "*excellent*", "*good*", "*bad*" (referring to services) as well as "*satisfied*", "*tolerating*", "*frustrated*" (referring to the users)

QoS evaluates the network while QoE evaluates the perception of a service from user standpoint

Decomposing the Service Delivery

- To proper evaluate the overall QoE, it is necessary to break the usage of a service in all its phases and evaluate them individually

- Each phase can be scored through QoS metrics whose correlation allows to obtain a single QoE:



QoS aspects related to different phases of service usage

- While some of the phases have a greater importance for mobile networks, the general concept can be applied to any kind of network delivering services to the user

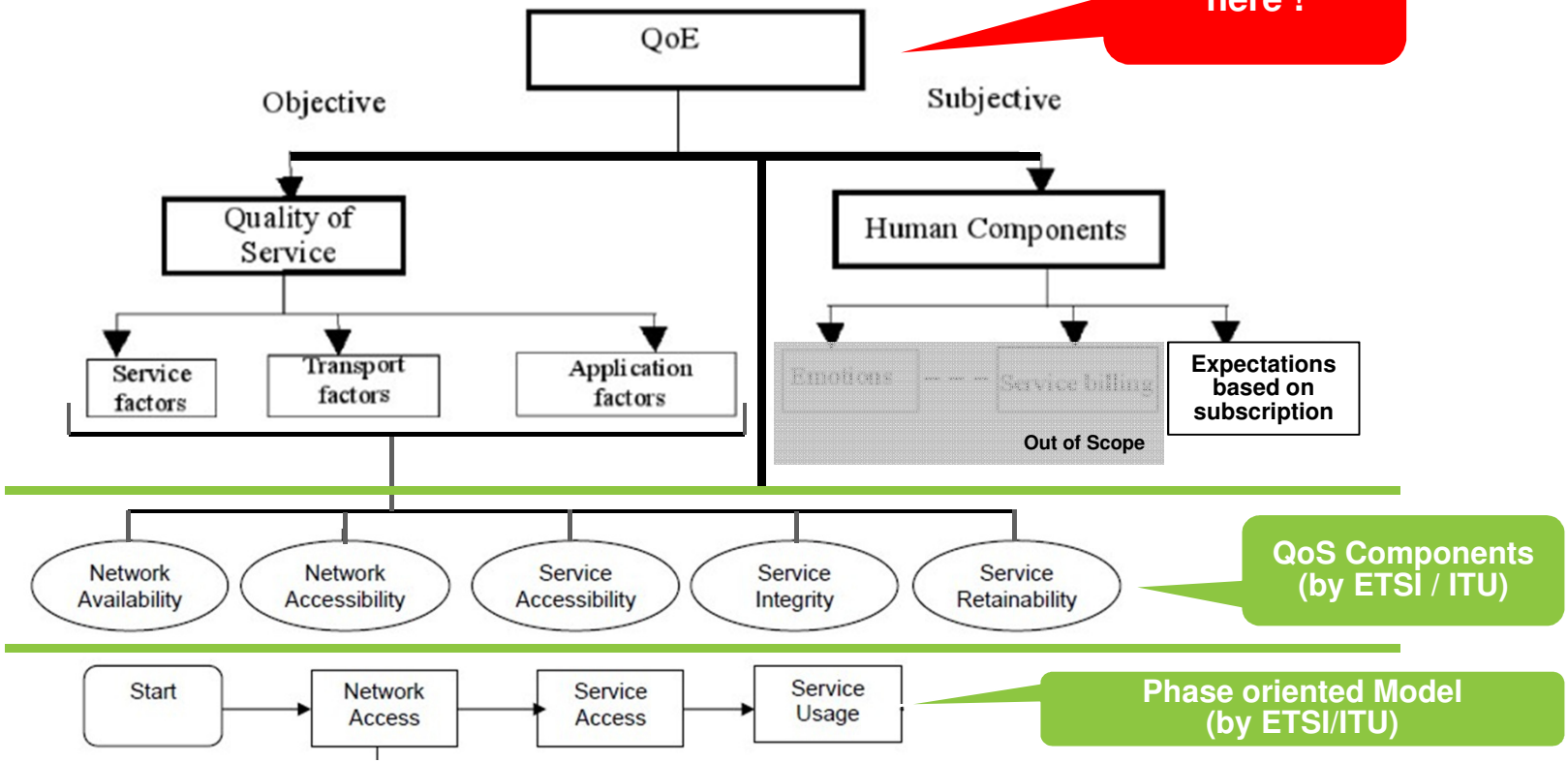
QoS Aspects To Analyze

- **Network Availability -** Probability that the services are offered to a user via a network infrastructure
- **Network Accessibility -** Probability that the user performs a successful registration on the network which delivers the service
- **Service Accessibility -** Probability that the user can access the desired service/content
- **Service Integrity (a.k.a. Performance) -** Describes the QoS during service use and contains metrics related to the performance
- **Service Retainability -** Describes the termination of services against the will of the user

...but they are not enough: QoE is impacted also by ***user expectations:***

«If I pay more I expect more»

Reference Models
ETSI TS 102 250-1 / ITU E.804



Problem !

How collecting all the required metrics to evaluate the QoS and correlate it to the QoE ?

Network nodes provide a lot of performance data but, unfortunately, not split by single subscriber

…solution is the ***Passive Probing***

Passive Probing: Definition

- Passive probing (a.k.a. *Non Intrusive Monitoring*) **is the main source of QoS information *per single subscriber* and *per service* (voice, video, data…)**
- It is the process of acquiring control or user traffic from a telecommunication network without disturbing the network being monitored
- This is particularly important for network management/OSS applications where disturbing the observed network with active devices can itself affect network operation and destroy the value of the probed data
- It is usually implemented through dedicated devices *("hardware appliances")* placed on the communication links between the physical nodes but…

…what about if the network nodes become virtual ?

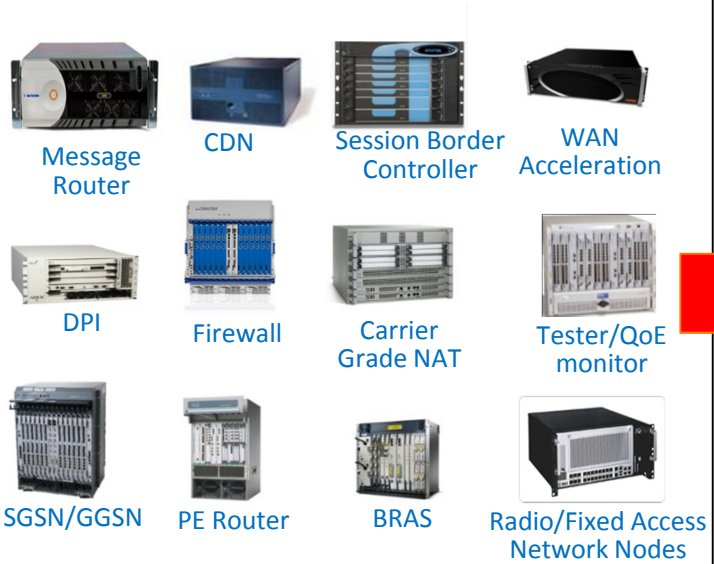
…and what does "virtual network" mean ?

QoE in Virtualized Networks

Introduction to NFV

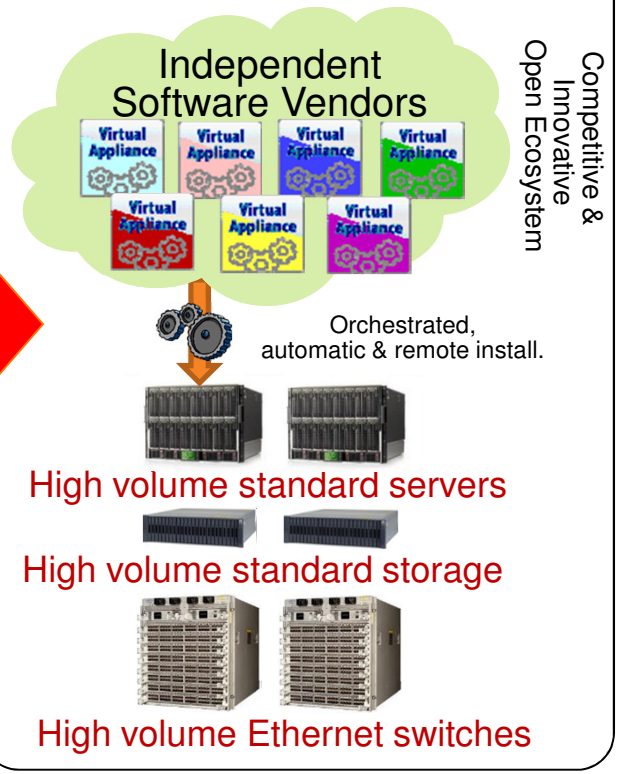
NFV: Definition by ETSI

Classical Network Appliance Approach



- Fragmented, purpose-built hardware
- Physical install per appliance per site
- Hardware development large barrier to entry for new vendors, constraining innovation & competition

Network Functions Virtualisation Approach



EMPIRIX

Warning about Terminology…

Virtualization and **NFV** are different concepts…and then there is also **SDN**…

Things Are Complex…

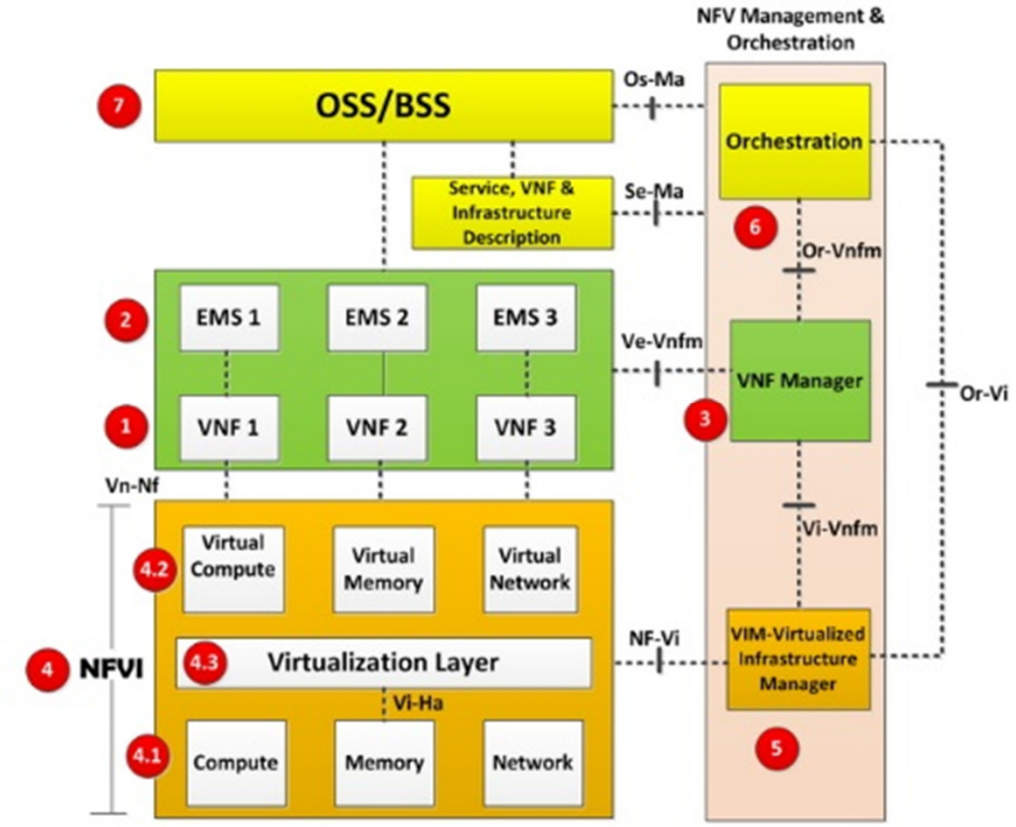
- **Virtualization:** run in software (i.e. into a Virtual Machine) a function that is traditionally executed on dedicated hardware. Each function is implemented into a single *Virtual Network Function* (VNF), running separately (e.g. DNS Server)
- **Network Function Virtualization:** combine the functions of multiple VNFs to provide network services (e.g. vEPC, vIMS…) under the control of a single Orchestrator
- **SDN** introduces the possibility to change the rules used by the switches to route traffic, through a software component (*SDN Controller*) and a protocol (*OpenFlow*)

In a nutshell:

"NFV requires Virtualization, but you can implement Virtualization without NFV"

"NFV is highly complementary to SDN but not dependent on it (or vice-versa). NFV can be implemented without SDN, although the two concepts and solutions can be combined to potentially get greater value"

NFV: ETSI Architecture



1 - VNF

Virtual Network Function

- A VNF is the basic block in NFV Architecture
- It is the virtualized network element
- For example when a router is virtualized, we call it “Router VNF”
- Even when one sub-function of a network element is virtualized, it is called VNF. For example in router case, various sub-functions of the router can be separate VNFs which together function as virtual router
- Other examples of VNF include firewalls, IPS, GGSN, SGSN, RNC, EPC etc.

2 - EMS

Element Management System

- This is the Element Management system for VNF
- This is responsible for the management of VNF operation, in the same way as physical network elements are managed by their respective EMS
- EMS provides FCAPS (Fault, Configuration, Accounting, Performance and Security) functions
- It may manage the VNFs through proprietary interfaces
- There may be one EMS per VNF or an EMS can manage multiple VNFs
- EMS itself can be a VNF

3 - VNF Manager

- A VNF Manager manages a VNF or multiple VNFs i.e. it does the life cycle management of VNF instances
- Life cycle management means setting up/ maintaining and tearing down VNFs
- A VNF manager can do the same functions as EMS but through open interface/reference point proposed in NFV architecture named Ve-Vnfm

4 - NFVI

Network Function Virtualization Infrastructure

- NFVI is the environment in which VNFs run

- This includes Physical resources, virtual resources and virtualization layer, described below

4.1 - Compute, Memory, Networking

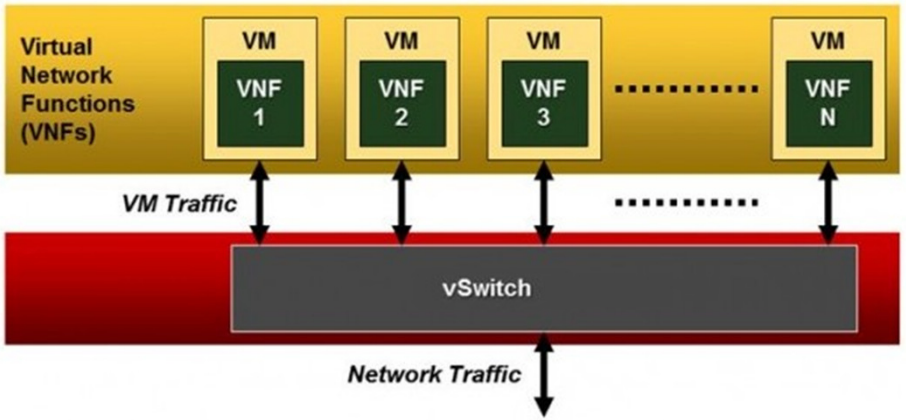
- This is the **physical part** in NFVI, defining the hardware resources available to run the VNF
- Virtual resources are instantiated on these physical resources
- Any commodity hardware (switches, physical server/storage servers…) is part of this category

4.2 - Virtual Compute, Memory and Networking

- This is the **virtual part** in NFVI
- The physical resources are abstracted into virtual resources that are ultimately utilized by VNFs
- Key component here is the Virtual Switch
- Examples of Virtual Switches are Open vSwitch (OVS), Wind River Accelerated Virtual Switch (AVS), Cisco Nexus 1000v, 6Wind OVS

Virtual Switch: Definition

- In the NFV scenario the virtual switch (vSwitch) is responsible for switching network traffic between outside the Cloud and the virtualized applications (VNFs) that are running in VMs (*North-South interfaces*)
- The vSwitch is also used to route the traffic between VMs (*East-West interfaces)*
- The vSwitch runs on the same server platform as the VNFs and its switching performance directly affects the number of subscribers that can be supported on a single server blade



Why it is Critical for NFV Monitoring

- vSwitch is critical to us as vendor of Virtual Probe because it will basically replace the physical Network Interface Card that today is provided on the hardware-based probe appliances

- Its performances will be therefore critical in order to receive the protocol packets without any delay that could affect our QoS / QoE analysis

- Note that deployment of a virtual probe will always require the configuration of the vSwitch in order to receive the right data (similar to what today must be done to enable Span Ports)

4.3 - Virtualization Layer

- This layer is responsible for abstracting physical resources into virtual resources
- The common industry term for this layer is "**Hypervisor**"
- This layer decouples software from hardware which enables the software to progress independently from hardware.
- Suppose, there is no virtualization layer, one may think that VNFs can run on physical resources directly
- However, as such by definition we CANNOT call them VNF nor it would be NFV architecture
- They may appropriately be called PNFs (Physical Network Functions)
- Examples of hypervisors are KVM and VMware ESXi

5 - VIM
Virtualized Infrastructure Manager

- This is the management system for NFVI
- It is responsible for controlling and managing the NFVI compute, network and storage resources within one operator's infrastructure domain
- It is also responsible for collection of performance measurements and events
- Example of VIM is Openstack

6 - NFV Orchestrator (NFVO)

- Generates, maintains and tears down network services of VNF themselves
- If there are multiple VNFs, orchestrator will enable creation of end to end service over multiple VNFs
- NFV Orchestrator is also responsible for global resource management of NFVI resources. For example managing the NFVI resources i.e. compute, storage and networking resources among multiple VIMs (if present) in network
- The Orchestrator performs its functions by NOT talking directly to VNFs but through VNFM and VIM
- Let's say there are multiple VNFs which need to be chained to create an end to end service
- One example of such case is a virtual Base station and a virtual EPC: they can be from same or different vendors
- There will be a need to create an end to end service using both VNFs
- This would demand a service orchestrator to talk to both VNFs and create an end to end service

7 - OSS/BSS

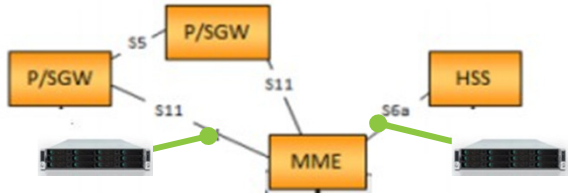
- Such concepts are not strictly related to NFV, being in Telecom Industry since many years
- OSS deals with network management, fault management, configuration management and service management.
- BSS deals with customer management, product management, order management, service fulfillment etc.
- Current OSS/BSS must be upgraded to manage both physical and virtualized network functions
- In the NFV architecture, the current BSS/OSS of an operator may be integrated with the NFV Management and Orchestration using standard interfaces

QoE in Virtualized Networks

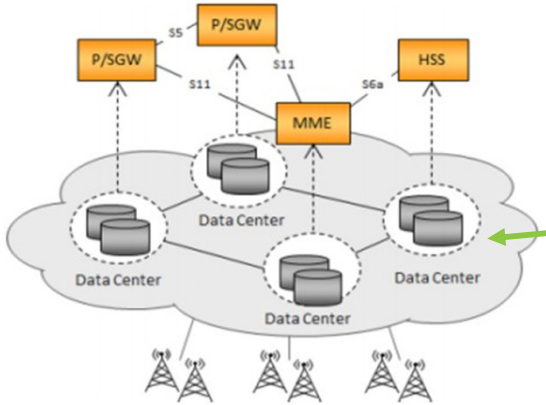
Passive Probing of NFV

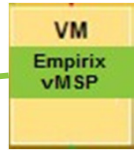
Example: from EPC to vEPC
...and the problem of how to monitor it...

- From the EPC as of today (with physical interfaces to monitor)…



- …to the vEPC (and physical interfaces *disappeared* into the Data Center's Cloud)





Virtual Probe must be deployed as VM running into the Cloud

Requirements for NFV Assurance

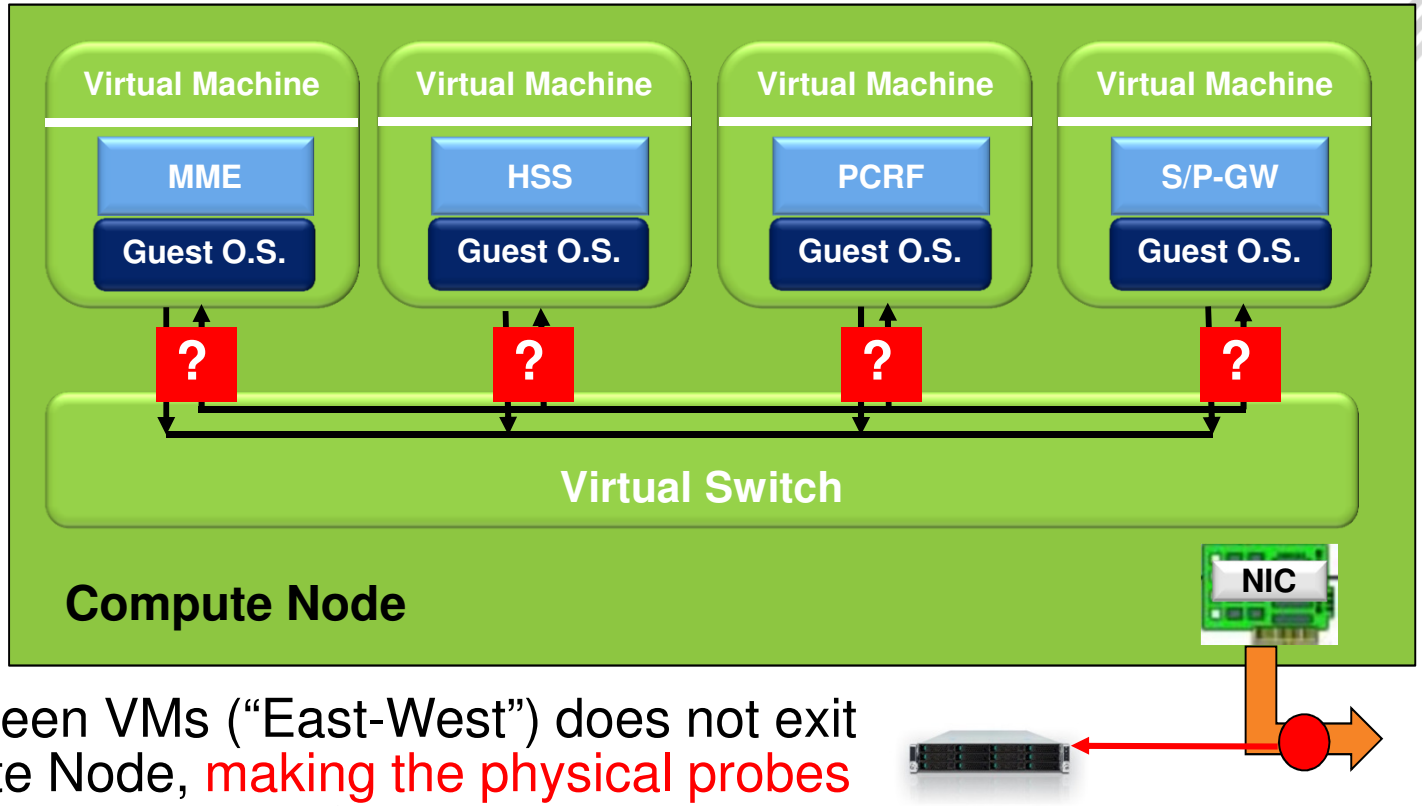
- ETSI has identified the "QoE Monitoring" as one of the functions that should be moved from hardware appliances to Virtual Network Functions

- This requires several core capabilities.

  - **Visibility of the traffic in the "cloud"** once the network interfaces (e.g. S11, Gn, S6a…) are all moved into a "Cloud" (i.e. *virtualized*), **including QoE scoring**
  - **Dynamically monitor virtualized environment**: network functions to monitor can be moved across the underlying hardware infrastructure by the Orchestrator, requiring the re-configuration of the Virtual Probes (possibly, automatically)
  - **Root Cause identification**: once a problem is detected, it is necessary to define if it is due to specific VNF, or to the interworking between VNF or how the VNF has been instantiated (e.g.: overload of CPU of the physical server hosting one or more VNF)
  - **Verify Orchestration Policies:** provide visibility of the effect of creating, removing or changing the operator's policies, relying on scoring the subscribers' QoE as main measurement parameter

Given these requirements, it will be critical for CSPs to have the same (or better…) level of monitoring capability within a NFV environment, compared to what available today on the physical network architectures

Challenge 1: Traffic Visibility !



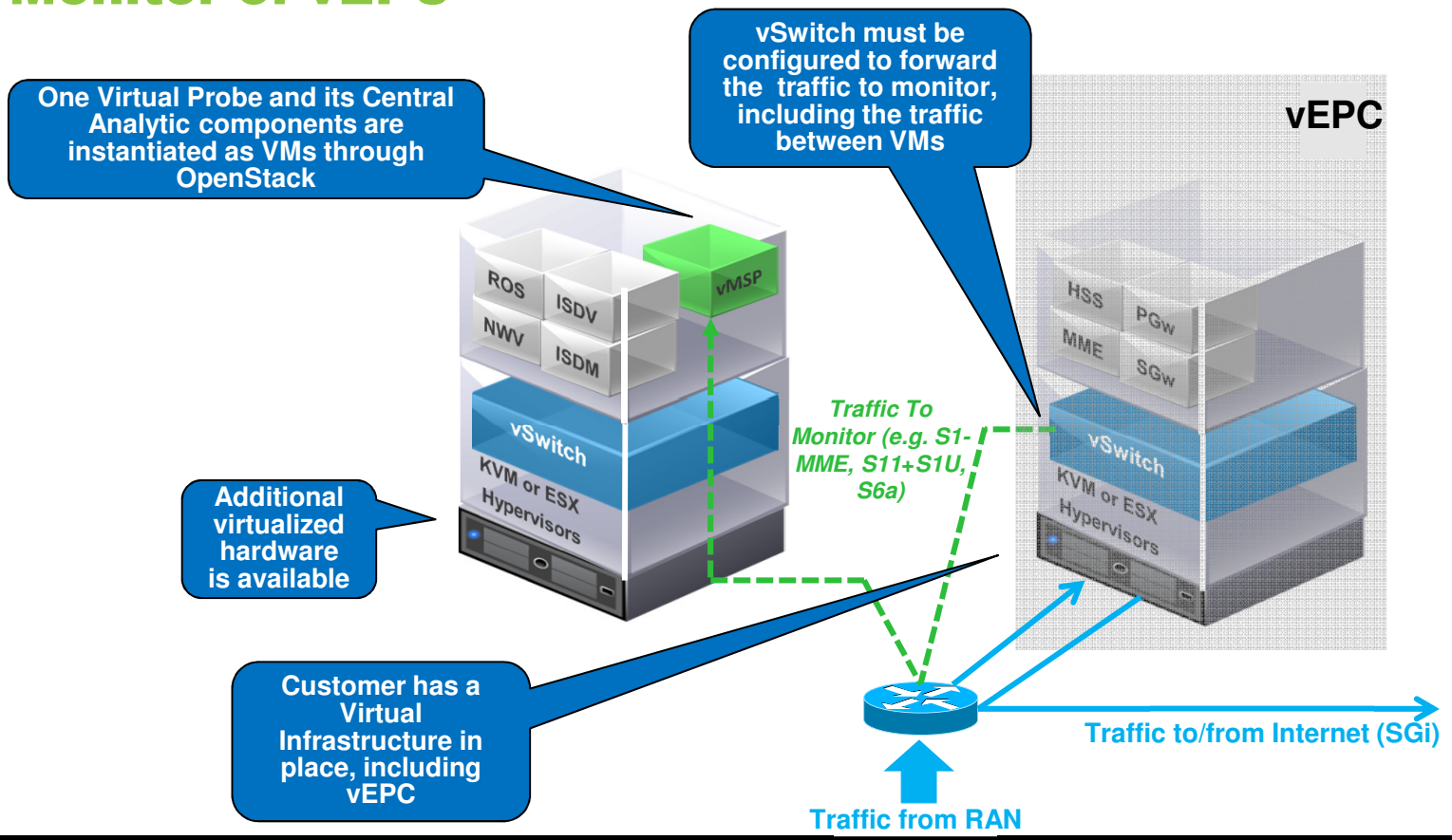
Traffic between VMs ("East-West") does not exit the Compute Node, making the physical probes "blind" except for "North-South" traffic

East-West Traffic Visibility: Options

Mirror Port from SDN Controller	*Virtual Switch Mirror Ports*	*Virtual Taps onto Hypervisor*	*TaaS (Tap-as-a-Service)*	*Probes integrated into VNF*
➢ PROs: probably the best method. As example, Juniper Contrail has a powerful GUI for such configuration ➢ CONs: none, but SDN controller must be available with its "virtual router" replacing OVS	➢ PROs: full visibility of east-west traffic ➢ CONs: load on vSwitch, probable additional resources are required for mirroring	➢ PROs: no load on vSwitch, possible distribution of traffic across multiple monitoring apps ➢ CONs: requires installation of software into the hypervisor, complexity	Currently an Open Source project within Openstack, performances and adoption by NFVI vendors still unknown…	➢ PROs: none ➢ CONs: available data are only the ones the node vendor decided to export. Service Assurance totally based on data coming from the nodes not successful in the past…

Virtual Probe Deployment Example

Monitor of vEPC



http://www.empirix.com/contact/about-empirix/careers/

Questions ?