EMPIRIX

Quality of Experience in Virtualized Networks (NFV)

April 29, 2016

Angelo Baccarani
Product Marketing Manager - Customer Experience Assurance

About the Author

- Angelo Baccarani is currently Product Marketing Manager at Empirix (www.empirix.com) for Customer Experience 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

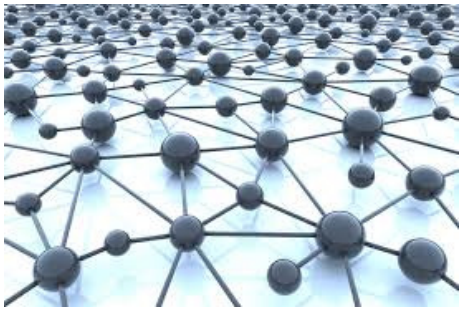
Presentation Summary

- 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*

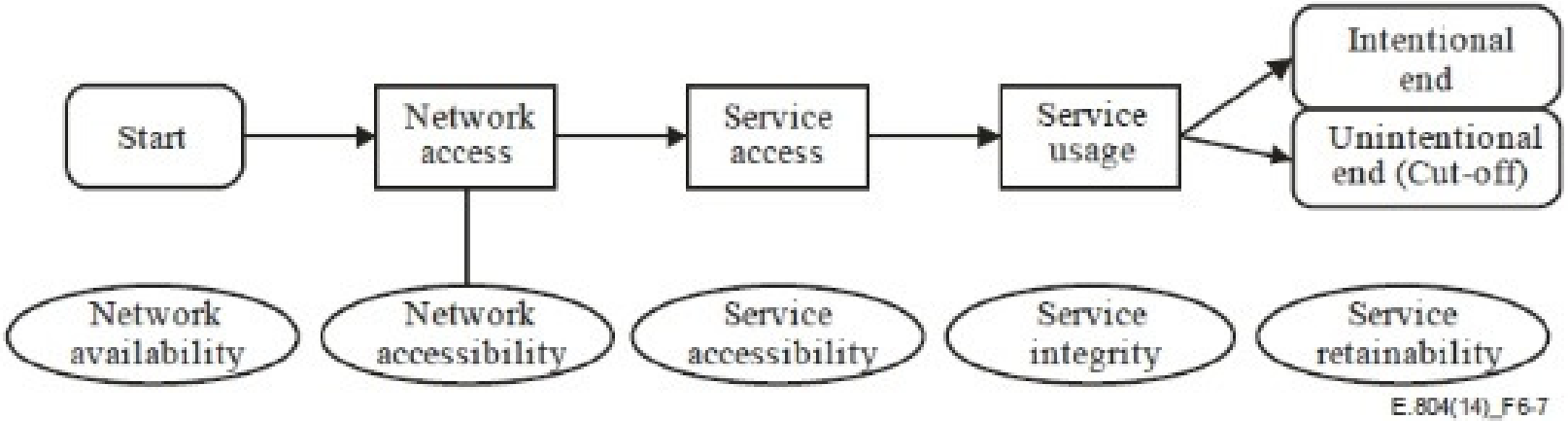
- Defined by indicators like "*excellen*t", "*good*", "*bad*" (referring to services) as well as "*satisfied*", "*tolerating*", "*frustrated*" (referring to the users)

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

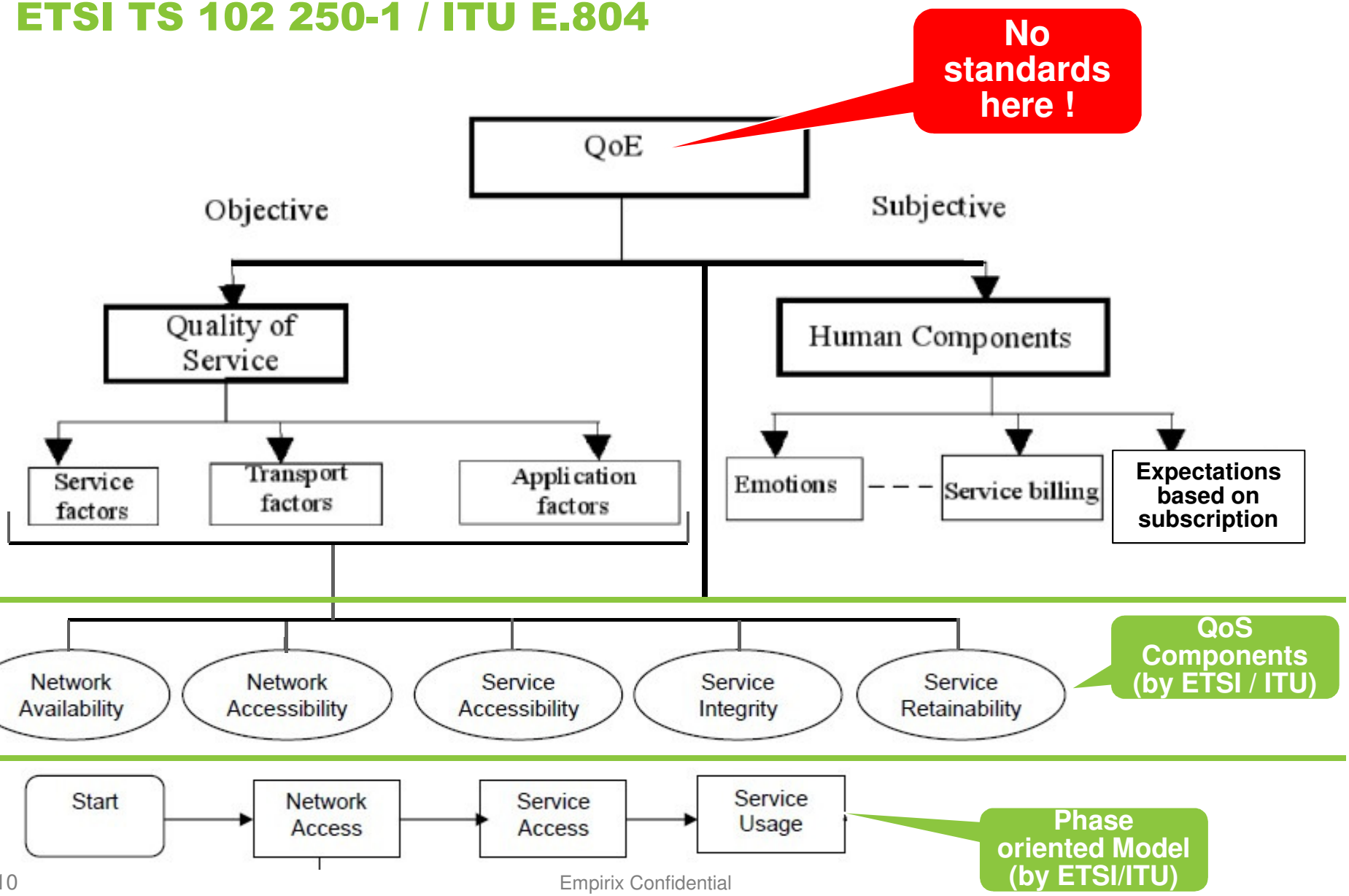
- **Network Availability -** Probability that the services are offered to a user via a network infrastructure
- **Network Accessibility -** Probability that the user performs a successful registration on the network which delivers the service
- **Service Accessibility -** Probability that the user can 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»

From QoS to QoE: ITU Model

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


Message Router


CDN


Session Border Controller


WAN Acceleration


DPI


Firewall


Carrier Grade NAT


Tester/QoE monitor


SGSN/GGSN

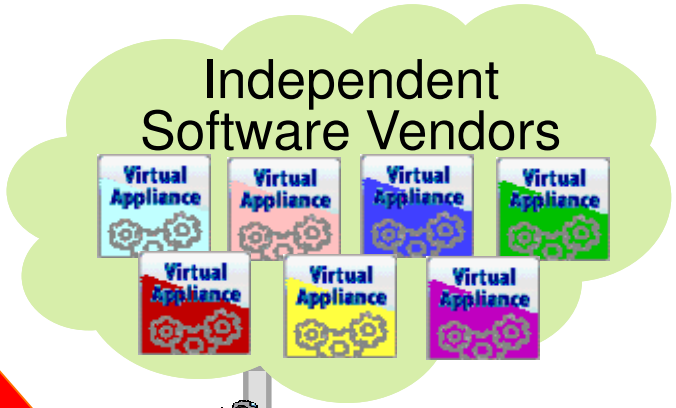

PE Router


BRAS


Radio/Fixed Access Network Nodes

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

Network Functions Virtualization Approach



Competitive & Innovative Open Ecosystem

Orchestrated, automatic & remote install.

High volume standard servers

High volume standard storage

High volume Ethernet switches

NVF in a Nutshell

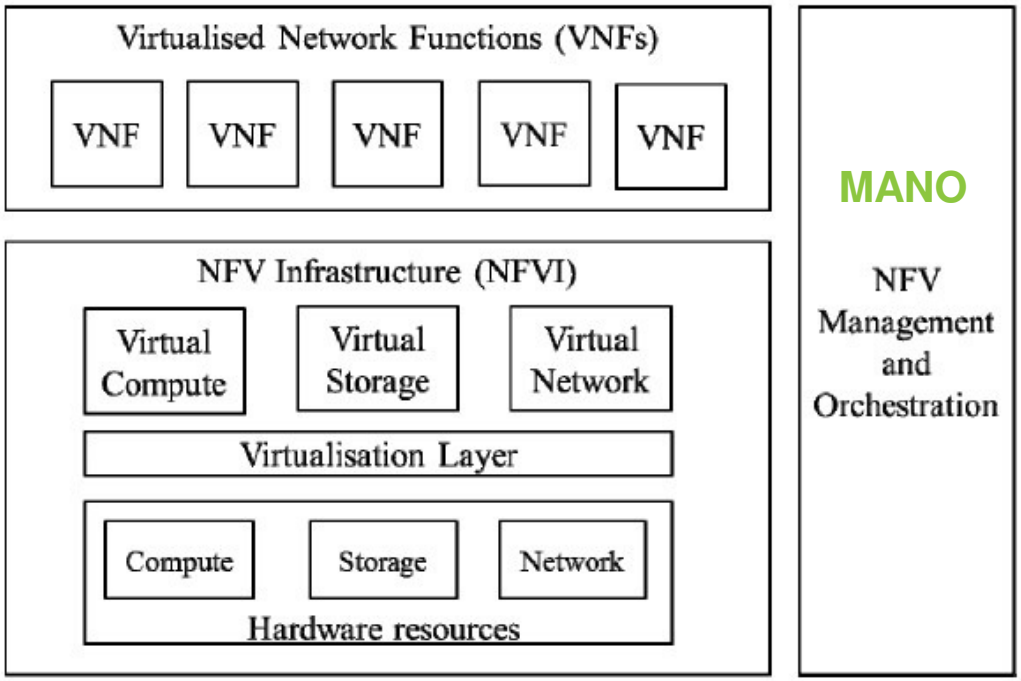
- What does an NFV environment look like in practice ?
- The starting point for NFV is a cloud environment of the kind that is widely used today to support IT workloads
- This includes at least 3 main ingredients:
  - ✓ Commercial off-the-shelf servers
  - ✓ A hypervisor such as KVM or VMware ESXi
  - ✓ A cloud management solution such as OpenStack or VMware vSphere
- But once you have your NFV in place, to provide network services you will also need a powerful *Service Orchestrator…*

NFV vs. IT Cloud: it's not the same…

- Although the current IT Cloud environment have many in common with NFV, current cloud environments have significant shortcomings in two areas, which need to be addressed in some degree in order to realize the full benefits of NFV:
  - Data plane throughput
  - Operations automation a.k.a. "orchestration"
- This is why the technologies for NFV differ from the ones already adopted in the IT Cloud

NFV Framework (ETSI GS NFV 002)

- Virtualised Network Function, as the software implementation of a network function which is capable of running over the NFVI.
- NFV Infrastructure (NFVI), including the diversity of physical resources and how these can be virtualised. NFVI supports the execution of the VNFs.
- NFV Management and Orchestration, which covers the orchestration and lifecycle management of physical and/or software resources that support the infrastructure virtualisation, and the lifecycle management of VNFs. NFV Management and Orchestration focuses on all virtualisation-specific management tasks necessary in the NFV framework.

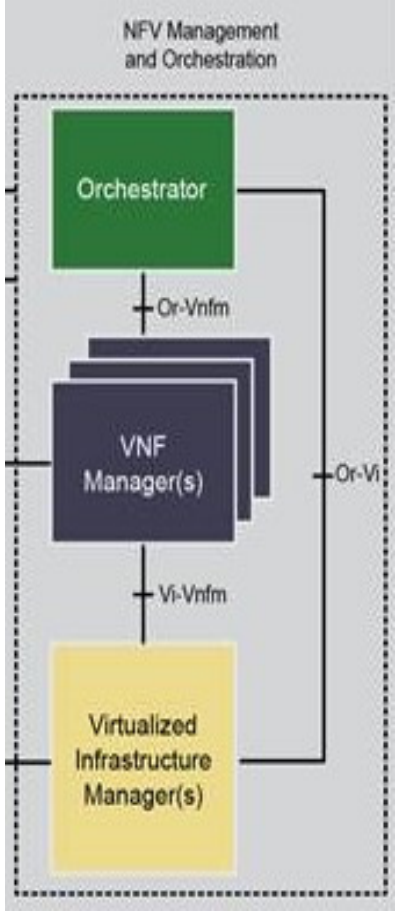


High-level NFV framework

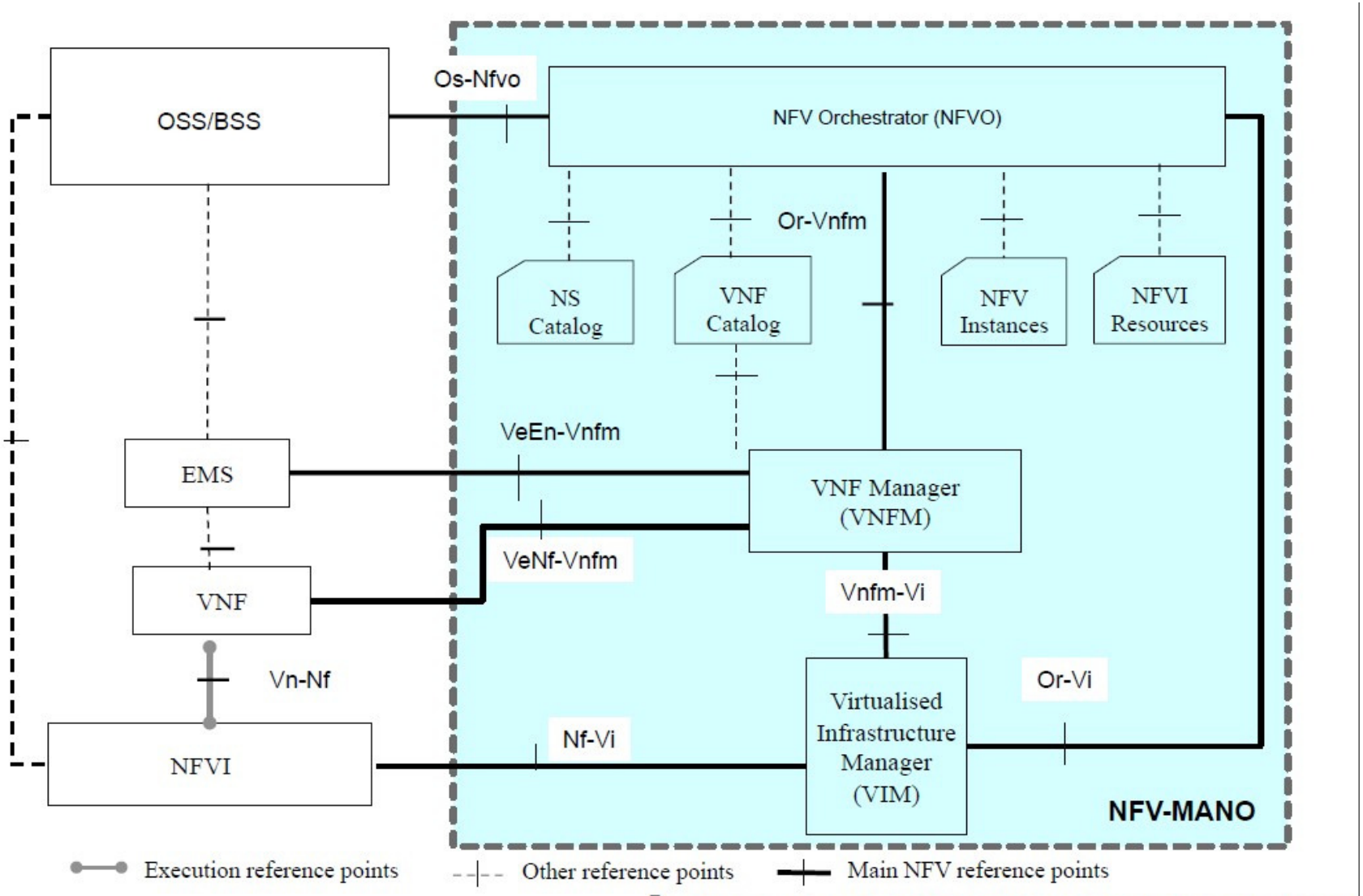
ETSI “MANO” Framework

- The ETSI MANO framework breaks down the management and orchestration needs for the NFV architecture into 3 functional layers:
  1) **Virtualized Infrastructure Managers (VIMs):** handles the virtualization of physical hardware in the data center. Using hypervisors, the VIM provides lifecycle management functions (create, edit, delete, start, and stop) for the virtual data center elements related to compute, network, and storage functions
  2) **VNF Managers (VNFMs):** The VNF manager must automatically detect all VNF failures and ensure that they are restarted so that there are no “silent failures”. Finally, as services are no longer required, the VNF manager implements automated VNF teardown through a graceful shutdown process
  3) **NFV Orchestrator (NFVO):** provides lifecycle management of the network services that includes instantiation, scale-out/-in (called elastic scaling), performance measurements, event correlation, resource management, validation and authorization for resource requests, and policy management

- Summarizing, VIM and VNFM manage respectively the hardware infrastructure and the VMs while the NFVO manages the network services

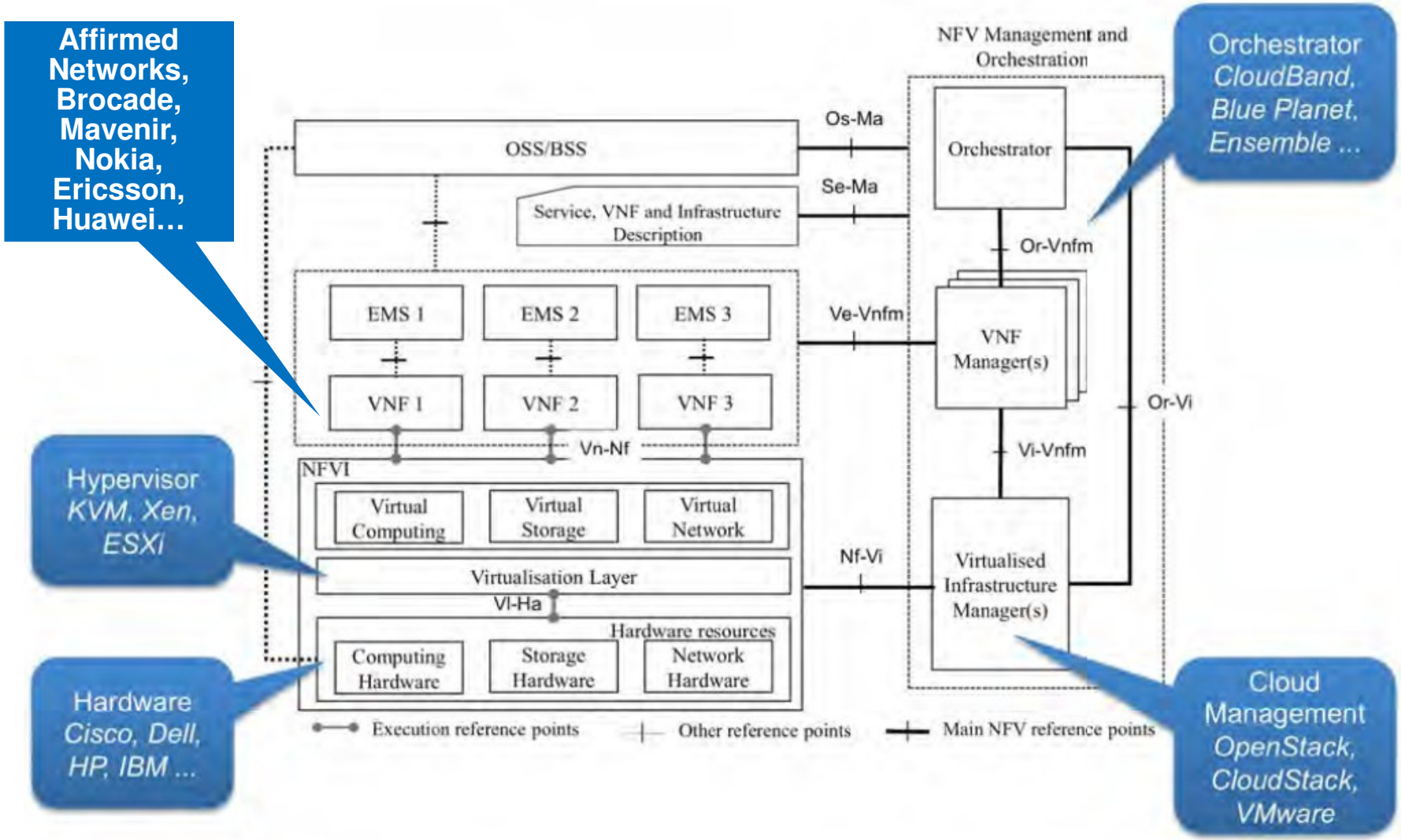


ETSI “MANO” Architecture



5 Source: ETSI NFV MANO WI document (ongoing work)

Some Vendors Names…

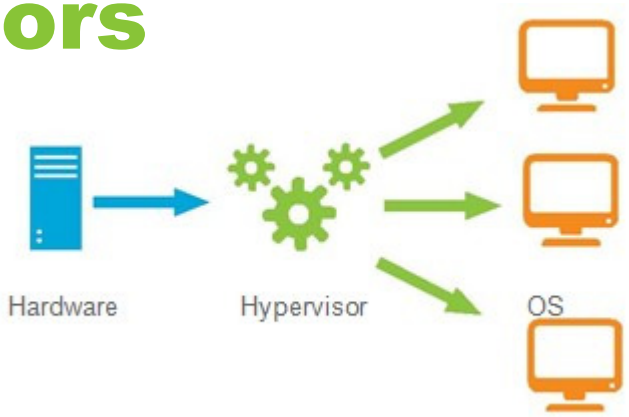


Hypervisor: Definition

- A hypervisor is one of two main ways to virtualize a computing environment (the other being *container)*
- 'Virtualize' mean to divide the resources (CPU, RAM etc.) of the physical computing environment (known as a host) into several smaller independent 'virtual machines' known as guests
- Each guest can run its own operating system, to which it appears the virtual machine has its own CPU and RAM, i.e. it appears as if it has its own physical machine even though it does not
- To do this efficiently, it requires support from the underlying processor (a feature called VT-x on Intel, and AMD-V on AMD)

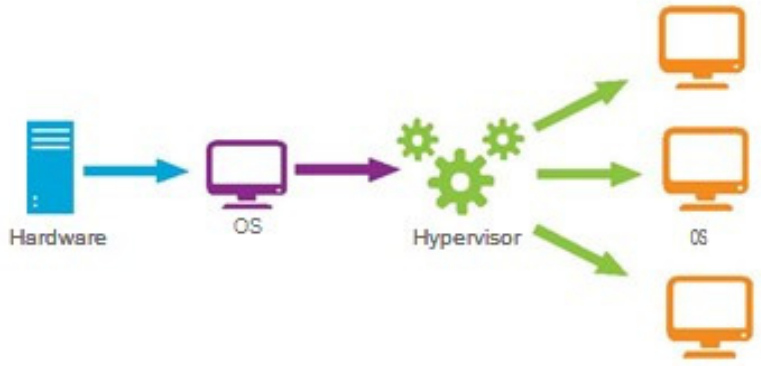
Type of Hypervisors

- **Type 1 (*native bare metal*):**



A Type 1 hypervisor (sometimes called a 'Bare Metal' hypervisor) runs directly on top of the physical hardware. Each guest operating system runs atop the hypervisor. VMware ESX/ESXi is an example (no OS is required)

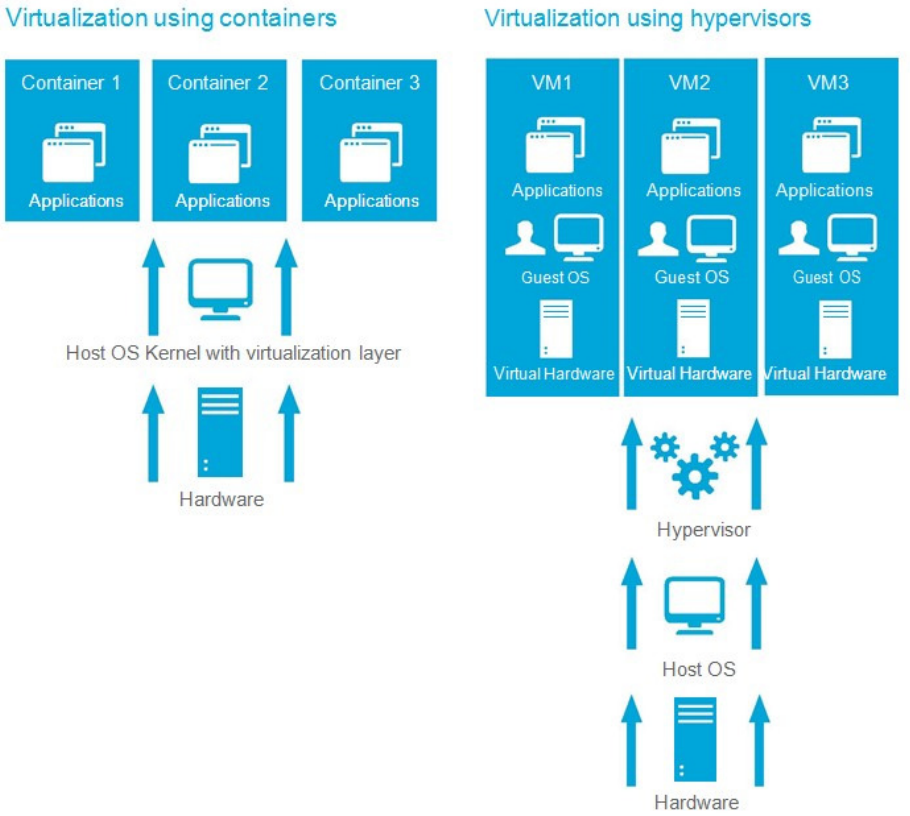
- **Type 2 (*hosted*):**



- A Type 2 hypervisor (sometimes called a 'Hosted' hypervisor) runs inside an operating system which in turn runs on the physical hardware. Each guest operating system then runs atop the hypervisor. KVM is an example and requires a Linux distribution installed

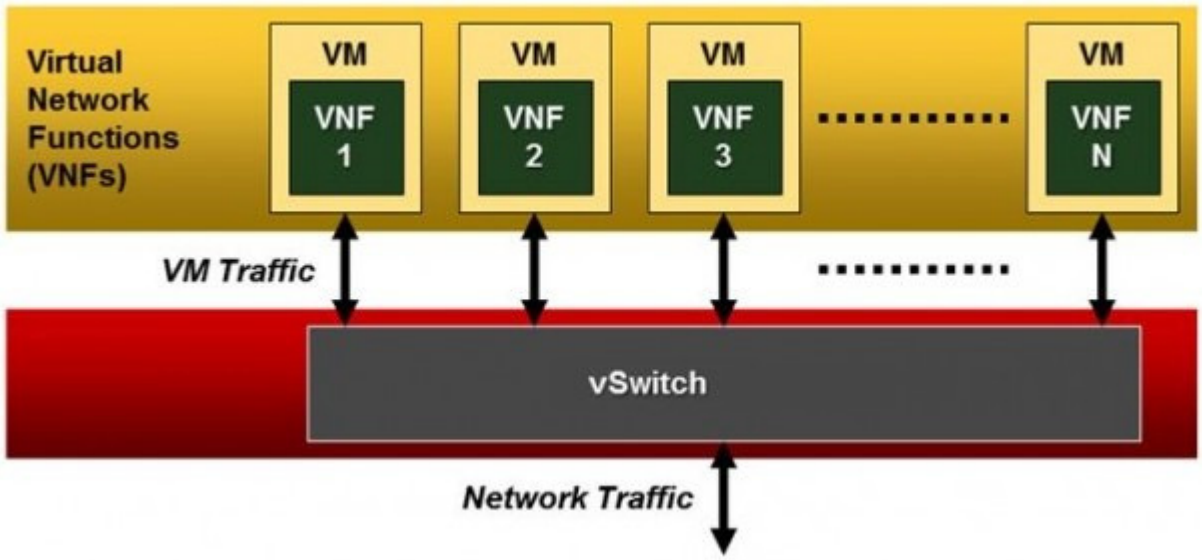
Containers

- A hypervisor segments the hardware by allowing multiple guest operating systems to run on top of it
- In a *container* system, the host operating is itself divided into multiple containers, each running a virtual machine
- Each virtual machine thus not only shares a single type of operating system, but also a single instance of an operating system (or at least a single instance of a kernel)



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

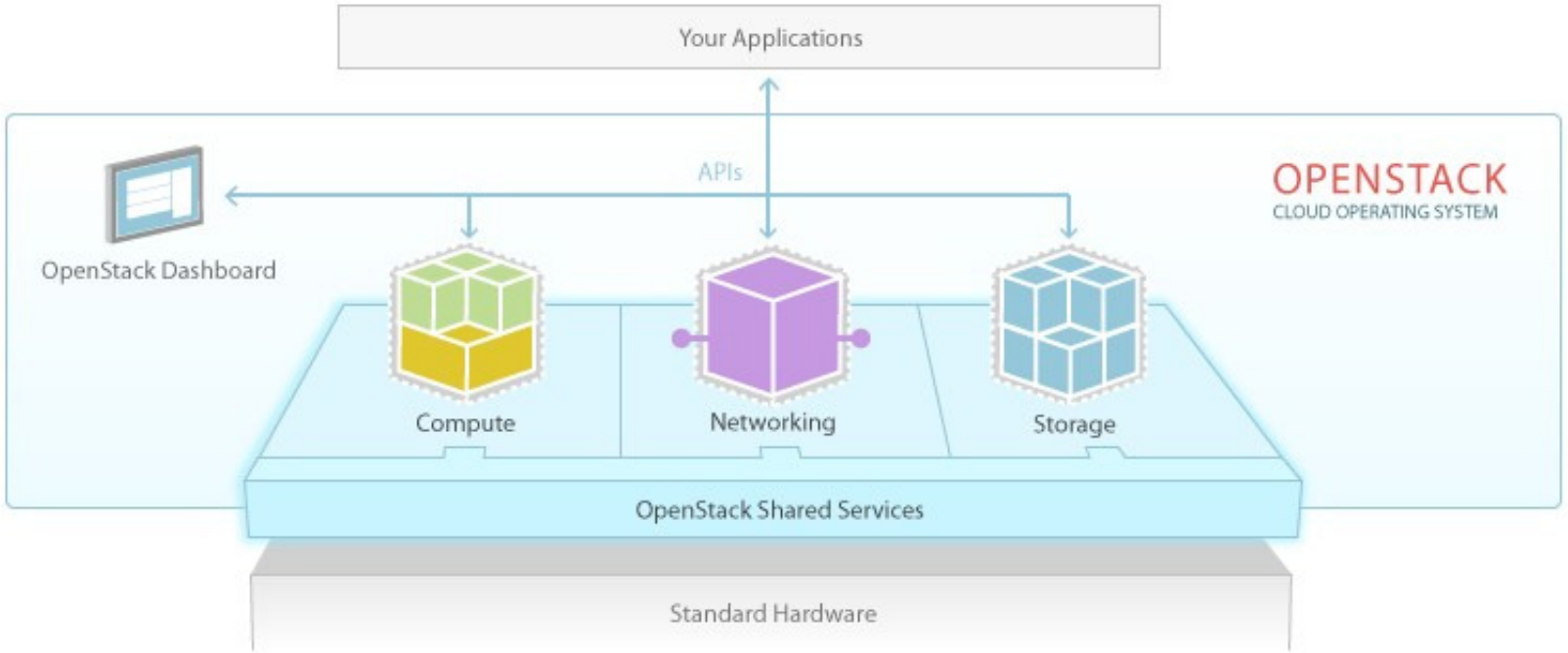
- vSwitch is critical to us as vendor of Virtual Probe because it will basically replace the physical Network Interface Card that today is provided on the hardware-based probe appliances

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

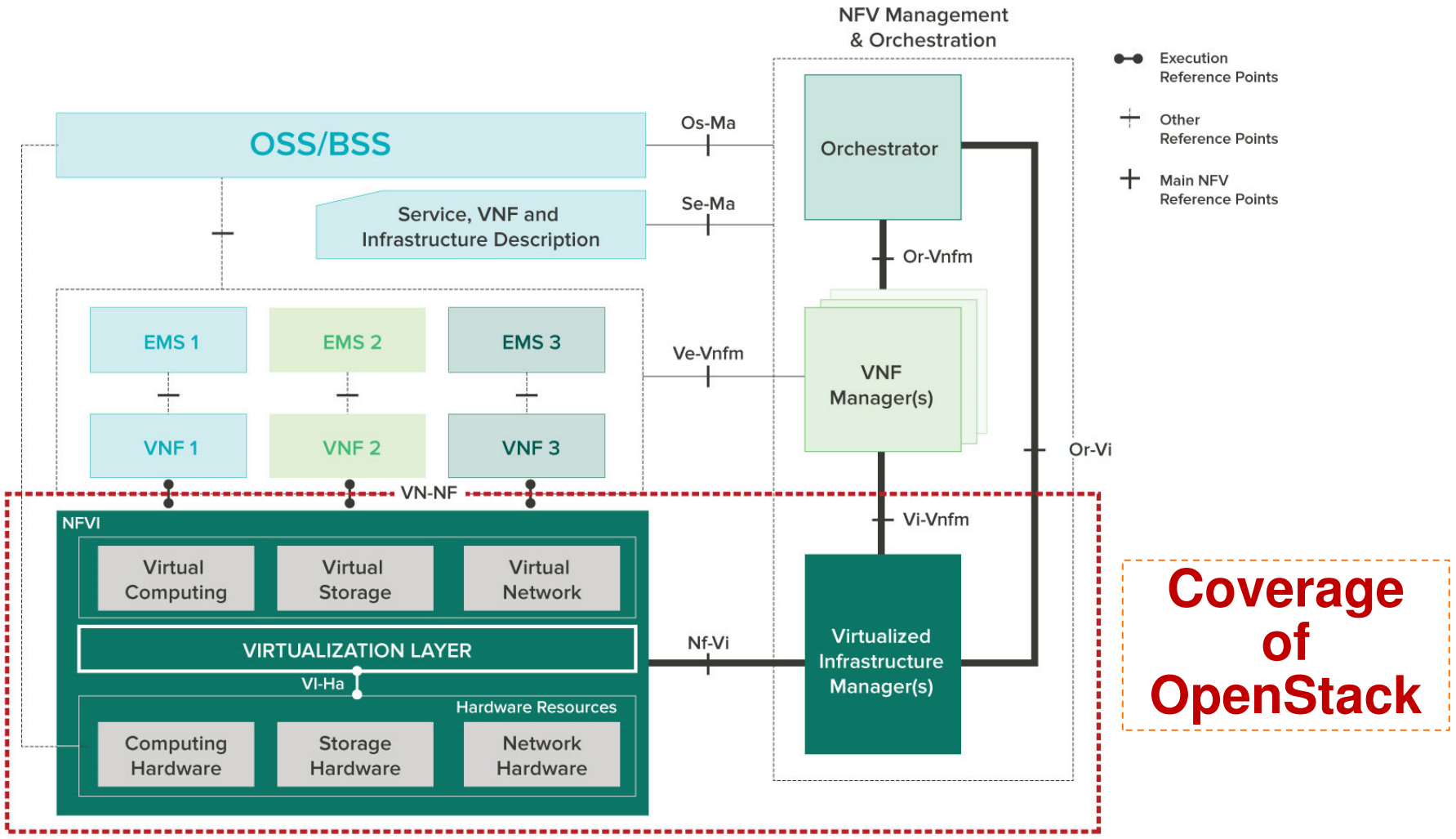
- Note that deployment of a virtual probe will always require the configuration of the vSwitch in order to receive the right data (similar to what today must be done to enable Span Ports)

VIM + NFVI: OpenStack

- OpenStack is a cloud operating system that controls large pools of compute, storage, and networking resources throughout a datacenter
- A Dashboard gives administrators control while empowering their users to provision resources (i.e. activating VMs) through a web interface
- OpenStack consists of a series of interrelated projects (Horizon, Nova…) delivering various components for a cloud infrastructure solution



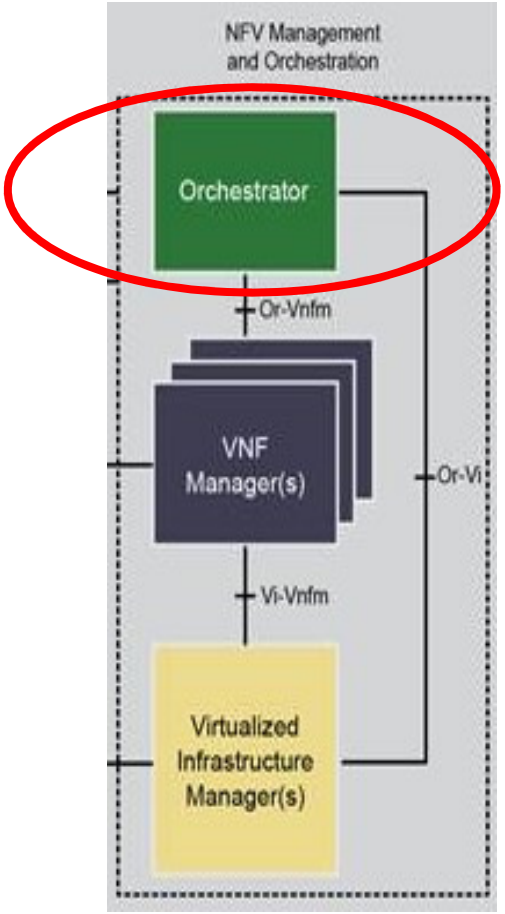
OpenStack in NFV Reference Model



Coverage of OpenStack

NFV Orchestrator: Definition

- It is the controlling logic for the lifecycle management of NFV services
- In ETSI terms, it's one of three MANO functions, with the others being the VNFM(s) and the VIM(s)



How Orchestrator Works

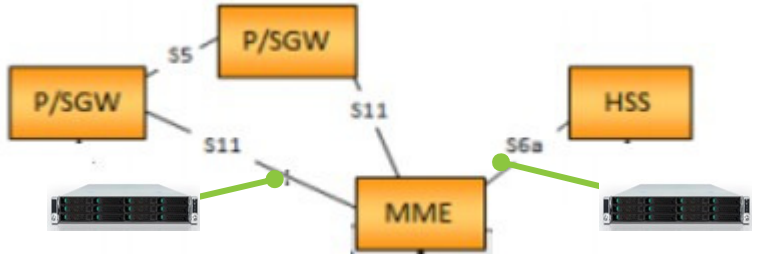
- When service provider introduces a new service request, the NFV orchestrator receives as input from the OSS/BSS the service data model that describes the new service to be instantiated, typically expressing it as a set of linked VNFs.
- The grouping of VNFs can be described in terms of either function graphs or service graphs
- The overall functionality of the service is decomposed into components with relationships described by connections and functionality (a.k.a. *Service Chaining*)
- NFV orchestrator determines the availability and features of the physical platform resources and generates an optimized map of resource locations, where VNFs should be instantiated and also the required connections between VNFs
- The VNFs themselves are instantiated through a series of actions performed by the VNF manager and the VIM (the latter, typically, based on OpenStack platform)

QoE in Virtualized Networks

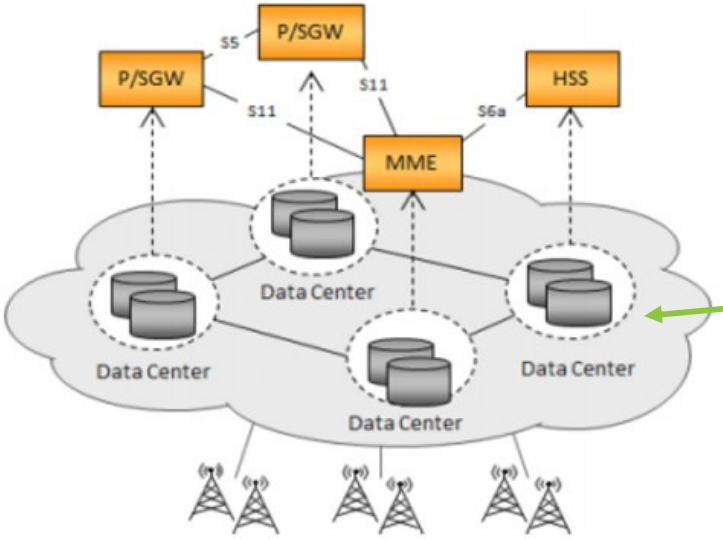
Passive Probing of NFV

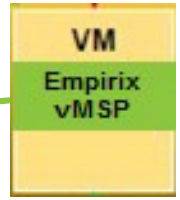
Example: from EPC to vEPC
...and the problem of how to monitor it...

- 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

NFV Passive Probing: Challenges

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

- However, passively monitoring Virtualized Networks poses various challenges depending on the level of "virtualization" that will be implemented:

  - **Potential lack of visibility of the traffic** once the network interfaces (e.g. S11, Gn, S6a…) are all moved into a "Cloud" (i.e. *virtualized*)

  - **Dynamicity of the 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 the subscribers' QoE as main measurement parameter

Options for Probing NFV

- Given such challenges, 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

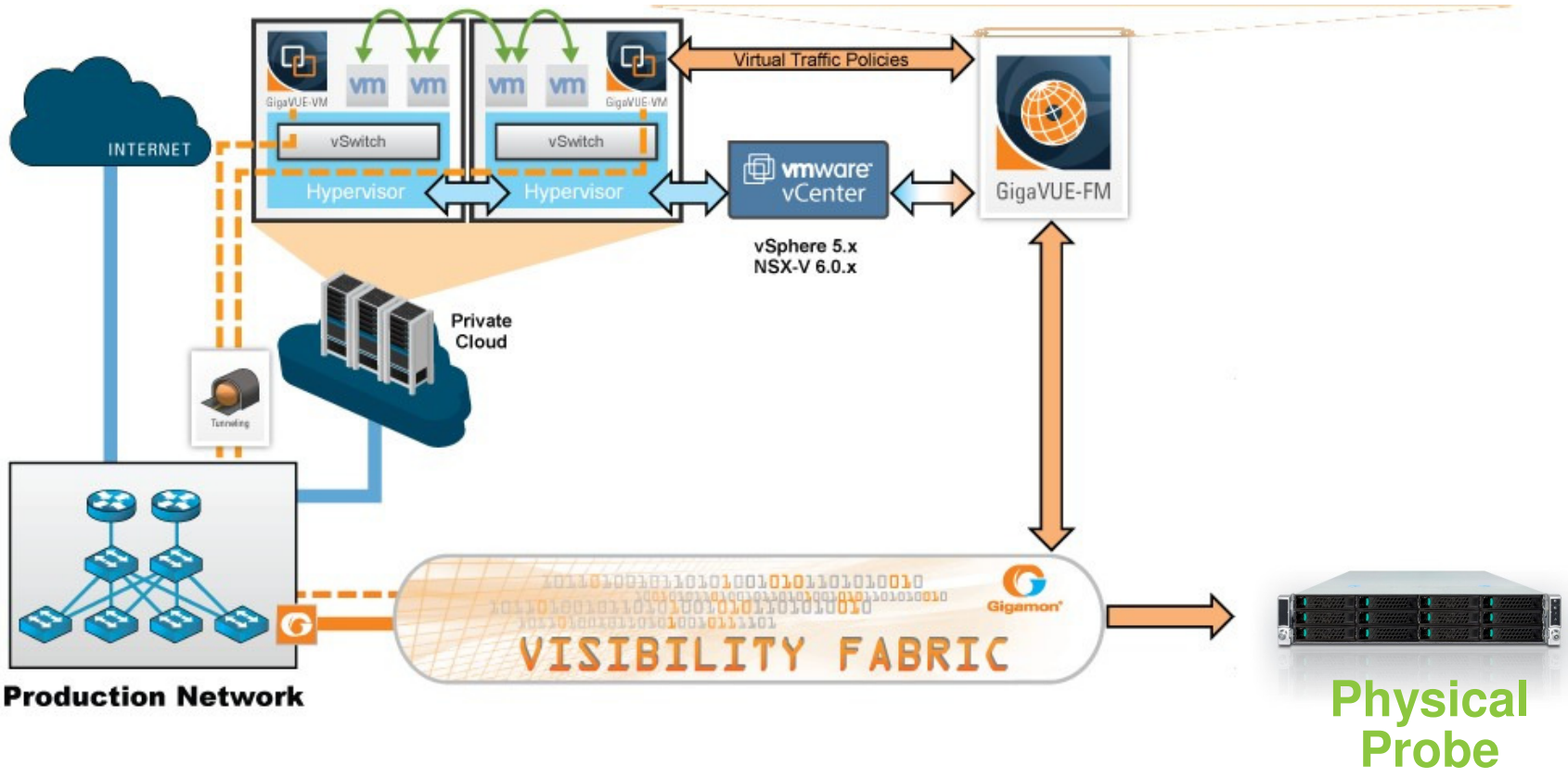
- There are three possible approaches toward that direction:

1) Deploy virtual TAPs within the NFV infrastructure (in the form of dedicated VMs), extract the desired traffic, forward it to an external aggregator that delivers the packets to physical probes

2) Integrate virtual probes functionality into the virtualized nodes

3) **Empirix solution**: deploy virtual probes that are fully independent of the VNF systems and receive a copy of the traffic to monitor from the virtual switches (just as like as the hardware probes today receive data from a mirror port or a physical tap)

Option 1: Virtual Tap

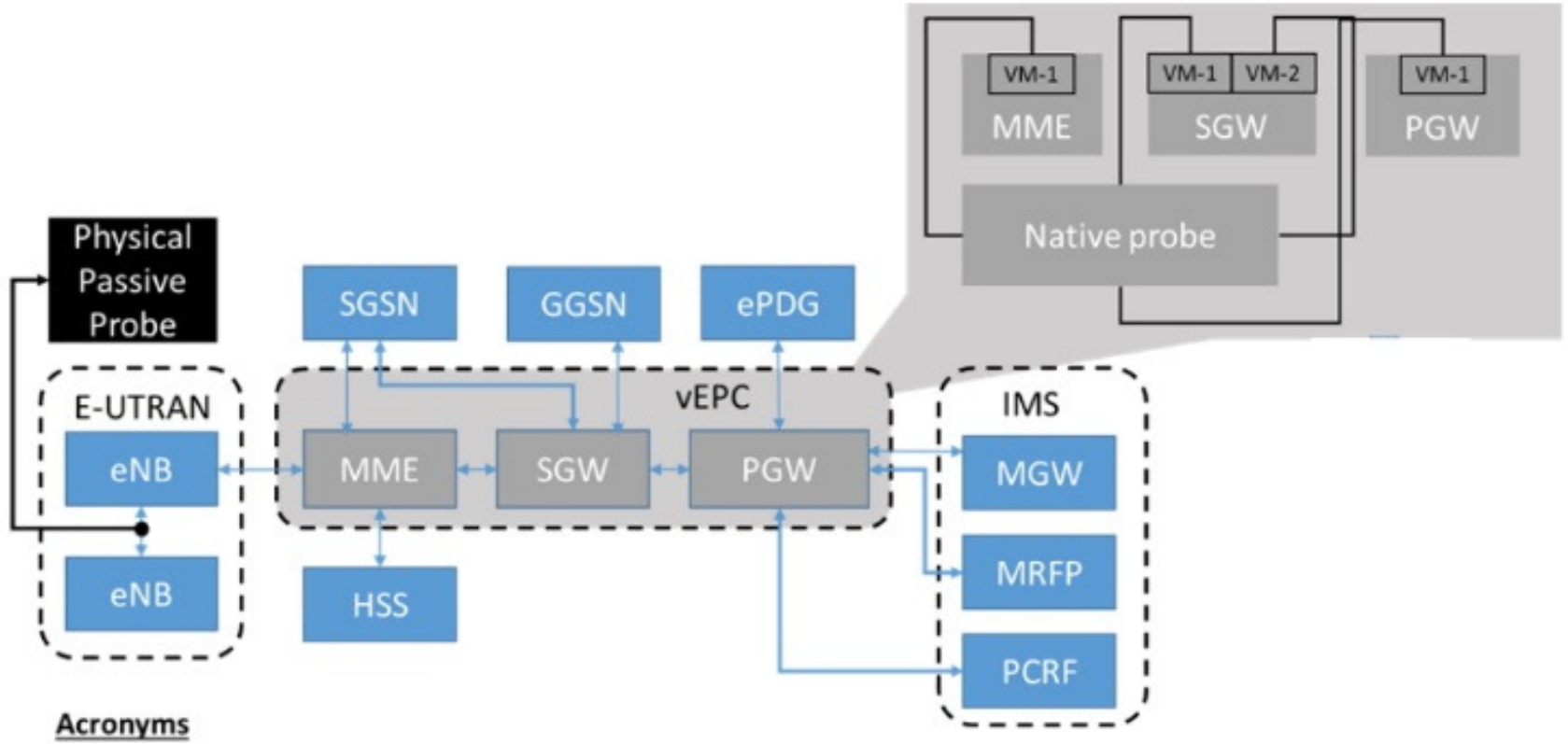


Source: Gigamon

Option 1: Strengths & Weaknesses

- This approach has the advantage to allow the CSP to re-use existing probes
- But does not allow the automatic scaling of the probe system (because still based on hardware appliances)
- Introduces some doubt about the accuracy of the QoS measurements (e.g. MOS), because the network packets have to flow through multiple components before reaching the probe
- It is also unclear why a *virtual tap* should replicate a job that a virtual switch can do (i.e., switching packets from source to destination based upon specific rules)

Option 2: Native Probes



Acronyms

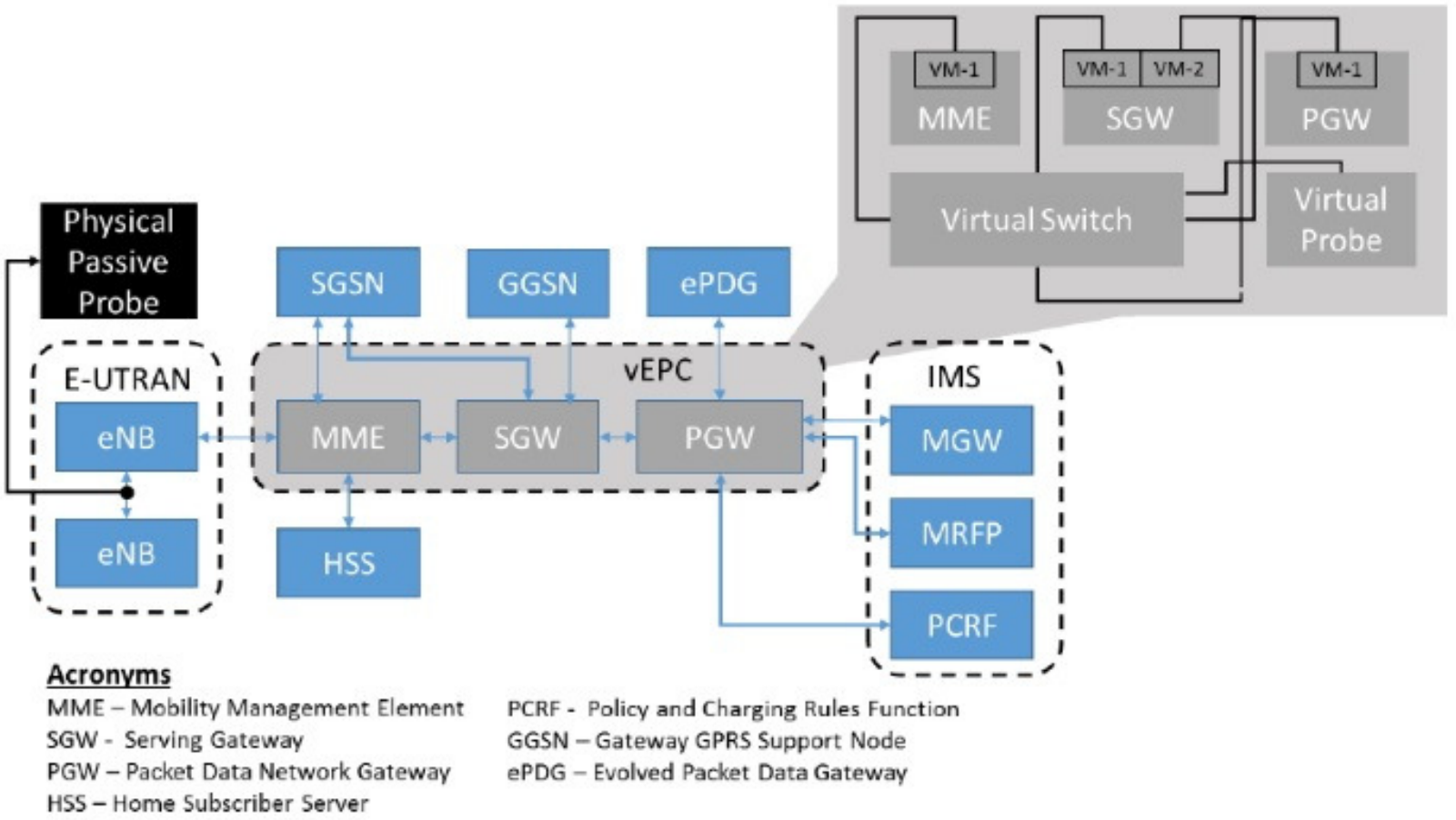
MME – Mobility Management Element
SGW - Serving Gateway
PGW – Packet Data Network Gateway
HSS – Home Subscriber Server
PCRF - Policy and Charging Rules Function
GGSN – Gateway GPRS Support Node
ePDG – Evolved Packet Data Gateway

Source: Appledore Research Group

Option 2: Strengths & Weaknesses

- Although it sounds appealing, this method also presents various disadvantages
- Data being exposed to the external applications are only the ones the node vendor has decided to export
- Furthermore, it provides only aggregated measurements that is good for Performance Monitoring while, to perform Troubleshooting, visibility down to a single packet is required
- Lastly, some CSPs may question using a monitoring solution from their network infrastructure vendor vs and independent monitoring solution
- Many CSPs already faced this issue in the past when they tried to implement Service Assurance totally based on data coming from the network nodes and they realized it was not an optimal solution

Option 3: Virtual Probes



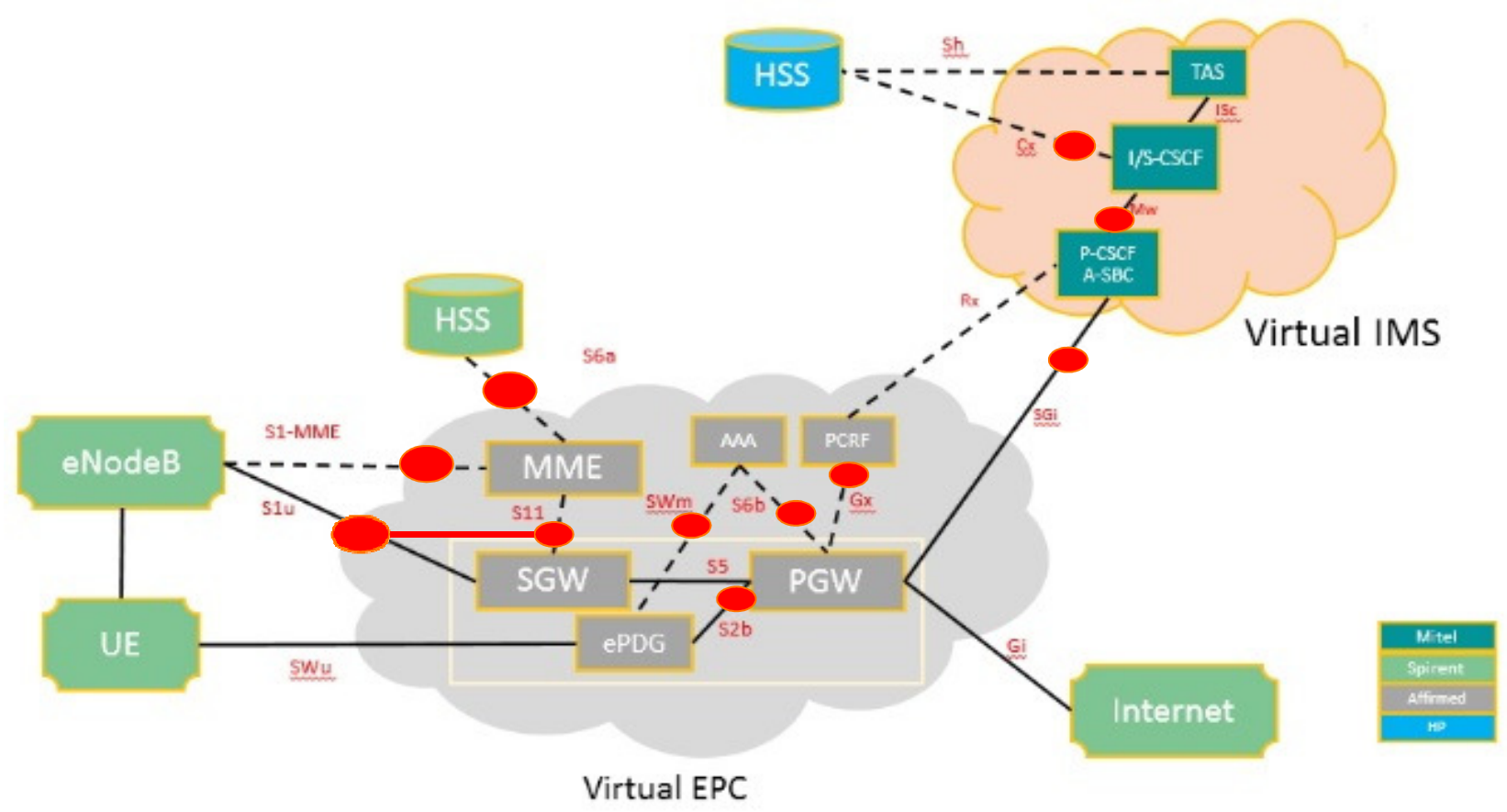
Source: Appledore Research Group

Option 3: Strengths & Weaknesses

- Virtual Probes, combined with a flexible centralized data collection and correlation system, can provide a unified view of the traffic down to single subscriber detail and are fully independent from the NFV vendor
- Because these virtual probes run as close as possible to the respective VNF they are monitoring, they provide very accurate measurements
- Additionally, virtual probes can automatically "*scale-up or scale-down*" as needed with the other NFV infrastructure being monitored (this is one of the promises of NFV, a.k.a. *network elasticity)*
- For example if the Orchestrator instantiates more vEPC components to satisfy an increasing traffic demand (a.k.a. "*scale-up")*, virtual probe capacity can be also increased accordingly. Once the traffic peak is over, the Orchestrator will release the hardware resources for both the vEPC and the virtual probes (a.k.a. "*scale-down")*
- Finally, because these probes are independent from the VNF vendors, they can be easily expanded to provide additional measurements as soon as new services are provided by the CSP

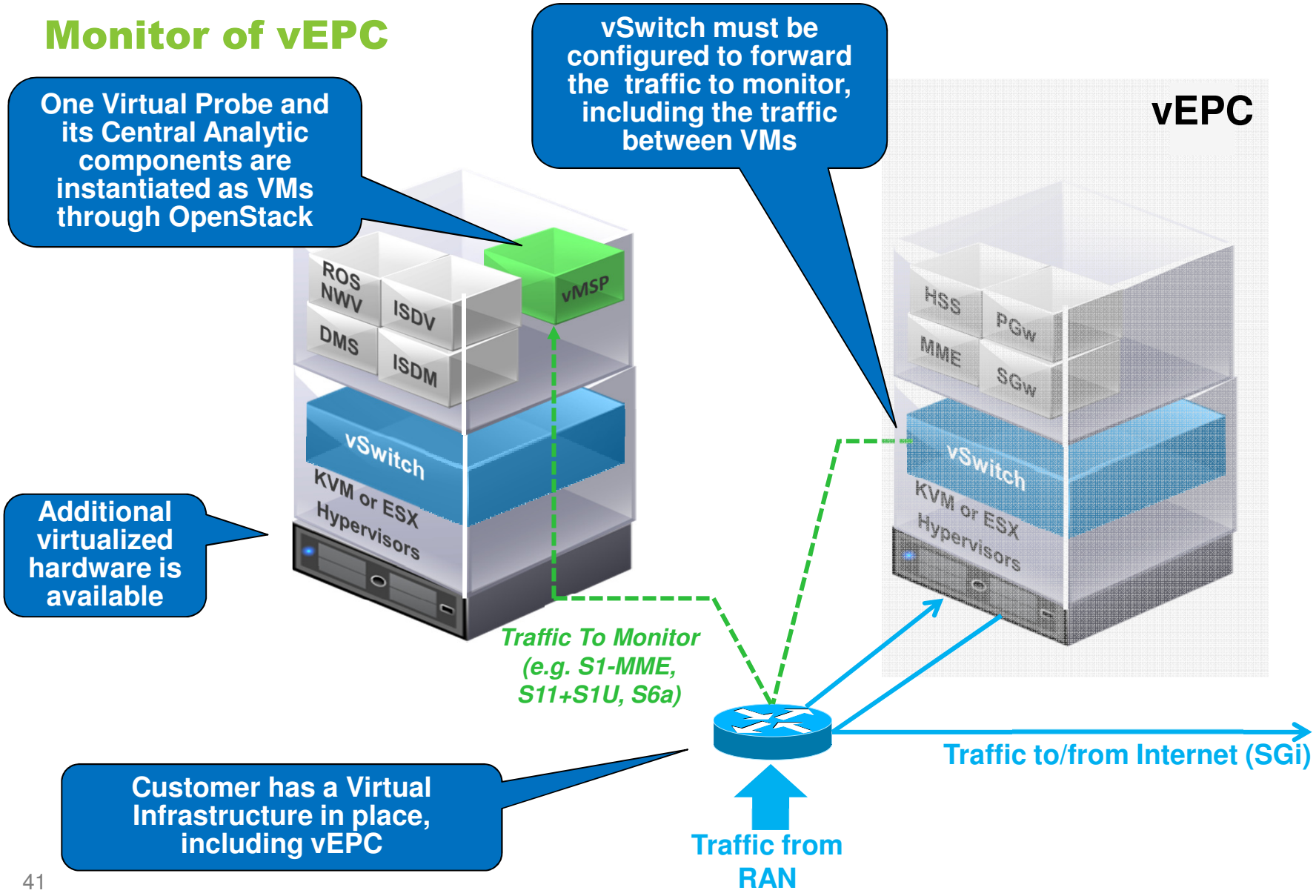
Real Scenario Example: vEPC + vIMS

Monitor Points (logical, not physical !)



Virtual Probe Deployment Example

Monitor of vEPC



Questions ?