Introduction to Network Function Virtualization: concept and standardization

Facultad de Informática, Universidad de Murcia

Miércoles, 12 de mayo de 2021

Carlos J. Bernardos <cjbc@it.uc3m.es>

Facultad de Informática

UNIVERSIDAD DE MURCIA

uc3m | Universidad Carlos III de Madrid

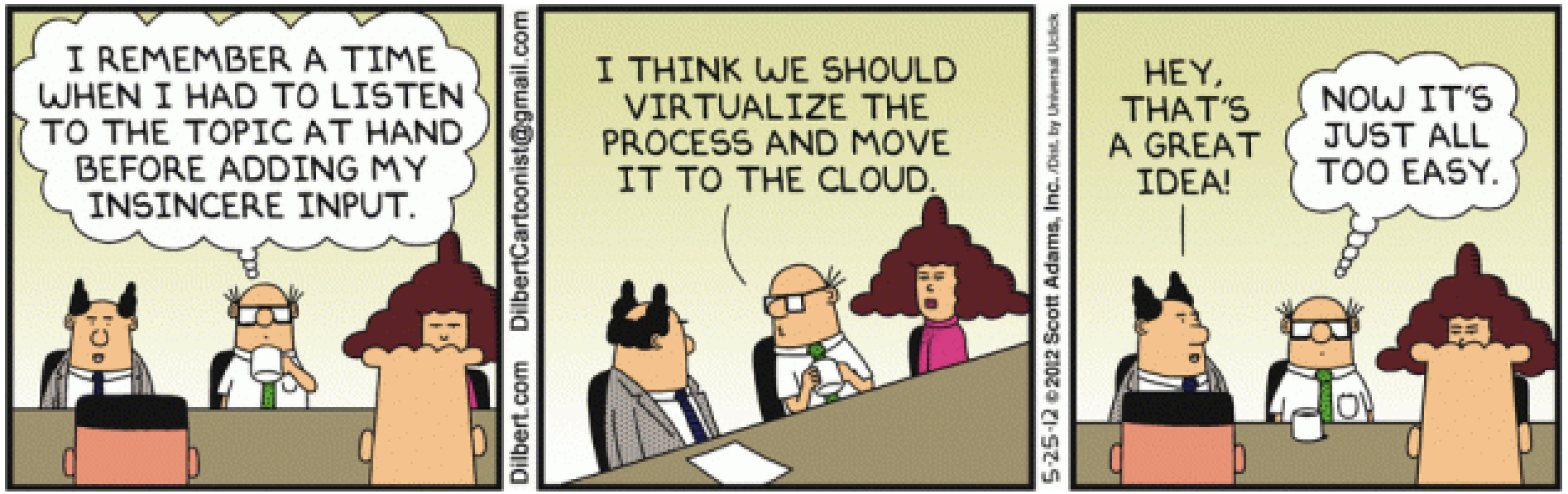
Who am I? who are you?

- Who am I?
  - Telecommunication Engineer, PhD in Telematics
  - Associate professor at UC3M
  - Research interests: mobility, Wireless networks and, lately, network virtualization and 5G
  - H2020 projects: coordinator of 5Growth
  - Standardization contributor: IETF and ETSI

Outline

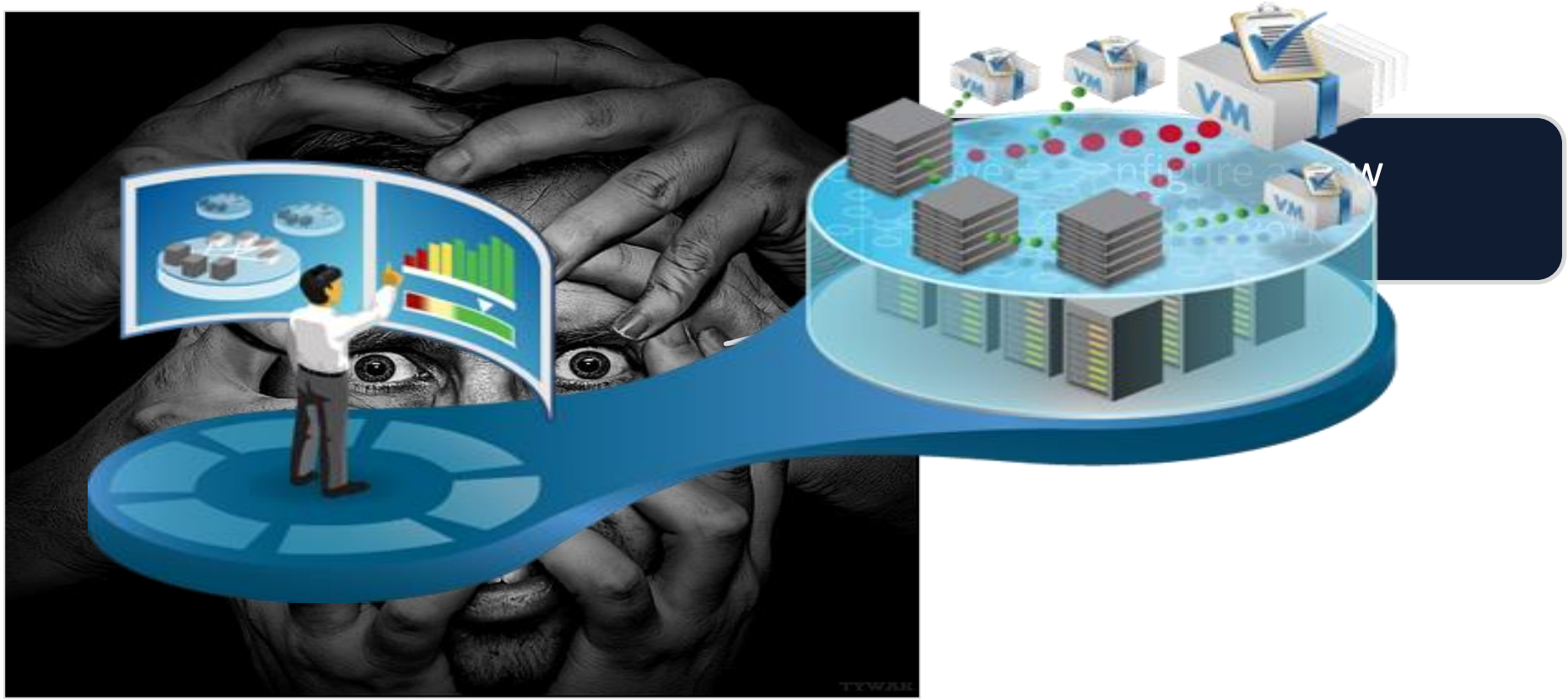
- Network function virtualization
  - Introduction: Motivation and history of NFV
  - Definition
  - Fields of Application and Use Cases
  - Benefits, Challenges and Requirements for NFV
  - Enablers for NFV
- NFV architecture
  - High-level architecture
  - Network services in NFV
  - NFV terminology
  - ETSI NFV reference architecture
- Virtual Network Functions Architecture
- NFV implementations
- References

Network function virtualization



Motivation

- **Where do we come from? Where are we going?**



Motivation

- Traditional telecommunications industry
  - Based on deploying physical proprietary equipment for each function that is part of a given service
  - Service components have strict chaining/ordering that must be reflected in the network topology
  - Requirements for high quality, stability and protocol adherence
    - ➢ This has led to long product cycles, very low service agility and heavy dependence on specialized hardware

Motivation

- Users increasingly demand more diverse and short-lived services with high data rates
  - Need for purchase, store and operate new physical equipment
  - New and rapidly changing skills to operate and manage the equipment
  - Dense deployment of network equipment

High CAPEX and OPEX

  - Cannot be translated in higher subscription costs
  - Providers forced to find new ways of building more dynamic and service-aware networks, with shorter product cycles, cheaper and more agile

History of NFV: ETSI NFV ISG

- Collaboration around NFV started in Oct. 2012
  - Leading operators and service providers authored the NFV Whitepaper
  - 7 of these operators selected the ETSI to be the home of the Industry Specification Group (ISG) for NFV: ETSI ISG NFV
- Now, much more people working on NFV
  - 79 members + 44 participants in ETSI NFV (Dec. 2020)
    - But, membership went under renovation in 2019: 125 members + 185 participants in ETSI NFV (as of Jan. 2018)
  - ISGs are not meant to develop standards
    - Their recommendations are expected to be enforced by other SDOs such as 3GPP
    - BUT, the ETSI NFV ISG is now doing standards

History of NFV: ETSI NFV ISG

- All ETSI NFV normative deliverables are grouped into *releases*
  - A release is defined as “a set of deliverables that specify a well defined, stable and internally consistent set of functions”
    - Group Specifications (GS)
    - Group Reports (GR)
  - Each release addresses a set of
    - Capabilities (Rel-2): “ability of an item to perform an action under given internal conditions in order to meet some demand”
    - Features (Rel-3): “functionality which represents added value to the system for a defined set of users”

History of NFV: ETSI NFV ISG

- Release 1 (2013-2014)
  - Completed in Jan. 2015 (first release in Oct. 2013)
  - 16 GS
- Release 2 (2015-2016)
  - “Completed” in Sep. 2016
  - 12 capabilities
  - 23 GS + 5 GR
- Release 3 (2017-2018)
  - Started in May 2017
  - 23 features (20 new and 3 carried over from Rel-2)
  - 23 GS + 14 GR
- Release 4 (2019-2020)

Table 5.1-1: Release 4 features

Feature name	Acronym	FEAT id	Notes
NFV-MANO upgrade	SWUP-MANO	FEAT01	Carried over from Release 3.
MEC in NFV	MECinNFV	FEAT12	Carried over from Release 3.
Licensing management	LIC	FEAT13	Carried over from Release 3.
Cloud-native VNFs and Container Infrastructure management	CNNFV	FEAT17	Carried over from Release 3.
Security management	SECMM	FEAT18	Carried over from Release 3
Network connectivity integration and operationalizatoin for NFV	NFV-Connect	FEAT19	New feature
NFV-MANO automation and autonomous networks	Auto	FEAT20	New feature
NFV enhancemetns for 5G	5GNFV	FEAT21	New feature
Multi-tenancy enhancements for NFV-MANO	M-Tenant	FEAT22	New feature
SBA for NFV-MANO	MANO-SBA	FEAT23	New feature
VNF generic management functions	VNF-OAM	FEAT24	New feature
Continuous VNF integration	VNF-CI	FEAT25	New feature
Policy Management Models	Policy-model	FEAT26	New feature

History of NFV: ETSI NFV ISG

- Working groups initially chartered (Release 1):
  - NFV INF (Infrastructure): Compute, Hypervisor, and Network Infrastructure domains
  - NFV MAN (Management and Orchestration): issues and recommendations around Management and Orchestration
  - NFV SWA (Software Architecture): software architecture for virtual network functions (VNFs)
  - NFV PER (Performance): performance and portability
    - This group also created the PoC Framework
  - NFV REL (Reliability): reliability and resiliency issues
  - NFV SEC (Security): security issues, both for the virtual functions and their management systems

History of NFV: ETSI NFV ISG

- In Release 2, more WGs (REL and SEC remain):
  - EVE: Evolution and Ecosystem
  - IFA: Interfaces and Architecture
  - REL: Reliability, Availability and Assurance
  - SEC: Security
  - TST: Testing, Experimentation and Open Source
  - SOL: Solutions
  - TSC: Technical Steering Committee
  - NOC: Network Operators
- Each working group is responsible for a series of Work Items (WIs)

History of NFV: ETSI NFV ISG

- In Release 3:
  - Information modelling
  - End-to-end multi-site services management
  - Additional considerations on management and orchestration
  - Acceleration technologies
  - Charging, billing and accounting
  - License management
  - Security analysis and management
  - Reliability and availability considerations
  - DevOps and continuous integration
  - Testing
  - Policy management
  - Identification of "Touchpoints" with information Models of other organizations

- **The NFV PoC Framework still plays a major role**
- **NFV Plugtests building on NFV PoC Framework key achievements**
- **Release 2 specification maintenance (bug fixes)**

History of NFV: ETSI NFV ISG

- In Release 4:
  - **NFVI evolution**, focusing on enhancements to support lightweight virtualization technologies, optimizing NFV Infrastructure (NFVI) abstraction for reducing the coupling of VNFs to infrastructure, and optimizing networking integration into the infrastructure fabric to ease the connectivity for Virtualized Network Functions (VNFs) and Network Services (NSes)
  - **Enhancing NFV automation and capabilities**, covering aspects such as: improving life-cycle management and orchestration, the simplification of VNF and NS management aspects leveraging virtualization, and handling advances in autonomous networking
  - **Evolving the NFV-MANO** (Management and Orchestration) framework, focusing primarily on optimizing internal NFV-MANO capability exposure and usage
  - **Accompanying operationalization aspects** which include: the simplification of NFV to ease development and deployment of sustainable NFV based solutions, verification (and certification) procedures and mechanisms, and operationalization, integration and use of NFV with other management and network frameworks

History of NFV: ETSI docs (up to Jan. 2019)

	Standard number	Document title
Rel1	GS NFV 001 (*)	Use Cases
Rel1	GS NFV 002	Architectural Framework
Rel1	GS NFV 003	Terminology for Main Concepts in NFV
Rel1	GS NFV 004	Virtualisation Requirements
Rel1	GS NFV-REL 001	Resiliency Requirements
Rel1	GS NFV-MAN 001	Management and Orchestration
Rel1	GS NFV-SWA 001	Virtual Network Functions Architecture
Rel1	GS NFV-INF 001	Infrastructure Overview
	GS NFV-IFA 001	Report on Acceleration Technologies & Use Cases
Rel1	GS NFV-SEC 001	NFV Security; Problem Statement
	GS NFV-PER 001	NFV Performance & Portability Best Practises
	GS NFV-SEC 002	Cataloguing security features in management software
	GS NFV-REL 002	Report on Scalable Architectures for Reliability Management
Rel1	GS NFV-PER 002	Proof of Concepts; Framework
Rel2	GS NFV-IFA 002 (*)	VNF Interfaces Specification
	GS NFV-EVE 003	Report on NFVI Node Physical Architecture Guidelines for Multi-Vendor Environment
Rel1	GS NFV-INF 003	Infrastructure; Compute Domain

History of NFV: ETSI docs (up to Jan. 2019)

	Standard number	Document title
Rel1	GS NFV-SEC 003	NFV Security; Security and Trust Guidance
	GS NFV-REL 003	Report on Models and Features for End-to-End Reliability
Rel1	GR NFV-SEC 003	Security and Trust Guidance
Rel2	GS NFV-IFA 003	vSwitch Benchmarking and Acceleration Specification
Rel1	GS NFV-INF 004	Infrastructure; Hypervisor Domain
	GS NFV-EVE 004	Report on the application of Different Virtualisation Technologies in the NFV Framework
	GS NFV-REL 004	Report on Active Monitoring and Failure Detection
	GS NFV-SEC 004	Report on Lawful Interception Implications
Rel2	GS NFV-IFA 004	Management Aspects Specification
	GS NFV-REL 005	Report on Quality Accountability Framework
Rel1	GS NFV-INF 005	Infrastructure; Network Domain
	GS NFV-EVE 005	Report on SDN Usage in NFV Architectural Framework
Rel2	GS NFV-IFA 005	Or-Vi reference point - Interface and Information Model Specification
	GS NFV-SEC 006	Report on Security Aspects and Regulatory Concerns
Rel2	GS NFV-IFA 006	Vi-Vnfm reference point - Interface and Information Model Specification
Rel1	GS NFV-INF 007	Infrastructure; Methodology to describe Interfaces and Abstractions

History of NFV: ETSI docs (up to Jan. 2019)

	Standard number	Document title
Rel2	GS NFV-IFA 007	Or-Vnfm reference point - Interface and Information Model Specification
Rel2	GS NFV-IFA 008	Ve-Vnfm reference point - Interface and Information Model Specification
	GS NFV-IFA 009	Report on Architectural Options
	GS NFV-SEC 009	Report on use cases and technical approaches for multi-layer host administration
Rel1	GS NFV-INF 010	Service Quality Metrics
	GS NFV-SEC 010	Report on Retained Data problem statement and requirements
Rel2	GS NFV-IFA 010	Functional requirements specification
Rel2	GS NFV-IFA 011	VNF Packaging Specification
Rel2	GS NFV-IFA 013	Os-Ma-Nfvo reference point - Interface and Information Model Specification
Rel2	GS NFV-IFA 014	Network Service Templates Specification
	GS NFV-TST 001	Report on Validation of NFV Environments and Services
	GS NFV-TST 002	Report on NFV Interoperability Testing Methodology
Rel2	GR NFV-IFA 015	Report on NFV Information Model
Rel2	GR NFV-IFA 016	Information Modeling; Papyrus Guidelines
Rel2	GR NFV-IFA 017	UML Modeling Guidelines
Rel3	GR NFV-IFA 023	Report on Policy Management in MANO

History of NFV: ETSI docs (up to Jan. 2019)

	Standard number	Document title
Rel2	GR NFV-IFA 024	Report on External Touchpoints related to NFV Information Model
Rel3	GR NFV-EVE 010	Report on License Management for NFV
Rel3	GR NFV-EVE 012	Report on Network Slicing Support with ETSI NFV Architecture Framework
Rel3	GS NFV-SEC 012	System architecture specification for execution of sensitive NFV components
Rel3	GS NFV-SEC 013	Security Management and Monitoring specification
Rel3	GR NFV-REL 007	Report on the resilience of NFV-MANO critical capabilities
Rel3	GR NFV-TST 004	Guidelines for Test Plan on Path Implementation throught NGVI
	GR NFV-TST 005	Report on use cases and recommendations for VNF Snapshot
Rel3	GR NFV-TST 007	Guidelines on Interoperability Testing for MANO
Rel2	GS NFV-TST 008	NFVI Compute and Network Metrics Specification
	GR NFV-SEC 009	Report on use cases and technical approaches for multi-layer host administration
Rel3	GS NFV-EVE 007	Hardware Interoperability Requirements Specification
Rel3	GS NFV-IFA 019	Acceleration Resource Management Interface Specification
Rel3	GS NFV-IFA 018	Network Acceleration Interface Specification
Rel3	GR NFV-EVE 008	Report on Usage Metering and Charging Use Cases and Architectural Study
Rel3	GR NFV-IFA 021	Report on management of NFV-MANO and automated deployment of EM and other OSS function

History of NFV: ETSI docs (up to Jan. 2019)

	Standard number	Document title
Rel3	GR NFV-IFA 028	Report on architecture options to support multiple administrative domain
	GR NFV-SEC 011	Report on NFV LI Architecture
Rel3	GR NFV-IFA 022	Report on Management and Connectivity for Multi-Site Services
Rel3	GS NFV-SEC 014	Security Specification for MANO Components and Reference points
Rel2	GS NFV-IFA 027	Performance Measurements Specification
Rel3	GS NFV-IFA 031	Requirements and interfaces specification for management of NFV-MANO
Rel3	GS NFV-IFA 030	Multiple Administrative Domain Aspect Interfaces Specification
Rel2	GS NFV-SOL 004	VNF Package specification
Rel2	GS NFV-SOL 003	RESTful protocols specification for the Or-Vnfm Reference Point
Rel2	GS NFV-SOL 002	RESTful protocols specification for the Ve-Vnfm Reference Point
Rel2	GS NFV-SOL 001	NFV descriptors based on TOSCA specification
Rel3	GS NFV-TST 009	Specification of Networking Benchmarks and Measurement Methods for NFVI
Rel3	GR NFV-IFA 012	Report on Os-Ma-Nfvo reference point - application and service management use cases and recommendations
Rel3	GS NFV-EVE 011	Specification of the Classification of Cloud Native VNF implementations

Plus, quite many drafts being discussed (Phase 4), available at:
https://docbox.etsi.org/ISG/NFV/Open/Drafts/

Summary of release evolution

Release 1

- Focused on the feasibility of NFV
- Delivered the baseline studies and specifications
- Set the NFV Architecture:
  - Infrastructure,
  - Virtualized network functions (VNF),
  - Integration of the VNFs into Network Services (NS), and
  - NFV Management and Orchestration (NFVMANO) aspects at different layers

Release 2

- Focuses on interoperability of NFV solutions
- Details requirements and specification of interfaces and descriptors
- Realizes the interoperability of solutions based on the NFV Architecture, detailing
  - VNF and NS Descriptors,
  - Acceleration,
  - Internal and external NFV-MANO interfaces

Release 3

- Focuses on feature enriching the NFV Architectural Framework, readying NFV for deployment
- Features such as:
  - Charging and billing,
  - Licensing,
  - Policy framework,
  - Multi-site,
  - Cloud-native support,
  - Etc.
- Details new requirements and specification of interfaces and descriptors

From: https://docbox.etsi.org/Workshop/2017/20170406_ETSI_SUMMIT_5G_NWK_INFRASTRUCTURE/02_SESSION_B_BEYOND_TODAYS_NWK_SERV_MANAGEM/5G_INFRASTRUCTURE_ENABLER_ETSI_NFV_TRIAY.pdf

Definition

- NFV is one (*the?*) way to address these challenges by leveraging virtualization technologies
- Main idea: decoupling of physical network equipment from the functions that run on them
  - Capacity vs functionality
  - Network functions provided as plain software
    - Opportunity for new players

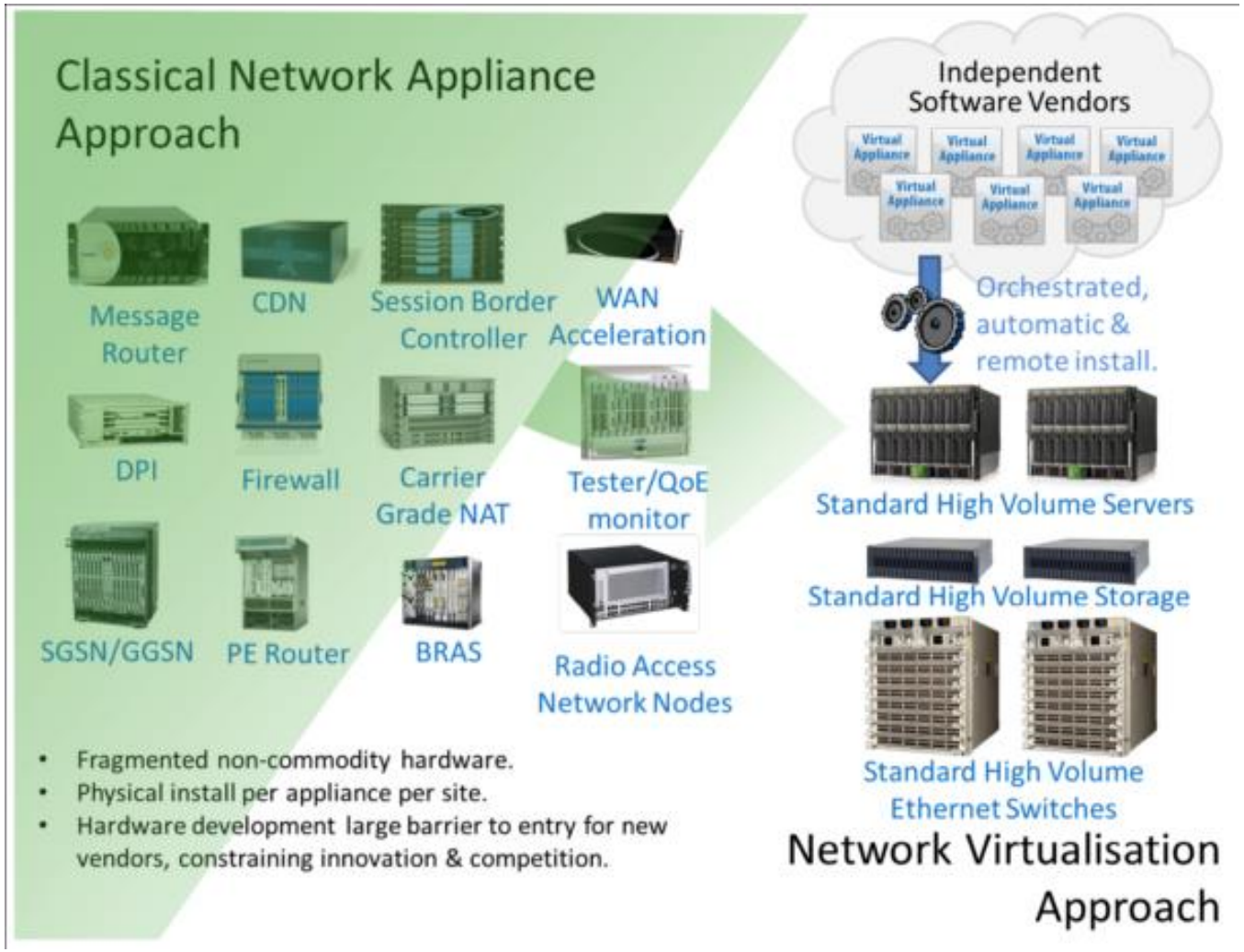
Definition

- According to the ETSI NFV ISG:

  “Network Functions Virtualisation aims to transform the way that network operators architect networks by evolving standard IT virtualisation technology to consolidate many network equipment types onto industry standard high volume servers, switches and storage, which could be located in Datacentres, Network Nodes and in the end user premises”

- A service can be decomposed into a set of Virtual Network Functions (VNFs)
  - VNFs may then be relocated and instantiated at different network locations, without requiring to buy and install new hardware

Definition



Source: ETSI NFV ISG – White Paper 1

Fields of Application and Use Cases

- NFV is applicable to any data plane packet processing and control plane function in mobile and fixed networks. Some examples:
  - Switching elements: BNG, CG-NAT, routers
  - Mobile network nodes: HLR/HSS, MME, SGSN, GGSN/PDN-GW, RNC, Node B, eNode B
  - Functions contained in home routers and set top boxes to create virtualized home environments
  - Tunneling gateway elements: IPsec/SSL VPN gateways
  - Traffic analysis: DPI, QoE measurement
  - Service Assurance, SLA monitoring, Test and Diagnostics
  - NGN signaling: IMS
  - Converged and network-wide functions: AAA servers, policy control and charging platforms
  - Application-level optimization: CDNs, Cache Servers, Load Balancers, Application Accelerators
  - Security functions: Firewalls, virus scanners, intrusion detection systems, spam protection

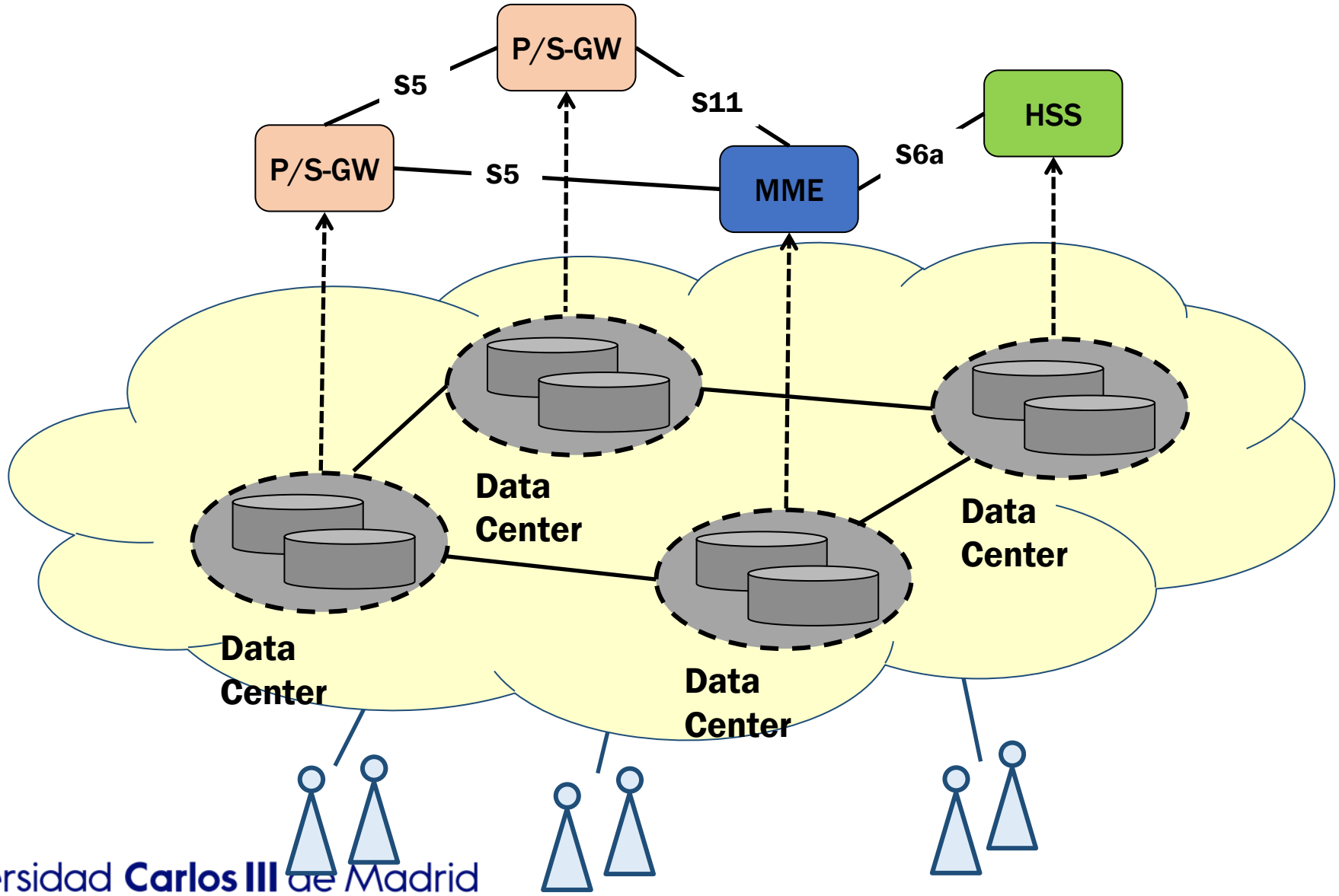
Fields of Application and Use Cases

- Many use cases considered. Some examples (proposed initially):
  - A software-based DPI, providing advanced traffic analysis and multi-dimensional reporting
    - Showing the possibility of making off-the-shelf hardware work at actual line rates
  - IP node implementations, supporting for example CG-NAT and BRAS capabilities on standard high-end servers
    - Offering the opportunity for an effective re-use of hardware as the demand for such capabilities evolves
  - The virtualization of services and capabilities that presently require dedicated hardware appliances on customer premises, including firewall, web security, etc
  - The virtualization of Content Distribution Networks (CDN)
    - Extending and scaling Content Delivery Services more easily
    - Maximizing hardware re-use in PoPs by being able to install other Service Delivery Applications (e.g. Web Acceleration) on demand
  - The virtualization of a mobile core network
    - More cost efficient production environment, better resource utilization, more flexible network management, hardware consolidation, easier multi-tenancy support and faster configuration of new services
  - …

One example of use case: vEPS

- Both the core (EPC) and the RAN can be mostly virtualized
- Motivation
  - Reduced Total Cost of Ownership (TCO)
  - Improved network usage efficiency
    - Due to flexible allocation of different NFs on the HW pool
  - Higher service availability and resiliency
    - Provided by dynamic network reconfiguration
  - Elasticity
    - Capacity dedicated to each NF can be dynamically modified according to actual load on the network, thus increasing scalability
  - Topology reconfiguration
    - Network topology can be dynamically reconfigured to optimize performance

One example of use case: vEPS



Benefits of NFV (I)

- Reduced equipment costs and reduced power consumption through consolidating equipment and exploiting the economies of scale of the IT industry
- Increased velocity of Time to Market by minimizing the typical network operator cycle of innovation
- Much more efficient test and integration
  - Production, test and reference facilities can be run on the same infrastructure
- Targeted service introduction based on geography or customer sets is possible
  - Services can be rapidly scaled up/down as required
  - Service velocity is improved by provisioning remotely in software without any site visits required

Benefits of NFV (II)

- Enabling a wide variety of eco-systems and encouraging openness
- Optimizing network configuration and/or topology in near real time based on the actual traffic/mobility patterns and service demand
- Supporting multi-tenancy thereby allowing network operators to provide tailored services and connectivity for multiple users, applications or internal systems or other network operators, all co-existing on the same hardware with appropriate secure separation of administrative domains
- Reduced energy consumption by exploiting power management features in standard servers and storage, as well as workload consolidation and location optimization
  - E.g., to concentrate the workload on a smaller number of servers during off-peak hours (e.g. overnight) so that all the other servers can be switched off

Benefits of NFV (III)

- Improved operational efficiency by taking advantage of the higher uniformity of the physical network platform and its homogeneity to other support platforms:
  - IT orchestration mechanisms provide automated installation, scaling-up and scaling-out of capacity, and re-use of Virtual Machine (VM) builds
  - Eliminating the need for application-specific hardware
  - Reduction in variety of equipment for planning & provisioning
  - Option to temporarily repair failures by automated re-configuration and moving network workloads onto spare capacity using IT orchestration mechanisms
  - The potential to gain more efficiency between IT and Network Operations
  - The potential to support in-service software upgrade (ISSU) with easy reversion by installing the new version of a Virtualized Network Appliance (VNA) as a new Virtual Machine (VM)

Challenges and Requirements for NFV (I)

- Portability/Interoperability
  - define a unified interface which clearly decouples the software instances from the underlying hardware
- Performance Trade-Off
  - keep the performance degradation as small as possible by using appropriate hypervisors and modern software technologies
- Migration and co-existence of legacy & compatibility with existing platforms
  - NFV must work in a hybrid network composed of classical physical network appliances and virtual network appliances
- Management and Orchestration
  - A consistent management and orchestration architecture is required → reducing cost and time to integrate VNFs

Challenges and Requirements for NFV (II)

- Automation
  - NFV will only scale if all of the functions can be automated
- Security & Resilience
  - The security, resilience and availability of networks must not be impaired
  - NFV should aim at improving network resilience and availability
- Integration
  - “mix & match” servers, hypervisors and virtual appliances from different vendors without incurring significant integration costs and avoiding lock-in

Challenges and Requirements for NFV (III)

- Network Stability
  - The stability of the network should not be impacted when managing and orchestrating a large number of virtual appliances between different hardware vendors and hypervisors
- Simplicity
  - Virtualized network platforms should be simpler to operate than those that exist today
  - Avoid trading the set of operational headaches existing today for a different but equally intractable set of operational headaches

Enablers for NFV (I)

- NFV leverages modern technologies such as those developed for cloud computing
  - Virtualization mechanisms
    - Hardware virtualization by means of hypervisors
    - Virtual Ethernet switches for connecting traffic between virtual machines and physical interfaces
    - High-performance packet processing through high-speed multi-core CPUs with high I/O bandwidth
    - Smart Ethernet NICs for load sharing and TCP Offloading, and routing packets directly to Virtual Machine memory
    - Poll-mode Ethernet drivers (rather than interrupt driven, for example Linux NAPI and Intel's DPDK)
  - Orchestration and management mechanisms
    - Enhance resource availability and usage (e.g., automatic instantiation of virtual appliances in the network)

Enablers for NFV (II)

- Availability of open APIs for management and data plane control, like OpenFlow, OpenStack, OpenNaaS
  - Provide an additional degree of integration of Network Functions Virtualization and cloud infrastructure
- The use of industry standard high volume servers is a key element in the economic case for NFV
  - NFV leverages the economies of scale of the IT industry. An industry standard high volume server is a server built using standardized IT components (e.g., x86 architecture)
    - There is a competitive supply of the subcomponents which are interchangeable inside the server
    - Application Specific Integrated Circuits (ASICs) will become increasingly uncompetitive against general purpose processors

NFV architecture

NFV vs current practice

- In current networks: Network Functions (NFs) are implemented as a combination of vendor specific software and hardware
- NFV introduces a number of differences:
  - Decoupling software from hardware
    - HW and SW can evolve independently
  - Flexible network function deployment
    - Sharing resources is much easier
    - Faster deployment of new services
  - Dynamic scaling
    - Greater flexibility, scaling can be done for example according to actual traffic

- Decoupling NFs from dedicated HW does not require *virtualization of resources*, but note the gains of doing so

“The” NFV architecture

- Widely embraced architecture defined by ETSI
  - Introduced in ETSI GS NFV 002
- Goals of the ETSI NFV architectural framework
  - Outline an architecture that supports VNF operation across different hypervisors and computing resources and which provides access to shared storage, computation, and physical/virtual networking
  - Outline a software architecture with VNFs as building blocks to construct VNF Forwarding Graphs
  - Define an interface between management and orchestration of NFV with other management systems, such as EMS, NMS, and OSS/BSS
  - Support a range of network services with different reliability and availability levels leveraging virtualization techniques

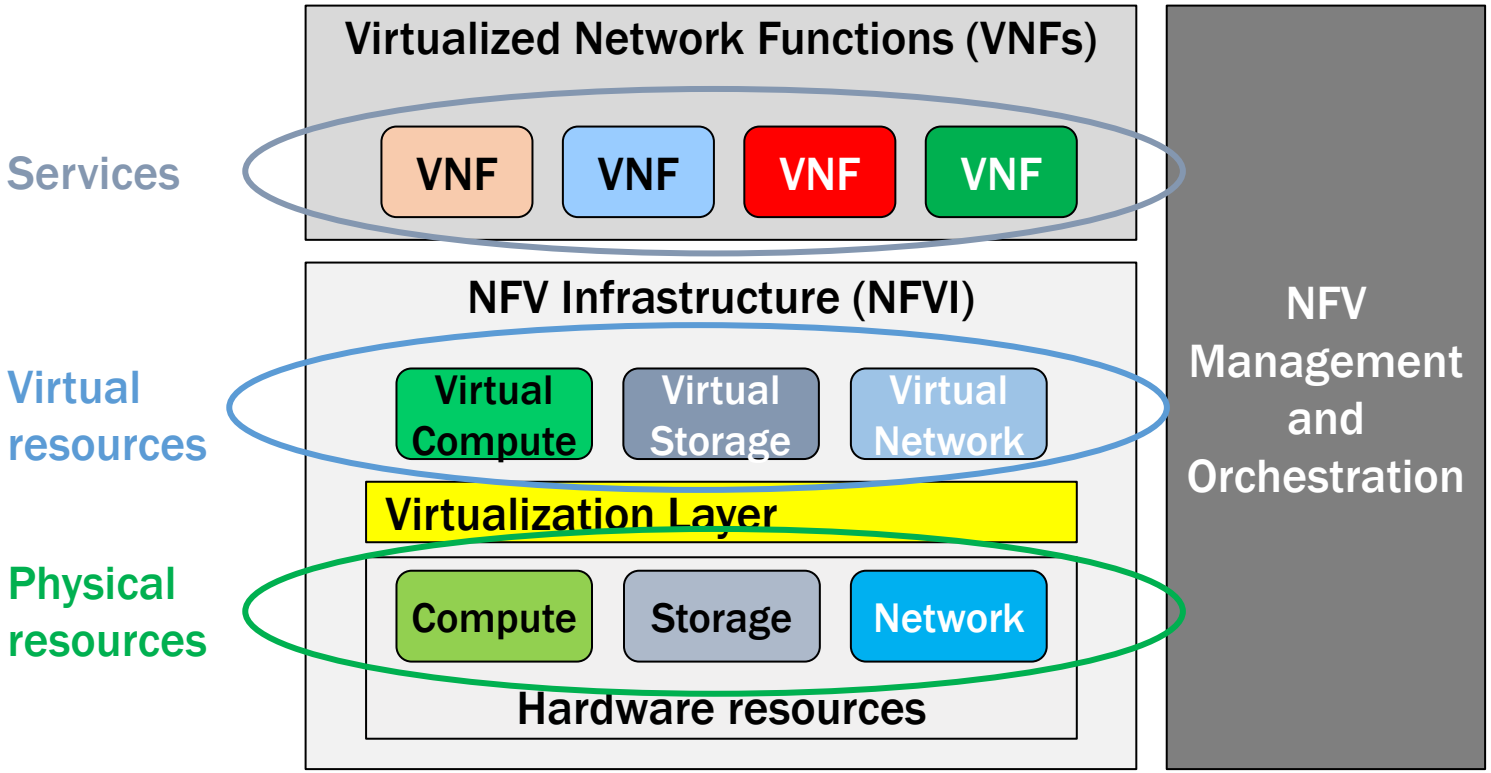
“The” NFV architecture

- Goals of the ETSI NFV architectural framework (cont’d)
  - Ensure the virtualization does not cause any new security threat
  - Address performance related issues unique to virtualization
  - Minimize the interworking impact between virtualized and non-virtualized network functions
- Aspects common to Physical and Virtualized Network Functions are *left out of the scope*
  - The specifics of the Network Functions themselves, their interface protocols, as well as management functions related to the functionality performed by the NF
  - Direct control, operation and management of physical network infrastructure
  - The actual packet flow, control, operation and management of the E2E network service
  - Implementation details of the architecture itself

High-level NFV framework

- Composed of 3 key elements / domains
  - Virtualized Network Function (VNF)
    - Software implementation of a network function which is capable of running over the NFVI
  - NFV Infrastructure (NFVI)
    - NFVI supports the execution of the VNF
    - Includes the diversity of physical resources and how these can be virtualized
  - NFV Management and Orchestration (MANO)
    - Covers the orchestration and lifecycle management of physical and/or software resources that support the infrastructure virtualization, and the lifecycle management of VNFs

High-level NFV framework



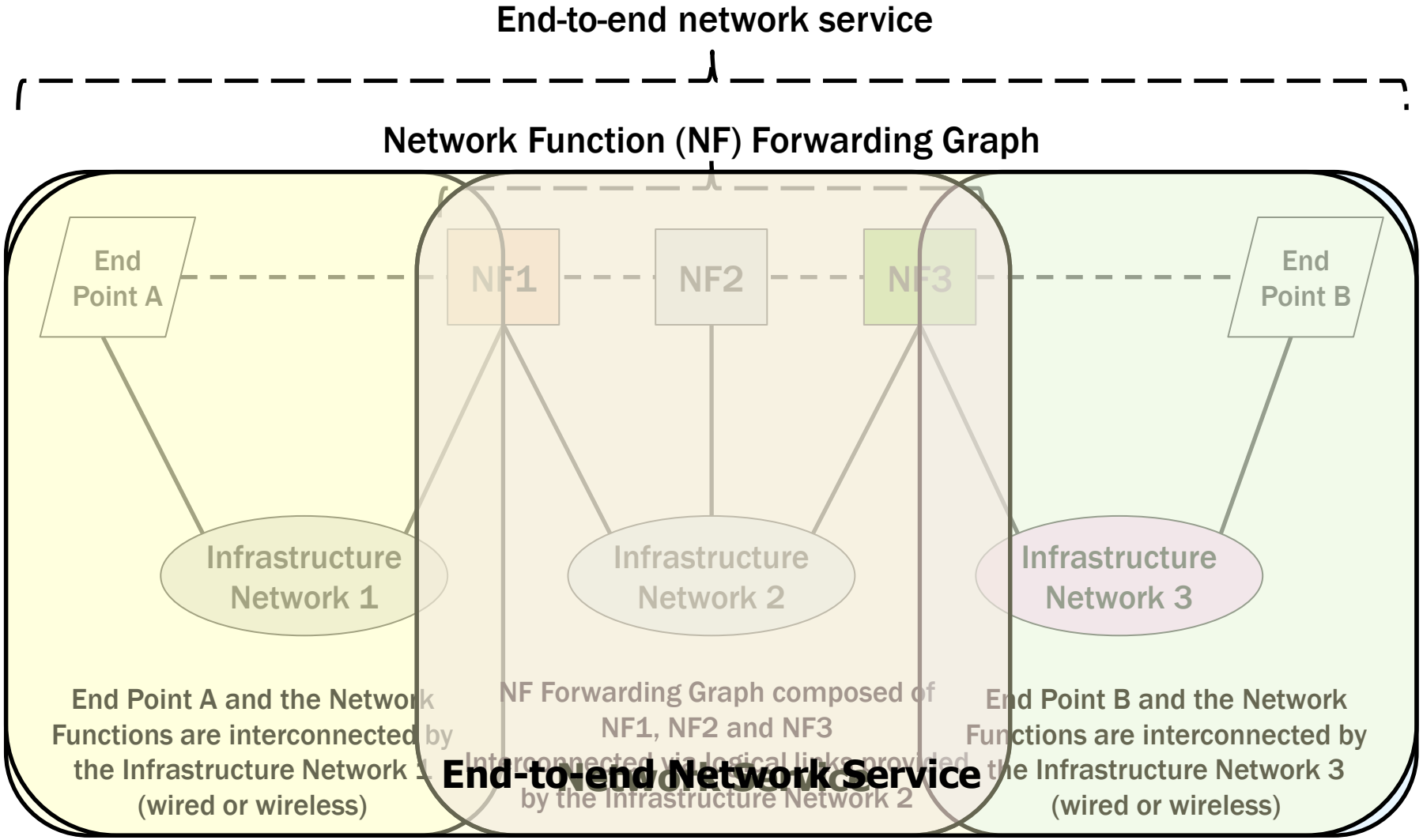
Network Services

- An end-to-end network service can be described by an NF Forwarding Graph of interconnected Network Functions (NFs) and end points
  - These network functions can be implemented in a single operator network or interwork between different operator networks
    - Some architectural options reported in GS NFV-IFA 009
  - The underlying network function behavior contributes to the behavior of the higher-level service
    - Network service behavior: combination of the behavior of its functional blocks (individual NFs, NF Sets, NF Forwarding Graphs, and/or the infrastructure network)

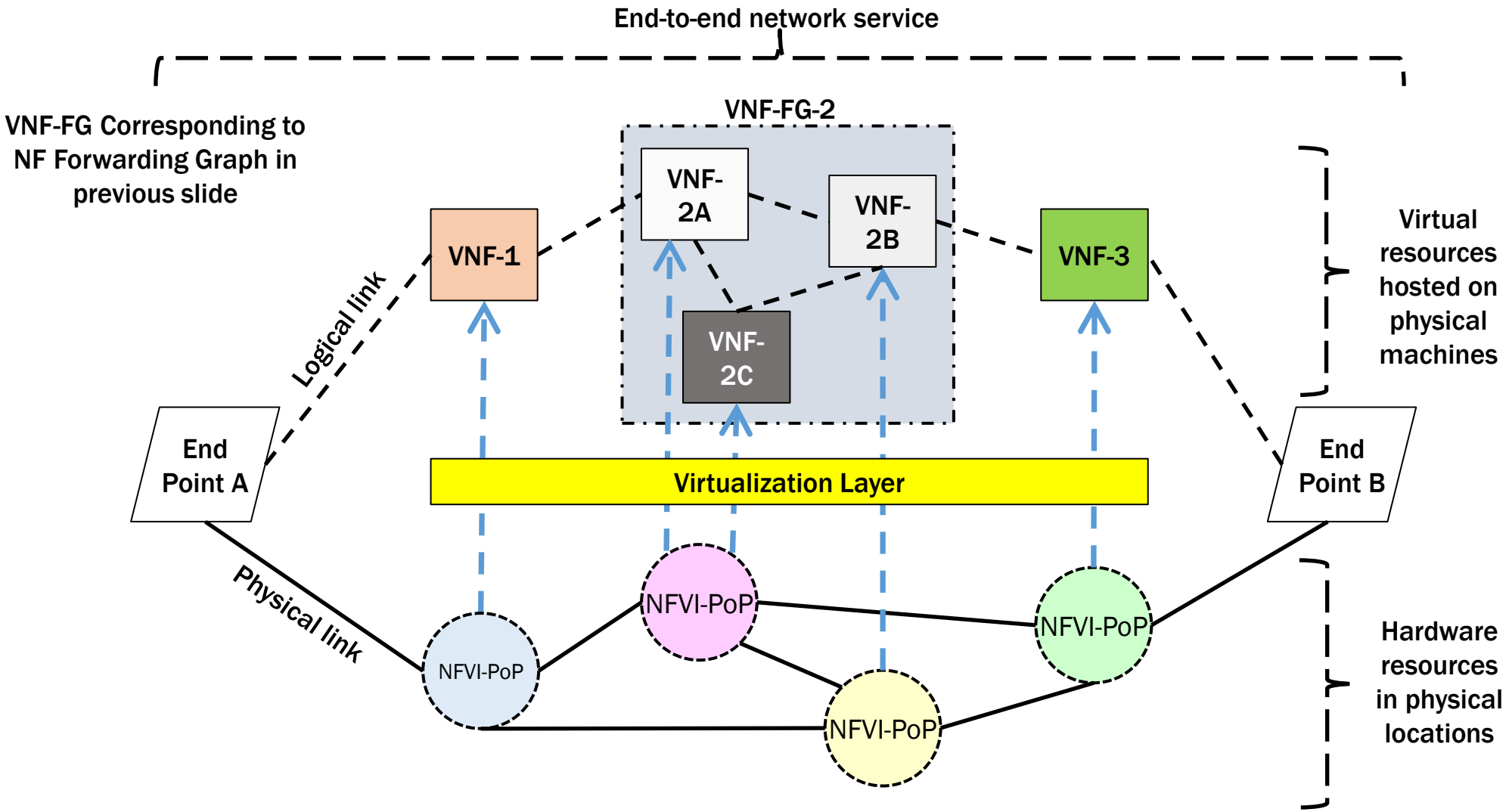
Network Services

- The end points and the network functions of the network service are represented as nodes
  - These nodes correspond to devices, applications, and/or physical server applications
- An NF Forwarding Graph can have network function nodes connected by logical links
  - Example: chain of network functions
  - NFV area of activity within the operator-owned resources
    - Customer-owned devices are out of the scope
    - But virtualization and network-hosting of customer functions is possible and is in the scope of NFV

Network Services



Network Services in NFV



NFV Principles

- VNFs are the building blocks used to create end-to-end network services
- Three key NFV principles are involved in creating practical network services:
  - Service chaining
    - VNFs are modular and each VNF provides limited functionality on its own
    - For a given traffic flow within a given application, the service provider steers the flow through multiple VNFs to achieve the desired network functionality
  - Management and orchestration (MANO)
    - Deploying and managing the lifecycle of VNF instances
      - Examples: VNF instance creation, VNF service chaining, monitoring, relocation, shutdown, and billing
    - MANO also manages the NFV infrastructure elements
  - Distributed architecture
    - A VNF may be made up of one or more VNF components (VNFC)
      - Each VNFC implements a subset of the VNF's functionality
      - Each VNFC may be deployed in one or multiple instances. These instances may be deployed on separate, distributed hosts to provide scalability and redundancy

Implications of NFV

- The NFV architectural framework addresses the following:
  - The functionality that is required to be realized by the NFVI — NFVI
  - The functionality that is required due to decoupling network functions into software and hardware — VNF
  - The functionality that is required for NFV-specific management and orchestration — MANO
- Let's look more closely at the NFV architecture

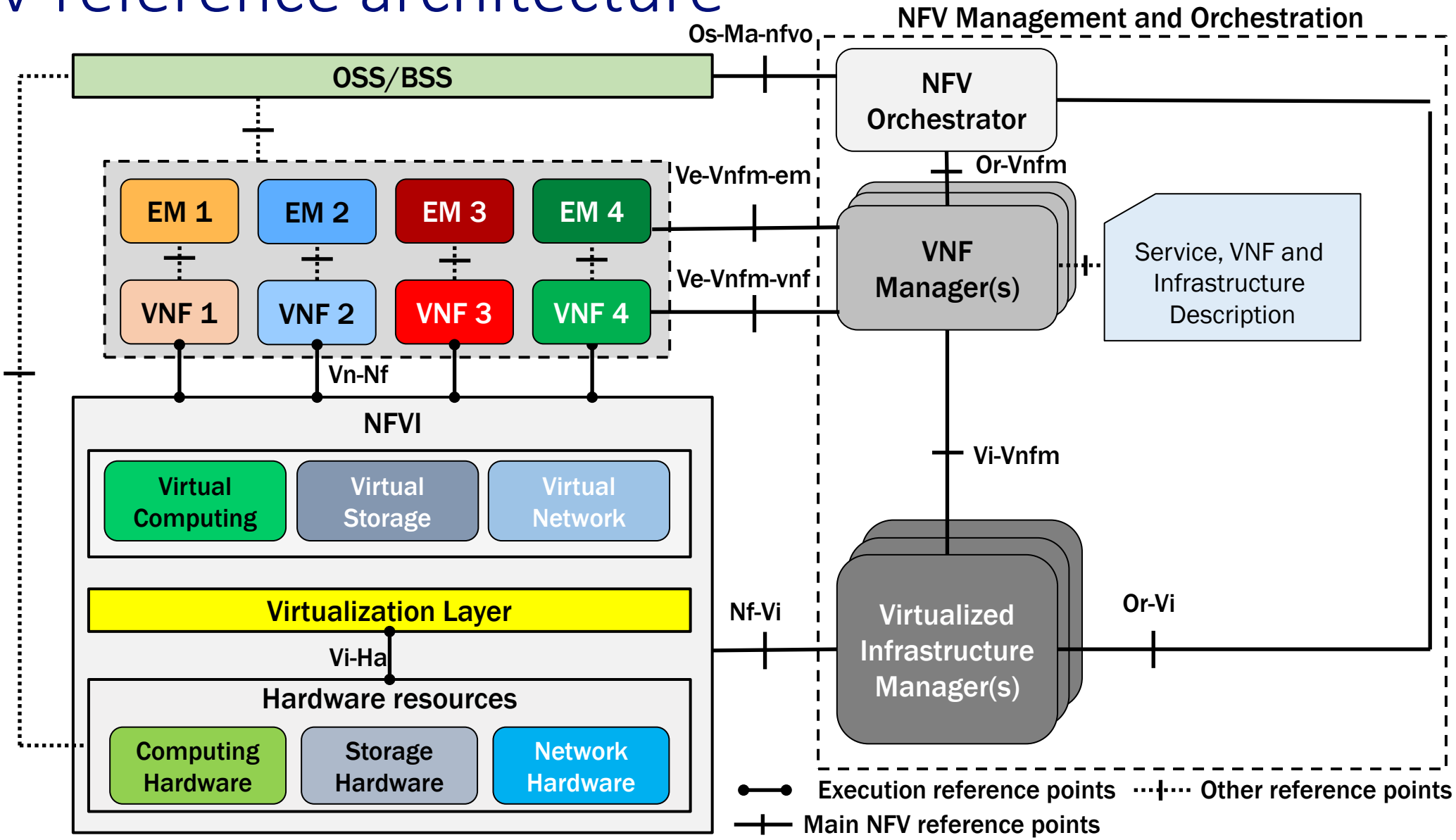
NFV terminology (I)

Term	Definition
Compute domain	Domain within the NFVI that includes servers and storage
Infrastructure network domain	Domain within the NFVI that includes all networking that interconnects compute/storage infrastructure
Network Function (NF)	Functional block within a network infrastructure that has well-defined external interfaces and well-defined functional behavior. Typically, a network node or physical appliance
Network Functions Virtualization (NFV)	Principle of separating network functions from the hardware they run on by using virtual hardware abstraction
Network Functions Virtualization Infrastructure (NFVI):	The totality of all hardware and software components that build up the environment in which VNFs are deployed. The NFV-Infrastructure can span across several locations. The network providing connectivity between these locations is regarded to be part of the NFVI
NFVI-Node	Physical device[s] deployed and managed as a single entity, providing the NFVI Functions required to support the execution environment for VNFs
NFVI-PoP	N-PoP where a Network Function is or could be deployed as Virtual Network Function (VNF)
Network forwarding path	Ordered list of connection points forming a chain of NFs, along with policies associated to the list
Network Point of Presence (N-PoP)	Location where a Network Function is implemented as either a Physical Network Function (PNF) or a Virtual Network Function (VNF)

NFV terminology (II)

Term	Definition
Network service	Composition of Network Functions and defined by its functional and behavioral specification
Physical Network Function (PNF)	An implementation of a NF via a tightly coupled software and hardware system. This is typically a proprietary system
Virtual Machine (VM)	A virtualized computation environment that behaves very much like a physical computer/server
Virtual network	A topological component used to affect routing of specific characteristic information. The virtual network is bounded by its set of permissible network interfaces. In the NFV architecture, a virtual network routes information among the network interfaces of VM instances and physical network interfaces, providing the necessary connectivity
Virtualized Network Function (VNF)	An implementation of an NF that can be deployed on a NFVI
VNF Forwarding Graph (VNF FG)	Graph of logical links connecting VNF nodes for the purpose of describing traffic flow between these network functions
VNF Set	Collection of VNFs with unspecified connectivity between them

NFV reference architecture



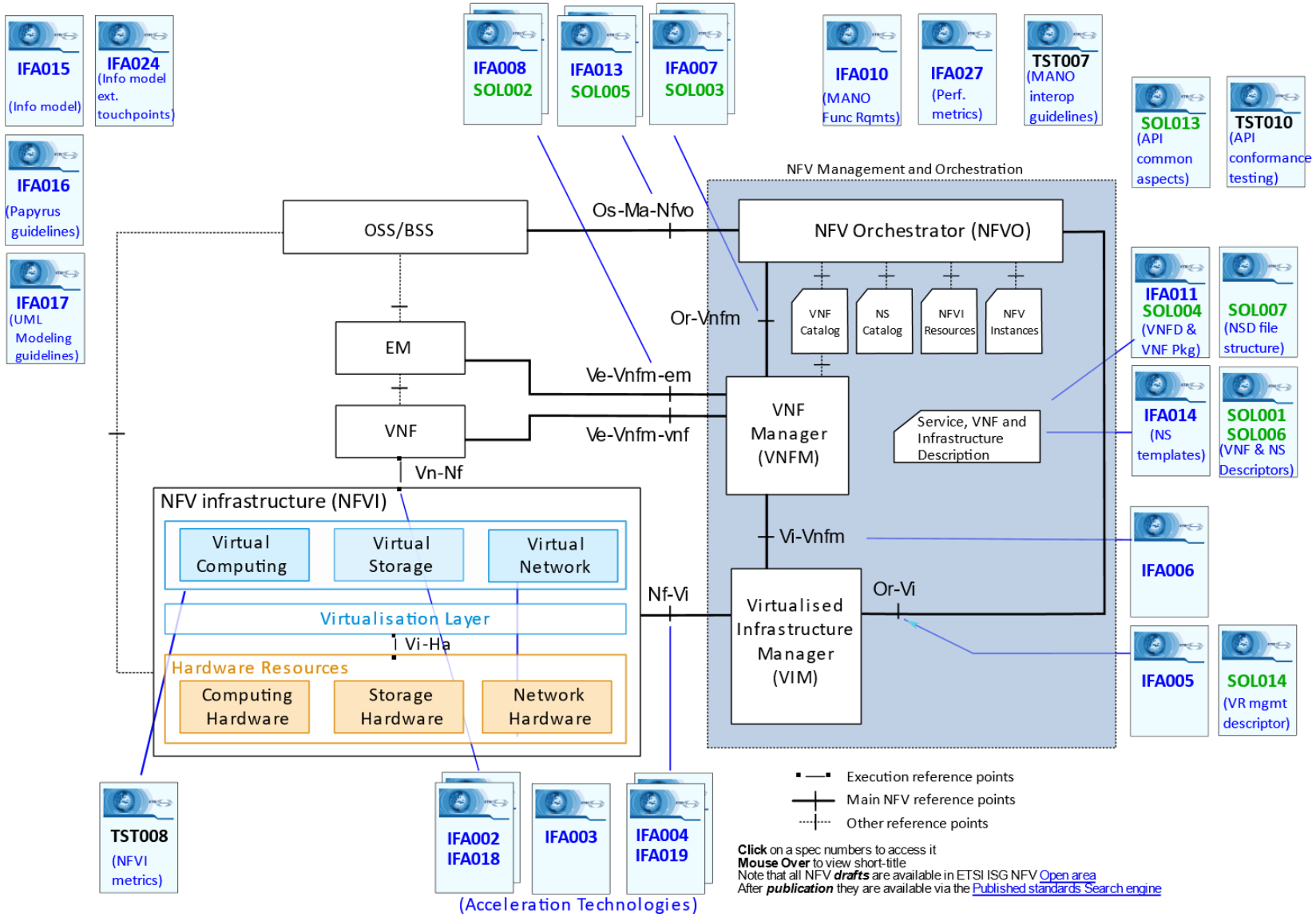
NFV reference architecture

- NFV infrastructure (NFVI)
  - HW and SW resources that create the environment in which VNFs are deployed
  - NFVI virtualizes physical computing, storage, and networking and places them into resource pools
- VNF/EM
  - Collection of VNFs implemented in SW to run on virtual computing, storage, and networking resources, and
  - Collection of element management systems (EMS) that manage the VNFs
- NFV management and orchestration (NFV-MANO)
  - Framework for the management and orchestration of all resources in the NFV environment (computing, networking, storage, and VM resources)
- OSS/BSS
  - Operational and business support systems implemented by the VNF service provider

NFV reference architecture

- The NFV Management and Orchestration (MANO) includes the following functional blocks:
- NFV orchestrator (NFVO)
  - Responsible for installing and configuring new network services (NS) and virtual network function (VNF) packages, NS lifecycle management, global resource management, and validation and authorization of NFVI resource requests
- VNF manager (VNFM)
  - Oversees lifecycle management (e.g. instantiation, update, query, scaling, termination) of VNF instances
- Virtualized infrastructure manager (VIM)
  - Controls and manages the interaction of a VNF with computing, storage, and network resources under its authority, in addition to their virtualization

NFV reference architecture: reference points



Source: ETSI NFV ISG webpage

NFVI

- The NFVI is the combination of both HW and SW components which build up the environment in which VNFs are deployed, managed and executed
  - Can span across several locations
    - Where NFVI-PoPs are operated
  - The network providing connectivity between these locations is considered part of the NFVI
- From VNF perspective, the virtualization layer and the HW resources are a single entity providing the desired virtualized resources

NFVI: HW resources

- Physical resources include computing HW, storage and network (nodes and links)
  - Computing HW assumed to be commercial-of-the-shelf (COTS)
  - Storage resources can be shared network attached storage (NAS) or storage that resides on the server itself
  - Network resources. 2 types of networks
    - NFVI-PoP network
      - Interconnecting the computing and storage resources contained in an NFVI-PoP
      - Also includes specific switching and routing devices to allow external connectivity
    - Transport network
      - Interconnecting NFVI-PoPs, NFVI-PoPs to other networks owned by the same or different network operator, and NFVI-PoPs to other network appliances or terminals not contained within the NFVI-PoPs

NFVI: Virtualization layer and Virtualized resources

- Virtual resources are abstractions of the computing, storage and network resources
  - Abstraction achieved using the Virtualization layer
    - Decouples the VNF software from the underlying hardware, thus ensuring a hardware independent lifecycle for the VNFs
  - Hypervisors and VMs for computing and storage resources
- The virtualization layer is responsible of
  - Abstracting and logically partitioning physical resources
  - Enabling the software that implements the VNF to use the underlying virtualized infrastructure
  - Providing virtualized resources to the VNF, so that the latter can be executed
- A VNF is envisioned to be deployed in one or several VMs
  - ETSI GS NFV-EVE 004 discusses other virtualization technologies

NFVI: Virtualization layer and Virtualized resources

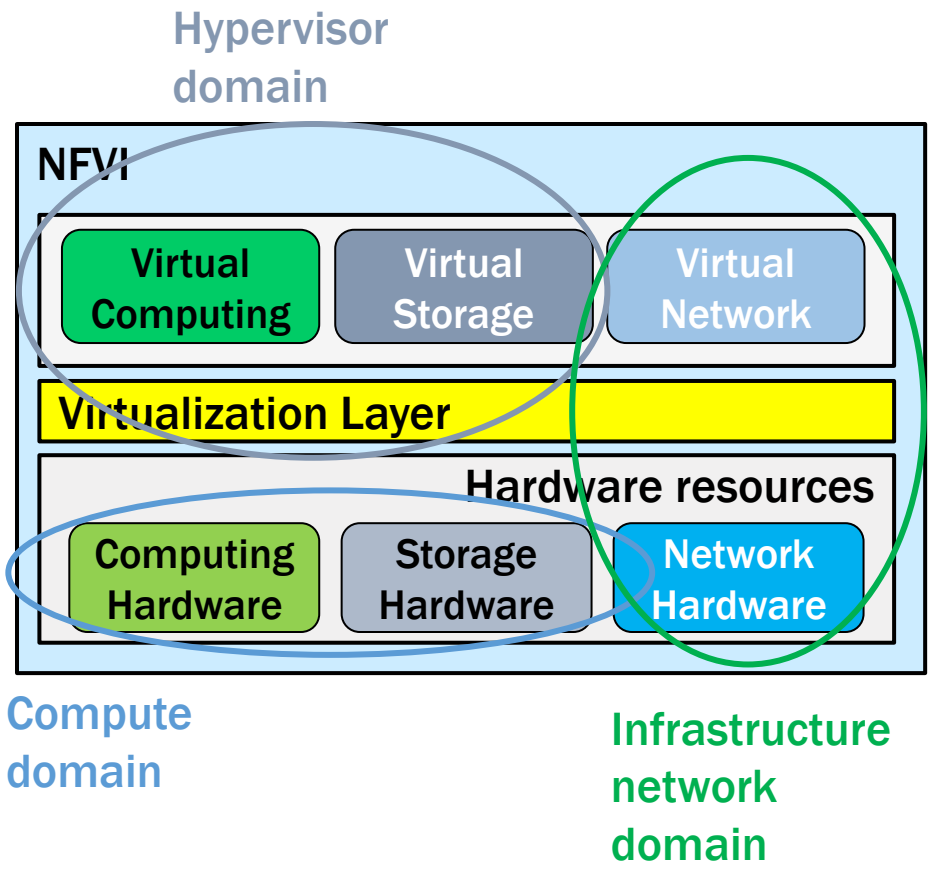
- Not restricted to any specific virtualization layer solution
  - E.g., In some cases VMs may have direct access to hardware resources (e.g., network interface cards) for better performance
- Hypervisors is one of the present typical solutions for the deployment of VNFs, but not the only possible one
  - VNF operation should be independent of its deployment scenario
- Network HW is abstracted by the virtualization layer to realize virtualized network paths that provide connectivity between VMs of a VNF and/or between different VNFs
  - Several techniques can be used, e.g., virtual networks and network overlays, such as VLAN, VxLAN, NVGRE, etc.
  - Also considered approaches that centralize the control plane of the transport network and separating it from the forwarding plane, such as SDN

Virtualization Layering and NFVI Support

- The primary tools to realize the virtualization layer are the hypervisors
  - The NFV architectural framework should accommodate a diverse range of hypervisors
- The primary means of VNF deployment is instantiating it in one or more VMs
  - The virtualization layer should provide open and standard interfaces
  - Independence of HW resources and portability
  - Performance and cost efficiency are also important

NFVI: domains

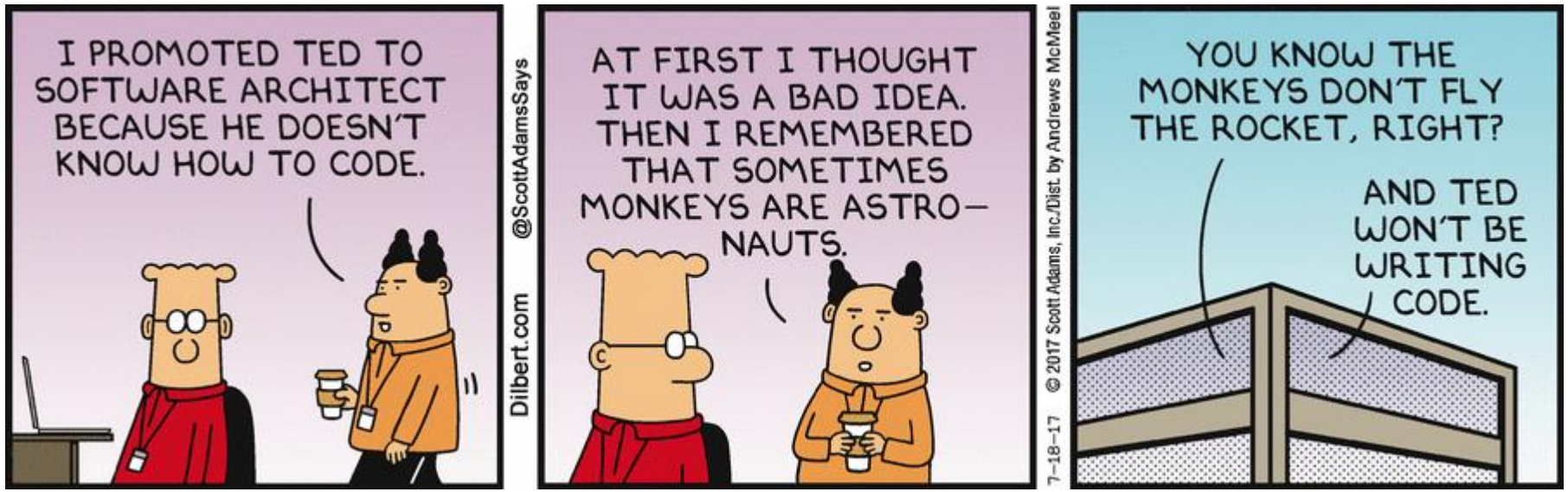
- The NFVI encompasses 3 domains
  - Compute domain
    - Provides commercial off-the-shelf (COTS) high-volume servers and storage
  - Hypervisor domain
    - Mediates the resources of the compute domain to the VMs of the software appliances, providing an abstraction of the hardware
  - Infrastructure network domain
    - Comprises all the generic high volume switches interconnected into a network that can be configured to supply infrastructure network services



NFV MANO

- The MANO
  - Provides the functionality required for the provisioning of the VNFs, and related operations
    - the configuration of the VNFs, and
    - the configuration of the infrastructure the VNFs run on
  - Includes orchestration and lifetime management of physical and/or software resources supporting the infrastructure virtualization and the lifecycle management of VNFs
  - Includes databases used to store information and data models defining deployment and lifecycle properties of functions, services and resources
  - Defines interfaces used for communications between components of the MANO, as well as coordination with traditional network management, such as OSS/BSS

VNF (software) architecture



VNF in the NFV architecture
NFV software architecture

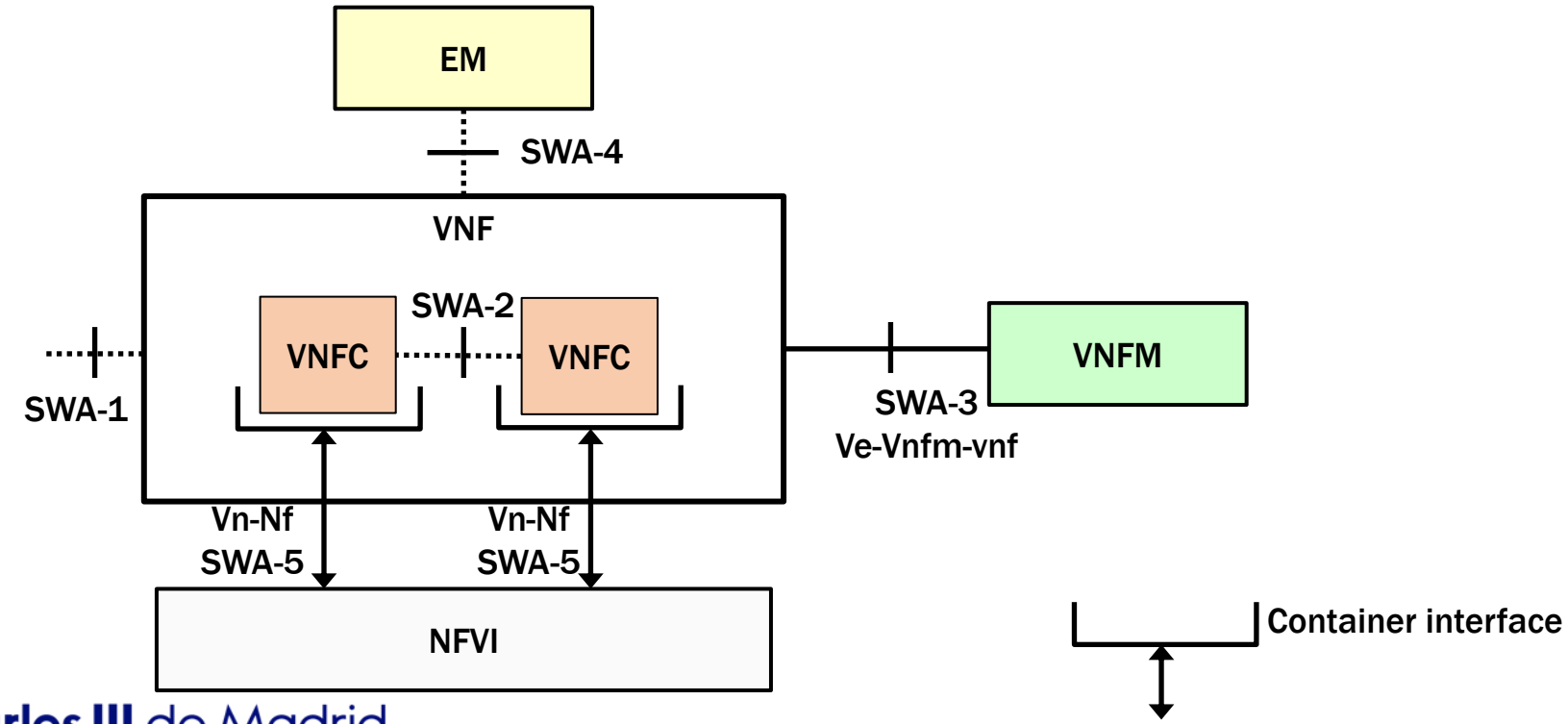
- Let's talk about virtualizing network functions
  - We know already some of the concepts behind NFV
  - But, when it's time to design a network service composed of VNFs, how do we do it?
    - What is the NFV software architecture?
      - Software architectures describe the functionality of software systems from the viewpoints of various stakeholders
      - In NFV: Service Provider, Network Operator, and Manufacturer
    - Some aspects have to be considered/covered
      - Function and interfaces with the NFV architecture
      - Support of MANO and NFVI requirements
      - Best practices for NFV design

ETSI GS NFV-SWA 001: "Virtual Network Functions Architecture"

VNF in the NFV architecture

VNF architecture

- A VNF is a Network Function capable of running on an NFVI and being orchestrated by a NFVO and VNFM
  - It has well-defined interfaces to other NFs via SWA1, the VNFM, its EM, and the NFVI and a well-defined functional behavior



VNF in the NFV architecture

VNF architecture

- A VNF may implement a single network entity (NE) while another VNF may implement groups of network entities
  - Interfaces and behavior of the NE is defined by standardization organizations (e.g., 3GPP or IETF)
- VNF Providers
  - Structure the software providing the VNF into software components (*implementation* view)
    - Called VNF Components (VNFCs)

Discussion: how does a VNF provider structure a VNF?

  - Package those components into one or more images (*deployment* view)
- VNFs are implemented with one or more VNFCs

VNF in the NFV architecture
VNF architecture

- Putting together all the relevant terms…
  - VNF: abstract entity that allows the software contract to be defined
  - VNF Instance: runtime instantiation of the VNF
  - VNFC: VNF Provider's specific component of a VNF
  - VNFC Instances (VNFCIs): executing constituents which make up a VNF Instance

  - Virtualisation Deployment Unit (VDU): it is a construct supporting the description of the deployment and operational behaviour of a VNFC
    - A VNFC instance created based on the VDU maps to a single virtualisation container (e.g. a VM)

VNF in the NFV architecture
VNF architecture

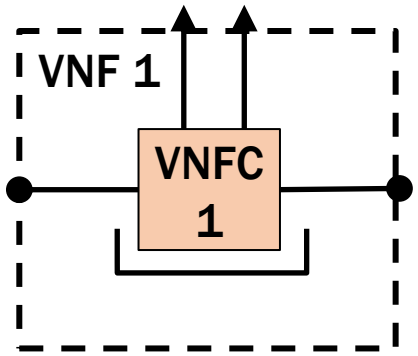
- How is a network function defined by a VNF instantiated?
  - VNF Manager create one or more VNFCIs
    - Each VNFCI is in its own virtualization container
    - These VNFCIs provide the functionality of the VNF, and expose whatever interfaces are provided by that VNF
  - The requirements for initial deployment state are described in the VNF Descriptor (VNFD)
    - including the connections between VNFCIs internal to the VNF (not visible to external entities at the VNF level)
    - Post-deployment operation capabilities (e.g., migration of the VMs containing VNFCIs, scale up/down/in/out, etc.) also described in the VNFD
    - Each VNF has exactly one associated VNFD

VNF Design Patterns

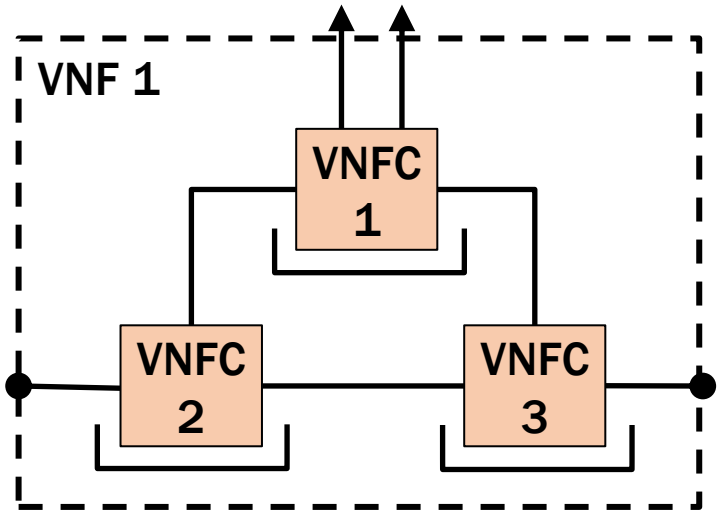
- We will go through common patterns in VNF design and operations
  - Goal is capturing practically relevant points in the design space, from which requirements on the VNFD, the NFVO and the NFVI can be derived

VNF Design Patterns:
VNF Internal Structure

- VNF = 1 or more VNFC
  - A VNFC is a software entity deployed in a virtualization container
  - VNFCs of a VNF are connected in a graph
- The same VNF may be realized differently by each VNF Provider



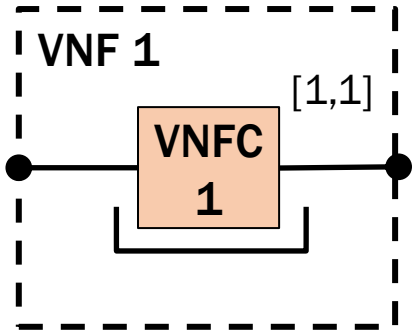
VNF with single component



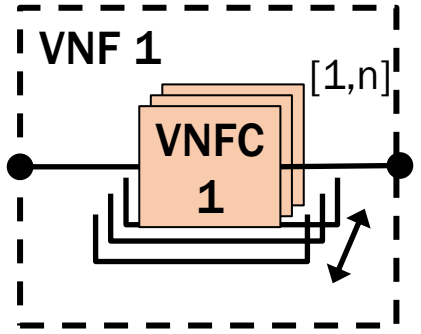
VNF with multiple components

VNF Design Patterns:
VNF Instantiation

- Each VNFC of a VNF is either parallelizable or non-parallelizable
  - If parallelizable, it may be instantiated multiple times per VNF Instance, but there may be a constraint on the minimum and maximum number of parallel instances
  - If non-parallelizable, it shall be instantiated exactly once per VNF Instance



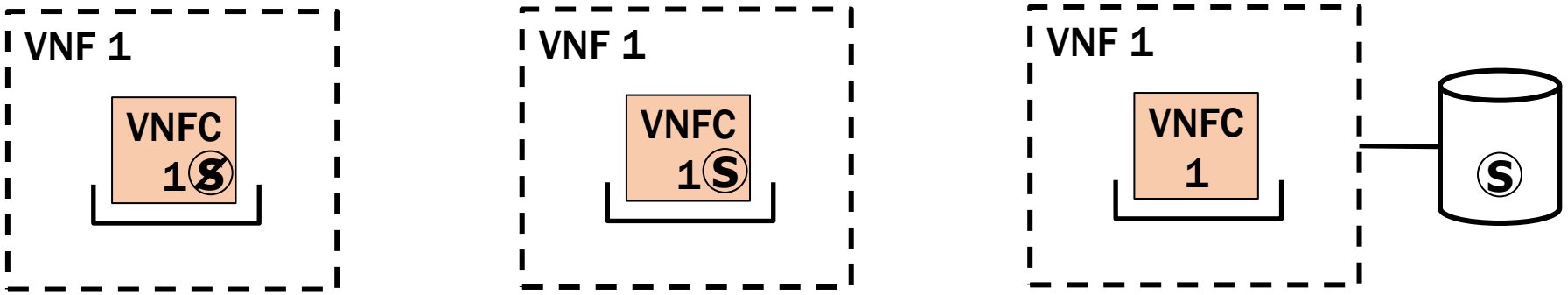
non-parallelizable VNFC



Parallelizable VNFC
(min. and max. # of instances)

VNF Design Patterns: VNF States

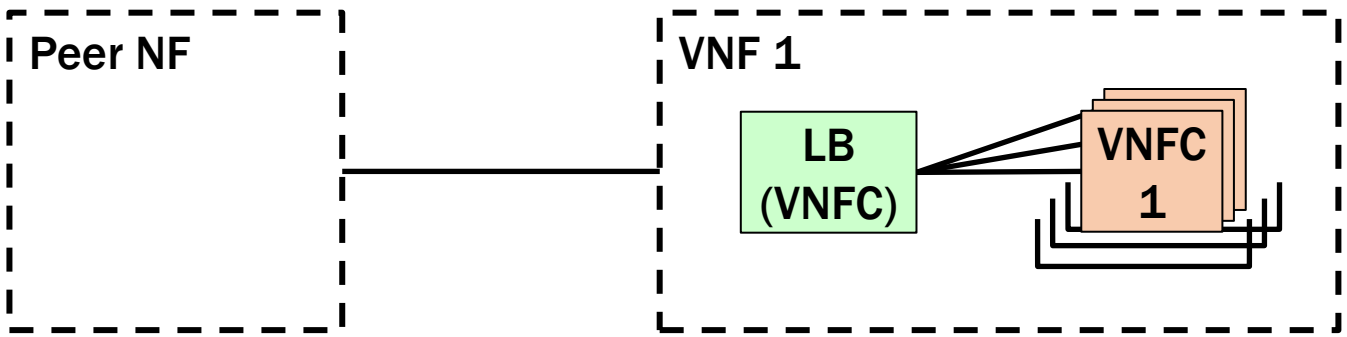
- Each VNFC of a VNF may need to handle state information
  - A VNFC that does not have to handle state information is a stateless VNFC
  - A VNFC that needs to handle state information may be implemented either as a stateful VNFC or as a stateless VNFC with external state (state data is held in a data repository external to the VNFC)



stateless VNFC | stateful VNFC | VNFC w/ external state

VNF Design Patterns:
VNF Load Balancing Models

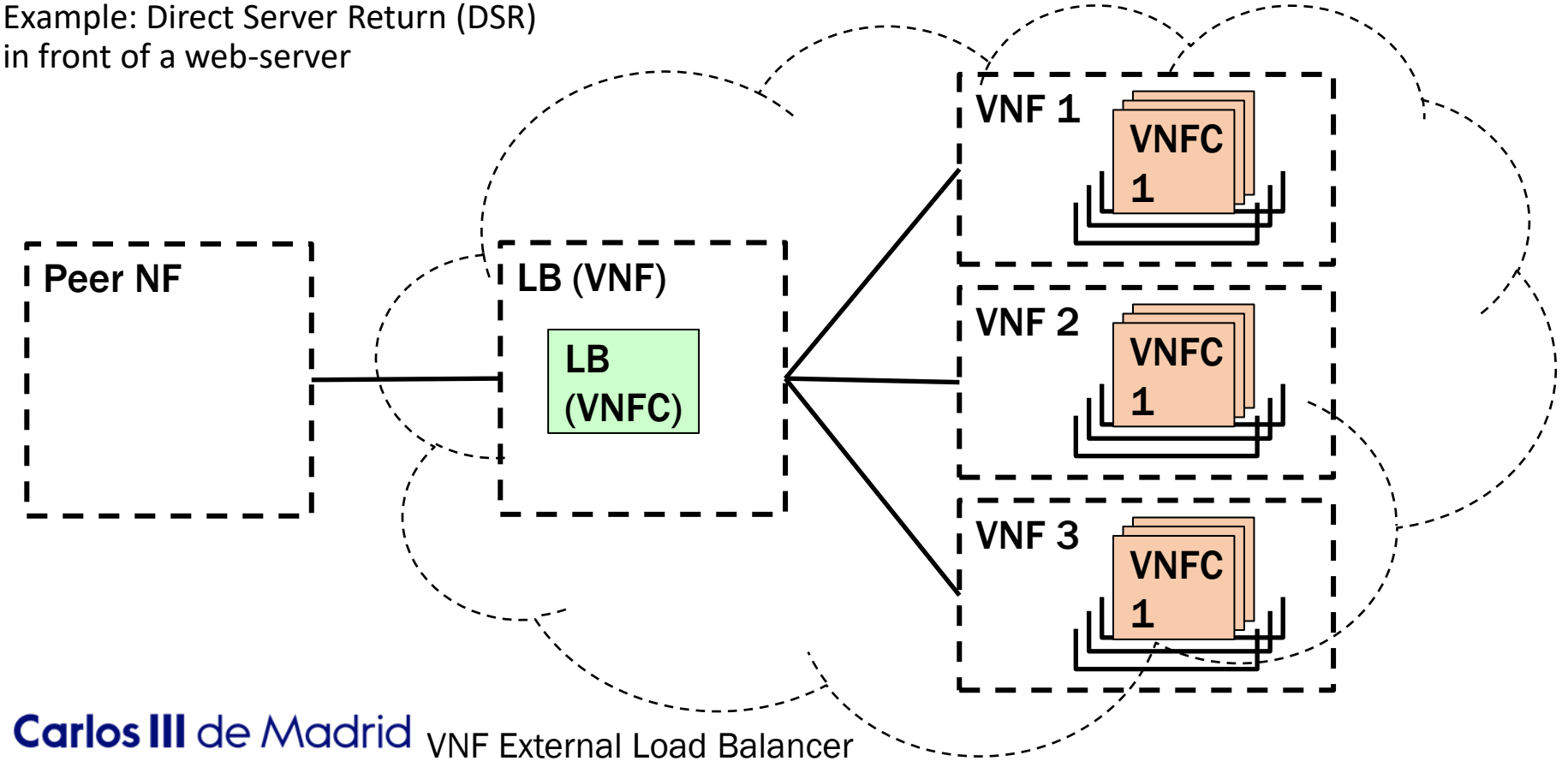
- 4 main models identified
  - VNF-internal Load Balancer
    - 1 VNF instance seen as 1 logical NF by a Peer NF
    - The VNF has at least one VNFC that can be replicated and an internal load balancer (which is also a VNFC)
      - The VNFM instantiates the LB
    - Examples: VNF Provider specific implementation of a scalable NF



VNF Internal Load Balancer

VNF Design Patterns:
VNF Load Balancing Models

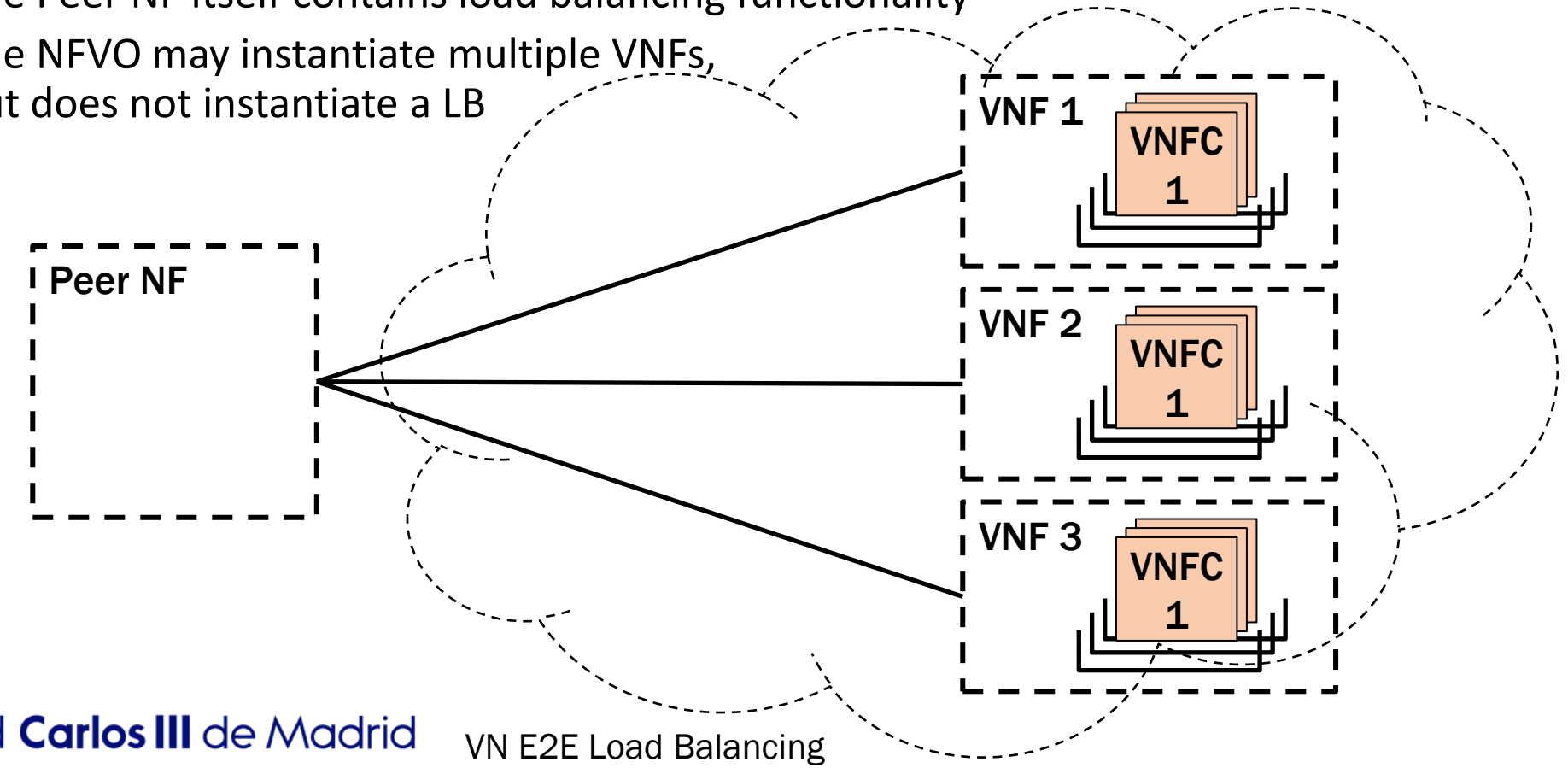
- VNF-external Load Balancer
  - N VNF Instances seen as 1 logical NF by a Peer NF
    - VNFs may be of different VNF Providers, e.g. to increase resilience
  - There is a load balancer external to the VNF (which may be a VNF itself)
    - The NFVO may instantiate the VNF multiple times and add a LB (V)NF
  - Example: Direct Server Return (DSR) in front of a web-server



VNF External Load Balancer

VNF Design Patterns:
VNF Load Balancing Models

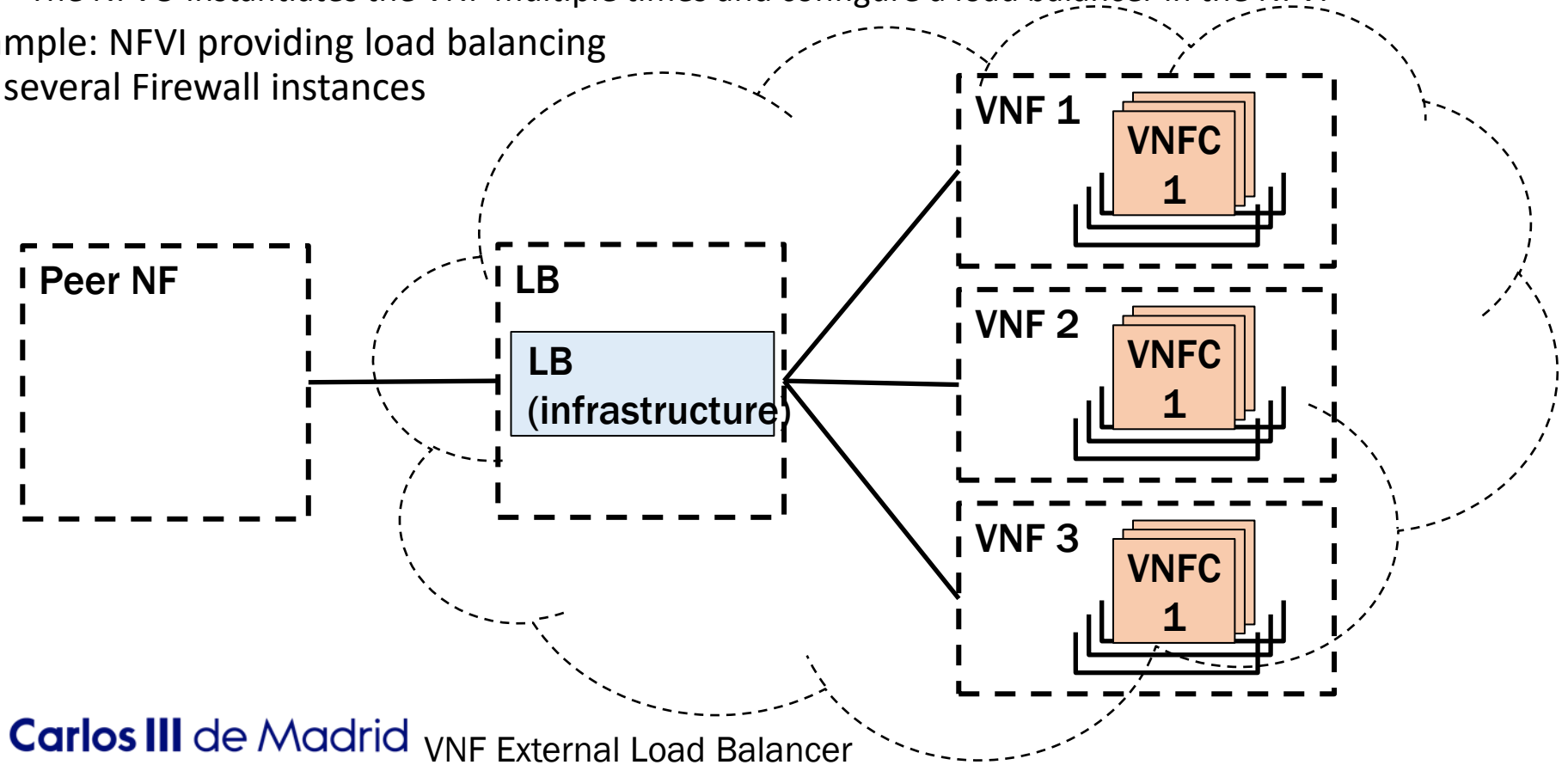
- End-to-End Load Balancing
  - N VNF instances seen as N logical NFs by a Peer NF
    - VNFs may be of different VNF Providers, e.g. to increase resilience
  - The Peer NF itself contains load balancing functionality
  - The NFVO may instantiate multiple VNFs, but does not instantiate a LB



VN E2E Load Balancing

VNF Design Patterns:
VNF Load Balancing Models

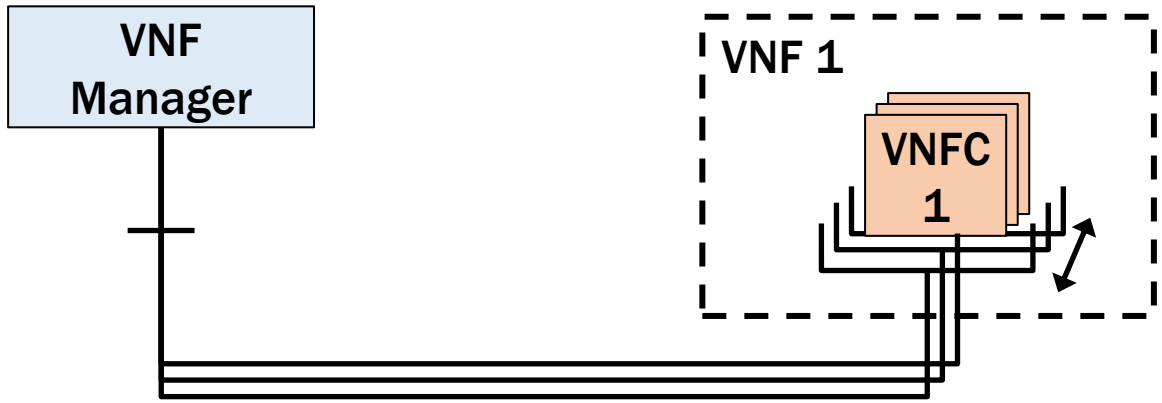
- Infrastructure Network Load Balancer
  - VNF instances seen as one logical NF by a Peer NF
    - VNFs may be of different VNF Providers, e.g. to increase resilience
  - The load balancer is provided by the NFVI
    - The NFVO instantiates the VNF multiple times and configure a load balancer in the NFVI
  - Example: NFVI providing load balancing for several Firewall instances



VNF External Load Balancer

VNF Design Patterns:
VNF Scaling Models

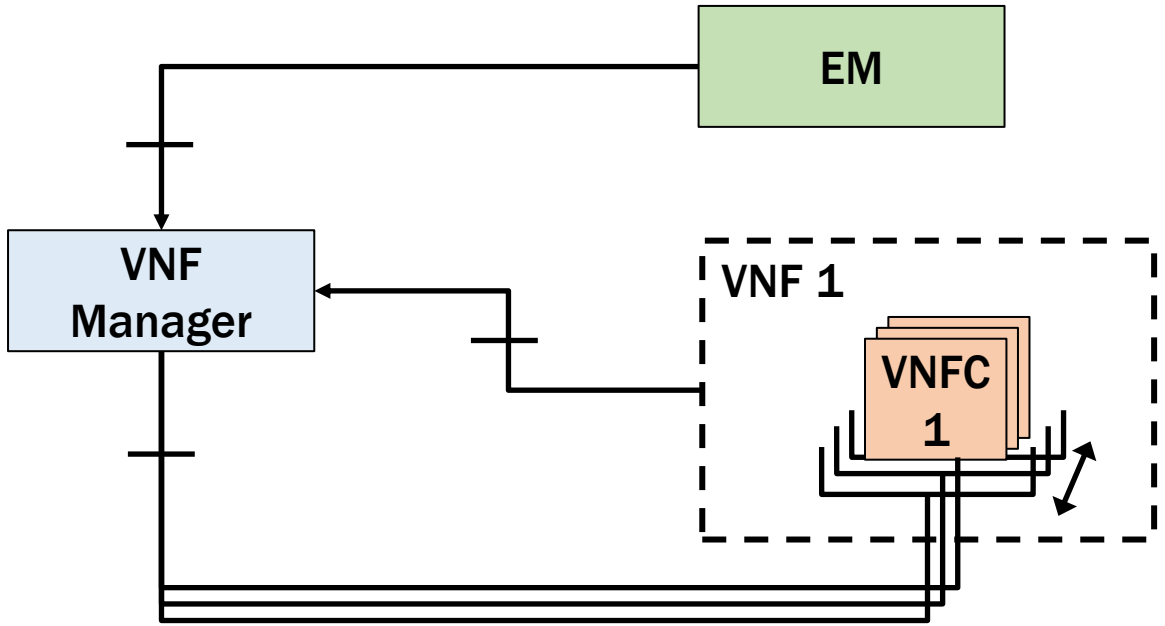
- 3 main models identified
  - Auto scaling
    - The VNFM triggers the scaling of VNF according to the rules in the VNFD
      - For example, based on monitoring of resource utilization of the VNF's VMs, upon events received from the VNF, the EM, the VIM, or locally generated
      - Both scale out/in and scale up/down may be supported



Auto Scaling triggered by the VNFM

VNF Design Patterns:
VNF Scaling Models

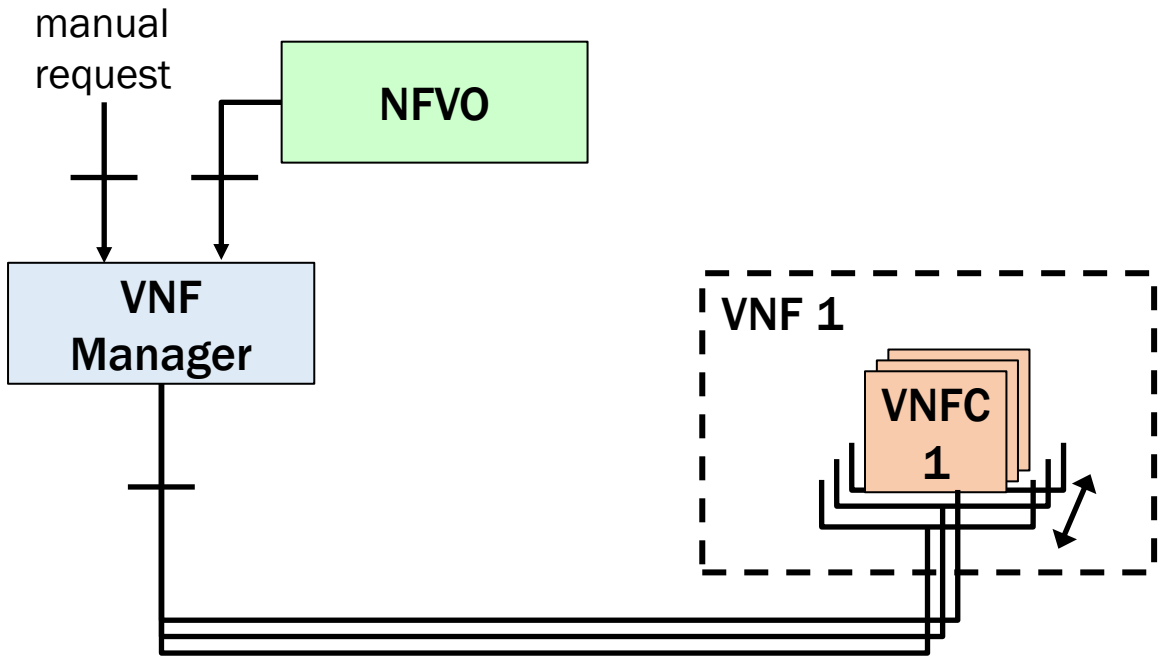
- On-demand scaling (from VNF or EM)
  - A VNF Instance or its EM monitors the states o the VNFC Instances and trigger a scaling operation to the VNFM
    - Through a explicit operation to add or remove VNFC instances (scale out/in) or to increase or decrease resources of one of more VNFC instances (scale up/down)



On-demand scaling

VNF Design Patterns:
VNF Scaling Models

- Scaling based on a management request
  - Manually triggered scaling (e.g. by NOC operators),
  - or OSS/BSS triggered scaling according to the rules in the VNFD by issuing requests to the NFVO via an appropriate interface
  - Both scale out/in and scale up/down may be supported



Scaling based on management request

VNF Design Patterns:
VNF Update and Upgrade

- As any other product, a VNF requires
  - Updates. A VNF update does not introduce new functionality and/or new interfaces
    - can be deployed without coordination with other VNFs participating in the same VNFFG
  - Upgrades. A VNF upgrade might introduce new functionality and/or new interfaces
    - may require planning on network service level
- Updates and Upgrades pose requirements for VNF Providers
  - Provision of automatic procedures to execute the VNF Instance update/upgrade as part of the VNF Package
    - Controlling the progress of the process (including requests of virtual resources from the NFV MANO)
    - Supporting the roll-back (including returning the obtained resources)

Attributes describing VNF's Requirements

- Virtualized Network Function Description (VNFD)
  - Describes the deployment configuration and operational behavior of a VNF
    - Deployment behavior: defines the state and environment for a VNF to be deployed
      - Deployment flavor
    - Operational behavior: defines the needed functions for a VNF to be operated and managed properly
  - It is a template capturing the general characteristics of each VNF and is used to on-board the VNF

- More details can be found in the specification ETSI GS NFV-IFA 011

Attributes describing VNF's Requirements

- The VNFD is composed of the following main information elements groupings
  - VNF identification data
  - VNF specific data, such as
    - Specific VNF configuration data
    - Connectivity requirements and inter-dependencies of VNFCs
  - VNFC data, such as
    - Virtualization container files/images references

    → VDU
  - Virtualized resource requirements, such as
    - Compute, Storage and Network resources

Attributes describing VNF's Requirements

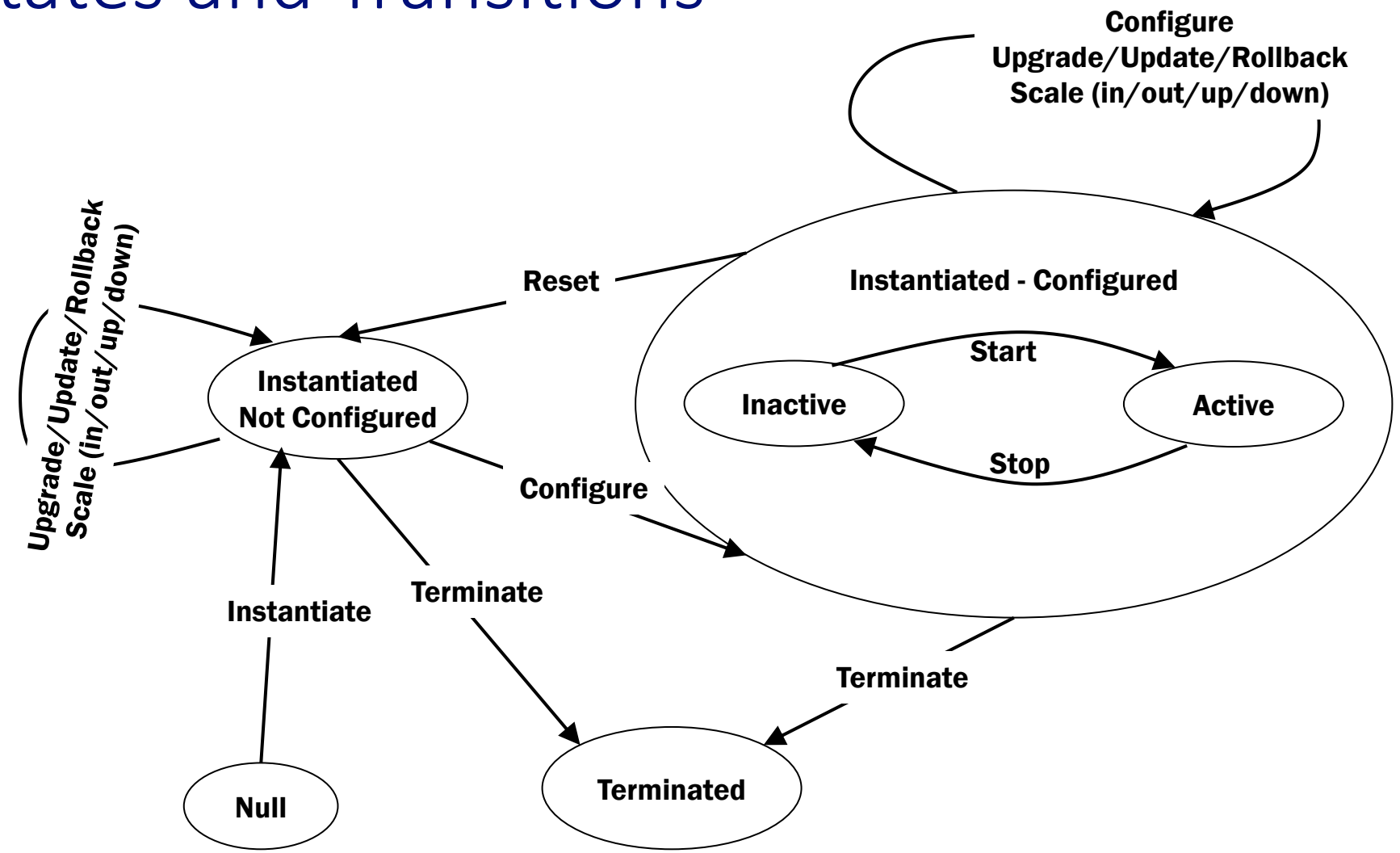
- Deployment Behavior
  - Virtualization containers
    - Number of VNFCs required for this VNFs instantiation, including the corresponding Virtualization container files/images references
  - NFVI Resources
  - Components and Relationship
  - Location
    - E.g., there might be a constraint for redundancy that dictates how many instances of a VNF can be collocated in the same location
  - Other constraints
    - For example, regarding degree of isolation
- Operational Behavior
  - Management Operations

VNF States and Transitions

- A number of generic internal states represent the status of the VNF
  - Before a VNF can start its lifecycle, it has to be on-boarded
    - On-boarding: process of registering the VNF with the NFVO and uploading the VNF data (VNFD, SW images, etc)
      - On-boarding is the responsibility of NFVO

State	Description
Null	A VNF Instance does not exist and is about to be created
Instantiated Not Configured	VNF Instance does exist but is not configured for service
Instantiated Configured - Inactive	A VNF Instance is configured for service
Instantiated Configured - Active	A VNF Instance that participates in service
Terminated	A VNF Instance has ceased to exist

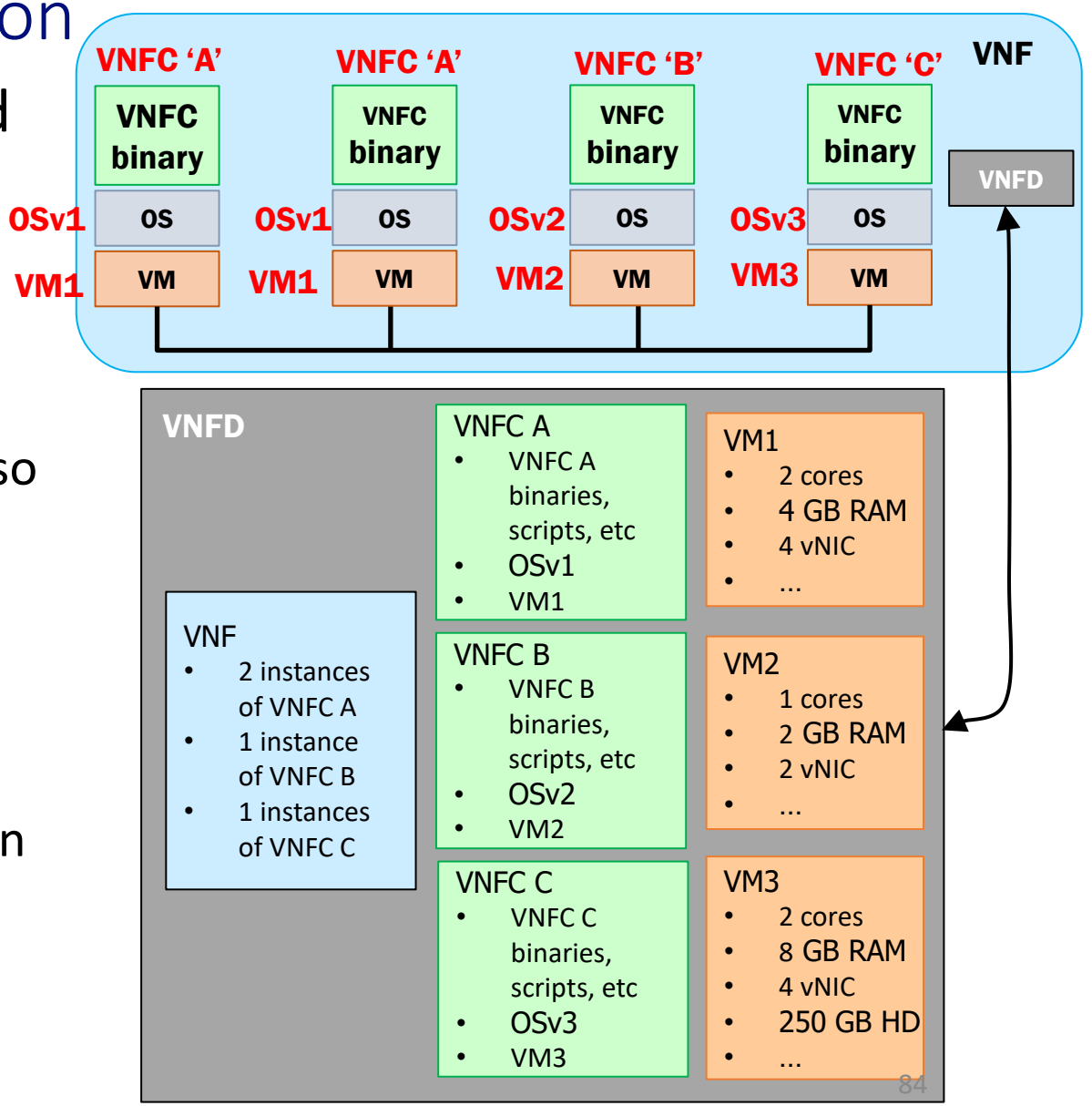
VNF States and Transitions



VNF instance state transitions

VNF States and Transitions:
The VNFD's role in VNF instantiation

- VNFD = specification template provided by the VNF Provider for describing virtual resource requirements of a VNF
  - Used by the MANO functions to determine how to execute VNF lifecycle operations (such as instantiation)
  - Besides resource requirements, a VNFD also contains unambiguous references to VNF binaries, scripts, configuration data, etc., necessary for the MANO functions to configure the VNF properly
  - The requirements for the NFVI resources (e.g., connectivity requirements, bandwidth, latency, etc.) are also present in the VNFD



This a bit more complex: VDUs, deployment flavors…

NFV implementations

NFV Implementations (I)

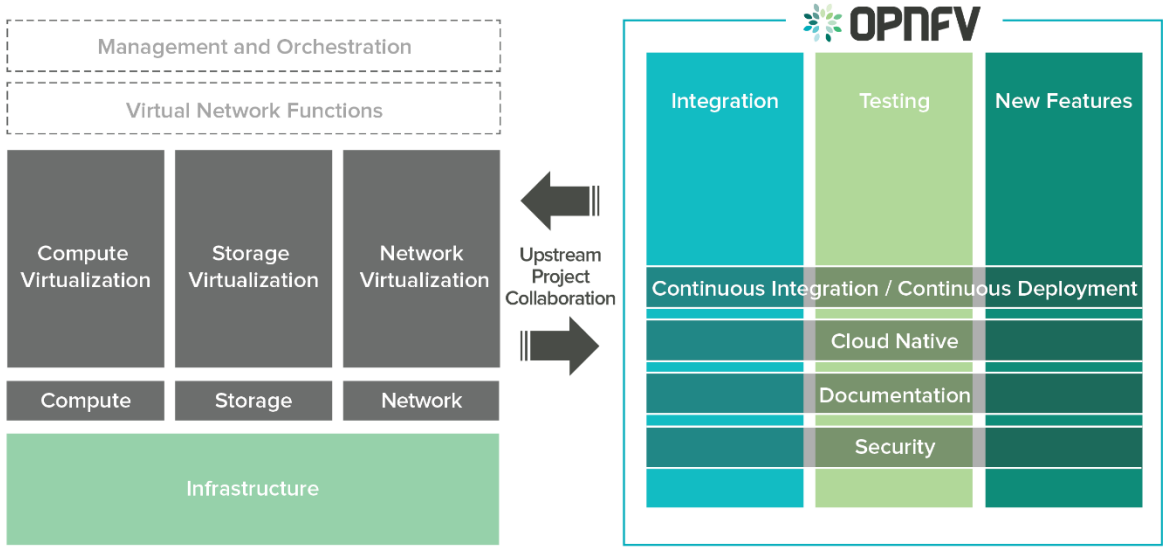
- OSM: Open Source MANO (http://osm.etsi.org)
  - ETSI-hosted project to develop an Open Source NFV Management and Orchestration (MANO) software stack aligned with ETSI NFV
    - EPA support (Enhanced Platform Awareness)
    - Multi VIM, multi site
    - 5G ready
  - Built from previously existing SW components:
    - OpenMANO for Resource Orchestration
    - Riftware for Service Orchestration
    - Juju for VNF Config and Mgmt
  - Nineth release available since Dec. 2020

NFV Implementations (II)

- OpenMANO (https://github.com/nfvlabs/openmano)
  - Open source project led by Telefonica,
  - Aimed at implementing the ETSI NFV MANO framework, and addressing the aspects related to performance and portability by applying Enhanced Platform Awareness (EPA) principles
  - 3 main components: openmano, openvim, and a graphical user interface (GUI)
  - Most of it has now moved to OSM

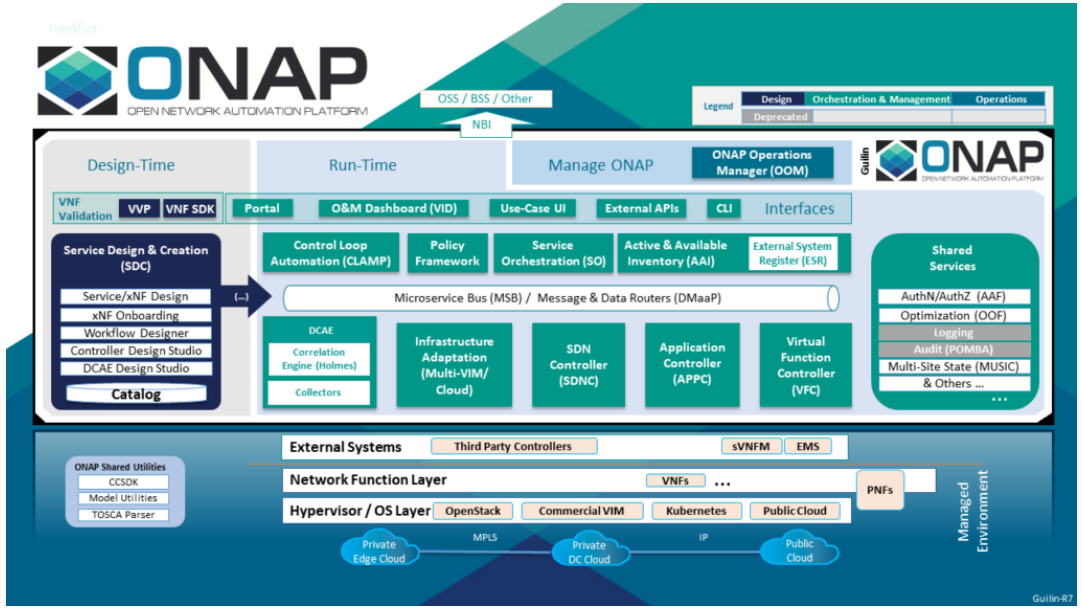
NFV Implementations (III)

- OPNFV (https://www.opnfv.org/)
  - Open source project founded and hosted by the Linux Foundation
  - Goal is to establish an open source reference platform which may be used to validate multi-vendor, inter-operable NFV solutions
  - Contributes improvements to relevant upstream open source projects, and develop necessary new functionality both within OPNFV and upstream projects
  - Tenth release (OPNFV Jerma) available since December 2020



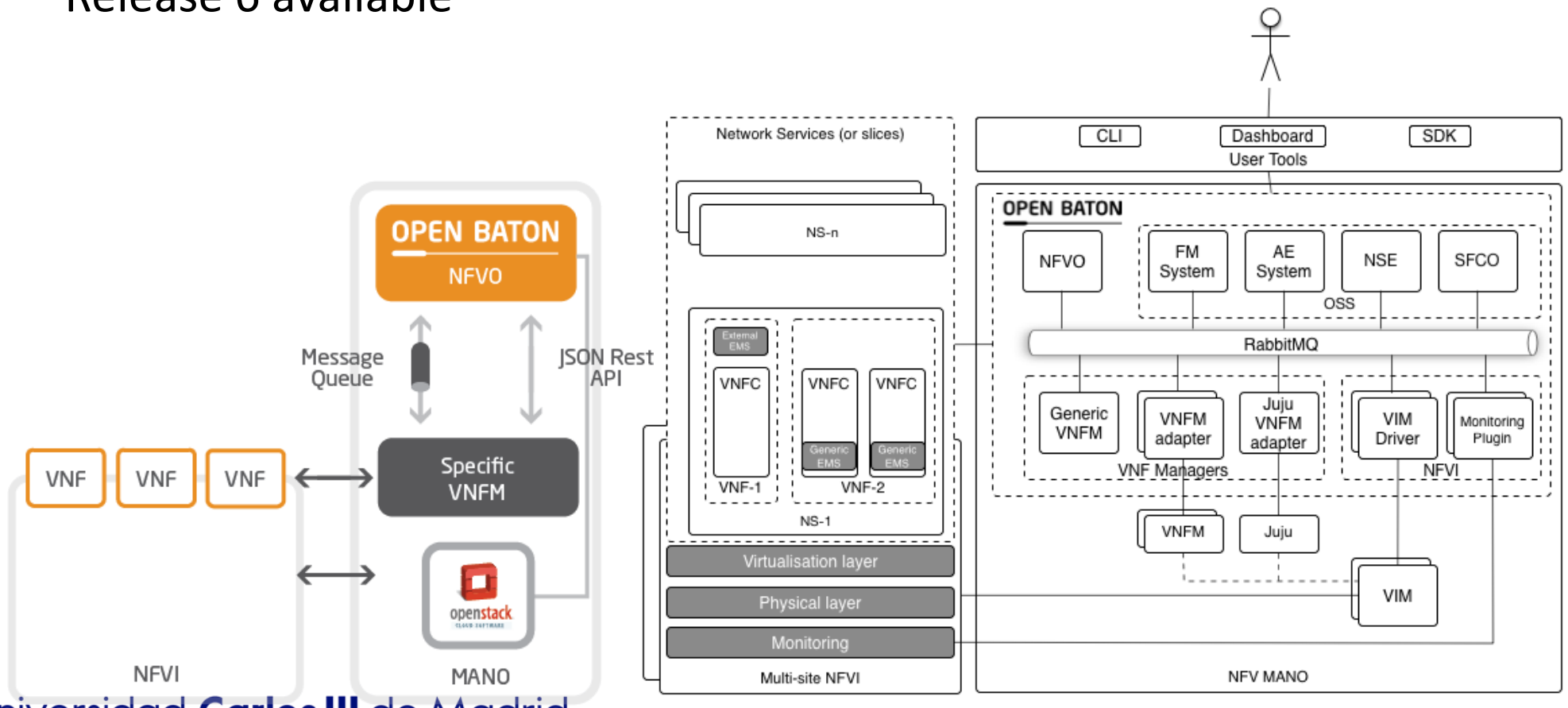
NFV Implementations (IV)

- ONAP: Open Network Automation platform (https://www.onap.org/)
  - Project combining ECOMP and Open-O
  - Open source project for real-time, policy-driven orchestration and automation of physical and virtual network functions
  - Seventh release (Guilin) available since December 2020



NFV Implementations (V)

- Open Baton (https://openbaton.github.io/)
  - Open Baton is a ETSI NFV compliant MANO framework
  - Release 6 available



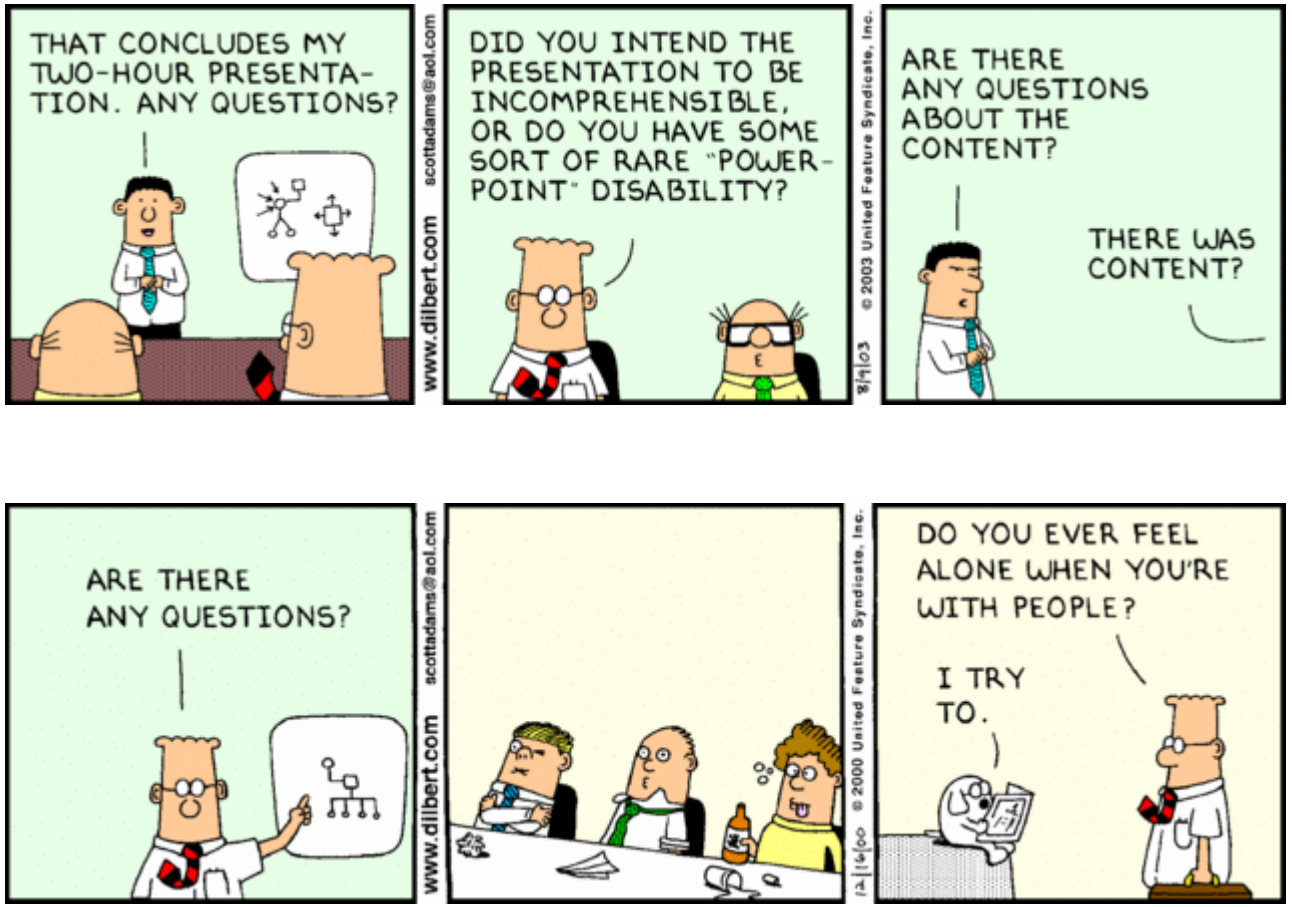
Summary

- NFV decouples SW from HW
  - Enabling independent evolution
  - Flexible network function deployment
  - Dynamic scaling
- ETSI NFV architecture as “de-facto” framework
- Lot of work done so far, but more coming still
- Other SDOs adopting virtualization as key tool/enabler

References

- ETSI NFV ISG documents
  - http://www.etsi.org/technologies-clusters/technologies/nfv
  - http://www.etsi.org/deliver/etsi_gs/
  - https://docbox.etsi.org/ISG/NFV/Open/Drafts/
- “Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud,” William Stallings, Addison-Wesley Professional, 1st edition, 2015
- “Network Function Virtualization,” Ken E. Gray and Thomas D. Nadeau, Morgan Kaufmann, 2016

Questions?


THAT CONCLUDES MY TWO-HOUR PRESENTATION. ANY QUESTIONS?
www.dilbert.com scottadams@aol.com
DID YOU INTEND THE PRESENTATION TO BE INCOMPREHENSIBLE, OR DO YOU HAVE SOME SORT OF RARE "POWERPOINT" DISABILITY?
© 2003 United Feature Syndicate, Inc.
8/9/03
ARE THERE ANY QUESTIONS ABOUT THE CONTENT?
THERE WAS CONTENT?
ARE THERE ANY QUESTIONS?
www.dilbert.com scottadams@aol.com
© 2000 United Feature Syndicate, Inc.
12/16/00
DO YOU EVER FEEL ALONE WHEN YOU'RE WITH PEOPLE?
I TRY TO.

References

- “Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud,” William Stallings, Addison-Wesley Professional, 1st edition, 2015
  - Sections 7.5, 8.1, 8.2 and 8.3
- “Network Functions Virtualisation (NFV); Architectural Framework,“ ETSI GS NFV 002, V1.2.1 (2014-12)
- “Network Function Virtualization: State-of-the-art and Research Challenges,” R. Mijumbi et al., in IEEE Communications Surveys & Tutorials, 2015