CMPE 209 Network Security
Network Function Virtualization

Chapter 7. NFV Concepts and Architecture

Dr. Younghee Park

SAN JOSÉ STATE
UNIVERSITY

Background and Motivation for NFV

- NFV originated from discussions among major network operators and carriers about how to improve network operation in the high-volume multimedia era
- The overall objective of NFV is leveraging standard IT virtualization technology to consolidate many network equipment types onto industry standard high-volume servers, switches, and storage, which could be located in data centers, network nodes, and in the end-user premises
- The NFV approach moves away from dependence on a variety of hardware platforms to the use of a small number of standardized platform types, with virtualization techniques used to provide the needed network functionality

Middleboxes

carrier-grade NAT

ad insertion

BRAS

WAN accelerator

transcoder

session border controller

IDS

load balancer

DDoS protection

firewall

QoE monitor

DPI

Virtual Machines

- Virtualization technology enables a single PC or server to simultaneously run multiple operating systems or multiple sessions of a single OS
- A machine running virtualization software can host numerous applications, including those that run on different operating systems, on a single hardware platform
- The host operating system can support a number of virtual machines (VMs), each of which has the characteristics of a particular OS and, in some versions of virtualization, the characteristics of a particular hardware platform

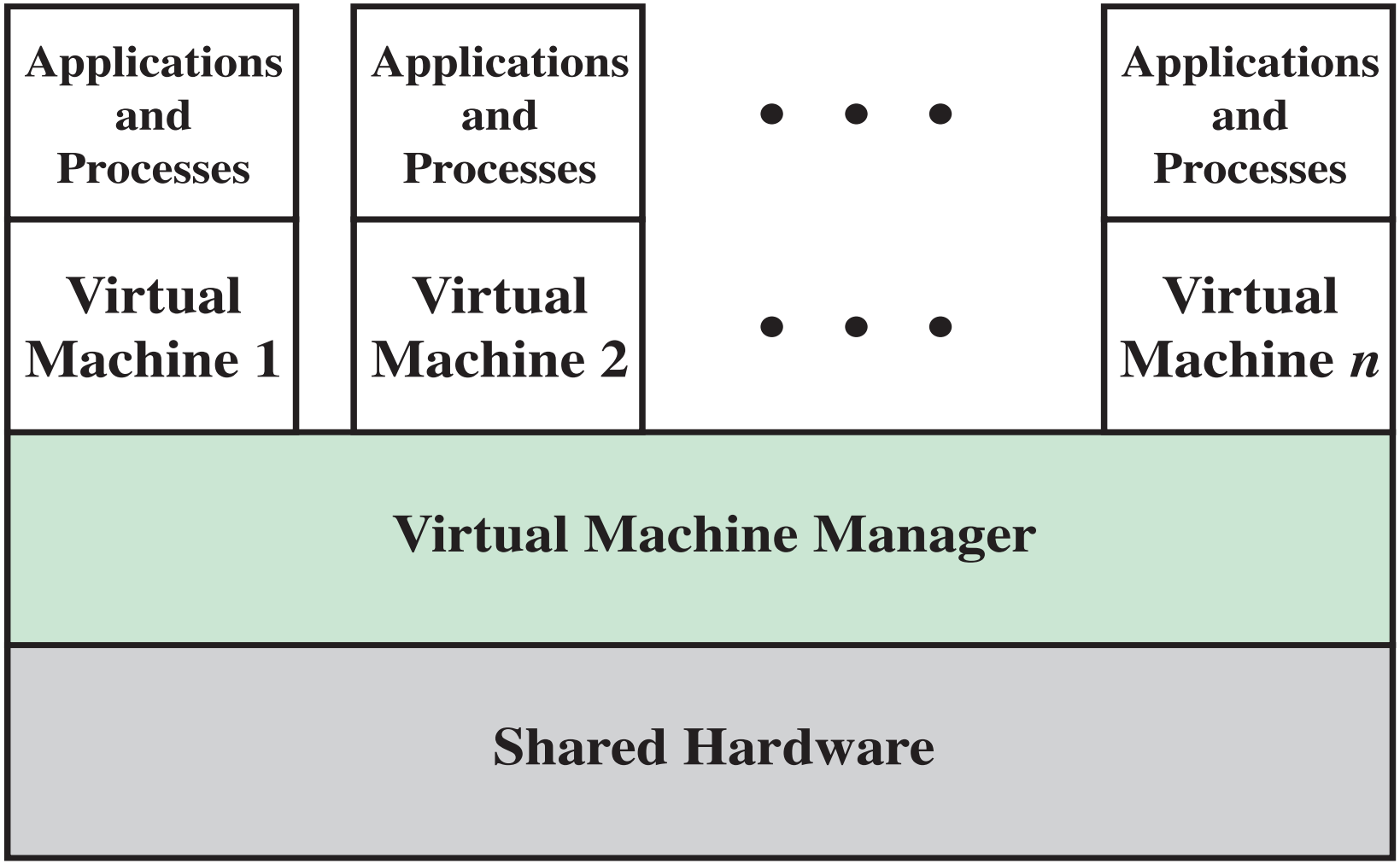


Figure 7.1 Virtual Machine Concept

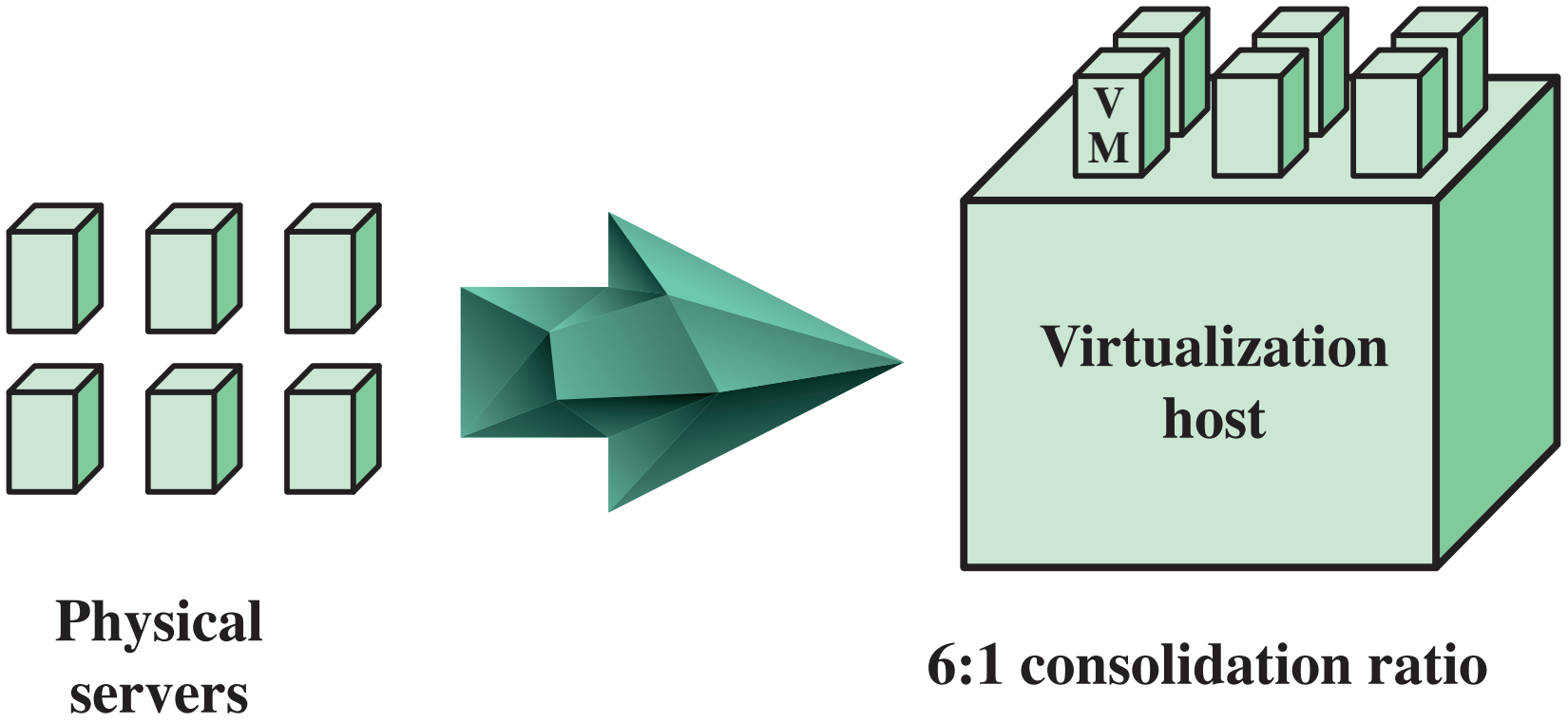


Figure 7.2 Virtual Machine Consolidation

Architectural Approaches

- Virtualization abstracts the physical hardware from the VMs it supports
  - Virtual machine monitor, or hypervisor, is the software that provides this abstraction
  - It acts as a broker, or traffic cop, acting as a proxy for the guests (VMs) as they request and consume resources of the physical host
- A VM is a software construct that mimics the characteristics of a physical server
  - It is configured with some number of processors, some amount of RAM, storage resources, and connectivity through the network ports
  - It can be powered on like a physical server, loaded with an operating system and applications, and used in the manner of a physical server
    - Unlike a physical server, this virtual server sees only the resources it has been configured with, not all the resources of the physical host itself
    - This isolation allows a host machine to run many VMs, each running the same or different copies of an operating system, sharing RAM storage, and network bandwidth, without problems

Architectural Approaches

- VMs are made up of files
  - There is a configuration file that describes the attributes of the VM; It contains:
    - The server definition
    - How many virtual processors (vCPUs) are allocated to this VM
    - How much RAM is allocated
    - Which I/O devices the VM has access to
    - How many network interface cards (NICs) are in the virtual server
  - It also describes the storage that the VM can access
- When a VM is powered on, or instantiated, additional files are created for logging, for memory paging, and other functions
- Because VMs are already files, copying them produces not only a backup of the data but also a copy of the entire server, including the operating system, applications, and the hardware configuration itself

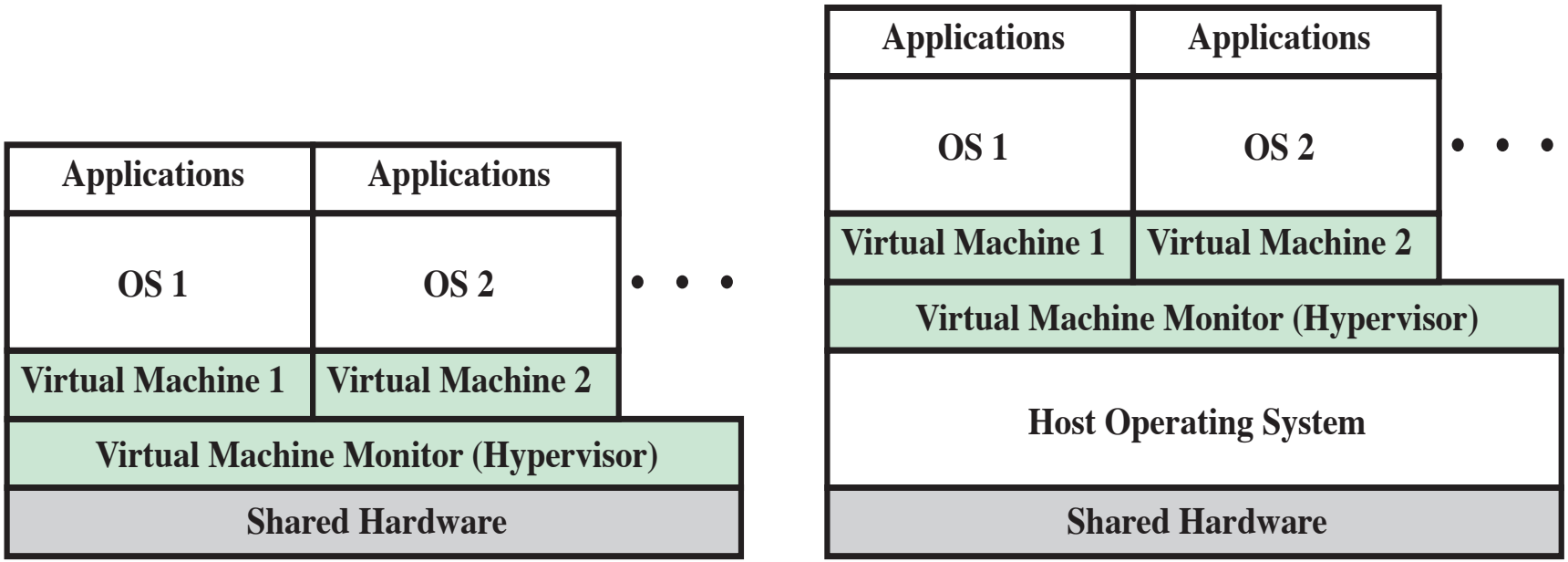


Figure 7.3 Type 1 and Type 2 Virtual Machine Monitors

- Type 1: VMware ESXi, Microsoft Hyper-V, and the various open source Xen variants, KVM, Virtual Box 6.0+.
- Type 2: VMware Workstation and Oracle, VM Virtual Box.

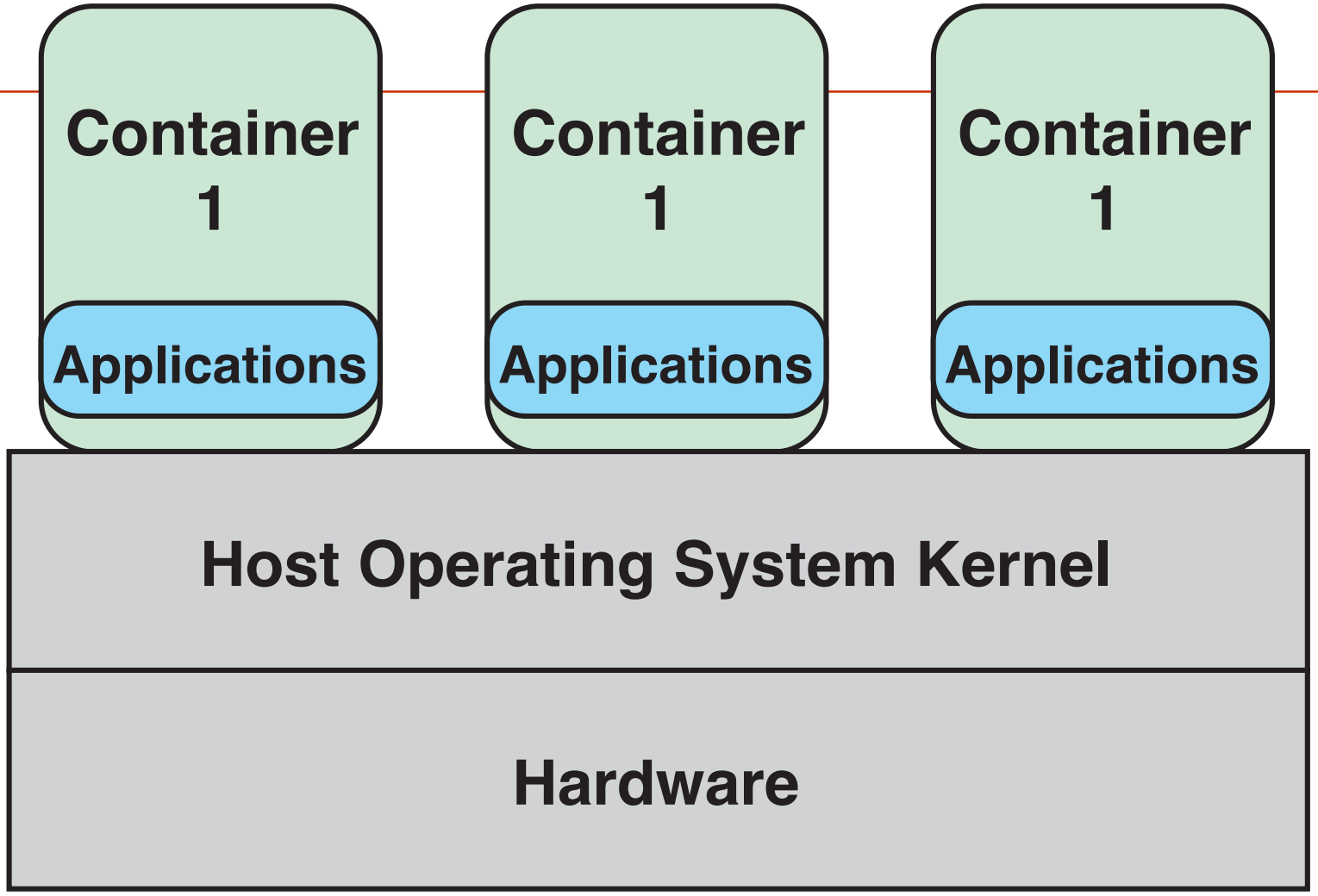


Figure 7.4 Container Virtualization

NFV Concepts

NFV

Is defined as the virtualization of network functions by implementing these functions in software and running them on VMs

Is a significant departure from traditional approaches to the design deployment, and management of networking services

Decouples network functions, such as Network Address Translation (NAT), firewalling, intrusion detection, Domain Name Service (DNS), and caching, from proprietary hardware appliances so that they can run in software on VMs

Builds on standard VM technologies, extending their use into the networking domain

NFV Concepts

- Virtual machine technology enables migration of dedicated application and database servers to commercial off-the-shelf (COTS) x86 servers
- The same technology can be applied to network-based devices, including:

Network function devices

- Such as switches, routers, network access points, customer premises equipment (CPE), and deep packet inspectors

Network-related compute devices

- Such as firewalls, intrusion detection systems, and network management systems

Network-attached storage

- File and database servers attached to the network

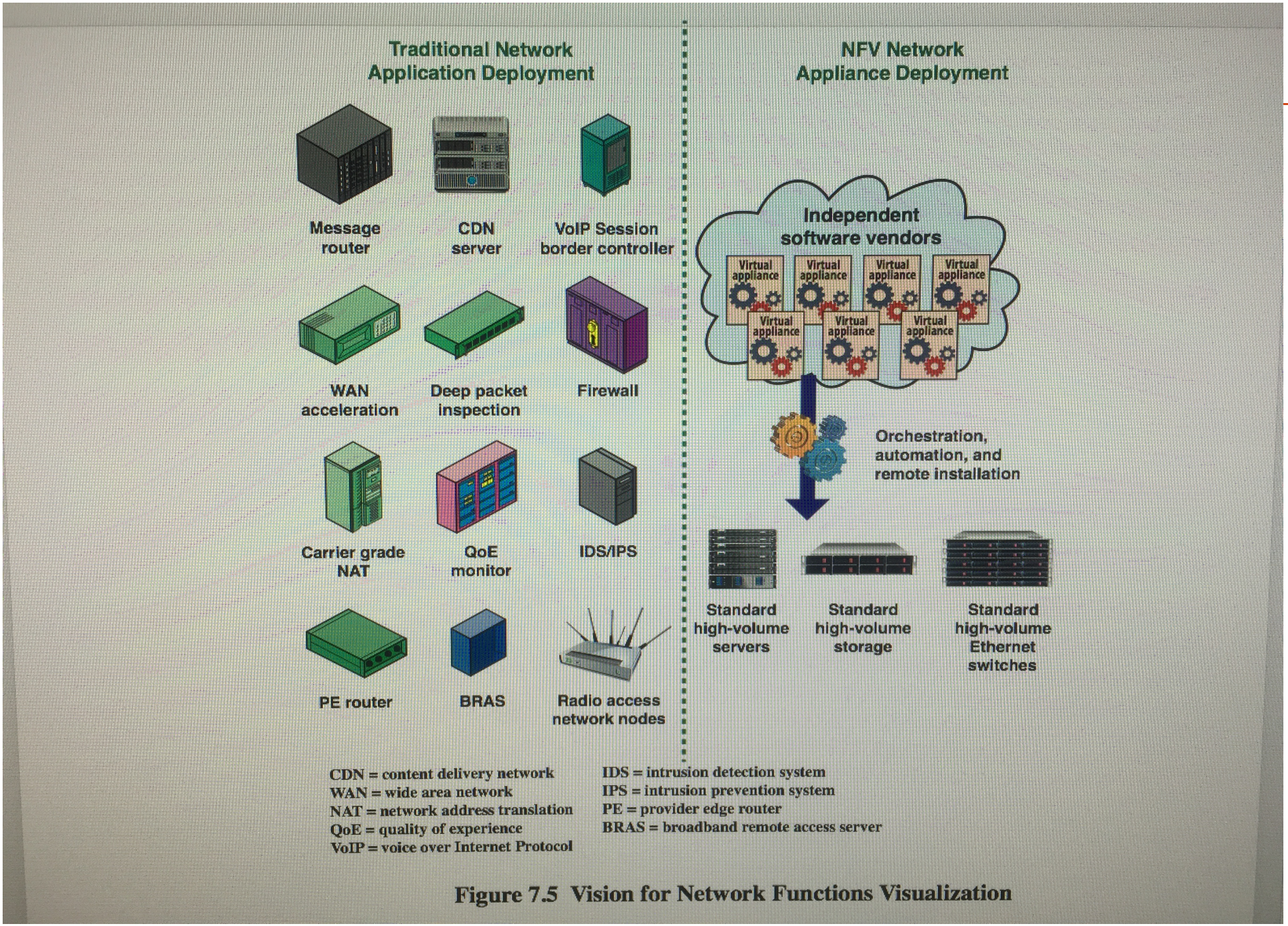


Figure 7.5 Vision for Network Functions Visualization

Table 7.1 ISG NFV Specifications

Standard Number	Standard Title
GS NFV 002	Architectural Framework
GS NFV-INF 001	Infrastructure Overview
GS NFV-INF 003	Infrastructure; Compute Domain
GS NFV-INF 004	Infrastructure; Hypervisor Domain
GS NFV-INF 005	Infrastructure; Network Domain
GS NFV-INF 007	Infrastructure; Methodology to describe Interfaces and Abstractions
GS NFV-MAN 001	Management and Orchestration
GS NFV-SEC 001	NFV Security; Problem Statement
GS NFV-SEC 003	NFV Security; Security and Trust Guidance
GS NFV-PER 001	NFV Performance & Portability Best Practices
GS NFV-PER 002	Proofs of Concept; Framework
GS NFV-REL 001	Resiliency Requirements
GS NFV-INF 010	Service Quality Metrics
GS NFV 003	Terminology for Main Concepts in NFV
GS NFV 001	Use Cases
GS NFV-SWA 001	Virtual Network Functions Architecture
GS NFV 004	Virtualization Requirements

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) A functional block within a network infrastructure that has well-defined external interfaces and well-defined functional behavior. Typically, this is a physical network node or other physical appliance.

network functions virtualization (NFV) The 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.

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 An 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 with the list.

network point of presence (N-PoP) A location where a network function is implemented as either a physical network function (PNF) or a VNF.

network service A composition of network functions that is defined by its functional and behavioral specification.

NFV infrastructure (NFVI) The totality of all hardware and software components that build up the environment in which VNFs are deployed. The NFVI can span across several locations, i.e., multiple N-PoPs. The network providing connectivity between these locations is regarded to be part of the NFVI.

physical network function (PNF) An implementation of a NF via a tightly coupled software and hardware system. This is typically a proprietary system.

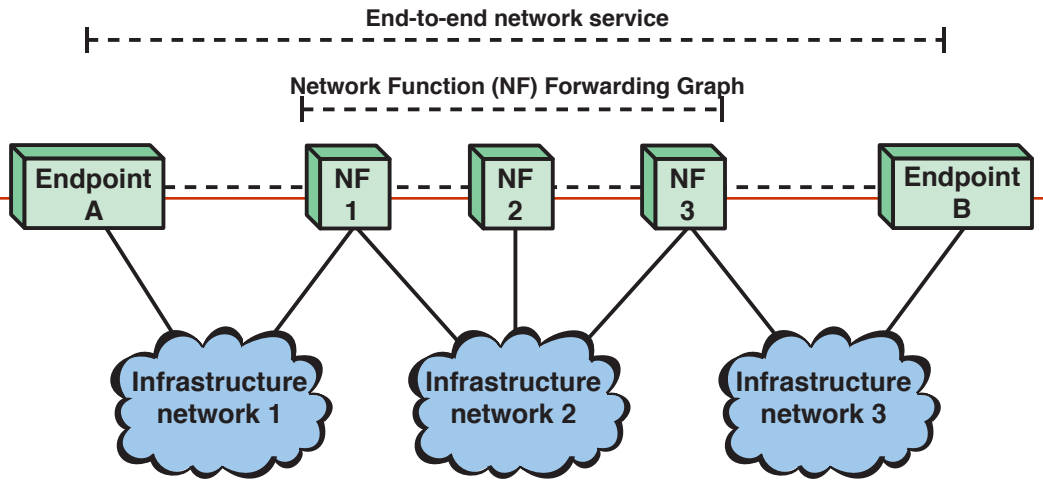
virtual machine (VM) A virtualized computation environment that behaves very much like a physical computer/server.

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 NFVI architecture, a virtual network routes information among the network interfaces of VM instances and physical network interfaces, providing the necessary connectivity.

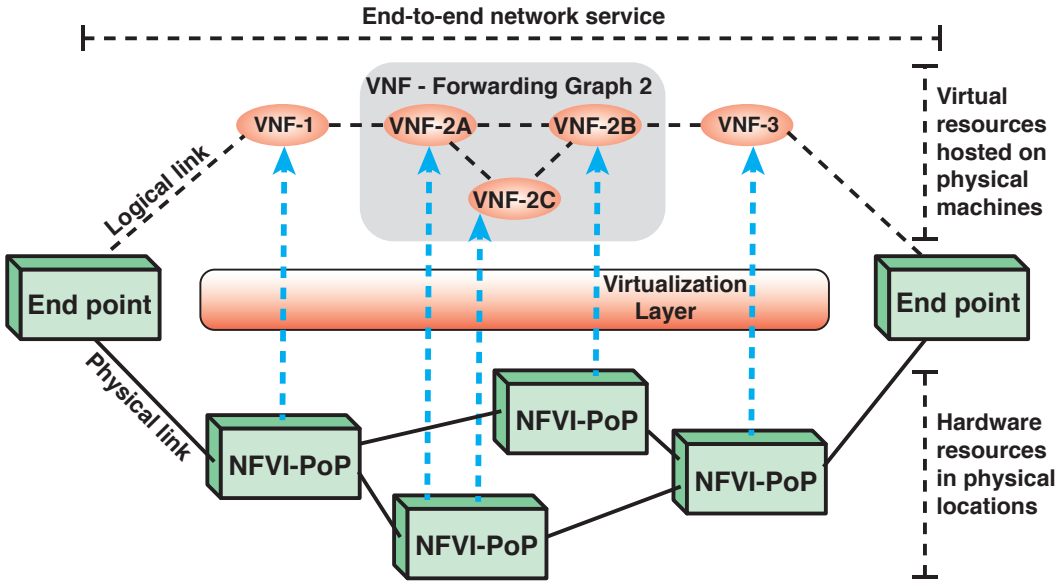
virtualized network function (VNF) An implementation of an NF that can be deployed on a NFVI.

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.



(a) Graph representation of an end-to-end network service



(b) Example of an end-to-end network service with VNFs and nested forwarding graphs

Figure 7.6 A Simple NFV Configuration Example

NFV Principles

- **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)

- This involves deploying and managing the lifecycle of VNF instances
- Examples include 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 of which 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

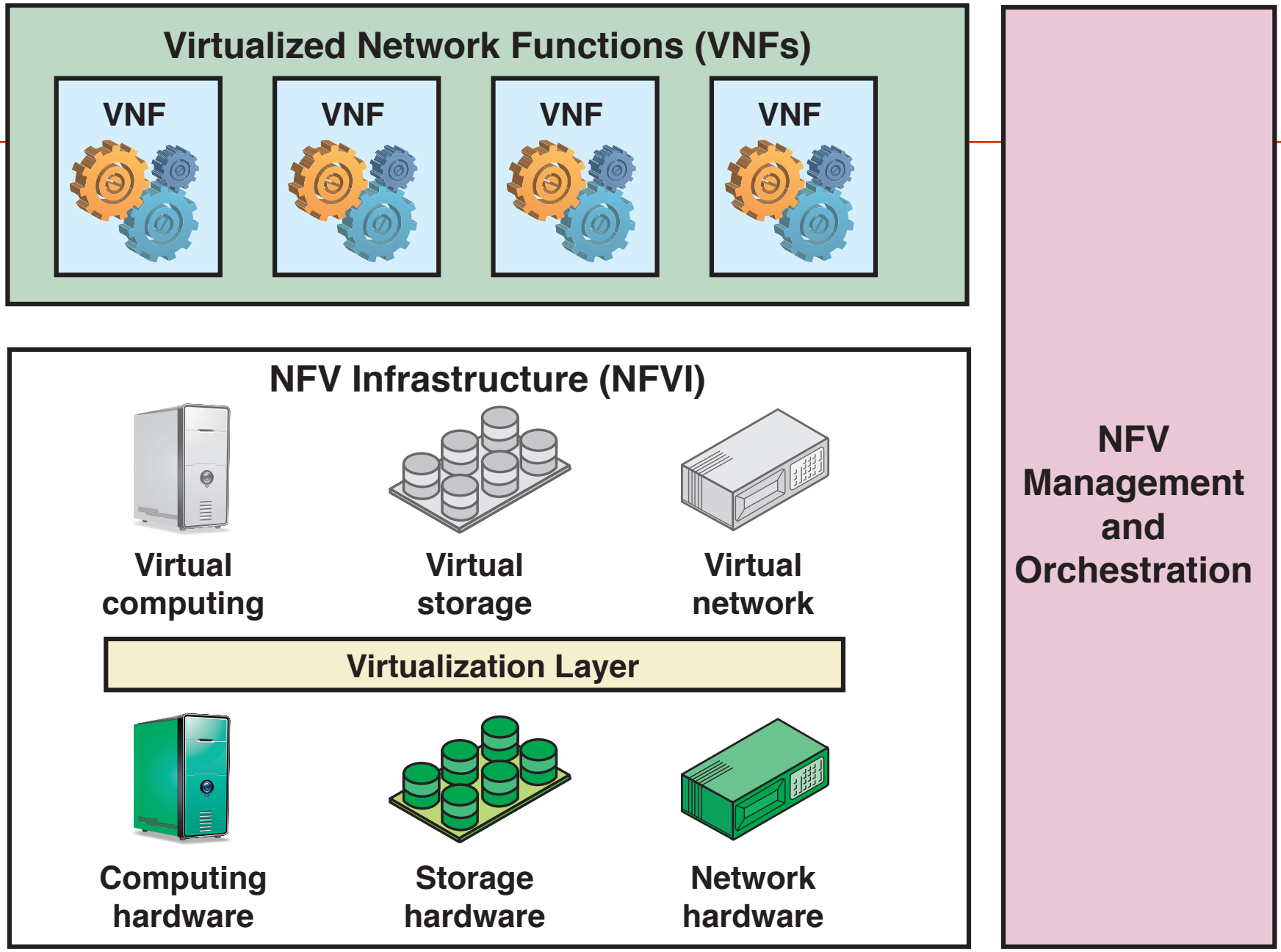


Figure 7.7 High-Level NFV Framework

NFV Benefits

- If NFV is implemented efficiently and effectively, it can provide a number of benefits compared to traditional networking approaches:
  - Reduced CapEx
  - Reduced OpEx
  - The ability to innovate and roll out services quickly
  - Ease of interoperability because of standardized and open interfaces
  - Use of a single platform for different applications, users and tenants
  - Provided agility and flexibility, by quickly scaling up or down services to address changing demands
  - Targeted service introduction based on geography or customer sets is possible
  - A wide variety of ecosystems and encourages openness

NFV Requirements

- NFV must be designed and implemented to meet a number of requirements and technical challenges, including:
  - Portability/interoperability
  - Performance trade-off
  - Migration and coexistence with respect to legacy equipment
  - Management and orchestration
  - Automation
  - Security and resilience
  - Network stability
  - Simplicity
  - Integration

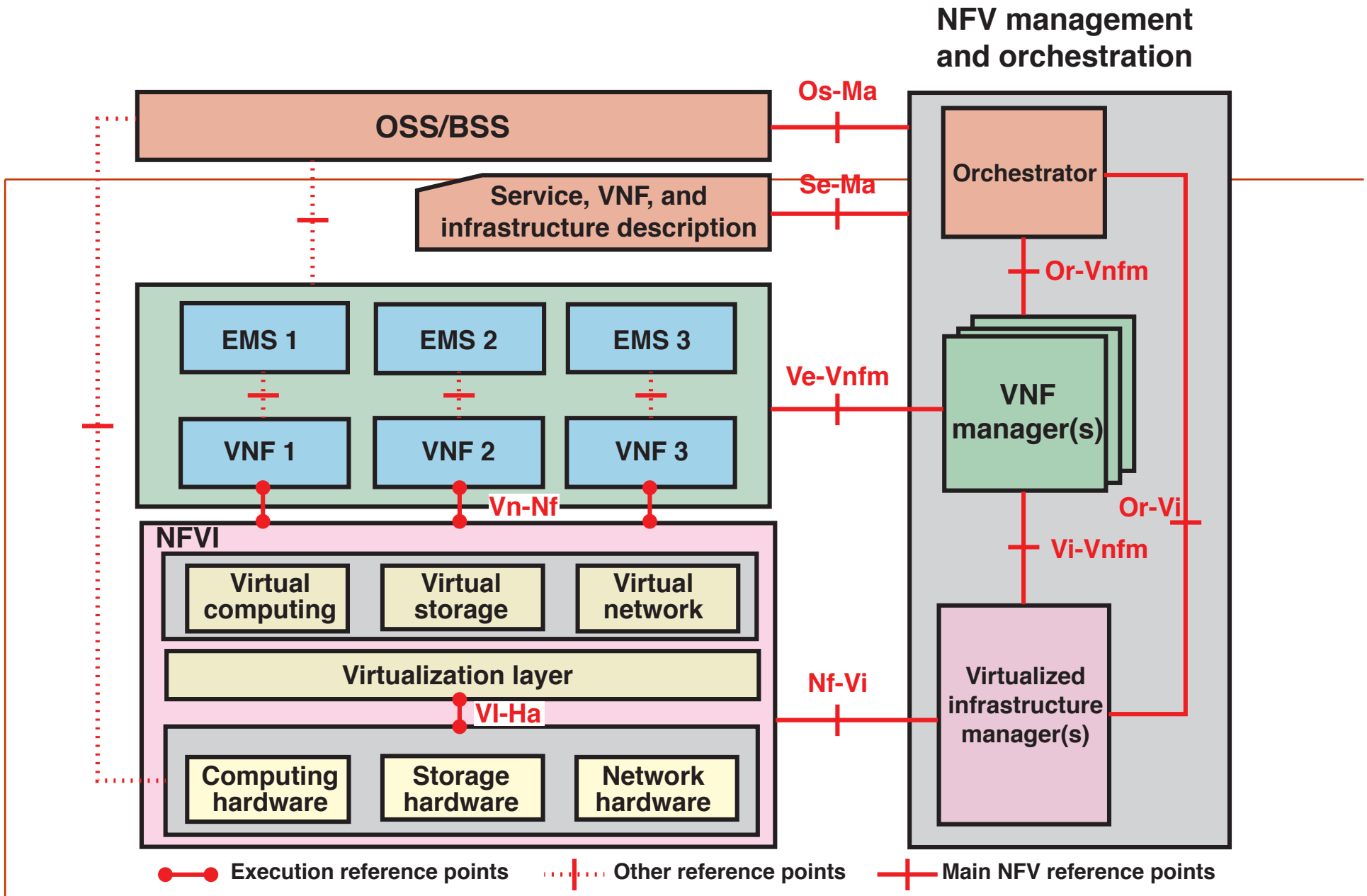


Figure 7.8 NFV Reference Architectural Framework

Figure 7.8 also defines a number of reference points that constitute interfaces between functional blocks. The main (named) reference points and execution reference points are shown by solid lines and are in the scope of NFV. These are potential targets for standardization. The dashed line reference points are available in present deployments but might need extensions for handling network function virtualization. The dotted reference points are not a focus of NFV at present.

The main reference points include the following considerations:

■ Vi-Ha: Marks interfaces to the physical hardware. A well-defined interface specification will facilitate for operators sharing physical resources for different purposes, reassigning resources for different purposes, evolving software and hardware independently, and obtaining software and hardware component from different vendors.

■ Vn-Nf: These interfaces are APIs used by VNFs to execute on the virtual infrastructure. Application developers, whether migrating existing network functions or developing new VNFs, require a consistent interface the provides functionality and the ability to specify performance, reliability, and scalability requirements.

■ Nf-Vi: Marks interfaces between the NFVI and the virtualized infrastructure manager (VIM). This interface can facilitate specification of the capabilities that the NFVI provides for the VIM. The VIM must be able to manage all the NFVI virtual resources, including allocation, monitoring of system utilization, and fault management.

■ Or-Vnfm: This reference point is used for sending configuration information to the VNF manager and collecting state information of the VNFs necessary for network service lifecycle management.

■ Vi-Vnfm: Used for resource allocation requests by the VNF manager and the exchange of resource configuration and state information.

■ **Nf-Vi: Marks interfaces between the NFVI and the virtualized infrastructure manager (VIM). This interface can facilitate specification of the capabilities that the NFVI provides for the VIM. The VIM must be able to manage all the NFVI virtual resources, including allocation, monitoring of system utilization, and fault management.**

■ **Or-Vnfm: This reference point is used for sending configuration information to the VNF manager and collecting state information of the VNFs necessary for network service lifecycle management.**

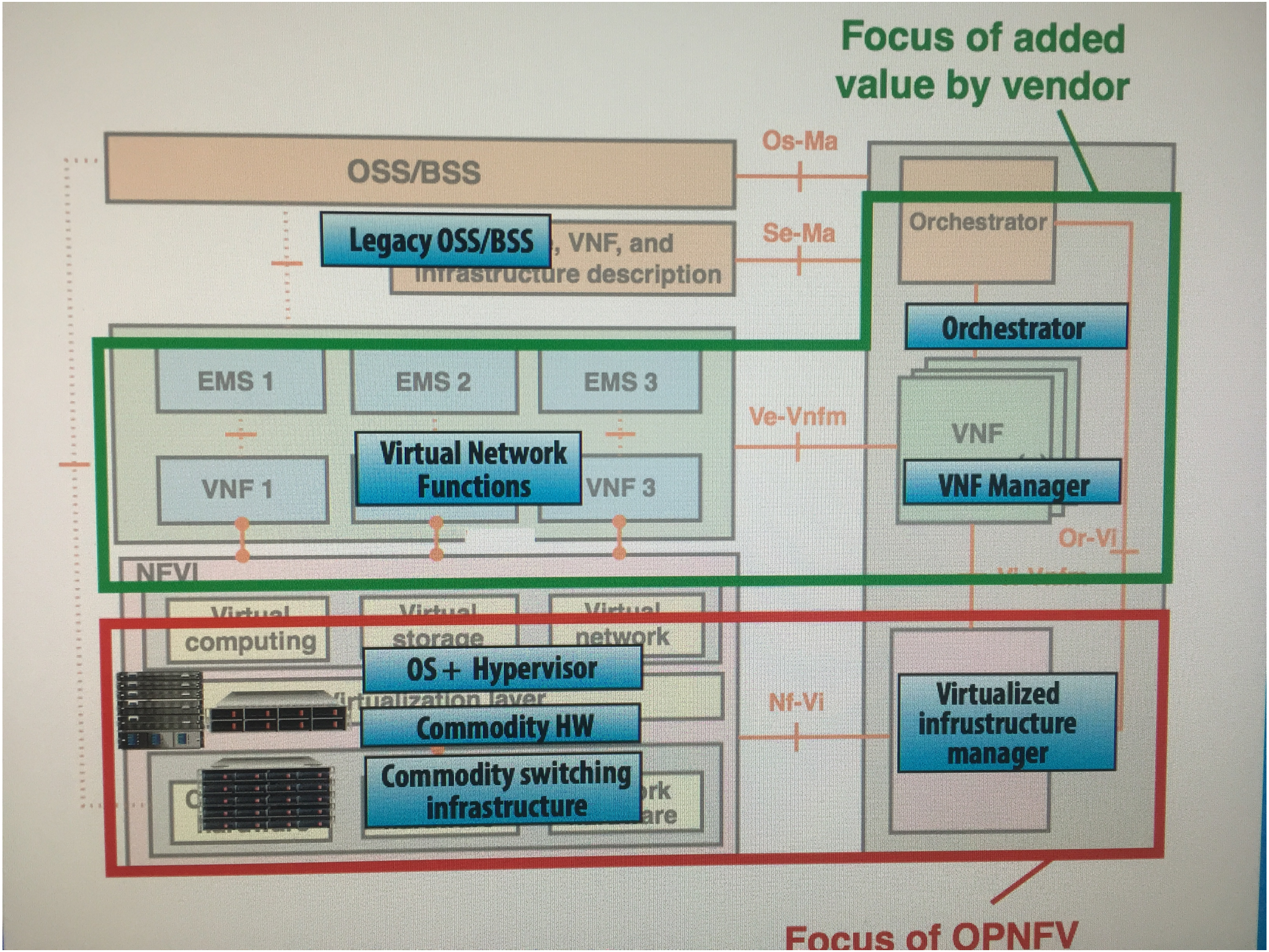
■ **Vi-Vnfm: Used for resource allocation requests by the VNF manager and the exchange of resource configuration and state information.**

■ **Or-Vi: Used for resource allocation requests by the NFV orchestrator and the exchange of resource configuration and state information.**

■ **Os-Ma: Used for interaction between the orchestrator and the OSS/BSS systems.**

■ **Ve-Vnfm: Used for requests for VNF lifecycle management and exchange of configuration and state information.**

■ **Se-Ma: Interface between the orchestrator and a data set that provides information regarding the VNF deployment template, VNF forwarding graph, service-related information, and NFV infrastructure information models.**


Focus of added value by vendor
OSS/BSS
Os-Ma
Legacy OSS/BSS
, VNF, and
infrastructure description
Se-Ma
Orchestrator
Orchestrator
EMS 1
EMS 2
EMS 3
Ve-Vnfm
VNF
Virtual Network Functions
VNF 1
VNF 3
VNF Manager
Or-Vi
NFVI
computing
storage
network
OS + Hypervisor
Commodity HW
Commodity switching infrastructure
Nf-Vi
Virtualized infrustructure manager
Focus of OPNFV