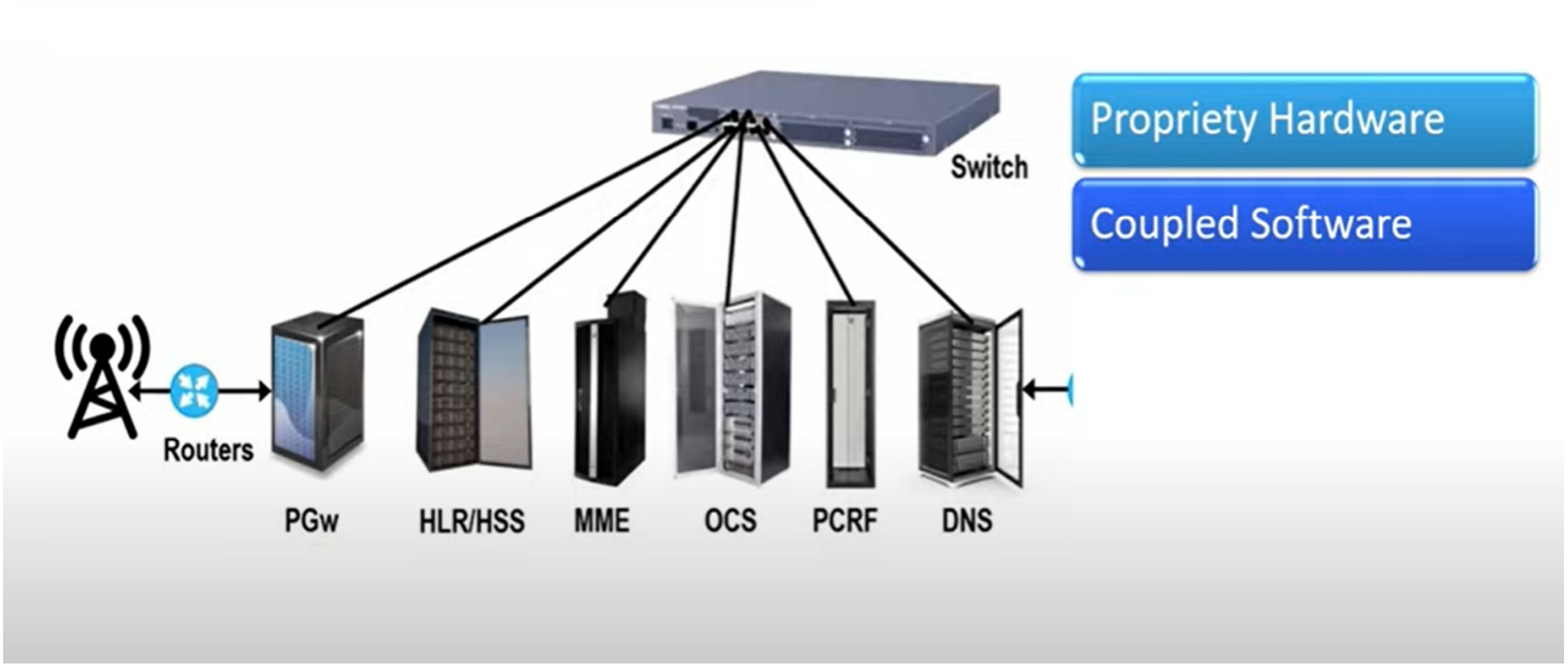
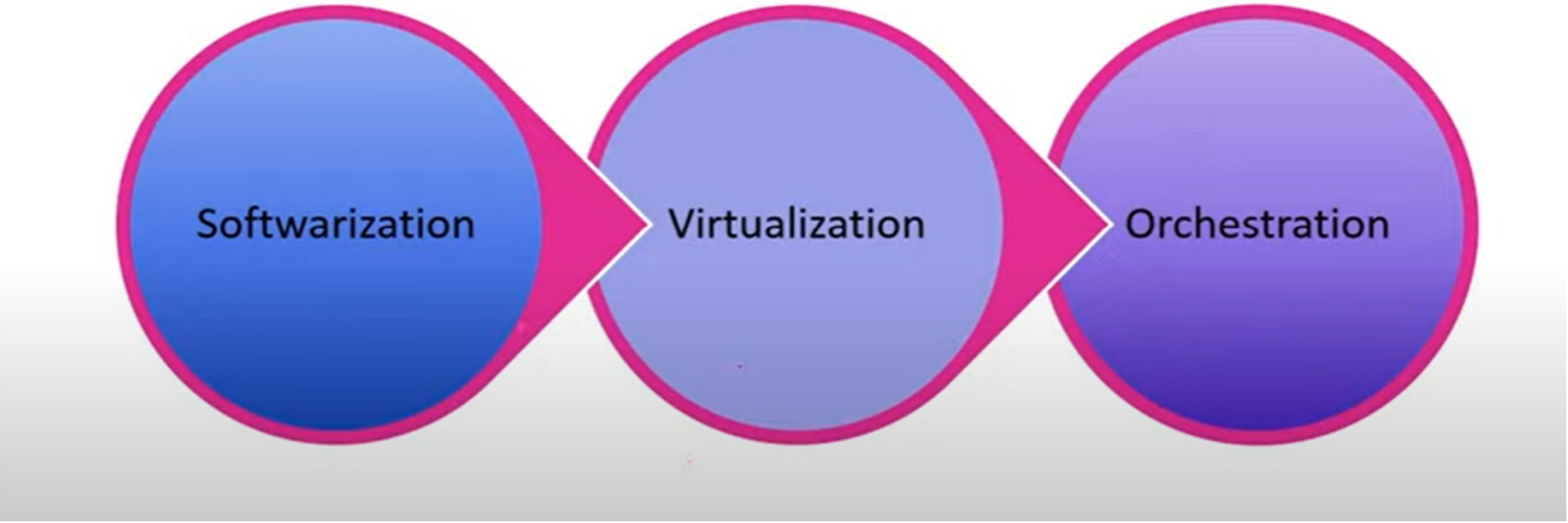
MODULE 5 :
NETWORK FUNCTION VIRTUALIZATION

Before Network Function Virtualization (NFV)



Network Function Virtualization (NFV)



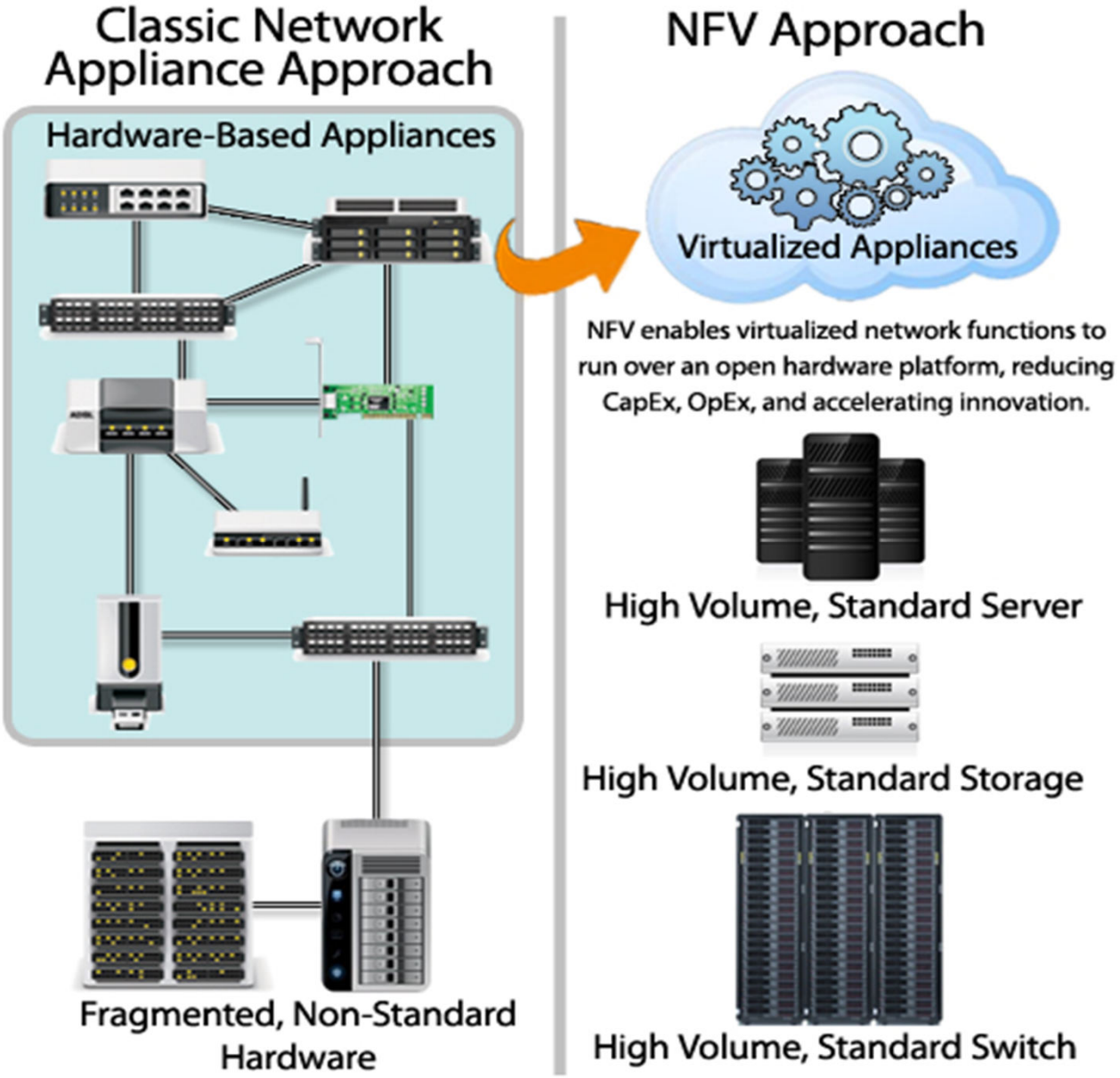
Network Function Virtualization (NFV)

- It is way to reduce cost and accelerate service deployment.
- Instead of installing expensive proprietary hardware, service providers can purchase inexpensive switches, storage and servers to run virtual machines that perform network functions.
- This collapses multiple functions into a single physical server, reducing costs and minimizing truck rolls.
- If a customer wants to add a new network function, the service provider can simply spin up a new virtual machine to perform that function.
- This virtualization of network functions reduces dependency on dedicated hardware appliances for network operators, and allows for improved scalability and customization across the entire network.
- Different from a virtualized network, NFV seeks to offload network functions only, rather than the entire network.

Network Function Virtualization (NFV)

- Purpose Built Hardware to generic Hardware
- Network Function functioning as Software
- Network Function and Capacity are separated
- Easy Scale Up and Scale Down
- VM/Containers becomes the building block

- https://youtu.be/xGZaZTnvR9A
- Refer above url for NFV introduction
- http://www.ciena.com/insights/articles/What-is-NFV-prx.html



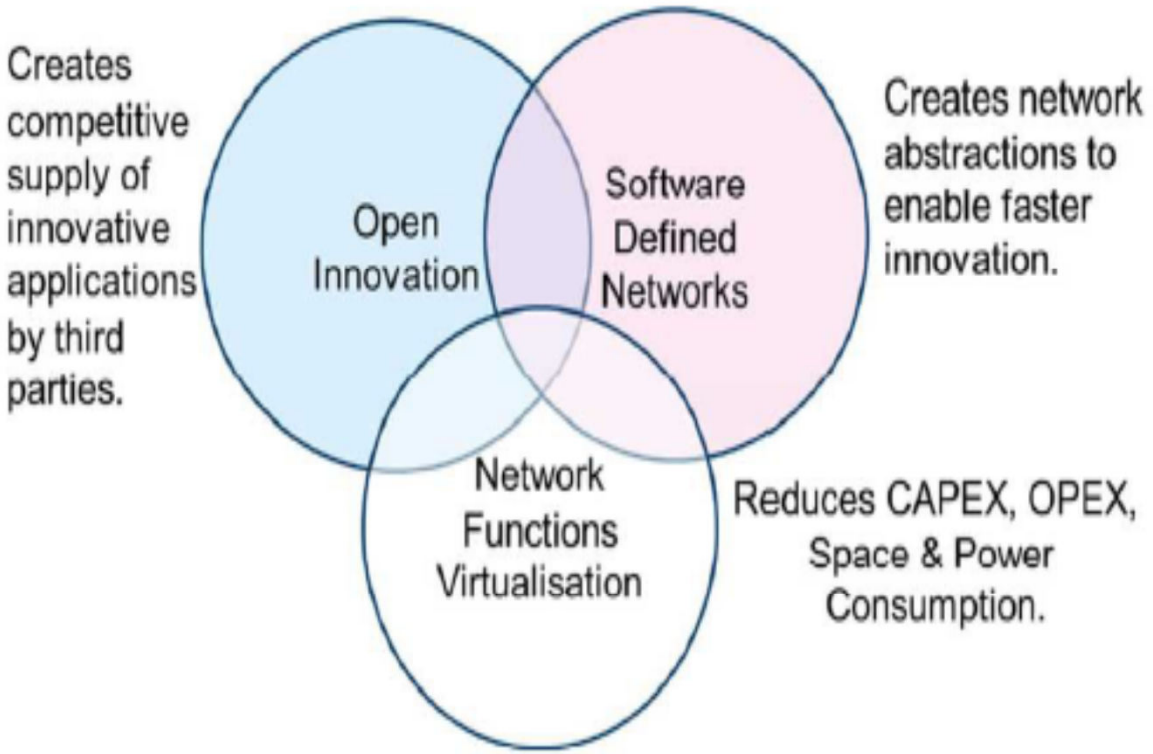


Figure 2: Network Functions Virtualisation Relationship with SDN (Source: ETSI)

Why We need NFV?

1. **Virtualization**: Use network resource without worrying about where it is physically located, how much it is, how it is organized, etc.
2. **Orchestration**: Manage thousands of devices
3. **Programmable**: Should be able to change behavior on the fly.
4. **Dynamic Scaling**: Should be able to change size, quantity
5. **Automation**
6. **Visibility**: Monitor resources, connectivity
7. **Performance**: Optimize network device utilization
8. **Multi-tenancy**
9. **Service Integration**
10. **Openness**: Full choice of Modular plug-ins

What network functions are being virtualized?

- The following network functions are being virtualized:
- **Security**
  - Firewall
  - Antivirus
  - DDoS (Distributed Denial of Service)
  - IPS/IDS (Intrusion Prevention System/Intrusion Detection System)
- **Application/WAN optimizers**
- **Edge**
  - Site-to-site gateway
  - L3 gateways
  - Routers
  - Switches
  - NAT
  - Load balancers (not necessarily at the edge)
  - HTTP proxy

What are the advantages of NFV?

- NFV reduces the need for dedicated hardware
- Separating network functions from hardware yields numerous benefits for the network operator, which include:
  - Reduced space needed for network hardware
  - Reduce network power consumption
  - Reduced network maintenance costs
  - Easier network upgrades
  - Longer life cycles for network hardware
  - Reduced hardware costs

- A virtualized network function, or VNF, may consist of one or more virtual machines running different software and processes, on top of standard high-volume servers, switches and storage devices, or even cloud computing infrastructure, instead of having custom hardware appliances for each network function.
- For example, a virtual session border controller could be deployed to protect a network without the typical cost and complexity of obtaining and installing physical network protection units. Other examples of NFV include virtualized load balancers, firewalls, intrusion detection devices and WAN accelerators.

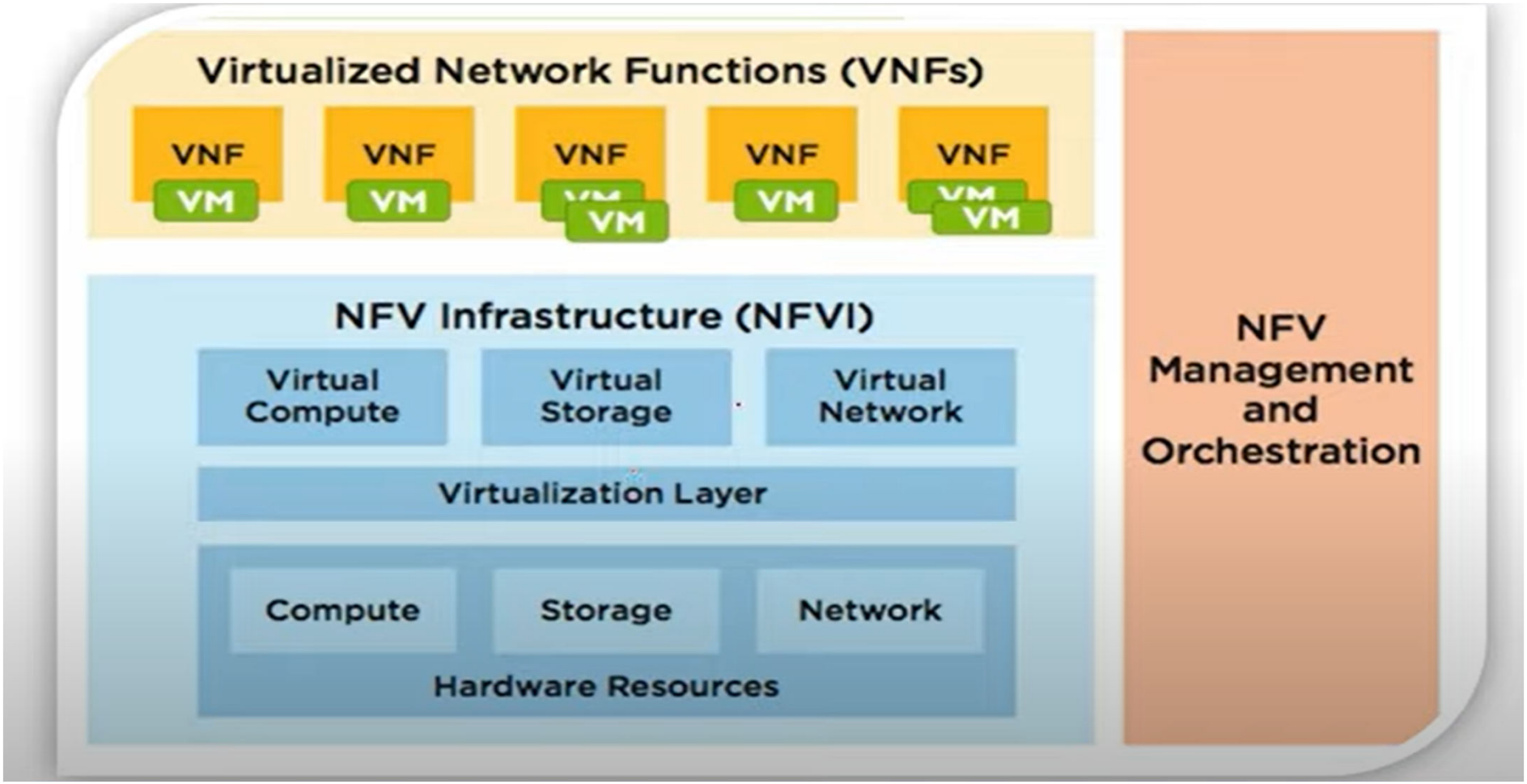
NFV Framework

- The NFV framework consists of three main components:

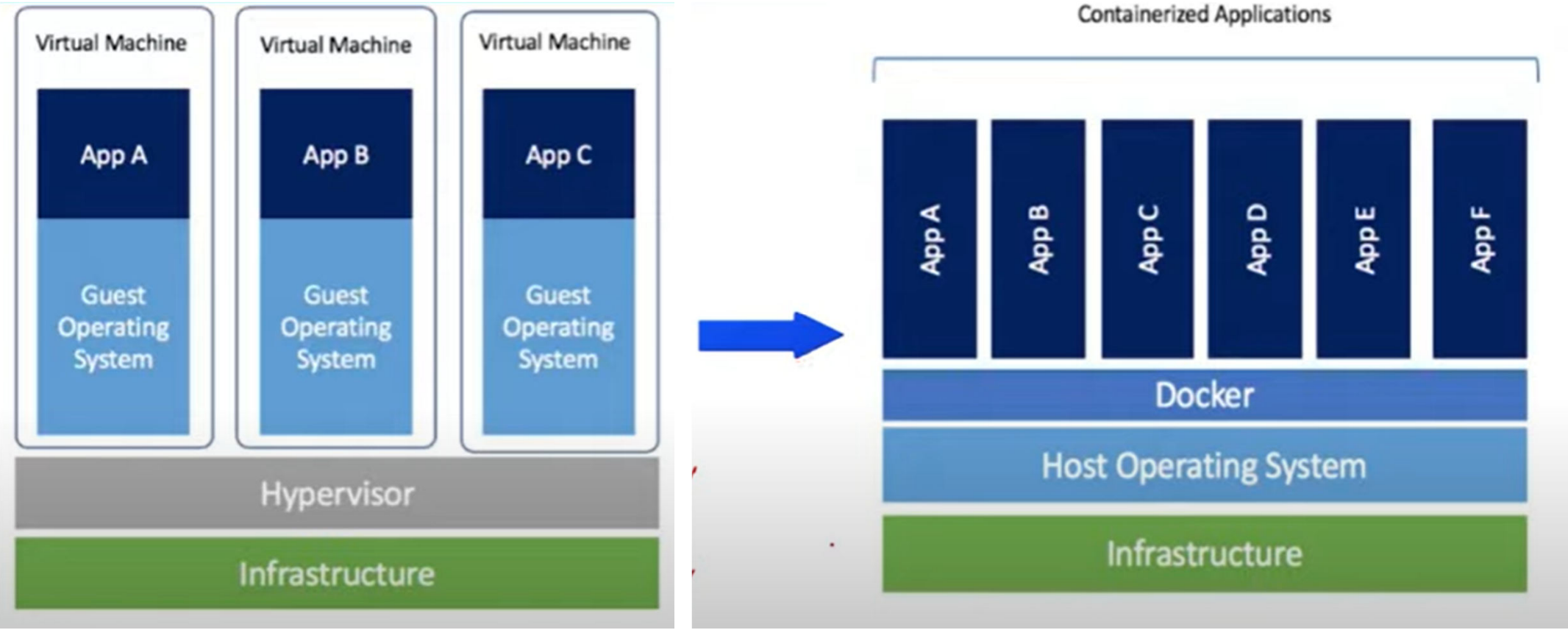
1. Virtualized network functions (VNFs) are software implementations of network functions that can be deployed on a network functions virtualization infrastructure (NFVI).
2. NFVI is the totality of all hardware and software components that build the environment where VNFs are deployed. The NFVI can span several locations. The network providing connectivity between these locations is considered as part of the NFV infrastructure.
3. Network functions virtualization management and orchestration architectural framework (NFV-MANO Architectural Framework) is the collection of all functional blocks, data repositories used by these blocks, and reference points and interfaces through which these functional blocks exchange information for the purpose of managing and orchestrating NFVI and VNFs.

- The building block for both the NFVI and the NFV-MANO is the NFV platform.
- In the NFVI role, it consists of both virtual and physical processing and storage resources, & virtualization software. In its NFV-MANO role it consists of VNF and NFVI managers and virtualization software operating on a hardware controller.
- The NFV platform implements carrier-grade features used to manage & monitor the platform components, recover from failures and provide effective security, all required for the public carrier N/W.

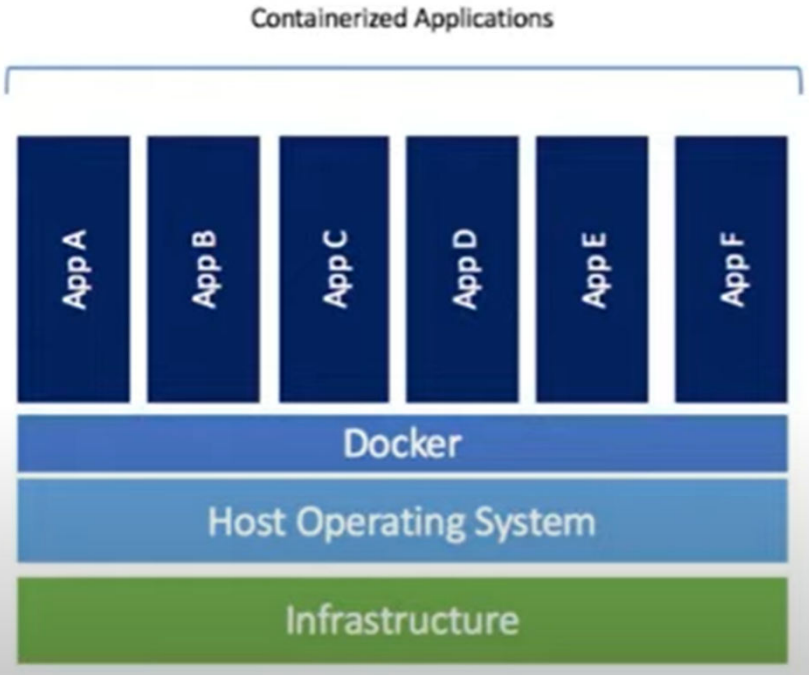
NFV Framework



NFV VMs Vs Container



Why Container



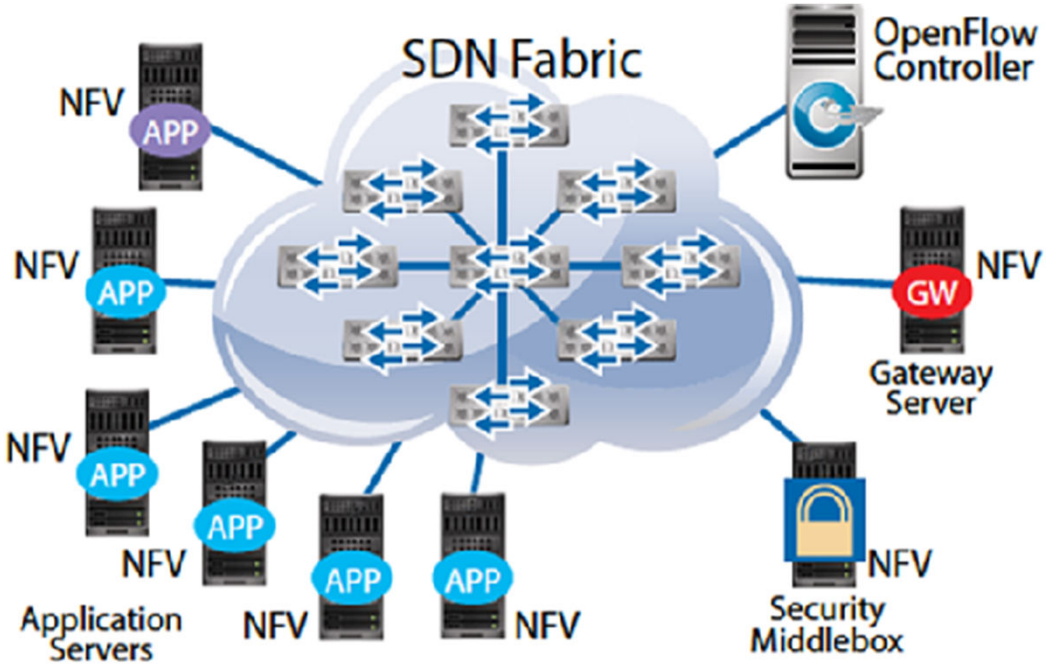
- More efficient use of system **resources**.
- Faster software delivery cycles.
- Application portability.
- Enables microservices architecture.

NFV & SDN

- Network functions virtualization and software-defined networking are two closely related technologies that often exist together, but not always.
- NFV and SDN are both moves toward network virtualization and automation, but the two technologies have different goals.
- An SDN can be considered a series of network objects -- such as switches, routers and firewalls -- that are deployed in a highly automated manner.
- The automation may be achieved by using commercial or open-source tools -- like SDN controllers and OpenFlow-- based on the administrator's requirements.
- A full software-defined network may cover only relatively straightforward networking requirements, such as VLAN and interface provisioning.

- In many cases, SDN will also be linked to server virtualization, providing the glue that sticks virtual networks together.
- This may involve NFV, but not necessarily.
- NFV is the process of moving services like load balancing, firewalls and intrusion prevention systems away from dedicated hardware into a virtualized environment.
- This is, of course, part of a wider movement toward the virtualization of applications and services.
- Functions like caching and content control can easily be migrated to a virtualized environment, but won't necessarily provide any significant reduction in operating costs until some intelligence is introduced.
- This is because a straight physical to virtual, from an operational perspective, achieves little beyond the initial reduction in power and rack-space consumption.
- Until some dynamic intelligence is introduced with an SDN technology, NFV network deployments inherit many of the same constraints as traditional hardware appliance deployments, such as static, administrator-defined and managed policies.

- A good example is virtualized application delivery controllers (ADCs).
- With careful configuration, it is possible to react to the network state and spin up or down application servers as demands rise and fall.
- Traditional hardware deployments have been able to do this for a while, however, and the configuration is very static; it doesn't cater to the scenario where the ADC itself becomes overloaded, or an additional application needs to be brought into production quickly.

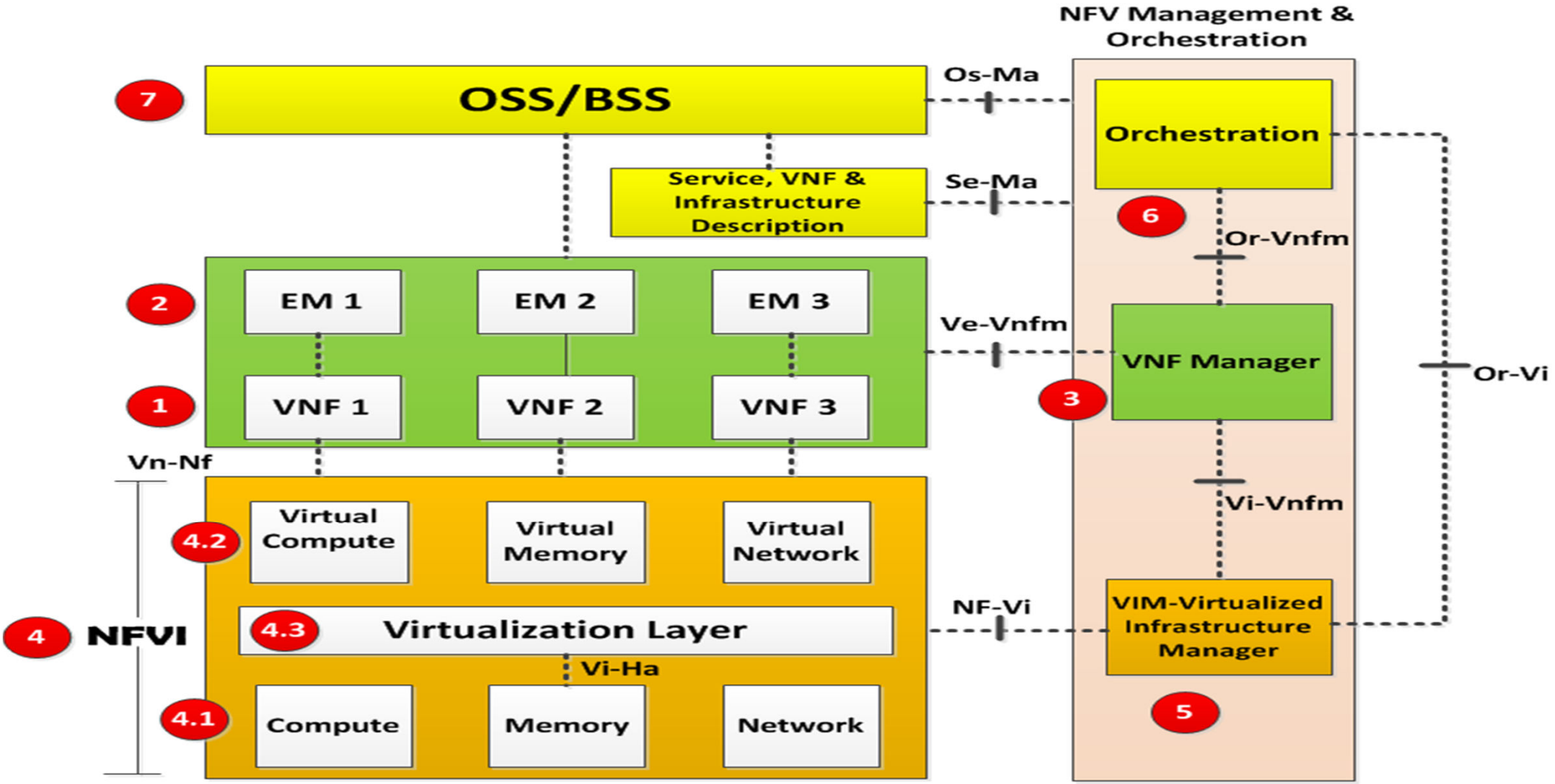


How SDN and NFV work together

- With SDN features driving an NFV network, several useful things start to happen.
- The virtual overlay created by SDN helps provision and manage the virtual network functions with NFV.
- SDN also helps manage traffic loads more efficiently, so the network can react when things need to change at micro and macro levels.
- An additional instance can be provisioned in a cluster of virtualized ADCs as the load increases, and production applications can easily be cloned and redeployed in a development environment.
- The potential for SDN and NFV is endless.
- So, it's perfectly possible to have NFV without the inclusion of a full-blown software-defined network.
- Still, NFV and SDN are often deployed together, and a software-defined network that drives NFV is a very powerful combination.

- Neither NFV nor SDN are turnkey services in early 2014 -- a great deal of integration and policy design still need to happen.
- Standards work for both SDN and NFV network architectures is still ongoing, and the two technologies need more proven deployments.
- But while the harness is not entirely in place, NFV and SDN can become a reality for many enterprises.
- That said, the tools are rapidly evolving, and many vendors are bringing technologies to market that support SDN or NFV deployments.
- Ultimately, the implementation of either or both technologies will be driven by the business needs.

NFV ARCHITECTURE



1. VNF (Virtual Network Function):

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

2. EM (Element Management):

- This is the element management system for VNF.
- This is responsible for the functional management of VNF i.e. FCAPS (Fault, Configuration, Accounting, Performance and Security Management).
- This may manage the VNFs through proprietary interfaces. There may be one EMS per VNF or an EMS can manage multiple VNFs. EMS itself can be a VNF.

3. VNF Manager:

- A VNF Manager manages a VNF or multiple VNFs i.e. it does the life cycle management of VNF instances.
- Life cycle management means setting up/ maintaining and tearing down VNFs.
- Additionally VNFM (VNF Manager) does the FCAPS for the virtual part of the VNF.
- The difference between EM and VNFM should be noted.
- EM does the management of functional components.
- While the VNFM does the management for the virtual components.
- An example would make it clear. In case where Mobile core is virtualized, the EM will do the management of the functional part (for example issues related to mobile signaling), while VNFM will do the management for the virtual part (for example issues related to bringing up an VNF itself)

4. NFVI (Network Function Virtualization Infrastructure):

- NFVI is the environment in which VNFs run.
- This includes Physical resources, virtual resources and virtualization layer, described below.

4.1 Compute, Memory and Networking Resources:

- This is the physical part in NFVI. Virtual resources are instantiated on these physical resources. Any commodity switch or physical server/storage server is part of this category.

4.2 Virtual Compute, Virtual Memory and Virtual Networking Resources:

- This is the virtual part in NFVI. The physical resources are abstracted into virtual resources that are ultimately utilized by VNFs.

4.3 Virtualization Layer:

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

5. VIM (Virtualized Infrastructure Manager):

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

6. NFV Orchestrator:

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

7. OSS/BSS(Operation Support System/Business Support System)

- OSS/BSS refers to OSS/BSS of an operator.
- OSS deals with network management, fault management, configuration management and service management.
- BSS deals with customer management, product management and order management etc.
- In the NFV architecture, the current BSS/OSS of an operator may be integrated with the NFV Management and Orchestration using standard interfaces.

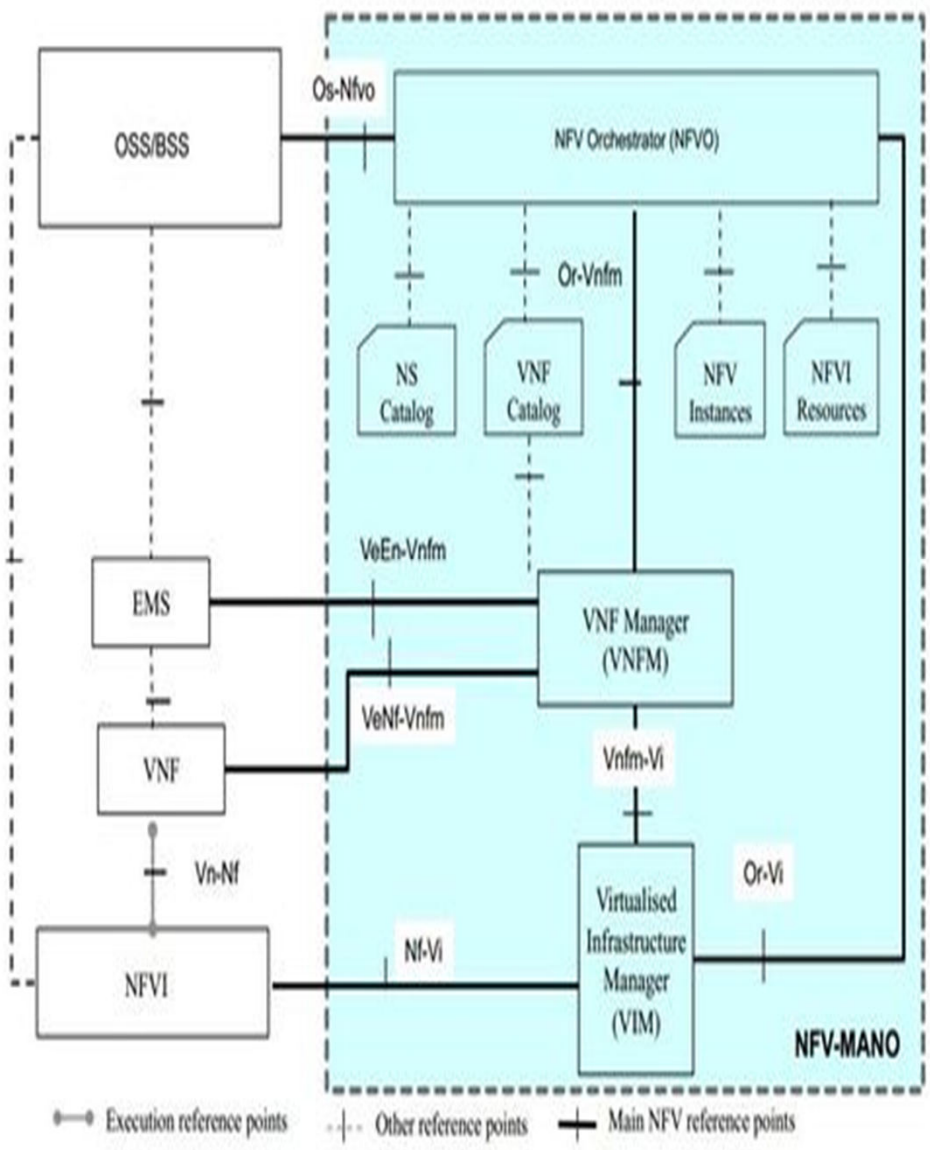
NFV MANO - MANAGEMENT AND ORCHESTRATION

- Having the ability to spin up network components in matter of hours instead of months, allows agility, but it can also create chaos!
- Within virtualization and NFV the need for proper management has been highlighted from an early stage.
- It is now being addressed in a formal way by the MANO stream. It's core purpose: allowing agile on-boarding and preventing chaos!

- MANO Functional Blocks:

1. NFV Orchestrator:
   - On-boarding of new Network Service (NS), VNF-FG and VNF Packages NS lifecycle management (including instantiation, scale-out/in, performance measurements, event correlation, termination) global resource management, validation and authorization of NFVI resource requests policy management for NS instances
2. VNF Manager:
   - Lifecycle management of VNF instances overall coordination and adaptation role for configuration and event reporting between NFVI and the E/NMS
3. Virtualized Infrastructure Manager (VIM):
   - Controlling and managing the NFVI compute, storage and network resources, within one operator's infrastructure sub-domain collection and forwarding of performance measurements and events

- Cloud orchestration and management has been around for a long time.
- The way virtualization providers have implemented automation and orchestration identified their strengths!
- For the MANO architecture to be effective, it needs to be integrated with open API's into the existing systems.
- Current OSS/BSS systems will need to be upgraded to allow to inter-operate with the Virtualization framework through the MANO layer.
- As per current automation systems, the NFV MANO layer will work with templates for the standard VNF's.
- Users will be able to request based upon existing catalogs, and choose from the existing NFVI resources to deploy their platform or element.



Fields of Application (examples)

- Application-level optimisation: CDNs, Cache Servers, Load Balancers, Application Accelerators
- Mobile networks: HLR/HSS, MME, SGSN, GGSN/PDN-GW, Base Station, EPC
- Home environment: home router, set-top-box
- Security functions: Firewalls, intrusion detection/protection systems, virus scanners, spam protection
- Tunnelling gateway elements: IPSec/SSL VPN gateways
- Traffic analysis/forensics: DPI, QoE measurement
- Traffic Monitoring, Service Assurance, SLA monitoring, Test and Diagnostics
- NGN signalling: SBCs, IMS
- Converged and network-wide functions: AAA servers, policy control and charging platforms
- Switching elements: BNG, CG-NAT, routers