Ch 4 – VT in Cloud Computing

Contents

- Introduction to Virtualization Technology,
- Hypervisors (ESXi),
- Hypervisor Networks,
- Virtual Machines,
- VM management and configurations,
- Cloud Data stores,
- Cloud Computing and Virtualization,
- Academic Environment and Virtualization.

Introduction to Virtualization

- Virtualization is an abstraction of computer resources. We can access resources in a consistent way before and after abstraction through virtualization. This kind of resource abstraction is not limited by implementation, geographical location or the underlying physical configuration.
- “Virtualization is a technology to run multiple same or different operating systems which is completely isolated from each other.”

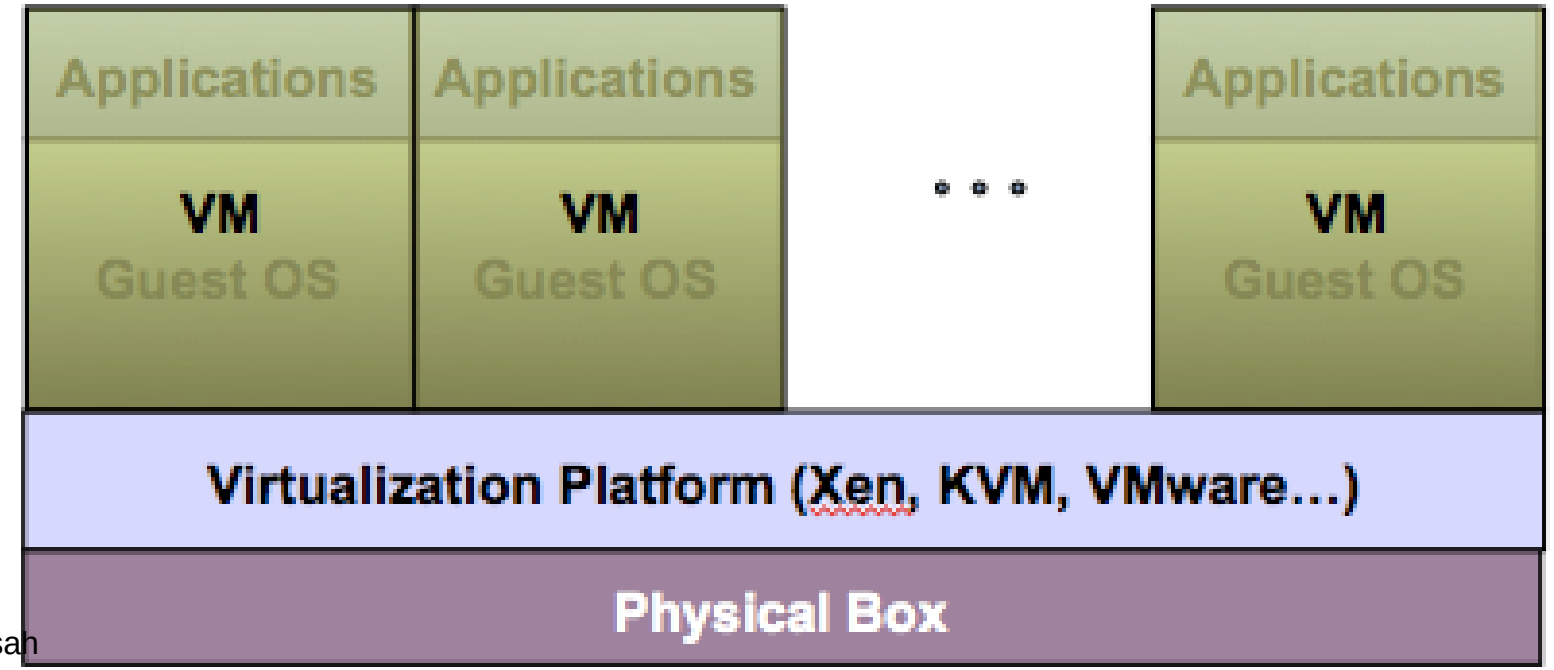
- For Example: Run both Windows and Linux on the same machine

Definition

- Virtualization is the ability to run multiple operating systems on a single physical system and share the underlying hardware resources*
- It is the process by which one computer hosts the appearance of many computers.
- Virtualization is used to improve IT throughput and costs by using physical resources as a pool from which virtual resources can be allocated.

Virtualization Architecture

- A Virtual machine (VM) is an isolated runtime environment (guest OS and applications)
- Multiple virtual systems (VMs) can run on a single physical system



Hypervisor

- A hypervisor, a.k.a. a virtual machine manager/monitor (VMM), or virtualization manager, is a program that allows multiple operating systems to share a single hardware host.
- Each guest operating system appears to have the host's processor, memory, and other resources all to itself. However, the hypervisor is actually controlling the host processor and resources, allocating what is needed to each operating system in turn and making sure that the guest operating systems (called virtual machines) cannot disrupt each other.

Benefits of Virtualization

- Sharing of resources helps cost reduction
- Isolation: Virtual machines are isolated from each other as if they are physically separated
- Encapsulation: Virtual machines encapsulate a complete computing environment
- Hardware Independence: Virtual machines run independently of underlying hardware
- Portability: Virtual machines can be migrated between different hosts.

Virtualization in Cloud Computing

Cloud computing takes virtualization one step further:

- You don’t need to own the hardware
- Resources are rented as needed from a cloud
- Various providers allow creating virtual servers:
  - Choose the OS and software each instance will have
  - The chosen OS will run on a large server farm
  - Can instantiate more virtual servers or shut down existing ones within minutes
- You get billed only for what you used

Virtual Machine Technology

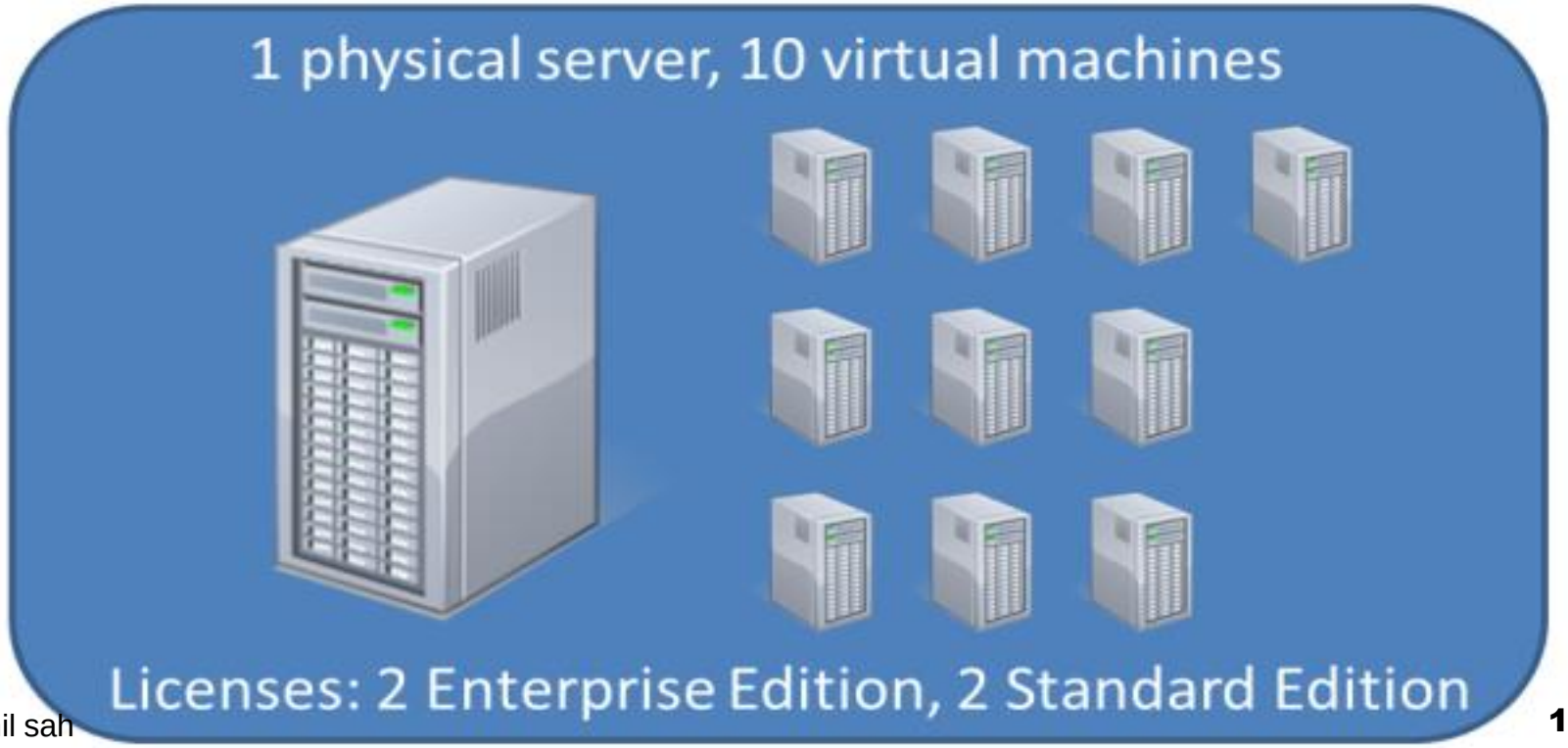
- Virtualization facilitates the providing and management of the dynamic data center's infrastructure
  - An essential and enabling technology of cloud computing environments
  - The abstraction of the four computing resources
    - Storage, processing power, memory, and network or I/O
  - Conceptually similar to emulation
    - A system pretends to be another system
    - Virtualization is a system pretending to be two or more of the same system

Virtual Machine Technology

Virtual Machine

Often called Virtual environment or container. A Virtual machine (VM) is a server environment that does not physically exist but is created within another server .

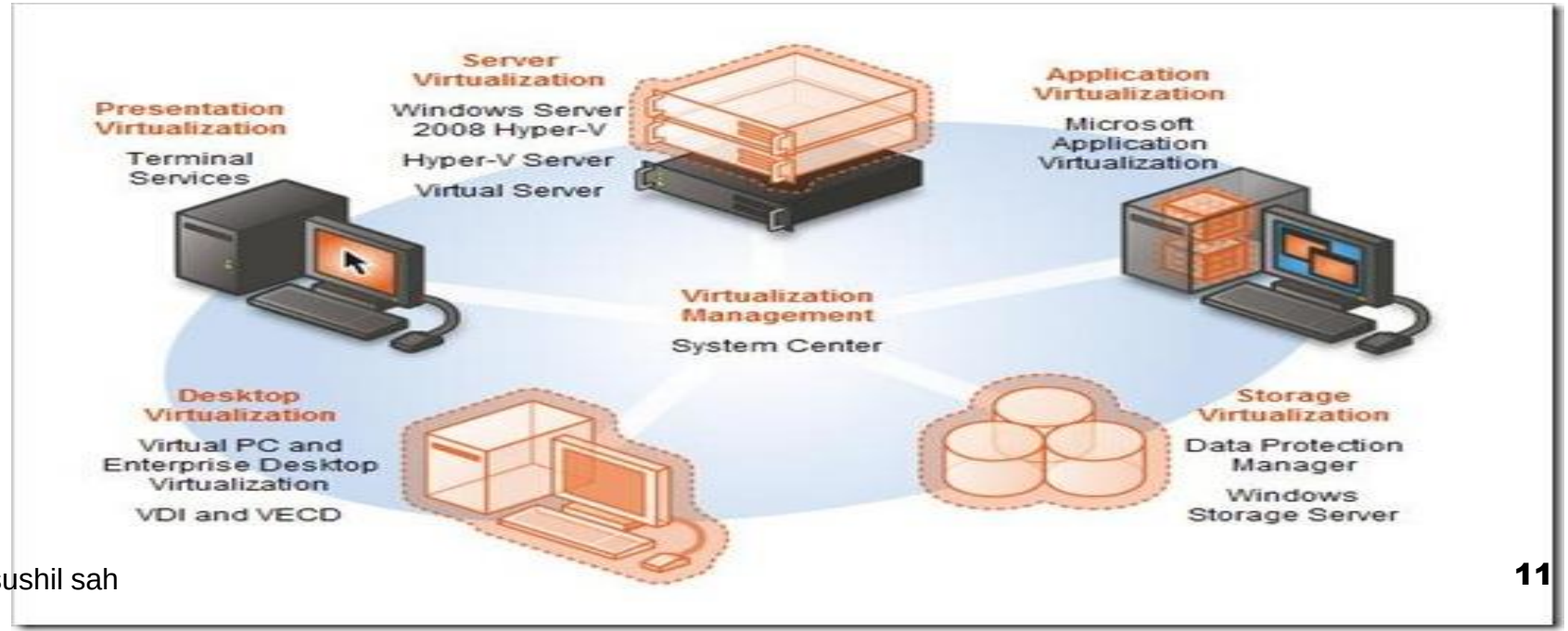
For user interacting with a VM is seen or presented as a physical machine providing access to an operating system and machine resources like CPU



Virtual Machine Technology

Two major types of virtualization technologies widely used are

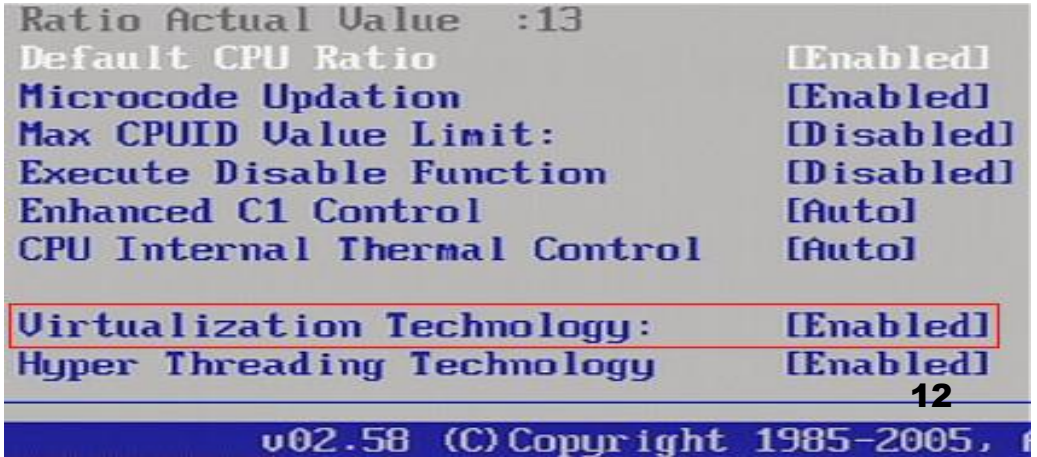
- Hardware Virtualization
  - virtualizes the server hardware
- OS virtualization
  - virtualizes application environment



Virtual Machine Technology

Hardware Virtualization

- Hardware virtualization is also known as Hypervisor based virtualization, bare-metal Hypervisor, TYPE 1 virtualization or simply hypervisors
- It has a virtualization layer running immediately on the hardware, which divides the server machine into several virtual machines or partitions. with guest operating systems running in each of the machines
- This approach provides binary transparency because the virtualization environment products themselves provide transparency to the operating system, and applications and middleware that operate above it
- Examples
  - IBM LPARs
  - Open Source KVM
  - Sun LDoms
  - HP IVM
  - Citrix Xen Server

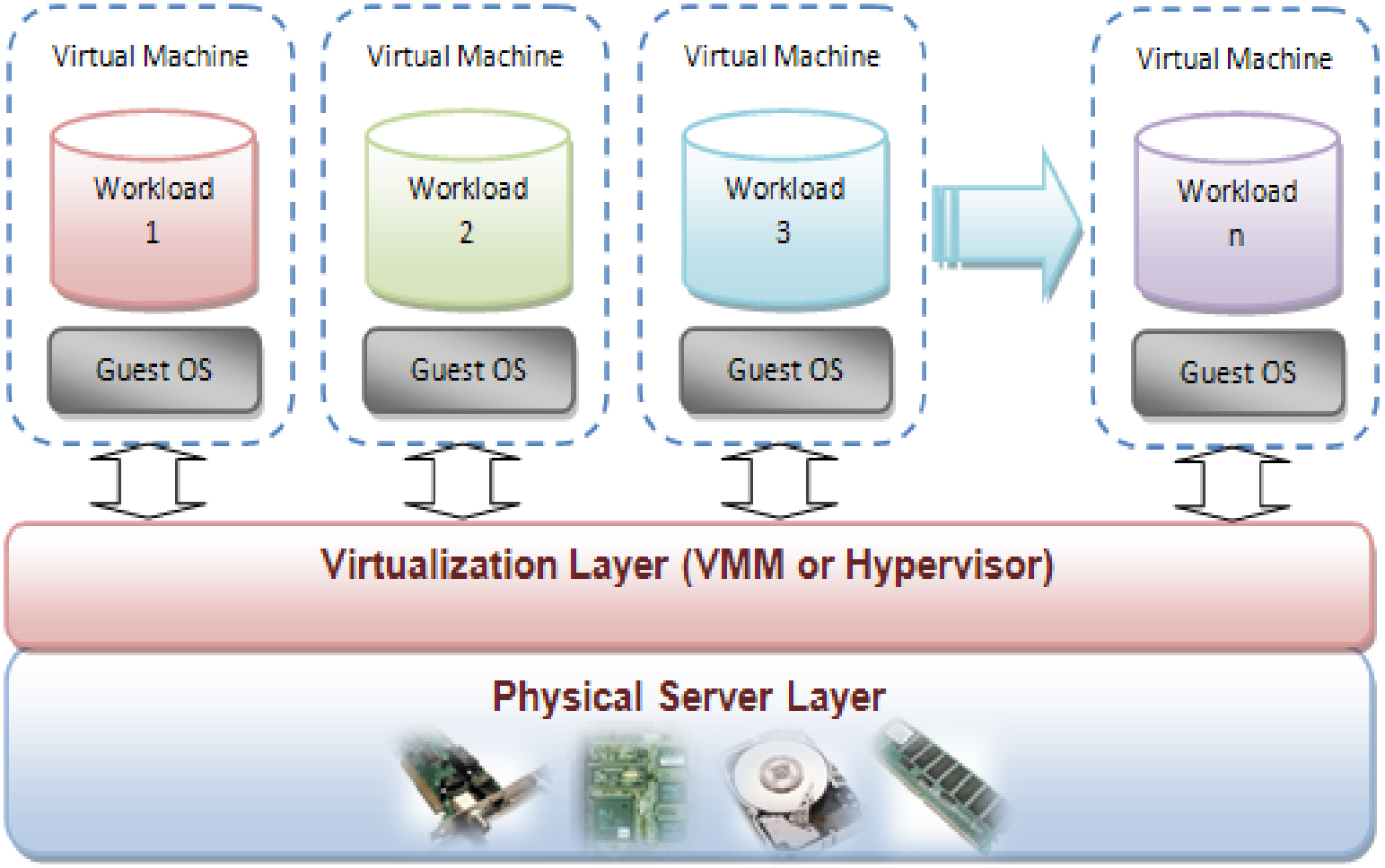


Virtual Machine Technology

OS Virtualization

- OS level virtualization or Type-2 creates virtual environments within a single instance of an operating system.
- These virtual environments created within an OS are called containers

Virtual Machine Technology



Virtual Machine Technology

- A layered virtualization technology architecture
  - The virtualization layer will partition the physical resource of the underlying physical server into multiple virtual machines with different workloads
  - Schedules, allocates the physical resource
  - Makes a virtual machine think it totally owns the whole underlying hardware's physical resource
    - Processor, disks, RAMs, etc.
- Virtual machine's technology manages resources in cloud computing environments

Virtual Machine Technology

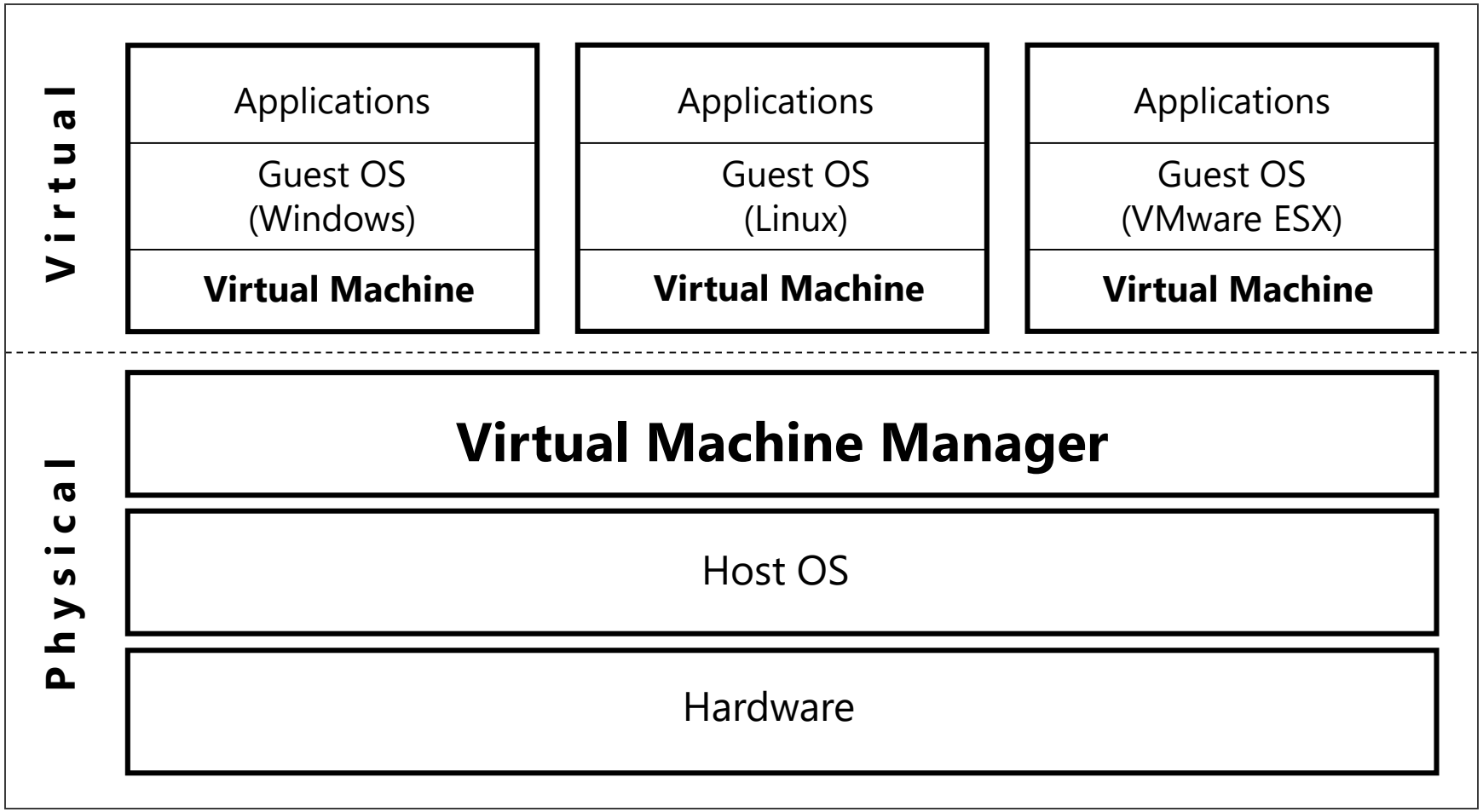
- Improves the utilization of such resources by multiplexing many virtual machines on one physical host
  - Server consolidation
- Machines can be scaled up and down on demand with a high level of resources' abstraction
- Enables high, reliable, and agile deployment mechanisms and management of services
  - Providing on-demand cloning and live migration services which improve reliability

- Having an effective management's suite for managing virtual machines' infrastructure is critical for a cloud computing IaaS vendor

Virtualization Types

- Desktop virtualization
- Network virtualization
- Server and machine virtualization
- Storage virtualization,
- System-level or OS virtualization
- Application virtualization

Desktop Virtualization



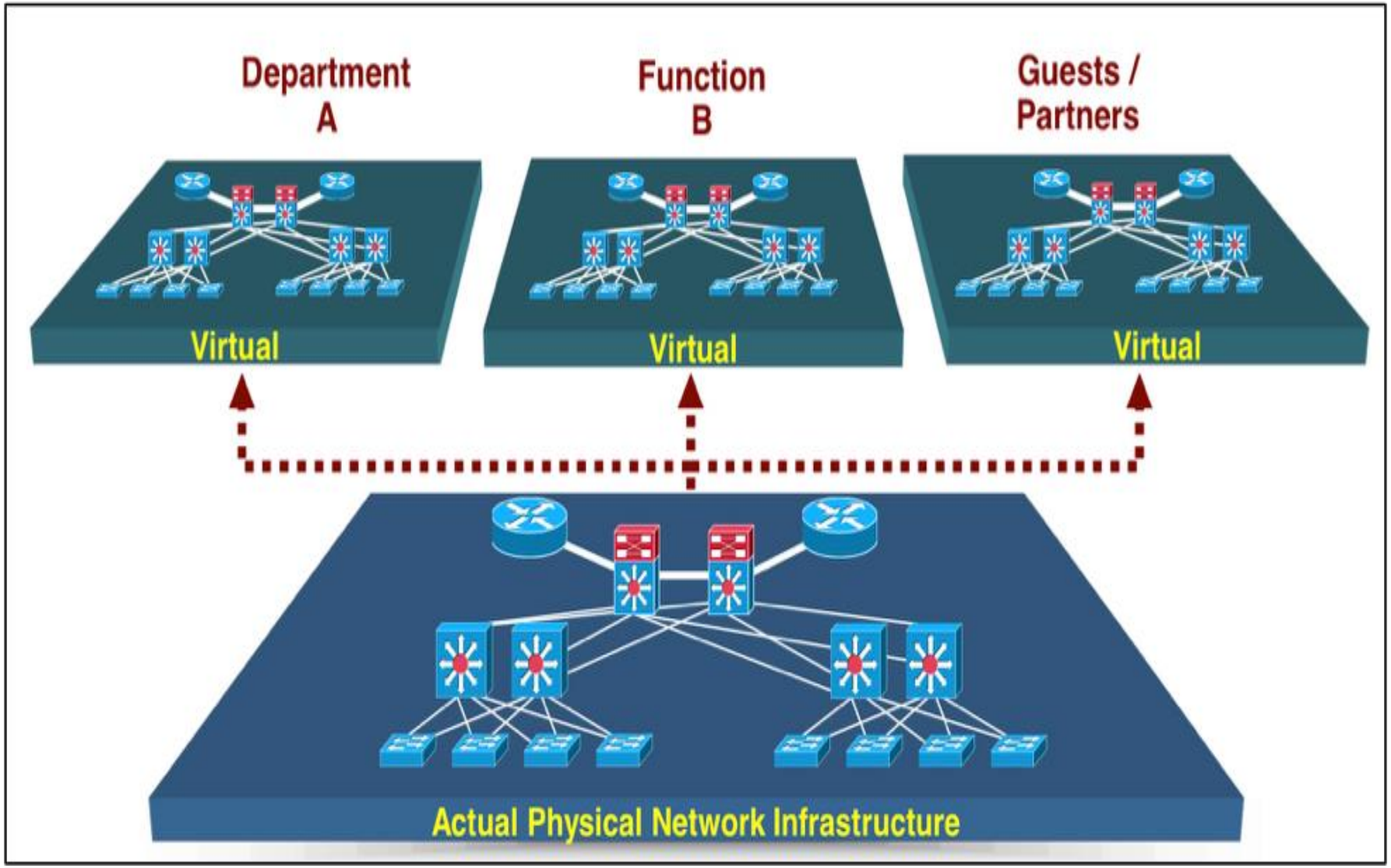
Desktop virtualization

- Same as server Virtualization
- User’s desktop runs on data servers as Virtual machines
- Secured by design
- Multiple OS runs on same Hypervisor host
- Centralized management
- Shared resources with maximum utilization
- Supports multimedia / memory intensive apps on VM .

Network virtualization

- It is the process of combining hardware and software network resources and functionality into a single, software-based administrative entity.
- Creating multiple virtual networks on a physical network.
- Each virtual network has a illusion as it is running as a physical network.
- Virtualizing a network divides the bandwidth into independent channels.

Network virtualization



Need for network virtualization

- Service consolidation

Some services have minimum performance requirement or higher priority.

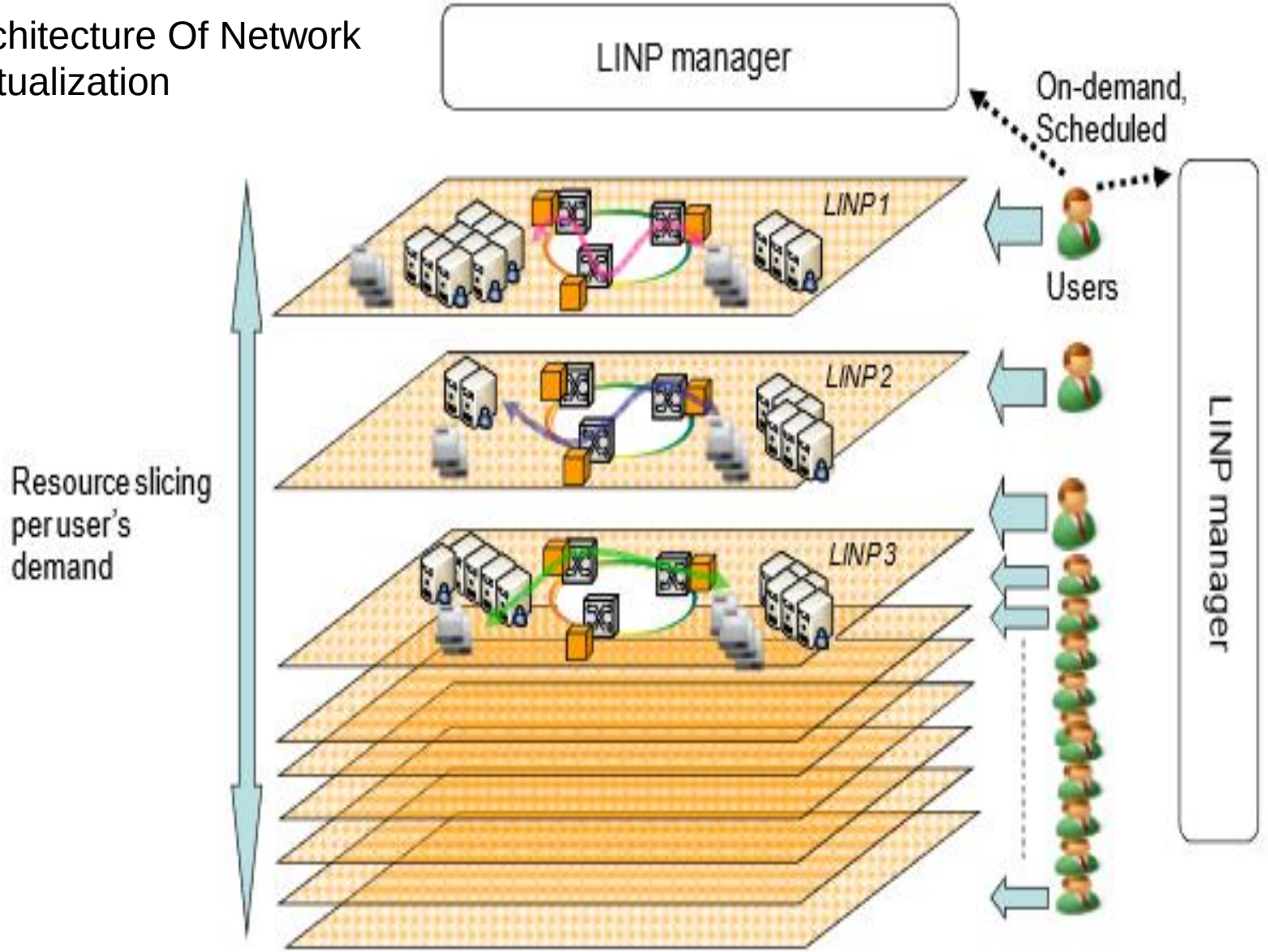
- Host consolidation

Users expect minimum performance level per virtual host.

- Network infrastructure

Network functions need high throughput, scalability and separation.

Architecture Of Network Virtualization



Features Of Network Virtualization

- Partitioning: Network virtualization allows creation of multiple logical network with a programmable control plane.
- Isolation : there is no interference among the virtual networks.
- Abstraction : Network abstraction allows hiding the underlying characteristics of network elements .
- Aggregation : Provide high performance resources for users by logically aggregating multiple resources into single resource

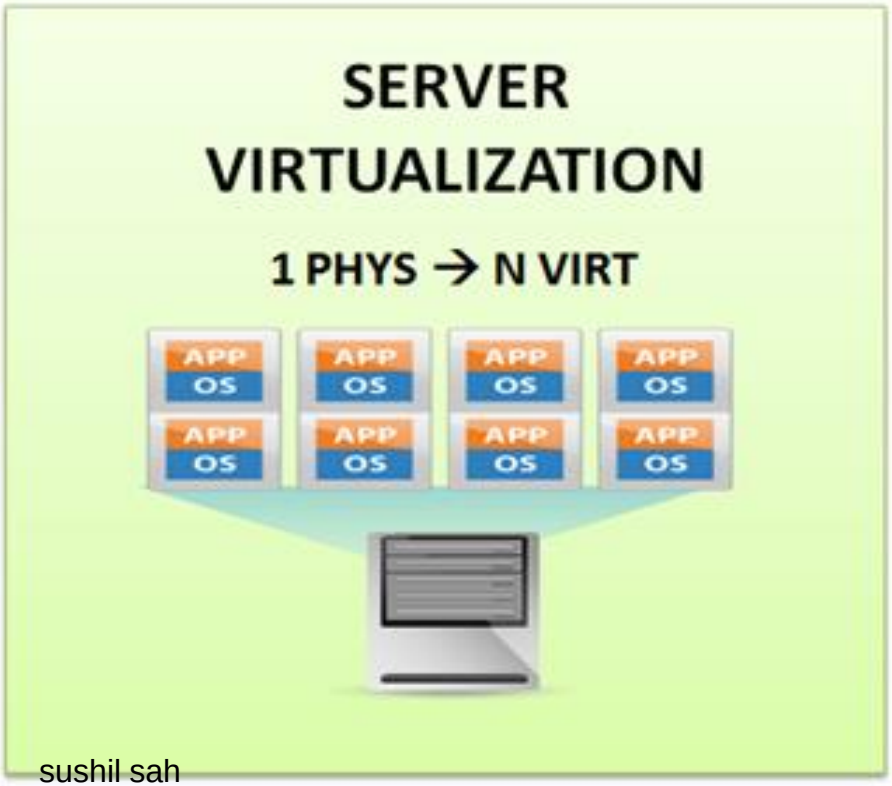
Network virtualization is categorized as

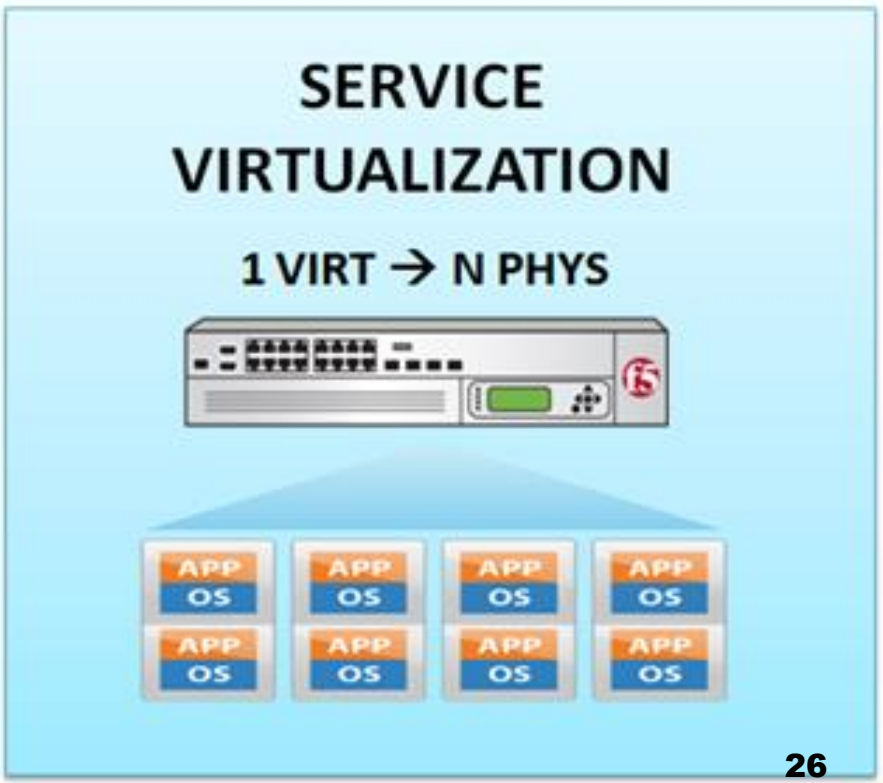
- External network virtualization: combination of multiple networks or parts of networks into a virtual unit.
- Internal network virtualization**:** Provides network-like functionality to software containers on a single network server.

Server and Machine Virtualization

Server virtualization

Server virtualization covers different types of virtualization such as client, storage and network .



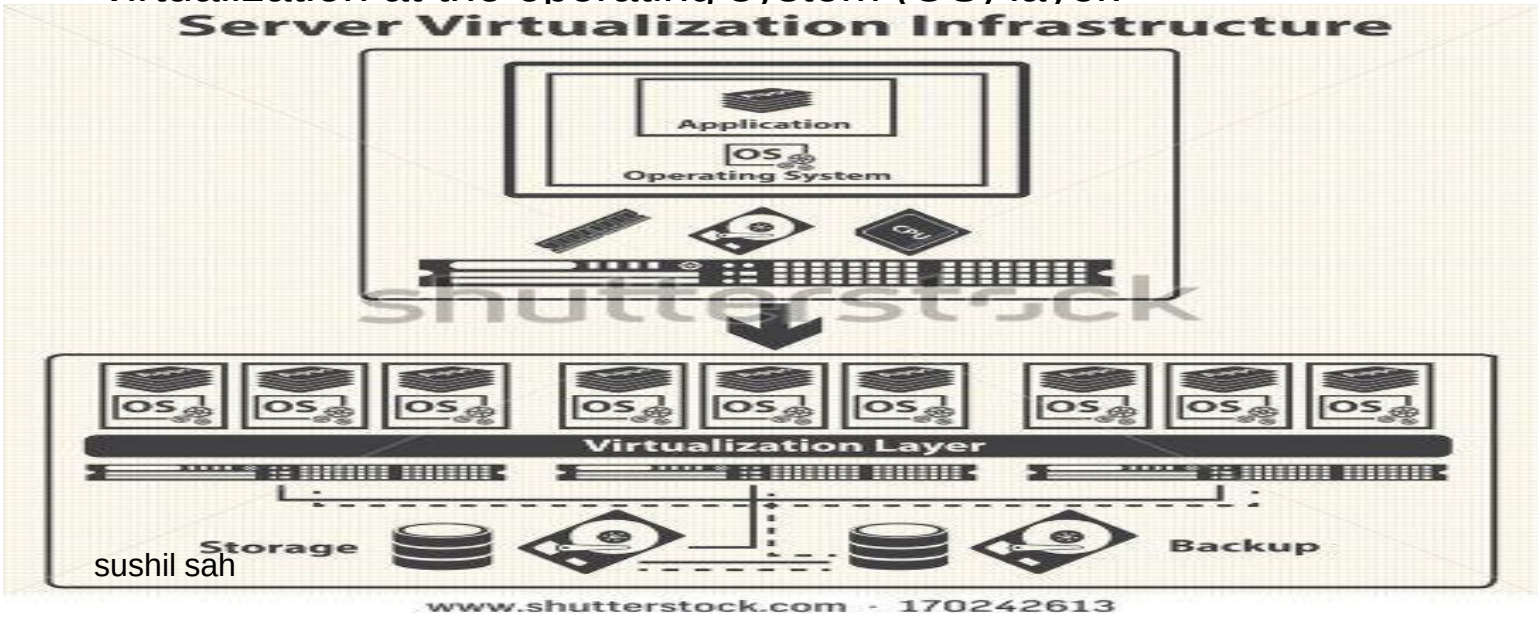


Server and Machine Virtualization

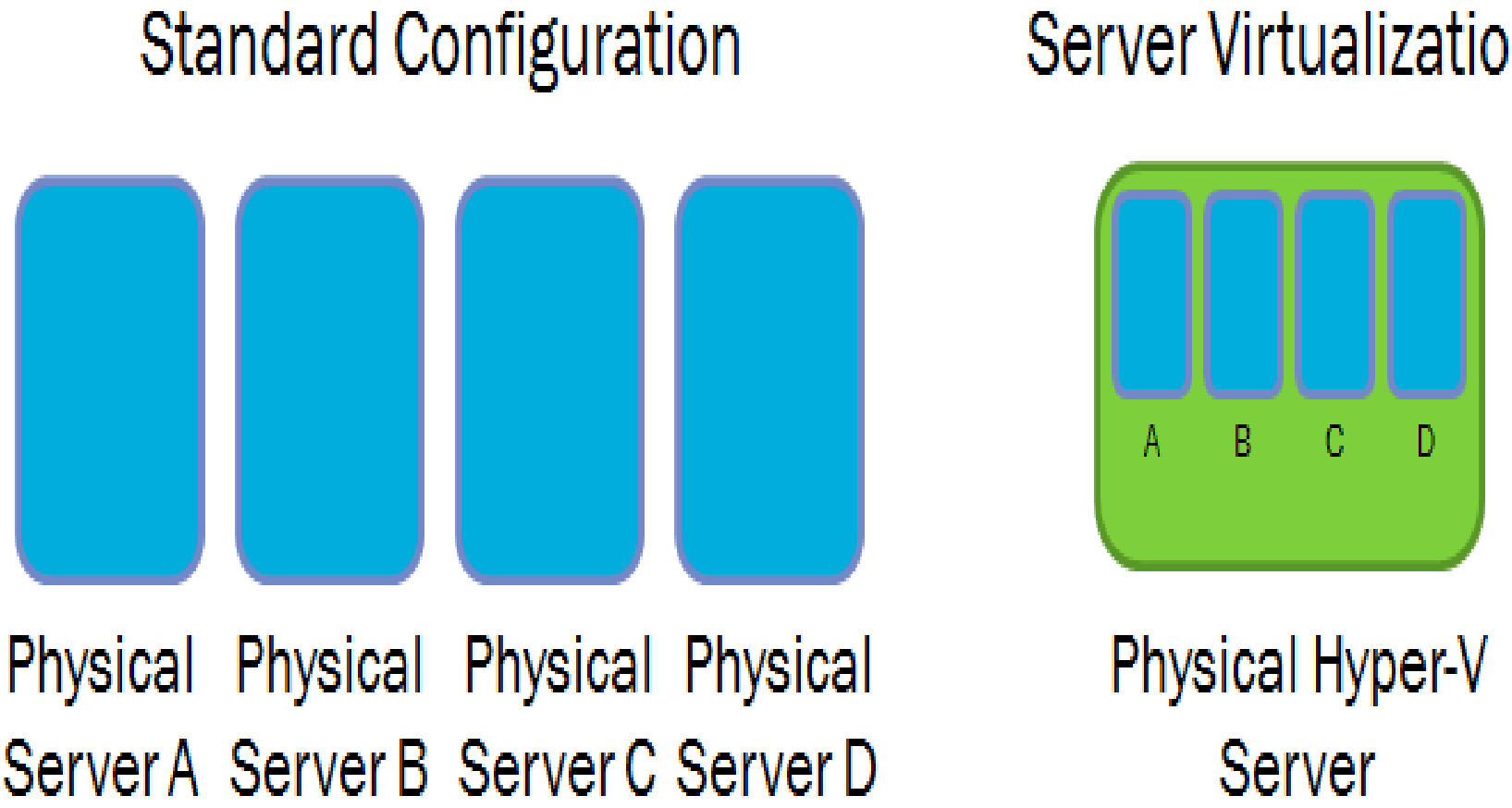
Server virtualization is the **masking of server resources**, including the number and identity of individual physical servers, processors, and operating systems, from server users. The server administrator uses a software application to divide one physical server into multiple isolated virtual environments. The virtual environments are sometimes called virtual private servers, but they are also known as guests, instances, containers or emulations.

There are three popular approaches to server virtualization:

- the virtual machine model,
- the paravirtual machine model, and
- virtualization at the operating system (OS) layer.



Server and Machine Virtualization



Server and Machine Virtualization

- **Benefits**
- Host servers connected over SAN
- Hardware fail tolerance
- High availability
- Online live migration
- Easy management
- Disaster Recovery
- Easily scalable, Adjustable
- Different Vendor, Type, Model servers controlled by Hypervisor
- Less hardware management / maintenance cost
- Better efficiency with less cost
- Maintain average utilization %

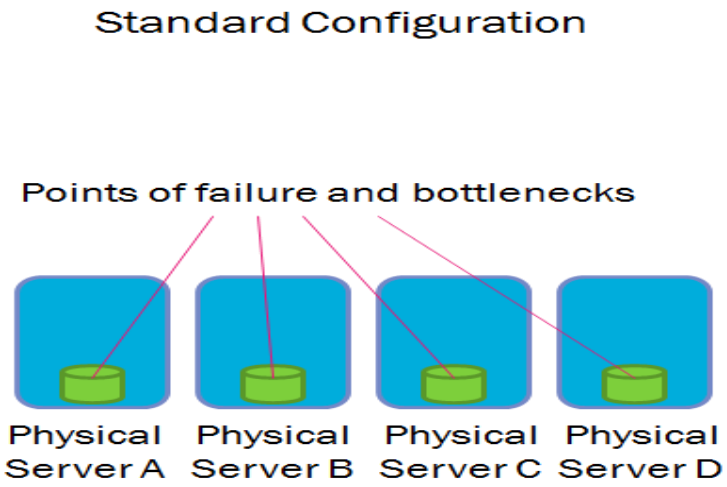
Storage Virtualization

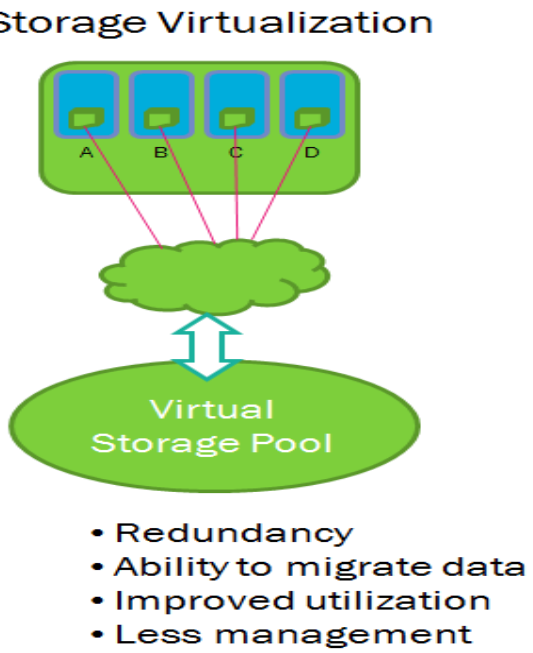
- In **Storage** virtualization, multiple network storage resources are present as a single storage device for easier and more efficient management of these resources. It provides various advantages as follows:
- Improved storage management in a heterogeneous IT environment
- Easy updates, better availability
- Reduced downtime
- Better storage utilization
- Automated management

In general, there are two types of storage virtualization:

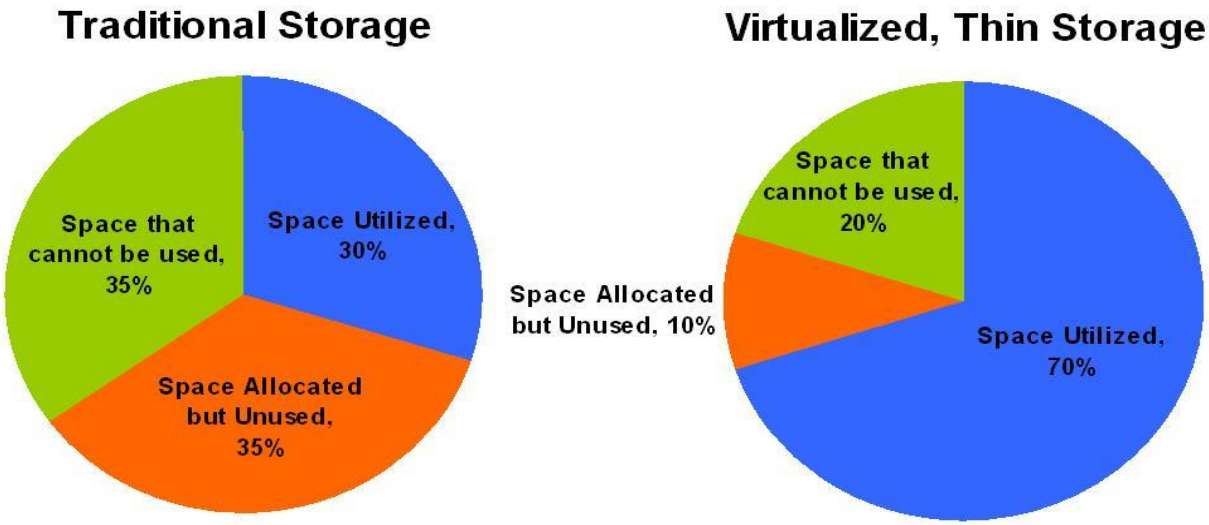
- **Block-** It works before the file system exists. It replaces controllers and takes over at the disk level.
- **File-** The server that uses the storage must have software installed on it in order to enable file-level usage.

Storage Virtualization





- Redundancy
- Ability to migrate data
- Improved utilization
- Less management



Operating System Virtualization

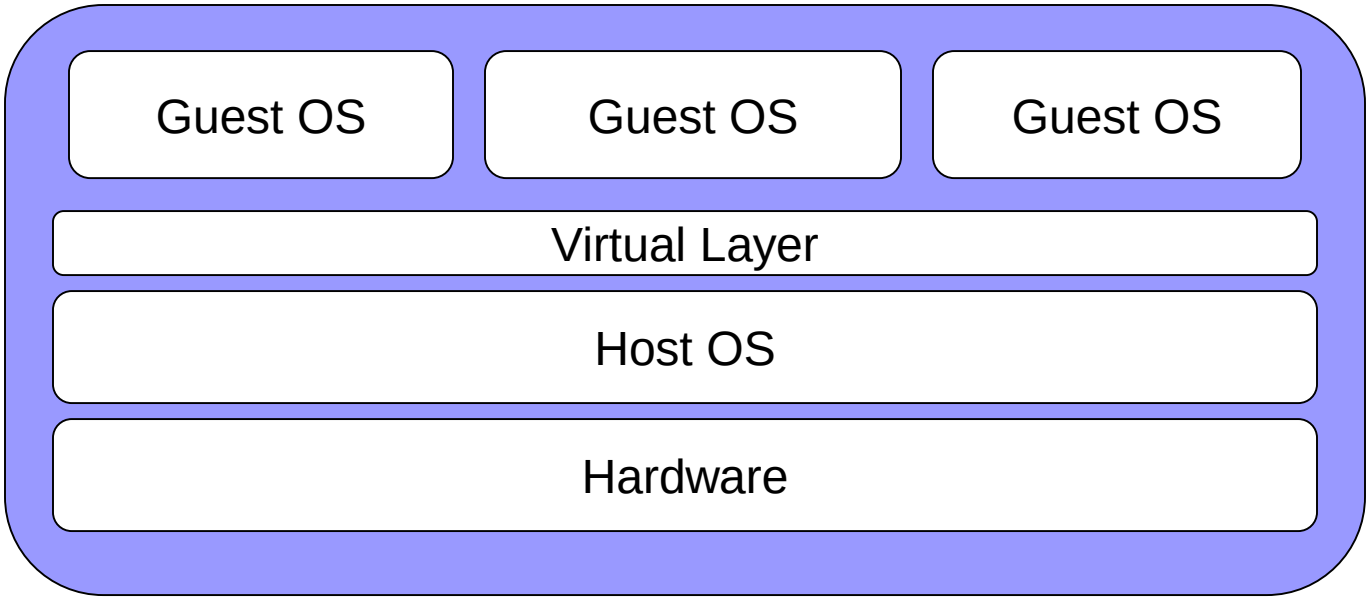
- **OS virtualization**
- OS allows multiple secure virtual servers to be run
- Guest OS is the same as the host OS, but appears isolated
- apps see an isolated OS
- Eg- Solaris Containers, BSD Jails, Linux V server

OS Virtualization

- Definition:
  - Broadly describes the (beneficial) separation of a resource or service from the typical physical means of providing it.
    - Examples:
      - Virtual Memory
      - Virtual Private Networks
      - Java Virtual Machine

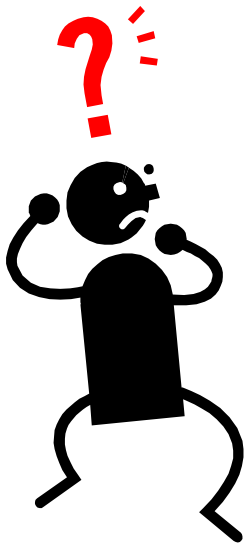
Virtualization

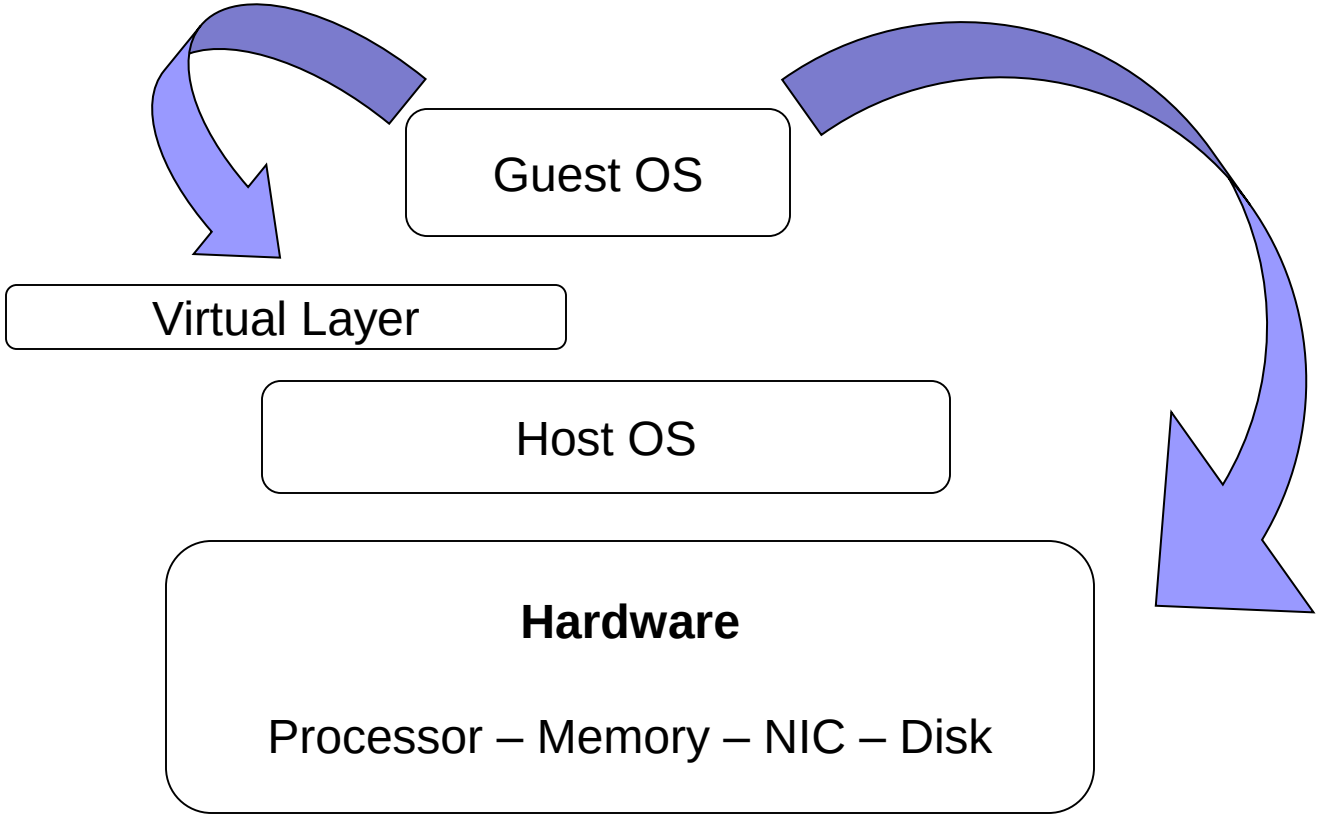
- OS Virtualization (Virtual Machines)
  - Separate OS from Physical Hardware
  - Host OS → Guest OS



OS Virtualization

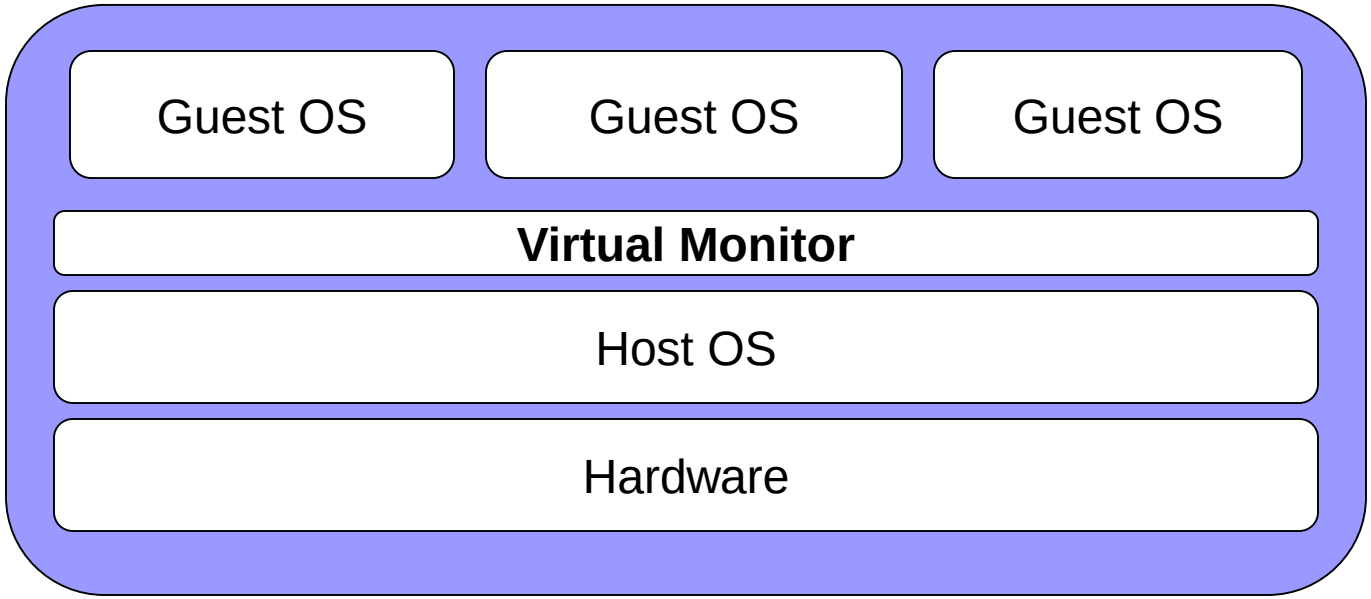
- How does Guest OS get to Hardware?





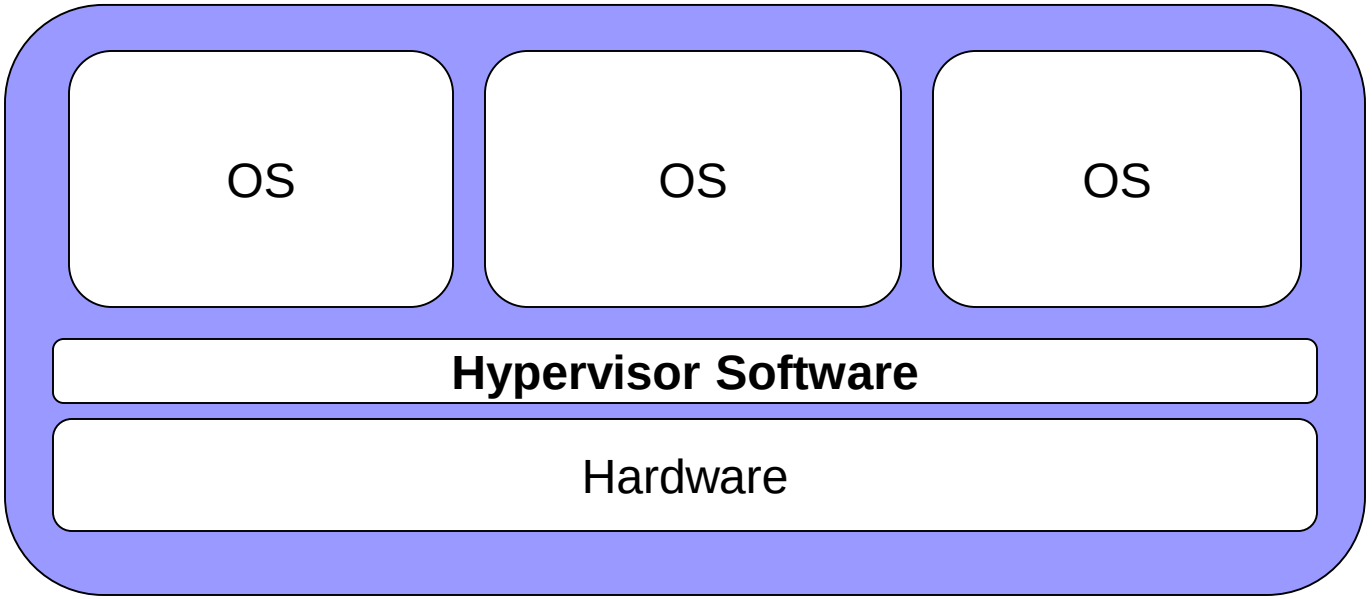
Virtualization Techniques

- Virtual Monitor
  - Qemu, Vmware Player, Microsoft Virtual PC
  - Sometimes called Emulation, e.g. x86 Emulation



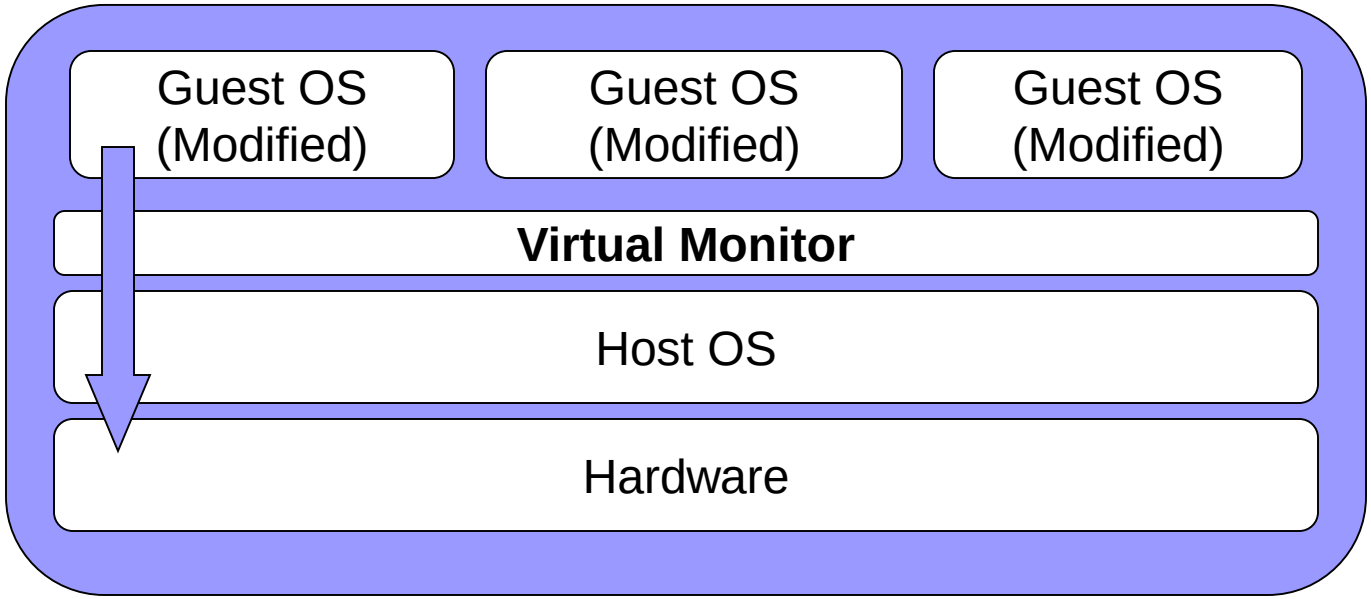
OS Virtualization

- Hypervisor
  - Vmware ESX Server, Parallels*



Virtualization Techniques

- Para-Virtualization
  - Xen, Vmware Tools*



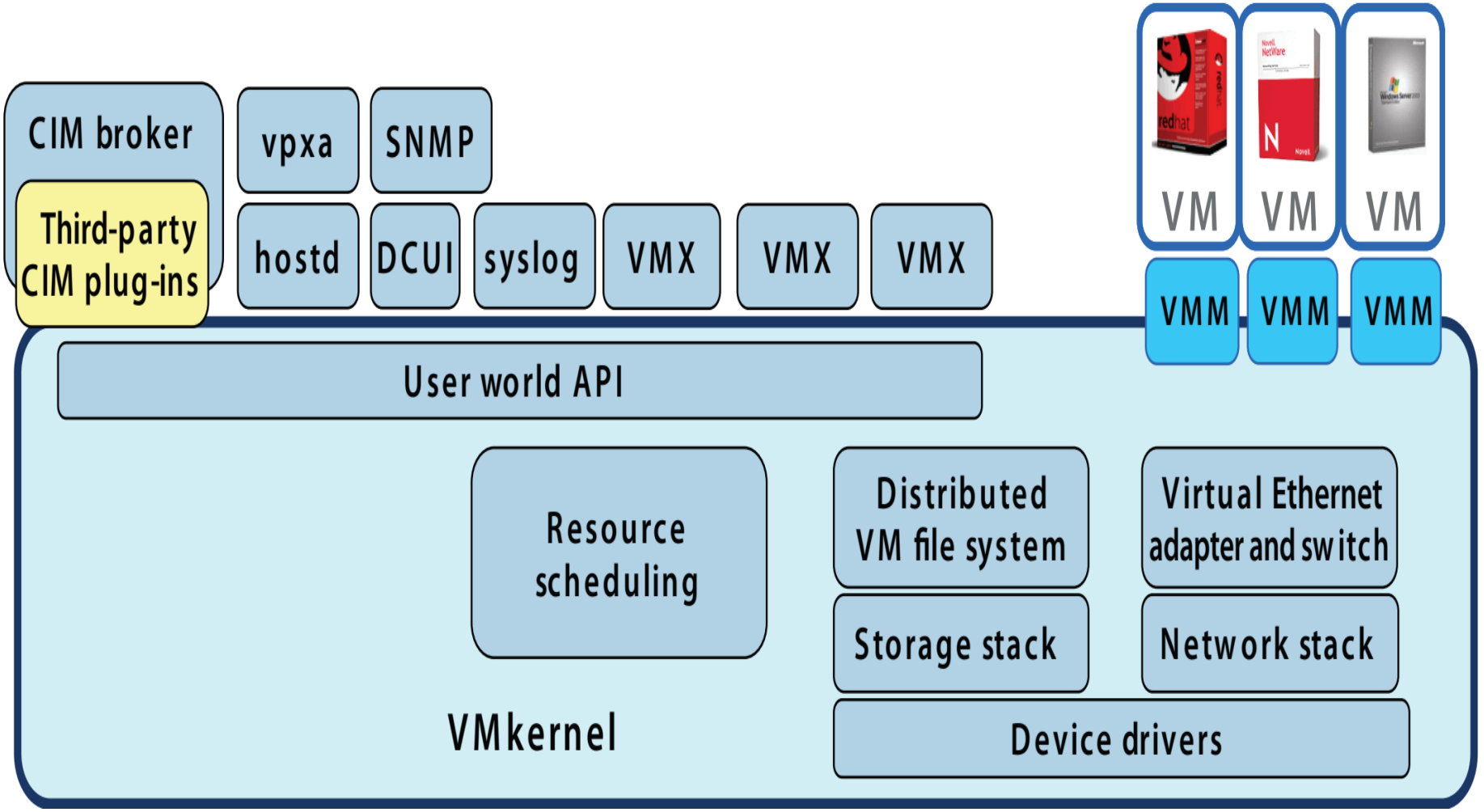
Hypervisors (ESXi)

- ESXi is the next-generation hypervisor, providing a new foundation for virtual infrastructure.
- ESX supports the Virtual Machine File System, Virtual Center, VMotion,Distributed Resource Scheduler, High Availability, Consolidated Backup.
- ESXi architecture comprises the underlying operating system, called Vmkernel (customized kernel for hypervisor).
- VMkernel provides means for running all processes on the system (hypervisor), including management applications and agents as well as virtual machines.

Hypervisors (ESXi)

- VMkernel has manage these main processes that run on top of it. They are:
- Direct Console User Interface (DCUI) — low-level configuration and management interface, accessible through the console of the server, used primarily for initial basic configuration.
- The virtual machine monitor, which is the process that provides the execution environment for a virtual machine, as well as a helper process known as VMX.
- Common Information Model (CIM) system: CIM is the interface that enables hardware-level management from remote applications via a set of standard APIs.

Hypervisors (ESXi)

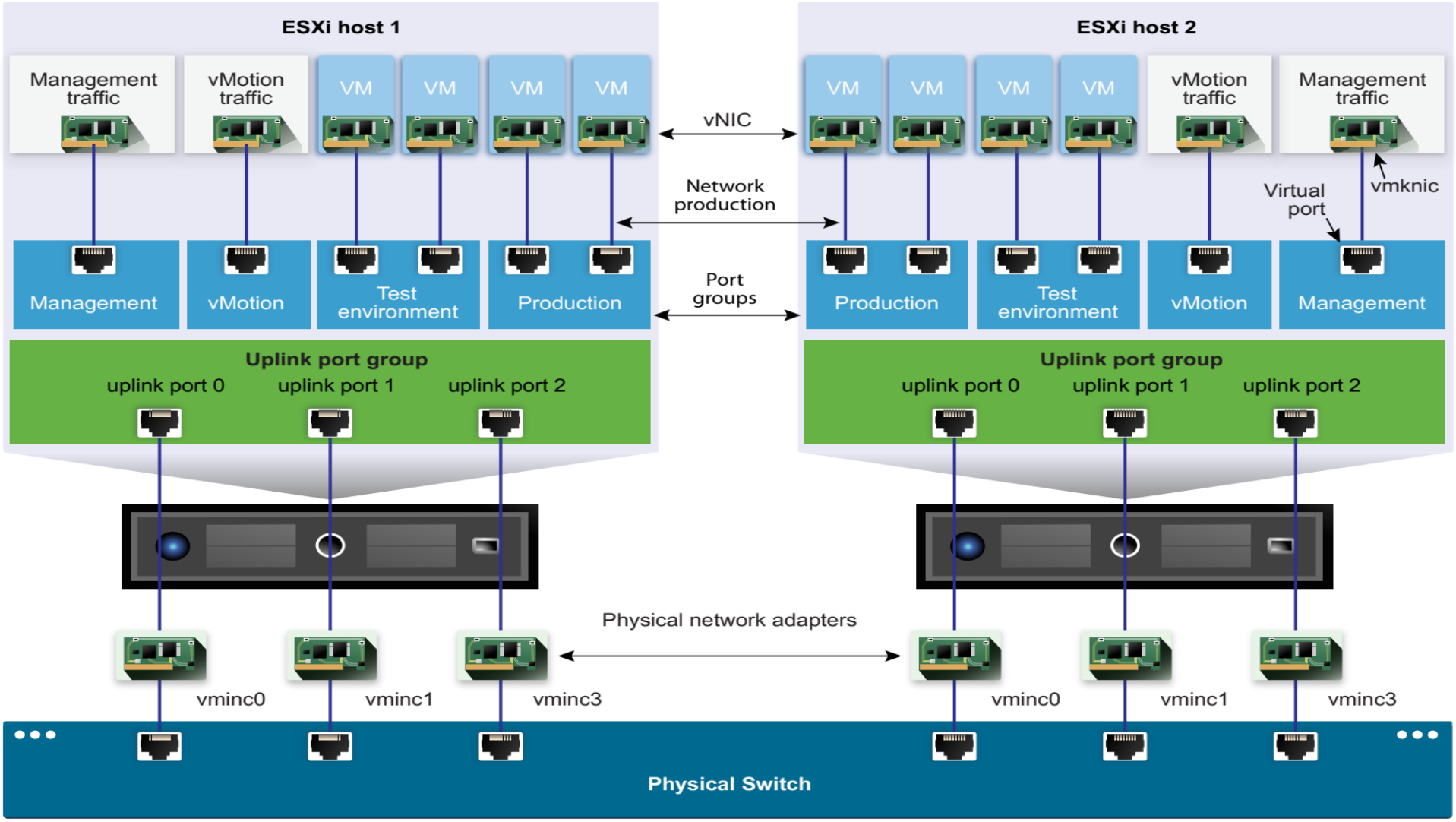


Hypervisor Component

Hypervisor Networks

- Hypervisor network is an abstracted network create using vSphere Standard Switches. You use standard switches to provide network connectivity to hosts and virtual machines.
- A standard switch can bridge traffic internally between virtual machines in the same VLAN and link to external networks.
- To provide network connectivity to hosts and virtual machines, connect the physical NICs of the hosts to uplink ports on the standard switch.
- Virtual machines have network adapters (vNICs) that use to connect to port groups on the standard switch.
- Every port group can use one or more physical NICs to handle their network traffic.

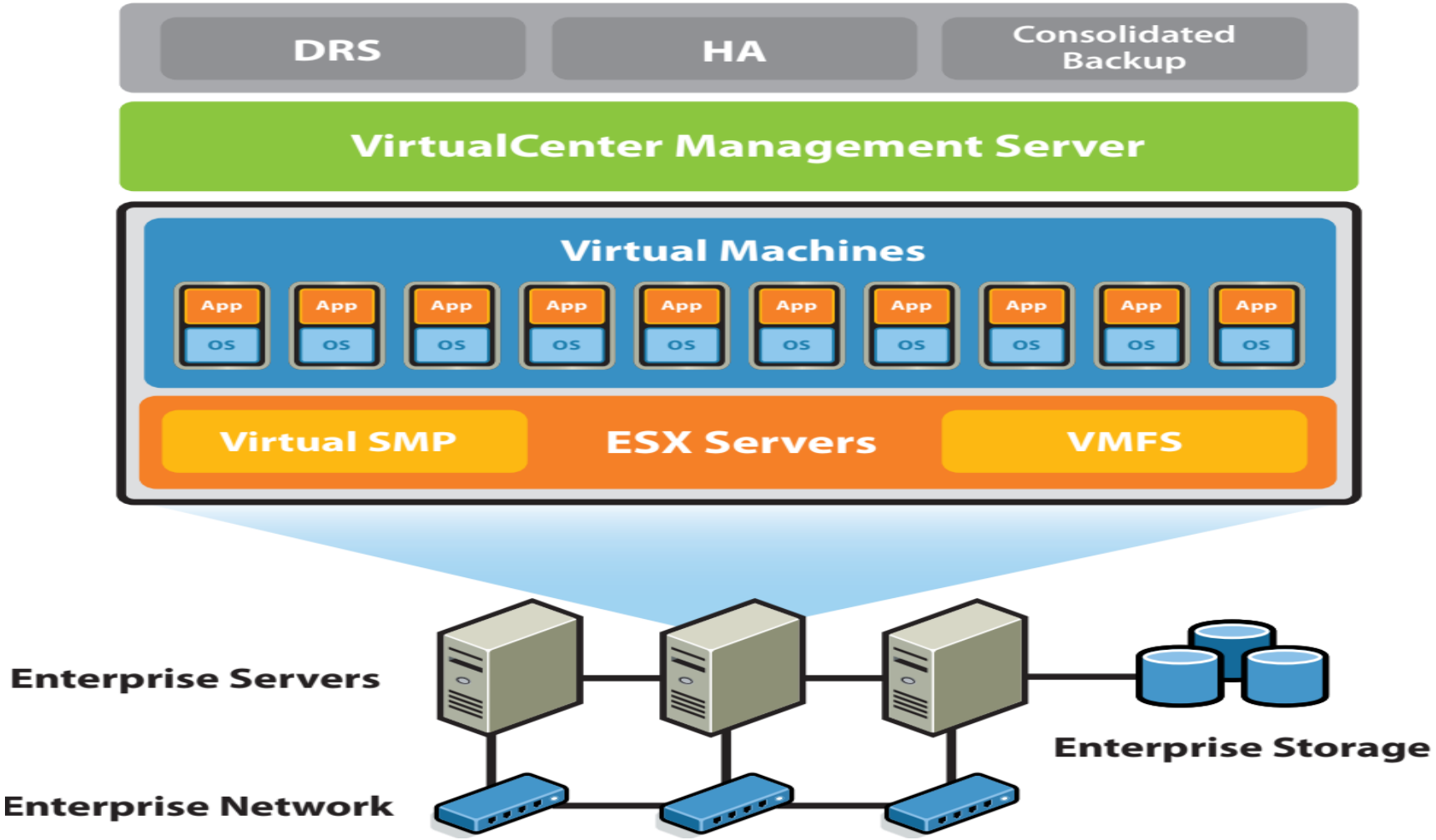
Hypervisor Networks



Hypervisor Networks

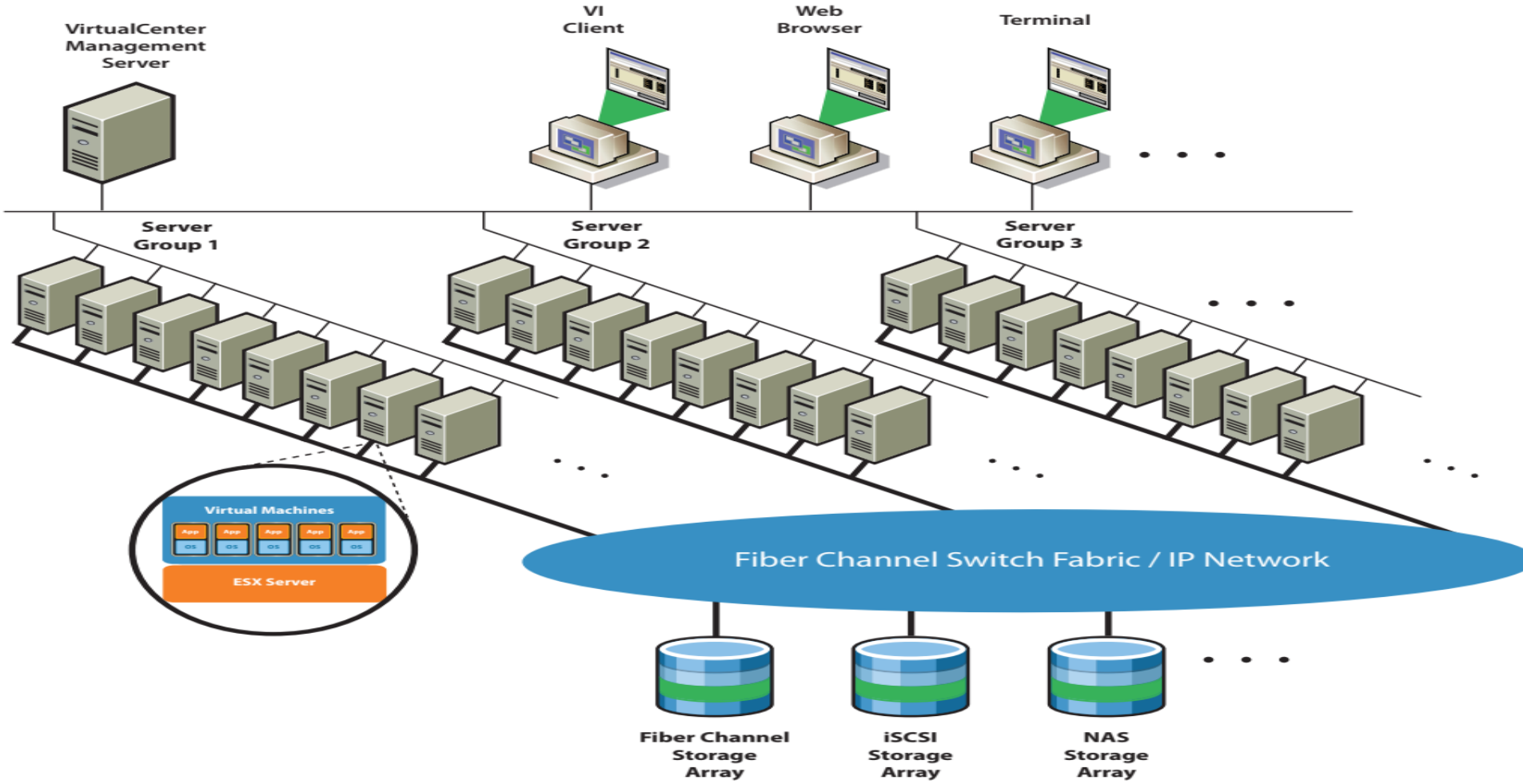
- ESXi Standard Switch is very similar to a physical Ethernet switch.
- Virtual machine network adapters and physical NICs on the host use the logical ports on the switch as each adapter uses one port.
- Each logical port on the standard switch is a member of a single port group.

Hypervisor Networks



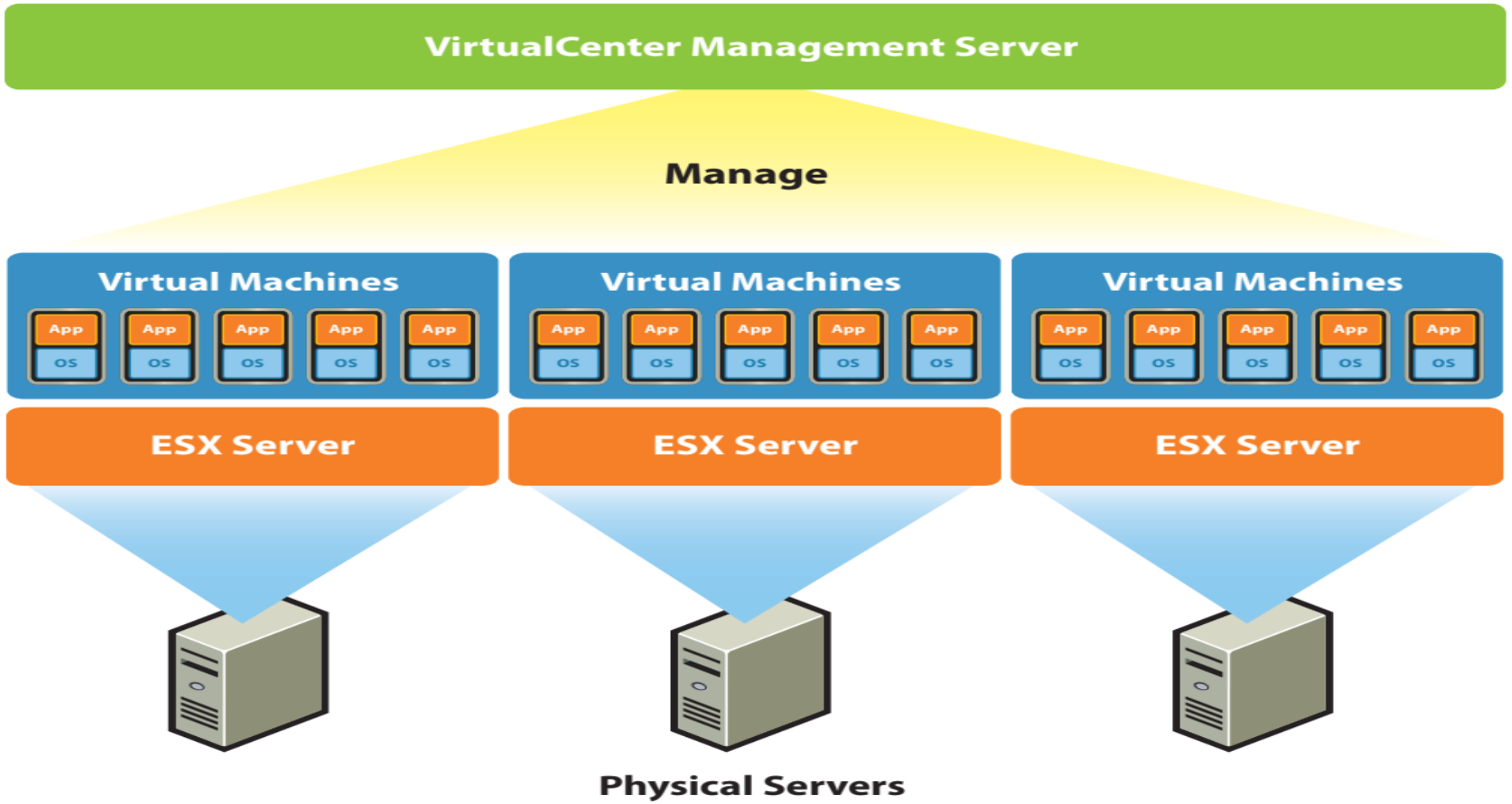
Grid View of VM network

Hypervisor Networks



VM infrastructure DC view

Hypervisor Networks



Vcenter management

Virtual Machines

- Any means by which many different users are able to simultaneously interact with a computing system while each perceiving that they have an entire ‘virtual machine’ to themselves, is a form of virtualization.
- virtual machines we usually refer to when discussing virtualization in enterprises or for infrastructure clouds such as Amazon’s EC2 are *system virtual machines* .
- Multiple *guest* operating systems can be installed on different VMs that each run as operating system processes under the supervision of the VMM called hypervisor.

Virtual Machines

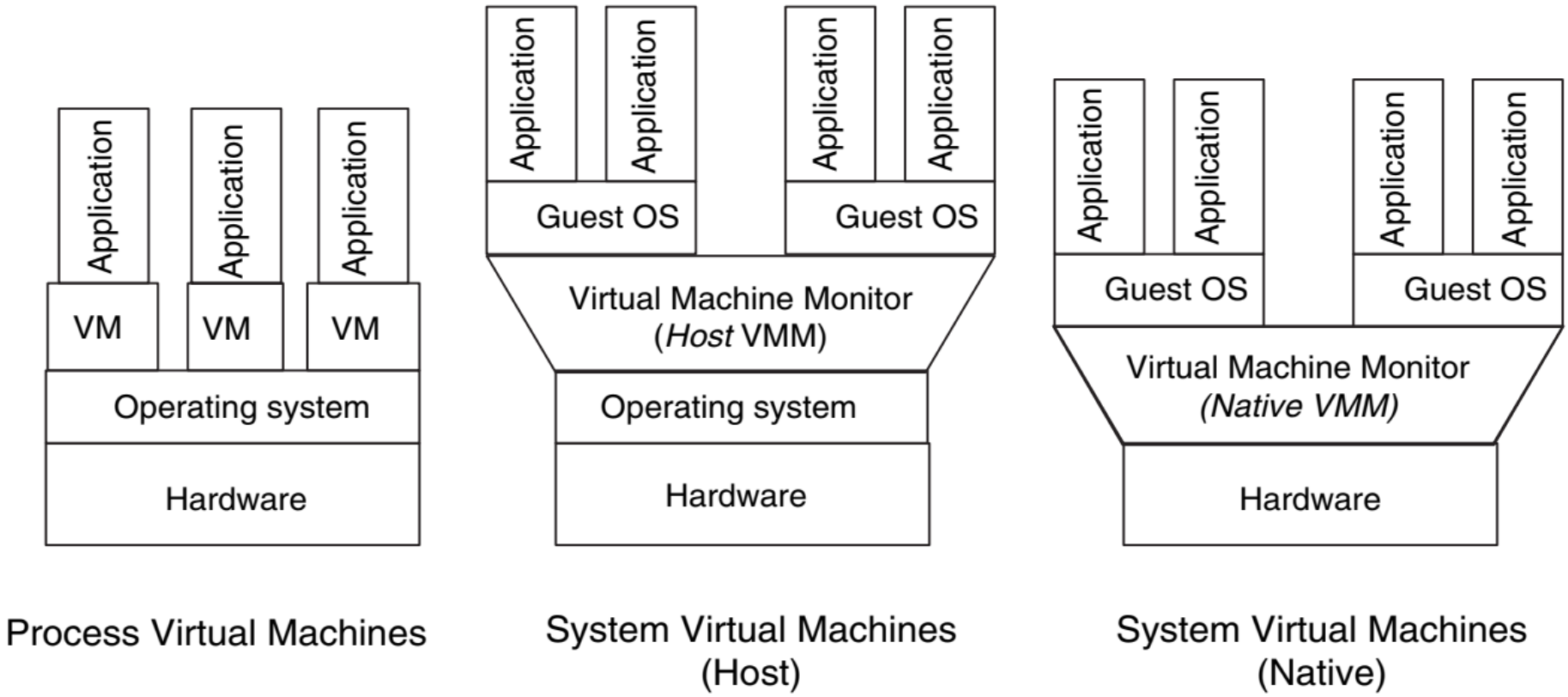


FIGURE 8.1. Virtual machines

Virtual Machines

- There are fundamental differences between the ‘virtual machine’ as perceived by a traditional operating system processes and a true system VM:
  - Processes under an operating system are allowed access to hardware through system calls, whereas a system VMM needs to provide a full hardware instruction set for use by each virtual machine.
  - Each system virtual machine needs to be able to run a full operating system, while itself maintaining isolation with other virtual machines.

VM Management

- Although the global adoption of virtualization is a relatively recent event, threats to the virtualized infrastructure are evolving just as quickly.
- Historically, the development and implementation of new technology has preceded the full understanding of its inherent security risks, and virtualized systems are no different.
- The Virtual Machine (VM), Virtual Memory Manager (VMM), and hypervisor or host OS are the minimum set of components needed in a virtual environment. They comprise virtual environments in a few distinct ways:
  - Type 1 virtual environments are considered “full virtualization” environments and have VMs running on a hypervisor that interacts with the hardware (see Figure 5-2).
  - Type 2 virtual environments are also considered “full virtualization” but work with a host OS instead of a hypervisor.
  - Para virtualized environments offer performance gains by eliminating some of the emulation that occurs in full virtualization environments.
  - Other type designations include hybrid virtual machines (HVMs) and hardware-assisted techniques.

Virtualization Management

VIRTUALIZATION MANAGEMENT ROLES

Typically, the VMware Infrastructure is managed by several users performing different roles. The roles assumed by administrators are the Virtualization Server Administrator, Virtual Machine Administrator, and Guest Administrator. VMware Infrastructure users may have different roles and responsibilities, but some functional overlap may occur. The roles assumed by administrators are configured in VMS and are defined to provide role responsibilities:

- **Virtual Server Administrator** – This role is responsible for installing and configuring the ESX Server hardware, storage, physical and virtual networks, service console, and management applications.
- **Virtual Machine Administrator** – This role is responsible for creating and configuring virtual machines, virtual networks, virtual machine resources, and security policies. The Virtual Machine Administrator creates, maintains, and provisions virtual machines.
- **Guest Administrator** – This role is responsible for managing a guest virtual machine or machines. Tasks typically performed by Guest Administrators include connecting virtual devices, adding system updates, and managing applications that may reside on the operating system.

Virtualization Management

VM THREAT LEVELS

When categorizing the threat posed to virtualized environments, often the vulnerability/threat matrix is classified into three levels of compromise:

- **Abnormally terminated** – Availability to the virtual machine is compromised, as the VM is placed into an infinite loop that prevents the VM administrator from accessing the VM's monitor.
- **Partially compromised** – The virtual machine allows a hostile process to interfere with the virtualization manager, contaminating stet checkpoints or over-allocating resources.
- **Totally compromised** – The virtual machine is completely overtaken and directed to execute unauthorized commands on its host with elevated privileges.[4]

Virtualization Management

Table 5-1: ESX Server Application Vulnerability Severity Code Definitions

CATEGORY	ESX SERVER APPLICATION
Category I – Vulnerabilities that allow an attacker immediate access into a machine, allow super-user access, or bypass a firewall	Vulnerabilities that may result in malicious attacks on virtual infrastructure resources or services. Attacks may include, but are not limited to, malware at the VMM, virtual machine–based rootkit (SubVirt), Trojan, DOS, and executing potentially malicious actions.
Category II – Vulnerabilities that provide information that have a high potential of giving access to an intruder	Vulnerabilities that may result in unauthorized users accessing and modifying virtual infrastructure resources or services.
Category III – Vulnerabilities that provide information that potentially could lead to compromise	Vulnerabilities that may result in unauthorized users viewing or possibly accessing virtual infrastructure resources or services.

Source: ESX Server V1R1 DISA Field Security Operations, 28 April 2008, Developed by DISA for the DoD.

Cloud Data stores

- Google in particular has developed a massively parallel and fault tolerant distributed file system (GFS) along with a data organization (BigTable) and programming paradigm (MapReduce) that is markedly different from the traditional relational model.
- Similarly, Amazon's SimpleDB) and programming paradigms (Hadoop on Amazon's EC2) available to users as part of their cloud platforms.
- At the same time there have been new advances in building specialized database organizations optimized for analytical data processing, in particular column-oriented databases such as Vertica.

Cloud Data stores

- We have multiple data store options in cloud:
- Traditional relational database systems.
- Cloud File Systems: GFS AND HDFS
- BIGTABLE, HBASE AND DYNAMO
- DYNAMO - Dynamo was designed specifically for supporting a large volume of concurrent updates, each of which could be small in size, rather than bulk reads and appends as in the case of BigTable and GFS.

Cloud Data stores

- We have multiple data store options in cloud:
- Traditional relational database systems.
- Cloud File Systems: GFS AND HDFS
- BIGTABLE, HBASE AND DYNAMO
- DYNAMO - Dynamo was designed specifically for supporting a large volume of concurrent updates, each of which could be small in size, rather than bulk reads and appends as in the case of BigTable and GFS.

Cloud Computing and Virtualization

- Virtualization - In computing, a process of creating a illusion of something like computer hardware, operating system (OS), storage device, or computer network resources is Virtualization.

- NIST Cloud Computing - cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Cloud Computing and Virtualization

- What is required for Cloud Computing?
- By Cloud Provider
  - Fast scalability . Quick addition and removal of servers
  - Service to customers should not be denied.
  - SLA should not be Violated
  - Efficient Resource Utilization
- Constraints with physical machines :

  High Provisioning time.
  Lower Resource Utilization.
  Space, Power, Cooling.
  Low fault tolerance
  Less Isolation - misbehaving application can affect all others.
  High downtime.

Cloud Computing and Virtualization

- Virtualization - Concept is not new.

- The concept came from Multi Programming- Each Process thinks it has complete control on all of the resources.
  -Virtual Memory
  -CPU Sharing

- In Multi Programming CPU is shared among processes but in virtualization CPU is shared among OSs.

Cloud Computing and Virtualization

- **Importance of Virtualization in Cloud Computing**
- Cloud can exist without Virtualization, although it will be difficult and inefficient.
- Cloud makes notion of "Pay for what you use" and "infinite availability- use as much you want".
  These notions are practical only if we have
  - lot of flexibility.
  - efficiency in the back-end.
- This efficiency is readily available in Virtualized Environments and Machines.

Cloud Computing and Virtualization

- **Importance of Virtualization in Cloud Computing**
- According to **Intel** "Here is the difference: Virtualization abstracts compute resources
  - Typically as virtual machines (VMs)
  - With associated storage and networking connectivity.
- The cloud determines how those virtualized resources are allocated, delivered, and presented. Virtualization is not necessary to create a cloud environment, but it enables rapid scaling of resources in a way that nonvirtualized environments find hard to achieve."

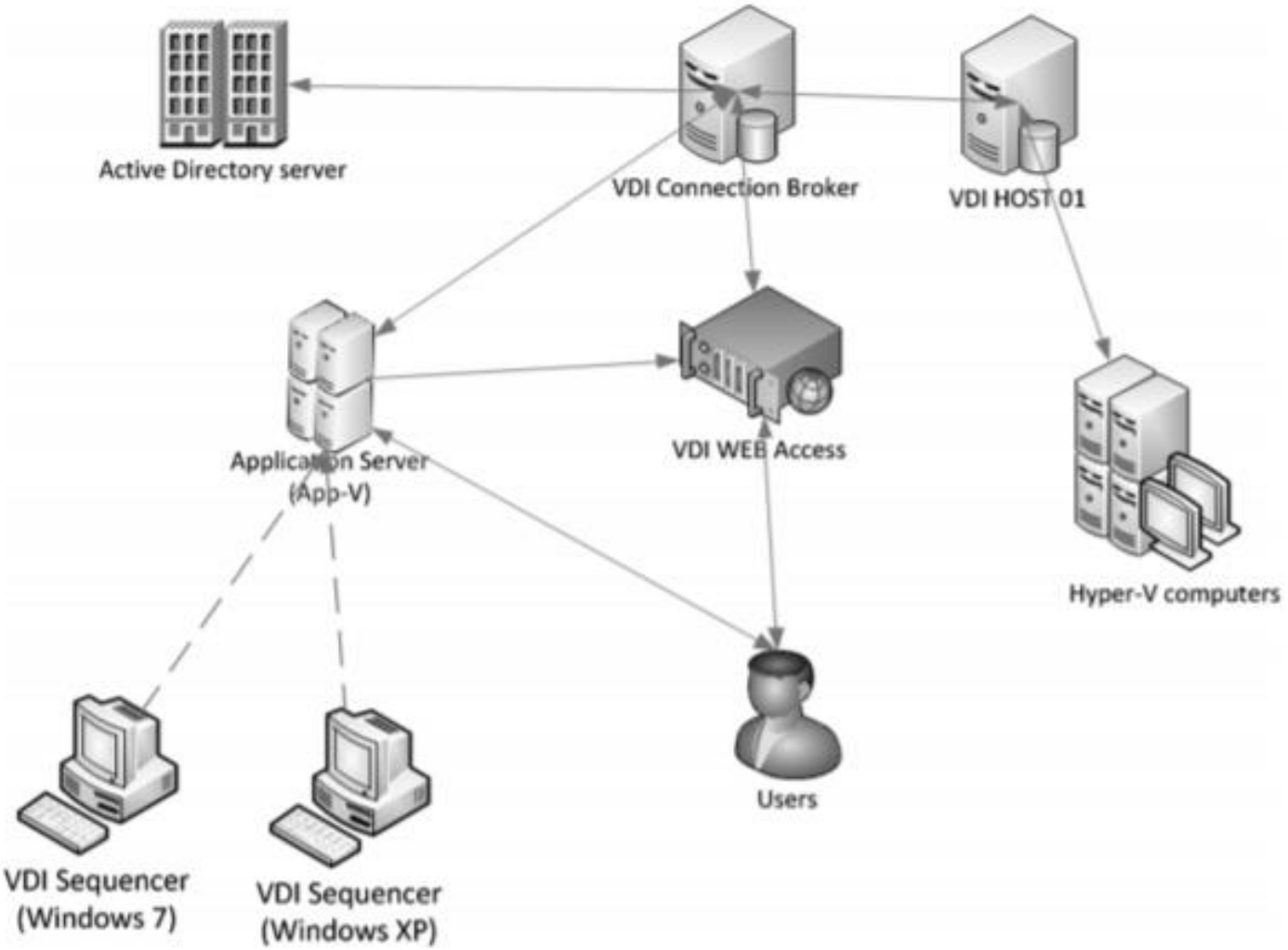
Academic Environment and Virtualization

- Benefits of Virtualization Technologies for academic environment is possible through the desktop virtualization (VDI).
- When used on the client machines, the hardware virtualization is often called Desktop virtualization,
- The virtualization technology which mixes the server and desktop virtualization is called Virtual Desktop Infrastructure (VDI)
- VDI executes the virtual machine operation on the server. In this way, the server hosts a number of desktop VM and the user can reach the virtual machine from any location.
- The VDI technology supports sufficient communications between the client and the server.

Academic Environment and Virtualization

- virtual machine, preventing the virtual machines from damaging one another's configurations and processes.
- Desktop virtualization helps to solve incompatibility between applications and desktop OS.
- This problem can be solved by creating a VM that runs older operating system and installing the application in that VM.
- Virtual Desktop Infrastructure (VDI) allows each user to interact with the desktop located in a data center through the network.
- Incompatibilities between an application and its operating system can also be resolved using Application virtualization.

Academic Environment and Virtualization



Academic Environment and Virtualization

- VDI offers the following benefit in academic environment:
  - Administrative maintenance costs – the implementation of VDI architecture allows to significantly simplify the process of administering, maintaining laboratories and computer stations.
  - Operating costs – energy saving
  - Hardware replacement costs
  - Central implementation and maintenance of virtual systems
  - Security policy – central antivirus.