PAGE NO.:
DATE: / /

VIRTUALIZATION TECHNOLOGY

*Definition of Virtualization -

Virtualization is the "creation of virtual (rather than actual) version of something, such as a server, a desktop, a storage device, an operating system or n/w resources."

Virtualization is a technique, which allows to share a single physical instance of a resource or an application among multiple customers and organizations.

The machine on which the virtual machine is going to create is known as Host machine and that virtual machine is referred as a Guest Machine.

Types of virtualization -

① Hardware virtualization
② Operating system virtualization
③ Server virtualization
④ Storage virtualization

① **Hardware Virtualization** - When the virtual machine software or Virtual machine Manager (VMM) is directly installed on the h/w system is known as hardware virtualization

PAGE NO.:
DATE: / /

The hypervisor (vmm) manages shared the physical resources of h/w between the guest operating system & host operating sys. Hardware virtualization is accomplished by abstracting the physical h/w layer by use of a hypervisor or vmm

The main job of hypervisor is to control & monitoring the processor, memory & other h/w resources.

Usage of Hardware Virtualization- H/w vir. is mainly done for the server platforms, because controlling virtual machine is much easier than controlling a physical server.

Advantages of H/w virtualization-
1. More Efficient Resource Utilization
2. Lower Overall Costs Because of Server Consolidation
3. Increased Uptime Because of Advanced H/w virtualization features
4. Increased IT Flexibility

2. Operating system Virtualization- When the VMM is installed on the Host OS instead of directly on the h/w system is known as O.S virtualization.

OS. virtualization is mainly used for testing the application on different platform of OS.

Teacher's Signature

PAGE NO.:
DATE: / /

With the help of OS virtualization nothing is pre-installed or permanently loaded on the local device & no-hard disk is needed. Everything runs from the n/w using a kind of virtual disk. This virtual disk is actually a disk image file stored on a remote server, SAN (Storage Area N/w) or NAS (Non-volatile Attached storage). The client will be connected by the n/w to this virtual disk & will boot with the O.S. installed on the virtual disk.

* Working of OS virtualization -

The components needed for using OS virtualization are-

① OS virtualization server- This server is the center point in the OS virtualization infrastructure. The server manages the streaming of the information on the virtual disk for the client & also determines which client will be connected to which virtual disk (using a database this info. is stored). The server also ensures that the client will be unique within the infrastructure.

② Client- Client contact the server to get connected to the virtual disk & asks for components stored on the virtual disk for running the O.S.

③ Database- Database are the supporting components for storing the configuration & setting for a server.

Teacher's Signature.....

PAGE NO.:
DATE: / /

* Steps of OS virtualization -

① Connecting to the OS virtualization server - first we start the machine & set up the connection with the OS virtualization server. The several possible methods to connect with the server are -

ⓐ PXE service (Pre-Boot Execution Environment)
ⓑ Boot strap

Each method initializes the NIC (N/w interface card), receiving a (DHCP-based) IP address & a connection to the server.

DHCP - Dynamic Host Configuration Protocol, also known as RFC 2131. It is a n/w protocol that allows a server to automatically assign an IP address from a specified range of numbers to a computer or device when it is connected to a given n/w.

② Connecting the Virtual Disk - When the connection is established between the client and the server, the server will look into its database for checking the client is known or unknown & which virtual disk is assigned to the client.

③ VDisk connected to the client - After the desired virtual disk is selected by the client, that vdisk is connected through the OS virtualization server. At the back-end, the OS virtualization server make sure that the client will be

Teacher's Signature

unique within the infrastructure. (for ex- computer name & identifier).

④ OS is "streamed" to the client- As soon the disk is connected, the server starts streaming the content of the virtual disk. The s/w knows which parts are necessary for starting the OS smoothly, so that these parts are streamed first.

⑤ Additional Streaming - After that the first part is streamed then the OS will start to run as expected. Additional virtual disk data will be streamed when required for running on starting a function called by the user.

③ Server Virtualization - When the VMM is directly installed on the server system is known as server virtualization. Server virtualization is done because a single physical server can be divided into multiple servers on the demand basis & for balancing the load. It is used to maximize the server resource.

In this vir., the resources of the server are itself hidden from the users, and a s/w is used to partition the physical server into several virtual environment, called as virtual servers or private servers.

Teacher's Signature

PAGE NO.:
DATE: / /

* Usage of server virtualization-
server virtualization is used-
→ to make more efficient use of server resources
→ to improve the server availability
→ to help in disaster recovery
→ development & testing
→ to centralize the server administration.

* Advantages of Server vir.-
① Each virtual server can be independently rebooted
② Server virtualization reduces the costs because less h/w is required.

④ Storage Virtualization- Storage virtualization is the process of grouping the physical storage from multiple n/w storage devices so that it looks like a single storage device.
Storage virtualization is also implemented by using s/w applications. Storage virtualization is mainly done for backup and recovery purposes.
storage virtualization is a major component for storage servers, in the form of functional RAID levels and controllers. OS & applications with device can access the disks directly by themselves for writing. The controllers configure the local storage in RAID groups & present the storage to the OS depending upon the configuration.

Teacher's Signature

PAGE NO.:
DATE: / /

Advantages of storage virtualization-

Data is stored in the more convenient locations away from the specific host. In the case of a host failure, the data is not compromised necessarily.

The storage devices can perform advanced functions like replication, deduplication & disaster recovery functionality.

* Benefits of Virtualization-

① Protection from system failure - While working in cloud environment there may be the risk of crashing down at the wrong time. To counter the risk of system crash, virtualization lets you open the same work on another device. There are usually two servers working side-by-side keeping all your data accessible. If one faces any problem, the other is always available to avoid any interruption.

② Hassle-free Transfer of Data - You can easily transfer data from a physical storage to a virtual server, and vice versa. Administrators don't have to waste time digging out hard drives to find data. With a dedicated server & storage, it's quite easy to locate the required files and transfer them within no time.

Teacher's Signature.....

PAGE NO.:
DATE: / /

③ Firewall & Security - Security is a major IT professionals have to focus on. Through virtualization, you get protected by a virtual switch that protects all your data & applications from harmful malware, viruses and other cyber threats.

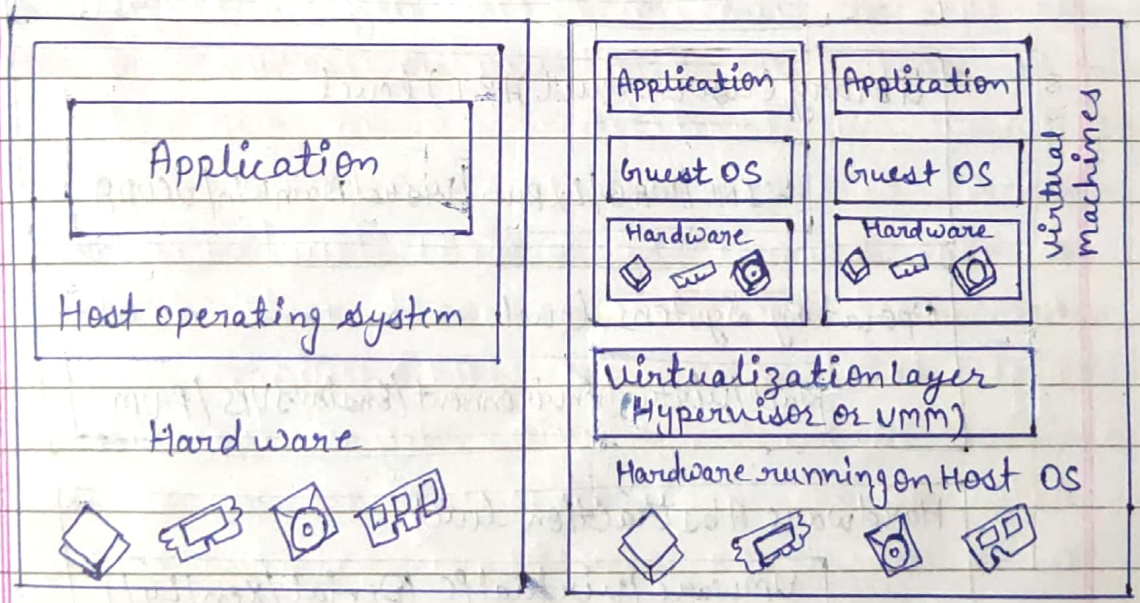
④ Flexible Operations - With the help of a virtual n/w, the work of IT professional is becoming more efficient and agile. With the help of virtualization in cloud computing, technical problems can solve in physical systems. It eliminates the problem of recovering the data from crashed or corrupted devices and hence saves times.

⑤ Economical - Virtualization in cloud computing, save the cost for a physical system such as n/w & servers. It store all the data in virtual server, which are quite economical. It reduces the wastage, decreases the electricity bills along with the maintenance cost.

PAGE NO.:
DATE: / /

Implementation Level of Virtualization-

A traditional computer runs with a host operating system specially tailored for its h/w architecture. After virtualization, different user applications managed by their own operating system (guest OS) can run on the same hardware independent of the host OS. This is often done by adding additional s/w, called a virtualization layer. This virtualization layer is known as hypervisor or virtual machine monitor (VMM).



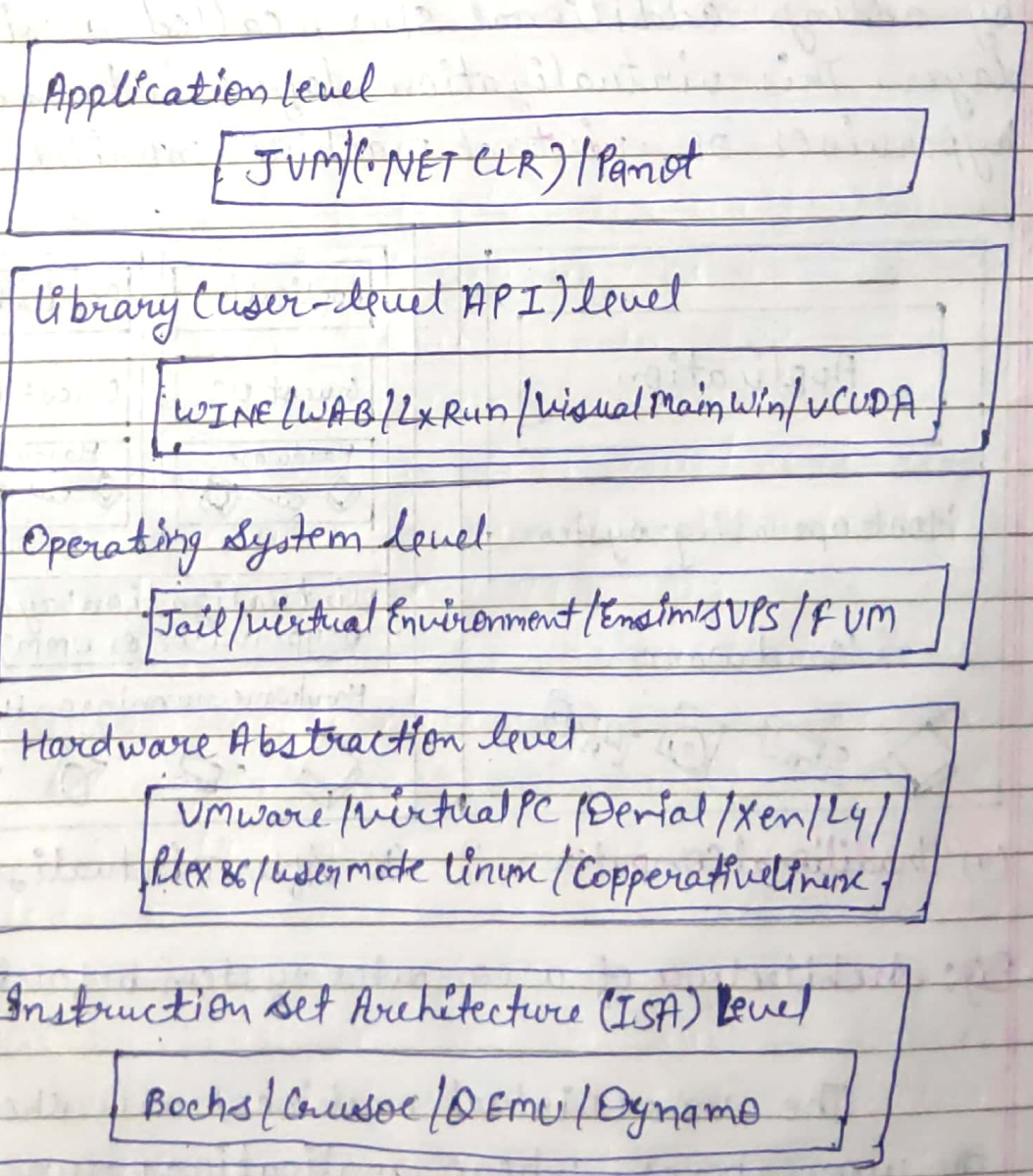
(a) Traditional computer (b) After virtualization

Fig: Architecture of a computer system before & after virtualization

The VMs (virtual machines) are shown in the upper boxes, where applications run with their own guest OS over the virtualized CPU, memory & I/O resources.

Teacher's Signature.....

The main function of the s/w layer for virtualization is to virtualize the physical h/w of a host machine into virtual resources to be used by the VMs, exclusively. This can be implemented at various operational levels. The virtualization s/w creates the abstraction of VMs by interposing a virtualization layer at various levels of a computer system.



PAGE NO.:
DATE: / /

Instruction set Architecture level- At the ISA level, virtualization is performed by emulating a given ISA by the ISA of the host machine. For ex, MIPS binary code can run on an x86-based host machine with the help of ISA emulation. With this approach, it is possible to run a large amount of legacy binary code written for various processors on any given new h/w host machine. Instruction set emulation leads to virtual ISAs created on any h/w machine.

Hardware Abstraction level- Hardware-level virtualization is performed right on top of the bare h/w. On the one hand, this approach generates a virtual h/w environment for a VM. On the other hand, the process manages the underlying h/w through virtualization. The idea is to virtualize a computer's resources, such as its processors, memory and I/O devices. The intention is to upgrade the h/w utilization rate by multiple users concurrently.

Operating System Level- This refers to an abstraction layer between traditional OS & user applications. OS-level virtualization creates isolated containers on a single physical server & the OS instances to utilize the h/w & s/w in data centers. The containers behave like real servers. OS-level virtualization commonly used in creating virtual hosting environments to allocate h/w resources among a large number of mutually distrusting users.

Teacher's Signature

PAGE NO.:
DATE: / /

Library support Level- most applications use APIs exported by user-level libraries rather than using lengthy system calls by the OS. Since most systems provide well-documented APIs, such as interface becomes another candidate for virtualization.

Vir. with library interface is possible by controlling the communication link between applications & the rest of a system through API hooks.

User-Application level- Virtualization at the application level virtualizes an app as a VM. On a traditional OS, an app often runs as a process. Therefore, application level-vir. is also known as process-level virtualization. The most popular approach is to deploy high level language (HLL) VMs.

In this scenario, the virtualization layer sites as an application prg. on top of the OS & the layer exports an abstraction of a VM that can run programs written and compiled to a particular abstract machine definition. Any prg written in HLL & compiled for this VM will be able to run on it.

The Microsoft .NET CLR & Java Virtual machine (JVM) are two good examples of this class of VM.

Teacher's Signature

Virtualization Structure | Tools & Mechanisms-

Before virtualization, the operating system manages the h/w. After virtualization, a virtualization layer is inserted between the h/w & the O.S. In such a case, the vir. layer is responsible for converting portion of the real h/w into virtual h/w. Therefore, different OS such as linux & windows can run on the same physical machine, simultaneously.

Depending on the position of the vir. layer, there are several classes of vm architecture-

⇒ Hypervisor architecture
⇒ Para-virtualization
⇒ host-based virtualization

Hypervisor-

The hypervisor supports h/w-level vir. on bare metal devices like CPU, memory, disk & n/w interfaces. The hypervisor s/w sits directly between the physical h/w & its OS.
Hypervisor is a h/w virtualization technique that allows multiple guest OS to run on a single host system at the same time.
The hypervisor is a s/w that can virtualize the h/w resources.

Types of hypervisor-

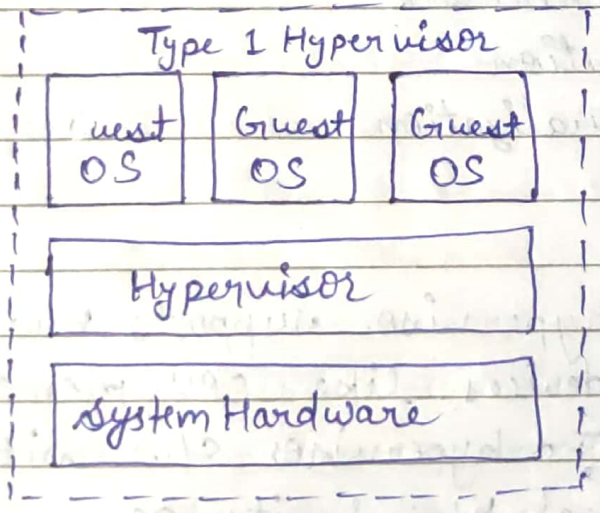
① Type 1 hypervisor (micro kernel)
② Type 2 hypervisor (monolithic)

PAGE NO.:
DATE: / /

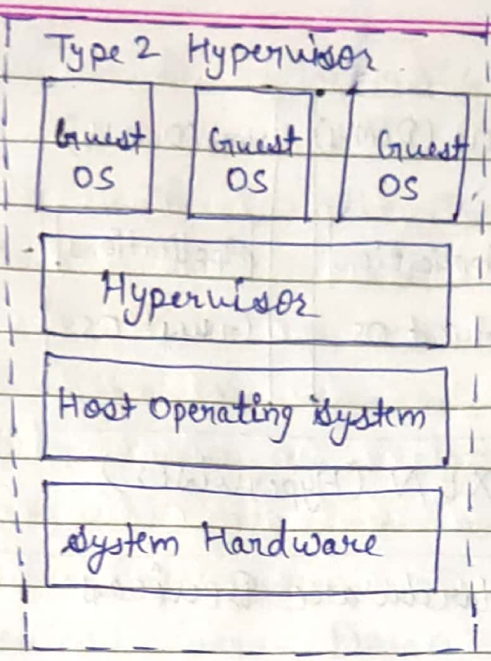
① Type 1 Hypervisor- Type 1 hypervisor run directly on the system h/w. They are often referred to as a "native" or "bare metal" or "embedded" hypervisor.

Type 1 hypervisor acts as an OS and in addition it also host virtual machines. It does not require any base server OS. It has direct access to h/w resources.

Ex → VMware ESX and ESXi
→ Microsoft Hyper-V
→ Citrix XenServer
→ Oracle VM



② Type 2 Hypervisor- Type 2 hypervisor also called Hosted Hypervisor. Type 2 Hypervisor run on a host OS that provides virtualization services, such as I/O device support & memory management.



Ex. → VMware Workstation / Fusion / Player
→ VMware Server
→ Microsoft Virtual PC
→ Oracle VM Virtual Box
→ Red Hat Enterprise Virtualization
→ KVM.

★ XEN Architecture –

Xen is an open source hypervisor program developed by Cambridge University. It is a Type 1 hypervisor. The Xen hypervisor implements all the mechanisms, leaving the policy to be handled by Domain 0. Xen does not include any device drivers natively.

It provides a mechanism by which a guest OS can have direct access to the physical devices. The core components of a Xen system are the hypervisor, kernal and applications. The organization of the three components is important.

Teacher's Signature.....

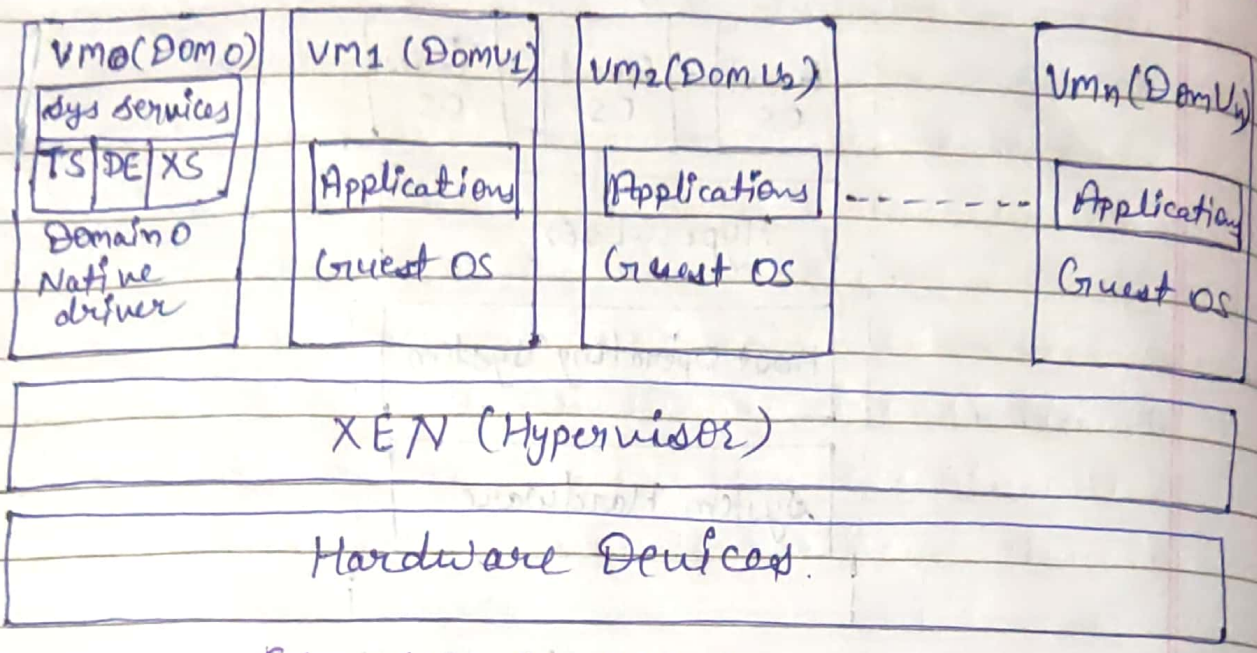


Fig- XEN Architecture

★ Xen Project Hypervisor- is an s/w layer that runs directly on the h/w and is responsible for managing CPU, memory & interrupts. It is the first program running after the bootloader exists.

★ Guest Domain / Virtual Machines- are virtualized environments, each running their own OS and applications. The hypervisor supports several different virtualization modes, which are described-

★ Control Domain (Domain 0) - is a specialized VM that has special privileges like the capability to access the h/w directly, handles all access to the system's I/O functions & interacts with the other VM.

Dom0 contains the following functions -

* System Services - such as XenStore/Xen Bus (XS) for managing settings, the Toolstack (TS) exposing a user interface to a Xen based system, Device Emulation (DE) which is based on QEMU in Xen based systems.
* Native Device Drivers - Dom0 is the source of physical device drivers and thus native h/w support for a Xen system.
* Virtual Device Drivers - Dom0 contain virtual device drivers (also called backends).
* Toolstack - allows a user to manage virtual machine creation, destruction and configuration.

* XEN Project Enabled Operating System - Domain 0 requires a Xen project-enabled kernal.

PAGE NO.:
DATE: / /

Full virtualization -

⇒ In this the guest OS is unaware that it is in a virtualized environment and therefore h/w is virtualized by the host O.S

⇒ Full virtualization does not need to modify the host OS. It relies on binary translation to trap and to virtualize the execution of certain sensitive, nonvirtualize instructions.

⇒ With full virtualization, noncritical instructions run on the h/w directly while critical ins are discovered & replaced with traps into the vmm to be emulated by s/w. This is because Non critical instructions do not control h/w or threaten the security of the system, but critical instruction can do.

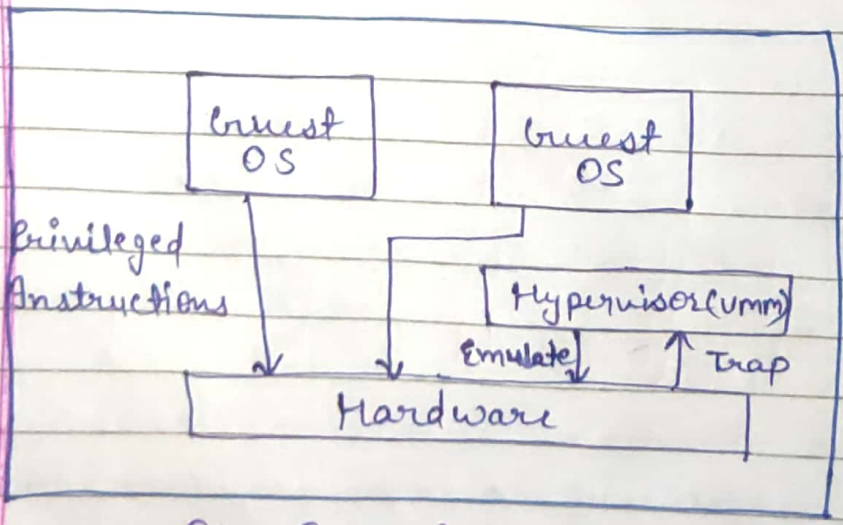


Fig - Full virtualization

Privileged Ins - ins. that if executed in user mode trap to kernel mode, but if executed in kernel mode they donot trap.

Teacher's Signature

PAGE NO.:
DATE: / /

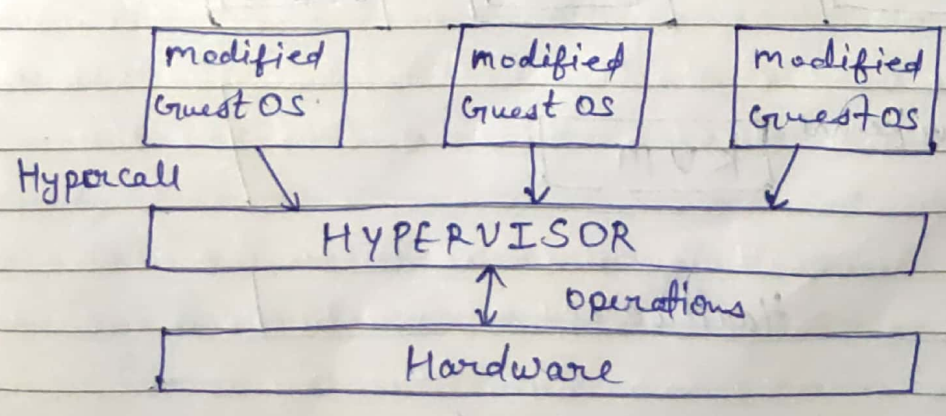
Host-Based Virtualization -

In this virtualization, a virtualization layer is installed on top of the host OS. This host OS is responsible for managing the h/w. The guest OS are installed & run on top of the virtualization layer.

The user can install the VM architecture without modifying the host OS. The VMM can rely on the host OS to provide device drivers & other low-level services. The performance of host based architecture may be low. When an application requests h/w access, it involves four layer of mapping which downgrades performance significantly

Para Virtualization -

Para virtualization needs to modify the guest OS. In this the guest OS is aware that it is a guest. A para-virtualized virtual machine provides special APIs requiring substantial OS modification in user application.



Teacher's Signature.....

In para-virtualization, OS hypercalls instructions are handled at compile time when the non-virtualizable OS instructions are replaced with hypercalls

KVM - (Kernal-based Virtual Machine)

→ KVM is a hypervisor which is built into the linux kernal.
→ Allows linux desktops or servers to simulate multiple pieces of h/w.
→ Full virtualization solution for linux on x86 h/w that contains virtualization extensions such as Intel VT or AMD-V
→ KVM uses QEMU (Quick Emulator) virtual machine format.

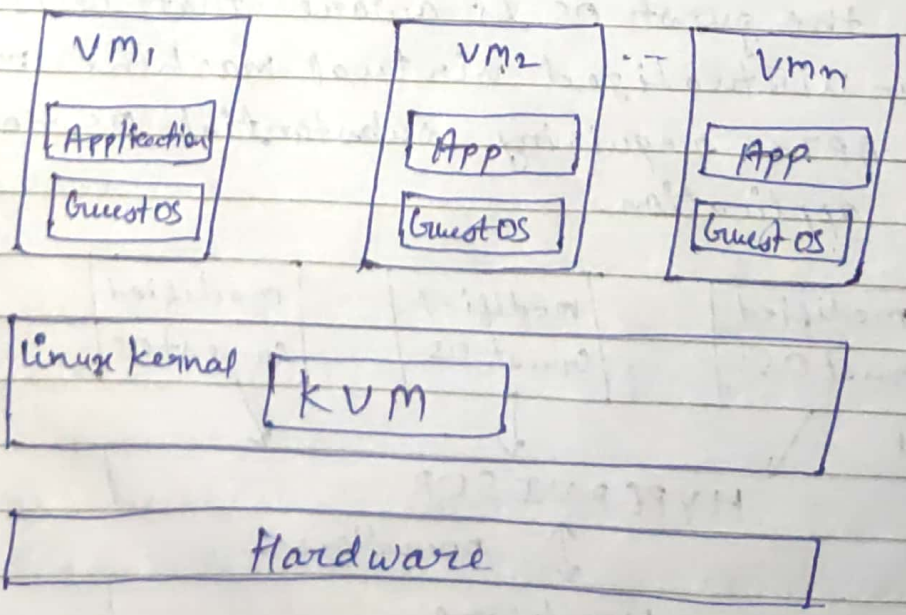


Fig: KVM Architecture

Teacher's Signature

DATE: / /

→ The KVM module creates a bare metal hypervisor on the Linux kernal.
→ Virtual Machines can be loaded onto this hypervisor running separate OSes.

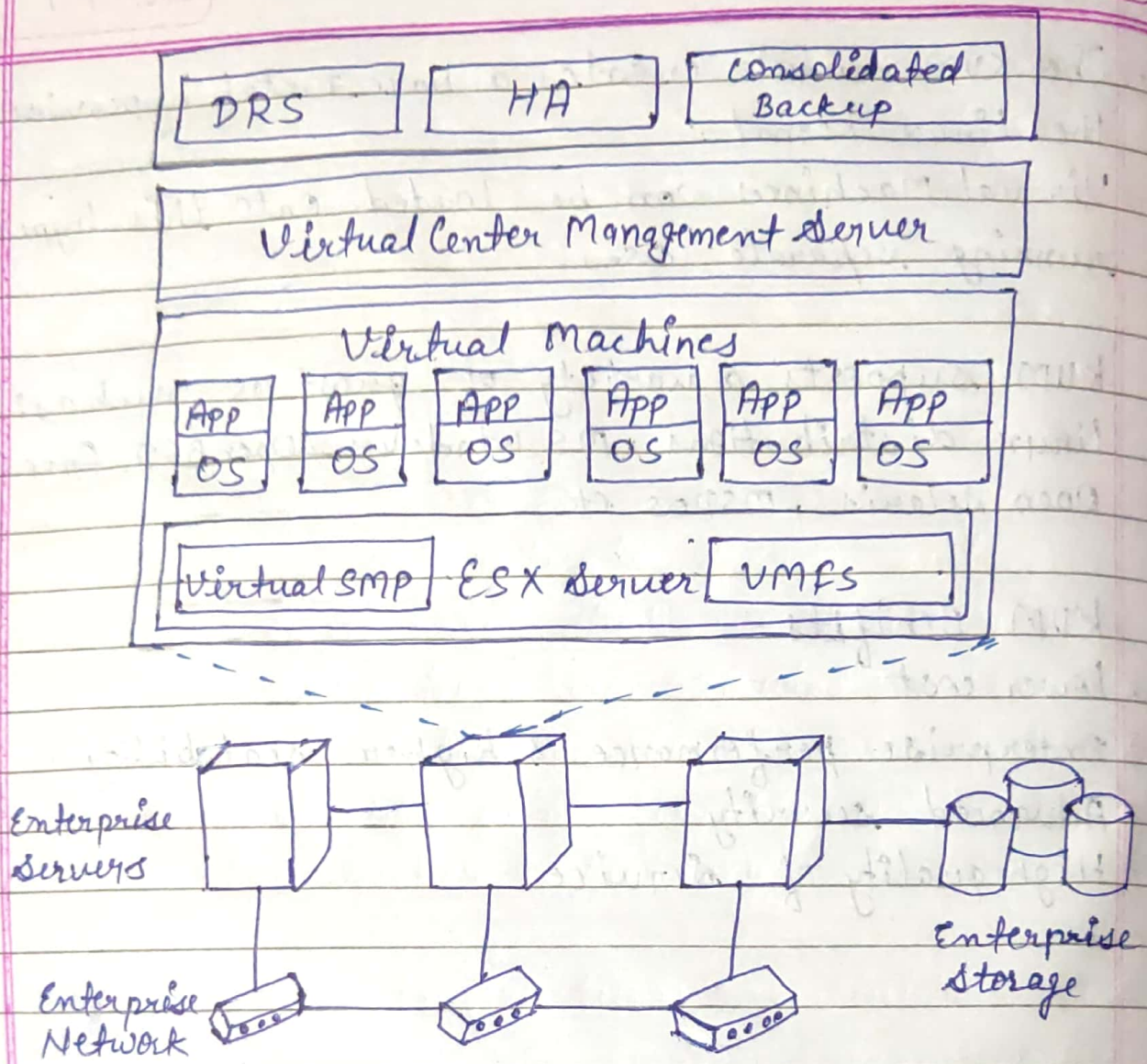
KVM supports a variety of guest OS such as: Linux distributions, MS windows, OpenBSD, FreeBSD, Open solaris, MSDOS etc.

KVM Benifits -
→ Lower cost
→ Enterprise performance & higher scalability
→ Advanced security
→ High quality of Service

★ VMware -

VMware is a virtualization and cloud computing Slw provider, founded in 1998.
With VMware server virtualization, a hypervisor is installed on the physical server to allow for multiple virtual machines (VMs) to run on the same physical server.
Each VM (virtual machines) can run its own OS, which means multiple OSes can run on one physical server.
All the VMs on the same physical server share resources, such as networking and RAM.

Teacher's Signature.....



VMware Infrastructure includes following components:

* VMware ESX server- It is a virtualization layer run on physical servers that abstract processor, memory, storage and networking resources to be provisioned to multiple virtual machines.

* VMware Virtual machine File System (VMFS)- A high-performance cluster file system for VMs.

* VMware virtual Symmetric Multi-Processing (SMP)- Enables a single virtual machine to use multiple physical processors simultaneously.

Teacher's Signature.....

PAGE NO.:
DATE: / /

Virtual Center Management Server - The central point for configuring, provisioning and managing virtualized IT infrastructure.

Virtual Infrastructure Client (VI Client) - An interface that allows administrators and users to connect remotely to the virtual Center Management Server or individual ESX server installation from any Windows PC.

VMware VMotion™ - Enables the live migration of running virtual machines from one physical server to another with zero downtime, continuous service availability & complete transaction integrity.

VMware High Availability (HA) - Provides easy-to use, cost effective high availability for applications running in virtual machines. In the event of server failure, affected virtual machines are automatically restarted on other production servers that have spare capacity.

VMware Distributed Resource Scheduler (DRS) - Intelligently allocates and balances computing capacity dynamically across collections of H/W resources for virtual machines.

VMware Consolidated Backup - Provides an easy to use, centralized facility for agent-free backup of of VM. It simplifies backup administration and reduces the load on ESX server installation.

Teacher's Signature.....

VMware infrastructure SDK - Provides a standard interface for VMware and third party solution to access VMware infrastructure.

☆ CPU Virtualization -

A VM is a duplicate of an existing computer system in which a majority of the VM instructions are executed on the host processor in native mode. Thus, unprivileged instruction of VMs run directly on the host machine for higher efficiency.

The critical instructions are divided into three categories:

Privileged instruction - execute in a privileged mode & will be trapped if executed outside this mode.

Control-sensitive instructions - attempt to change the configuration of resources used.

Behavior-sensitive instructions - have different behaviors depending on the configuration of resources, including the load and store operations over the virtual memory.

A CPU architecture is virtualizable if it supports the ability to run the VM's privileged and unprivileged instructions in the CPU's

Teacher's Signature

user mode while the VMM runs in supervisor mode. When the privileged instructions including control- and behavior-sensitive instruction of a VM are executed, they are trapped in the VMM. In this case, the VMM acts as a unified mediator for h/w access from different VMs to gurantee the correctness and stability of the whole system.

However not all CPU architectures are virtualizable. RISC CPU architecture can be naturally virtualized because all control-& behavior-sensitive instructions are privileged instructions.

Hardware-Assisted CPU virtualization - This technique attempts to simplify virtualization. Intel and AMD add an additional mode called privilege mode level (Ring 1) to x86 processors. Therefore OS can run at Ring 0 and the hypervisor can run at Ring 1. All the privileged and sensitive instructions are trapped in the hypervisor automatically. This technique removes the difficulty of implementing binary translation of full virtualization. It also lets the OS run in VMs without modification.

"In hardware-assisted virtualization, the h/w provides architectural support that facilitates building a VMM and allows guest OS to be run in isolation!"

Teacher's Signature.....

PAGE NO.:
DATE: / /

Ex:- Intel Hardware-Assisted CPU virtualization.

Intel's VT-x technology is an example of h/w-assisted virtualization. Intel calls the privilege level of x86 processors the VMX Root Mode. In order to control the start & stop of a VM & allocate a memory page to maintain the CPU state for VMs, a set of additional instructions is added.

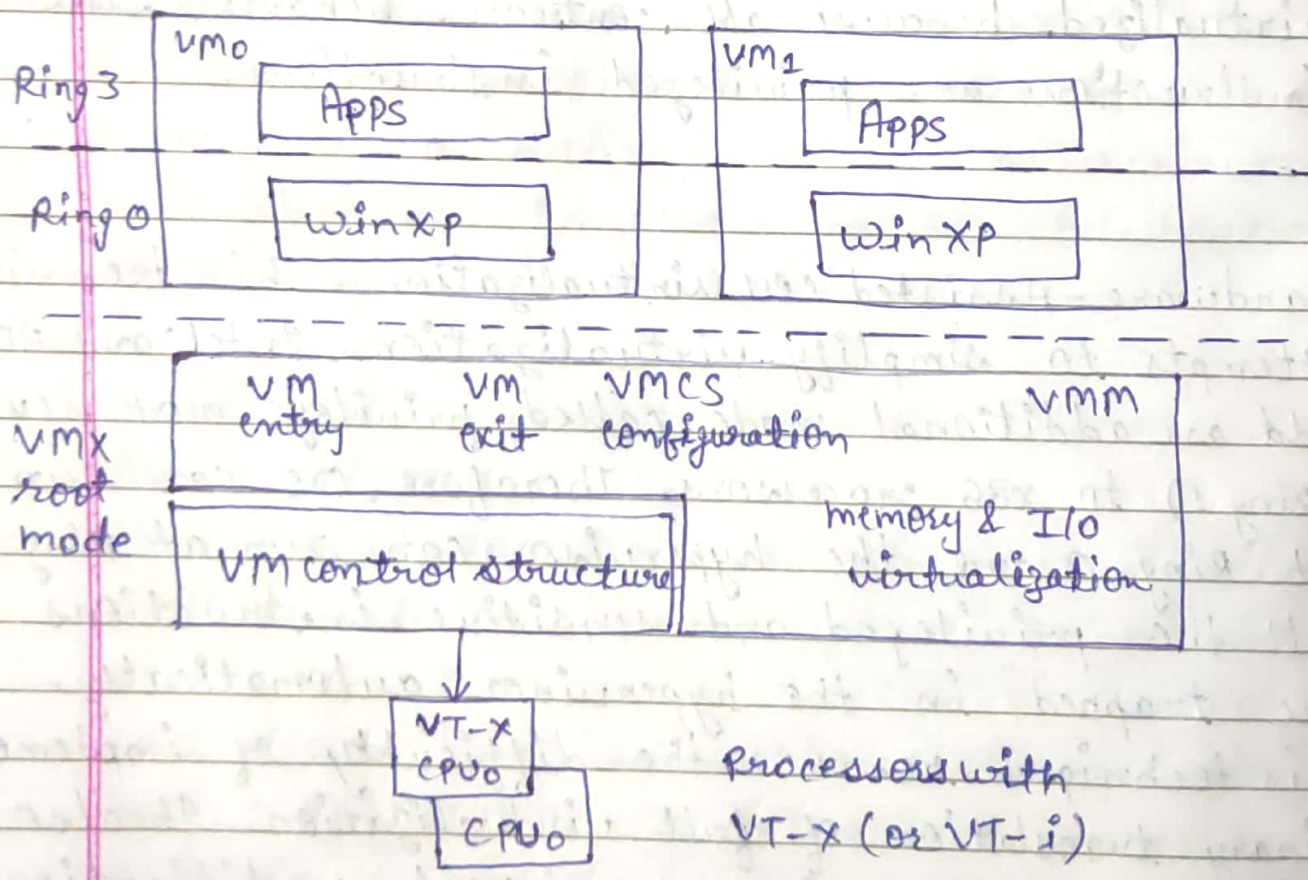


Fig- Intel hardware-assisted CPU virtualization

PAGE NO.:
DATE: / /

* Memory Virtualization-

All modern x86 CPUs include memory management unit (MMU) and a translation lookaside buffer (TLB) to optimize virtual memory performance. Virtual memory virtualization involves sharing the physical system memory in RAM and dynamically allocating it to the physical memory of the VMs.

A two-stage mapping process is maintained by the guest OS and the VMM respectively: virtual memory to physical memory & physical memory to machine memory. The guest OS can't directly access the actual machine memory. The VMM is responsible for mapping the guest physical memory to the actual machine memory.

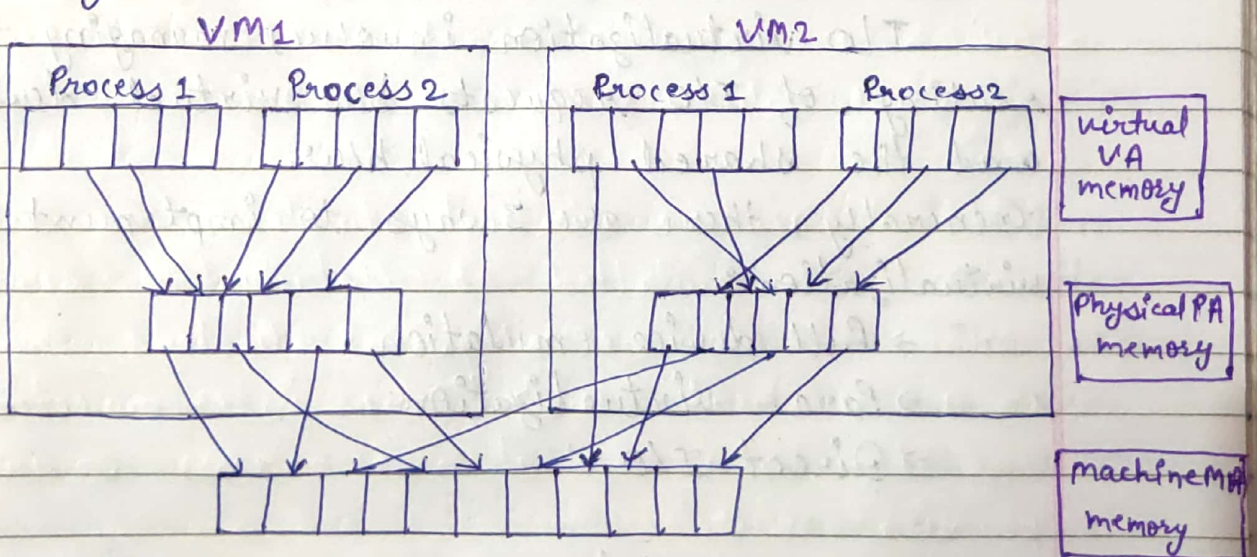


Fig: Two level memory mapping procedure

Since each page table of the guest OSes has a separate page table in the VMM corresponding to it, the VMM page table is called the "shadow page table".

Teacher's Signature

The MMU already handles virtual-to-physical translations as defined by the OS. Then the physical memory addresses are translated to machine addresses using another set of page tables defined by the hypervisor.

Vmware uses shadow page table to perform virtual-memory to machine-memory address translation. Processors use TLB h/w to map the virtual memory directly to the machine memory to avoid the two levels of translation on every access.

I/O Virtualization-

I/O virtualization involves managing the routing of I/O requests b/w virtual devices and the shared physical h/w.
Generally, there are 3 ways to implement I/O virtualization:

- → Full device emulation.
- → Para-virtualization
- → Direct I/O.

* Full device emulation- This approach emulates well known, real world devices. All the functions of a device or bus infrastructure, such as device enumeration, identification, interrupts & DMA are replicated in s/w.

Teacher's Signature

This slw is located in the VMM and acts as a virtual device. The I/O access requests of the guest OS are trapped in the VMM which interacts with the I/O devices.

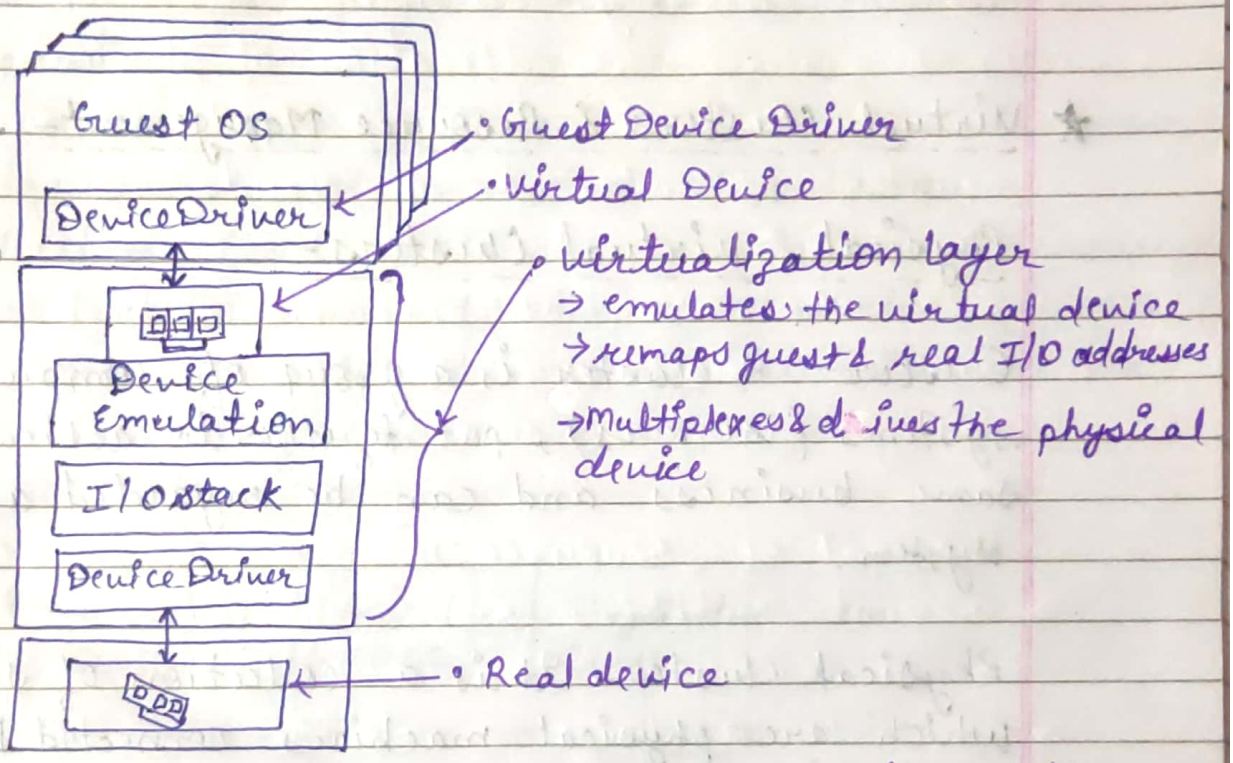


Fig - Full device emulation for I/O virtualization.

★ Para virtualization - This method is used in Xen. It is also known as the split driver model consisting of a frontend driver and a backend driver. The frontend driver running in Domain U and the backend driver is running in Domain 0. They interact with each other via a block of shared memory. The frontend driver manages the I/O requests of the guest OS & the backend driver is responsible for managing the real I/O devices and multiplexing the I/O data of different virtual machines.

Teacher's Signature.....

DATE: / /

Direct I/O virtualization - lets the VM access devices directly. It can achieve close-to-native performance without high CPU costs.

★ Virtual Clusters & Resource Management -

Physical & Virtual Clusters -

Cluster - A Cluster is a group of computer systems (servers), put together to achieve the same business and can be regarded as one system.

Physical Cluster - It is a collection of servers which are physical machines connected by a physical n/w such as a LAN.

Virtual Cluster - virtual clusters are built with VMs installed at distributed servers from one or more physical clusters. The VMs in a virtual cluster are interconnected logically by a virtual n/w across several physical n/w.

The provisioning of VMs to a virtual cluster is done dynamically to have the following properties -

→ The virtual cluster nodes can be either physical or virtual machines. Multiple Vs running

Teacher's Signature

with different OSes can be deployed on the same physical node.

→ A VM runs with a guest OS, which is often different from the host OS, that manages the resources in the physical machine, where VM is implemented.

→ VMs can be colonized (replicated) in multiple servers for the purpose of promoting distributed parallelism, fault tolerance & disaster recovery.

→ The size of (number of nodes) of a virtual cluster can grow or shrink dynamically, similar to the way an overlay nlw varies in size in a peer-to-peer (P2P) nlw.

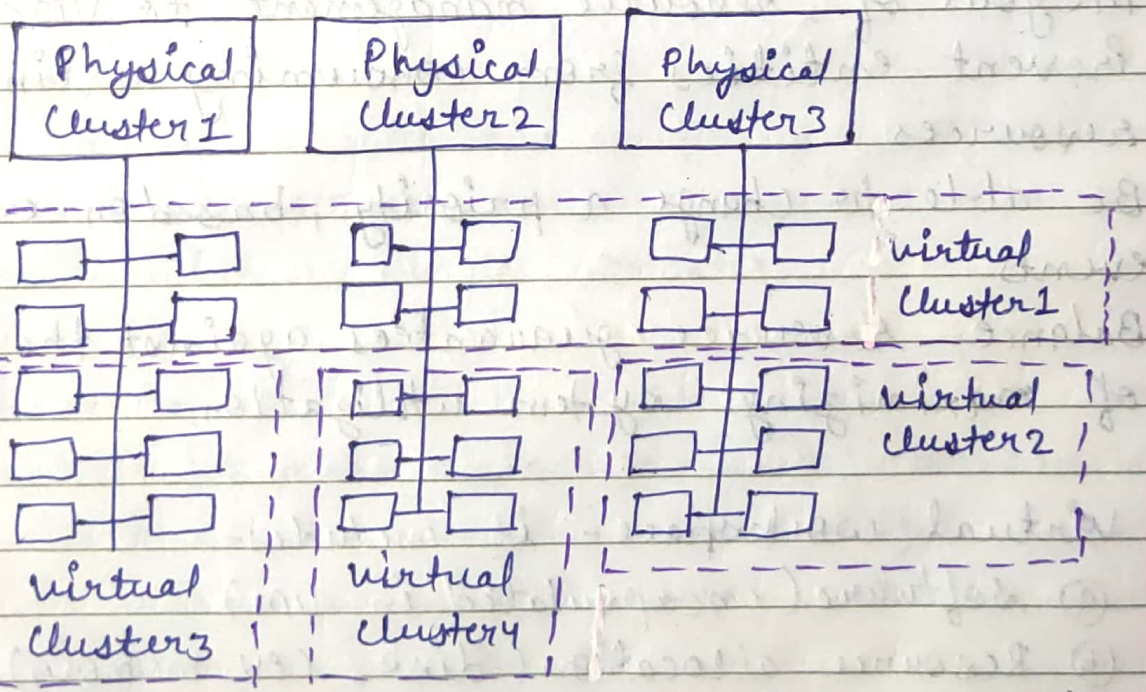


Fig- Physical & virtual clusters.

Advantages of cluster making-

→ Fast deployment and Effective scheduling
→ High Performance virtual storage
→ Load balancing

Teacher's Signature.....

PAGE NO.:
DATE: / /

★ Resource Management -

Resource management is an essential technique to utilize the underlying h/w of the cloud efficiently. The role of resource manager is to manage the allocation of physical resources to the virtual machines deployed on a cluster of nodes in a cloud.

Management of resource is important, because limited number of resources are shared among many consumers (virtual machines).

The goal of resource management to VMs are-

→ Prevent entities from consuming unlimited resources.

→ Be able to change a priority, based on external events.

→ Balance resource guarantees against the goal of maximizing system utilization.

Virtual workspace - it includes-

ⓐ software (encapsulated in VM)

ⓑ Resource allocation (disk, CPU, memory).

→ A virtual workspace is deployed at the CSP using the physical workspace.

→ workspaces are VMs running on the resource provider's node.

PAGE NO.:
DATE: / /

→ Users interact with workspace pretending as physical resources.

★ Server Virtualization –

It is a technique through which physical servers are partitioned into similar virtual servers that in turn maximizes server resources.

The resources of the server are hidden/masked from user & a sw is used to divide the physical server into multiple virtual servers.

Example:-

Web Server - Instead of giving a separate computer to each web server, multiple servers can run inside with a single computer.

★ Server virtualization is used:
→ to make more efficient use of server resources
→ to improve the server availability
→ to help in disaster recovery.
→ development & testing
→ to centralized the server administration

★ Advantages-

① Each virtual server is independent of other virtual server as it has its own operating system.

Teacher's Signature

② Low cost as less h/w is required
③ Save space as multiple machines can be consolidated into single server running multiple virtual environment.
④ Extreme (full) usage of resources & save operational costs.

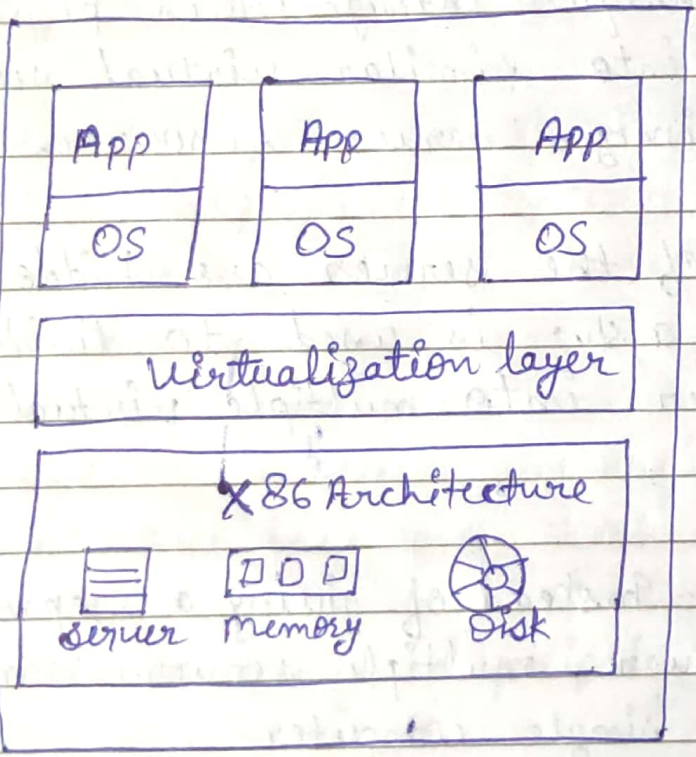


Fig- Server Virtualization

★ Desktop Virtualization-

→ Desktop virtualization, often called client virtualization, is a virtualization used to separate a computer desktop environment from the physical computer.

→ It is a client server computing model because the virtualized desktop is stored on a centralized or remote server.

→ Desktop virtualization virtualizes desktop computers and these virtual desktop environments are served to users on the n/w, as a physical desktop.

→ It allows to remotely log in to access desktop from any location.

→ VDI (Virtual Desktop Infrastructure / Interface) is a popular method of desktop virtualization.

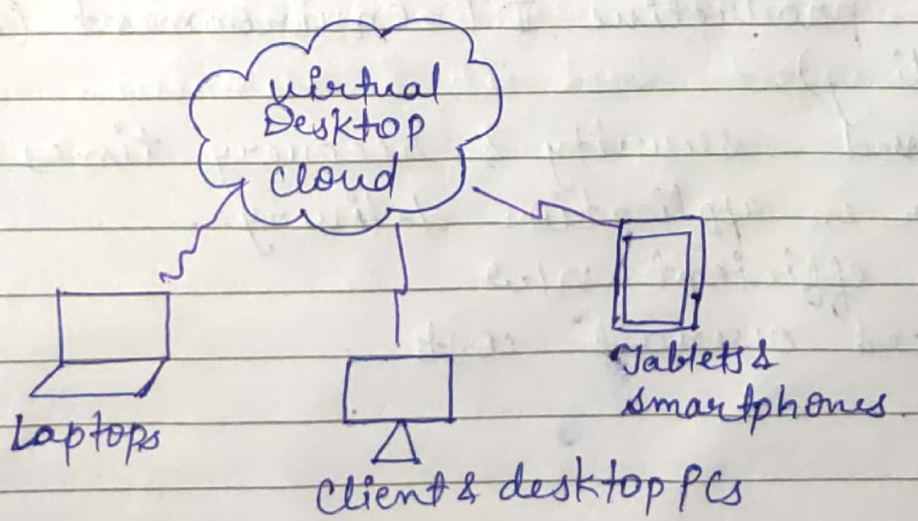


fig- Desktop virtualization.

Teacher's Signature.....

PAGE NO.:
DATE: / /

★ Network virtualization-

N/w virtualization is a method of combining the available resources in a n/w to consolidate or combine multiple physical n/w, divide a n/w into segments or create s/w networks between Virtual machines

N/w virtualization is intended to optimize n/w speed, reliability, flexibility, scalibility and security.

N/w vir. works by combining the available resources in a n/w & spliting up the available bandwidth into channel, each of which is independent from the others & each of which can be assigned (or assigned) to a particular server or device in real time.

Advantages of N.V.—

→ More productive IT environment (i.e. efficient scaling).
→ Improved security & recovery times.
→ Faster in application delivery.
→ More efficient n/w
→ Reduced overall costs.

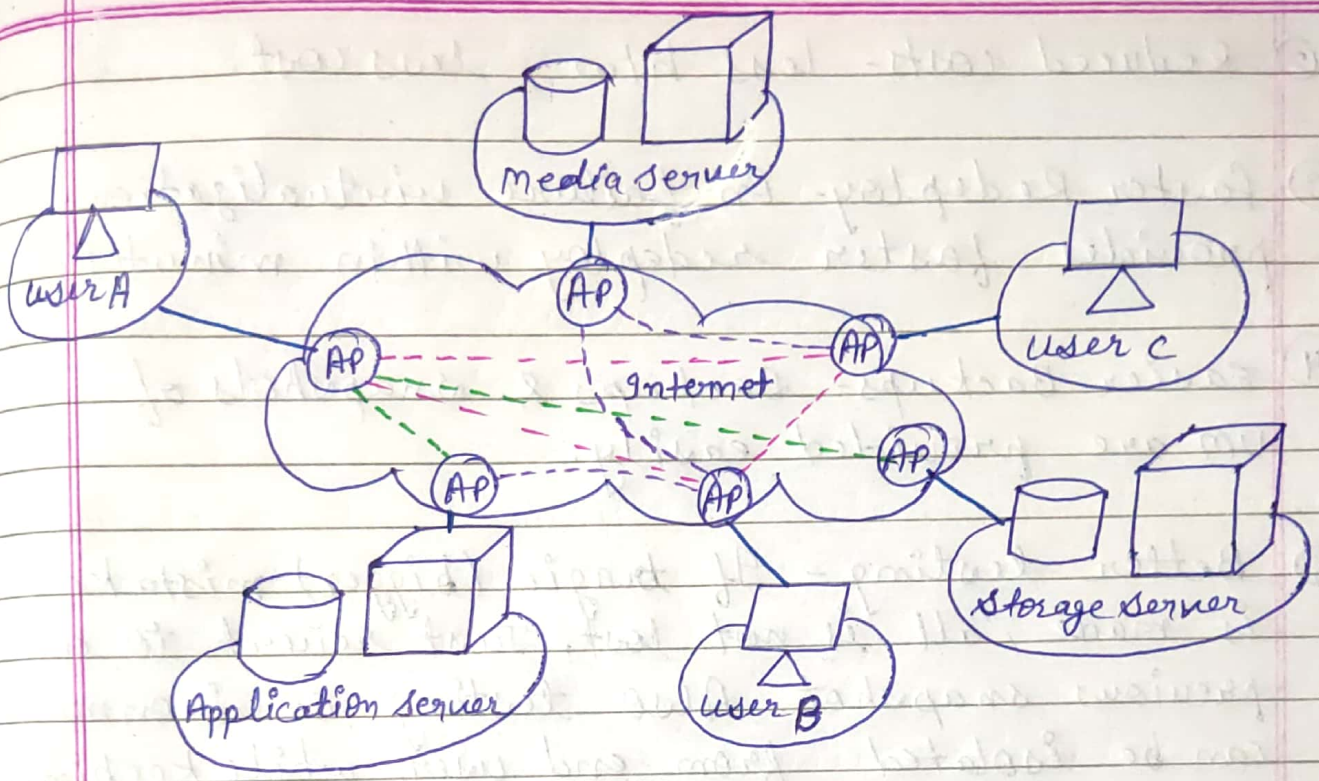


Fig- Network Virtualization

★ Virtualization of Data Center -

Data Center virtualization is the process of designing, developing and deploying a data center on virtualization and cloud computing technologies.

Data center virtualization can reduce costs on facilities, power, cooling and h/w, simplify administration and mintenance.

Benifits of vir. in data center -

① less Heat buildup - less physical h/w is used hence less heat is generated.

PAGE NO.:
DATE: / /

② Reduced costs- less h/w, less cost.

③ Faster Redeploy- On failure virtualization provides faster redeploy within minutes.

④ Easier Backups- Backups & snapshots of VM are provided easily.

⑤ Better testing - If tragic (bigger) mistake is made, all is not lost. Just revert to a previous snapshot. Also testing environment can be isolated from end user while keeping them online.

⑥ Easier migration to a cloud- Beyond the actual virtual machine, virtualized technology gets you closer to a cloud based mindset making migration more easy.

⑦ Better disaster Recovery - with up to date snapshots of virtual machines, you can quickly get back up & running.