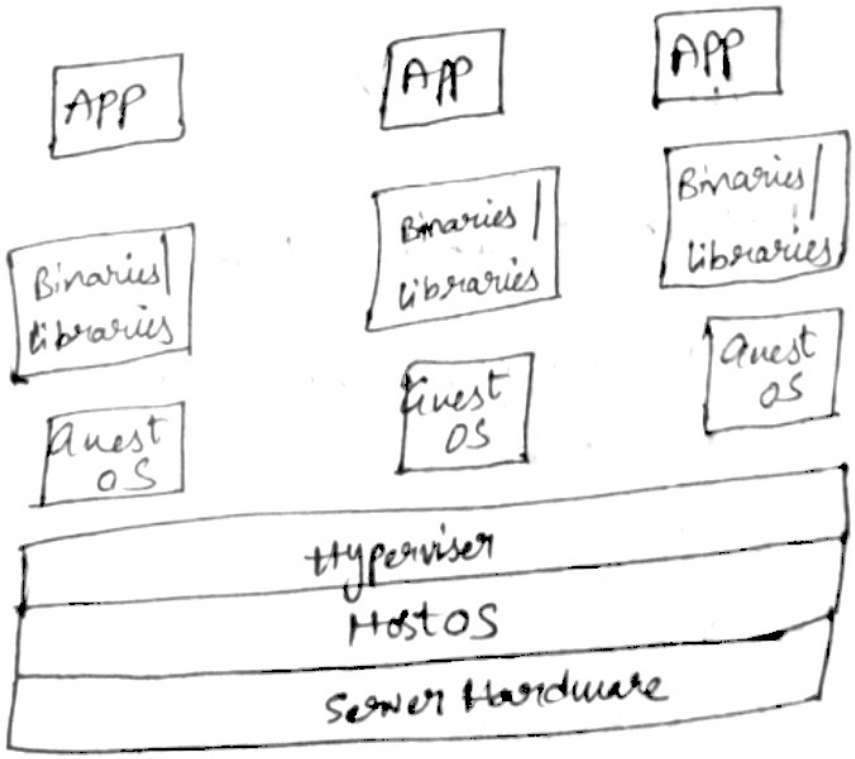
UNIT-II.

Virtualization:- It is a technique for creating a virtual platform of storage devices and the server OS.

→ It helps the user make use of multiple machines sharing one single physical instance of any resource across the network of other users respectively using their machines.

→ Moreover, virtualization technologies provide a virtual environment for not only executing applications but also for storage, memory, and networking.

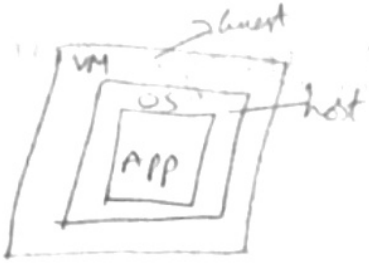


Virtualization.

* we can implement any services in cloud computing through virtualisation.

Ex: I had a laptop, wanted to install linux in MacOS and to use both s/w at a time now that laptop should be divided virtually not physically.

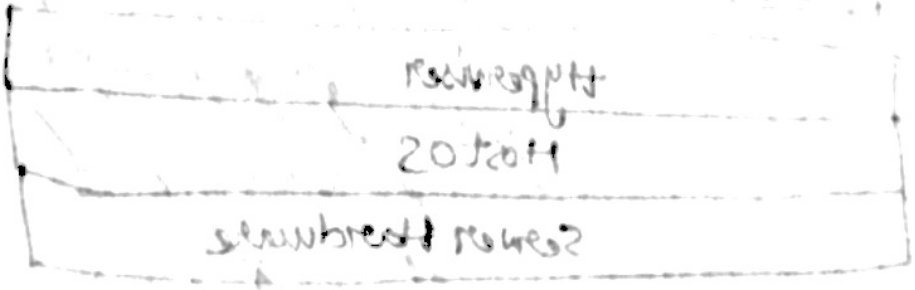
This complete process is known as virtualisation.



windows - host
↓
linux - Guest
(External installation)

* hypervisor - s/w

This s/w work is how to divide virtually and how many divisions it should take.



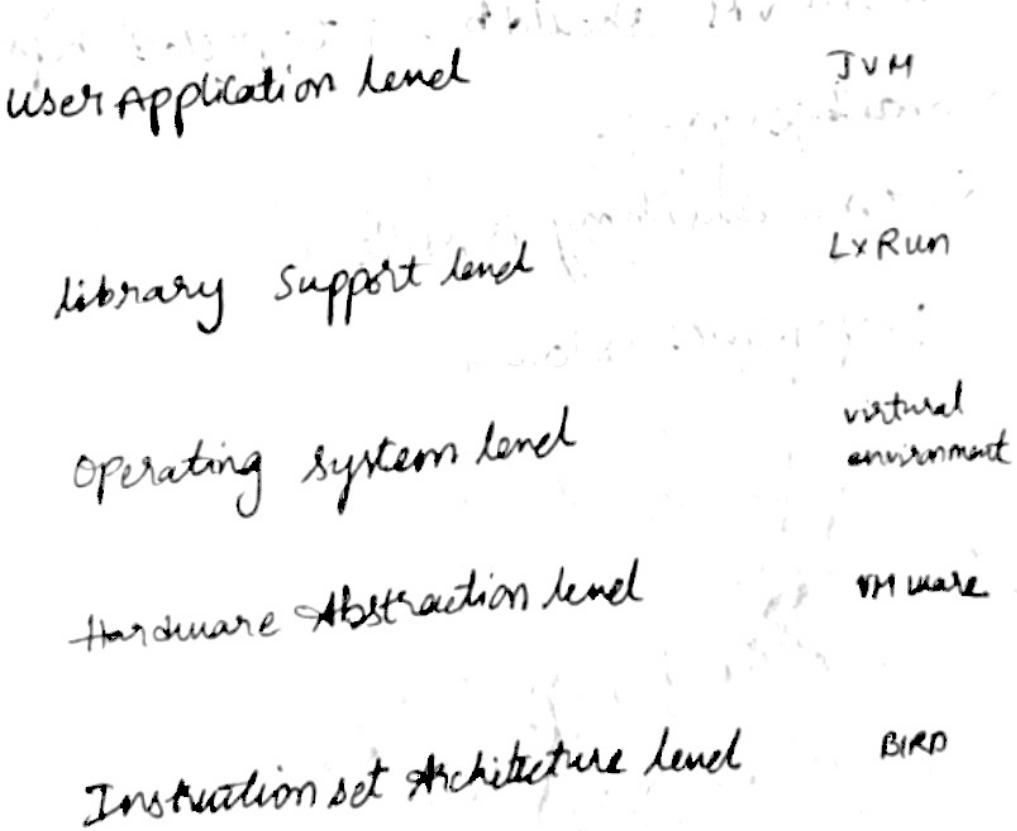
Implementation levels of virtualisation:-

There are 5 levels of virtualisation. They are:-

1. ISA (Instruction set Architecture level)
2. Hardware abstraction layer
3. Operating system level
4. Library support level
5. Application level

ISA:- It is used to run many legacy codes.

These codes run on any VM using ISA.



① ISA:- This level is an interface b/w s/w & h/w.

using this instruction s/w communicate with h/w.

→ when virtualisation is carried at this level, we create an emulator.

↓

→ It receives all instructions from VM & interprets them, then it maps those instruction to the instruction of host machine.

→ This technique is simple but every instruction from VM should be interpreted before mapping.

disadvantages are:-

So time consuming is more

Performance is low.

(2) HAL:-

→ In ISA level, performances goes down, due to interpretation of every instruction.

→ To overcome that we map virtual resources with physical resources.

→ When accessing of H/w come to virtual resources, they forwarded directly to physical resources.

→ Here every instruction is not interpreted, but we check whether instruction is privileged ↓ Some memory instruction. or non-privileged.

→ If instruction is non privileged, normal execution is done.

→ If it is privileged, then ctrl is passed to VMM which handles them accordingly.
↓
virtual machine monitor.

③ Operating system level:-

The layer is present b/w operating system and the applications is known as operating system layer.

* At this level, virtualization can be done using isolated containers which act as real servers and are created on only one physical server.

④ Library Support level:-

Virtualization at library level can be done simply by managing the API's associated with the applications and the system.

Ex:- wine tool developed for allowing windows application over UNIX system.

⑤ Application level:-

At this level user application is virtualized as a virtual machine. It is also called as process level virtualization because O.S considers each application as a process.

* In this, an application is made as virtual

machine and attached to the OS as a layer which manages different virtual machines.

Eg:- Sand boxing, application isolation.

VIRTUALIZATION STRUCTURES/TOOLS AND MECHANISMS:-

* Before virtualisation, the operating system manages the hardware.
* After virtualisation, a virtualization layer is inserted between the hardware and the operating system.
  In such case, the virtualization layer is responsible for converting portions of the real hardware into virtual hardware.
* Different operating systems such as linux and windows can run on the same physical machine simultaneously.
* Depending on the position of the virtualization layer, there are several classes of VM architectures.

→ Hypervisor architectures
→ Para-virtualization architecture
→ host-based virtualisation architectures.

* The hypervisor is known as VMM (virtual machine monitor)
* They both perform the same virtualization operations.

Hypervisor :-

* A hypervisor is a h/w virtualization technique allowing multiple operating systems, called guests to run on a host machine.

Two types of hypervisor. They are:
→ Bare metal hypervisor.
→ hosted hypervisor.

Type-1 :- Bare metal hypervisor :-

* Sits on the Bare metal computer h/w like CPU, memory etc.

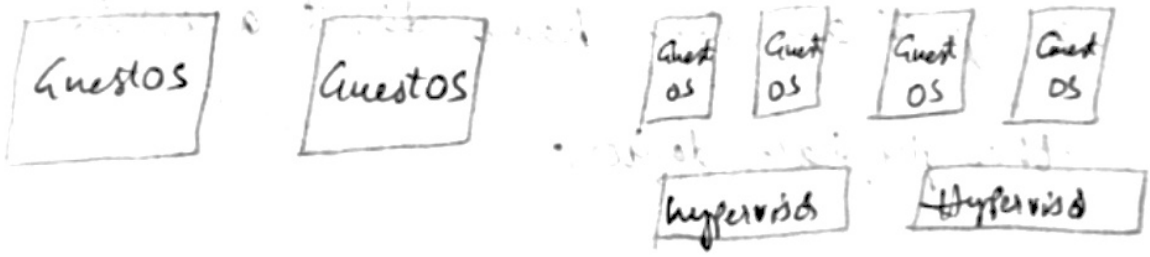
* All guest operating systems are a layer above the hypervisor.

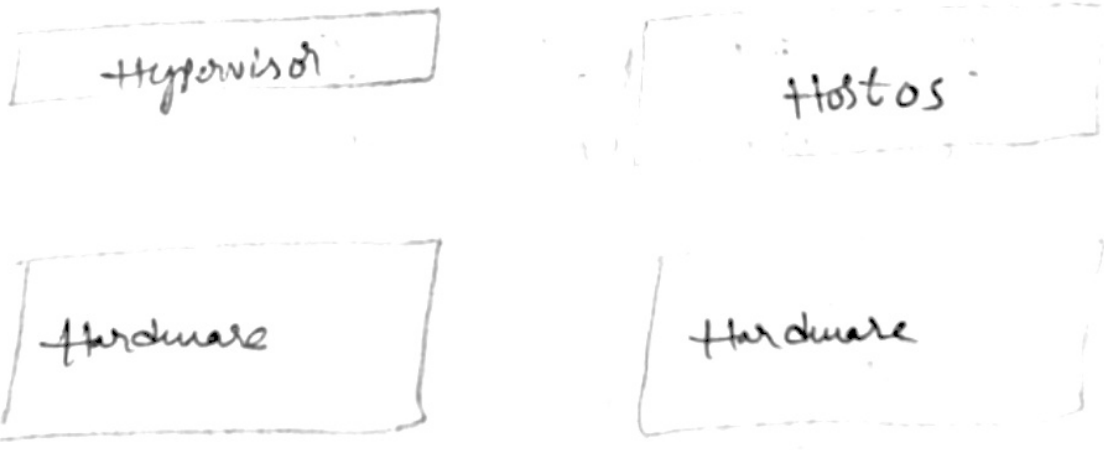
Ex:- CP/CMS (control program / cambridge monitor system) developed by IBM.

Type-2:- Hosted hypervisor:-

* In this one separate extra layer is installed (added) known as Host OS.

* Host OS is unaware of virtualization.





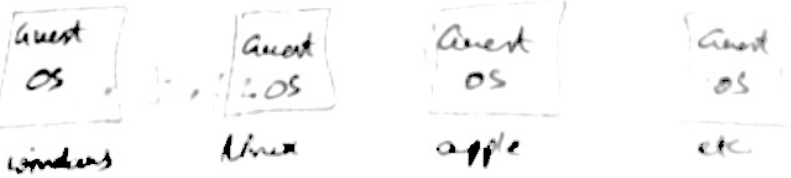
Type 1 (Bare-metal)

Type 2 (hosted)

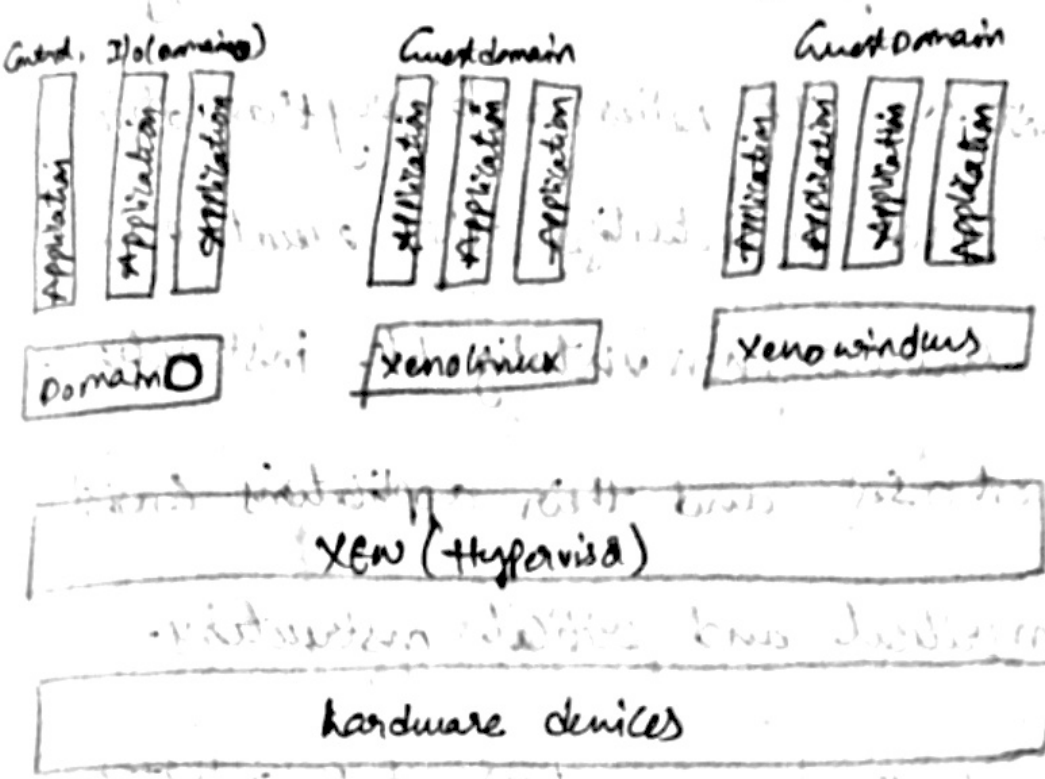
Example for bare metal hypervisor is XEN Architecture

XEN ARCHITECTURE:-

* xen is an open source hypervisor program developed by cambridge university.
* It makes possible to run many instances of an operating system & indeed different operating systems parallel on a single machine (& host).
* It just provides a mechanism by which a guest OS can have direct access to the physical devices.



Architecture of XEN:-



BINARY TRANSLATION WITH FULL VIRTUALIZATION:-

* Depending on implementation technologies, hardware virtualization can be classified into two categories

They are:

→ Full virtualization

→ Host-based virtualization.

* Full virtualization doesn't need to modify the host OS. It relies on binary translation to trap and to virtualizes the execution of certain sensitive, non virtualizable instructions.
* The guest OSes and their applications consist of non critical and critical instructions.
* In a host-based system, both a host OS and a guest OS are used. A virtualization software layer is built between the host OS and guest OS.

Para Visualization :-

It is a type of virtualization where software instructions from the guest OS running inside a virtual machine can use 'hypercalls' that communicate directly with the hypervisor.

Virtualization of cpu :-

H/w virtualization :-

H/w virtualization refers to the creation of virtual versions of computers and operating systems.

→ developed by intel and AMD for their server platforms

→ And designed to improve the performance of the processor.

→ This term H/w virtualization is known as h/w - assisted virtualization.

Advantages :-

→ H/w Virtualization has many advantages because controlling virtual machines is much easier than controlling a physical machine

→ lower cost.

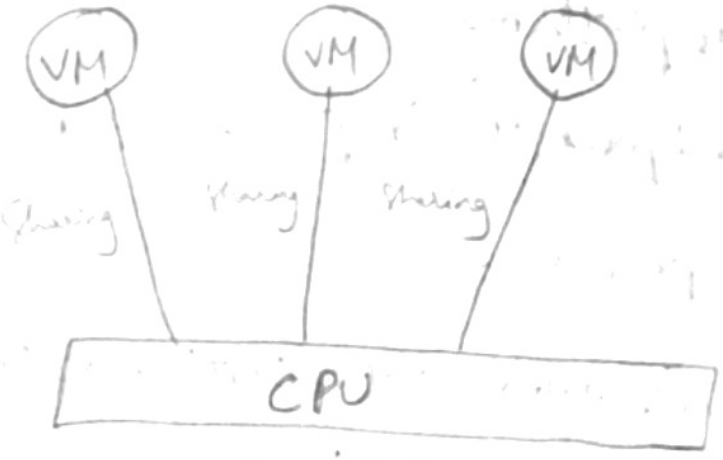
→ Decrease the quantity of rack space.

→ reduce no. of servers.

CPU virtualization:-

Central processing unit virtualization.

→ It allows a single CPU to be divided into multiple virtual CPUs for use by multiple VMs.



→ All VMs acts as physical machines and distribute their hosting resources like having various virtual processors.

→ sharing of physical resources takes place to each VM when all hosting services get request.

→ Finally VM's get a share of single CPU allocated to them, being a single processor

acting as dual-processor.

Types of CPU virtualization:-

① S/W Based CPU virtualization.
② H/W-Assisted CPU virtualization.
③ Virtualization and Processor-specific behaviour.
④ Performance implications of CPU virtualization.

① S/W Based CPU virtualization:-

→ Application code gets executed on the processor and the privileged code gets translated first, and that translated code gets executed directly on the processor.

→ The code that gets translated is very large in size and also slow at the same time on execution.

② H/W-Assisted CPU virtualization:-

→ Here Guest user uses a different version of code and mode of execution known as a guest mode.

→ there there is no requirement for translation while using for h/w assistance.

→ System calls runs faster than expected.

③ virtualization & Processor - Specific Behaviour:-

→ The VM still helps in detecting the processor model on which the system runs.

→ The processor model is different based on the CPU and the wide variety of features it offers, whereas the applications that produce the output generally utilize such features.

④ Performance Implications of CPU virtualization:-

→ It adds the amount of overhead based on the workloads and virtualization used.

→ Any application depends mainly on CPU power waiting for the instructions to

get Executed first.

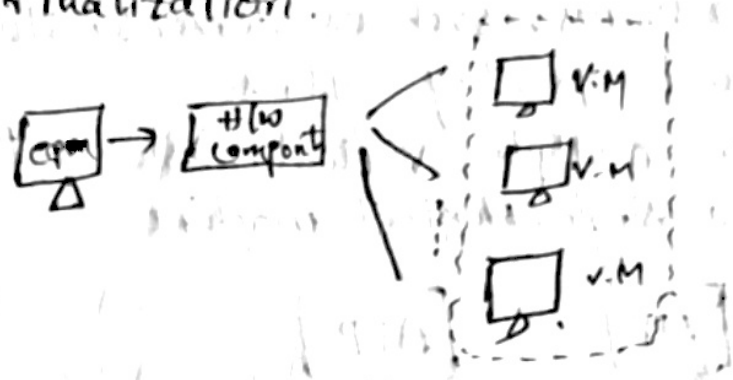
→ Such applications require the use of CPU virtualization that gets the command & executions that are needed to be executed first.

→ This overhead takes the overall processing time and results in an overall degradation in performance and CPU virtualisation execution.

VIRTUALIZATION OF MEMORY

Virtualization:

→ The process which allows a computer to share its h/w components to multiple virtual machines (virtual Environment) is known as virtualization.



Virtualization of Memory:

→ Virtual memory virtualization is similar to VM support provided by modern OS.

→ In a traditional execution the OS maintains mappings of VM to MM using page tables, which is a one-stage mapping from VM to MM.

→ All modern x86 CPUs include a MMU and a Translation Lookaside buffer (TLB) to optimize VM performance.

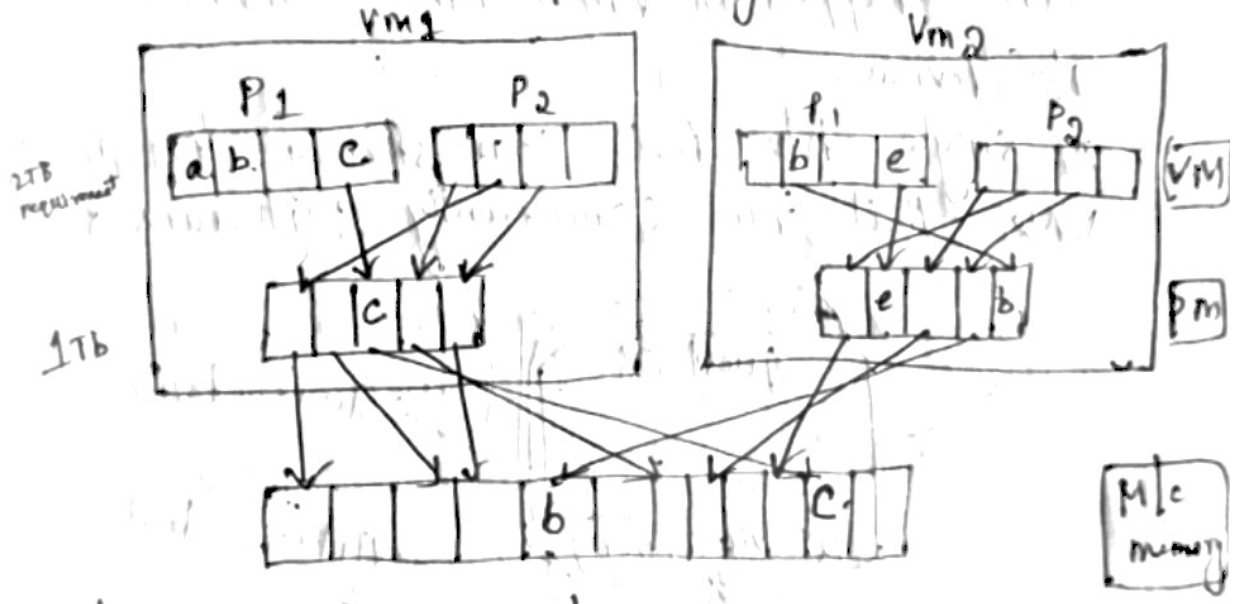
→ However virtual memory virtualization involves sharing the physical system memory in RAM and dynamically allocating it to the pm of VMs.

→ That means a two-stage mapping process should be maintained by the guest OS and VMM respectively 1) VM to PM 2) PM to MM.

→ Furthermore MMU virtualization should be supported, which is transparent to the guest OS

→ The guest OS continues to control the mapping of VA to the PMA of VM's. But the guest OS cannot directly access the actual m/c memory.

→ The VMM is responsible for mapping guest PM to actual m/c memory.



I/O VIRTUALIZATION:

Definition: It is a process which involves managing the data flow of I/O requests b/w virtual devices and shared physical h/w.

→ At the time of writing there are three ways to implement I/O virtualization:

1. Full device emulation
2. Para virtualization
3. Direct I/O

1. FULL DEVICE EMULATION:

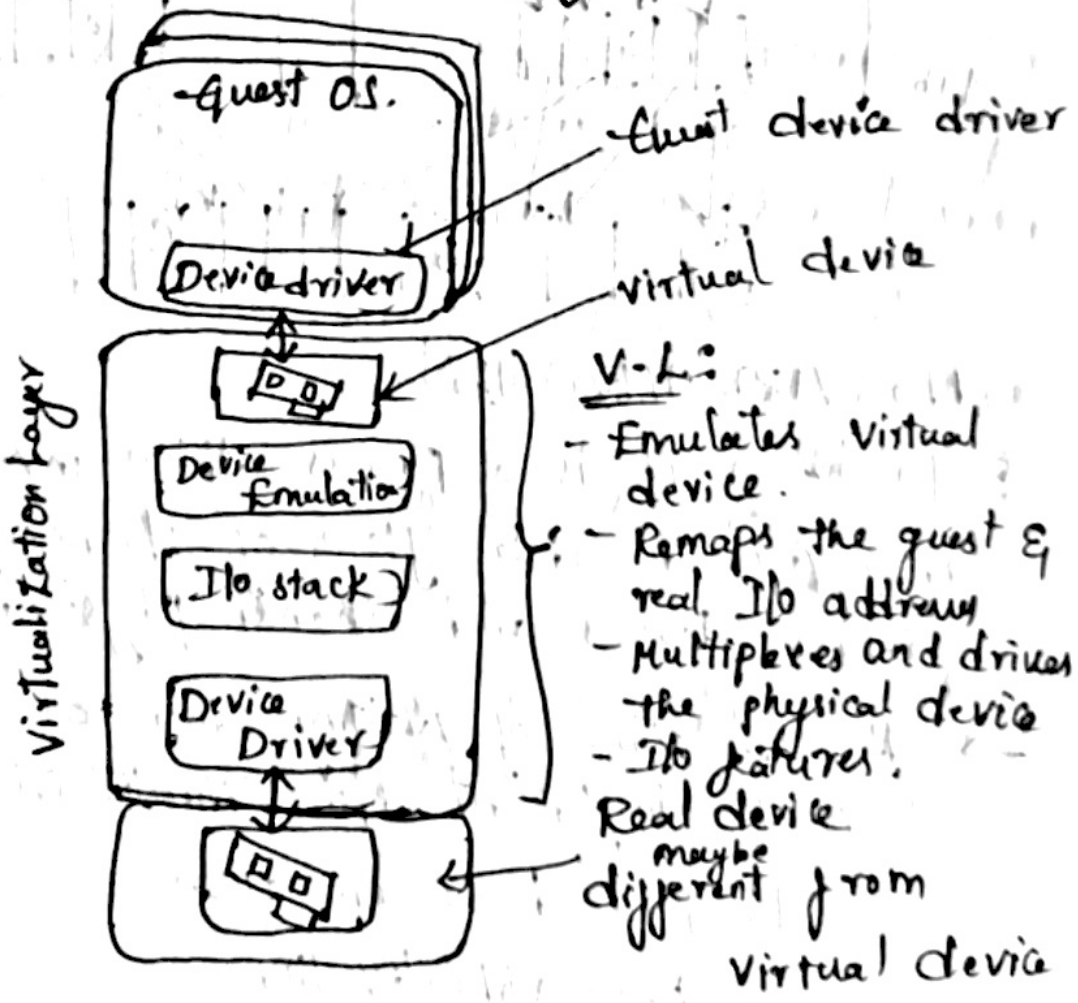
→ It emulates the well-known, real-world devices

→ All the functions of a device such as device enumeration, identification, interrupts & DMA are replicated in s/w.

→ This s/w is located in VMM acts as virtual device.

→ The I/o accss requests of the guest OS are trapped in VMM which interacts with I/o devices.

→ A single h/w device can shared by multiple VMs that run concurrently. & it runs slower



2. PARA VIRTUALIZATION:

→ It consist of frontend driver and backend driver

→ The frontend driver is running in Domain U and backend driver is running in Domain 0

* Domain 0: The guest OS which has control ability, is called Domain 0.

* Remaining are called Domain U.

→ The frontend driver manages the I/o requests of the guest OSes

→ Backend driver is responsible for managing the real I/o devices and multiplexing the I/o data of guest OSes. different VM.

→ Achieves better device performance than full device emulation.

3. DIRECT I/O:

→ It allows virtual machines to access devices directly.

→ It can achieve close-to-native performance without high CPU costs

VIRTUAL CLUSTERS AND RESOURCE MANAGEME

Physical versus Virtual cluster:

Cluster: cluster is a group of servers, computers and other resources that act like a single system

Physical cluster: It is a collection of servers (physical machines) interconnected by a physical N/W such as LAN.

Virtual cluster: Virtual machines are grouped and configured for high performance computing (or) Parallel computing

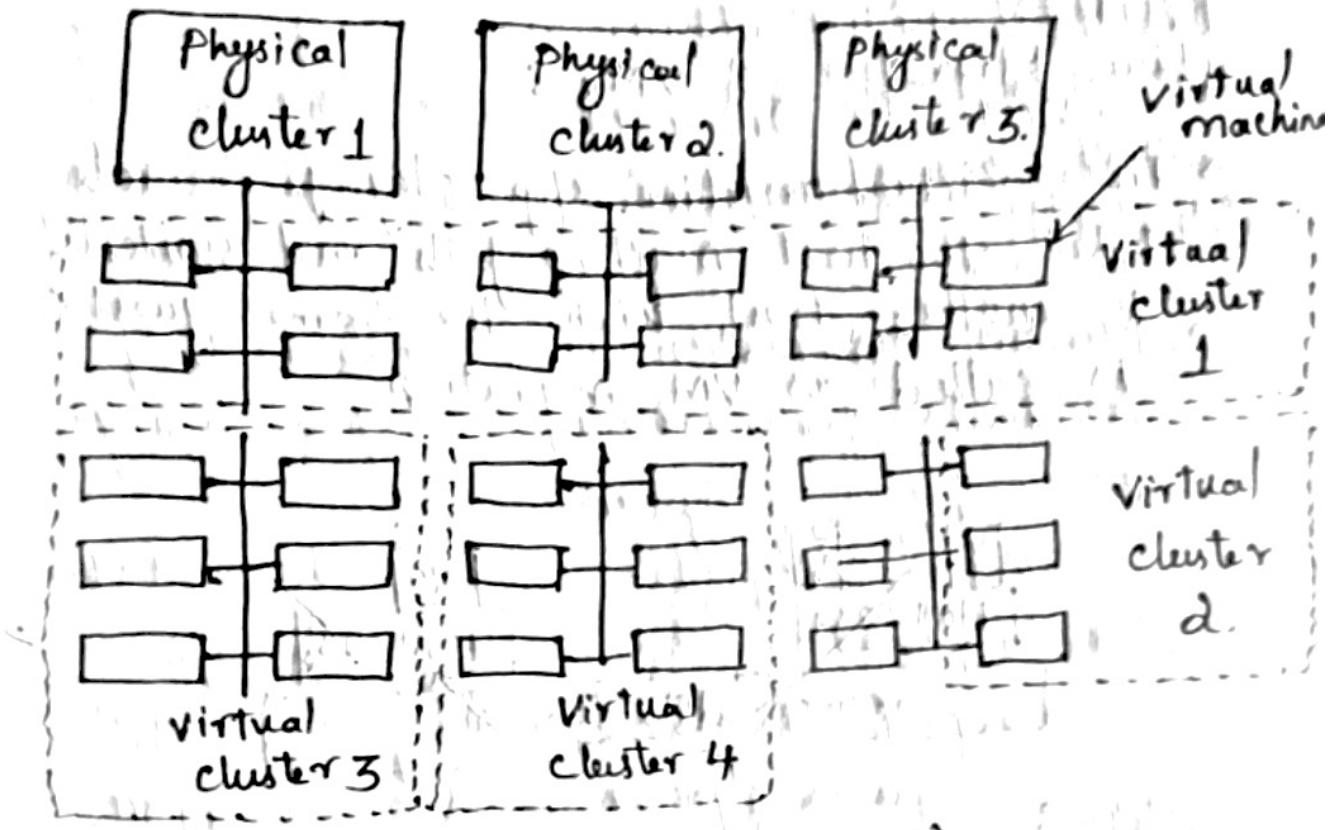
→ When a virtual cluster is created, different cluster features can be used such as load balancing, live migration of VM's across physical hosts

Virtual cluster properties:

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

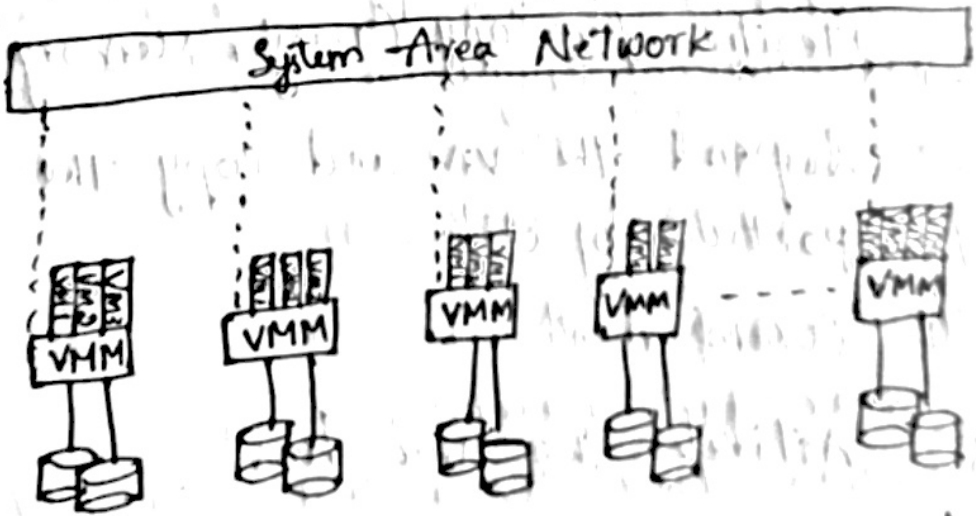
→ The failure of any physical nodes may disable some VMs installed on the failing nodes. But the failure of VMs will not pull down the host system.

→ VMs can be replicated in multiple servers for the purpose of promoting distributed parallelism, fault-tolerance, and disaster recovery.



SYSTEM AREA NETWORKS (SAN)

→ These are high-performance, connection oriented n/w's that link Computer clusters.

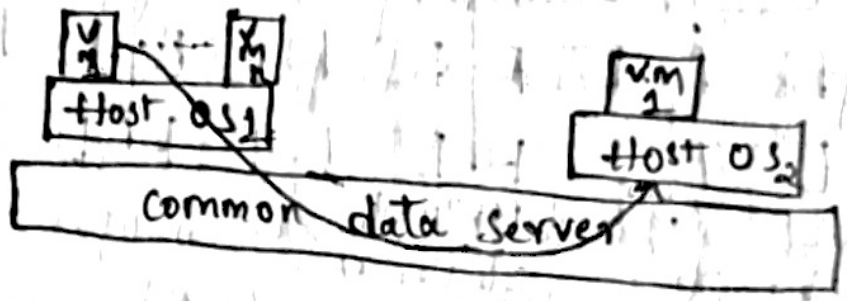


Virtual cluster nodes for different applications like A, B, C, D ....

Live VM migration steps and Performance effects

Live Migration of VMs:

→ The "virtual machine stop playing its role. When the host machine fails and switched to another host with the same guest OS. is called as "VM migration"



Steps:

Step 0: pre-migration

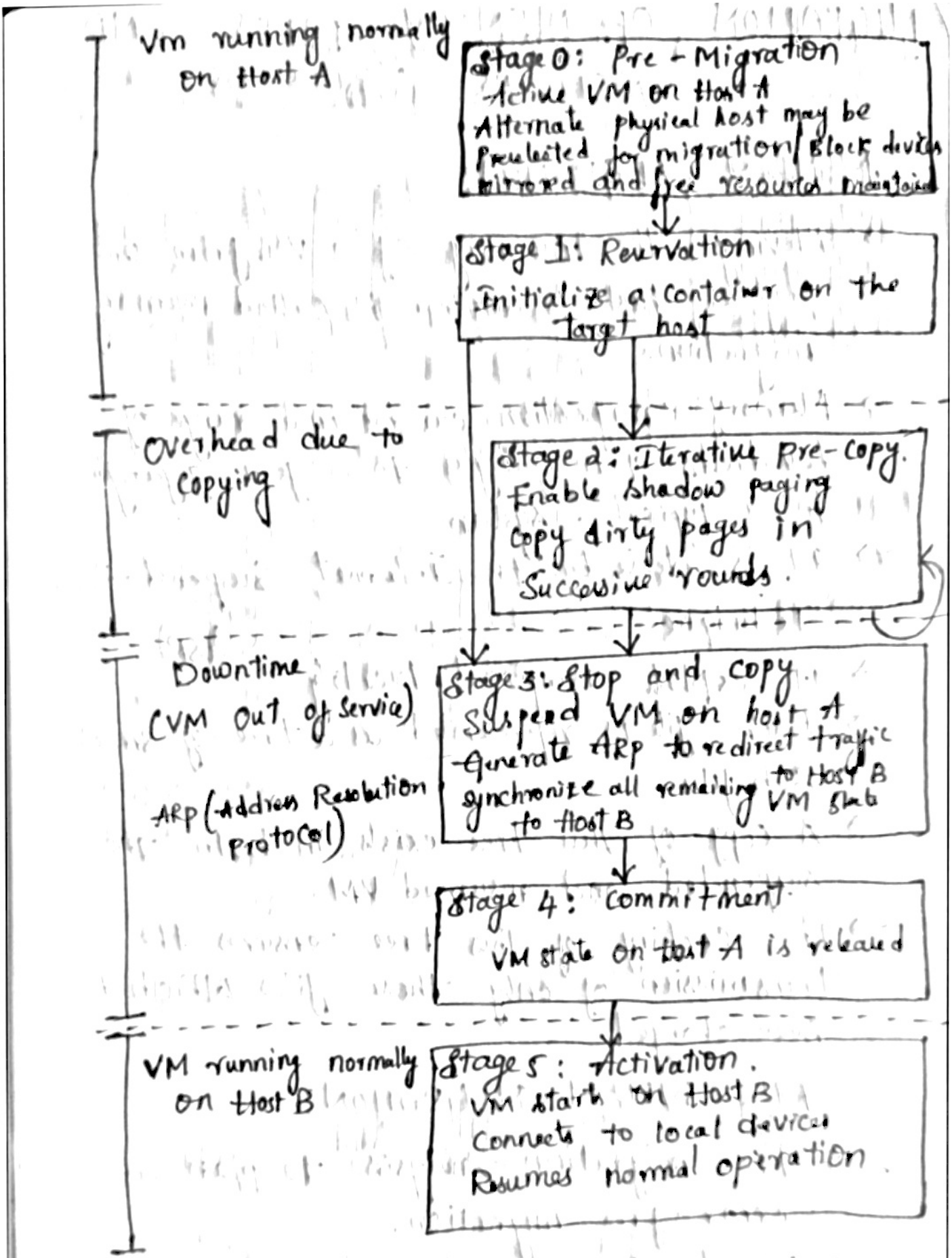
Step-1: Reservation

Step-2: Iterative pre-copy (Transfer Memory)

Step-3: Suspend the VM and copy the last portion of data

Step-4: Commitment

Step-5: Activate the new host



Live migration process of a VM from one host to another.

MIGRATION OF MEMORY, FILES AND NETWORK RESOURCES

MEMORY MIGRATION:

→ Moving the memory of a VM from one physical host to another is called memory migration.

→ Memory migration can be in a range of hundreds of megabytes to a few gigabytes in a typical system.

→ It is done by the Internet Suspend-Resume Technique. (ISR)

→ It explots temporal locality

→ Each file is represented as a tree of small sub-files

→ A copy of this tree exists in both the suspended and resumed VM.

→ the caching of this tree ensures the transmission of only those files which have been changed.

FILE SYSTEM MIGRATION:

→ Pre-migration analysis to plan an error-free migration.

→ Migrate large-sized files and folders without any restriction

→ Migrate specific data from file server

-to destination using filters
→ cloudMigrator can be used to migrate file system files to google drive, Microsoft OneDrive (or) Sharepoint.
→ This technique significantly reduces the amount of actual physical data that has to be moved

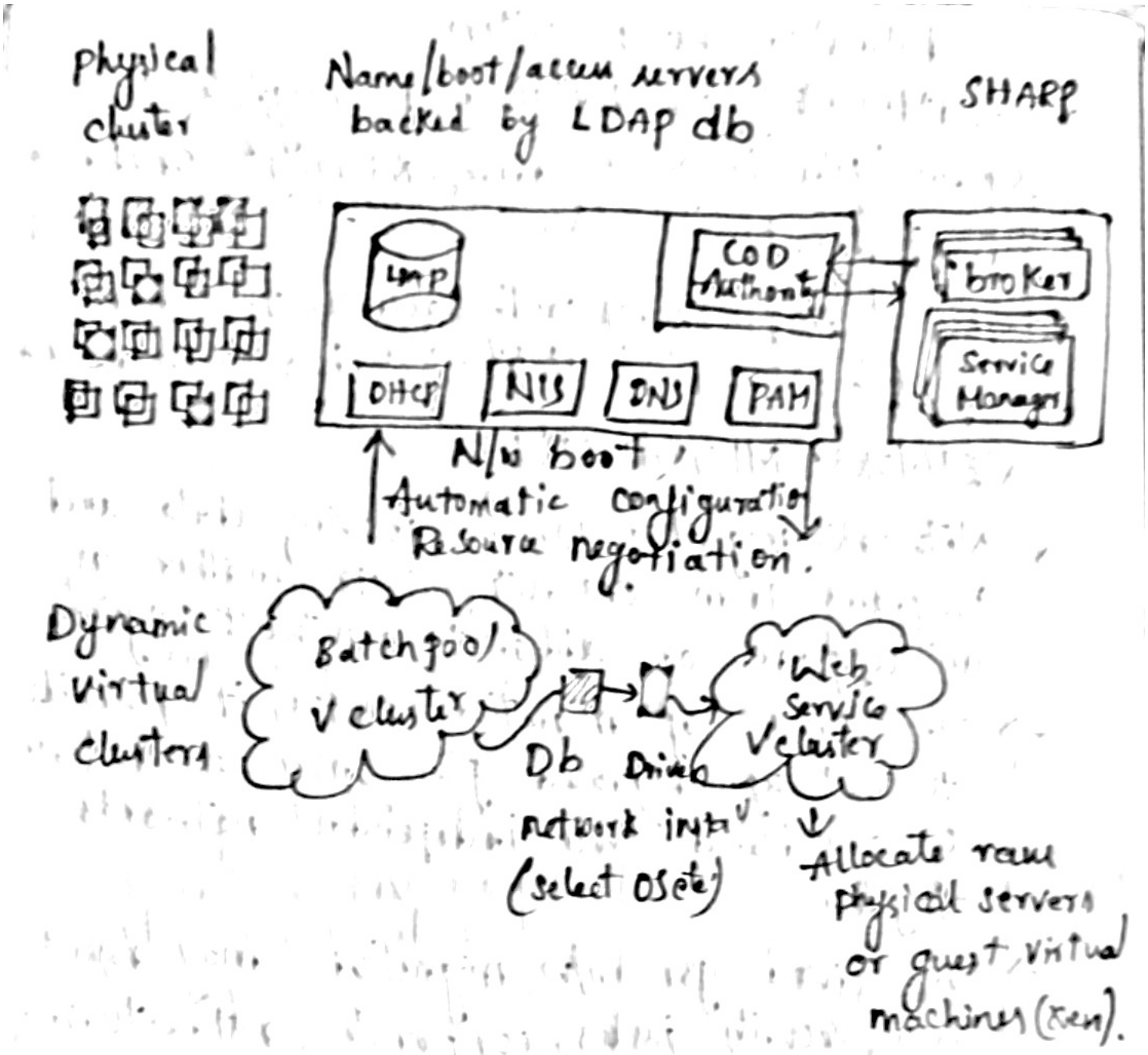
NETWORK MIGRATION:

→ Network migration involves moving data and Programs from one network, to another as an upgrade or add-on to a network system.
→ The process of migration makes it possible to set up migrated files on a new network or to blend two independent networks together
→ The need for n/w migration may result from security issues, corporate restructuring, increased storage needs and many other issues.

DYNAMIC DEPLOYMENT OF VIRTUAL CLUSTERS.

→ LDAP (Light Weight Directory Access Protocol)
→ It is a set of open protocols used to access and modify centrally stored information over a network.

DHCP-(Dynamic Host Configuration Protocol)
→ It is a protocol that provides quick, automatic, and central management for the distribution of IP addresses within a n/w


Physical cluster
Name/boot/accm servers backed by LDAP db
SHARP
LDAP
COD Authority
broker
Service Manager
DHCP
NIS
DNS
PAM
N/w boot, Automatic configuration Resource negotiation.
Dynamic virtual clusters
Batch pool Vcluster
Web service Vcluster
Db Disk
network into (select OS etc)
Allocate raw physical servers or guest virtual machines (Xen).

VIRTUALIZATION FOR DATA-CENTRE AUTOMATION

Cloud	Data Center
→ An off-premises form of computing that stores data on the internet	→ An on-premise h/w that store data within an organization local n/w
→ Cloud services are outsourced to third party cloud providers who perform all updates and ongoing maintenance	→ Data Centers are typically run by an in house IT department

Data Centers:

→ DATA Centers are where, computing facilities and networking equipment are located and centralized.

→ They are tasked to collect, store, process, and distribute large amount of data.

→ They are also responsible for data backup and recovery, as well as networking.

DATA CENTER VIRTUALIZATION:

→ It is basically a process where the design, development and deployment of data center on cloud computing and virtualization technology is performed.

→ It reduces operational and data center capital cost and also supports the optimization of infrastructure and resource utilization.

BENEFITS:

→ Reduce capital

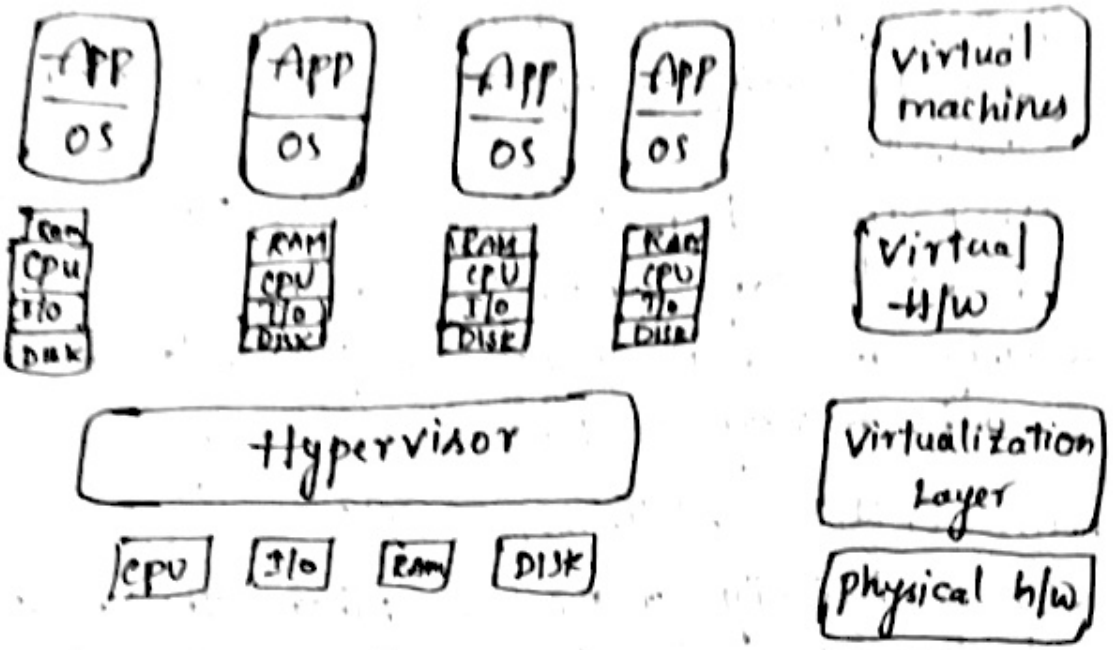
→ Deliver High Application Availability

→ Improve Business continuity

→ Increase productivity

→ Improve Responsiveness.

DATA CENTER-SERVER VIRTUALIZATION:



A:- Data centers have grown rapidly in recent years, and all major IT companies are pouring their resources into building new data centers.

→ In addition, Google, Yahoo!, Amazon, Microsoft, Hp, Apple, and IBM are all in the game.

→ All these companies have invested billions of dollars in data center construction and automation

→ Now data centers consist of thousands of potent and tiny servers that run non-stop around the clock

→ It means that huge volumes of h/w S/w and db resources in these data centers can be allocated dynamically to millions of Internet users simultaneously, with

guaranteed Quality of Service and Cost effectiveness.

→ Virtualization is moving towards enhancing, mobility, reducing planned downtime and increasing the number of virtual clients

→ The latest virtualization development highlights high availability (HA), backup services, workload balancing, and further increases in client bases.

SERVER CONSOLIDATION IN DATA CENTERS:

Def: It is an approach to improve the low utility ratio of h/w resources by reducing the no. of physical servers.

VBS

→ Consolidation is most powerful technique

→ It is common that most servers in data centers are underutilized

→ A large amount of h/w, space, power, and management cost of these servers is wasted

→ Among several server consolidation techniques such as centralized and physical consolidation ...

→ In virtualized data centers an efficient on-demand, fine-grained scheduler is one of the key factors to improve resource utilization.

→ Scheduling and reallocations can be done in a wide range of levels in set of data centers.

→ To automate data center operations, one must consider resource scheduling, architectural support, power management, automatic (or) autonomic resource management, Performance of analytical models and many.

VIRTUAL STORAGE MANAGEMENT:

→ The most important aspects of system virtualization are encapsulation and isolation.

→ Traditional operating system and applications running on them can be encapsulated in VM's.

→ only one OS runs in a virtualization while many applications run in the OS

→ System virtualization allows multiple VM's to run on a physical machine and the VM's are completely isolated.

→ To achieve encapsulation and isolation both system s/w and h/w platform, such as CPUs and chipsets, are rapidly updated. However storage is lagging.

→ The storage systems become the main bottleneck of VM deployment.

CLOUD OS FOR VIRTUALIZED DATA CENTERS

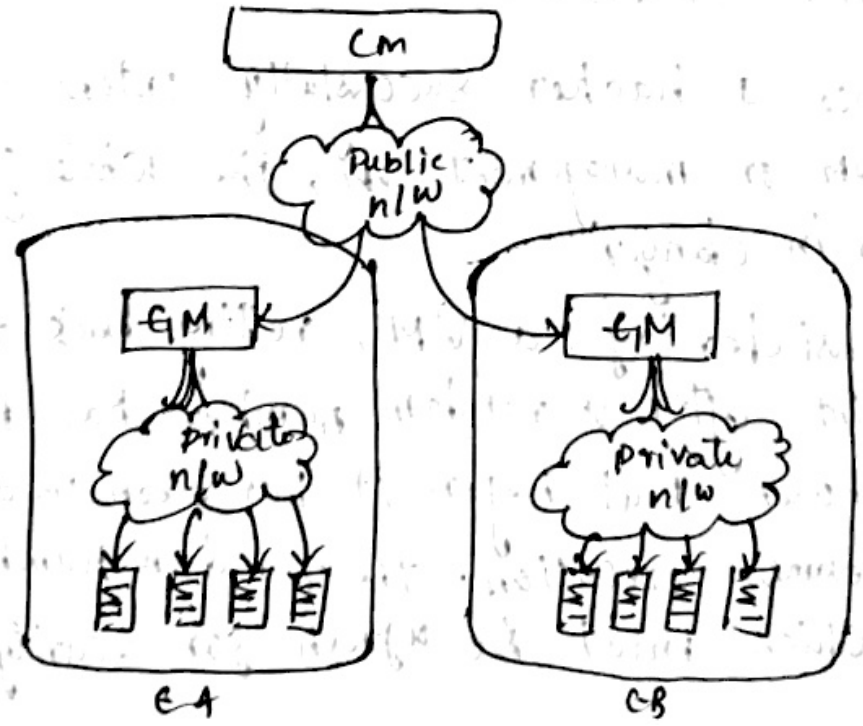
→ Eucalyptus is an open source s/w system intended mainly for supporting (IaaS) clouds

→ The system primarily supports virtual n/wing and the management of VM's. Virtual storage is not supported

→ Its purpose is to build private clouds that can interact with end users through Ethernet or the internet.

→ The system also supports interaction with other private clouds or public clouds over the Internet.

→ The system is short on security and other desired features for general-purpose grid or cloud application.



Instance Manager:

→ Controls the execution inspection, and terminating of VM instances on the host where it runs

Group Manager:

→ Gathers information about and schedules VM execution on specific instance managers, as well as manages virtual instance n/w

Cloud Manager:

→ It is the entry-point into the cloud for users and administrators.

→ It queries node managers for information about resources, makes scheduling decisions, and implements them by making requests to group managers

TRUST MANAGEMENT IN VIRTUALIZED DATA CENTERS

→ Once a hacker successfully enters the VMM or management VM, the whole system is in danger

→ Considering a VM, rolling back to a point after a random number has been chosen but before it has been used, resumes execution; the random number, which must be fresh for security purpo

is reused.

→ With a stream cipher too difficult plaintexts could be encrypted under the same key stream, which could in turn expose both plaintexts if the plain texts have sufficient redundancy.

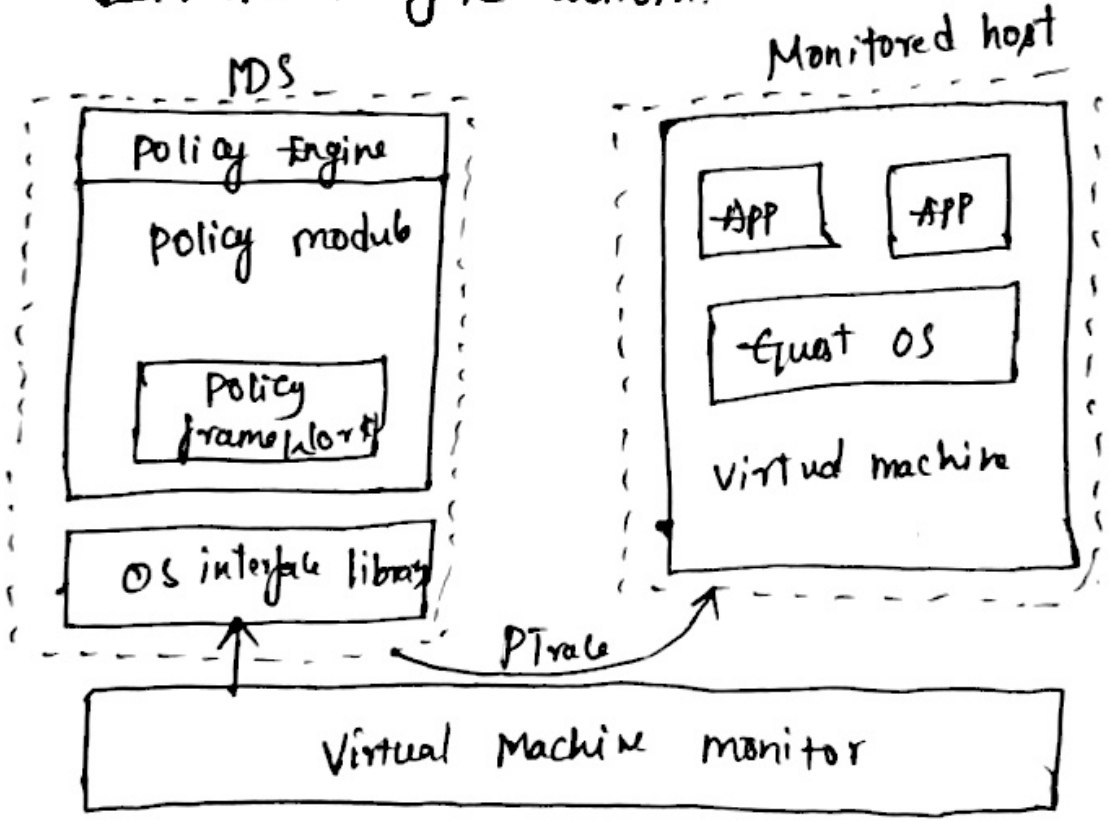
VM-Based Intrusions Detection:

→ Intrusions are unauthorized access to a certain computer from local or n/w users

→ It is used to recognize the unauthorized access.

→ It is built on OS.

→ Network intrusion Detection System (NIDS) is based on the flow of n/w traffic which can't detect fake actions.



→ VM Based IDS contains a policy Engine and a policy module.

→ The policy framework can monitor events in different guest VMs by OS interface library and pTrace indicates Trace to Secure policy of monitored host.

→ It is difficult to predict and prevent all intrusions without delay.

→ The IDS log service is based on the OS kernel. Thus, when an OS is invaded by attackers, the log service should be unaffected.