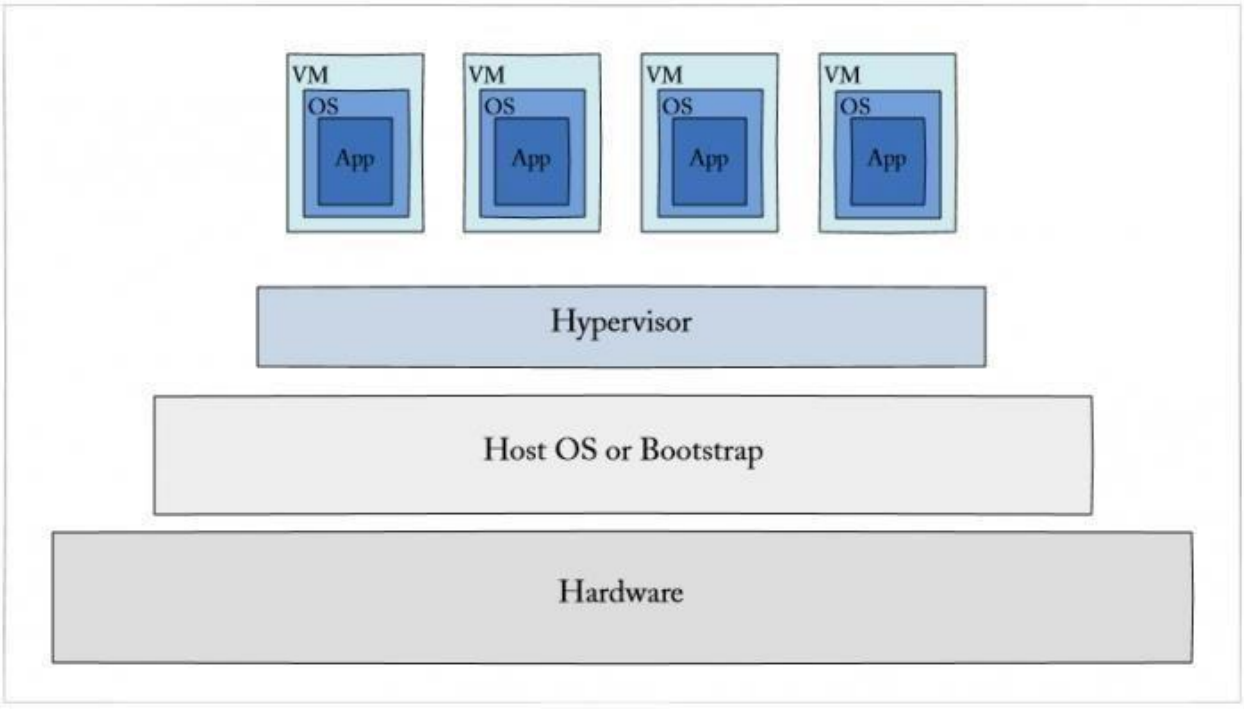
Unit 3: Cloud Virtualization technology

Overview of Virtualization Techniques

- Virtualization is the "creation of a virtual (rather than actual) version of something, such as a server, a desktop, a storage device, an operating system or network resources".
- In other words, Virtualization is a technique, which allows to share a single physical instance of a resource or an application among multiple customers and organizations.
- It does by assigning a logical name to a physical storage and providing a pointer to that physical resource when demanded.



Unit 3: Cloud Virtualization technology

What is the concept behind the Virtualization?

- Creation of a virtual machine over existing operating system and hardware is known as Hardwar Virtualization.
- A Virtual machine provides an environment that is logically separated from the underlying hardware.
- 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
- This virtual machine is managed by a software or firmware, which is known as hypervisor.

Difference between Virtualization and Cloud

- Though cloud technology requires the concept of virtualization. Virtualization is a technology. it can also be treated as software that can manipulate hardware. At the same time, cloud computing is a service that is the result of manipulation.

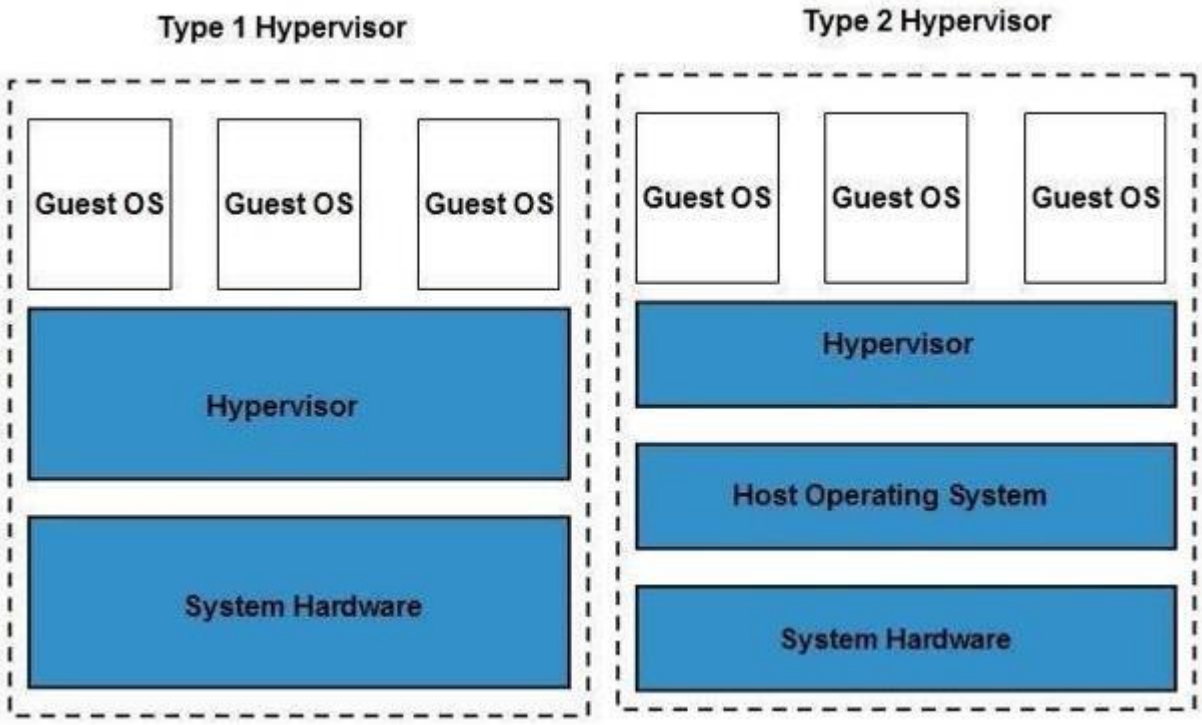
- Virtualization is the foundation element of cloud computing, whereas Cloud technology is the delivery of shared resources as a service-on-demand via the internet.
- Cloud is essentially made-up of the concept of virtualization.

Hypervisor

- The hypervisor is a firmware or low-level program that acts as a Virtual Machine Manager.
- There are two types of hypervisor:

- **Type 1 hypervisor** executes on physical hardware. The type1 hypervisor does not have any host operating system. Eg. LynxSecure, RTS Hypervisor, Oracle VM, Sun xVMServer, VirtualLogic VLX

- **Type 2 hypervisor** is a software interface that runs on top of an existing operating system Eg. Containers, KVM, Microsoft Hyper V, VMWare Fusion, Virtual Server 2005 R2, Windows Virtual PC and VMWare workstation 6.0.



Unit 3: Cloud Virtualization technology

Types of Virtualizations

- Hardware Virtualization
    - Full Virtualization
    - Paravirtualization (OS Assisted Virtualization)
    - Emulation Virtualization
- Operating System Virtualization.
- Server Virtualization.
    - Hypervisor
    - Full Virtualization
    - Para Virtualization
    - Operating System Virtualization
    - Hardware Assisted Virtualization
    - Kernel-Level Virtualization
- Storage Virtualization.
- Network Virtualization
- Desktop Virtualization

Hardware Virtualization

- The hypervisor manages shared physical resources of the hardware between the guest operating systems and host operating system. The physical resources become abstracted versions in standard formats regardless of the hardware platform. The abstracted hardware is represented as actual hardware. Then the virtualized operating system looks into these resources as they are physical entities.

- Virtualization means abstraction. Hardware virtualization is accomplished by abstracting the physical hardware layer by use of a hypervisor or VMM (Virtual Machine Monitor).

- When the virtual machine software or VMM or hypervisor software is directly installed on the hardware system is known as hardware virtualization.

- The main job of hypervisor is to control and monitoring the processor, memory and other hardware resources.
- After virtualization of hardware system, we can install different operating system on it and run different applications on those OS.

Usage of Hardware Virtualization

- It is mainly used for the server platforms, because controlling virtual machines is much easier than controlling a physical server.

Advantages of Hardware Virtualization

1. More Efficient Resource Utilization: Physical resources can be shared among virtual machines.
2. Lower Overall Costs Because of Server Consolidation: Co-existence of multiple operating systems on a single hardware platform drops significantly the number of servers, rack space, and power consumption.

3. Increased Uptime Because of Advanced Hardware Virtualization Features:

Advanced hardware virtualization technologies improve system uptime, availability, and reliability by reducing downtime caused by hardware failures**,** maintenance**,** or resource limitations**.**

4. Increased IT Flexibility: It helps for quick deployment of server resources in a managed and consistent ways.

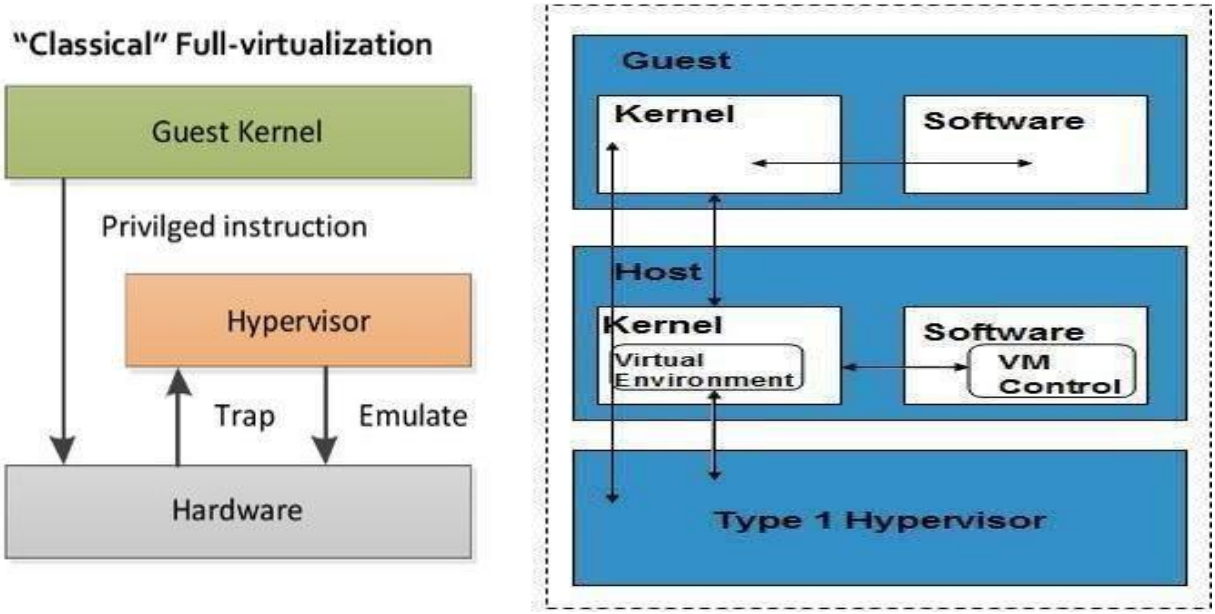
Types of Hardware Virtualization

Full Virtualization

- The hypervisor completely simulates the underlying hardware.
- Guest software does not require any modification to run.

- Full virtualization uses a combination of direct execution and binary translation. This allows direct execution of non-sensitive CPU instructions, whereas sensitive CPU instructions are translated on the fly into safe, equivalent instructions that the physical CPU can understand and execute.
- To improve performance, the hypervisor maintains a cache of the recently translated instructions.
- VMware's ESXi server uses this technique to achieve server virtualization.
- In full virtualization, trap and emulate allows an unmodified guest OS to run by trapping privileged instructions and having the hypervisor emulate them. The guest OS is unaware it is running inside a VM, but this method is slower due to the overhead of trapping and emulating

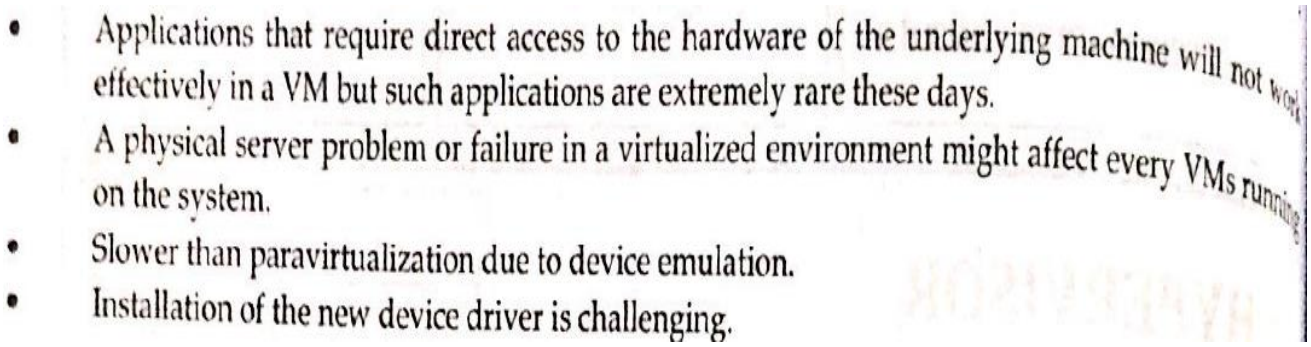
instructions. For example, when the guest OS tries to access hardware, the CPU traps the instruction, and the hypervisor performs it safely.



Advantages

- Full virtualization does not require OS assistance to virtualize a computer or create VMs so no modification to the Guest operating system is required. The hypervisor manages resources and translates instructions quickly and it also enables the OS to emulate new hardware, which can improve reliability, security, and productivity in a system.
- Enables admins to run applications on a completely isolated guest OS, which provides support for multiple OS simultaneously - such as Windows Server 2016 in one VM, Windows Server 2019 in another VM, and Ubuntu in another VM, and so on - all on the same computer.
- Provides features, such as easy VM backups and migrations, enabling VMs to be easily moved from one computer to another without disrupting the VM and its workload.

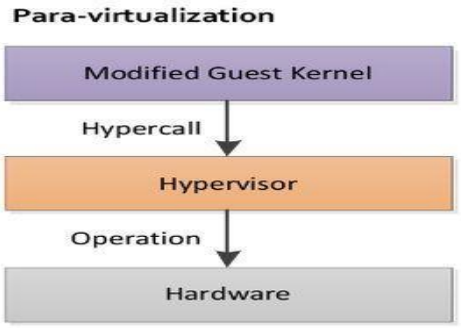
Disadvantages

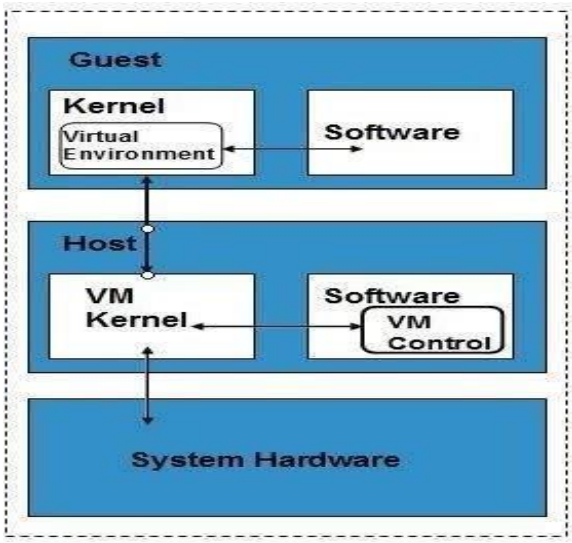


- Applications that require direct access to the hardware of the underlying machine will not work effectively in a VM but such applications are extremely rare these days.
- A physical server problem or failure in a virtualized environment might affect every VMs running on the system.
- Slower than paravirtualization due to device emulation.
- Installation of the new device driver is challenging.

Paravirtualization (OS Assisted Virtualization)

- The hypervisor doesn't simulate underlying hardware
- The guest software run their own isolated domains.
- The guest OS uses hyper calls to execute sensitive CPU instructions
- In para-virtualization, hypercall**s** are used, where the guest OS is modified to directly call the hypervisor instead of executing sensitive instructions. This avoids traps and is faster, allowing efficient communication between the guest OS and hypervisor. Hypercalls are used for tasks like memory allocation or I/O requests. Overall, trap and emulate is used for unmodified OSs, while hypercalls require a modified OS but provide better performance.
- VMware sphere is highly developed infrastructure that offers a management infrastructure framework for virtualization.
- It virtualizes the system, storage and networking hardware.
- The open-source Xen project uses the paravirtualization technique.





Advantages:

- Direct communication between the guest kernel and the hypervisor enhances overall performance.
- The thin software layer developed in PV manages virtual server traffic by enabling a single guest OS to have access to the physical hardware device while blocking access to all other guest OS.
- There is less virtualization overhead since PV does not attempt to entirely reconstruct the hardware.
- PV does not provide device drivers since it makes use of the drivers that are already available in the guest OS. Therefore, organizations can take full advantage of the hardware in the server instead of being limited to hardware with available drivers, as is the case in full virtualization.

Disadvantages:

- Any interaction with the PV interfaces requires modifications to the guest OS
- Because paravirtualization cannot function with unaltered guest operating systems, its interoperability and portability with systems such as Microsoft Windows are limited.
- Because the production environment requires extensive guest kernel changes, significant support and maintenance difficulties may occur.

Emulation Virtualization

- The virtual machine simulates the hardware and hence becomes independent of it.
- Emulation is a virtualization technique in which a virtual machine simulates the complete hardware of a computer in software. This allows an operating system or application designed for one hardware platform to run on a completely different platform.
- The guest operating system does not require modification
- The emulator software translates the instructions of the guest system into instructions that the host system can understand.
- The guest system operates as if it is running on its native hardware, even if the actual hardware is different.

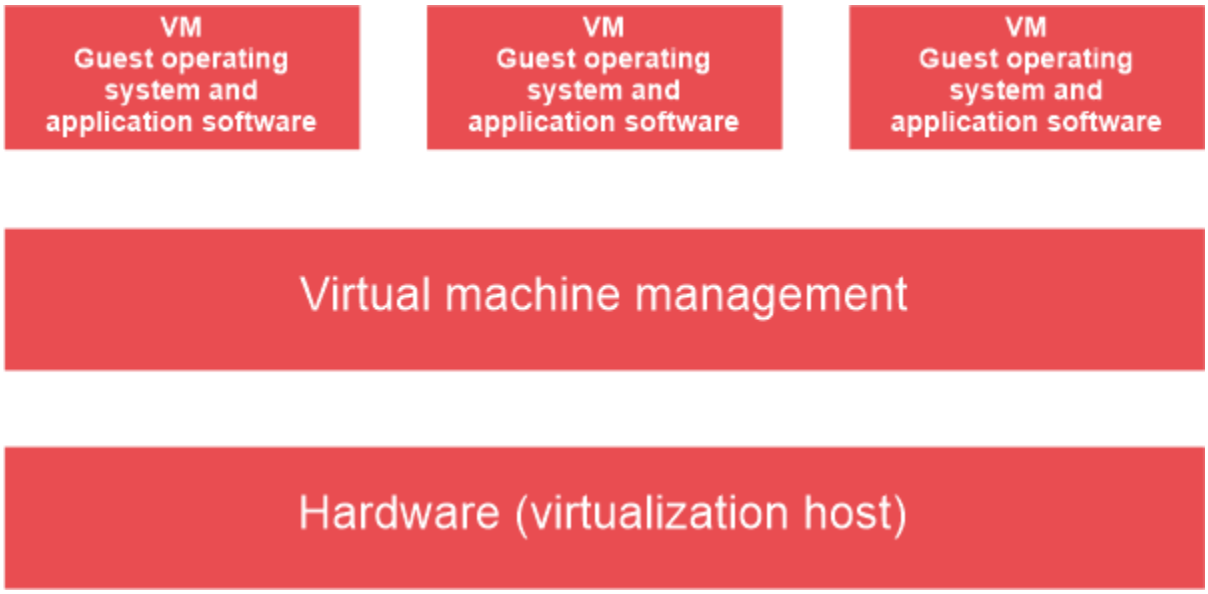
Key Differences Between Full Virtualization and paravirtualization

S. N.	Full Virtualization	Paravirtualization
1.	In Full virtualization, the virtual machine permits the execution of the instructions with running of unmodified OS in an entirely isolated way.	In paravirtualization, the virtual machine does not implement full isolation of the OS but rather provides a different API which is utilized when the OS is subjected to alteration.
2.	Full Virtualization is less secure.	Paravirtualization is more secure than Full Virtualization.
3.	Full Virtualization uses binary translation and a direct approach as a technique for operations.	Paravirtualization uses *hypercalls* at compile time for operations.
4.	Full Virtualization is slower than paravirtualization in operation.	Paravirtualization is faster in operation as compared to full virtualization.
5.	Full Virtualization is more portable and compatible.	Paravirtualization is less portable and compatible.
6.	Examples of full virtualization are Microsoft and Parallels systems.	Examples of paravirtualization are VMware and Xen.

Hardware-Assisted Virtualiz

Operating System Virtualization

- Operating System Virtualization is a technique where the host operating system allows multiple isolated user-space instances, called containers, to run on the same kernel. Unlike hardware virtualization, it **does** not emulate hardware and all containers share the same OS kernel.
- In Operating System (OS) Virtualization, there are no traditional virtual machines (VMs) like in hardware virtualization. Instead, OS virtualization uses containers or isolated user-space instances**.**
- Best for running multiple isolated applications on the same OS
- With the help of OS virtualization nothing is pre-installed or permanently loaded on the local device and no-hard disk is needed.
- Everything runs from the network using a kind of virtual disk. This virtual disk is actually a disk image file stored on a remote server, SAN (Storage Area Network) or NAS (Network Attached Storage).
- The client will be connected by the network to this virtual disk and will boot with the Operating System installed on the virtual disk.



How does OS Virtualization work?

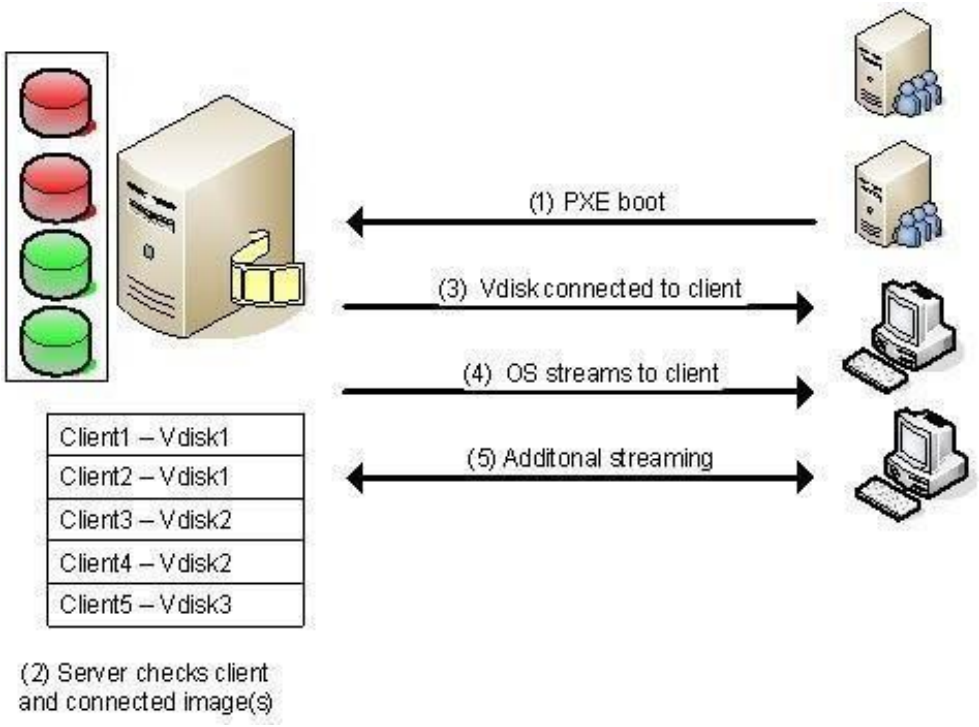
- The first component is the OS Virtualization server. This server is the center point in the OS Virtualization infrastructure. The server manages the streaming of the information on the virtual disks for the client and also determines which client will be connected to which virtual disk (using a database, this information is stored). Also, the server can host the storage for the virtual disk locally or the server is connected to the virtual disks via a SAN (Storage Area Network). In high availability environments there can be more OS Virtualization servers to create no redundancy and load balancing. The server also ensures that the client will be unique within the infrastructure.

- Secondly, there is a client which will contact the server to get connected to the virtual disk and asks for components stored on the virtual disk for running the operating system.
- The available supporting components are database for storing the configuration and settings for the server, a streaming service for the virtual disk content, a (optional) TFTP service and a (also optional) Preboot Execution Environment (PXE) boot service for connecting the client to the OS Virtualization servers.
- As the virtual disk contains an image of a physical disk from the system that will reflect to the configuration and the settings of those systems which will be using the virtual disk. When the virtual disk is created then that disk needs to be assigned to the client that will be using this disk for starting. The connection between the client and the disk is made through the administrative tool and saved within the database.

When a client has an assigned disk, the machine can be started with the virtual disk using the following process as displayed in the given below Figure:

1. **Connecting to the OS Virtualization server:** First we start the machine and set up the connection with the OS Virtualization server. Most of the products offer several possible methods to connect with the server. One of the most popular and used methods is using a PXE service, but also a bootstrap is used a lot (because of the disadvantages of the PXE service). Although each method initializes the network interface card (NIC), receiving a (DHCP-based) IP address and a connection to the server.

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 and which virtual disk is assigned to the client. When more than one virtual disk are connected then a boot menu will be displayed on the client side. If only one disk is assigned, that disk will be connected to the client which is mentioned in step number 3.
3. **VDisk connected to the client:** After the desired virtual disk is selected by the client, that virtual disk is connected through the OS Virtualization server. At the back-end, the OS Virtualization server makes sure that the client will be unique (for example computer name and identifier) within the infrastructure.
4. **OS is "streamed" to the client:** As soon the disk is connected the server starts streaming the content of the virtual disk. The software knows which parts are necessary for starting the operating system smoothly, so that these parts are streamed first. The information streamed in the system should be stored somewhere (i.e. cached). Most products offer several ways to cache that information. For examples on the client hard disk or on the disk of the OS Virtualization server.
5. **Additional Streaming:** After that the first part is streamed then the operating system will start to run as expected. Additional virtual disk data will be streamed when required for running or starting a function called by the user (for example starting an application available within the virtual disk).



Advantages of OS Virtualization

1. OS virtualization usually imposes little or no overhead.
2. OS Virtualization is capable of live migration
3. It can also use dynamic load balancing of containers between nodes and a cluster.
4. The file level **copy-on-write** (CoW) mechanism is possible on OS virtualization which makes easier to back up files, more space-efficient and simpler to cache than the block- level copy-on- write schemes.

Virtual Disks in OS Virtualization

- The client will be connected via the network to the virtual disk & will boot the OS installed on virtual disk.
- Two types of virtual disks are there for implementation.
- These are:
    1. **Private Virtual Disk:** is used by one client only like that of a local hard disk. Users can save information on the virtual disk based on the rights assigned. So as the client restart the system, the settings are retained just like working with physical local hard disk.
    2. **Shared/Common Virtual Disk:** It is used by multiple clients at the same time. The changes are saved in a special cache & these caches gets cleaned as the user restarts or shutdowns the system. In other words, when a client is booting up, it will use the default configuration available on the virtual disk.

Server Virtualization

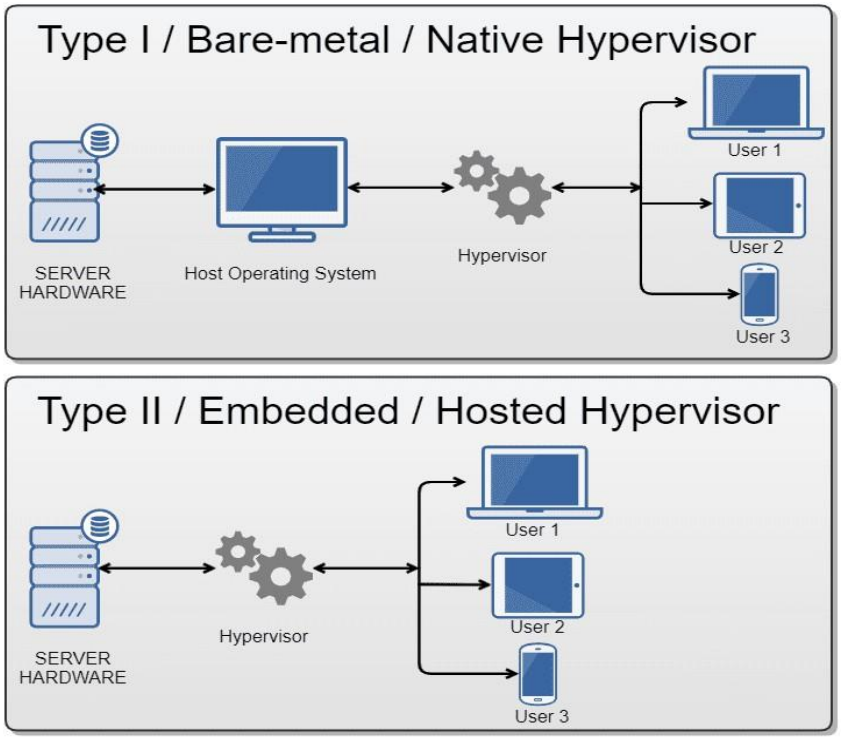
- Server Virtualization is the process of dividing a physical server into several virtual servers, called virtual private servers. Each virtual private server can run independently.
- The concept of Server Virtualization widely used in the IT infrastructure to minimizes the costs by increasing the utilization of existing resources.
- Types of Server Virtualization
    1. Hypervisor

2. Full Virtualization
3. Para Virtualization
4. Hardware-Assisted Virtualization
5. Operating System Virtualization
6. Kernel-Level Virtualization

Hypervisor

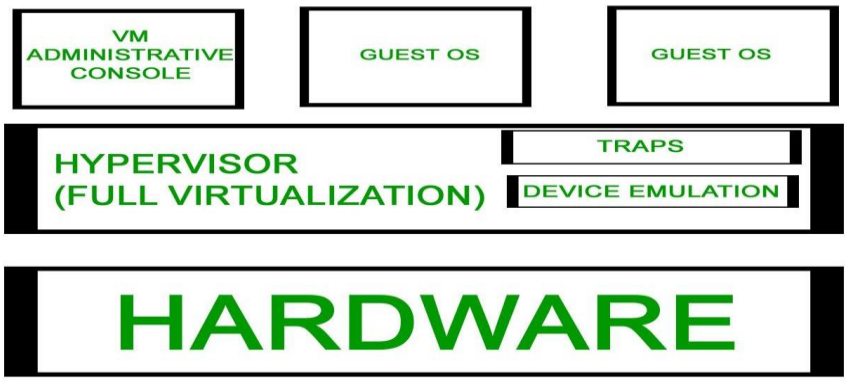
- In the Server Virtualization, Hypervisor plays an important role. It is a layer between the operating system (OS) and hardware.
- There are two types of hypervisors.
    - **Type 1** hypervisor (also known as **bare metal** or **native hypervisors**)
    - **Type 2** hypervisor (also known as **hosted** or **Embedded hypervisors**)

- The hypervisor is mainly used to perform various tasks such as allocate physical hardware resources (CPU, RAM, etc.) to several smaller independent virtual machines, called "guest" on the host machine.



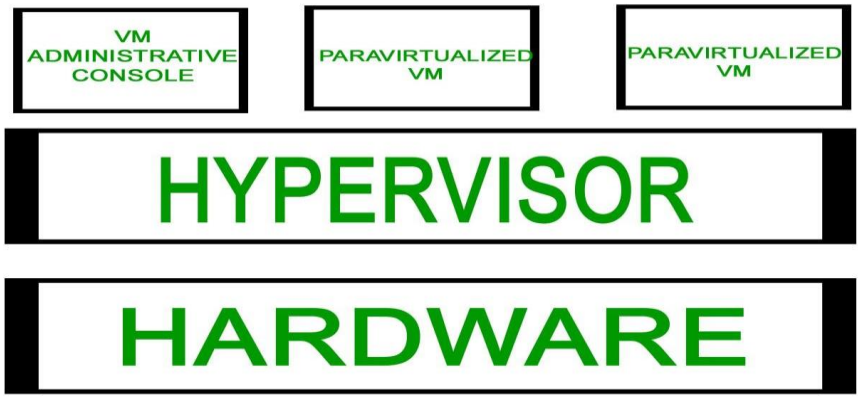
Full Virtualization

- Full Virtualization uses a hypervisor to directly communicate with the CPU and physical server. It provides the best isolation and security mechanism to the virtual machines.
- The biggest disadvantage of using hypervisor in full virtualization is that a hypervisor has its own processing needs, so it can slow down the application and server performance.
- **VMWare ESX server** is the best example of full virtualization.



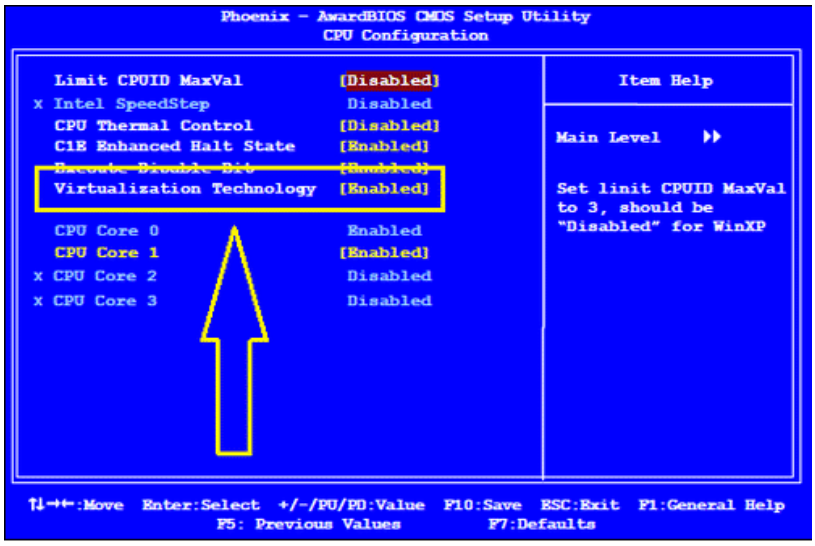
Para Virtualization

- Para Virtualization is quite similar to the Full Virtualization.
- The advantage of using this virtualization is that it is easier to use, Enhanced performance, and does not require emulation overhead.
- Xen primarily and UML use the Para Virtualization.
- The difference between full and pare virtualization is that, in para virtualization hypervisor does not need too much processing power to manage the OS.



Hardware-Assisted Virtualization

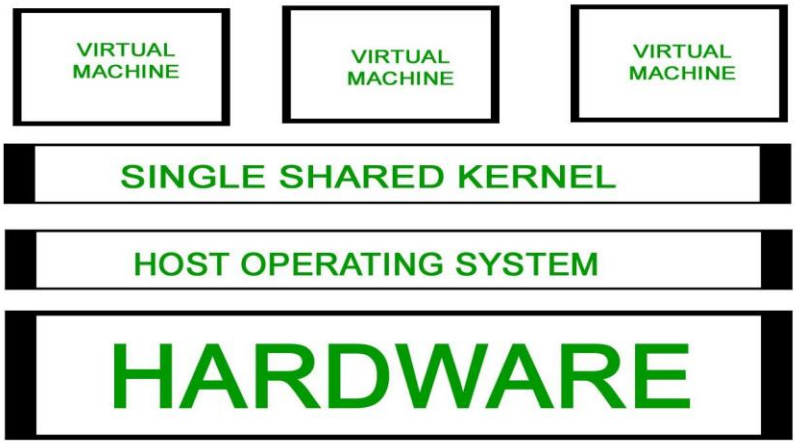
- Hardware Assisted Virtualization was presented by AMD and Intel.
- It is also known as Hardware virtualization, AMD virtualization, and Intel virtualization.
- It is designed to increase the performance of the processor.
- The advantage of using Hardware Assisted Virtualization is that it requires less hypervisor overhead.



Operating System Virtualization

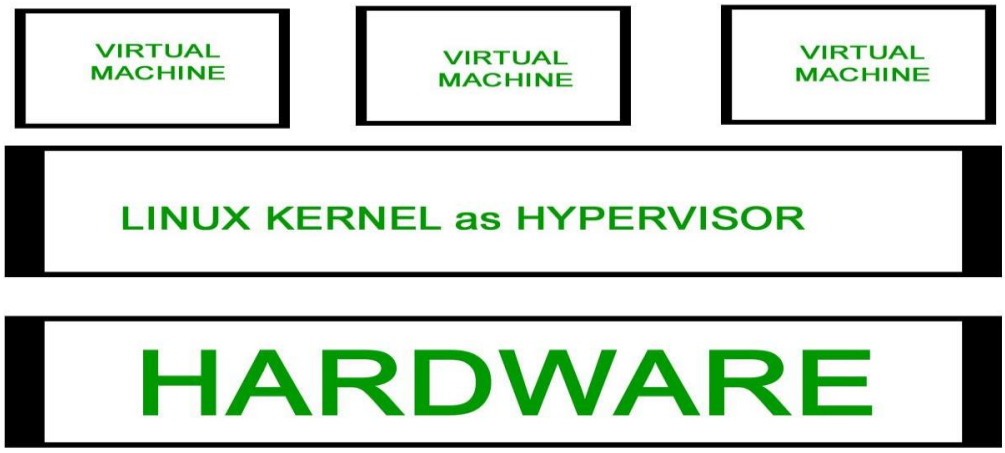
- Operating system virtualization is also called as **system-lever virtualization**.
- It is a server virtualization technology that divides one operating system into multiple isolated user-space called **virtual environments**.

- The biggest advantage of using server visualization is that it reduces the use of physical space, so it will save money.
- Linux OS Virtualization and Windows OS Virtualization are the types of Operating System virtualization.
- FreeVPS, OpenVZ, and Linux Vserver are some examples of System-Level Virtualization.



Kernel-Level Virtualization

- Kernel-level virtualization is one of the most important types of server virtualization.
- It is an open- source virtualization which uses the Linux kernel as a hypervisor.
- The advantage of using kernel virtualization is that it does not require any special administrative software and has very less overhead.
- User Mode Linux (UML) and Kernel- based virtual machine are some examples of kernel virtualization.



Advantages of Server Virtualization

1. Independent Restart - In Server Virtualization, each server can restart independently and does not affect the working of other virtual servers.

2. Low Cost - Server Virtualization can divide a single server into multiple virtual private servers, so it reduces the cost of hardware components.
3. Disaster Recovery - It is one of the best advantages of Server Virtualization. In Server Virtualization, data can easily and quickly move from one server to another and these data can be stored and retrieved from anywhere.

4. Faster deployment of resources - Server virtualization allows us to deploy our resources in a simpler and faster way.
5. Security - It allows uses to store their sensitive data inside the data centers.

Disadvantages of Server Virtualization

1. The biggest disadvantage of server virtualization is that when the server goes offline, all the websites that are hosted by the server will also go down.

2. There is no way to measure the performance of virtualized environments.
3. It requires a huge amount of RAM consumption.
4. It is difficult to set up and maintain.
5. Some core applications and databases are not supported virtualization.
6. It requires extra hardware resources.

Uses of Server Virtualization

- Server Virtualization is used in the testing and development environment.
- It improves the availability of servers.
- It allows organizations to make efficient use of resources.
- It reduces redundancy without purchasing additional hardware components.

Storage Virtualization

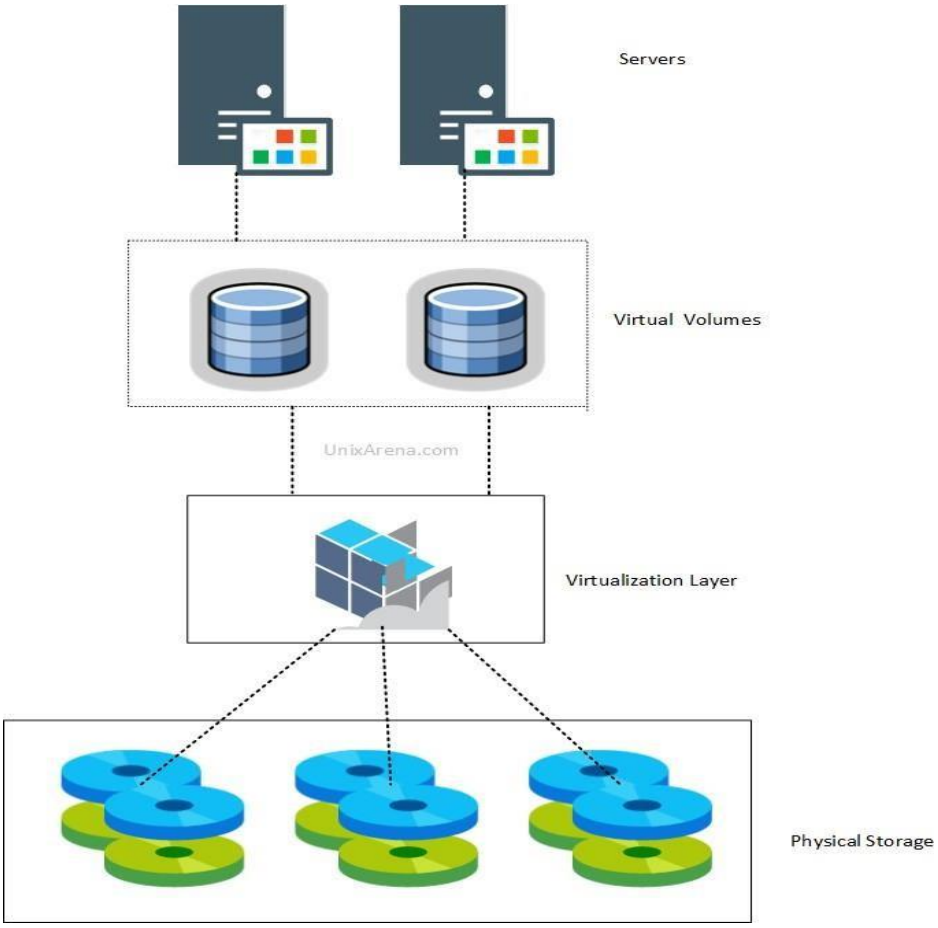
Storage virtualization is a major component for storage servers, in the form of functional RAID (Redundant Array of Independent disks) levels and controllers.

Operating systems and applications with device can access the disks directly by themselves for writing. The controllers configure the local storage in RAID groups and present the storage to the operating system depending upon the configuration.

However, the storage is abstracted and the controller is determining how to write the data or retrieve the requested data for the operating system.

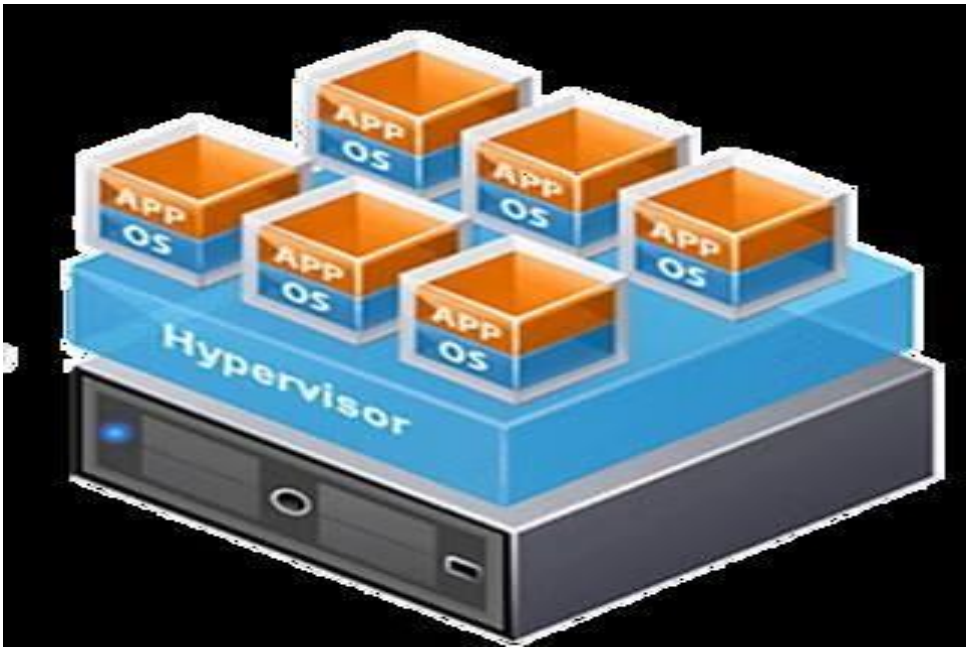
Advantages of Storage Virtualization

1. 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.
2. The storage devices can perform advanced functions like replication, reduplication, and disaster recovery functionality.
3. By doing abstraction of the storage level, IT operations become more flexible in how storage is provided, partitioned, and protected.



Desktop Virtualization

- Desktop virtualization provides a way for users to maintain their individual desktops on a single, central server. The users may be connected to the central server through a LAN, WAN or over the Internet.
- Desktop virtualization has many benefits, including a lower total cost of ownership (TCO), increased security, reduced energy costs, reduced downtime and centralized management.
- Limitations of desktop virtualization include difficulty in maintenance and set up of printer drivers; increased downtime in case of network failures; complexity and costs involved in Virtual Desktop Infrastructure (VDI) deployment and security risks in the event of improper network management



Benefits of Desktop Virtualization

1. Resource Management: Desktop virtualization helps IT departments get the most out of their hardware investments by consolidating most of their computing in a data center. Desktop virtualization then allows organizations to issue lower-cost computers and devices to end users because most of the intensive computing work takes place in the data center. By minimizing how much computing is needed at the endpoint devices for end users, IT departments can save money by buying less costly machines.
2. Remote Work: Desktop virtualization helps IT admins support remote workers by giving IT central control over how desktops are virtually deployed across an organization's devices. Rather than manually setting up a new desktop for each user, desktop virtualization allows IT to simply deploy a ready-to-go virtual desktop to that user's device. Now the user can interact with the operating system and applications on that desktop from any location and the employee experience will be the same as if they were working locally.
3. Security: Desktop virtualization software provides IT admins centralized security control over which users can access which data and which applications. If a user's permissions change because they leave the company, desktop virtualization makes it easy for IT to quickly remove that user's access to their persistent virtual desktop and all its data—instead of having to manually uninstall everything from that user's devices. And because all company data lives inside the data center rather than on each machine, a lost or stolen device does not post the same data risk. If someone steals a laptop

using desktop virtualization, there is no company data on the actual machine and hence less risk of a breach.

Network Virtualization

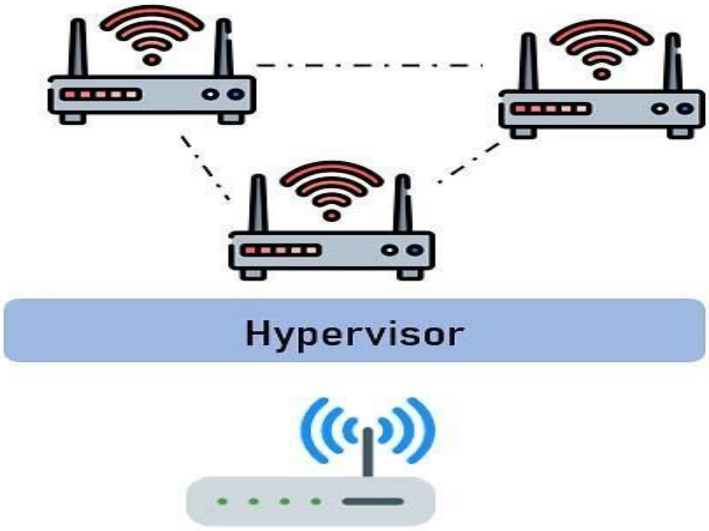
- Network virtualization is a method of combining the available resources in a network to consolidate multiple physical networks, divide a network into segments or create software networks between virtual machines (VMs).
- IT managers that use network virtualization can administrate their environment as a single software-based network. Network virtualization is intended to optimize network speed, reliability, flexibility, scalability and security. It is said to be especially useful in networks that experience sudden, large and unexpected flows in usage.

Types of network virtualization:

- Software-defined networking (SDN) virtualizes hardware that controls

  network traffic routing.

- Network function virtualization (NFV) virtualizes hardware appliances that provide network-specific functions easier to configure and manage, e.g., firewall, etc.



Advantages of Network Virtualization:

1. More productive IT environments (i.e., efficient scaling).
2. Improved security and recovery times.
3. Faster in application delivery.
4. More efficient networks.
5. Reduced overall costs.

Disadvantages of Network Virtualization:

1. Increased upfront costs (investing in virtualization software).
2. Need to license software.
3. There may be a learning curve if IT managers are not experienced.
4. Not every application and server will work in a virtualized environment.
5. Availability can be an issue if an organization can't connect to their virtualized data

Benefits of Virtualization

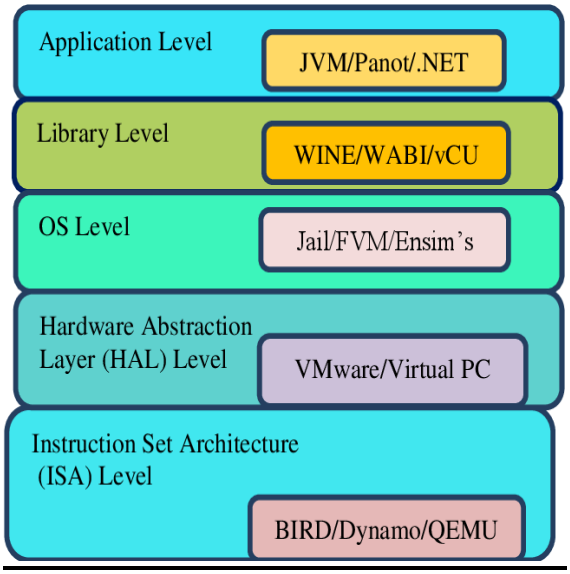
- Virtualization can increase IT agility, flexibility, and scalability while creating significant cost savings. Workloads get deployed faster, performance and availability increase and operations become automated, resulting in IT that's simpler to manage and less costly to own and operate.
- Additional benefits include:
    - Reduce capital and operating costs.
    - Minimize or eliminate downtime.
    - Increase IT productivity, efficiency, agility and responsiveness.
    - Provision applications and resources faster.
    - Enable business continuity and disaster recovery.
    - Simplify data center management.
    - Build a true Software-Defined Data Center

Implementation Levels of Virtualization

- A traditional computer runs with a host operating system specially tailored for its hardware architecture. After virtualization, different user applications managed by their own operating systems (guest OS) can run on the same hardware, independent of the host OS.
- It is not simple to set up virtualization. Our computer runs on an operating system that gets configured on some particular hardware. It is not feasible or easy to run a different operating system using the same hardware.
- To do this, we will need a hypervisor. Now, what is the role of the hypervisor? It is a bridge between the hardware and the virtual operating system, which

allows smooth functioning. The virtualization software creates the abstraction of VMs by interposing a virtualization layer at various levels of a computer system.

Virtualization can be implemented at various operational levels as given below:



- Instruction Set Architecture (ISA) level
- Hardware Abstract Level
- Operating System Level
- Library Support Level
- Application Level

Unit 3: Cloud Virtualization technology

1. **Instruction Set Architecture Level (ISA)**

- Instruction Set Architecture (ISA) is the part of a computer system that defines how software communicates with hardware. It acts as a bridge between the processor (CPU) and the programs that run on it.
- ISA virtualization works by imitating (emulating) an ISA.
- This helps run old programs made for different hardware on a virtual machine.
- With this, programs that needed extra support before can now run on x86 computers and can also be adjusted for x64 systems.
- A basic emulator uses an interpreter, which reads the original code and changes it into a format that the hardware can understand and process.
- The basic emulation method is through code interpretation. An interpreter program interprets the source instructions to target instructions one by one. One source instruction may require tens or hundreds of native target instructions to perform its function. Obviously, this process is relatively slow. For better performance, dynamic binary translation is desired. This approach translates basic blocks of dynamic source instructions to target instructions. Instruction set emulation requires binary translation and optimization. A virtual instruction set architecture (V-ISA) thus requires adding a processor-specific software translation layer to the compiler.

2. **Hardware Abstraction Level (HAL)**

- It lets the virtualization perform at the **level of the hardware**.
- This makes use of a **hypervisor** which is used for functioning.
- At this level, the virtual machine is formed, and this manages the hardware using the process of virtualization. It allows the virtualization of each of the

hardware components, which could be the input-output device, the memory, the processor, etc.

- Multiple users will be able to use the same hardware and also use multiple virtualization instances at the very same time. This is mostly used in the cloud-based infrastructure.
- More recently, the Xen hypervisor has been applied to virtualize x86-based machines to run Linux or other guest OS applications.

3. **Operating System Level**
    - At the level of the operating system, the virtualization model is capable of creating a layer that is abstract between the operating system and the application.
    - This is an isolated container that is on the operating system and the physical server, which makes use of the software and hardware. Each of these then functions in the form of a server.
    - When there are several users, and no one wants to share the hardware, then this is where the virtualization level is used. Every user will get his virtual environment using a virtual hardware resource that is dedicated.

4. **Library Level**
    - The Library-level virtualization allows applications to run in an isolated environment by intercepting system calls and providing a virtualized interface to system libraries
    - The operating system is cumbersome, and this is when the applications make use of the API that is from the libraries at a user level.

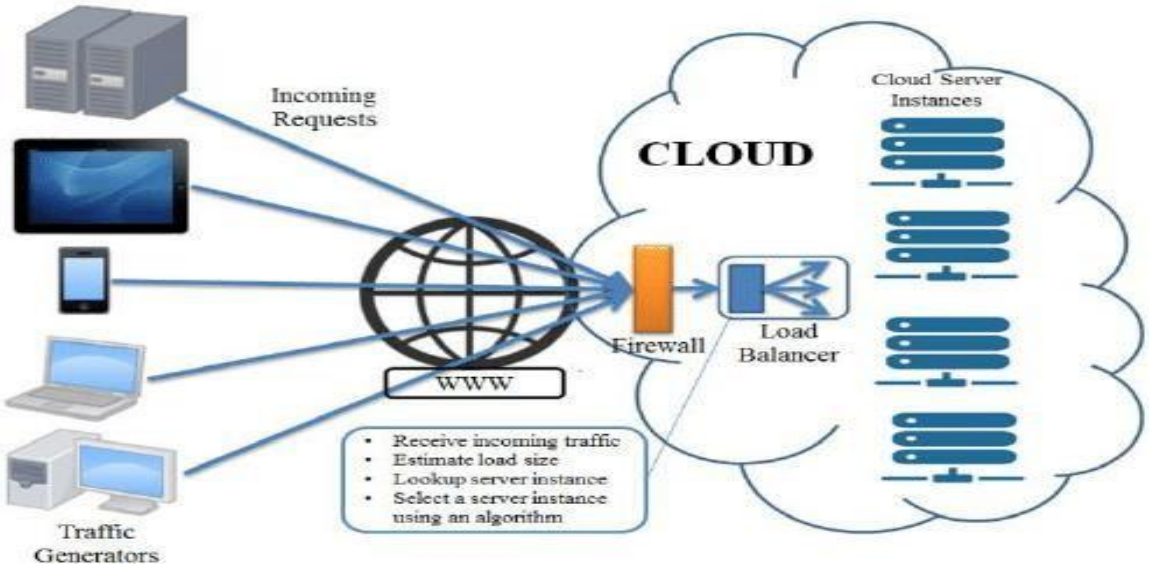
- API hooks make it possible as it controls the link of communication from the application to the system.
- Instead of directly calling the OS, applications interact with a virtualized library that mimics system functions.
- **Wine** Runs Windows applications on Linux by translating Windows API calls.

5. Application Level

- The application-level virtualization is used when there is a desire to virtualize only one application
- One does not need to virtualize the entire environment of the platform.
- Applications run directly from a virtualized environment, so users don't need to install them on individual systems.
- When we run virtual machines that use high-level programming languages (like Java, Python, etc.), the application doesn't directly interact with the underlying operating system or hardware. Instead, the application is virtualized and runs in an isolated environment.
- The virtualized application runs above the virtualization layer. The virtualization layer acts as an intermediary that abstracts the actual hardware and operating system. It allows the application to function as if it’s running on a regular system, but without direct
- Applications built for older operating systems or configurations can be run on modern systems without compatibility issues.
- It is also used When employees need to access applications from multiple devices and locations.

Load Balancing in Cloud Environment

- Load balancing is an essential technique used in cloud computing to optimize resource utilization and ensure that no single resource is overworked with traffic.
- It is a process of distributing workloads across multiple computing resources, such as servers, virtual machines, or containers, to achieve better performance, availability, and scalability.
- Load balancing helps to improve the overall performance and reliability of cloud-based applications by ensuring that resources are used efficiently and that there is no single point of failure (SPOF).
- It also helps to scale applications on demand and provides high availability and fault tolerance to handle spikes in traffic or server failures.



Load Balancing Techniques:

1. **Network Load Balancing:**
    - This technique is used to balance the network traffic across multiple servers or instances.
    - It is implemented at the network layer and ensures that the incoming traffic is distributed evenly across the available servers.
2. **Application Load Balancing:**
    - This technique is used to balance the workload across multiple instances of an application.
    - It is implemented at the application layer and ensures that each instance receives an equal share of the incoming requests.
3. **Database Load Balancing:**
    - This technique is used to balance the workload across multiple database servers.
    - It is implemented at the database layer and ensures that the incoming queries are distributed evenly across the available database servers.

Advantages:

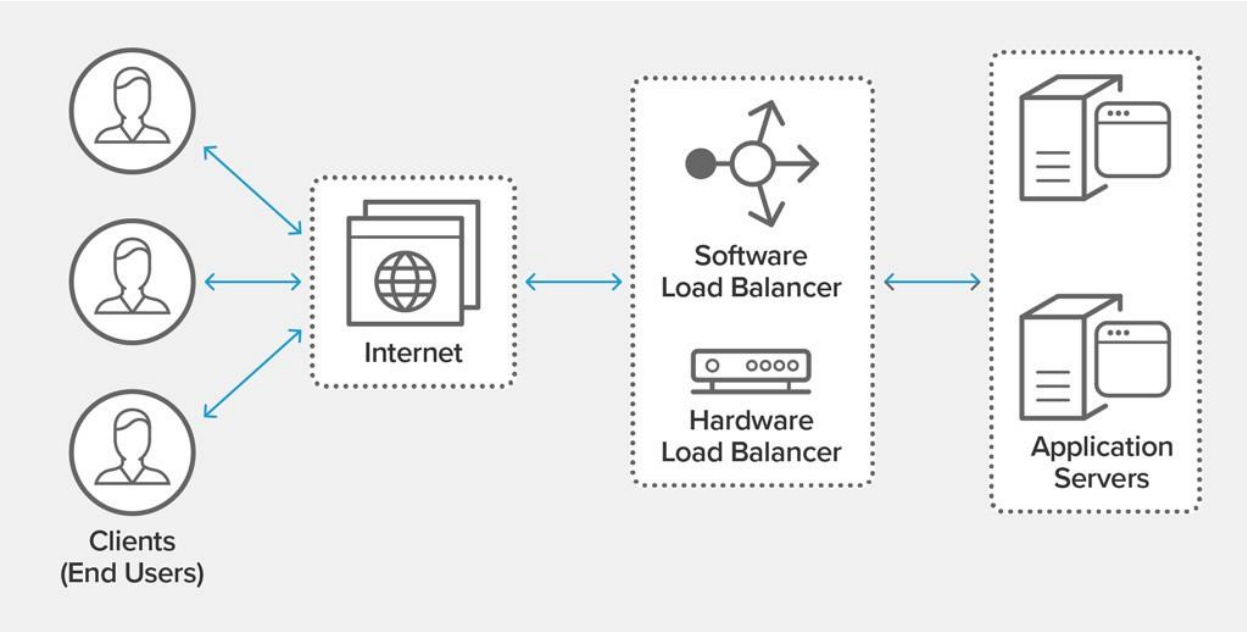
- **Improved Performance:** Load balancing helps to distribute the workload across multiple resources, which reduces the loadon each resource and improves the overall performance of the system.

- **High Availability:** Load balancing ensures that there is no single point of failure in the system, which provides high availability and fault tolerance to handle server failures.
- **Scalability:** Load balancing makes it easier to scale resources up or down as needed, which helps to handle spikes in traffic or changes in demand.
- **Efficient Resource Utilization:** Load balancing ensures that resources are used efficiently, which reduces wastage and helps to optimize costs.

Disadvantages:

- **Complexity:** Implementing load balancing in cloud computing can be complex, especially when dealing with large-scale systems. It requires careful planning and configuration to ensure that it works effectively.
- **Cost:** Implementing load balancing can add to the overall cost of cloud computing, especially when using specialized hardware or software.
- **Single Point of Failure:** While load balancing helps to reduce the risk of a single point of failure, it can also become a single point of failure if not implemented correctly.
- **Security:** Load balancing can introduce security risks if not implemented correctly, such as allowing unauthorized access or exposing sensitive data.

Types of Load balancing solutions



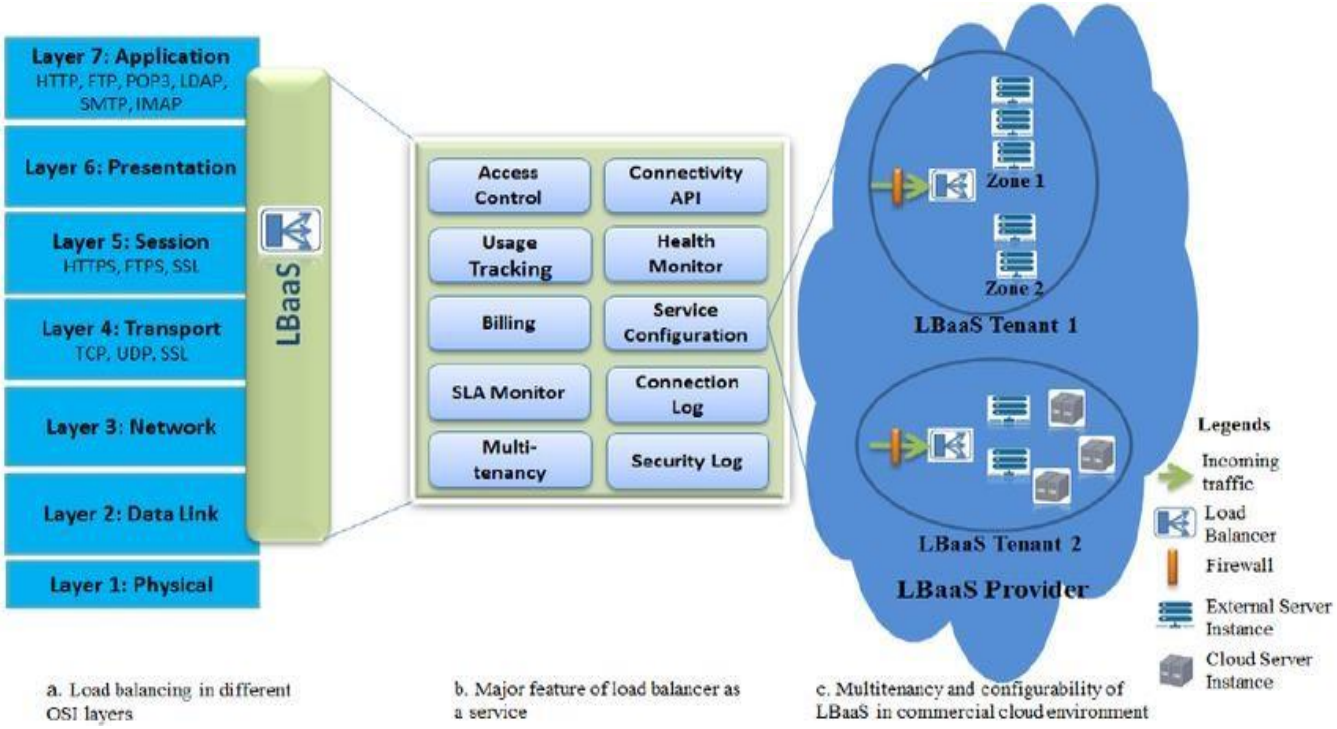
A **software-based load balancer** is a load balancing solution implemented through software running on general-purpose servers or virtual machines. It uses operating system-level services and resources to manage and distribute traffic.

Examples: NGINX, HAProxy, Apache HTTP Server (with mod proxy)

A **hardware-based load balancer** is a dedicated, physical device designed specifically to manage and distribute traffic across multiple servers. These devices are often built to handle high volumes of traffic with specialized hardware optimized for load balancing tasks.

Examples: F5 Networks BIG-IP, Citrix NetScaler.

Load Balancing as a Service (LBaaS)



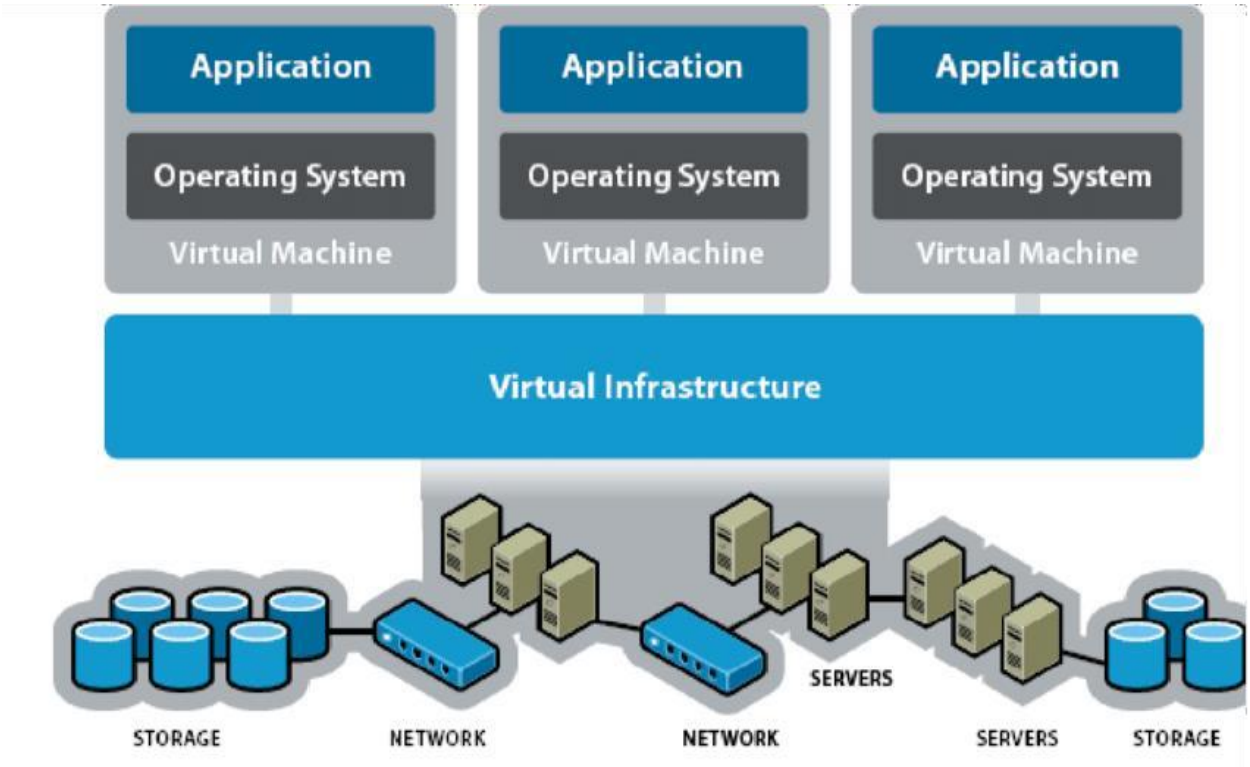
a. Load balancing in different OSI layers

b. Major feature of load balancer as a service

c. Multitenancy and configurability of LBaaS in commercial cloud environment

Infrastructure requirement for virtualization

- Virtual infrastructure is a collection of software defined components that make up an enterprise IT environment.
- It provides the same IT capabilities as physical resources, but with software, so that IT teams can allocate these virtual resources quickly and across multiple systems, based on the varying needs of the enterprise.
- By decoupling physical hardware from an operating system, a virtual infrastructure can help organizations achieve greater IT resource utilization, flexibility, scalability and cost savings.
- These benefits are especially helpful to small businesses that require reliable infrastructure but can't afford to invest in costly physical hardware.



Virtual Infrastructure Components

- **Virtualized compute(Hardware):**
    - This component offers the same capabilities as physical servers, but with the ability to be more efficient.
    - Through virtualization, many operating systems and applications can run on a single physical server, whereas in traditional infrastructure servers were often underutilized.
    - Virtual compute also makes newer technologies like cloud computing and containers possible.
- **Virtualized storage:**
    - This component frees organizations from the constraints and limitations of hardware by combining pools of physical storage capacity into a single, more manageable repository.
    - By connecting storage arrays to multiple servers using storage area networks, organizations can support their storage resources and gain more flexibility in provisioning them to virtual machines.
- **Virtualized networking and security:**
    - This component decouples networking services from the underlying hardware and allows users to access network resources from a centralized management system.

- Key security features ensure a protected environment for virtual machines, including restricted access, virtual machine isolation and user provisioning measures.

- **Management solution:**
  - This component provides a user-friendly console for configuring, managing and provisioning virtualized IT infrastructure, as well automating processes.
  - A management solution allows IT teams to migrate virtual machines from one physical server to another without delays or downtime, while enabling high availability for applications running in virtual machines, disaster recovery and back-up administration.

Virtual Infrastructure Requirement

From design to disaster recovery, there are certain virtual infrastructure requirements organizations must meet to reap long-term value from their investment.

1. **Plan ahead:** When designing a virtual infrastructure, IT teams should consider how business growth, market fluctuations and advancements in technology might impact their hardware requirements and reliance on compute, networking and storage resources.
2. **Look for ways to cut costs:** IT infrastructure costs can become unwieldly if IT teams don't take the time to continuously examine a virtual infrastructure and its deliverables. Cost- cutting initiatives may

range from replacing old servers and renegotiating vendor agreements to automating time-consuming server management tasks.

3. **Prepare for failure:** Despite its failover hardware and high availability, even the most resilient virtual infrastructure can experience downtime. IT teams should prepare for worst- case scenarios by taking advantage of monitoring tools, purchasing extra hardware and relying on clusters to better manage host resources.

Virtual Infrastructure Architecture

- **Host:** A virtualization layer that manages resources and other services for virtual machines. Virtual machines run on these individual hosts, which continuously perform monitoring and management activities in the background. Multiple hosts can be grouped together to work on the same network and storage subsystems, culminating in combined computing and memory resources to form a cluster. Machines can be dynamically added or removed from a cluster.
- **Hypervisor:** A software layer that enables one host computer to simultaneously support multiple virtual operating systems, also known as virtual machines. By sharing the same physical computing resources, such as memory, processing and storage, the hypervisor stretches available resources and improves IT flexibility.
- **Virtual Machine:** These software-defined computers encompass operating systems, software programs and documents. Managed by a virtual infrastructure, each virtual machine has its own operating system called a guest operating system. The key

advantage of virtual machines is that IT teams can provision them faster and more easily than physical machines without the need for hardware procurement. Better yet, IT teams can easily deploy and suspend a virtual machine, and control access privileges, for greater security. These privileges are based on policies set by a system administrator.

- **User Interface:** This front-end element means administrators can view and manage virtual infrastructure components by connecting directly to the server host or through a browser- based interface.

Virtualization Software

- Virtualization software refers to a set of technologies and tools that enable the creation and management of virtual machines (VMs) or virtual environments on a physical computer or server. It allows multiple operating systems (OS) and applications to run simultaneously on a single hardware platform, sharing its resources such as memory, processing power, and storage.
- Virtualization software creates a layer of abstraction between the underlying hardware and the virtual machines, allowing each VM to operate independently as if it were running on its dedicated physical machine. This abstraction enables better resource utilization, scalability, and flexibility in managing and deploying applications and services.
- The virtualization software typically consists of a hypervisor responsible for managing and allocating the hardware resources to the virtual machines. The hypervisor can be either a Type 1 hypervisor (bare-metal), which directly runs on the host hardware, or a Type 2 hypervisor (hosted) within a traditional operating system.

Assignments

1. Explain the different types of virtualization briefly.
2. Explain virtualization software