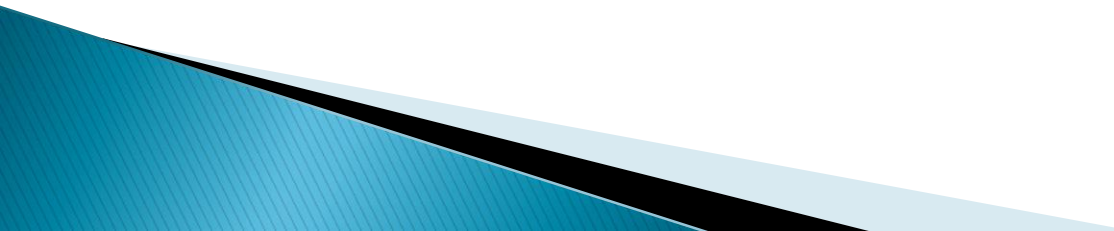


Unit II-Cloud Enabling technology and Virtualization

Cloud-Enabling Technology: Broadband Networks and Internet Architecture, Data Center Technology, Virtualization Technology, Web Technology, Multitenant Technology, Service Technology.

Implementation Levels of Virtualization, Virtualization Structures/Tools and Mechanisms, Types of Hypervisors, Virtualization of CPU, Memory, and I/O Devices, Virtual Clusters and Resource Management, Virtualization for Data-Center Automation.

Agenda

- Broadband Networks and Internet Architecture,
 - Data Center Technology,
 - Virtualization Technology,
 - Virtualization Structures/Tools and Mechanisms,
 - Types of Hypervisors,
 - Virtualization of CPU, Memory, and I/O Devices,
 - Virtual Clusters and Resource Management,
 - Virtualization for Data-Center Automation.
- 

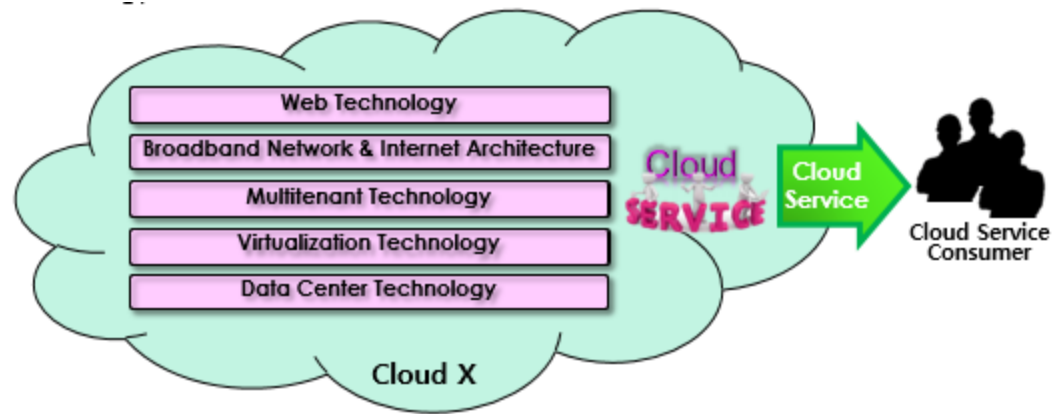
Cloud Enabling Technology

❑ Integrated technology

- Not something entirely new – combined of & integrated from a number of existing technologies
- Integrating a number of existing core technologies into a single service – already matured and some of them more evolved on the way

❑ Existing technologies enabled cloud computing include:

- Broadband networks & internet architecture
- Data center technology
- Virtualization technology
- Web technology
- Multitenant technology
- Service technology



Broadband Networks & Internet Architecture

❑ Cloud service

- Requires remotely accessible service by definition – network connections are inevitable
- Implies inherent dependency on internet technology
- Enables remote provisioning of IT resources via ubiquitous network access (VPN or public network)
- Advances in accordance with the advancements of internet technology and QoS

Broadband Networks & Internet Architecture

❑ Internet Service Providers (ISPs)

- An organization providing national-wide or world-wide internet access service
- Governed by Internet Corporations for Assigned Names and Numbers (ICANN)
- No comprehensive governing by ICANN – ISPs freely deploys, operates and manages their own networks based on basically decentralized provisioning and management models
- Fundamental governmental and regulatory laws applied within national borders
- Internet topology – a dynamic and complex aggregate of ISPs highly interconnected via its core protocols
- Worldwide connectivity via a hierarchical topology composed of Tier 1 (large-scale international ISPs), Tier 2 (large regional ISPs) and Tier 3 (local ISPs)
 - Two fundamental components of internetworking architecture: connectionless packet switching vs. router-based interconnectivity

Broadband Networks & Internet Architecture

- ❑ **Connectionless packet switching (datagram network)**
 - End-to-end (sender-receiver pair) data message divided into packets of limited size
 - Each packet processed through network switches and routers, queued and forwarded from one intermediary node to the next
 - Necessary transfer information carried by each packet in accordance with corresponding protocols such as Internet Protocol (**IP**) address or Media Access Control (**MAC**) address

Broadband Networks & Internet Architecture

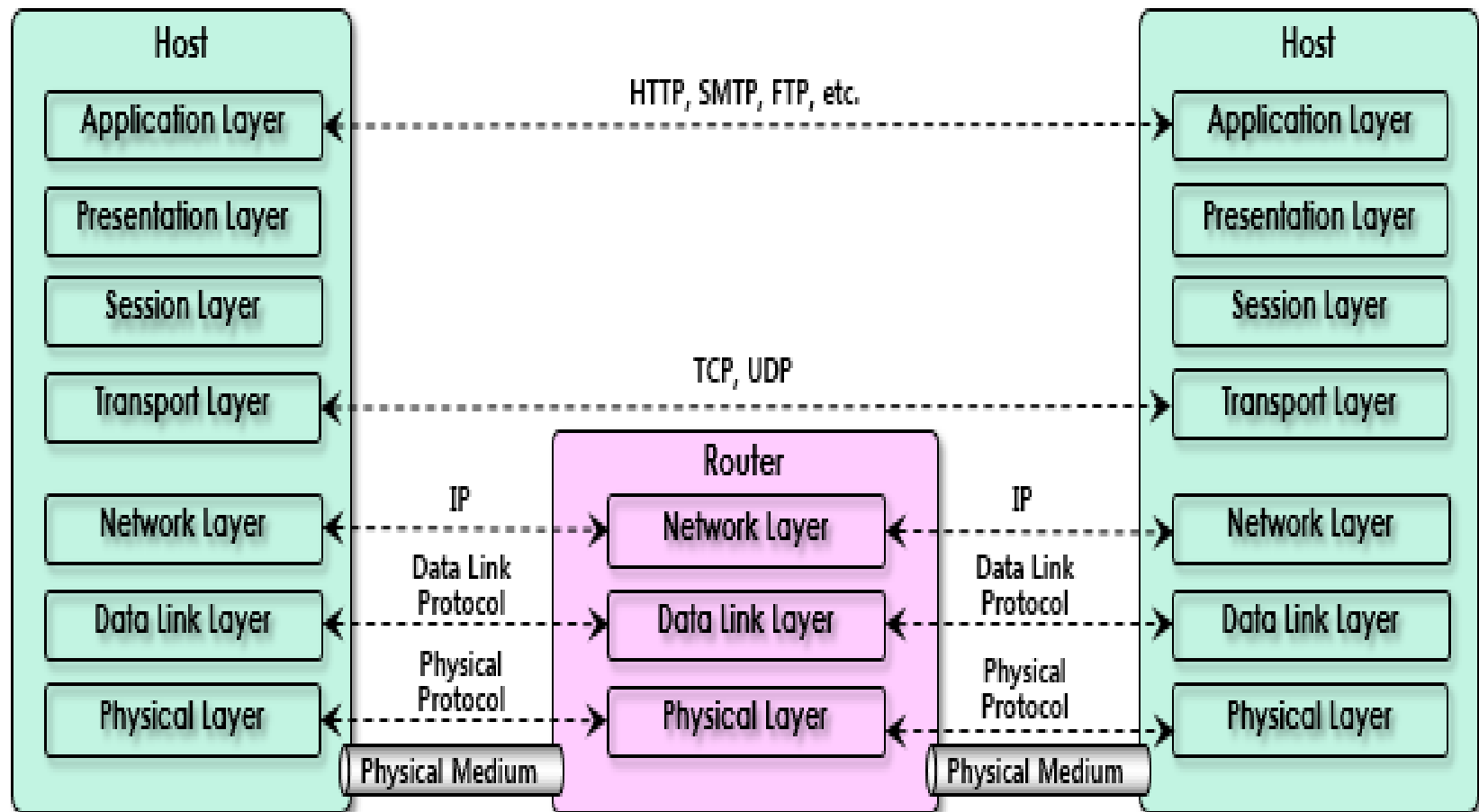
❑ Router-based interconnectivity

- A router – a device connected to multiple networks through which it forwards packets
- Each packet transferred (stored & forwarded at each router) to destination individually via possibly different routes from each other \Rightarrow routing information (IP addresses of the source & the destination, sequential number, etc.) included in each packet
- Packets reassembled into a message on the destination node (at the network layer)
- Each router responsible for finding the most efficient hop for packet delivery at runtime
- Possibly multiple ISP networks between a cloud customer and its cloud provider
- 7 abstraction layer model defined in **OSI** (Open Systems Interconnection) project by **ISO/IEC 7498-1**
 - physical layer (1), data link layer (2), network layer (3), transport layer (4), session layer (5), presentation layer (6), application layer (7)

Broadband Networks & Internet Architecture

Layer	Protocol Data Unit (PDU)	Function
7. Application	Data	High-level APIs, including resource sharing, remote file access – HTTP, FTP etc.
6. Presentation		Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption
5. Session		Managing communication sessions, i.e. continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes
4. Transport	Segment (TCP) / Datagram (UDP)	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing
3. Network	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control
2. Data Link	Frame	Reliable transmission of data frames between two nodes connected by a physical layer
1. Physical	Bit	Transmission and reception of raw bit streams over a physical medium

Broadband Networks & Internet Architecture



Broadband Networks & Internet Architecture

❑ OSI 7 layer model

■ Physical layer (Layer 1)

- Defines for the electrical and physical specifications of the data connection
- Defines the relationship between a device and a physical transmission medium (e.g., a copper or fiber optical cable, radio frequency) including the layout of pins, voltages, line impedance, cable specifications, signal timing and similar characteristics for connected devices and frequency (5 GHz or 2.4 GHz etc.) for wireless devices
- Responsible for transmission and reception of unstructured raw data in a physical medium
- Defines the network topology as bus, mesh, or ring being some of the most common
- Includes **Parallel SCSI**, **Ethernet** & other local-area networks such as **token ring**, **FDDI**, **ITU-T G.hn**, and **IEEE 802.11** (Wi-Fi)
- Defines personal area networks such as **Bluetooth** and **IEEE 802.15.4** as well
- Defines low-level networking equipment, such as network adapters, repeaters, network hubs, modems, and fiber media converters
- Protocol independent - never concerned with protocols or other such higher-layer items

Broadband Networks & Internet Architecture

❑ OSI 7 layer model

■ Data link layer (layer 2)

- Provides node-to-node data transfer – a link between two directly connected nodes
- Detects and possibly corrects errors that may occur in the physical layer
- Defines the protocol to establish and terminate a connection between two physically connected devices as well as the protocol for flow control between them
- High-speed local area networking over existing wires (power lines, phone lines and coaxial cables) defined by The **ITU-T G.hn** standard in this data link layer, providing both error correction and flow control by means of a selective-repeat sliding-window protocol

Broadband Networks & Internet Architecture

❑ OSI 7 layer model

■ Data link layer (layer 2)

- Provides node-to-node data transfer – a link between two directly connected nodes
- Detects and possibly corrects errors that may occur in the physical layer
- Defines the protocol to establish and terminate a connection between two physically connected devices as well as the protocol for flow control between them
- High-speed local area networking over existing wires (power lines, phone lines and coaxial cables) defined by The **ITU-T G.hn** standard in this data link layer, providing both error correction and flow control by means of a selective-repeat sliding-window protocol
- Divided into two sublayers by IEEE 802:
 - **Media Access Control (MAC)** layer - responsible for controlling how devices in a network gain access to medium and permission to transmit it
 - **Logical Link Control (LLC)** layer - responsible for identifying Network layer protocols and then encapsulating them and controls error checking and frame synchronization
- Includes the MAC and LLC layers of IEEE 802 networks such as **802.3 Ethernet**, **802.11 Wi-Fi**, and **802.15.4 ZigBee**
- Defines the Point-to-Point Protocol (**PPP**) that can operate over several different physical layers, such as synchronous and asynchronous serial lines

Broadband Networks & Internet Architecture

❑ OSI 7 layer model

■ Network layer (Layer 3)

- Provides the functional and procedural means of transferring variable length data sequences (called **datagrams**) from one node to another connected to the same "network"
- A network – a communication medium to which many nodes with **addresses** (e.g., IP) can be connected, allowing each member node to transfer a message to any other member nodes via **address resolution** or **routing** through intermediate nodes
- Large messages divided into several fragments before sending and reassembled again upon receiving at the network layer
- May report delivery errors – message delivery at the network layer is not necessarily guaranteed to be reliable; a network layer protocol may provide reliable message delivery, but it need not do so.
- Defines a number of layer-management protocols (a function defined in the *management annex*, ISO 7498/4) including routing protocols, multicast group management, network-layer information and error, and network-layer address assignment – determined by the payload that makes these belong to the network layer, not the protocol that carries them

Broadband Networks & Internet Architecture

❑ OSI 7 layer model

■ Transport layer (Layer 4)

- Provides the functional and procedural means of transferring variable-length data sequences from a source to a destination host via one or more networks, while maintaining the quality of service functions - Transmission Control Protocol (TCP) usually built on top of the Internet Protocol (IP) is an example of a transport-layer protocol in the standard Internet stack
- Controls the reliability of a given link through flow control, segmentation/desegmentation, and error control
- Some protocols are state- and connection-oriented implying that the transport layer can keep track of the segments and re-transmit those that fail.
- Also provides the acknowledgement of the successful data transmission and sends the next data if no errors occurred
- Creates packets out of the message received from the application layer. Packetizing is a process of dividing the long message into smaller messages.
- Five classes of connection-mode transport protocols defined by OSI, ranging from class 0 (which is also known as TP0 and provides the fewest features) to class 4 (TP4, designed for less reliable networks, similar to the Internet)
 - Class 0: contains no error recovery and designed for use on network layers that provide error-free connections
 - Class 4: closest to TCP, although TCP contains functions, such as the graceful close, which OSI assigns to the session layer
 - All OSI TP connection-mode protocol classes provide expedited data and preservation of record boundaries.
- Similar to a post office which deals with the dispatch and classification of mail and parcels sent

Broadband Networks & Internet Architecture

❑ OSI 7 layer model

- Packets are then encapsulated into higher level protocols, such as cryptographic presentation services that can be read by the addressee only.
- Non-IP tunneling protocols operating at the transport layer: IBM's **SNA**, Novell's **IPX** over an IP network, or end-to-end encryption with **IPsec**
- While Generic Routing Encapsulation (GRE) might seem to be a network-layer protocol, if the encapsulation of the payload takes place only at endpoint, GRE becomes closer to a transport protocol that uses IP headers but contains complete frames or packets to deliver to an endpoint.
- L2TP carries PPP frames inside transport packet.
- Although not developed under the OSI Reference Model and not strictly conforming to the OSI definition of the transport layer, the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) of the Internet Protocol Suite are commonly categorized as layer-4 protocols within OSI.

Broadband Networks & Internet Architecture

Feature Name	TP0	TP1	TP2	TP3	TP4
Connection-oriented Network	Yes	Yes	Yes	Yes	Yes
Connectionless Network	No	No	No	No	Yes
Concatenation and Separation	No	Yes	Yes	Yes	Yes
Segmentation and Reassembly	Yes	Yes	Yes	Yes	Yes
Error Recovery	No	Yes	Yes	Yes	Yes
Reinitiate Connection*	No	Yes	No	Yes	No
Multiplexing / Demultiplexing over Single Virtual Circuit	No	No	Yes	Yes	Yes
Explicit Flow Control	No	No	Yes	Yes	Yes
Retransmission on Timeout	No	No	No	No	Yes
Reliable Transport Service	No	Yes	No	Yes	Yes
* If an excessive number of PDUs are unacknowledged					

Broadband Networks & Internet Architecture

❑ OSI 7 layer model

■ Session layer (Layer 5)

- Controls the dialogues (connections) between computers - establishing, managing and terminating the connections between the local and remote application
- Provides for full-duplex, half-duplex, or simplex operation, and establishes checkpointing, adjournment, termination, and restart procedures
- Also provides graceful close of sessions which is a property of the Transmission Control Protocol and session checkpointing and recovery which is not usually used in the Internet Protocol Suite
- Commonly implemented explicitly in application environments that use remote procedure calls

Broadband Networks & Internet Architecture

❑ OSI 7 layer model

■ Presentation layer (Layer 6)

- Establishes context between application-layer entities, in which the application-layer entities may use different syntax and semantics if the presentation service provides a mapping between them
- Encapsulates presentation service data units into session protocol data units that are then passed down the protocol stack If a mapping is available
- Provides independence from data representation (e.g., encryption) by translating between application and network formats
- Transforms data into the form that the application accepts - formatting and encrypting data to be sent across a network (sometimes called the syntax layer)
- The original presentation structure used the Basic Encoding Rules of Abstract Syntax Notation One (ASN.1) with capabilities such as converting an EBCDIC-coded text file to an ASCII-coded file, or serialization of objects and other data structures from and to XML.

Broadband Networks & Internet Architecture

❑ OSI 7 layer model

■ Application layer (Layer 7)

- The OSI layer closest to the end user which means both the OSI application layer and the user interact directly with the software application
- Interacts with software applications (outside the scope of the OSI model) that implement a communicating component
- Includes functions such as identifying communication partners, determining resource availability, and synchronizing communication
- Determines the identity and availability of communication partners for an application with data to transmit when identifying communication partners
- Must decide whether sufficient network resources for the requested communication are available when determining resource availability

Broadband Networks & Internet Architecture

❑ Technical and business considerations

■ Connectivity issues

➤ Traditional deployment model

- Via the corporate network (VPN) which provide uninterrupted Internet connectivity
- Completely controlled by the organizations with their own safeguard based on firewalls and various monitoring tools
- Each organization responsible for deploying, operating and managing their IT resources and Internet connectivity

➤ Cloud deployment model

- Continuous access to centralized servers and applications granted to end-user devices as long as they are connected to the network through the Internet in the cloud
- Centralized IT resources accessible using the same network protocols regardless of whether users reside inside or outside of a corporate network
- Cloud IT resources configured by cloud providers to be accessible for both external and internal users through an Internet connection and for cloud consumers to provide Internet-based services to external users

Broadband Networks & Internet Architecture

On-premise IT Resources	Cloud-based IT Resources
Internal end-user devices access corporate IT services through the corporate network.	Internal end-user devices access corporate IT services through an Internet connection.
Internal users access corporate IT services through the corporate Internet connection while roaming in external networks.	Internal users access corporate IT services while roaming in external networks through the cloud provider's Internet connection.
External users access corporate IT services through the corporate Internet connection.	External users access corporate IT services through the cloud provider's Internet connection.

Broadband Networks & Internet Architecture

- Network bandwidth and latency issues
 - Network QoS: bandwidth, latency, jitter
 - **Bandwidth** – how much data can be transferred within a unit time
 - End-to-end bandwidth determined by the transmission capacity of the shared data links that connect intermediary nodes
 - Attempt to improve end-to-end bandwidth by ISPs with technologies such as broadband network technology & web acceleration technologies – dynamic caching, compression, pre-fetching, etc.
 - Critical for applications requiring substantial amount of data transfer

Broadband Networks & Internet Architecture

- Network bandwidth and latency issues
 - **Latency** – how fast a request can be satisfied (time for a packet to travel from one node to another)
 - The longer a packet travels the larger the latency is – web caching technology can apply
 - The more network traffic is the larger the latency is – more queuing delay at each hop
 - Critical for applications with a business requirement of fast response time

Broadband Networks & Internet Architecture

- Network bandwidth and latency issues
 - **Jitter** – how consistent the given latency is
 - A gap between the smallest latency and the largest latency
 - Response time less than a millisecond in general, but frequently more than several seconds
 - Internet-wide QoS control required to guarantee small jitter
 - QoS of the underlying network inherited to QoS of the given cloud service

Broadband Networks & Internet Architecture

- Network bandwidth and latency issues
- Cloud carrier and cloud provider selection
 - Involves multiple cloud carriers to achieve the necessary level of connectivity and reliability for the given cloud applications resulting in additional costs
 - QoS determined by multiple ISPs involved & required collaboration of the cloud carriers
 - Wise to adopt more relaxed latency and bandwidth requirements

Data Center Technology

❑ Data center

- Grouping IT resources in close proximity with one another (rather than having them geographically dispersed) for power sharing, higher efficiency in shared IT resource usage and improved accessibility for IT personnel – reason for popularizing data center concept
- Characterized for centralized IT resources such as servers, storages, databases, networking & telecommunication devices and software solutions via applying a number of technologies

Data Center Technology

❑ **Standardization and modularity**

- Built upon standardized commodity hardware and designed with modular architecture
- Aggregating multiple identical building blocks of facility infrastructure and equipment to support scalability, growth and speedy hardware replacements
- Reduces investment and operational costs as they enable economies of scale for the procurement, acquisition, deployment, operation and maintenance processes
- IT resource consolidation favored by common virtualization strategies and the constantly improving capacity and performance of physical devices

Data Center Technology

❑ **Virtualization**

- Virtualization: an abstraction layer with mapping or redirection capability
- Physical IT resources: the facility infrastructure that houses computing/networking systems and equipment, together with hardware systems and their operating systems
- Virtual IT resources: comprised of operational and management tools that are often based on virtualization platforms that abstract the physical computing and networking IT resources as virtualized components that are easier to allocate, operate, release, monitor and control (more details later)

❑ **Automation**

- Reduces operational costs and the error rate in data center via automated management without human supervision – provisioning, configuration, patching and monitoring
- Enables self-configuration and self-recovery – basis of automatic computing technology

Data Center Technology

❑ Remote operation and management

- Most operational and administrative tasks of IT resources in data center can be commanded through the network's remote (within data center boundary in general) consoles and management systems.
- Most operational and administrative tasks carried out from the control room in data center except for those requiring physical operations such as hardware jobs or cabling
- Remote operation from outside of data center boundary strictly prohibited in general.

Data Center Technology

❑ High availability

- All resources in data center are subject to fail anytime based on current hardware and software technologies.
- Most resource failures affect service continuity and underlying business as well.
- In general, data center provides fail-safe technologies mainly based on redundancy in every possible layer – fault-tolerant or fault-resilient technologies on top of redundant resources: power supply, cabling, networking, servers, storages and software licenses.
- Fault-avoidance technologies: load balancing, scaling-up/down, etc.

Data Center Technology

❑ Security-aware design, operation and management

- The level of security determines the credibility of the given data center.
- Security issue is the main concern that prohibits many organizations from migrating their IT resources from on-premise to cloud-based.
- Security threats that make organizations hesitate to outsource IT environment are two-fold: possible malicious attack from outside and anxiety about keeping data outside of organization's physical boundary (not only business-wise but also legality-wise).
- Various levels of protection and security mechanisms: network isolation, firewalls and monitoring tools – big data analysis recently

Data Center Technology

❑ Facilities

- Typically custom-designed computing resources, storages and network equipment for the given purpose
- Several functional layout areas based on power supplies, cabling, environmental control stations that regulate heating, ventilation, air conditioning, fire protection, (physical) security & access control system, monitoring system, etc.

Data Center Technology

❑ Computing hardware

- Mainly composed of standardized commodity servers with a number of computing hardware technologies such as:
 - Rack technology – standardized rack with interconnects for power, network, and internal cooling
 - CPU architecture – support for various CPU types: x86-32bits, x86-64bits, RISC, CISC, etc.
 - Multi-core CPU architecture – hundreds of physical & logical processing core in single unit of standardized racks
 - Redundancy & hot-swap technology – hard disks, power supplies, network interfaces, storage controller cards, etc.

Data Center Technology

❑ Computing hardware

- Blade server technologies with rack-embedded physical interconnections (blade enclosures), fabrics (switches), power supply units, cooling fans, etc.
- Maximizes and enhances inter-component networking and management while optimizing physical space & power via individual server hot-swapping, scaling, replacement and maintenance
- Benefits the deployment of fault-resilient (tolerant) systems based on cluster technology
- Several industry-standard and proprietary operational and management software tools that configure, monitor, and control hardware IT resources from remote & centralized consoles – self-provisioning
- Hundreds or even thousands of physical or virtual servers (IT resources) operated by a single operator

Data Center Technology

❑ Storage hardware

- Needs to deal with tons of data created every day – easily reaching PBs of total scale in general
- One of the most difficult task to deal with in data center and many different levels of technologies for fast access, data availability, massive data accommodation, etc.:
 - RAID (Redundant Array of Independent/Inexpensive Disks) – integrating hundreds of individual HDD to provide fast, reliable, massive storage space
 - IO caching – at different layers: storage controllers, each physical/virtual servers, separate caching servers
 - Hot-swapping – replacing faulty HDD without requiring prior power down (a part of RAID technology)
 - Storage virtualization – abstracted storage layer creating virtual storage device free from the physical property of member storage devices
 - Data replication – memory snapshot, volume cloning, mirroring, DR, CDP, etc.
 - Distributed storage – file, block, object-level distributed storage: HDFS, Ceph, etc.

Data Center Technology

- Storage Topology
 - DAS (Direct Attached Storage): storages directly attached to a host system via block-level channel protocol such as SCSI/FC
 - NAS (Network Attached Storage): storages attached to a number of host systems via file-level network protocols such as NFS/CIFS/SMB – while providing file-level data sharing among multiple hosts
 - SAN (Storage Area Network): storages attached to multiple hosts via block-level network protocols such as Fibre Channel, Infiniband, iSCSI, etc.
- Data backup issues in data center

Data Center Technology

❑ Network hardware

- One of the most important IT capabilities for data center to support remote IT access – broken down into five network subsystems in general
 - Carrier & external network interconnection ⇒ internetworking infrastructure comprised of backbone routers that provide routing between external WAN connections and LANs in the given data center including firewalls and VPN gateways
 - Web-tier load balancing and acceleration ⇒ for even distribution of web traffics and acceleration of web protocols comprised of XML pre-processors, encryption/decryption appliances (web acceleration), layer 7 switching devices (content-aware load balancing), etc.
 - LAN fabric ⇒ intranetworking infrastructure comprised of multiple layer 4 or lower switching devices up to ~10G bandwidth providing several virtualization functions such as LAN segregation into VLANs, link aggregation, control routing between networks, load balancing, failover (redundant connectivity), etc.
 - SAN fabric ⇒ data networking infrastructure composed of multiple SAN switching devices based on data networking protocols such as Fibre Channel (FC), Fibre Channel over Ethernet (FCoE), Infiniband (IB), Internet Small Computer Systems Interface (iSCSI)
 - NAS gateway ⇒ shared file-transfer networking infrastructure composed of a number of NAS-based storage devices based on file-transfer protocols such as NFS and SMB/CIFS (Samba)

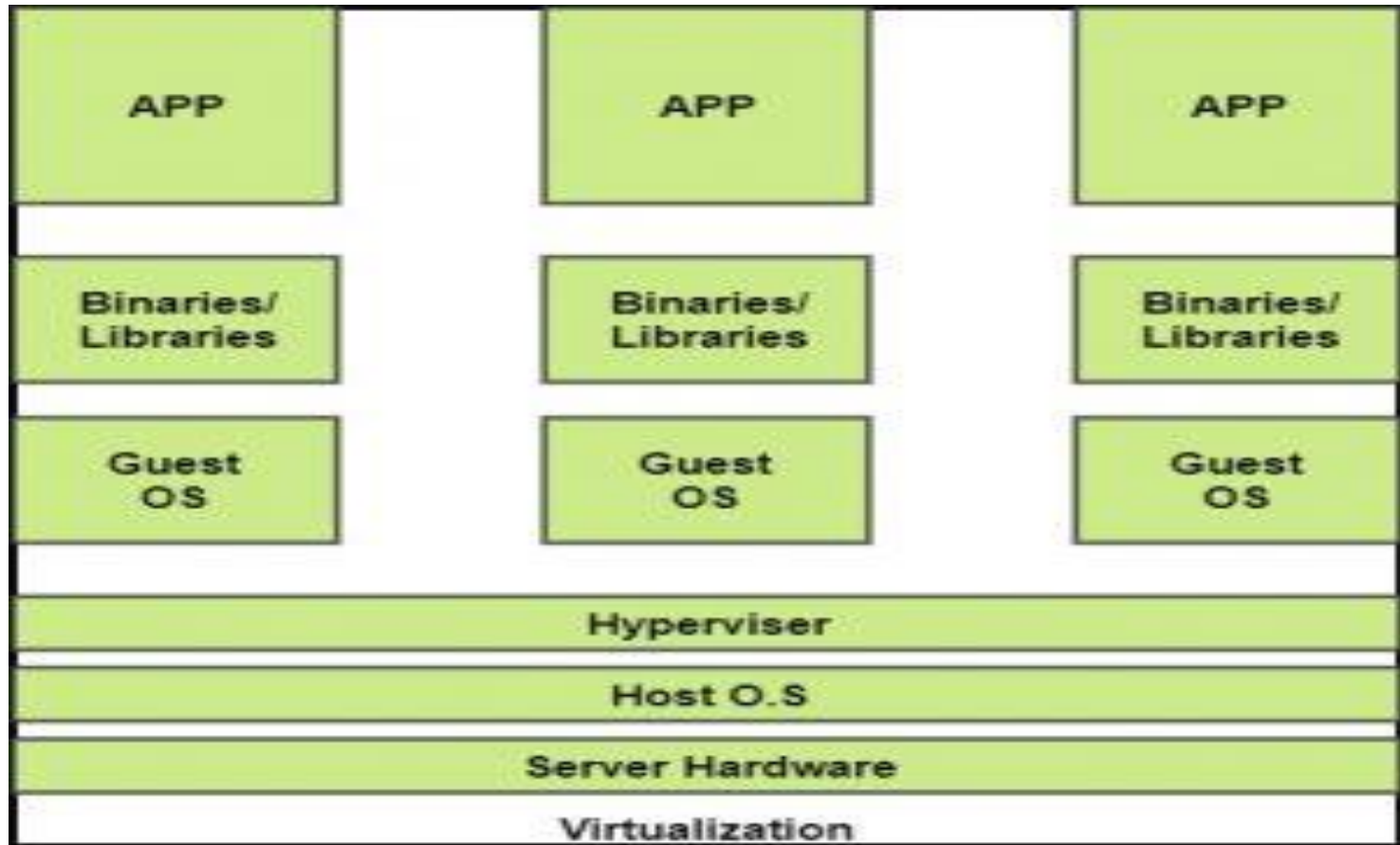
Data Center Technology

- Basically redundant and/or fault-tolerant networking configurations for scalability and high availability
- DWDM (Dense Wavelength Driven Multiplexing) devices for ultra high-speed networking and improved resiliency \Rightarrow in general for the purpose of high-speed real-time data replication between data centers
- **Other consideration**
 - Technological obsolescence, heterogeneity, security, vast quantities of data and their backup, etc.

Virtualization Technology

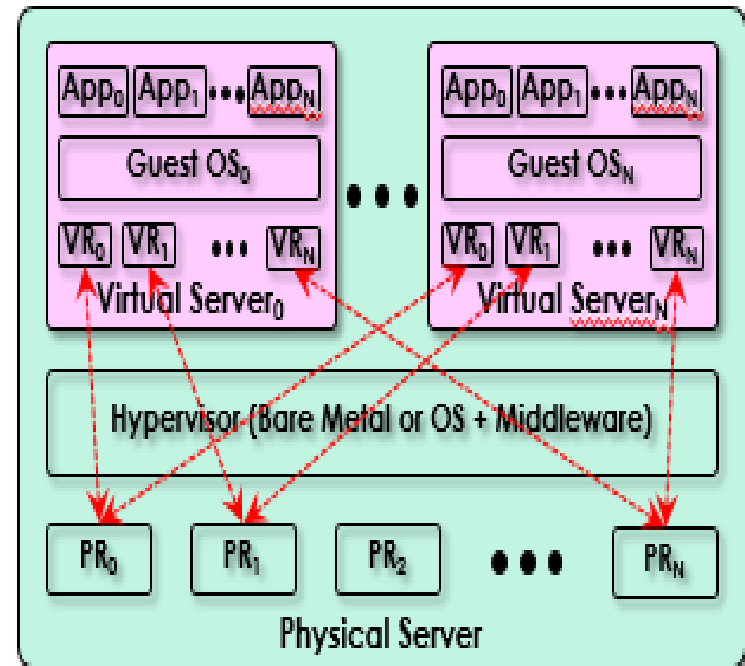
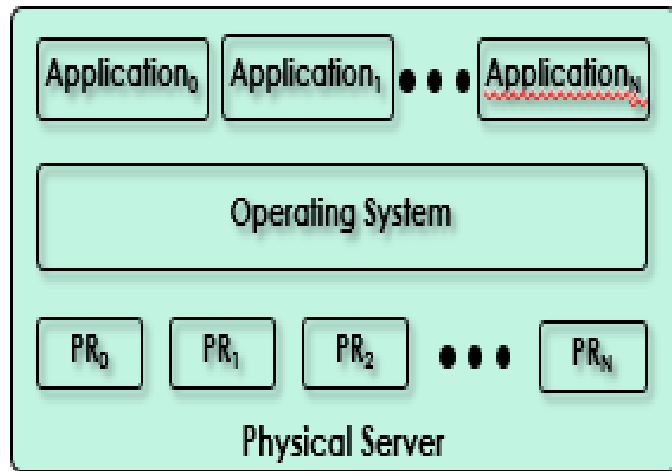
- Virtualization is a technique of how to separate a service from the underlying physical delivery of that service. It is the process of creating a virtual version of something like computer hardware.
- It involves using specialized software to create a virtual or software-created version of a computing resource rather than the actual version of the same resource.
- With the help of Virtualization, multiple operating systems and applications can run on same machine and its same hardware at the same time, increasing the utilization and flexibility of hardware.

Virtualization Technology



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

Virtualization Technology



Benefits of Virtualization

1. More flexible and efficient allocation of resources.
2. Enhance development productivity.
3. It lowers the cost of IT infrastructure.
4. Remote access and rapid scalability.
5. High availability and disaster recovery.
6. Pay peruse of the IT infrastructure on demand.
7. Enables running multiple operating systems.

Types of Virtualization

1. Application Virtualization.
2. Network Virtualization.
3. Desktop Virtualization.
4. Storage Virtualization.
5. Server Virtualization.
6. Data virtualization.

Application Virtualization

1. Application virtualization helps a user to have remote access of an application from a server. The server stores all personal information and other characteristics of the application but can still run on a local workstation through the internet.
2. Example of this would be a user who needs to run two different versions of the same software. Technologies that use application virtualization are hosted applications and packaged applications.

Network Virtualization

- ▶ The ability to run multiple virtual networks with each has a separate control and data plan. It co-exists together on top of one physical network. It can be managed by individual parties that potentially confidential to each other.
- ▶ Network virtualization provides a facility to create and provision virtual networks—logical switches, routers, firewalls, load balancer, Virtual Private Network (VPN), and workload security within days or even in weeks.

Desktop Virtualization

- ▶ Desktop virtualization allows the users' OS to be remotely stored on a server in the data centre. It allows the user to access their desktop virtually, from any location by a different machine.
- ▶ Users who want specific operating systems other than Windows Server will need to have a virtual desktop. Main benefits of desktop virtualization are user mobility, portability, easy management of software installation, updates, and patches.

Storage Virtualization

- ▶ Storage virtualization is an array of servers that are managed by a virtual storage system.
- ▶ The servers aren't aware of exactly where their data is stored, and instead function more like worker bees in a hive. It makes managing storage from multiple sources to be managed and utilized as a single repository.

Server Virtualization

- ▶ This is a kind of virtualization in which masking of server resources takes place. Here, the central-server(physical server) is divided into multiple different virtual servers by changing the identity number, processors.
- ▶ So, each system can operate its own operating systems in isolate manner. Where each sub-server knows the identity of the central server. It causes an increase in the performance and reduces the operating cost by the deployment of main server resources into a sub-server resource.

Data Virtualization

- ▶ This is the kind of virtualization in which the data is collected from various sources and managed that at a single place
- ▶ And without knowing more about the technical information like how data is collected, stored & formatted then arranged that data logically so that its virtual view can be accessed by its interested people and stakeholders, and users through the various cloud services remotely.

Virtualization Technology

❑ **Hardware independence**

- Creating standardized soft (virtual) copies of physical IT resources \Rightarrow eliminating hardware dependency
- Easy automated VM migration or failover between different physical servers

❑ **Server consolidation**

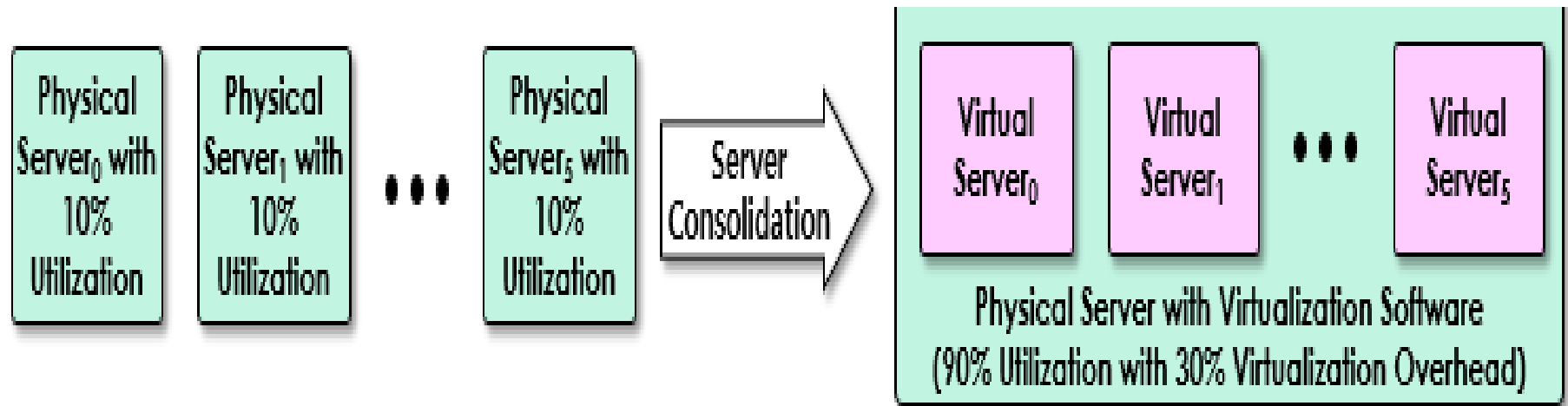
- Creating different multiple virtual servers on a single physical server
- Mainly for Increasing server utilization, load balancing or optimizing IT resource utilization
- Support for common cloud features such as on-demand usage, resource pooling, elasticity, scalability and resiliency

Virtualization Technology

❑ Resource replication

- Virtual servers are implemented as virtual disk images (configuration, memory state, etc.) containing binary file copies of hard disk content and being accessible via simple file operations such as copy and move host OS.
- Easy to be replicated, migrated, backed up and manipulated enabling:
 - Easy creation of standardized VM images with guest OS and pre-packaged application software in virtual disk images for instantaneous deployment
 - Increased agility in the migration and deployment of a virtual machine's new instance by being able to rapidly scale out and up
 - Ability to roll back for instantaneous creation of VM snapshot by saving the state of the virtual server's memory and hard disk image to a host-based file
 - Easy implementation of business continuity with efficient backup and restoration

Virtualization Technology

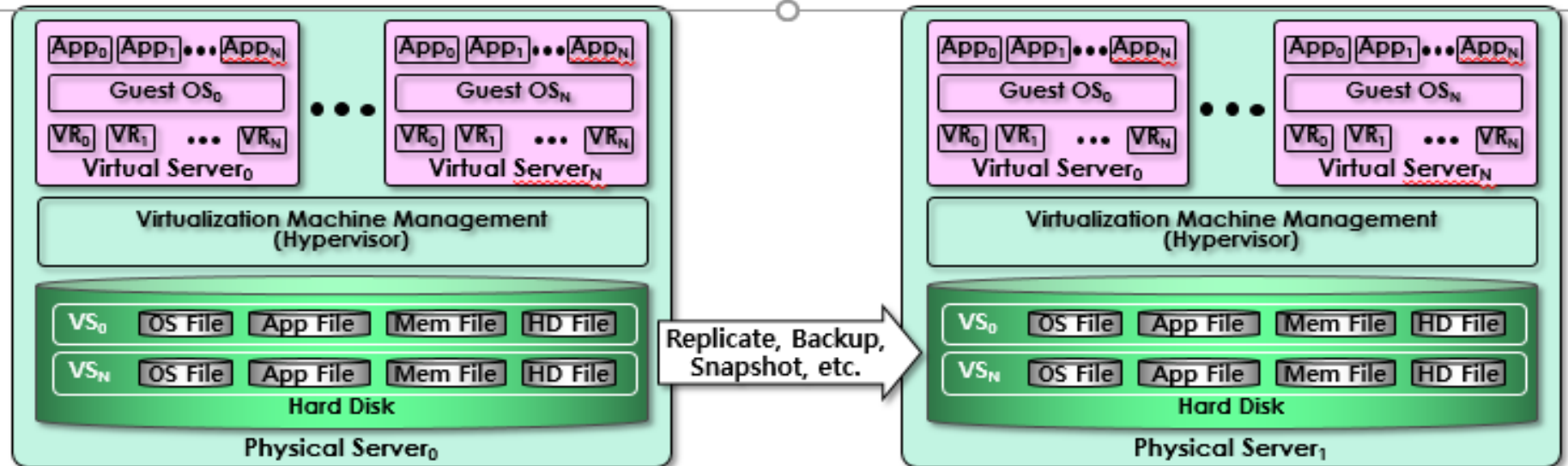


Virtualization Technology

❑ Operating system-based virtualization

- Install virtualization software in a pre-existing operating system (host vs. guest)
- Act as an application or more precisely as a middleware
- Easy to deal with hardware compatibility issues even with absence of a specific hardware driver
- Host OS services to be utilized: backup/recovery, integration to directory service, security management
 - Performance degradation due to:IT resource (CPU, Memory, etc.) sharing with host and guest OSs
 - Several additional traverse for each system call
- Additional license cost for host OS (Windows license or Linux subscription)

Virtualization Technology



Virtualization Technology

❑ **Virtualization management**

- Easier to administrate virtual servers than physical servers
- Many administration tasks automated by virtualization software
- VIM (Virtualization Infrastructure Management) tools – collectively manage virtual IT resources from a centralized & dedicated management computer (controller)

Virtualization Technology

❑ Other consideration

- Performance overhead
 - Not ideal for complex systems with heavy workload
 - Excessive or unnecessary performance overhead with poorly formulated virtualization plan
 - Para-virtualization APIs – modified to reduce the guest OS's processing overhead \Rightarrow need to customize guest OSs to adapt them at the cost of sacrificing portability
- Special hardware compatibility
 - There are many vendors supplying specialized hardware devices and not all of them are compatible with the given virtualization software.
 - Old and existing software may not support those hardware recently released.
 - Solution: standardization, commoditization and frequent virtualization software update/upgrade
- Portability
 - Poor portability due to automated & programmatic VS management interfaces for their own
 - Demand for international standard such as OVF (Open Virtualization Format) for standardization of virtual disk formats in order to insure a wide range of VS management portability

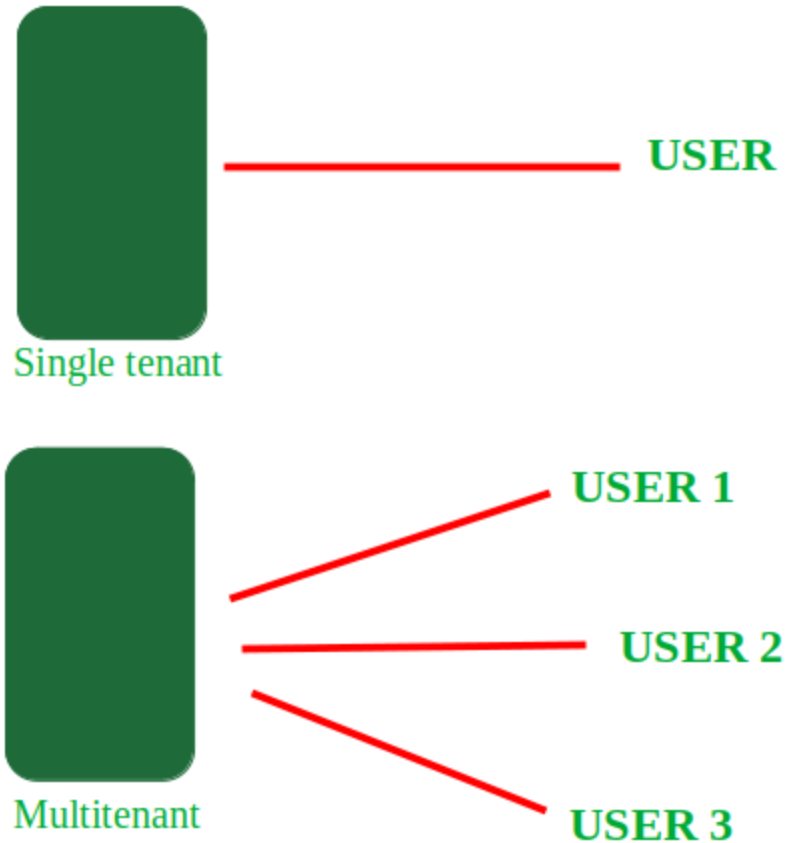
Multitenant Technology

- ❑ Multitenancy is a type of software architecture where a single software instance can serve multiple distinct user groups.
- ❑ It means that multiple customer's of cloud vendor are using same computing resources .
- ❑ As they are sharing same computing resources but the data of each Cloud customer is kept totally separate and secure. It is very important concept of Cloud Computing.
- ❑ In cloud computing Multitenancy also refer as shared host where same resources are divided among different customer's.

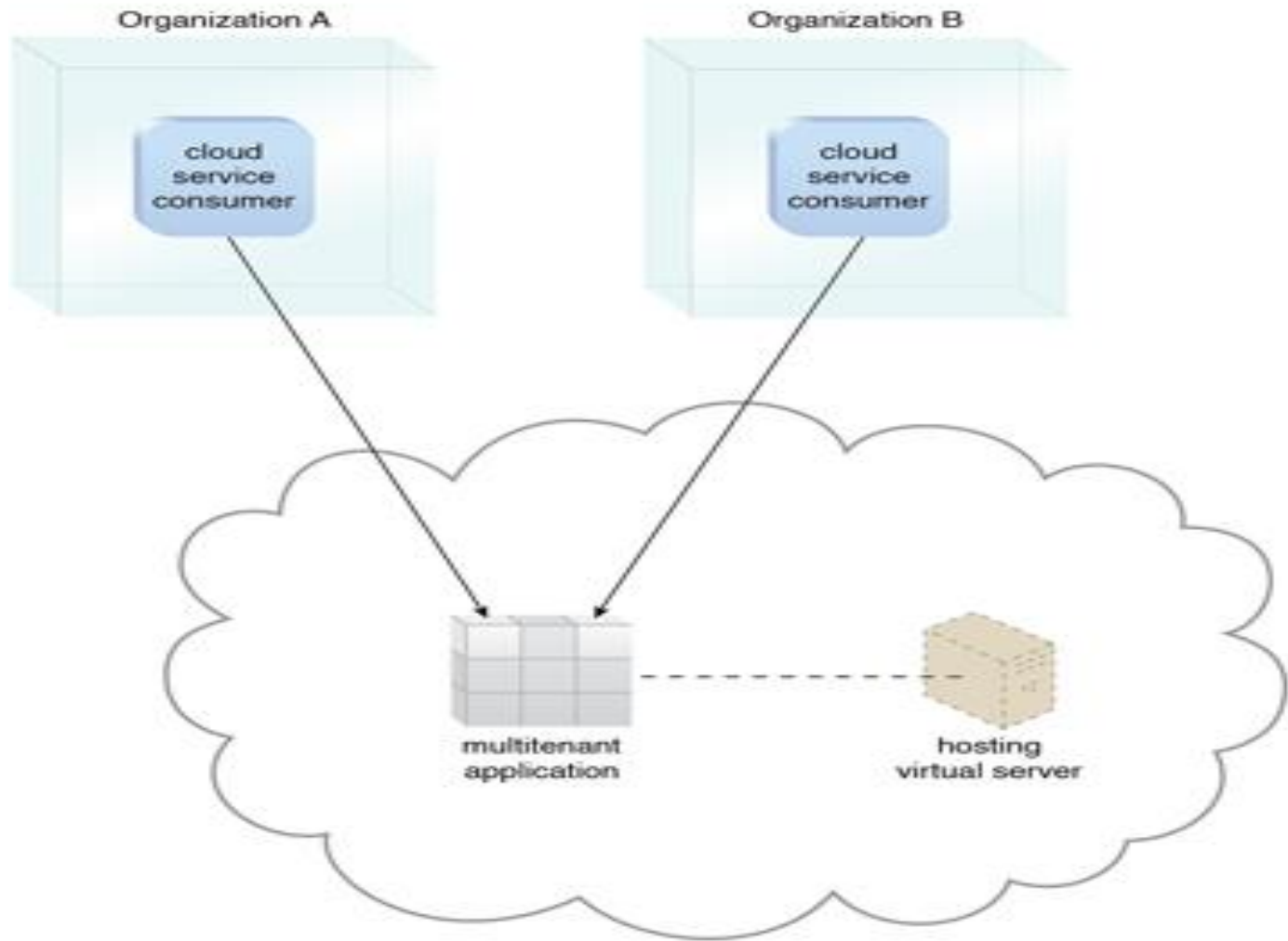
Multitenant Technology

- ❑ The multitenant application design was created to enable multiple users (tenants) to access the same application logic simultaneously.
- ❑ Each tenant has its own view of the application that it uses, administers, and customizes as a dedicated instance of the software while remaining unaware of other tenants that are using the same application.

Multitenant Technology



Multitenant Application



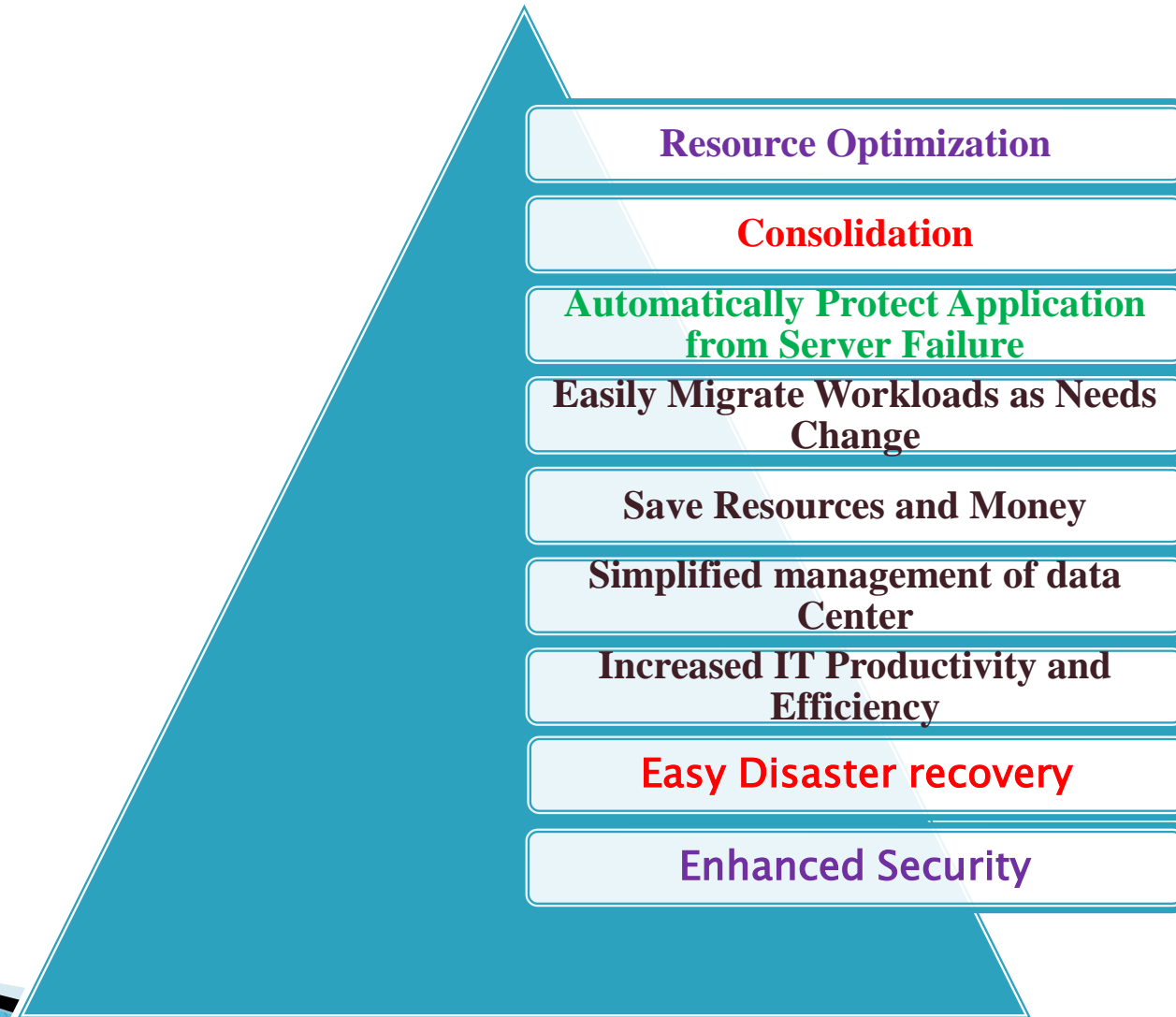
Advantages of Multitenant Technology

- ▶ Use of Available resources is maximized by sharing resources.
- ▶ Customer's Cost of Physical Hardware System is reduces.
- ▶ It reduce usage of physical devices and thus power consumption and cooling cost save.
- ▶ Save Vendor's cost as it become difficult for cloud vendor to provide separate Physical Services to each individual.

Disadvantages of Multitenant Technology

- ▶ As data is stored in third party services , this reduces security of our data and put it into vulnerable condition .
- ▶ Unauthorized access will cause damage of data.

Need of virtualization/Advantages of Virtualization



Disadvantages of Virtualization

It can be Expensive

Might not be compatible with other
server and application

Needs training to network
administrators

It still has limitations

Creates Security risk

Creates resource availability issue

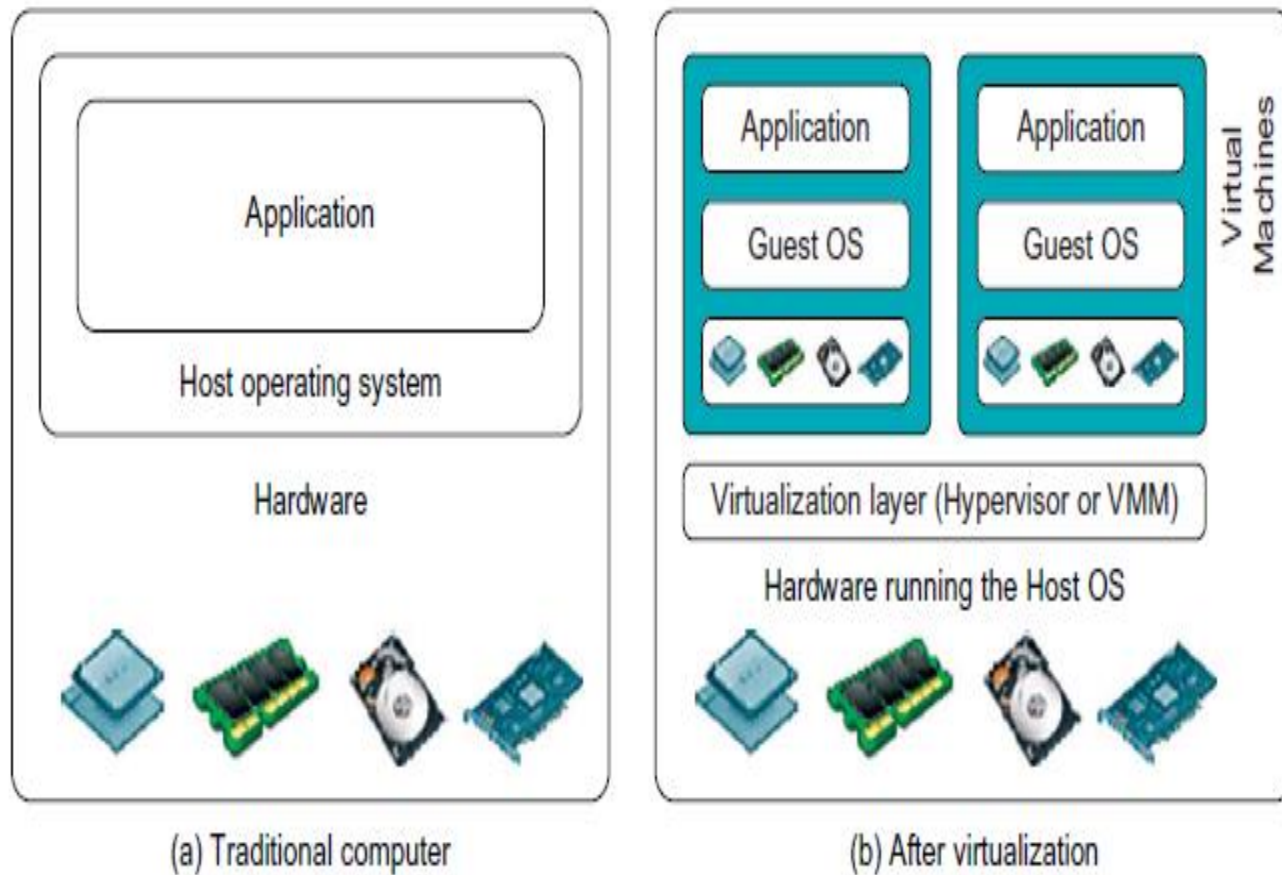
Creates Scalability issue

Requires several links in a chain that
must work together cohesively

Implementation Levels of Virtualization

- Traditional computer runs under the control of its operating system which is basically tailored for its hardware architecture
- After the implementation of virtualization, various user applications which are handled by their own operating system can be executed on the same hardware, independent of the host OS
- This is usually implemented by introducing additional software called a virtualization layer or Hypervisor
- The important functionality of the software layer in the process of virtualization is to virtualize the physical hardware owned by the host machine in the form of virtual resources to be utilized by the VMs

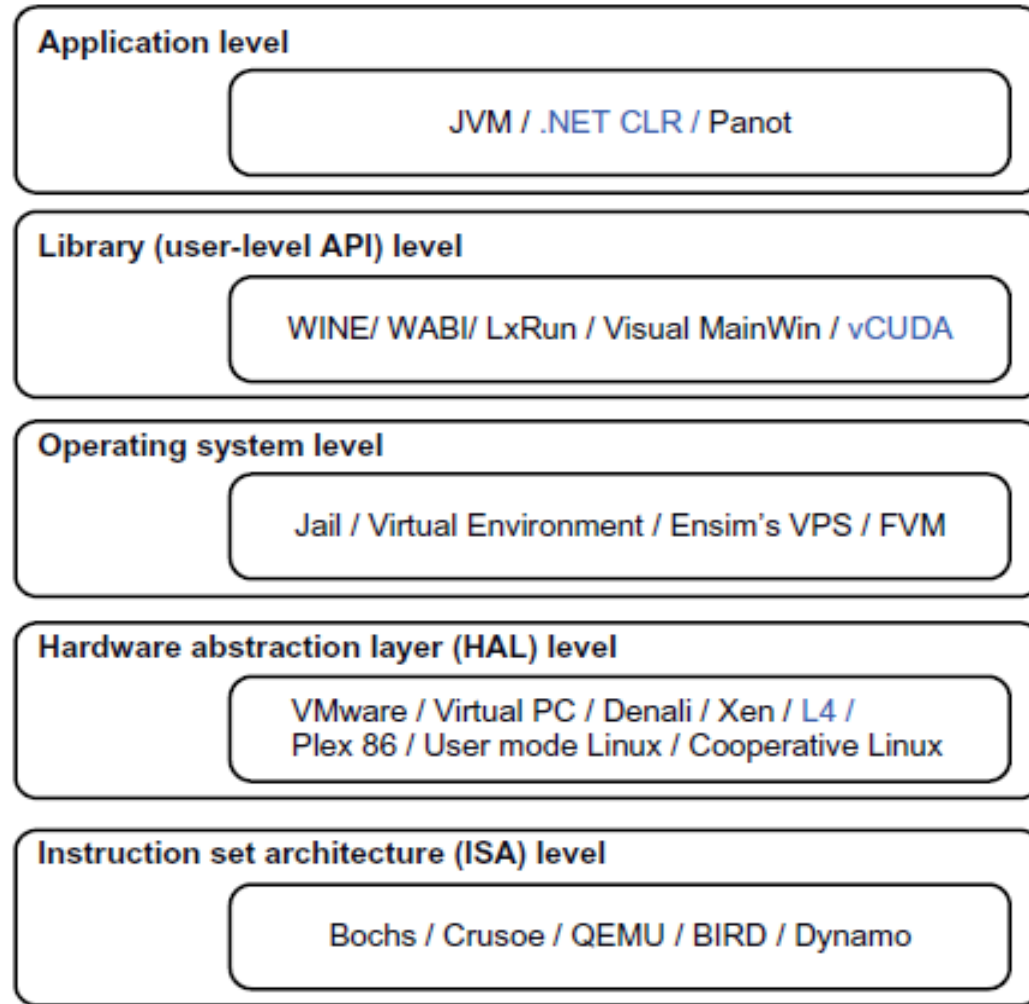
Implementation Levels of Virtualization



Implementation Levels of Virtualization

- ▶ Functionality of software layer is implemented at different operational levels
- ▶ The virtualization layer includes following levels:
 - Instruction Set Architecture(ISA) level
 - Hardware level
 - Operating System Level
 - Library Support Level
 - Application Level

Implementation Levels of Virtualization



Virtualization at ISA (Instruction Set Architecture) level

- ▶ Emulating a given ISA by the ISA of the host machine.
 - e.g, MIPS binary code can run on an x-86-based host machine with the help of ISA emulation.
 - Typical systems: Bochs, Crusoe, Qemu, BIRD, Dynamo
- ▶ **Advantage:**
 - It can run a large amount of legacy binary codes written for various processors on any given new hardware host machines
 - best application flexibility
- ▶ **Shortcoming & limitation:**
 - One source instruction may require tens or hundreds of native target instructions to perform its function, which is relatively slow.
 - V-ISA requires adding a processor-specific software translation layer in the compiler.

Virtualization at Abstraction Level

- ▶ *Virtualization at Hardware Abstraction level:*

- ▶ Virtualization is performed right on top of the hardware.
- It generates virtual hardware environments for VMs, and manages the underlying hardware through virtualization.
- Typical systems: VMware, Virtual PC, Denali, Xen
- ▶ **Advantage:**
 - Has higher performance and good application isolation
- ▶ **Shortcoming & limitation:**
 - Very expensive to implement (complexity)

Virtualization at OS Level

- ▶ It is an abstraction layer between traditional OS and user applications.
- This virtualization creates isolated containers on a single physical server and the OS-instance to utilize the hardware and software in datacenters.
- Typical systems: Jail / Virtual Environment / Ensim's VPS / FVM
- ▶ **Advantage:**
 - Has minimal startup/shutdown cost, low resource requirement, and high scalability; synchronize VM and host state changes.
- ▶ **Shortcoming & limitation:**
 - All VMs at the operating system level must have the same kind of guest OS
 - Poor application flexibility and isolation.

Virtualization at OS Level

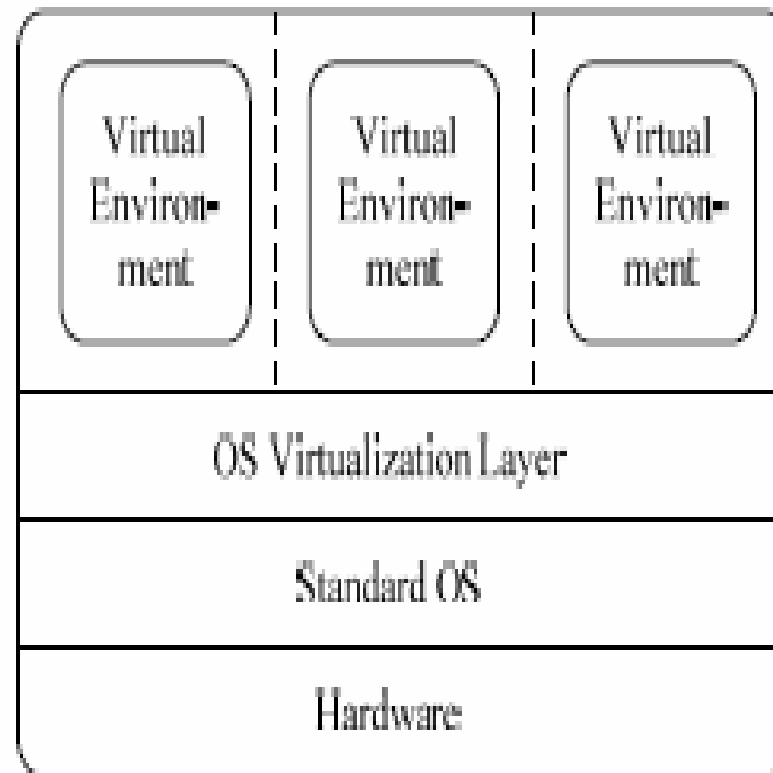
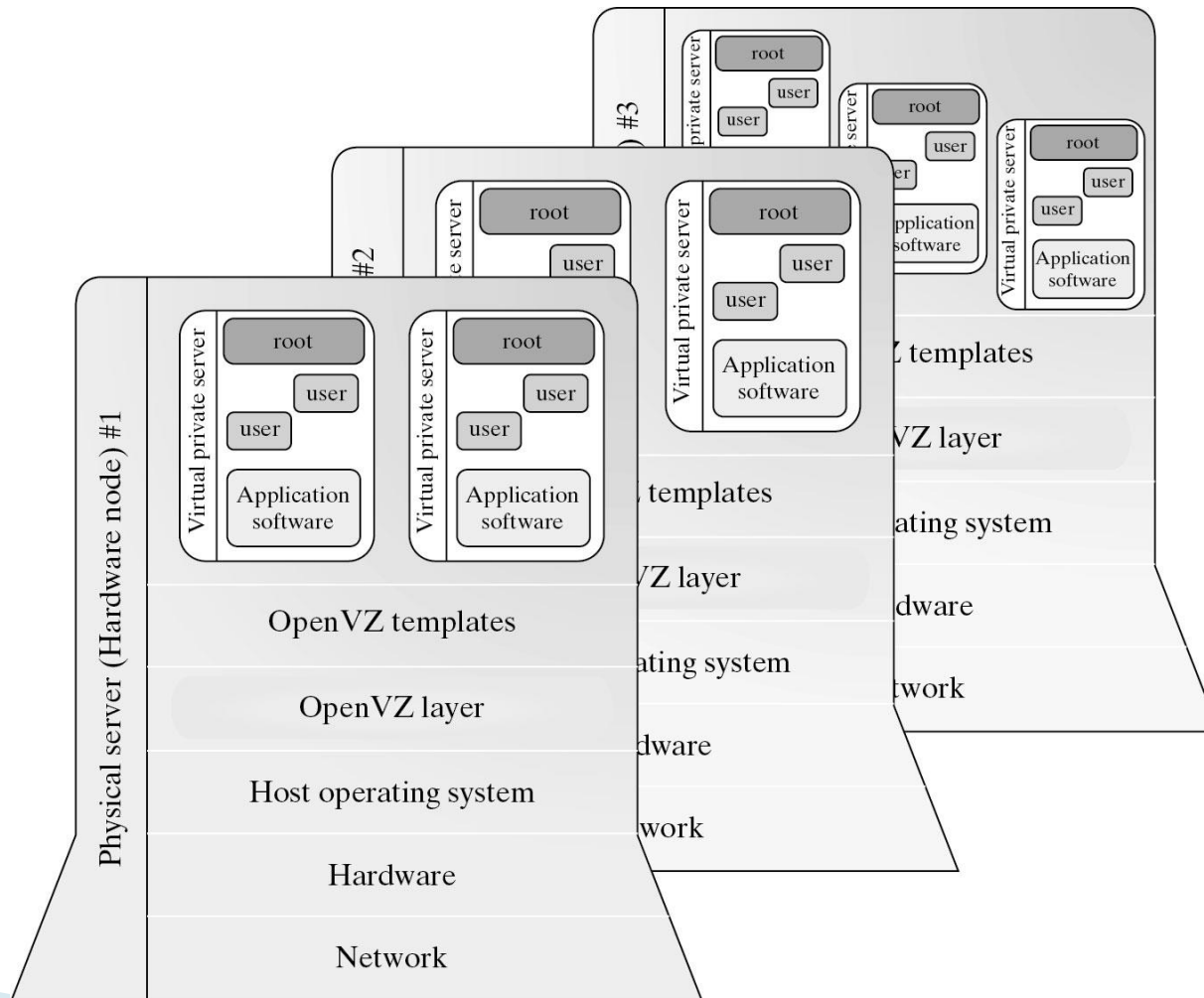


Figure 6.3 The virtualization layer is inserted inside an OS to partition the hardware resources for multiple VMs to run their applications in virtual environments

Virtualization for Linux



Virtualization at Library Support Level

- ▶ It creates execution environments for running alien programs on a platform rather than creating VM to run the entire operating system.
- It is done by API call interception and remapping.
- Typical systems: Wine, WAB, LxRun , VisualMainWin
- ▶ **Advantage:**
- It has very low implementation effort
- ▶ **Shortcoming & limitation:**
- poor application flexibility and isolation

Virtualization with Middleware Support

Table 3.4 Middleware and Library Support for Virtualization

Middleware or Runtime Library and References or Web Link	Brief Introduction and Application Platforms
WABI (http://docs.sun.com/app/docs/doc/802-6306)	Middleware that converts Windows system calls running on x86 PCs to Solaris system calls running on SPARC workstations
Lxrun (Linux Run) (http://www.ugcs.caltech.edu/~steven/lxrun/)	A system call emulator that enables Linux applications written for x86 hosts to run on UNIX systems such as the SCO OpenServer
WINE (http://www.winehq.org/)	A library support system for virtualizing x86 processors to run Windows applications under Linux, FreeBSD, and Solaris
Visual MainWin (http://www.mainsoft.com/)	A compiler support system to develop Windows applications using Visual Studio to run on Solaris, Linux, and AIX hosts
vCUDA (Example 3.2) (IEEE <i>IPDPS</i> 2009 [57])	Virtualization support for using general-purpose GPUs to run data-intensive applications under a special guest OS

The vCUBE for Virtualization of GPGPU

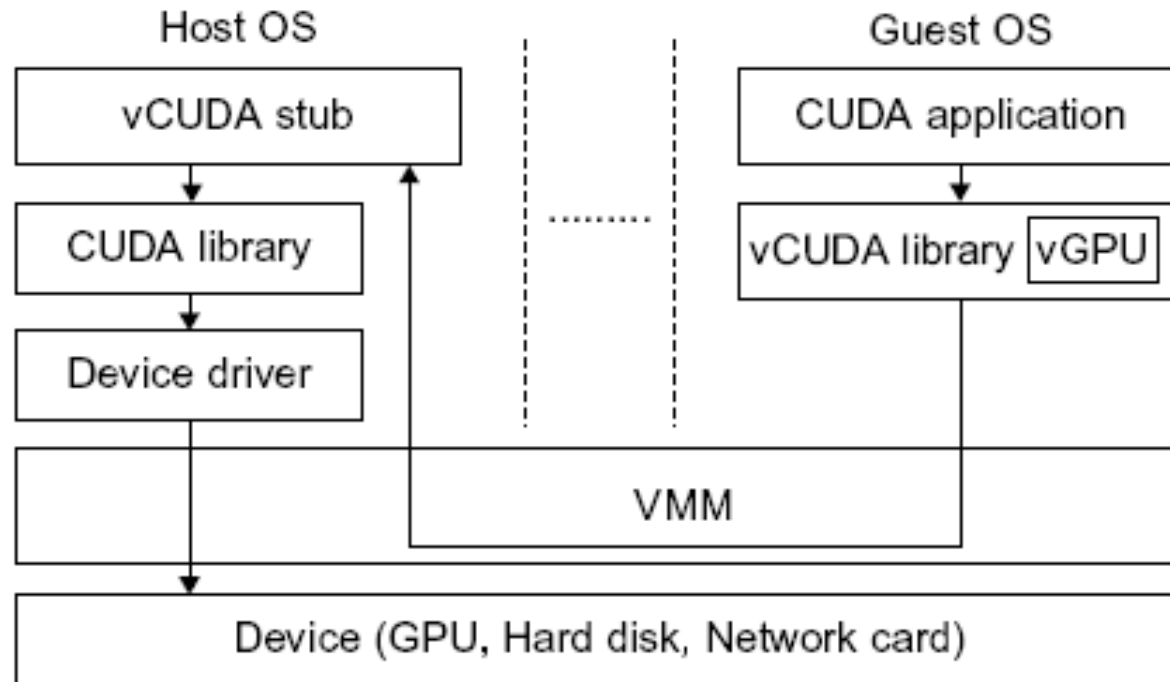


FIGURE 3.4

Basic concept of the vCUDA architecture.

(Courtesy of Lin Shi, et al. [57])

Virtualization at User Application Level

- ▶ It virtualizes an application as a virtual machine.
- This layer sits as an application program on top of an operating system and exports an abstraction of a VM that can run programs written and compiled to a particular abstract machine definition.
- Typical systems: JVM , NET CLI , Panot
- ▶ **Advantage:**
- has the best application isolation
- ▶ **Shortcoming & limitation:**
- low performance, low application flexibility and high implementation complexity.

Relative Merits of Different Approaches

- ▶ The column heading corresponds to four technical heading
 - ▶ – Higher Performance
 - ▶ – Application Flexibility
 - ▶ – Implementation Complexity[implies the implementation cost of virtualization level]
 - ▶ – Application Isolation[refers to the effort required to isolate resource committed to different VMs]

Level of Implementation	Higher Performance	Application Flexibility	Implementation Complexity	Application Isolation
ISA	X	XXXXX	XXX	XXX
Hardware-level virtualization	XXXXX	XXX	XXXXX	XXXX
OS-level virtualization	XXXXX	XX	XXX	XX
Runtime library support	XXX	XX	XX	XX
User application level	XX	XX	XXXXX	XXXXX

VMM Design Requirements and Providers

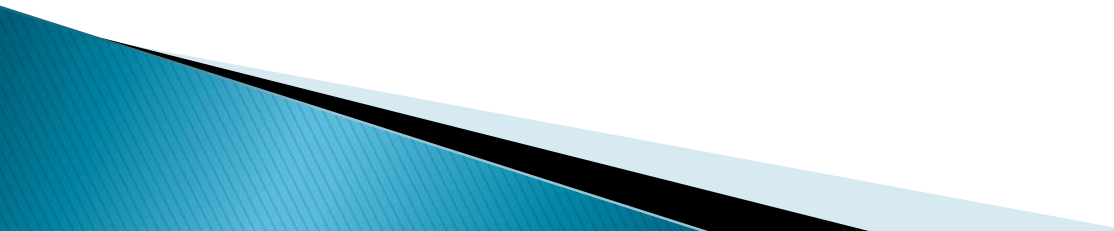
- Hardware-level virtualization insert a layer between real hardware and traditional Operating systems call as Virtual Machine Monitor(VMM)
- It manages hardware resources of a computing system
- There are three requirements for VMM
 - VMM should provide an environment for program which is essentially Identical to original machine
 - Program run in this environment should show, at worst, only minor decrease in speed
 - VMM should be in complete control of system resources

Provider and References	Host CPU	Host OS	Guest OS	Architecture
VMware Workstation [71]	x86, x86-64	Windows, Linux	Windows, Linux, Solaris, FreeBSD, Netware, OS/2, SCO, BeOS, Darwin	Full Virtualization
VMware ESX Server [71]	x86, x86-64	No host OS	The same as VMware Workstation	Para-Virtualization
Xen [7,13,42]	x86, x86-64, IA-64	NetBSD, Linux, Solaris	FreeBSD, NetBSD, Linux, Solaris, Windows XP and 2003 Server	Hypervisor
KVM [31]	x86, x86-64, IA-64, S390, PowerPC	Linux	Linux, Windows, FreeBSD, Solaris	Para-Virtualization

Virtualization Structure/Tools and Mechanisms

- Before the implementation of virtualization, the hardware is managed by operating system
- After virtualization process, a virtualization layer is placed in between the hardware and the OS
- Converting the real hardware into virtual hardware is the responsibility of this virtualization layer
- There are several classes of VM architecture which depends on the position of the virtualization layer. These are mainly Hypervisor architecture, Para Virtualization, Full virtualization

Hypervisor and Xen Architecture

- Hypervisor is a type of hardware level virtualization
 - The hypervisor software is exactly paced between physical hardware and its operating system
 - Hyper calls are provided by the hypervisor for the guest OS and application
 - It is very important that the hypervisor should have capability to convert physical devices into virtual resources
- 

Xen Architecture

- It is an open source hypervisor program which is developed by Cambridge University
- All the machine are implemented by Xen hypervisor, and policy handling is the responsibility of Domain 0

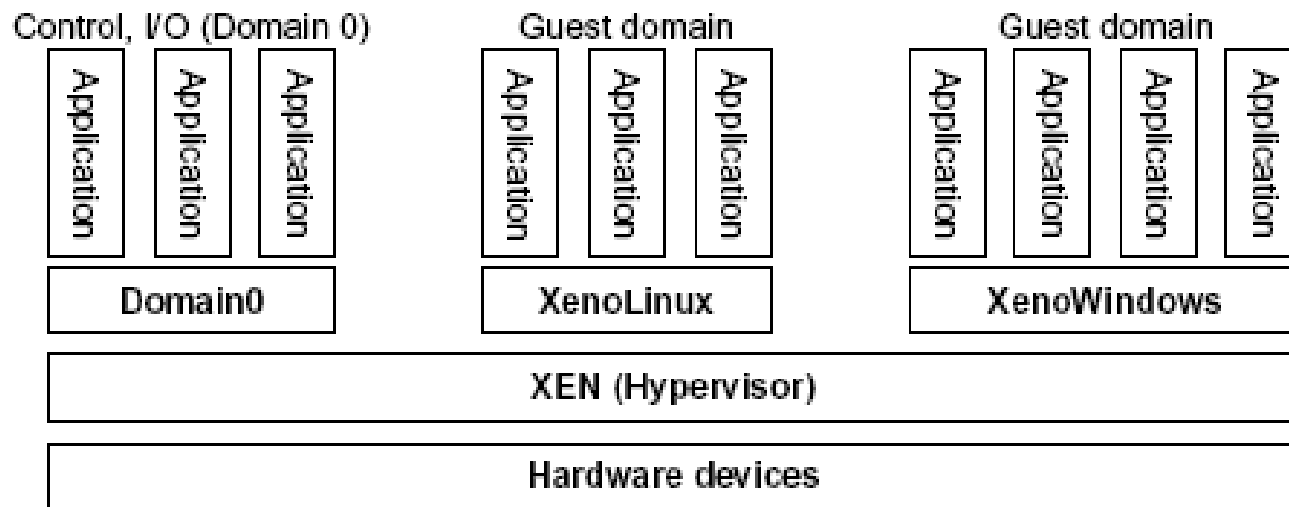


FIGURE 3.5

The Xen architecture's special domain 0 for control and I/O, and several guest domains for user applications.

- In Xen, no device drivers are included natively, just a mechanism is provided by Xen with the help of which guest OS can have direct access to the physical device
- Like other virtualization, number of guest OS can be executed on top of hypervisor
- The guest OS, which can control other OS is known as **Domain 0** while other are known as **Domain U**
- Domain 0 is considered as privilege guest OS of Xen
- Initially Domain 0 is loaded when Xen boots
- The basic aim behind design of Domain 0 is to access hardware directly as well as manage device
- Allocating and mapping hardware resources for the guest domain (Domain U) is responsibility of Domain 0

Full Virtualization

- Hardware virtualization can be classified into two categories based on the implementation technology:

Full Virtualization and Host-based virtualization

➤ Full Virtualization:

- Does not need to modify guest OS
- Non-critical instructions execute on hardware directly
- Critical instruction are trapped into VMM for binary translation
- VMware Workstation applies full virtualization, which uses binary translation to automatically modify x86 software on-the-fly to replace critical instructions.

➤ Advantage:

- no need to modify OS.

➤ Disadvantage:

- binary translation slows down the performance.

Binary Translation of Guest OS Request using VMM

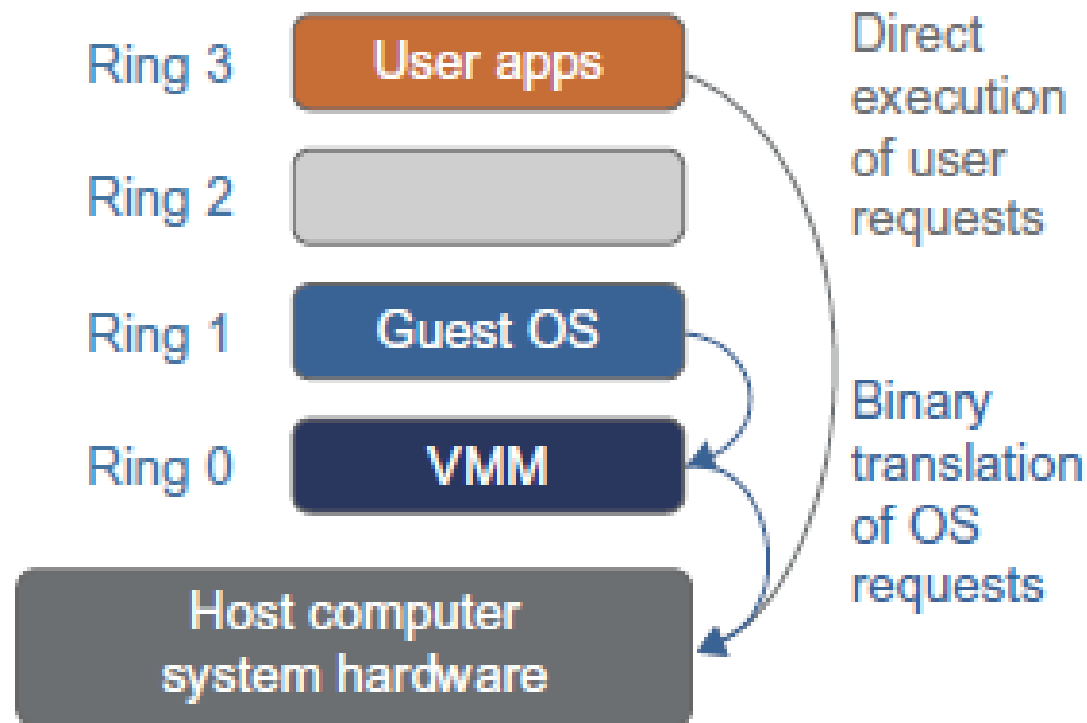
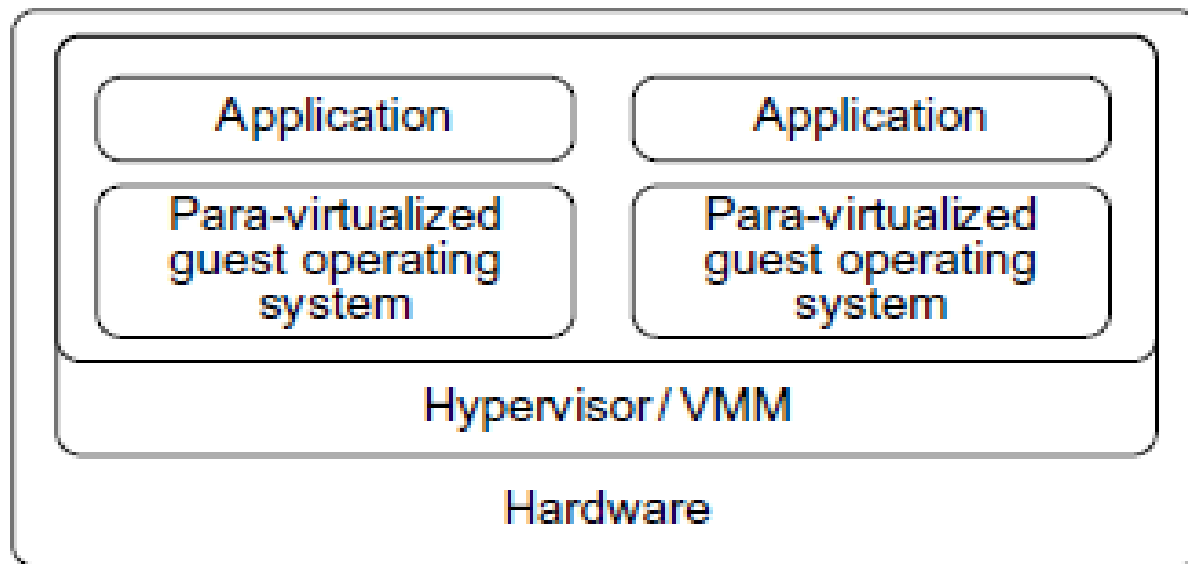


FIGURE 3.6

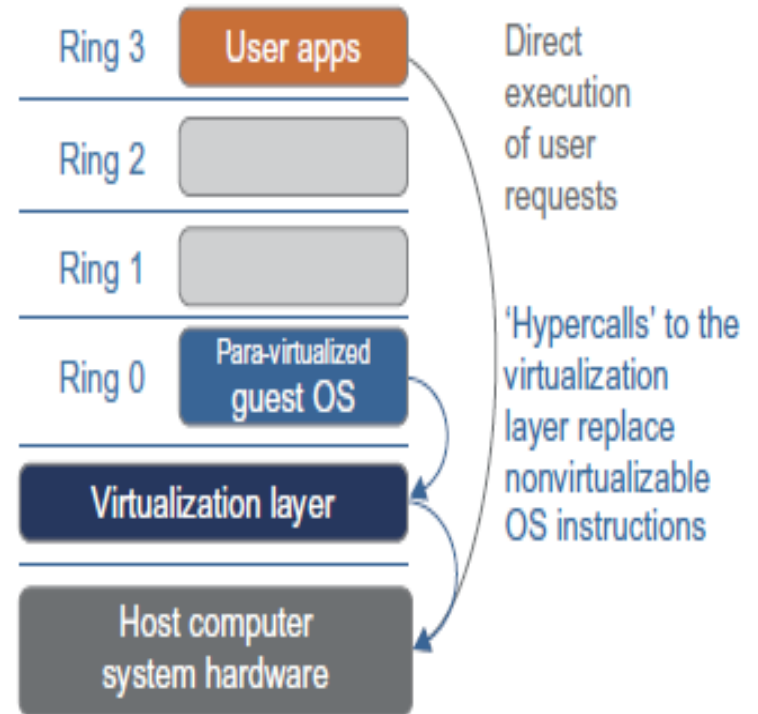
Indirect execution of complex instructions via binary translation of guest OS requests using the VMM plus direct execution of simple instructions on the same host.

Para-Virtualization

- The guest OS are modified by the Para-Virtualization
- Special API is provided by the para-virtualized VM which requires substantial OS modification in the user application
- Following fig. illustrate the concept of para-virtualized VM architecture



- In the traditional x86 processor, there are four instruction execution rings: Ring 0,1,2,3
- The lower the ring number, higher the privilege of instruction being executed
- The hardware management and execution of privileged instruction is done by the OS so implemented at Ring 0, while user-level application are executed at Ring 3



Types of Hypervisor

A hypervisor is a hardware virtualization technique allowing multiple operating systems, called guests to run on a host machine. This is also called the Virtual Machine Monitor (VMM).

Type 1: Bare Metal Hypervisor

- sits on the bare metal computer hardware like the CPU, memory, etc.
- All guest operating systems are a layer above the hypervisor.
- The original CP/CMS hypervisor developed by IBM was of this kind.

Type 2: hosted hypervisor

- Run over a host operating system.
- Hypervisor is the second layer over the hardware.
- Guest operating systems run a layer over the hypervisor.
- The OS is usually unaware of the virtualization

THANK YOU!