VIRTUALIZATION

Dr. Manjunath Hegde
Dept. of Computer Applications
Manipal Institute of Technology, Manipal

INTRODUCTION (1/3)

- Logical abstraction of computing resources
- i.e. Separation of resource and/or service request from underlying physical delivery of that service request
- A means of separating hardware from a single operating system
- Allows multiple operating system instances to run concurrently on a single computer.

INTRODUCTION (2/3)

- 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 was initially developed during the mainframe era.
- 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.

INTRODUCTION (3/3)

- In other words, one of the main cost effective, hardware reducing, and energy saving techniques used by cloud providers is virtualization.
- Virtualization allows to share a single physical instance of a resource or an application among multiple customers and organizations at one time.
- It does this by assigning a logical name to a physical storage and providing a pointer to that physical resource on demand.
- The term virtualization is often synonymous with hardware virtualization, which plays a fundamental role in efficiently delivering Infrastructure-as-a-Service (IaaS) solutions for cloud computing.
- Moreover, virtualization technologies provide a virtual environment for not only executing applications but also for storage, memory, and networking.

BENEFITS

- More flexible and efficient allocation of resources.
- Enhance development productivity.
- It lowers the cost of IT infrastructure.
- Remote access and rapid scalibility.
- High availability and disaster recovery.
- Pay per use of the IT infrastructure on demand.
- Enables running multiple operating system.

CONCEPT AND TYPES

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

Types of Virtualization:

- Data Virtualization
- Hardware Virtualization.
- Application Virtualization.
- Network Virtualization.
- Desktop Virtualization.
- Storage Virtualization.
- Server Virtualization.
- Operating system Virtualization.

CHARACTERISTICS (1/5)

Increased Security

- The ability to control the execution of a guest programs in a completely transparent manner opens new possibilities for delivering a secure, controlled execution environment.
- All the operations of the guest programs are generally performed against the virtual machine, which then translates and applies them to the host programs.
- A virtual machine manager can control and filter the activity of the guest programs, thus preventing some harmful operations from being performed.
- Resources exposed by the host can then be hidden or simply protected from the guest.
- Increased security is a requirement when dealing with untrusted code.

EXAMPLES

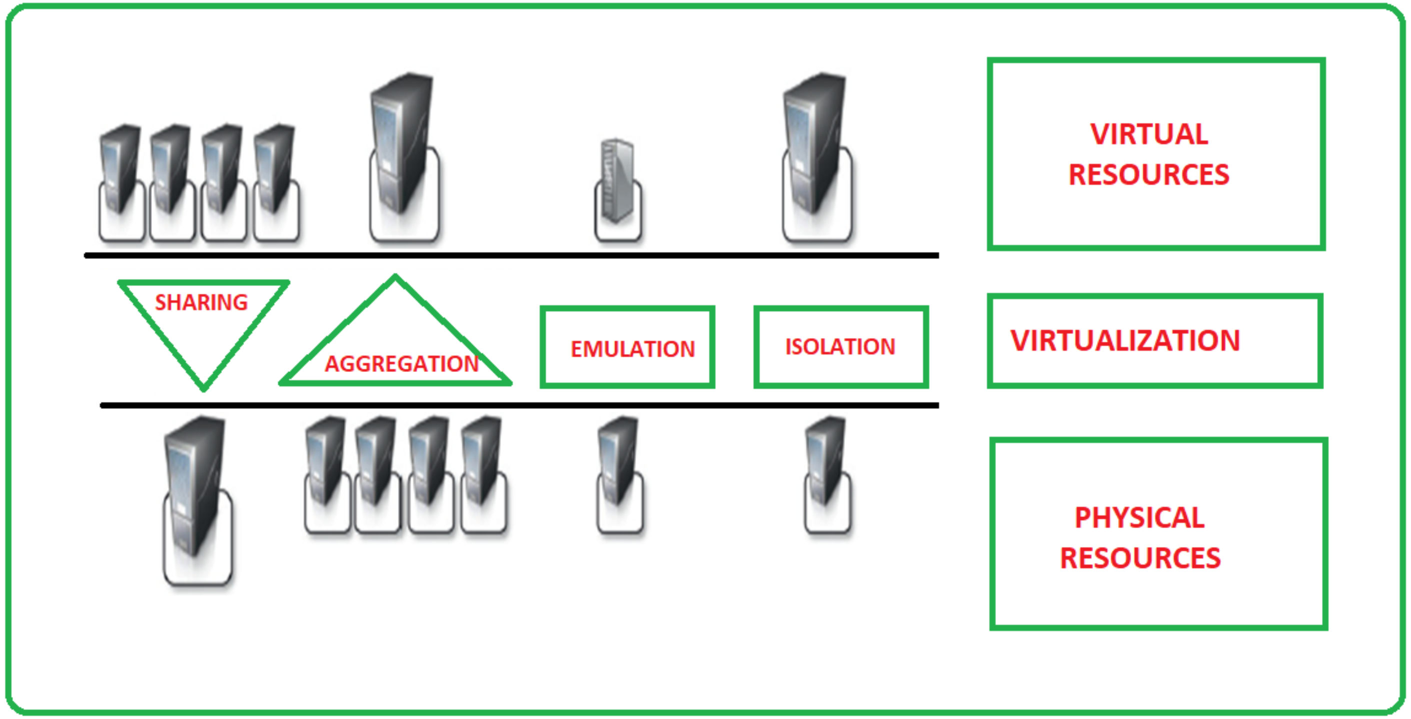
- **Example-1:** Untrusted code can be analyzed in Cuckoo sandboxe environment. The term sandbox identifies an isolated execution environment where instructions can be filtered and blocked before being translated and executed in the real execution environment.

- **Example-2:** The expression sandboxed version of the Java Virtual Machine (JVM) refers to a particular configuration of the JVM where, by means of security policy, instructions that are considered potentially harmful can be blocked.

CHARACTERISTICS (2/5)

Managed Execution

- In particular, sharing, aggregation, emulation, and isolation are the most relevant features.



CHARACTERISTICS (3/5)

Sharing

- Virtualization allows the creation of a separate computing environments within the same host.
- This basic feature is used to reduce the number of active servers and limit power consumption.

Aggregation

- Not only possible to share physical resource among several guests, but virtualization also allows aggregation, which is the opposite process.
- A group of separate hosts can be tied together and represented to guests as a single virtual host.
- This functionality is implemented with cluster management software, which harnesses the physical resources of a homogeneous group of machines and represents them as a single resource.

CHARACTERISTICS (4/5)

Emulation

- Guest programs are executed within an environment that is controlled by the virtualization layer, which ultimately is a program.
- Also a completely different environment with respect to the host can be emulated, thus allowing the execution of guest programs requiring specific characteristics that are not present in the physical host.

Isolation

- Virtualization allows providing guests—whether they are operating systems, applications, or other entities—with a completely separate environment, in which they are executed.
- The guest program performs its activity by interacting with an abstraction layer, which provides access to the underlying resources.
- The virtual machine can filter the activity of the guest and prevent harmful operations against the host.

CHARACTERISTICS (5/5)

Portability

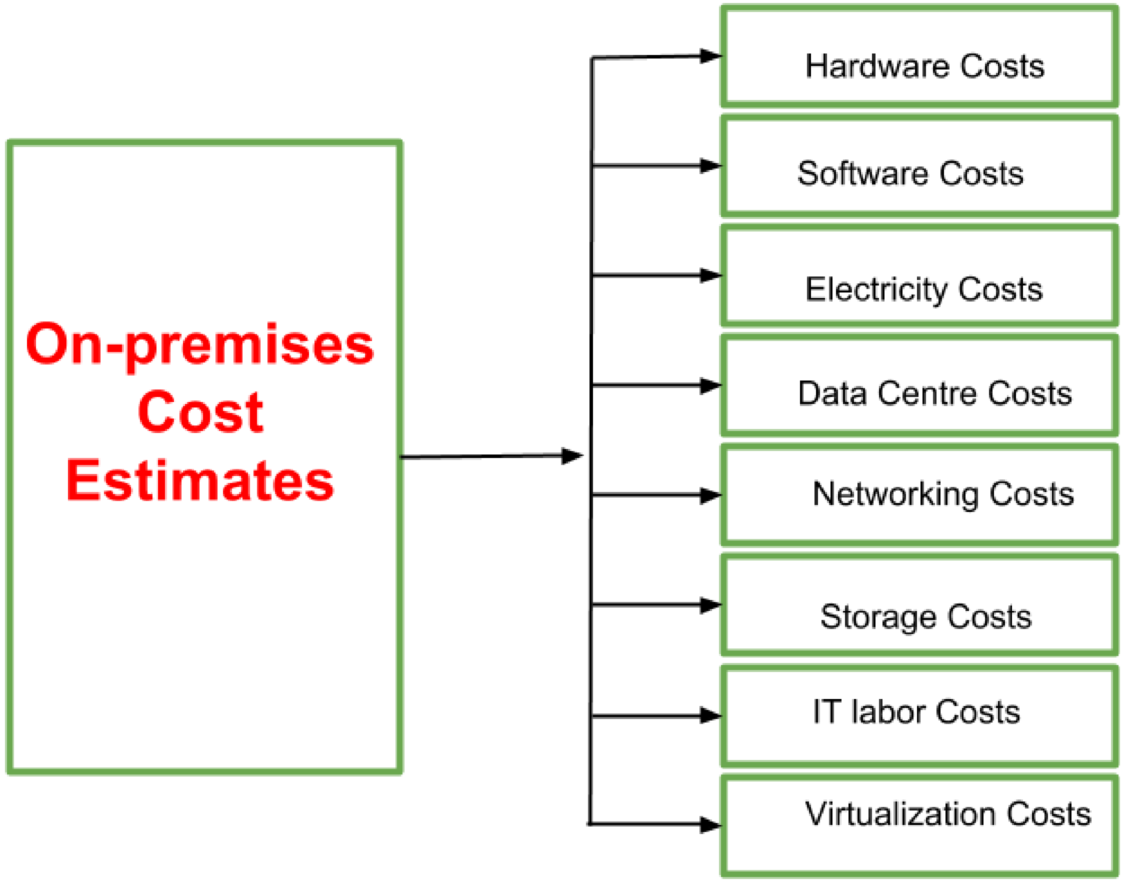
- The concept of portability applies in different ways according to the specific type of virtualization considered.
- In the case of a hardware virtualization solution, the guest is packaged into a virtual image that, in most cases, can be safely moved and executed on top of different virtual machines.
- In the case of programming-level virtualization, as implemented by the JVM or the .NET runtime, the binary code representing application components (jars or assemblies) can run without any recompilation on any implementation of the corresponding virtual machine

HYPERVISOR

- A program that allows multiple operating systems to share a single hardware host.
- Also called Virtual machine manager/monitor (VMM), or virtualization manager.
- Hypervisor actually controls processor and resources, allocating what is needed to each operating system in turn and making sure that the guest operating systems (VMs) don't disrupt each other.

- Virtual machine: A self-contained computing environment that behaves as if it is a separate computer.

COST ESTIMATION (1/4)



COST ESTIMATION (2/4)

Hardware costs

- Based on the user's description, the calculator uses estimated market rates to project the costs of requisite physical hardware.

Software costs

- If the user specifies an operating system for the environment, then the calculator provides an estimate of the OS licensing costs based on the number of cores required by the user's environment.

Electricity costs

- Estimates the approximate electricity consumption costs. This is done by allocating a power rating to the user's hardware configuration and then multiplying it with an estimate of the power consumed and an industry standard rate for power consumption.

COST ESTIMATION (3/4)

Data center costs

- Based on the user's description, the calculator estimates the requisite amount of normalized rack space.

Networking costs

- Networking hardware and software costs are estimated to be a fixed percentage of the on-premises hardware and software costs. The calculator also adds a service provider cost based on the outbound bandwidth requirements specified by the user.

Storage costs

- The calculator computes storage cost by multiplying an estimated market rate the amount of disk space specified by the user.

COST ESTIMATION (4/4)

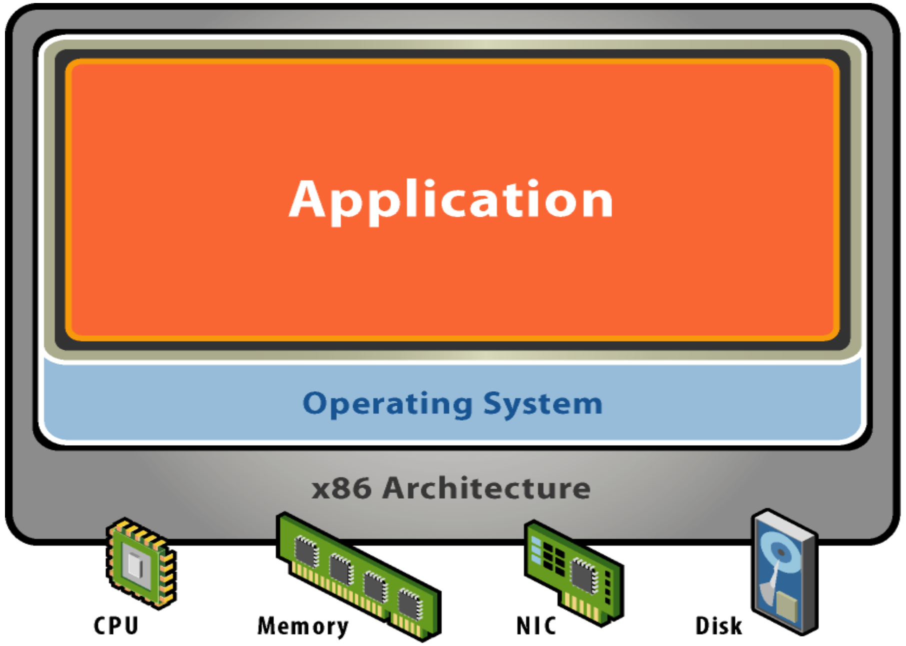
IT labor costs

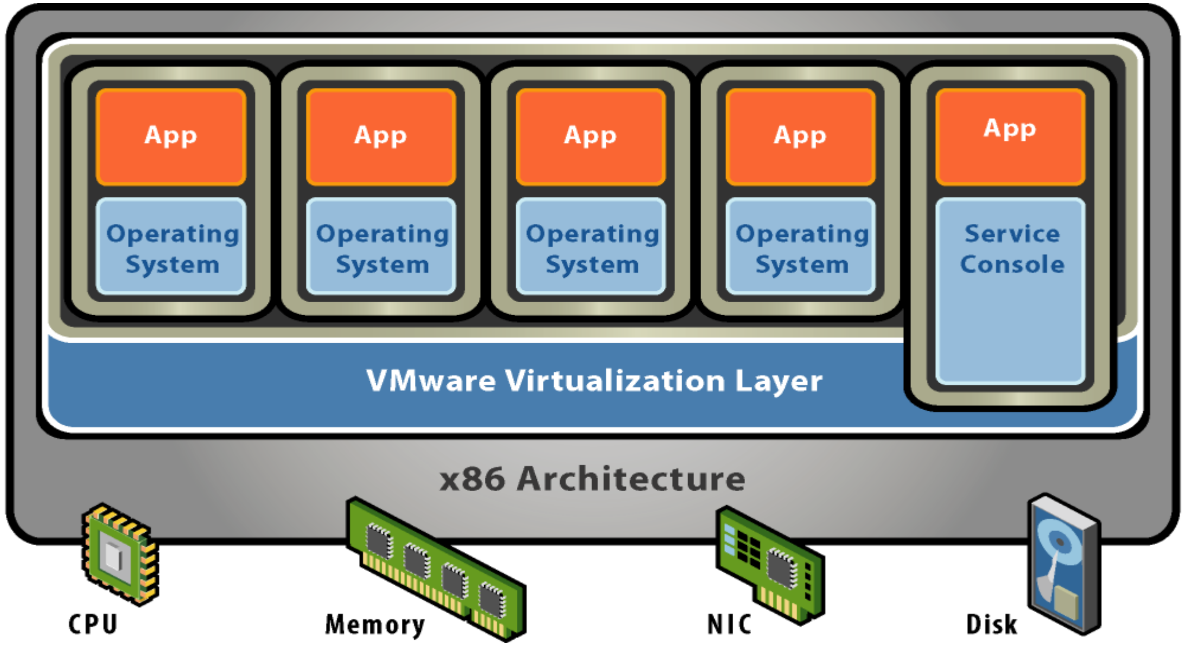
- Based on the user’s description, the calculator estimates the number of IT administrator man-hours that will be required to maintain the on-premises environment.

Virtualization costs

- If the user’s description includes virtual machines, the calculator uses an industry standard per virtual machine management rate to estimate the total virtualization costs.

ARCHITECTURE DIFFERENCES





DIFFERENCES (1/2)

Before Virtualization:

- Single OS image per machine
- Software and hardware tightly coupled
- Running multiple applications on same machine often creates conflict
- Underutilized resources
- Inflexible and costly infrastructure.

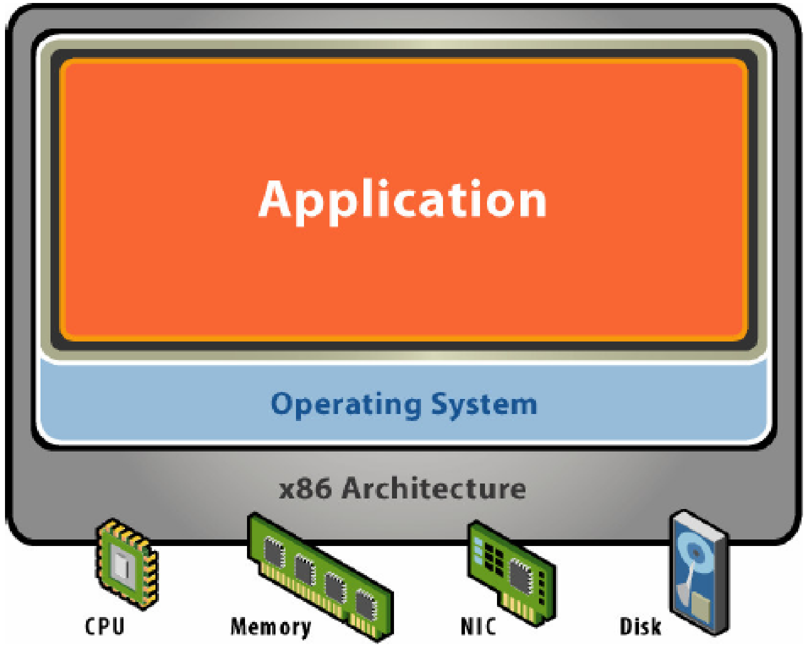
After Virtualization:

- Hardware-independence of operating system and applications
- Virtual machines can be provisioned to any system
- Can manage OS and application as a single unit by encapsulating them into virtual machines

DIFFERENCES (2/2)

- Traditional computing architecture has :
  - Hardware
  - Operating system
  - Application program(s)
- Virtualization architecture has :
  - Hardware (Centralized / Decentralized)
  - Virtualization layer (VMM)
  - Host Operating System
  - Application program(s) //VM
  - Hosted (guest) operating system(s)
  - Hosted (guest) application program(s)

Starting Point: A Physical Machine



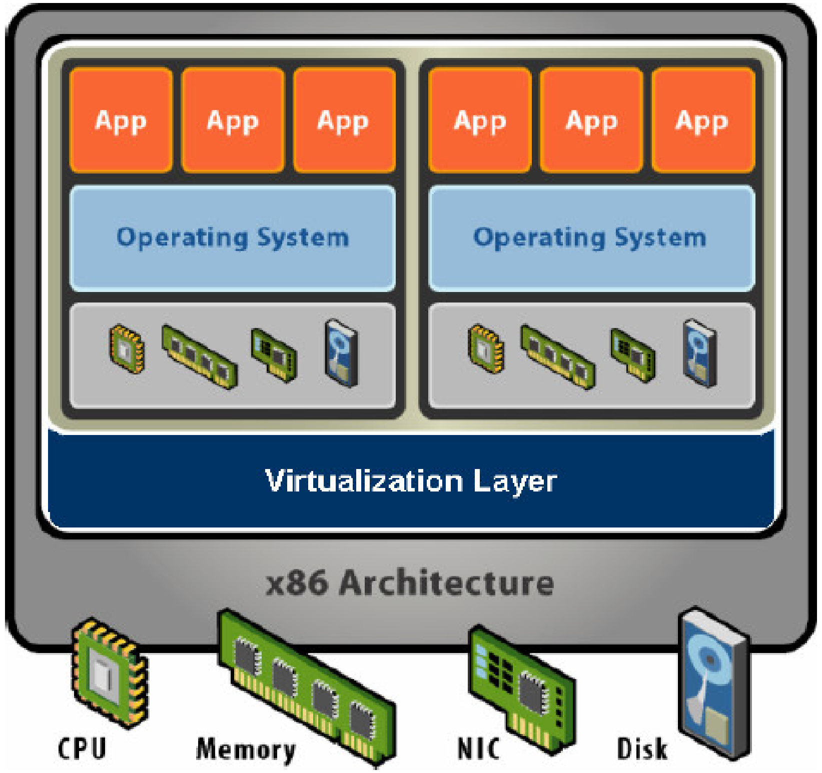
Physical Hardware

- Processors, memory, chipset, I/O bus and devices, etc.
- Physical resources often underutilized

Software

- Tightly coupled to hardware
- Single active OS image
- OS controls hardware

What is a Virtual Machine?



Hardware-Level Abstraction

- Virtual hardware: processors, memory, chipset, I/O devices, etc.
- Encapsulates all OS and application state

Virtualization Software

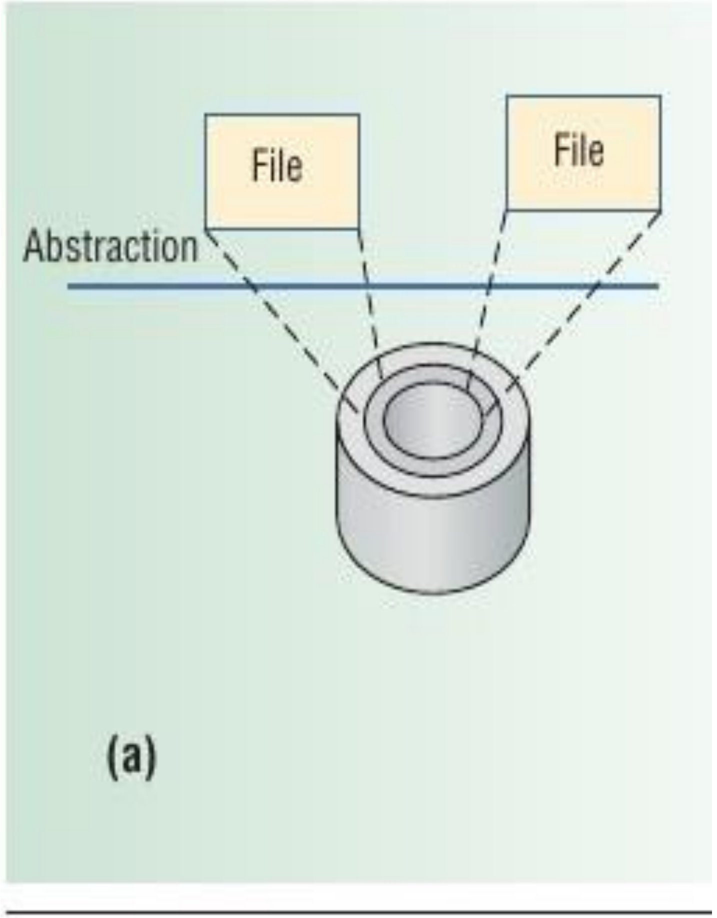
- Extra level of indirection decouples hardware and OS
- Multiplexes physical hardware across multiple "guest" VMs
- Strong isolation between VMs
- Manages physical resources, improves utilization

ARCHITECTURE OF VIRTUAL MACHINES

- VM can support individual processes or a complete system
- Virtualization can be from OS to programming languages to processor architecture.
- VMs enhance
  - Software interoperability (to work together)
  - System impregnability (having strength)
  - Platform versatility

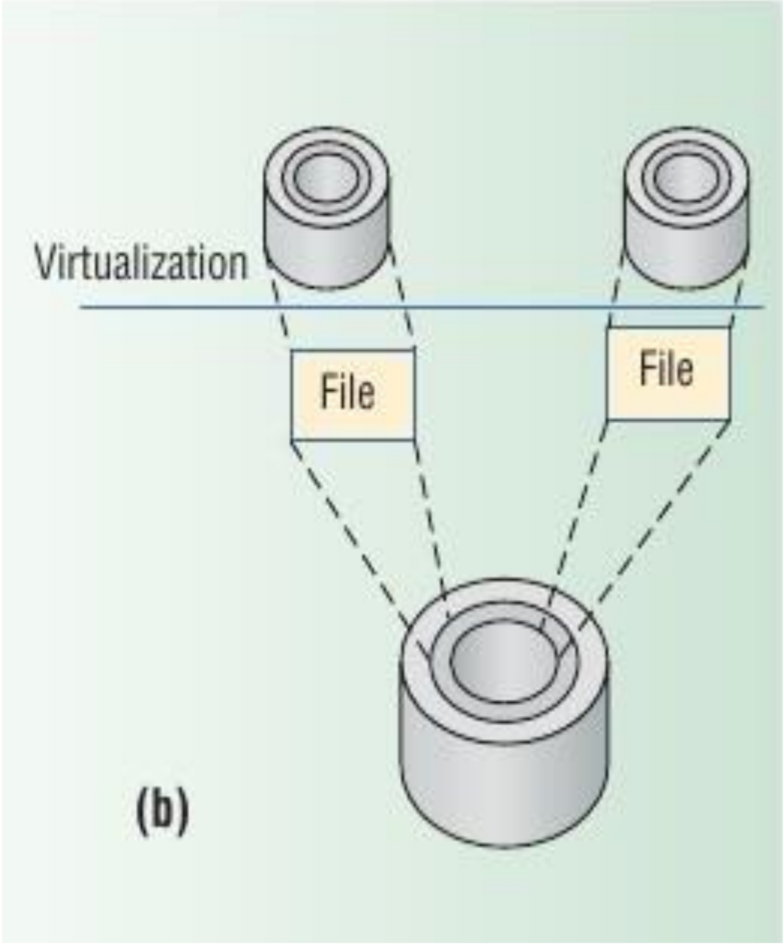
ABSTRACTION AND VIRTUALIZATION

- Computer system is complex, and yet it continue to evolve.
- Computer is designed as hierarchies of well- defined interfaces that separate level of abstraction
- Simplifying abstractions hide lower-level implementation details
- Abstraction
  - Ex. Disk storage
  - Hides hard-disk addressing details (sectors and tracks)
  - It appears to application software as a variable sized files.
  - User can create, write and read files without knowing the underneath details.



VIRTUALIZATION

- Virtualization of system or components like – processor, memory or an I/O device – at a given abstraction level.
- It transforms a entire system or components of the system

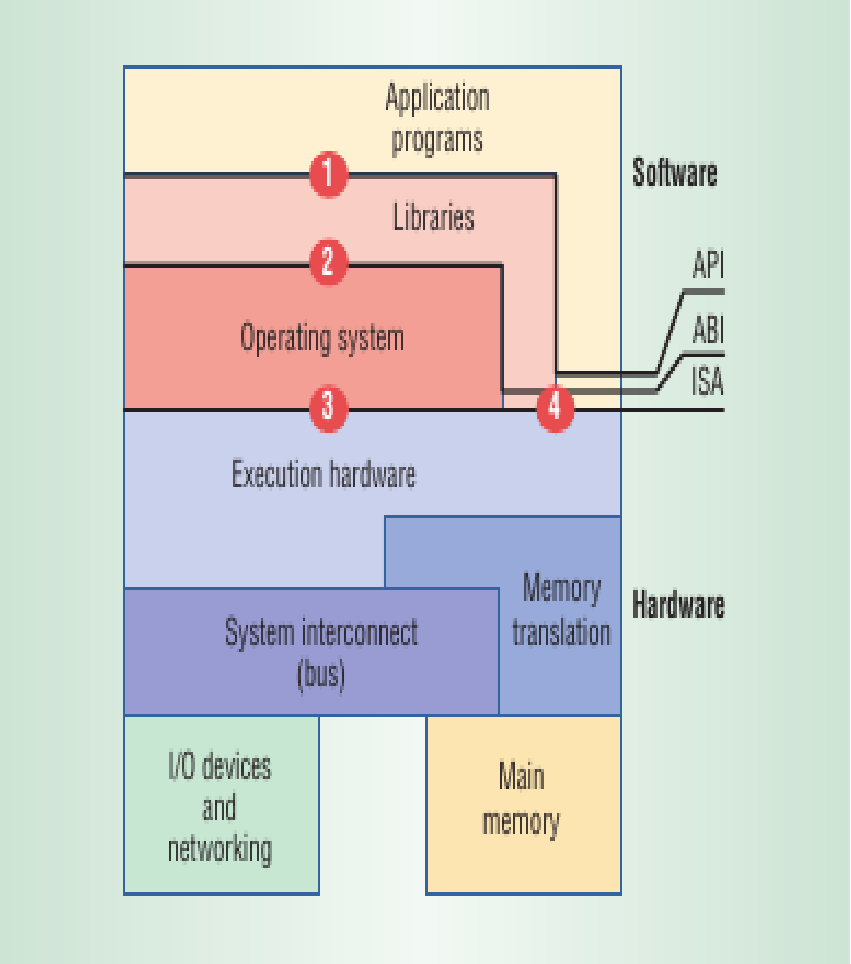


ARCHITECTED INTERFACES

- Architecture, as applied to computer systems, refer to a formal specification to an interface in the system, including the logical behavior of the resources managed via the interface.
- Implementation describes the actual embodiment of an architecture.
- Abstraction levels correspond to implementation layers, having its own interface or architecture.

COMPUTER SYSTEM ARCHITECTURE

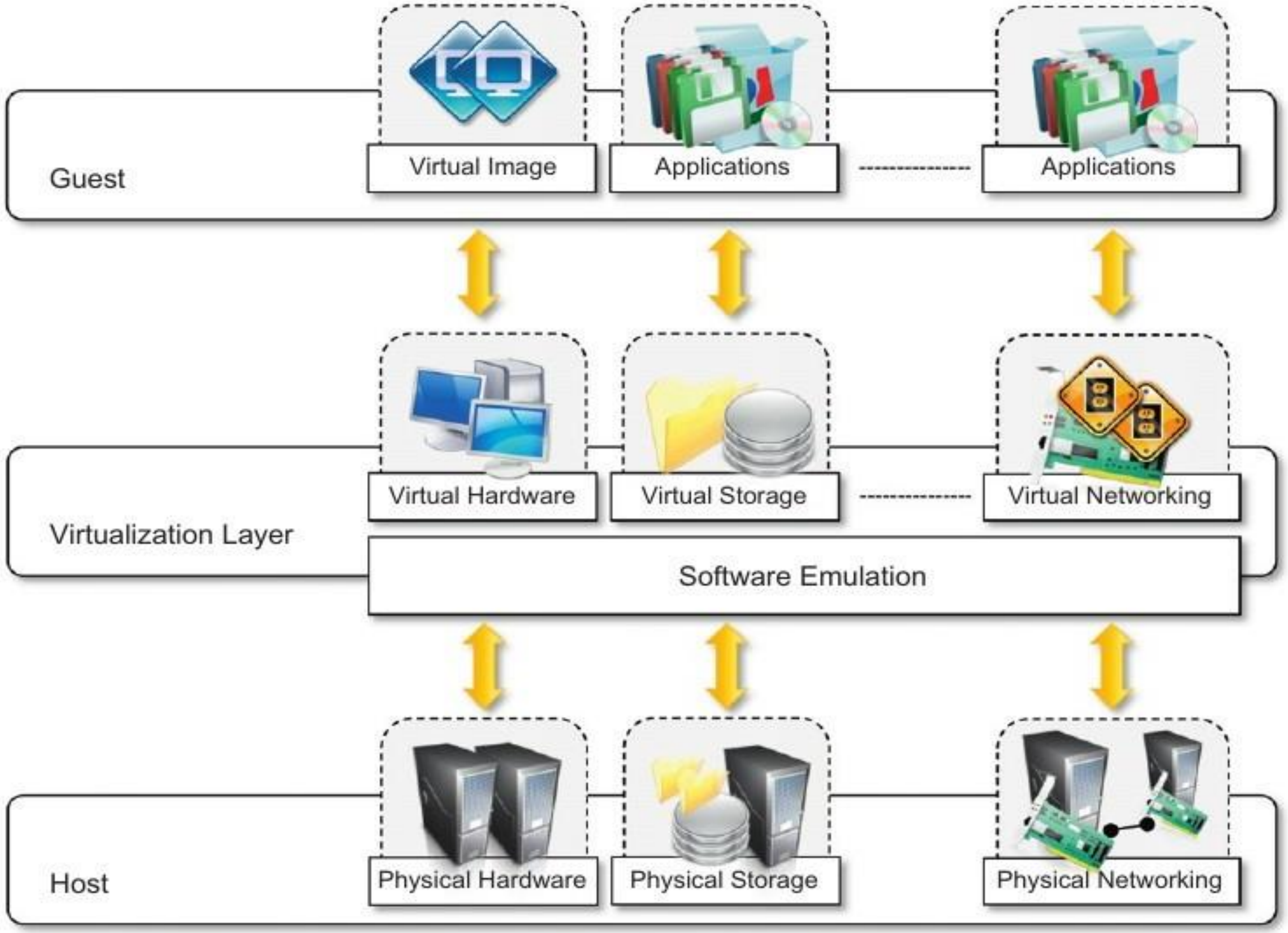
- Interfaces at or near the H/w S/w boundary
- ISA – Instruction Set Architecture.
- API – Application Program Interface
- ABI – Application Binary Interface



VIRTUALIZED ENVIRONMENTS

- Three major components of Virtualized Environments
- **Guest –** system component that interacts with Virtualization Layer.
- **Host –** original environment where guest runs.
- **Virtualization Layer –** recreate the same or different environment where guest will run.

VIRTUALIZATION REFERENCE MODEL



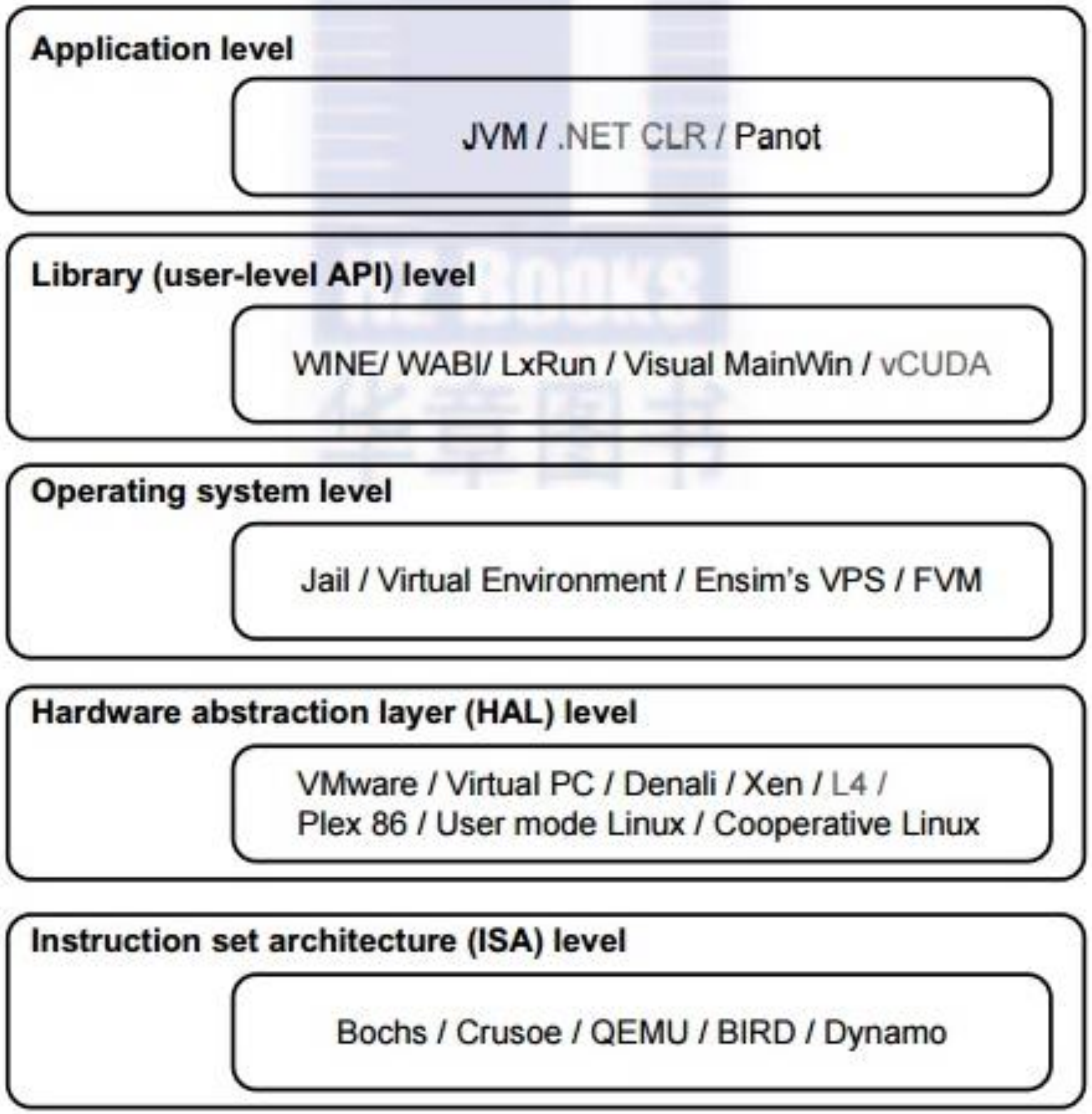
LEVELS OF VIRTUALIZATION IMPLEMENTATION

LEVELS OF VIRTUALIZATION IMPLEMENTATION

- 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.
- This is often done by adding additional software, called a virtualization layer.
- This virtualization layer is known as hypervisor or virtual machine monitor.

CONT..

- The main function of the software layer for virtualization is to virtualize the physical hardware of a host machine into virtual resources to be used by the VMs, exclusively.
- This can be implemented at various operational levels.
- The virtualization software creates the abstraction of VMs by interposing a virtualization layer at various levels of a computer system.
- Common virtualization layers include the
  - Instruction set architecture (ISA) level
  - Hardware abstraction level (HAL)
  - Operating system level
  - Library support level
  - Application level


Application level
JVM / .NET CLR / Panot
Library (user-level API) level
WINE/ WABI/ LxRun / Visual MainWin / vCUDA
Operating system level
Jail / Virtual Environment / Ensim's VPS / FVM
Hardware abstraction layer (HAL) level
VMware / Virtual PC / Denali / Xen / L4 /
Plex 86 / User mode Linux / Cooperative Linux
Instruction set architecture (ISA) level
Bochs / Crusoe / QEMU / BIRD / Dynamo

ISA LEVEL (1/2)

- At the ISA level, virtualization is performed by emulating a given ISA by the ISA of the host machine.
- For example, MIPS (Million Instructions Per Second) binary code can run on an x86-based host machine with the help of ISA emulation.
- With this approach, it is possible to run a large amount of binary code written for various processors on any given new hardware host machine.
- Instruction set emulation leads to virtual ISAs created on any hardware machine.

ISA LEVEL (2/2)

- Instruction Set Architecture (ISA) defines the instruction set for the processor, registers, memory, and interrupt management.
- It is an interface between software and hardware
- It is mandatory for the operating system (OS) developer (system ISA) developers of applications who directly manages core hardware (user ISA).
- The operating system layer is separated by the application binary interface (ABI) from the application and libraries, which are managed by operating system.

HARDWARE ABSTRACTION LEVEL

- Hardware-level virtualization is performed right on top of the bare hardware.
- On the one hand, this approach generates a virtual hardware environment for a VM.
- On the other hand, the process manages the underlying hardware through virtualization.
- The idea is to virtualize a computer's resources, such as its processors, memory, and I/O devices.
- The intention is to upgrade the hardware utilization rate by multiple users concurrently.
- The idea was implemented in the IBM VM/370 in the 1960s. More recently, the Xen hypervisor has been applied to virtualize x86-based machines to run Linux or other guest OS applications.

OPERATING SYSTEM LEVEL

- This refers to an abstraction layer between traditional OS and user applications.
- OS-level virtualization creates isolated containers on a single physical server and the OS instances to utilize the hardware and software in data centers.
- The containers behave like real servers. OS-level virtualization is commonly used in creating virtual hosting environments to allocate hardware resources among a large number of mutually distrusting users.
- It is also used, to a lesser extent, in consolidating server hardware by moving services on separate hosts into containers or VMs on one server.

LIBRARY SUPPORT LEVEL

- Most applications use APIs exported by user-level libraries rather than using lengthy system calls by the OS.
- Since most systems provide well documented APIs, such an interface becomes another candidate for virtualization.
- Virtualization with library interfaces is possible by controlling the communication link between applications and the rest of a system through API hooks.
- The software tool WINE has implemented this approach to support Windows applications on top of UNIX hosts.
- Another example is the vCUDA which allows applications executing within VMs to leverage GPU hardware acceleration.

USER-APPLICATION LEVEL

- Virtualization at the application level virtualizes an application as a VM.
- On a traditional OS, an application often runs as a process.
- Therefore, application-level virtualization is also known as process-level virtualization. The most popular approach is to deploy high level language (HLL)
- VMs. In this scenario, the virtualization layer sits as an application program on top of the operating system, and the layer exports an abstraction of a VM that can run programs written and compiled to a particular abstract machine definition.
- Any program written in the HLL and compiled for this VM will be able to run on it.
- The Microsoft .NET CLR and Java Virtual Machine (JVM) are two good examples of this class of VM.

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 (1/2)

- Hardware-level virtualization inserts a layer between real hardware and traditional operating systems.
- This layer is commonly called the Virtual Machine Monitor (VMM) and it manages the hardware resources of a computing system.
- Each time programs access the hardware the VMM captures the process. In this sense, the VMM acts as a traditional OS.
- One hardware component, such as the CPU, can be virtualized as several virtual copies.
- Therefore, several traditional operating systems which are the same or different can sit on the same set of hardware simultaneously.

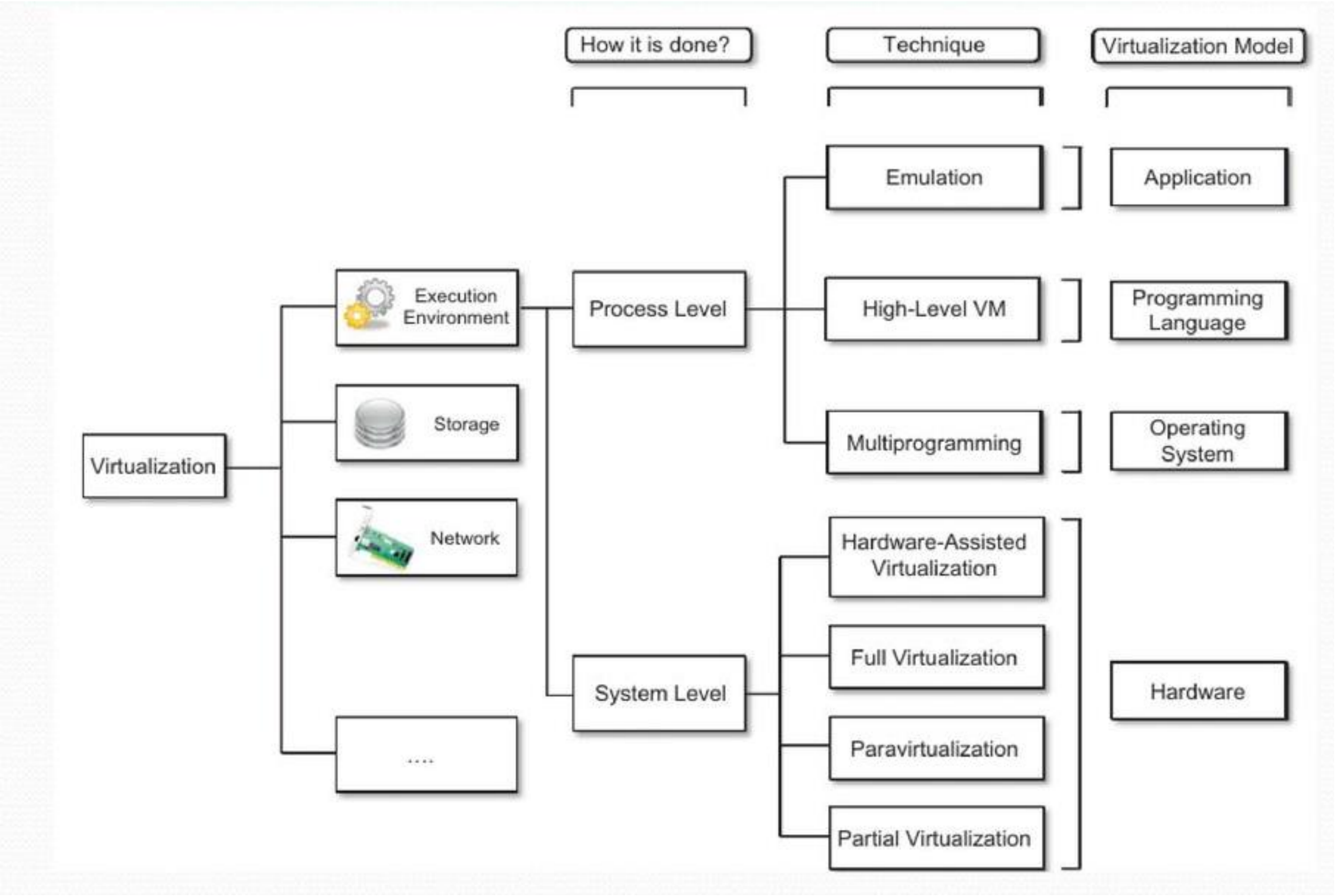
VMM DESIGN REQUIREMENTS (2/2)

- There are three requirements for a VMM.
  - A VMM should provide an environment for programs which is essentially identical to the original machine.
  - Programs run in this environment should show, at worst, only minor decreases in speed.
  - A VMM should be in complete control of the system resources. Any program run under a VMM should exhibit a function identical to that which it runs on the original machine directly.
- Two possible exceptions in terms of differences are permitted with this requirement:
  - Differences caused by the availability of system resources
  - Differences caused by timing dependencies.
- The differences arises when more than one VM is running on the same machine.

TAXONOMY OF VIRTUALIZATION TECHNIQUES

- Virtualization is mainly used to emulate execution environment , storage and networks.
- Execution Environment classified into two :-
  - Process-level – implemented on top of an existing operating system.
  - System-level – implemented directly on hardware and do not or minimum requirement of existing operating system

TAXONOMY OF VIRTUALIZATION TECHNIQUES

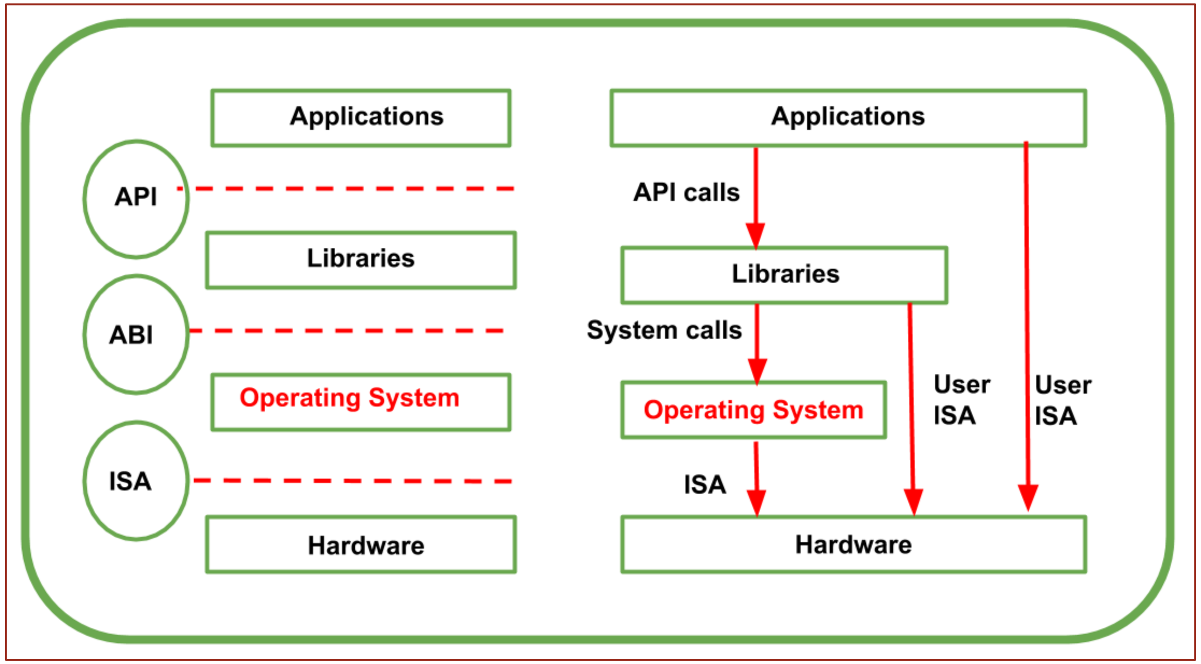


MACHINE REFERENCE MODEL

- It defines the interfaces between the levels of abstractions, which hide implementation details.
- Virtualization techniques actually replace one of the layers and intercept the calls that are directed towards it.

MACHINE REFERENCE MODEL

- Hardware is expressed in terms of the Instruction Set Architecture (ISA).
  - ISA for processor, registers, memory and the interrupt management.
- Application Binary Interface (ABI) separates the OS layer from the application and libraries which are managed by the OS.
  - System Calls defined
  - Allows portabilities of applications and libraries across OS.



MACHINE REFERENCE MODEL

- API – it interfaces applications to libraries and/or the underlying OS.
- Layered approach simplifies the development and implementation of computing system.
- ISA has been divided into two security classes:-
  - Privileged Instructions
  - Nonprivileged Instructions

APPLICATION BINARY INTERFACE (ABI)

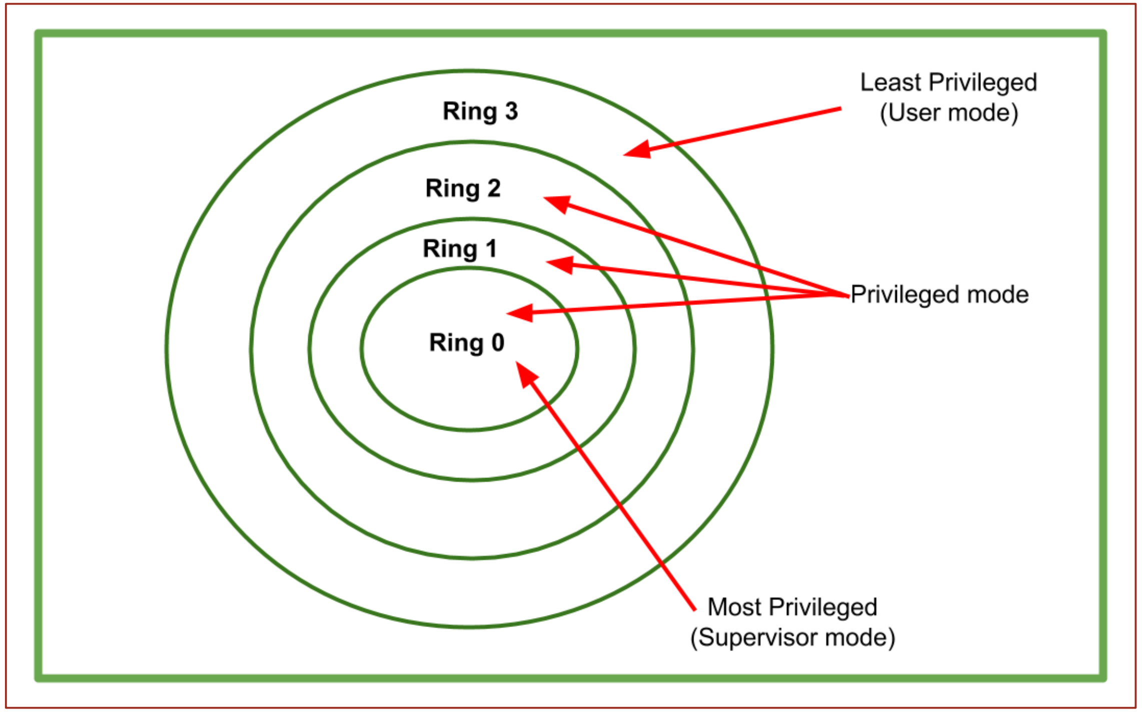
- Application Binary Interface (ABI) covers facts such as low-level data types and call conventions
- It also defines a format for many programs. Mainly, system calls are defined at this level.
- Moreover, this type of interface enables portability of various applications and libraries across OS which employ the same ABI. Application programming interface (API) is represented by the highest level of abstraction. This API interfaces applications to libraries and/or the core OS.

ISA: SECURITY CLASSES

- Nonprivileged instructions
  - That can be used without interfering with other tasks because they do not access shared resources. Ex. Arithmetic , floating & fixed point.
- Privileged instructions
  - That are executed under specific restrictions and are mostly used for sensitive operations, which expose (behavior-sensitive) or modify (control-sensitive) the privileged state.
    - Behavior-sensitive – operate on the I/O
    - Control-sensitive – alter the state of the CPU register.

ISA: SECURITY CLASSES

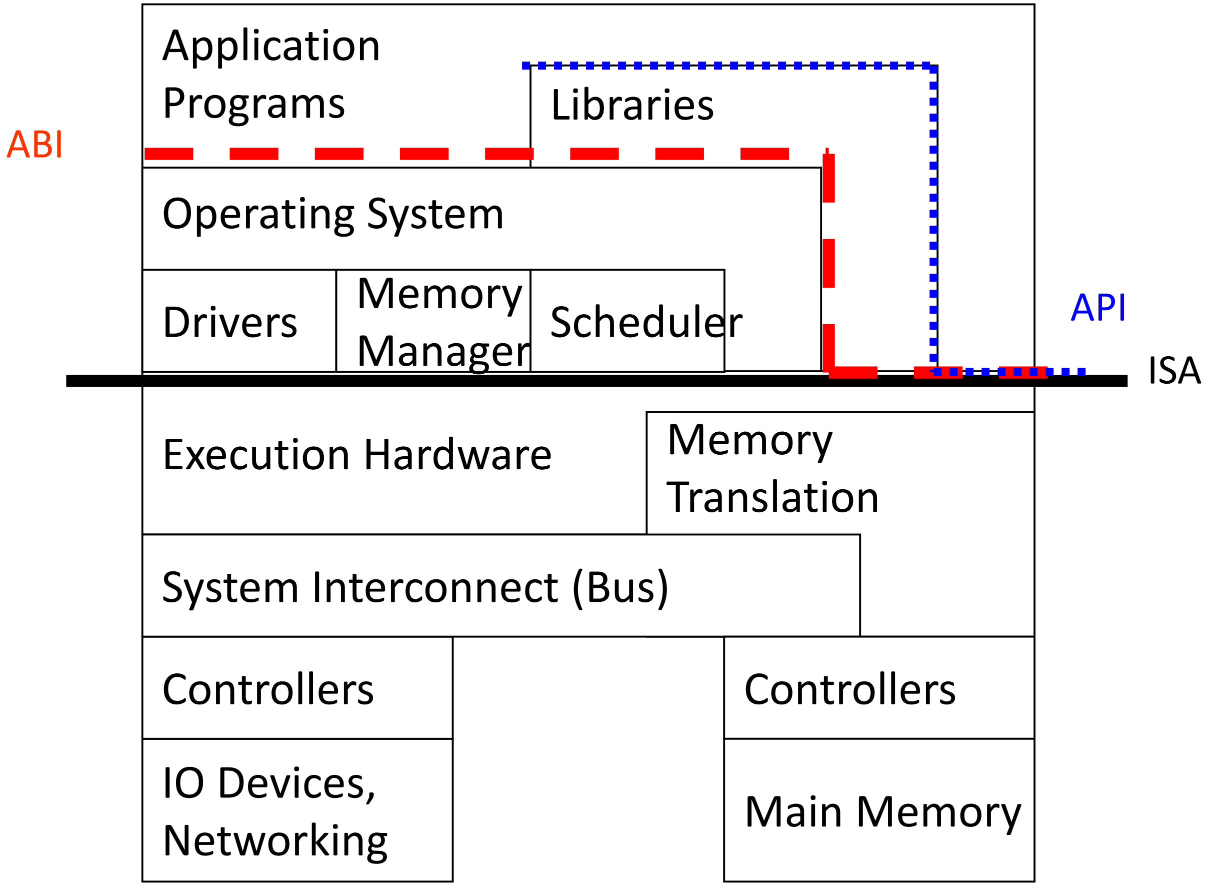
- Privileged Hierarchy: Security Ring
- Ring-0 is in most privileged level , used by the kernel.
- Ring-1 & 2 used by the OS-level services
- R3 in the least privileged level , used by the user.
- Recent system support two levels :-
  - Ring 0 – supervisor mode*
  - Ring 3 – user mode



*Supervisor mode is "an execution mode on some processors which enables execution of all instructions, including privileged instructions.

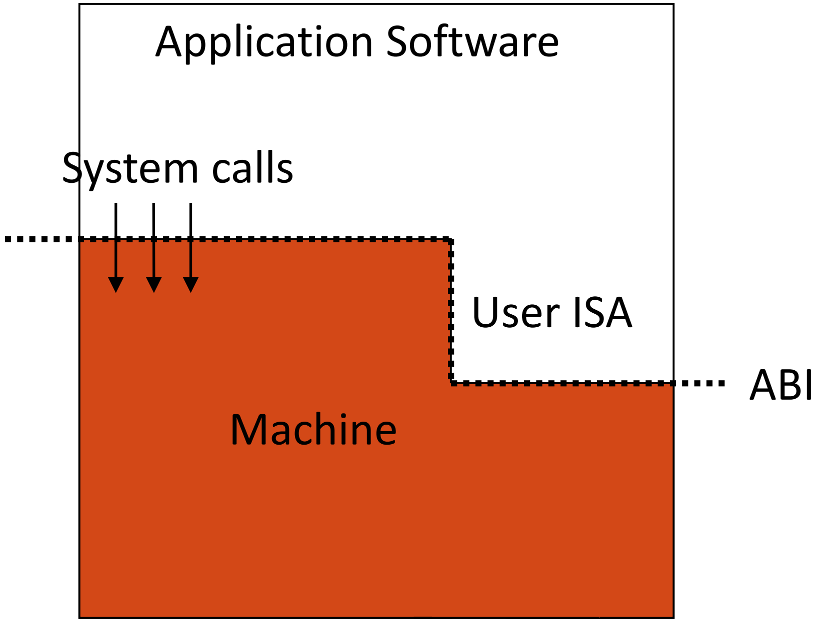
ABSTRACTION LEVEL

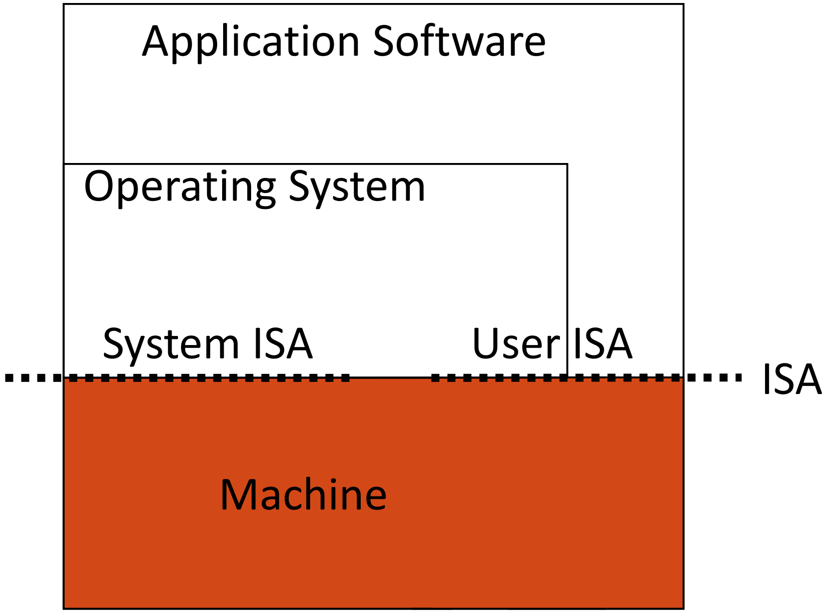
- Instruction Set Architecture (ISA)
  - Divides hardware and software
- Application Binary Interface (ABI)
  - Provides a program with access to the hardware resource and services available in a system
- Application Programming Interface (API)
  - Key element is Standard Library (or Libraries)
  - Typically defined at the source code level of High Level Language



VIRTUAL MACHINE

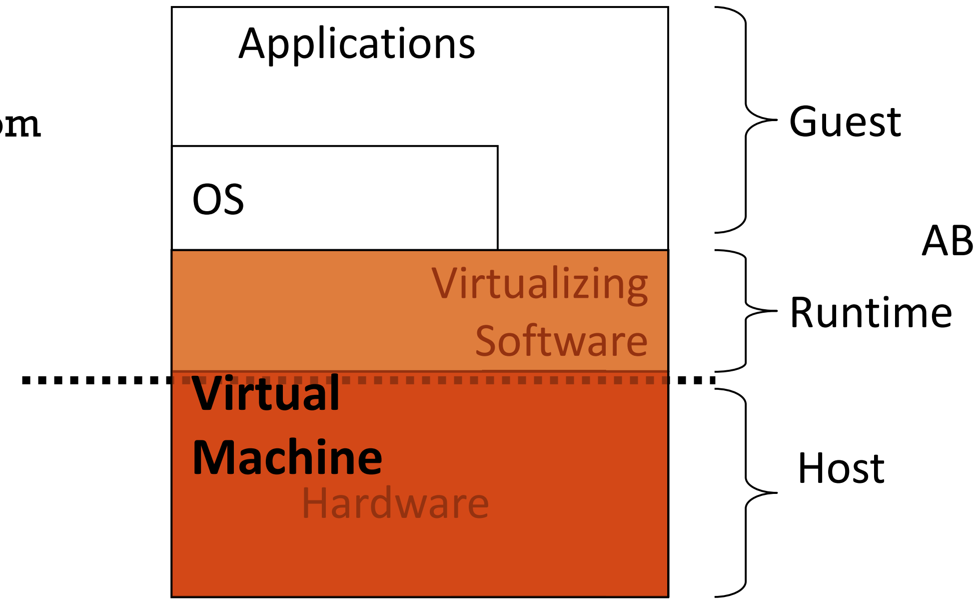
- VM has 2 perspectives :
  - Machine from the perspective of a process
    - ABI provides interface between process and machine
  - Machine from the perspective of a system
    - ISA provides interface between system and machine

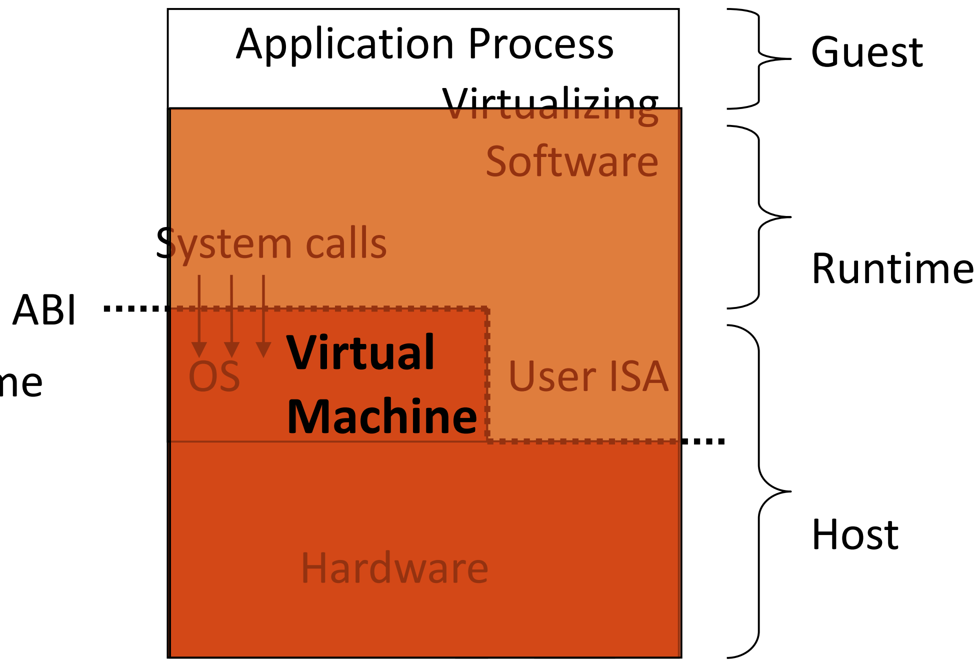




VIRTUAL MACHINE

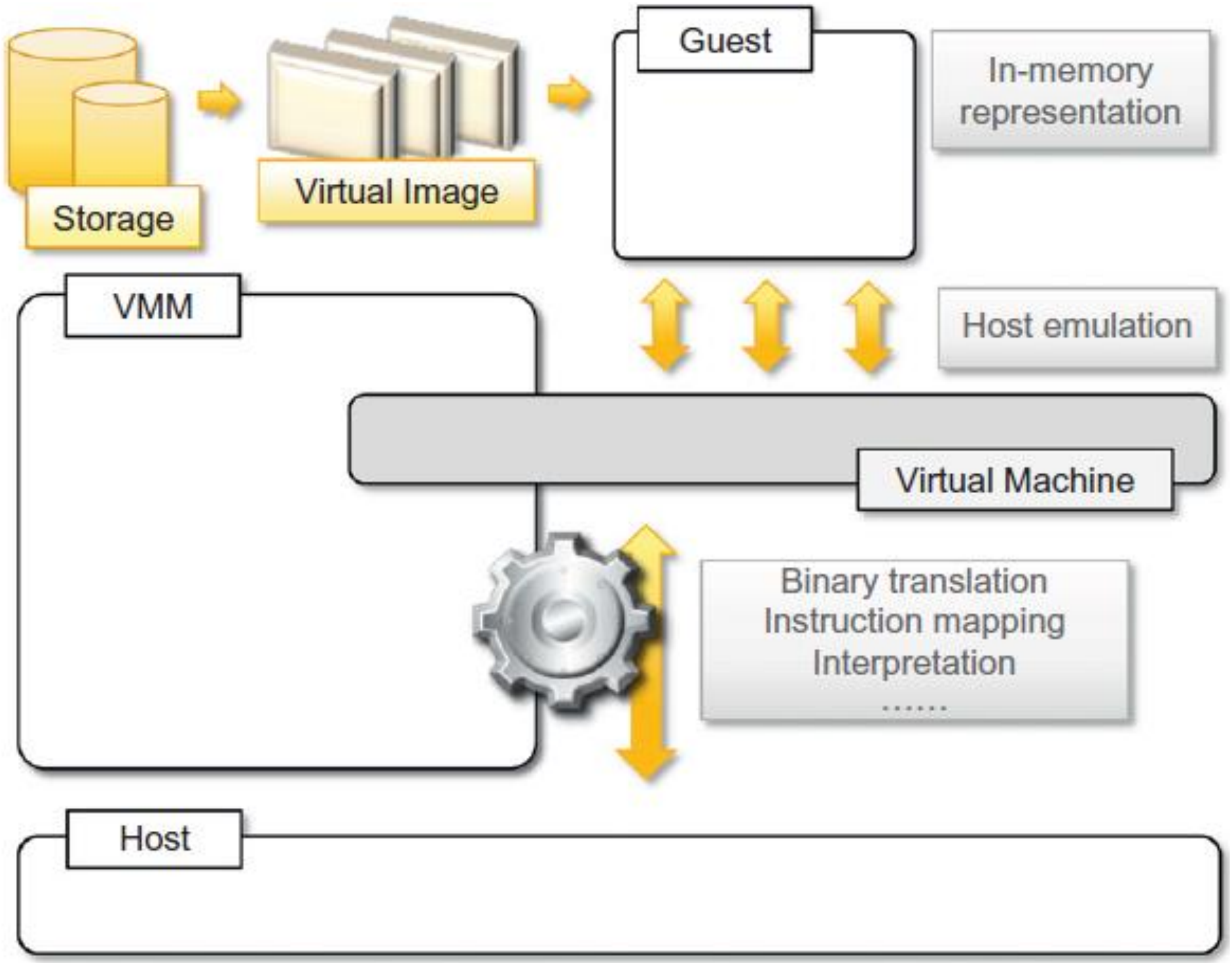
- 2 types of VM
  - Process-level VM
    - VM is just a process from the view of host OS
    - Application on the VM cannot see the host OS
  - System VM
    - Provides a system environment





HARDWARE-LEVEL VIRTUALIZATION

- It is a virtualization technique that provides an abstract execution environment in terms of computer hardware on top of which a guest OS can be run.
- It is also called as system virtualization.
- It recreates a h/w environment.
- It is a piece of s/w that enables us to run one or more VMs on a physical server(host).
- Two major types of hypervisor
  - Type -I
  - Type-II

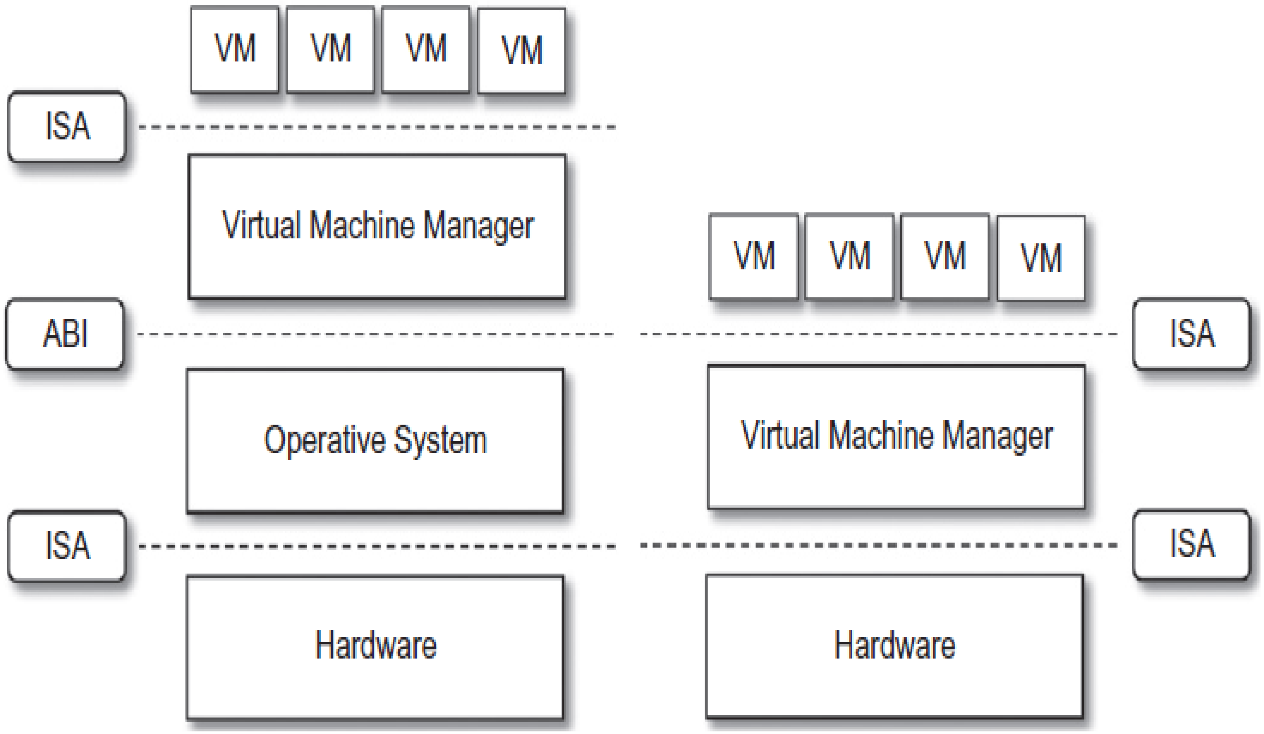


Storage
Virtual Image
Guest
In-memory representation
VMM
Host emulation
Virtual Machine
Binary translation
Instruction mapping
Interpretation
……
Host

HOSTED & NATIVE VIRTUAL MACHINE

- **Type-1, native or bare-metal VM**
  - These VMs run directly on the host's hardware to control the hardware and to manage guest operating systems.
  - For this reason, they are sometimes called bare metal VMs.
  - The first hypervisors, which IBM developed in the 1960s, were native hypervisors.
- **Type-2 or hosted VM**
  - These VMs run on a conventional operating system (OS) just as other computer programs do.
  - A guest operating system runs as a process on the host.
  - Type-2 hypervisors abstract guest operating systems from the host operating system.
  - Parallels Desktop for Mac, QEMU, VirtualBox, VMware Player and VMware Workstation are examples of type-2 hypervisors.

HOSTED & NATIVE VIRTUAL MACHINE



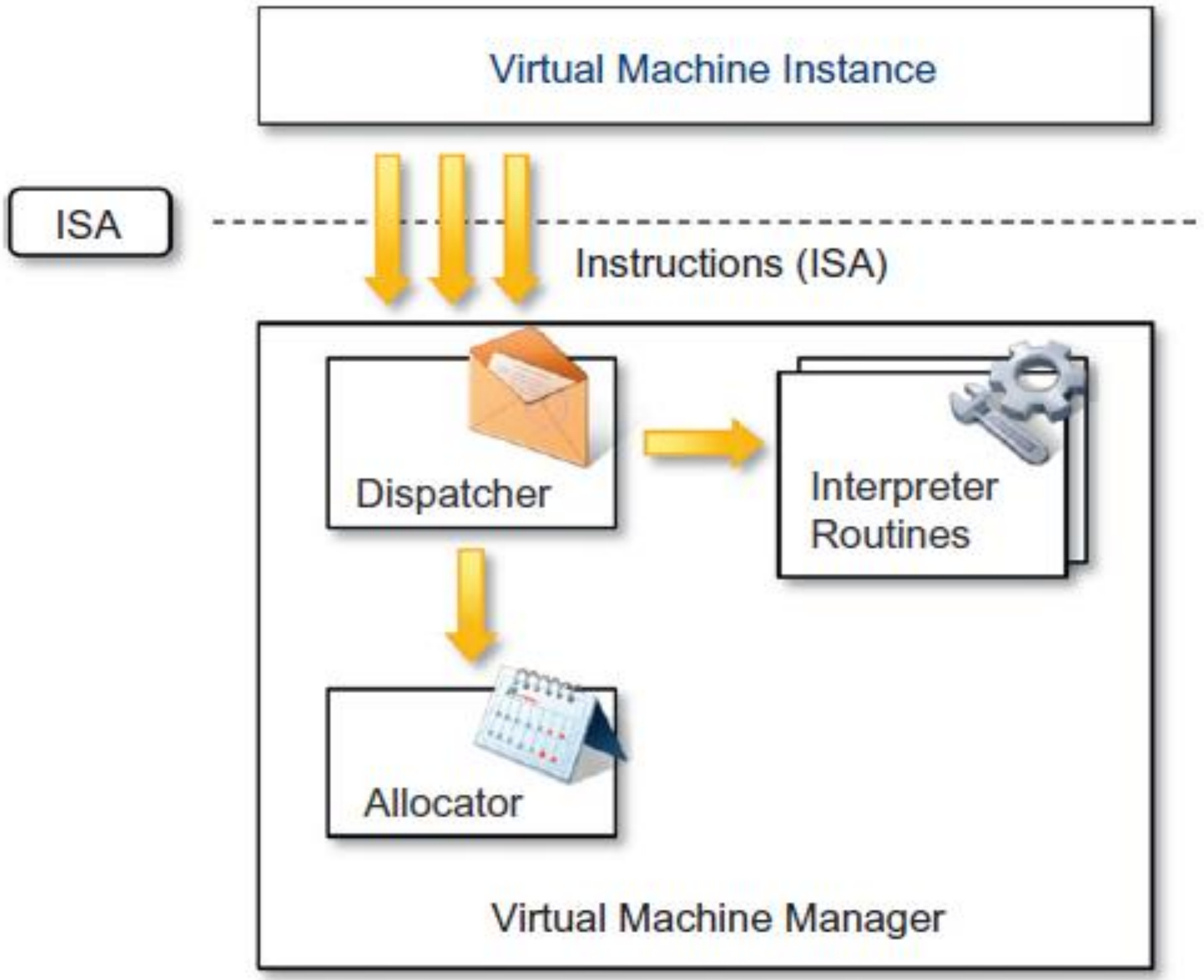
Hosted Virtual Machine
TYPE - II

Native Virtual Machine
TYPE -I

HYPERVISOR REFERENCE ARCHITECTURE

Main Modules

- Dispatcher
  - Entry Point of VMM
  - Reroutes the instructions issued by VM instance.
- Allocator
  - Deciding the system resources to be provided to the VM.
  - Invoked by dispatcher
- Interpreter
  - Consists of interpreter routines
  - Executed whenever a VM executes a privileged instruction.


Virtual Machine Instance
ISA
Instructions (ISA)
Dispatcher
Interpreter
Routines
Allocator
Virtual Machine Manager

CRITERIA OF VMM

- Equivalence
  - Same behavior as when it is executed directly on the physical host.
- Resource control
  - It should be in complete control of virtualized resources.
- Efficiency
  - A statistically dominant fraction of the machine instructions should be executed without intervention from the VMM

THEOREMS

- Popek and Goldberg provided a classification of the instruction set and proposed three theorems that define the properties that hardware instructions need to satisfy in order to efficiently support virtualization.
- Classification of IS
  - Privileged Instructions
  - Control sensitive Instructions
  - Behavior sensitive Instructions

THEOREMS

- Theorem 1
  - For any conventional third-generation computer, a VMM may be constructed if the set of sensitive instructions for that computer is a subset of the set of privileged instructions.
- Theorem 2
  - A conventional third-generation computers is recursively virtualizable if:
    - It is virtualizable and
    - A VMM without any timing dependencies can be constructed for it.
- Theorem 3
  - A hybrid VMM may be constructed third- generation machine in which the set of user-sensitive instructions is a subset of the set of privileged instructions*.
  - In HVM, more instructions are interpreted rather than being executed directly.

*A machine code instruction that may only be executed when the processor is running in supervisor mode**.

HARDWARE VIRTUALIZATION TECHNIQUES

- CPU installed on the host is only one set, but each VM that runs on the host requires their own CPU.
- It means CPU needs to virtualized, done by hypervisor.
- Four Types
  - Full virtualization
  - Para-virtualization
  - Hardware-assisted virtualization
  - Partial virtualization

FULL VIRTUALIZATION

- Full Virtualization provides a complete simulation of the underlying hardware allowing execution of unmodified operating systems in the virtual machines.
- It requires that every salient feature of the hardware be reflected into every one of several virtual machines.
- In Full Virtualization machine language code of the guest OS is converted into the machine language code of the host through a binary translation process.
- It causes the hypervisor to "trap*" the machine operations, the OS uses to read or modify the system's status or perform input/output (I/O) operations.
- After it has trapped them, the hypervisor emulates these operations in software and returns status codes consistent with what the real hardware would deliver.
- The guest operating system is unaware that it is in a virtualized environment

*trap, also known as an exception or a fault, is typically a type of synchronous interrupt caused by an exceptional condition

FULL VIRTUALIZATION

- Ability to run program (OS) directly on top of a virtual machine and without any modification.
- VMM require complete emulation of the entire underneath h/w
- Advantages
  - Complete isolation
  - Enhanced security
  - This approach operates invisibly from the perspective of the guest OS.
  - It requires no changes to the guest OS or the applications running under that guest.
- Ease of emulation of different architectures and coexistence
- Key challenge is interception of privileged instructions

FULL VIRTUALIZATION

- Full Virtualization Hypervisor has Ring 0 authority and , guest OS has Ring 1 authority
- ISA of guest OS are converted into ISA of host using binary translation process.
- Privileged instructions are traped.

PARAVIRTUALIZATION

- Paravirtualization is a type of virtualization in which a guest operating system (OS) is recompiled, installed inside a virtual machine (VM), and operated on top of a hypervisor program running on the host OS.
- Eliminates much of the trapping-and-emulation overhead associated with software implemented virtualization by requiring that the guest OS cooperates in creating the virtualizing illusion.
- Guest operating system (the one being virtualized) is aware that it is a guest and accordingly issue commands directly to the host operating system
- Adv :- Fast
- Disadv:- It requires the use of a specially modified guest OS

PARAVIRTUALIZATION

- Not-transparent virtualization
- Expose software interface to the virtual machine that is slightly modified from the host.
- Guest OS need to be modified.
- Simply transfer the execution of instructions which were hard to virtualized, directly to the host.
- Privileged instructions of guest OS is delivered to the hypervisor by using hypercalls*
- Hypercalls handles these instructions and accesses the h/w and return the result.
- Guest has authority to directly control of resources.

*A hypercall is a software trap from a domain to the hypervisor, just as a syscall is a software trap from an application to the kernel.

HARDWARE-ASSISTED VIRTUALIZATION

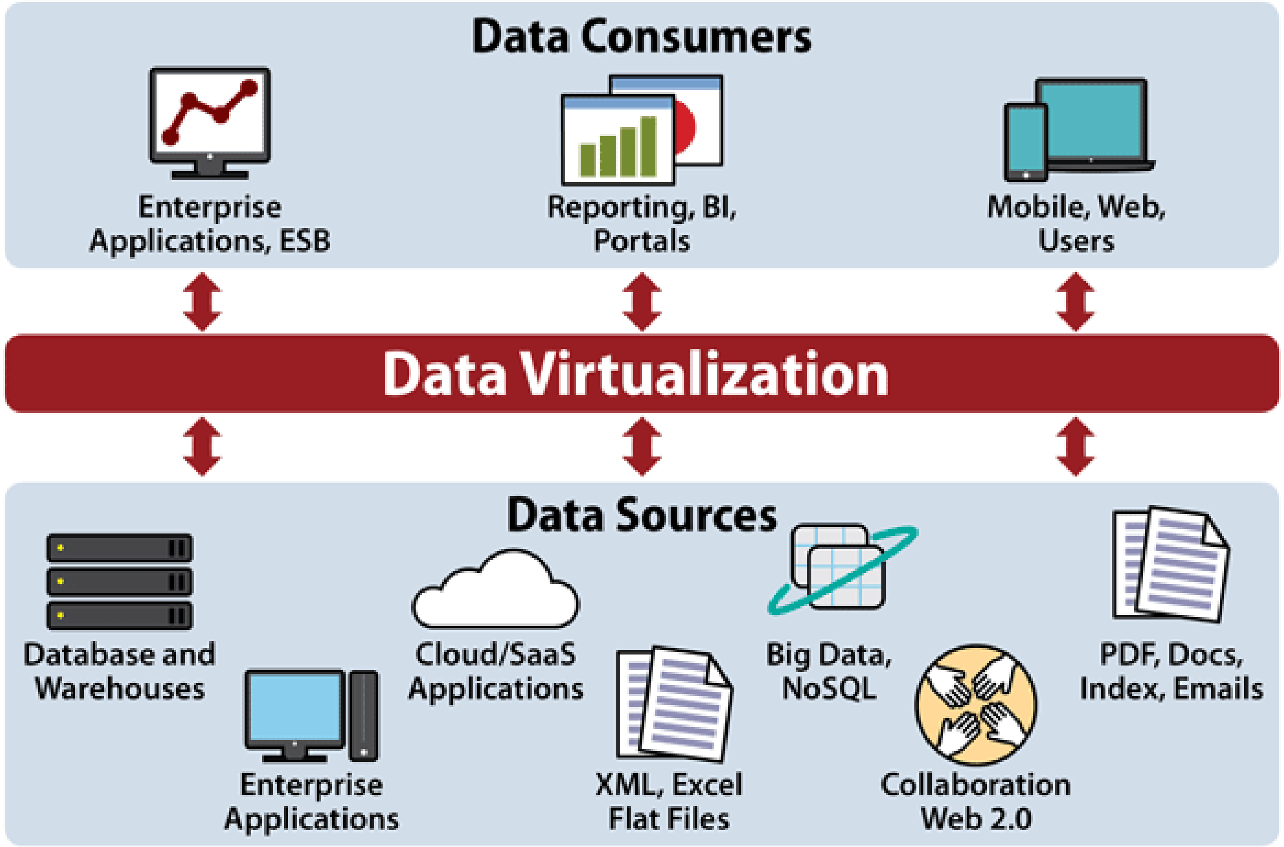
- Hardware-assisted virtualization is the use of a computer's physical components to support the software that creates.
- It relies on hardware extensions to the x86 system architecture to eliminate much of the hypervisor overhead associated with trapping and emulating I/O operations and status instructions executed within a guest OS.
- In this hardware provides architectural support for building a VMM able to run a guest OS in complete isolation.
- Early products were using binary translation to trap some sensitive instructions and provide an emulated version
- Additional Ring -1
- No binary translation of privileged instructions
- Commands are executed directly to h/w via the hypervisor

PARTIAL VIRTUALIZATION

- When entire operating systems cannot run in the virtual machine, but some or many applications can, it is known as Partial Virtualization.
- Basically, it partially simulates the physical hardware of a system.
- This type of virtualization is far easier to execute than full virtualization.
- This is very successful when computer resources are shared among-st multiple users.
- It includes address space virtualization, the virtual machine simulates multiple instances of particularly address spaces.
- Partial emulation of the underlying hardware
- Address space virtualization used in time- sharing system.

DATA VIRTUALIZATION

- Data virtualization is the process of retrieve data from various resources without knowing its type and physical location where it is stored.
- It collects heterogeneous data (structured and unstructured data) from different resources and allows data users across the organization to access this data according to their work requirements.
- This heterogeneous data can be accessed using any application such as web portals, web services, E-commerce, Software as a Service (SaaS), and mobile application.
- Data virtualization integrates data from disparate sources without copying or moving the data, thus giving users a single virtual layer that spans multiple applications, formats, and physical locations.
- Data virtualization is not a data store replicator. Data virtualization does not normally persist or replicate data from source systems. It only stores metadata for the virtual views and integration logic.


Data Consumers
Enterprise Applications, ESB
Reporting, BI, Portals
Mobile, Web, Users
Data Virtualization
Data Sources
Database and Warehouses
Enterprise Applications
Cloud/SaaS Applications
XML, Excel Flat Files
Big Data, NoSQL
Collaboration Web 2.0
PDF, Docs, Index, Emails

DATA VIRTUALIZATION CAPABILITIES

- **Cost savings:** It's cheaper to store and maintain data than it is to replicate and spend resources transforming it to different formats and locations.
- **Logical abstraction and decoupling:** Heterogeneous data sources can now interact more easily through data virtualization.
- **Data governance:** Through central management, data governance challenges can be lessened, and rules can be more easily applied to all of the data from one location.
- **Bridging structured and unstructured:** Data virtualization can bridge the semantic differences of unstructured and structured data, integration is easier and data quality improves across the board.
- **Increased productivity:** Aside from the above-mentioned, bridging of data, virtualization also makes it easier to test and deploy data-driven apps, since less time is needed integrating data sources.

NEVER CONFUSE

- It is not regular virtualization. When the term "virtualization" is used, it typically refers to server hardware virtualization.
- It is not virtualized data storage. Some use the term data virtualization to describe virtualized database software or storage hardware virtualization products, but they are stand-alone data storage products, not a means of spanning data sources.
- It is not data visualization. The two sound similar but visualization is the display of data in charts, graphs, maps, reports, 3D images, and so on.
- It is not a Logical Data Warehouse. LDW is an architectural concept, not a platform. You draw data from a LDW through data virtualization.
- It is not containers. In the contrast between virtualization vs. containers, virtualization is more or an abstract layer, whereas containers are a software-based wrapping for an application and its various supporting components.

DATA VIRTUALIZATION TOOLS

- **DataCurrent:** Places emphasis on data stored in NoSQL repositories, cloud services and application data as well as supporting business intelligence tools to connect to these data sources.
- **Denodo:** Specializing in real-time data, Denodo is known for being easy to learn and use.
- **Oracle Data Service Integrator:** Powerful data integrator that works best with Oracle products.
- **Red Hat JBoss Data Virtualization:** Written in Java, works best with any JDBC interface. ODBC is said to be lacking.
- **SAS Federation Server:** Places great emphasis on securing data.
- **TIBCO Data Virtualization:** Known for connecting to a wide variety of data sources

SOFTWARE VIRTUALIZATION

- Managing applications and distribution becomes a typical task for IT departments.
- Installation mechanism differs from application to application. Some programs require certain helper applications or frameworks and these applications may have conflict with existing applications.
- Software virtualization is just like a virtualization but able to abstract the software installation procedure and create virtual software installations.
- Virtualized software is an application that will be "installed" into its own self-contained unit.
- Example of software virtualization is VMware software, virtual box etc.

ADVANTAGES

- Client Deployments Become Easier:
  - Copying a file to a workstation or linking a file in a network then we can easily install virtual software.
- Easy to manage:
  - To manage updates becomes a simpler task. You need to update at one place and deploy the updated virtual application to the all clients.
- Software Migration:
  - Without software virtualization, moving from one software platform to another platform takes much time for deploying and impact on end user systems.
  - With the help of virtualized software environment the migration becomes easier.

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.

NETWORK VIRTUALIZATION

- Network virtualization works by combining the available resources in a network and splitting up the available bandwidth into channels.
- Each channel is independently secured. Every subscriber has shared access to all the resources on the network from a single computer.
- Network virtualization is intended to improve productivity, efficiency and job satisfaction of the administrator by performing many of these tasks automatically, thereby disguising the true complexity of the network.
- Files, images, programs and folders can be centrally managed from a single physical site.
- Storage media can be easily added or reassigned. Storage space can be shared or reallocated among the servers.

TYPES

- Virtual networks exist in two forms;
- Internal: refers to using network-like functionality in software containers on a single network server. Internal software allows VMs to exchange data on a host without using an external network.
- External: virtualization will use tools such as switches, adapters or a network to combine one or more networks into virtual units.

ADVANTAGES AND DISADVANTAGES

- Advantages:
  - More productive IT environments (i.e., efficient scaling).
  - Improved security and recovery times.
  - Faster in application delivery.
  - More efficient networks.
  - Reduced overall costs.
- Disadvantages:
  - Increased upfront costs (investing in virtualization software).
  - Need to license software.
  - There may be a learning curve if IT managers are not experienced.
  - Not every application and server will work in a virtualized environment.
  - Availability can be an issue if an organization can't connect to their virtualized data.

NEVER CONFUSE

SDN vs. network virtualization

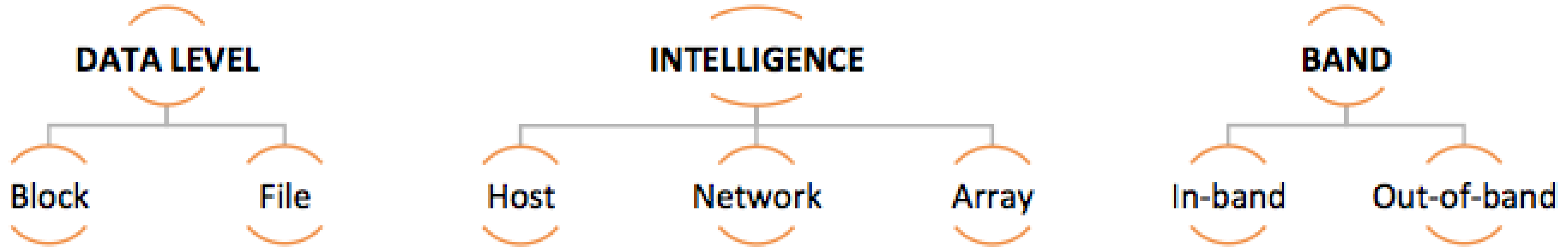
- Network virtualization shares common elements with software-defined networking (SDN) which can create confusion for some.
- For example, both share the goal of improving the network resources to VMs and consolidating or segmenting networks.
- However, SDNs focus on the separation of control and data plane as well as programmability to improve network configurations, performance and monitoring.
- SDNs do this by centralizing a network through separating the forwarding process of network packets from routing processes.

STORAGE VIRTUALIZATION

- Storage virtualization is the technology of abstracting physical data storage resources to make them appear as if they were a centralized resource.
- Virtualization masks the complexities of managing resources in memory, networks, servers and storage.
- Storage virtualization runs on multiple storage devices, making them appear as if they were a single storage pool.
- Pooled storage devices can be from different vendors and networks.
- The storage virtualization engine identifies available storage capacity from multiple arrays and storage media, aggregates it, manages it and presents it to applications.

Storage virtualization can occur in a variety of different scenarios.

Where Storage Virtualization Occurs



**Adapted from SNIA's Taxonomy of Storage Virtualization*

DATA LEVEL: BLOCK OR FILE

- Block-Based
  - Block-based virtualization abstracts the storage system's logical storage from its physical components.
  - Physical components include memory blocks and storage media, while logical components include drive partitions.
- File Level
  - File level virtualization works over Network Attached Storage (NAS) devices to pool and administrate separate NAS appliances.

INTELLIGENCE: HOST, NETWORK, ARRAY

- Host-Based:
  - Virtualizing storage for VM environments and online applications.
  - Some servers provide virtualization from the OS level. The OS virtualizes available storage to optimize capacity and automate tiered storage schedules.
- Network-Based:
  - Storage Area Network (SAN) storage virtualization.
  - Network-based storage virtualization is the most common type for SAN owners, who use it to extend their investment by adding more storage.
- Array-Based
  - Primary use case is Storage tiering.
  - Virtualizing multiple physical disks into a single logical array.
  - Specialized storage controller that intercepts I/O requests from secondary storage controllers and automatically tiers data within connected storage systems.

BAND: IN-BAND, OUT-OF-BAND

- In-Band
  - In-band storage virtualization occurs when the virtualization engine operates between the host and storage.
  - Both I/O requests and data pass through the virtualization layer, which allows the engine to provide advanced functionality like data caching, replication and data migration.
- Out-of-Band
  - Out-of-band storage virtualization splits the path into control (metadata) and data paths.
  - Only the control path runs through the virtualization appliance, which intercepts I/O requests from the host, looks up and maps metadata on physical memory locations, and issues an updated I/O request to storage.
  - Data does not pass through the device, which makes caching impossible.

BENEFITS OF STORAGE VIRTUALIZATION

- Enables dynamic storage utilization and virtual scalability of attached storage resources, both block and file.
- Avoids downtime during data migration. Virtualization operates in the background to maintain data's logical address to preserves access.
- Centralizes a single dashboard to manage multi-vendor storage devices, which saves management overhead and money.
- Protects existing investments by expanding available storage available to a host or SAN.
- Can add storage intelligence like tiering, caching, replication and a centralized management interface in a multi-vendor environment.

SERVER VIRTUALIZATION

- Server virtualization is the process of dividing a physical server into multiple unique and isolated virtual servers by means of a software application.
- Each virtual server can run its own operating systems independently.
- Server virtualization is a cost-effective way to provide web hosting services and effectively utilize existing resources in IT infrastructure.
- Without server virtualization, servers only use a small part of their processing power.
- This results in servers sitting idle because the workload is distributed to only a portion of the network's servers.
- Data centers become overcrowded with underutilized servers, causing a waste of resources and power.

SERVER VIRTUALIZATION

- By having each physical server divided into multiple virtual servers, server virtualization allows each virtual server to act as a unique physical device.
- Each virtual server can run its own applications and operating system.
- This process increases the utilization of resources by making each virtual server act as a physical server and increases the capacity of each physical machine.

TYPES

- Full Virtualization:
  - Full virtualization uses a hypervisor.
  - The hypervisor monitors the physical server's resources and keeps each virtual server independent and unaware of the other virtual servers.
  - It also relays resources from the physical server to the correct virtual server as it runs applications.
- Para-Virtualization:
  - Unlike full virtualization, para-virtualization involves the entire network working together as a cohesive unit.
  - Since each operating system on the virtual servers is aware of one another in para-virtualization, the hypervisor does not need to use as much processing power to manage the operating systems.
- OS-Level Virtualization:
  - OS-level visualization does not use a hypervisor.
  - The virtualization capability, which is part of the physical server operating system, performs all the tasks of a hypervisor.
  - However, all the virtual servers must run that same operating system in this server virtualization method.

BENEFITS

- Higher server ability
- Cheaper operating costs
- Eliminate server complexity
- Increased application performance
- Deploy workload quicker

OPERATING SYSTEM VIRTUALIZATION

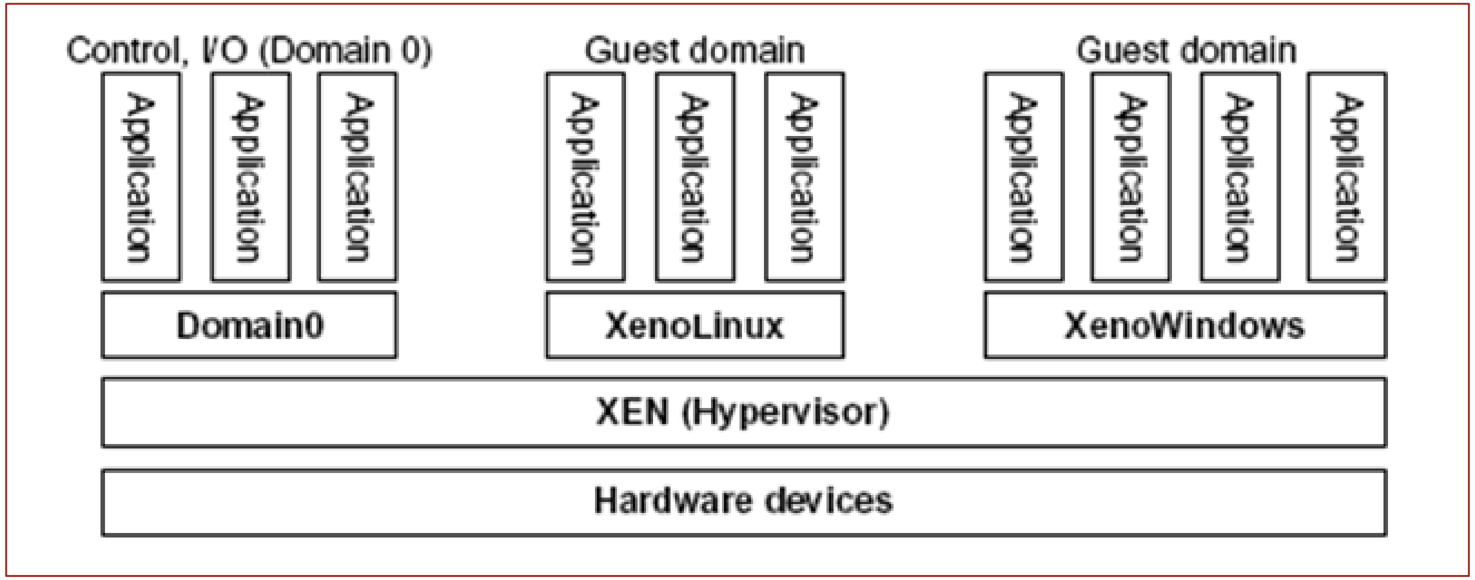
- Operating system Virtualization refers to an operating system feature in which the kernel enables the existence of various isolated user-space instances.
- The installation of virtualization software also refers to Operating system-based virtualization.
- It is installed over a pre-existing operating system and that operating system is called the host operating system.
- In this virtualization, a user installs the virtualization software in the host operating system.
- Here, the virtualization software allows direct access to any of the created virtual machine to the user.
- As the host OS can provide hardware devices with the mandatory support, operating system virtualization may affect compatibility issues of hardware even when the hardware driver is not allocated to the virtualization software.

VIRTUALIZATION STRUCTURES/TOOLS AND MECHANISMS

- Before virtualization, the operating system manages the hardware.
- After virtualization, a virtualization layer is inserted between the hardware and the operating system. In such a case, the virtualization layer is responsible for converting portions of the real hardware into virtual hardware.
- Therefore, different operating systems such as Linux and Windows can run on the same physical machine, simultaneously.
- Depending on the position of the virtualization layer, there are several classes of VM architectures, namely the hypervisor architecture, para-virtualization, and host-based virtualization.
- The hypervisor is also known as the VMM (Virtual Machine Monitor). They both perform the same virtualization operations.

HYPERVISOR: THE XEN ARCHITECTURE

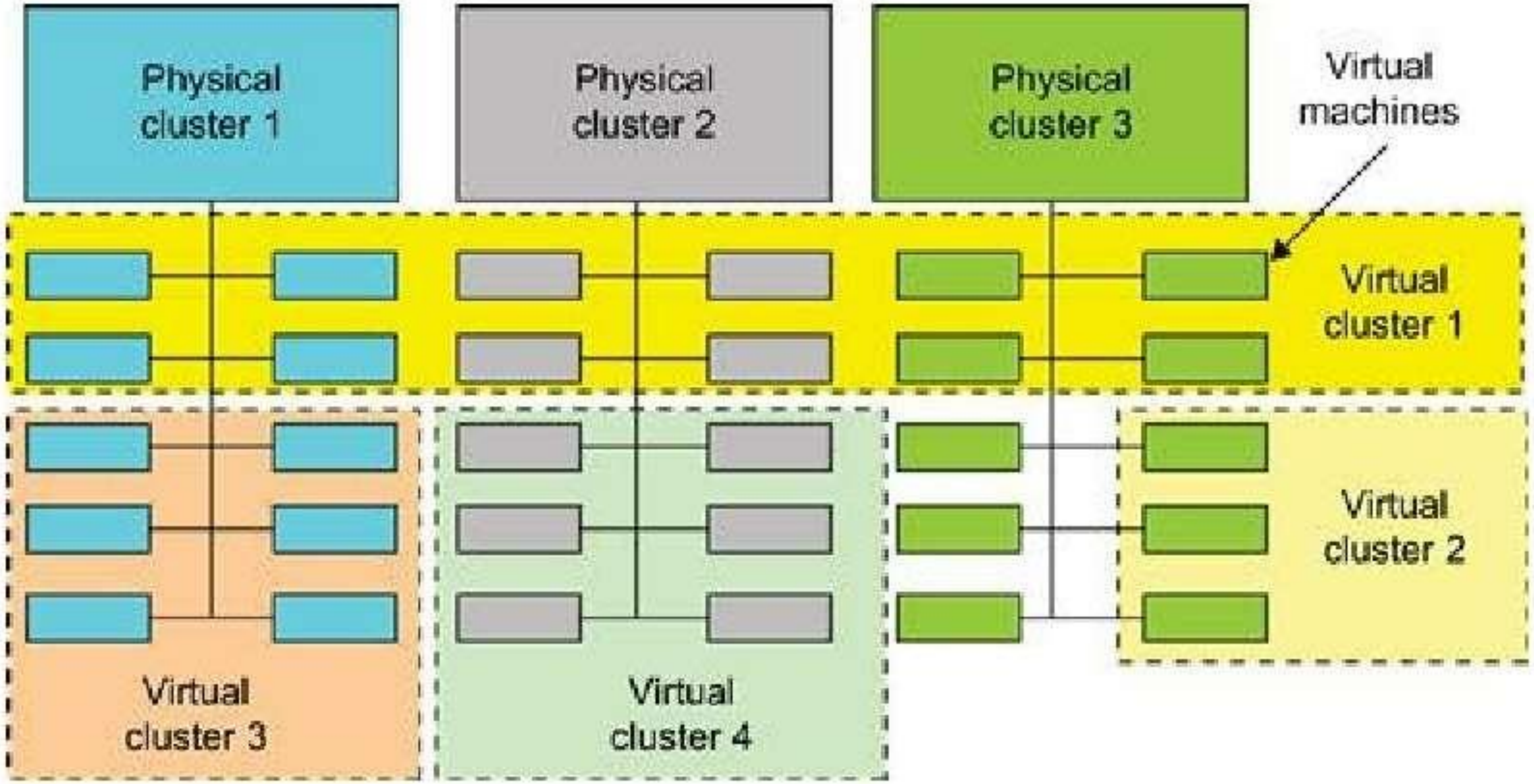
- Xen is an open source hypervisor program developed by Cambridge University. Xen is a micro-kernel hypervisor, which separates the policy from the mechanism.
- Xen does not include any device drivers natively . It just provides a mechanism by which a guest OS can have direct access to the physical devices.
- As a result, the size of the Xen hypervisor is kept rather small.



VIRTUAL CLUSTERS AND RESOURCE MANAGEMENT

- A physical cluster is a collection of servers (physical machines) interconnected by a physical network such as a LAN
- Virtual clusters are built with VMs installed at distributed servers from one or more physical clusters.
- The VMs in a virtual cluster are interconnected logically by a virtual network across several physical networks.
- Each virtual cluster is formed with physical machines or a VM hosted by multiple physical clusters.
- The virtual cluster boundaries are shown as distinct boundaries.

VIRTUAL CLUSTERS AND RESOURCE MANAGEMENT



VIRTUAL CLUSTERS AND RESOURCE MANAGEMENT

- The provisioning of VMs to a virtual cluster is done dynamically to have the following interesting properties:
- The virtual cluster nodes can be either physical or virtual machines. Multiple VMs running with different OSes can be deployed on the same physical node.
- A VM runs with a guest OS, which is often different from the host OS, that manages the resources in the physical machine, where the VM is implemented
- The purpose of using VMs is to consolidate multiple functionalities on the same server. This will greatly enhance server utilization and application flexibility
- VMs can be colonized (replicated) in multiple servers for the purpose of promoting distributed parallelism, fault tolerance, and disaster recovery.
- The size (number of nodes) of a virtual cluster can grow or shrink dynamically, similar to the way an overlay network varies in size in a peer-to-peer (P2P) network.
- The failure of any physical nodes may disable some VMs installed on the falling nodes. But the failure of VMs will not pull down

VIRTUALIZATION FOR DATA-CENTER AUTOMATION

- Data-center automation means that huge volumes of hardware, software, and database resources in these data centers can be allocated dynamically to millions of Internet users simultaneously, with guaranteed OS and cost-effectiveness.
- Google, Yahoo!, Amazon, Microsoft, HP, Apple, and IBM companies have invested billions of dollars in data-center construction and automation.

SERVER CONSOLIDATION IN DATACENTERS

- In data centers, a large number of heterogeneous workloads can run on servers at various times. These heterogeneous workloads can be roughly divided into two categories:
  - Chay workloads and
  - Noninteractive workloads.
- Chay workloads may burst at some point and return to a silent state at some other point. A online movie service is an example of this, whereby a lot of people use it at weekend and few people use it during the weekday.
- Noninteractive workloads do not require people's efforts to make progress after they are submitted. High-performance computing is a typical example of this. At various stages, the requirements for resources of these workloads are dramatically different.

SERVER CONSOLIDATION IN DATA CENTERS

- It is common that most servers in data centers are underutilized. A large amount of hardware, space, power, and management cost of these servers is wasted.
- Server consolidation is an approach to improve the low utility ratio of hardware resources by reducing the number of physical servers.
- Among several server consolidation techniques such as centralized and physical Consolidation, virtualization-based server consolidation is the most powerful.
- Consolidation enhances hardware utilization. Many underutilized servers are consolidated into fewer servers to enhance resource utilization. Consolidation also facilitates backup services and disaster recovery.
- This approach enables more agile provisioning and deployment of resources. In a virtual environment, the images of the guest OSes and their applications are readily cloned and reused.
- The total cost of ownership is reduced. I n this sense, server virtualization causes deferred purchases of new servers, a smaller data-center footprint, lower maintenance costs, and lower power, cooling, and cabling requirements.
- This approach improves availability and business continuity. The crash of a guest OS has no effect on the host OS or any other guest OS. It becomes easier to transfers a VM from one server to another, because virtual servers are unaware of the underlying hardware.

VIRTUAL STORAGE MANAGEMENT

- In system virtualization, virtual storage includes the storage managed by VMMs and guest OSes. Generally, the data stored in this environment can be classified into two categories:
  - VM images and
  - Application data.
- The VM images are special to the virtual environment,
- The application data includes all other data which is the same as the data in traditional OS environments.
- The most important aspects of system virtualization are encapsulation and isolation.
- Traditional operating systems and applications running on them can be encapsulated in VMs. Only one operating system runs in a virtualization while many applications run in the operating system. System virtualization allows multiple VMs to run on a physical machine and the VMs are completely isolated.

VIRTUAL STORAGE MANAGEMENT

- To achieve encapsulation and isolation both the system software and the hardware platform, such as CPUs and chipsets, are rapidly updated. However, storage is lagging. The storage systems become the main bottleneck of VM deployment.
- Parallax is a distributed storage system customized for virtualization environments.
- Contet Addressable Storage (CAS) is a solution to reduce the total size of VM images, and therefore supports a large set of VM based systems in data centers.

CLOUD OS FOR VIRTUALIZED DATA CENTRES

- Data centers must be virtualized to serve as cloud providers.
- The table summarizes four virtual infrastructure (VI) managers and OSes.
- These VI managers and OSes are specially tailored for virtualizing data centers which own a large number of servers in clusters.
- Nimbus, Eucalyptus, and Open Nebula are all open source software available to the general public. Only vSphere 4 is a proprietary OS for cloud resource virtualization and

Table 3.6 VI Managers and Operating Systems for Virtualizing Data Centers [9]

Manager/ OS, Platforms, License	Resources Being Virtualized, Web Link	Client API, Language	Hypervisors Used	Public Cloud Interface	Special Features
Nimbus Linux, Apache v2	VM creation, virtual cluster, www .nimbusproject.org/	EC2 WS, WSRF, CLI	Xen, KVM	EC2	Virtual networks
Eucalyptus Linux, BSD	Virtual networking (Example 3.12 and [41]), www .eucalyptus.com/	EC2 WS, CLI	Xen, KVM	EC2	Virtual networks
OpenNebula Linux, Apache v2	Management of VM, host, virtual network, and scheduling tools, www.opennebula.org/	XML-RPC, CLI, Java	Xen, KVM	EC2, Elastic Host	Virtual networks, dynamic provisioning
vSphere 4 Linux, Windows, proprietary	Virtualizing OS for data centers (Example 3.13), www .vmware.com/ products/vsphere/ [66]	CLI, GUI, Portal, WS	VMware ESX, ESXi	VMware vCloud partners	Data protection, vStorage, VMFS, DRM, HA

TRUST MANAGEMENT IN VIRTUALIZED DATA CENTERS

- A VMM changes the computer architecture. It provides a layer of software between the operating systems and system hardware to create one or more VMs on a single physical platform.
- VMM can provide secure isolation and a VM accesses hardware resources through the control of the VMM, so the VMM is the base of the security of a virtual system. Normally, one VM is taken as a management VM to have some privileges such as creating, suspending, resuming, or deleting a VM.
- Once a hacker successfully enters the VMM or management VM, the whole system is in danger.

VM-BASED INTRUSION DETECTION

- Intrusion detection is used to recognize the unauthorized access.
- An intrusion detection system (IDS) is built on operating systems, and is based on the characteristics of intrusion actions.
- A typical I DS can be classified as a host-based IDS (HIDS) or a network based IDS (NIDS), depending on the data source.
- A HI DS can be implemented on the monitored system. When the monitored system is haacked by hackers, the HI DS also faces the risk of being hacked. A NIDS is based on the flow of network traffic which can’t detect fake actions.
- Virtualization-based intrusion detection can isolate guest VMs on the same hardware platform. Even some VMs can be invaded successfully; they never influence other VMs

CASE STUDY

As computing needs continued to grow, an online financial service company faced a problem that is too common in today's data centers. The company was running out of the space to house physical servers, and existing cooling infrastructure couldn't keep up. New workloads meant additional physical systems, and valuable time was spent configuring those systems and balancing power distribution. But the company didn't found any solution. Suggest a solution to resolve the problem for the financial service company

Questions……?