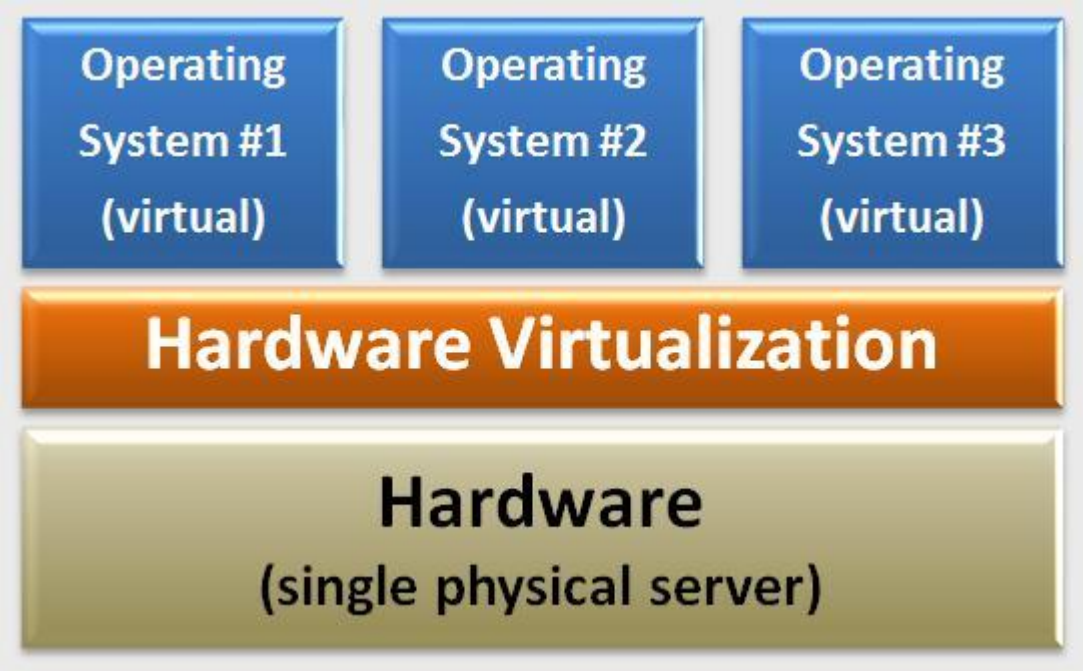
Chapter 4 Virtualization

1. INTRODUCTION

Introduction

- Virtualization is a large umbrella of technologies and concepts that are meant to provide an abstract environment.



Introduction

- Virtualization levels:
  - Hardware level
  - OS level
  - Programming language level
  - Application level

Introduction

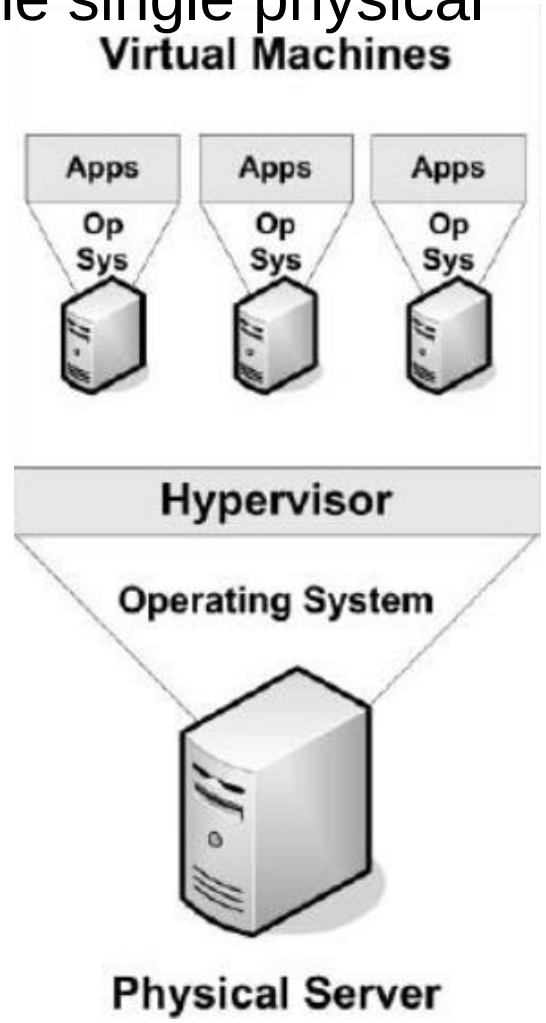
- Types of Virtualization:
  - Server virtualization
  - Application virtualization
  - Network virtualization
  - Storage virtualization
  - Desktop virtualization

Introduction

- Server virtualization:
  - It allows many servers to run on the single physical server.

Advantages:

1. Decreased energy usage.
2 . More floor space.

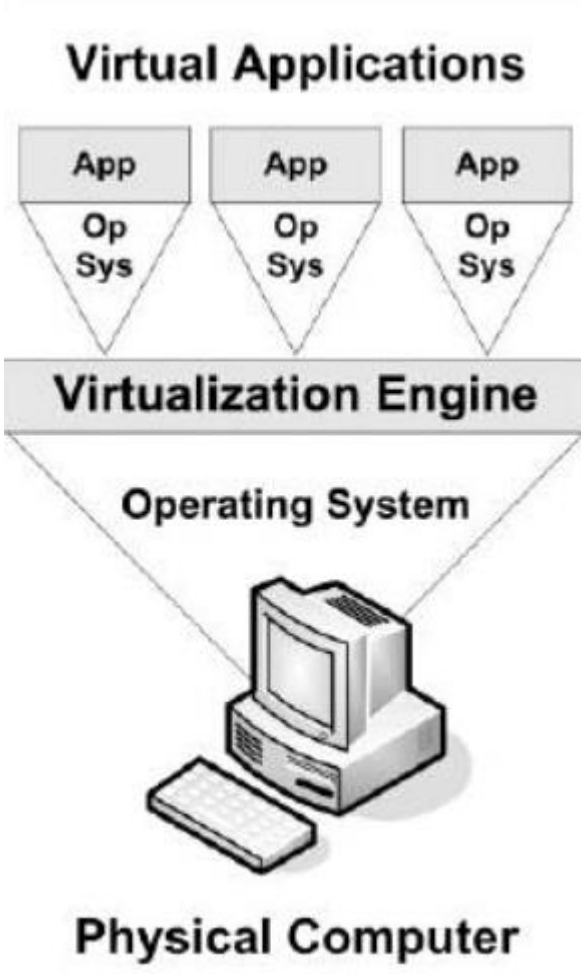


Introduction

- Application virtualization:
  - Allows applications to run independently of the underlying host operating system.

Advantages:

1. Can be deployed without having administrative rights. .
2 . Applications can be safely run on the same physical machine
3. Applications can be executed from portable media.

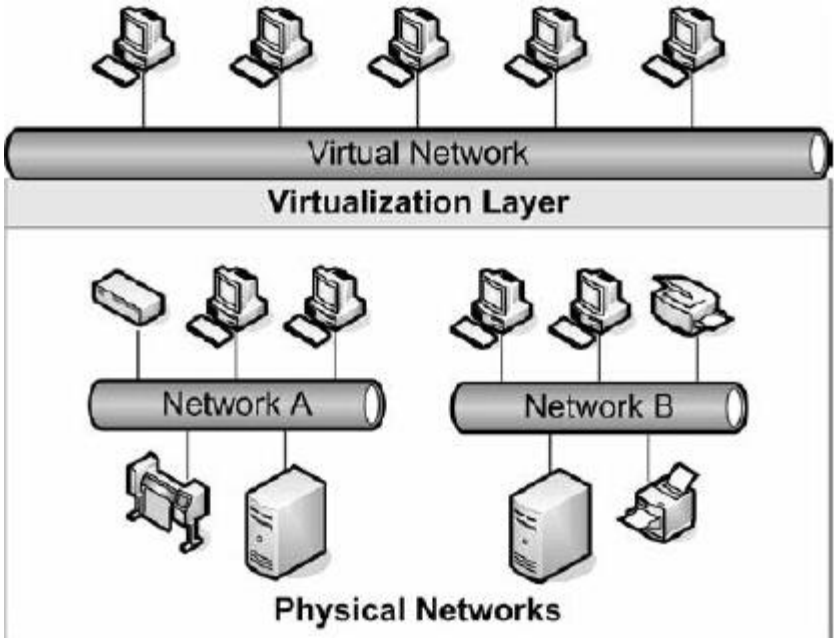


Introduction

- Network virtualization:
  - Allows us to combine all of the resources available on a network by splitting up the available bandwidth into independent channels.

Advantages:

1. Consolidation of many physical networks into one virtual network.
2. Partitioning of a single physical network into many virtual networks.

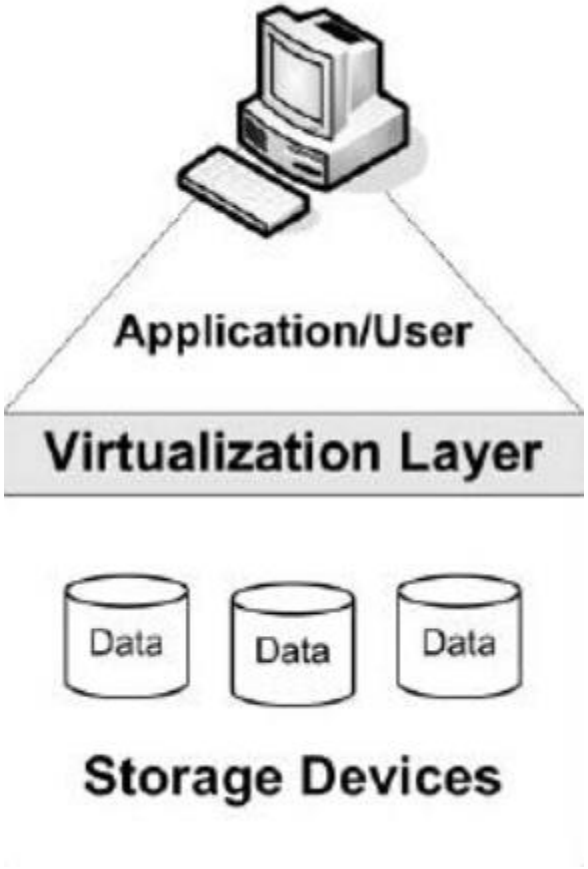


Introduction

- Storage virtualization:
  - Allows multiple storage devices to be combined as a one large storage device.

Advantages:

1. Easier administration as virtualized storage can be managed from a single administrative console.
2. Storage growth can be closely monitored and managed, making upgrade planning easier.

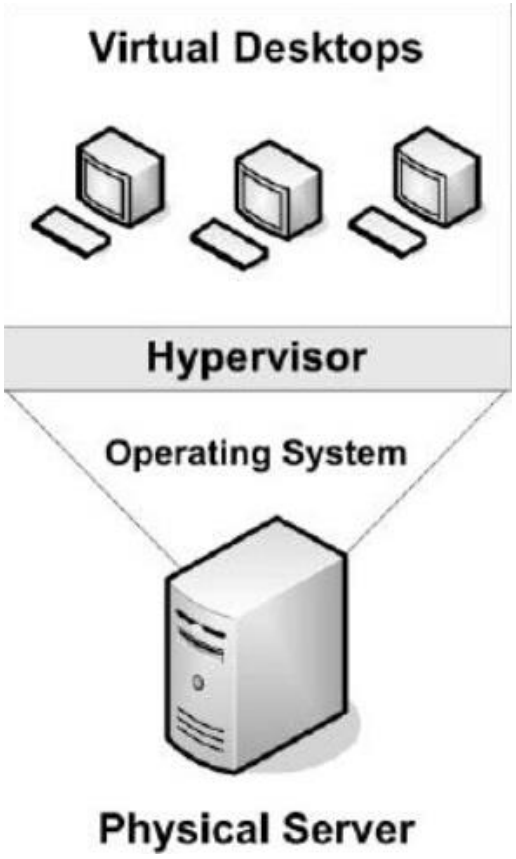


Introduction

- Desktop virtualization:
  - Allows virtual desktops to be centrally managed on a server and run by the end user on a thin client machine.

Advantages:

1. Access to typical desktop features.
2. Disaster recovery at the desktop is simplified.

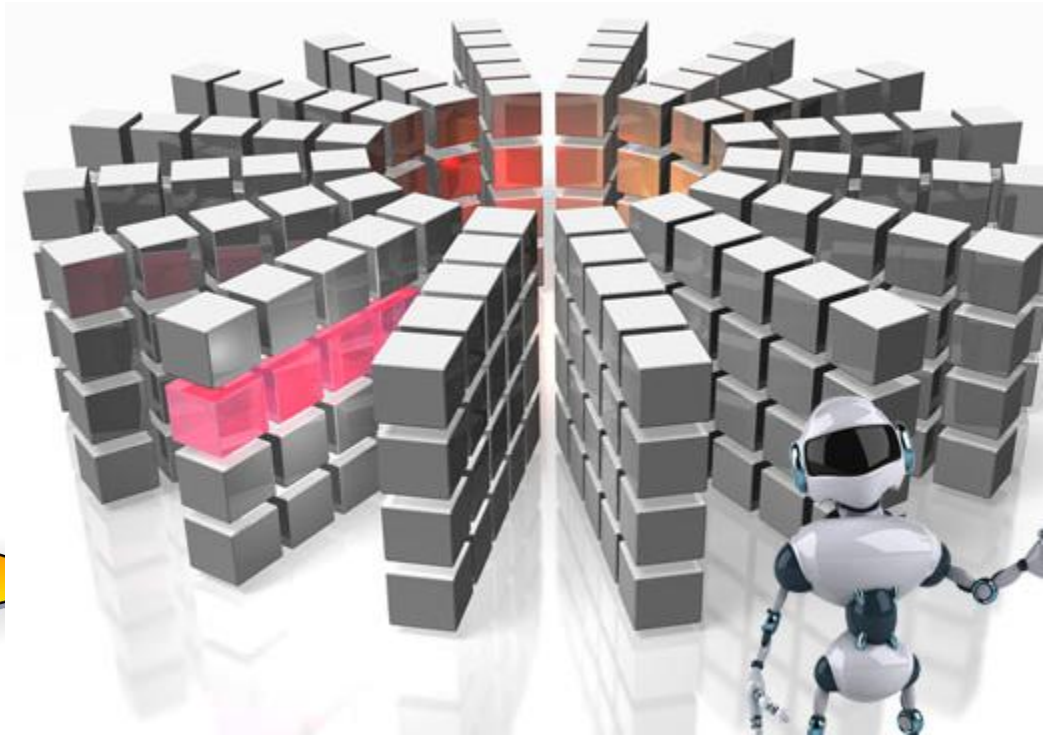


Introduction

- Virtualization gained interest:
  - Increased performance and computing capacity
  - Underutilized hardware and software resources
  - Lack of space
  - Greening initiatives
  - Rise of administrative costs

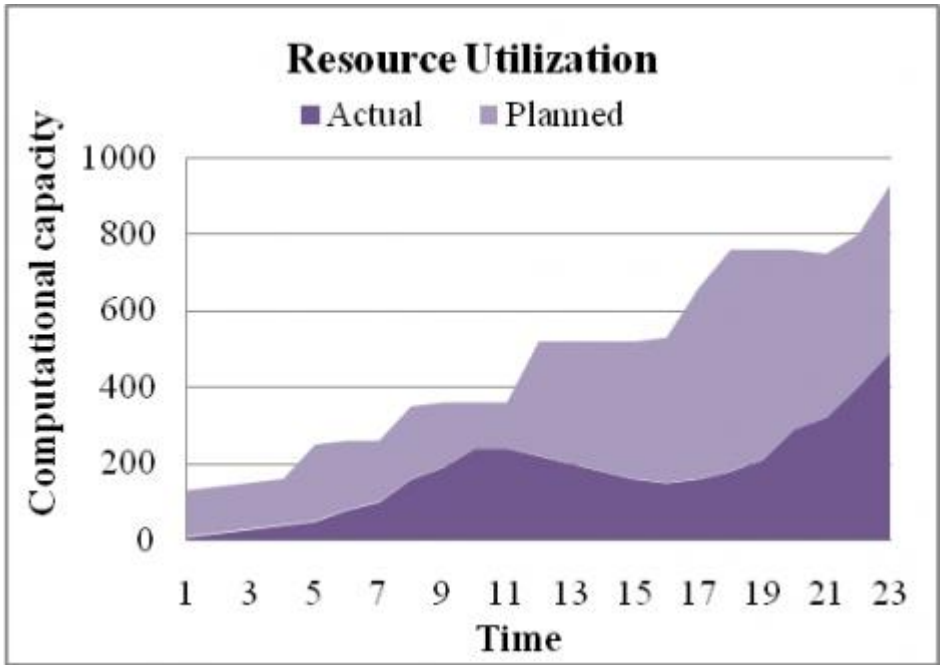
Introduction

- Increased performance and computing capacity
  - Average end-user desktop PCs are powerful enough with extra capacity.
  - High-end supercomputers having immense computing power.



Introduction

- Underutilized hardware and software resources
  - Limited use of increased performance & computing capacity.



Introduction

- Lack of space
  - Continuous need for additional capacity.

Introduction

- Greening initiatives
  - Reduce carbon footprints.
  - Reducing the number of servers, reduce power consumption.

Data Centers Contribute To Reduce The Carbon Footprint

Introduction

- Rise of administrative costs
  - Power and cooling costs are higher than the cost of IT equipments.
  - More servers, more administrative costs.

Introduction

- Virtual machine-based programming languages:

2. VIRTUAL MACHINE

Architecture of Virtual Machines

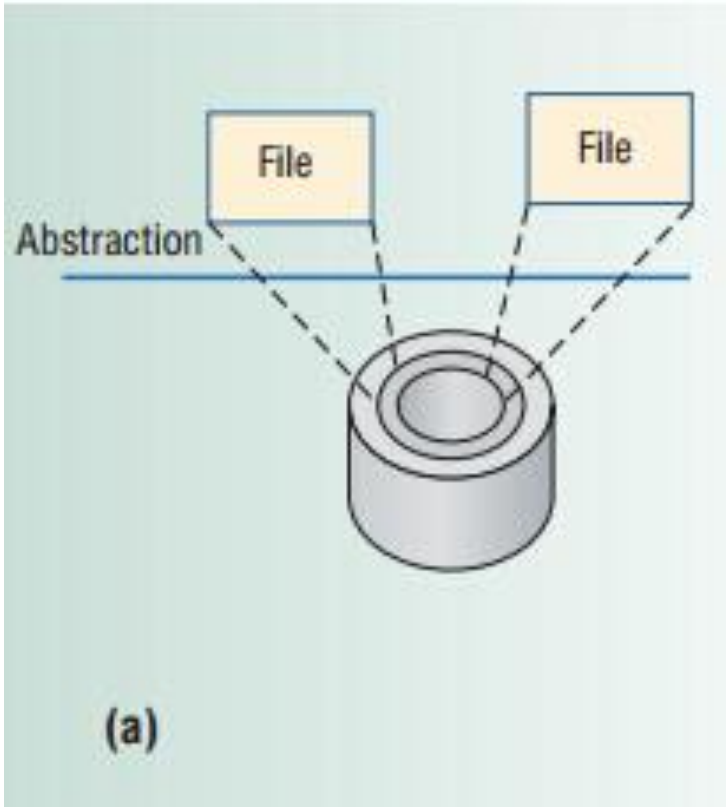
- VM can support individual ***processes*** or a ***complete system***
- Virtualization can be from ***OS*** to ***programming languages*** to ***processor architecture***.
- VMs enhance
  - Software interoperability (to work together)
  - System impregnability (having strength)
  - Platform versatility

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***.



Abstraction provides a simplified interface to underlying resources.

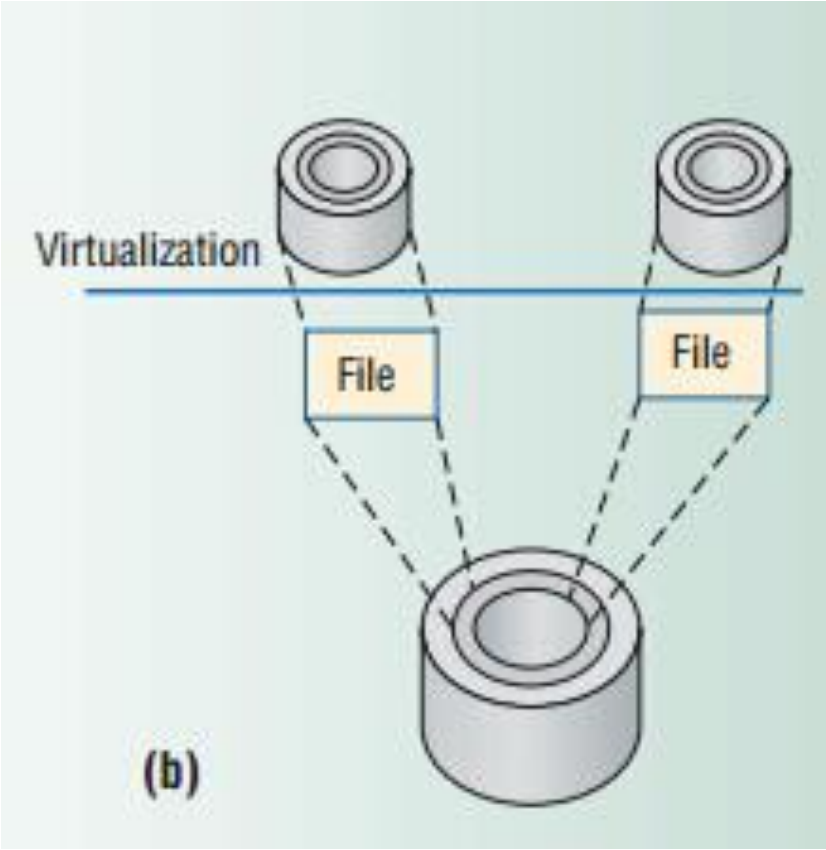
Pros and cons of Abstraction

- Well-defined interfaces ***permit development of interacting computer subsystems*** not only in *different organization* but also at *different time*.

- Limitation of well-defined interfaces , designed ***specification to one interface*** will not work for other.

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
- Ex. disk storage



Virtual Machine

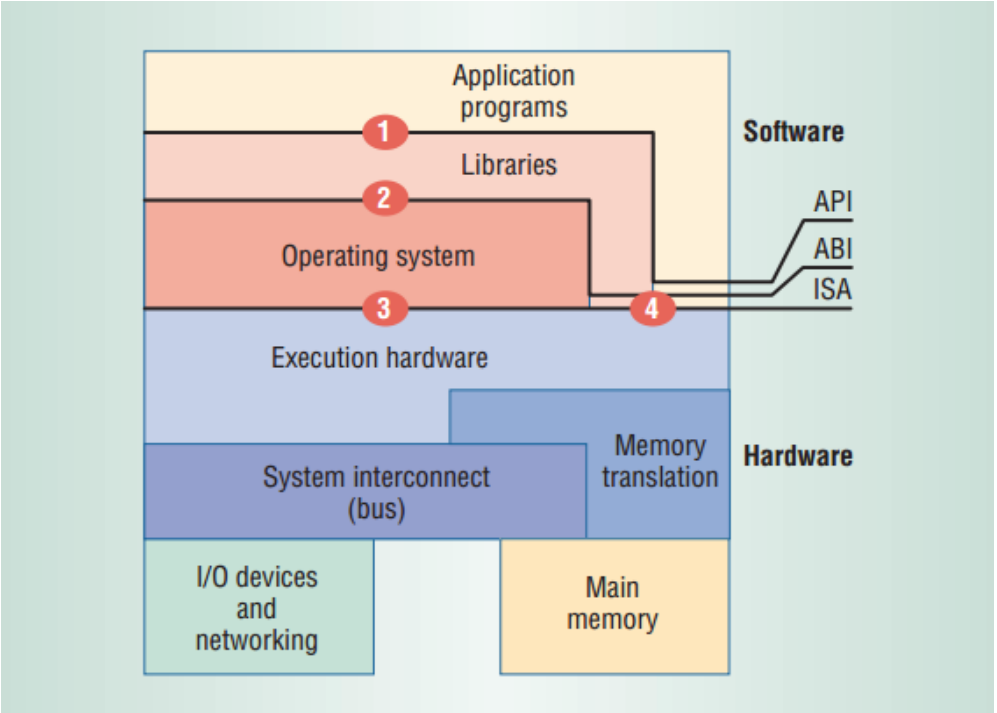
- Virtualization can be applied to entire machine.
- VM can be implemented by ***adding a software layer*** to a real machine to ***support desired architecture***.
- VM implementation lie at ***architected interfaces***

Architected Interfaces

- **Architecture**, as applied to computer systems,refer to a formal specification to an ***interface in the system***,including the l***ogical 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



Process and System VMs

Machine

- From process perspective:
- Logical memory address space assigned to the process along with user-level instructions and registers.
- I/O is visible only through the operating system.
- From OS perspective:
- The entire system runs on an underlying machine.
- Supports numerous processes simultaneously.

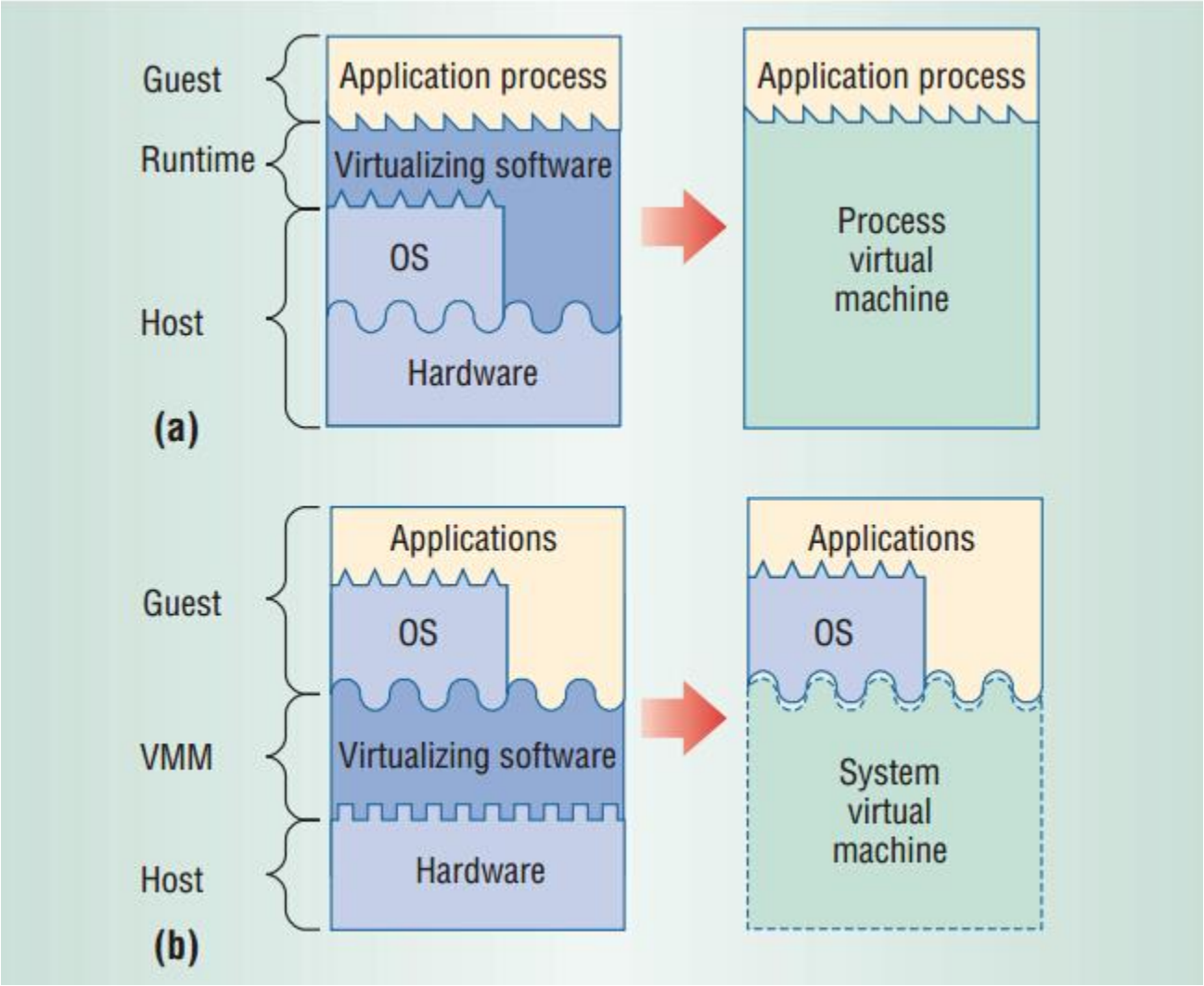
Process and System VMs

- A *process* VM is a virtual platform that executes an individual process.
- A *system* VM provides a complete, persistent system environment that supports an operating system along with its many user processes.

Process and System VMs

- **Guest**: The process or system that runs on a VM.
- **Host**: The underlying platform that supports the VM.
- **Runtime**: The virtualizing software that implements a process VM.
- **VMM**: The virtualizing software in a system VM.

Process and System VMs

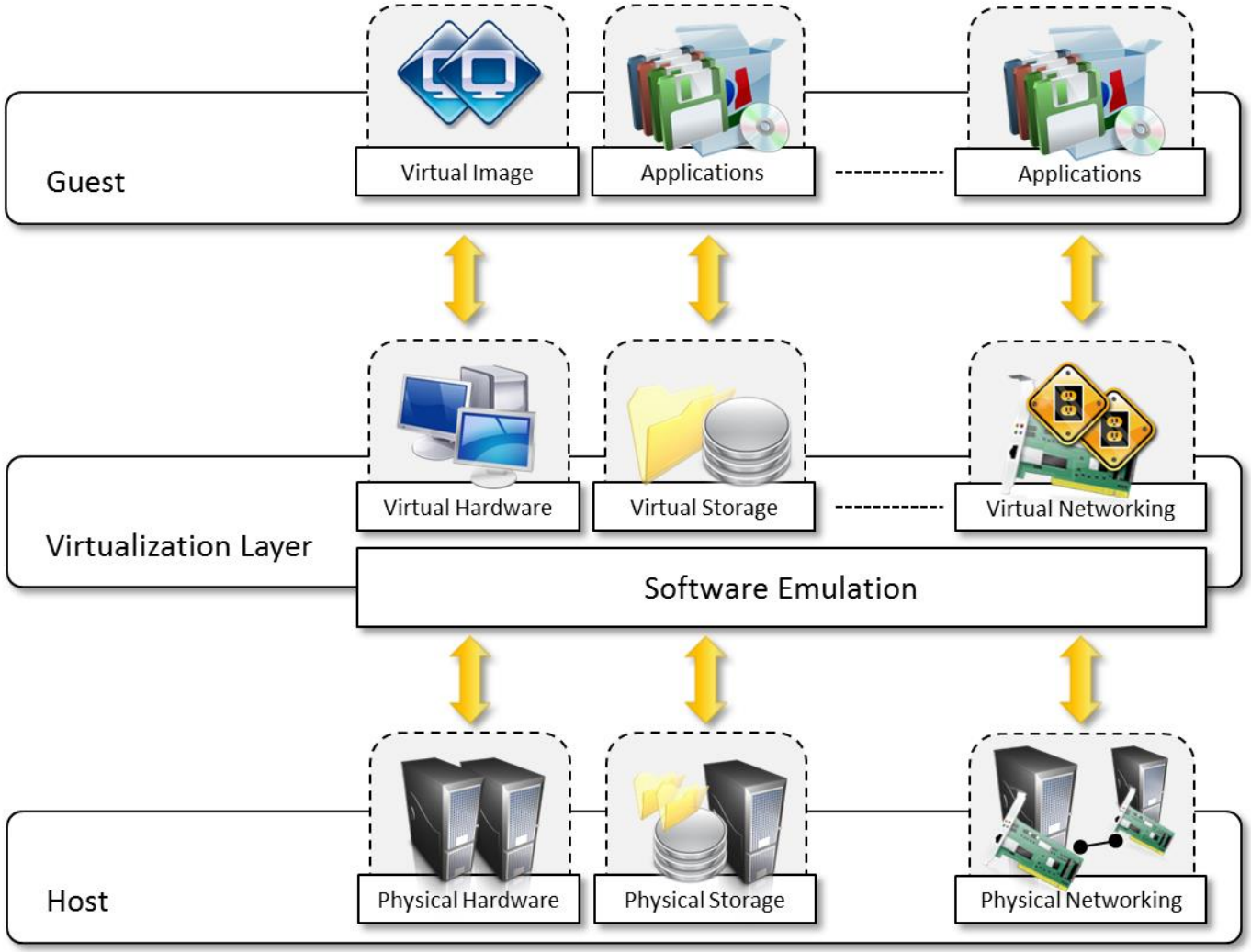


3. CHARACTERISTICS OF VIRTUALIZED ENVIRONMENTS

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.

Characteristics of virtualized environments



Characteristics of virtualized environments

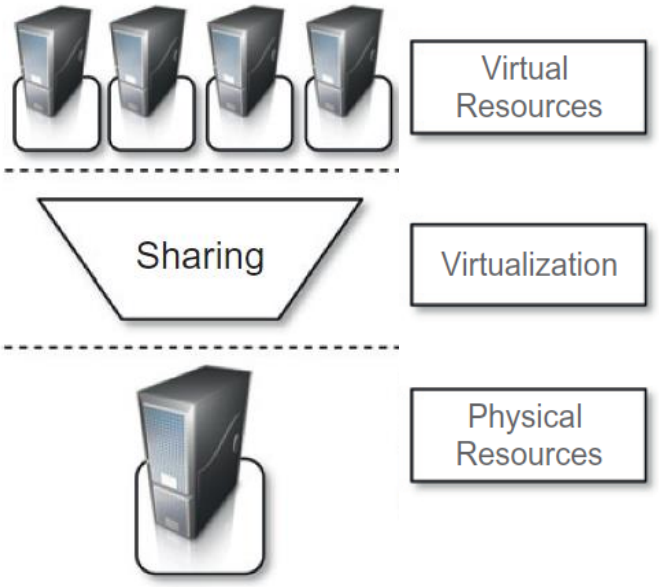
- In the case of *hardware virtualization*, the guest is represented by a system image comprising an operating system and installed applications.
- These are installed on top of virtual hardware that is controlled and managed by the virtualization layer, also called the *virtual machine manager*.
- The guest— applications and users—interacts with a virtual network, such as a *virtual private network (VPN)*, which is managed by specific software (VPN client) using the physical network available on the node.
- The virtual environment is created by means of a *software program*.

Advantages of Virtualization

Increased security

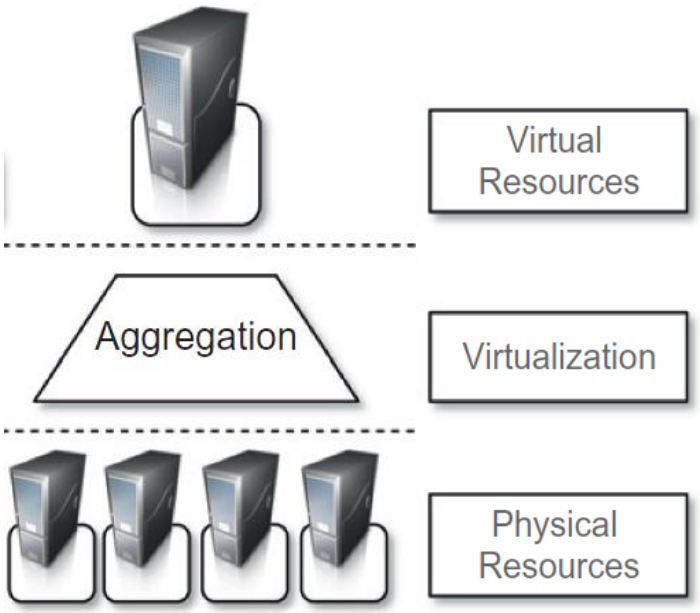
- Ability to control the execution of a guest
- Guest is executed in emulated environment.
- Virtual Machine Manager control and filter the activity of the guest.
- Hidding of resources.
- Having no effect on other users/guest environment.

Advantages of Virtualization
Managed execution types - Sharing



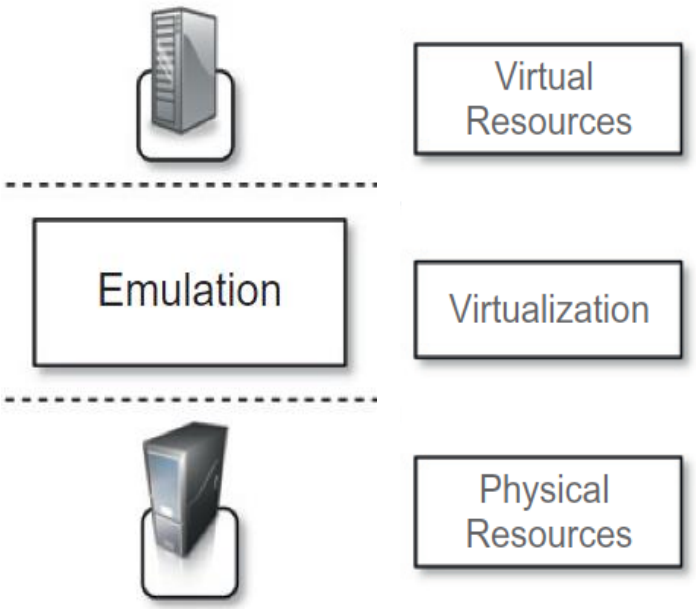
- Creating separate computing environment within the same host.
- Underline host is fully utilized.

Advantages of Virtualization
Managed execution types- Aggregation



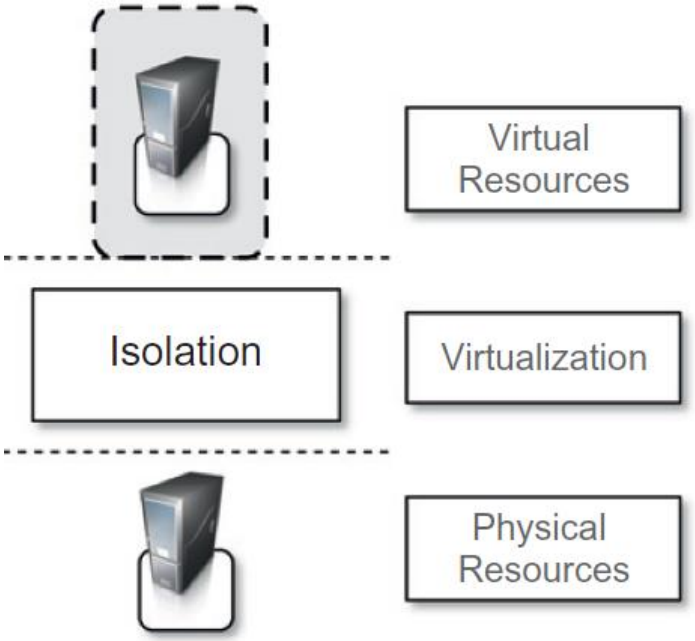
- A group of separate hosts can be tied together and represented as single virtual host.

Advantages of Virtualization
Managed execution types - Emulation



- Controlling & Tuning the environment exposed to guest.

Advantages of Virtualization
Managed execution types - Isolation

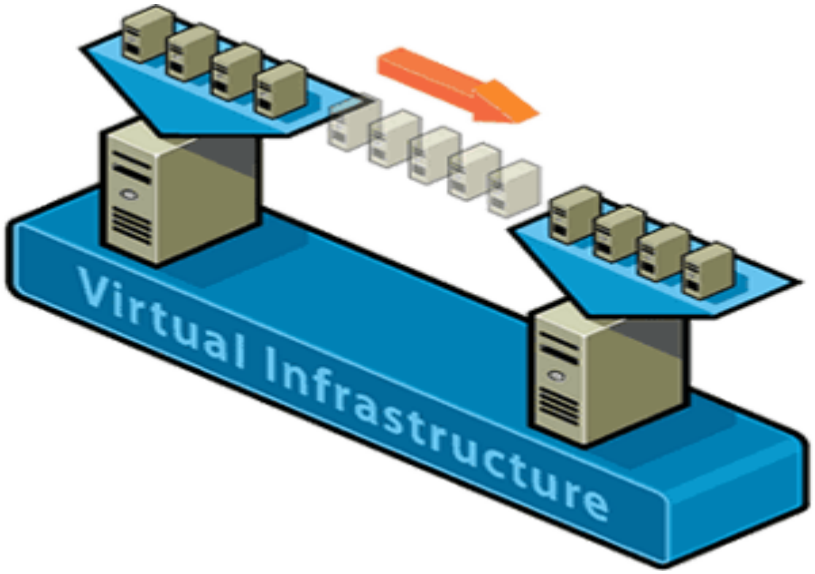


- Complete separate environment for guests.

Advantages of Virtualization

Managed execution

- **Performance Tuning** –
  - control the performance of guest.
- **Virtual Machine Migration** –
  - move virtual image into another machine.



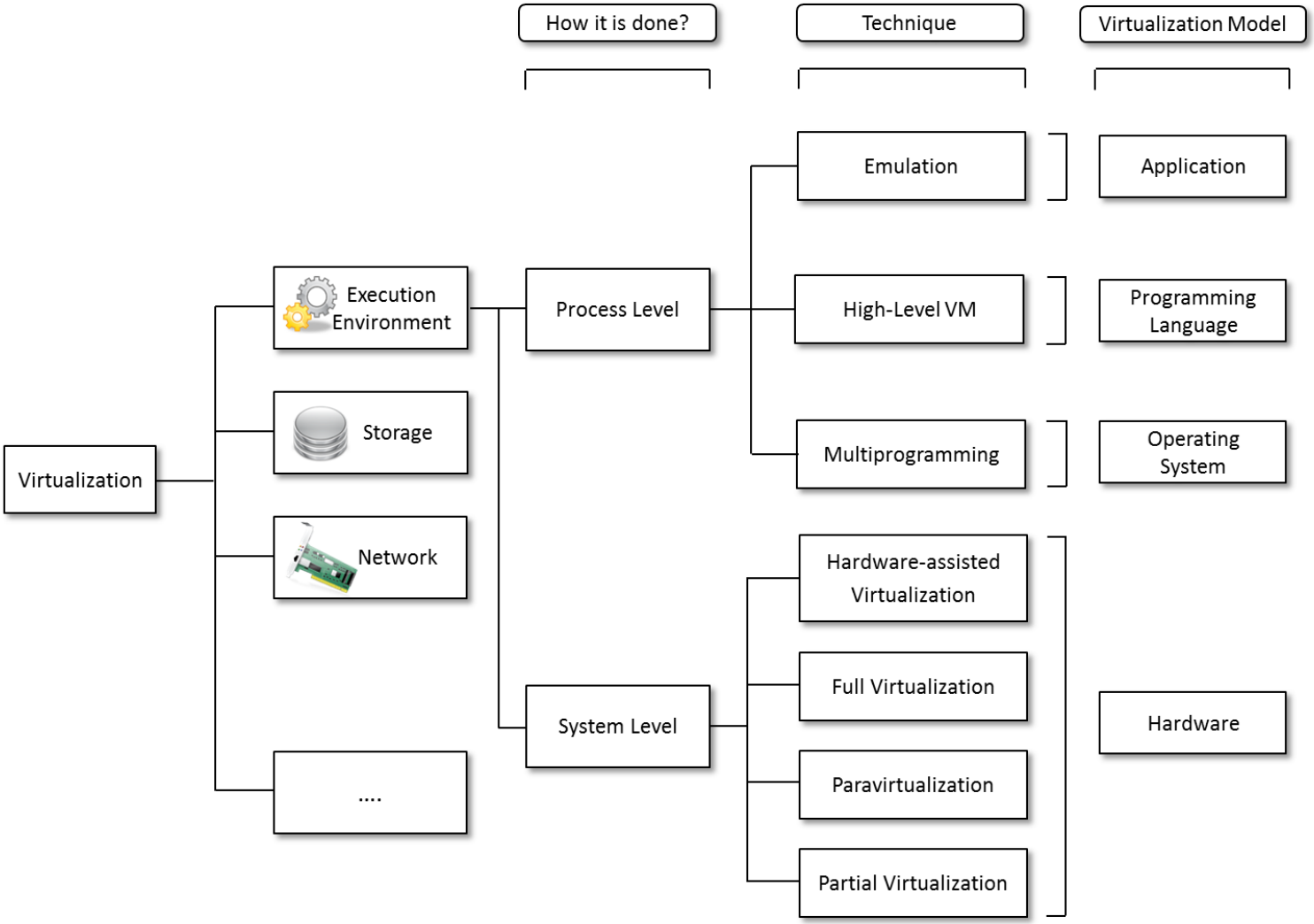
Advantages of Virtualization

Portability

- **Portability** –
  - Safely moved and executed on top of different virtual machine.
  - Availability of system is with you.

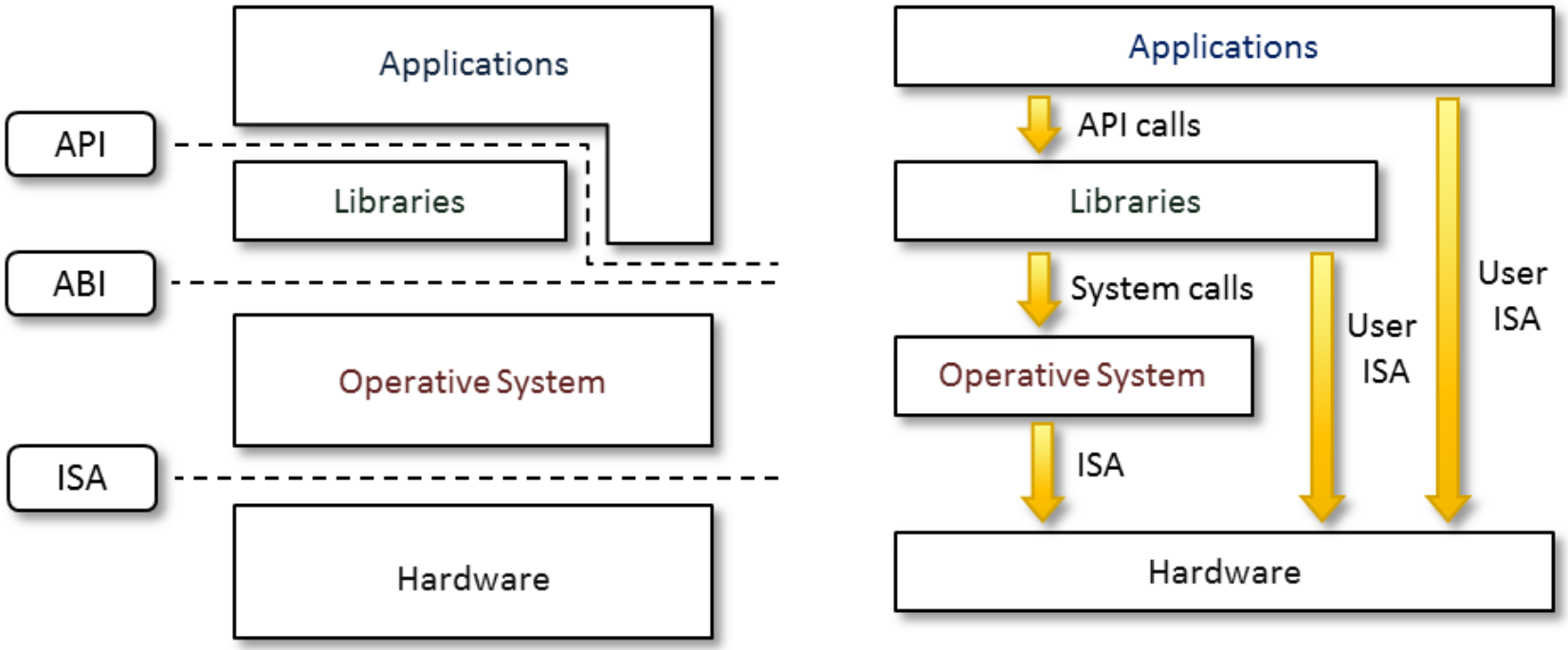
4. TAXONOMY OF VIRTUALIZATION TECHNIQUES

Taxonomy of virtualization techniques



Execution virtualization
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.



- 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

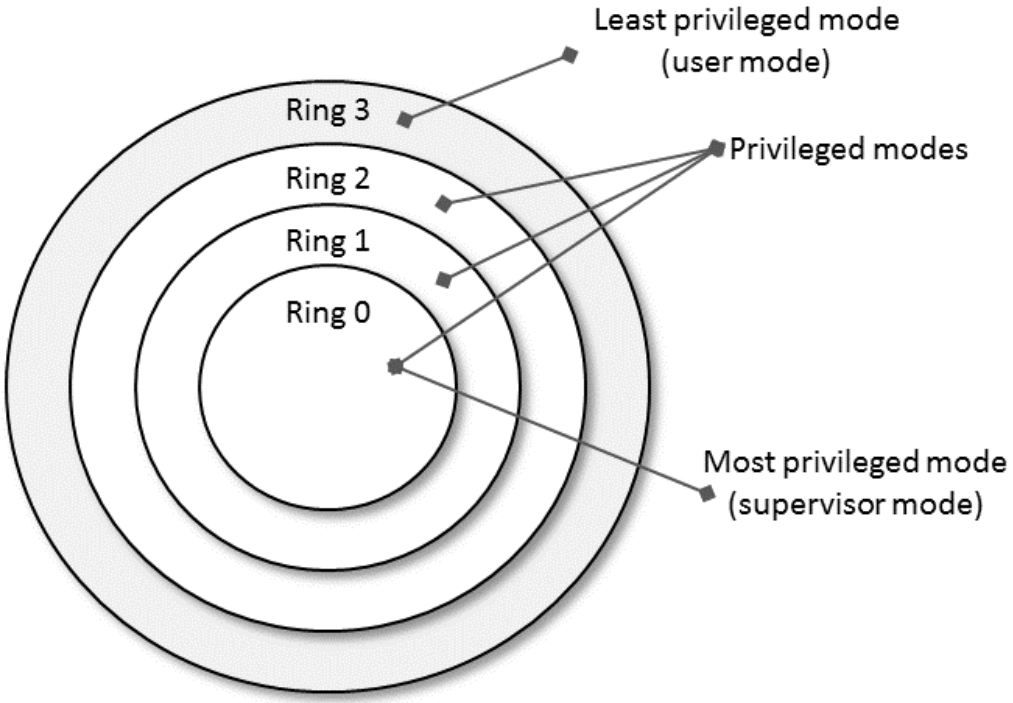
- API – it interfaces applications to libraries and/or the underlying OS.
- Layered approach simplifies the development and implementation of computing system.
- ISA has been divided into two security classes:
  - ***Privileged Instructions***
  - ***Nonprivileged Instructions***

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.

Privileged Hierarchy:

Security Ring



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

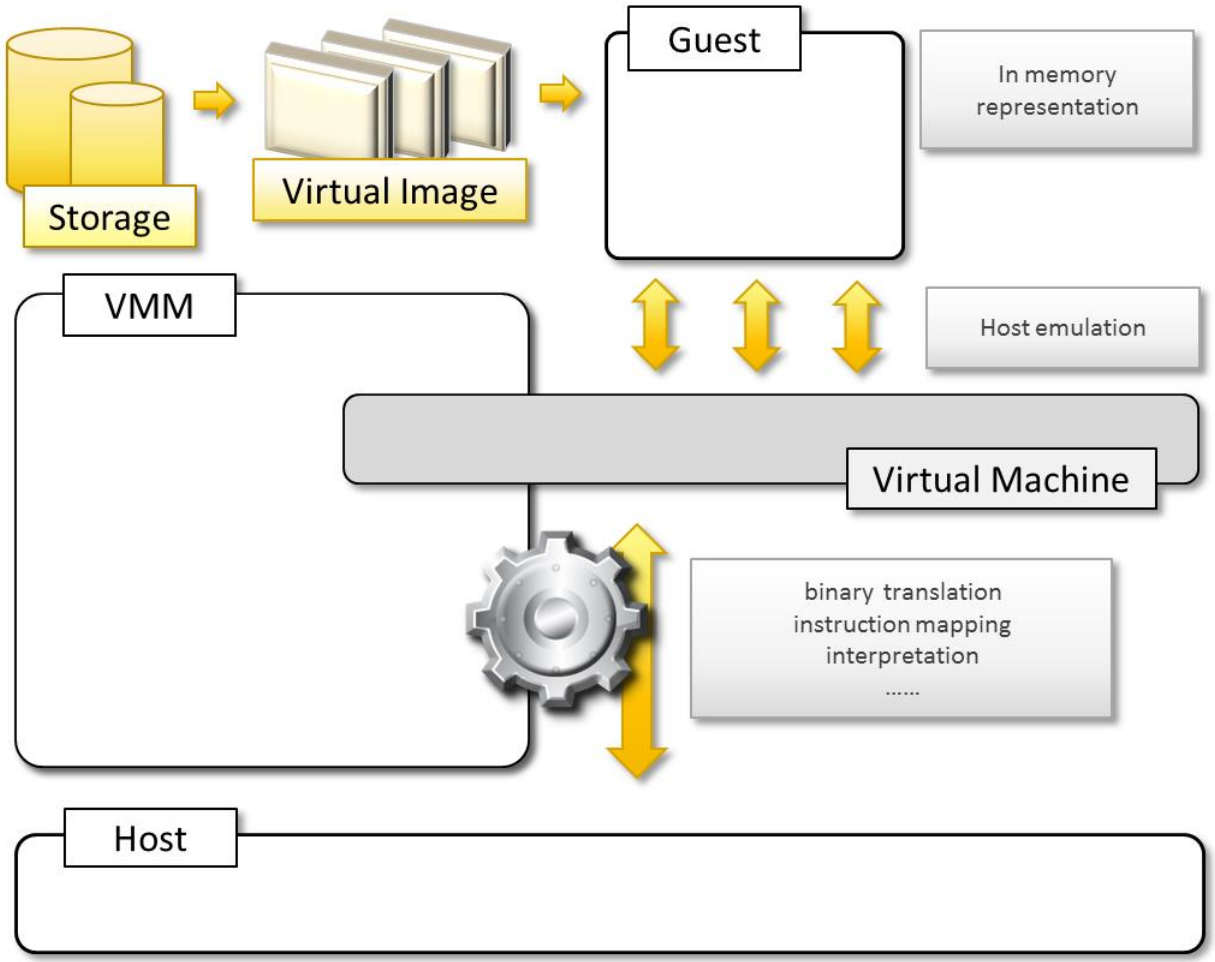
Execution Modes

- Two execution modes: *supervisor mode* and *user mode*.
- *Supervisor mode*: all the instructions (privileged and nonprivileged) can be executed without any restriction.
- *User mode*, there are restrictions to control the machine-level resources.

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.

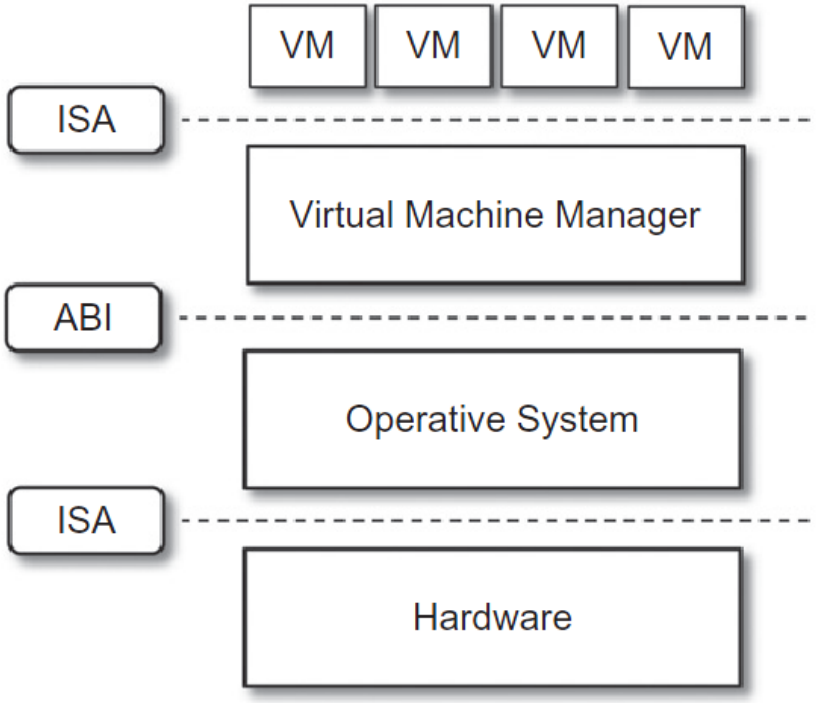
Hardware-level virtualization



Hypervisor

- Hypervisor runs above the supervisor mode.
- It runs in supervisor mode.
- 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***

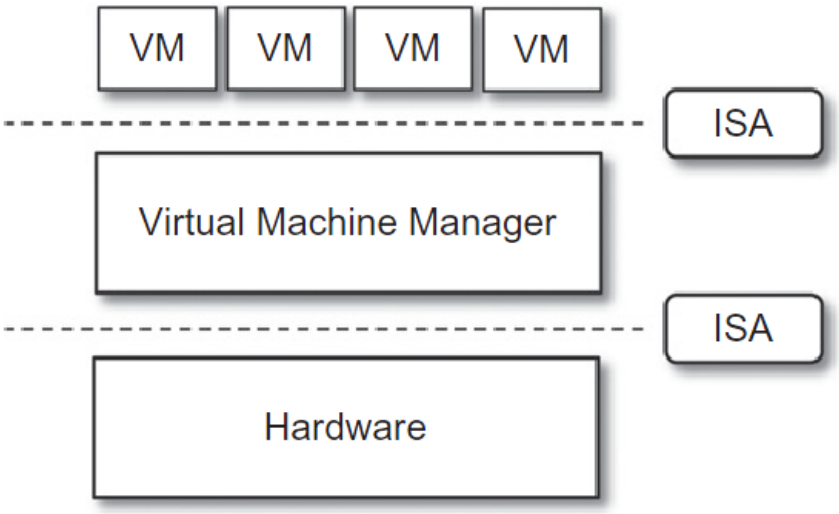
Hypervisor – Type I



- It runs directly on top of the hardware.
- Takes place of OS.
- Directly interact with the ISA exposed by the underlying hardware.

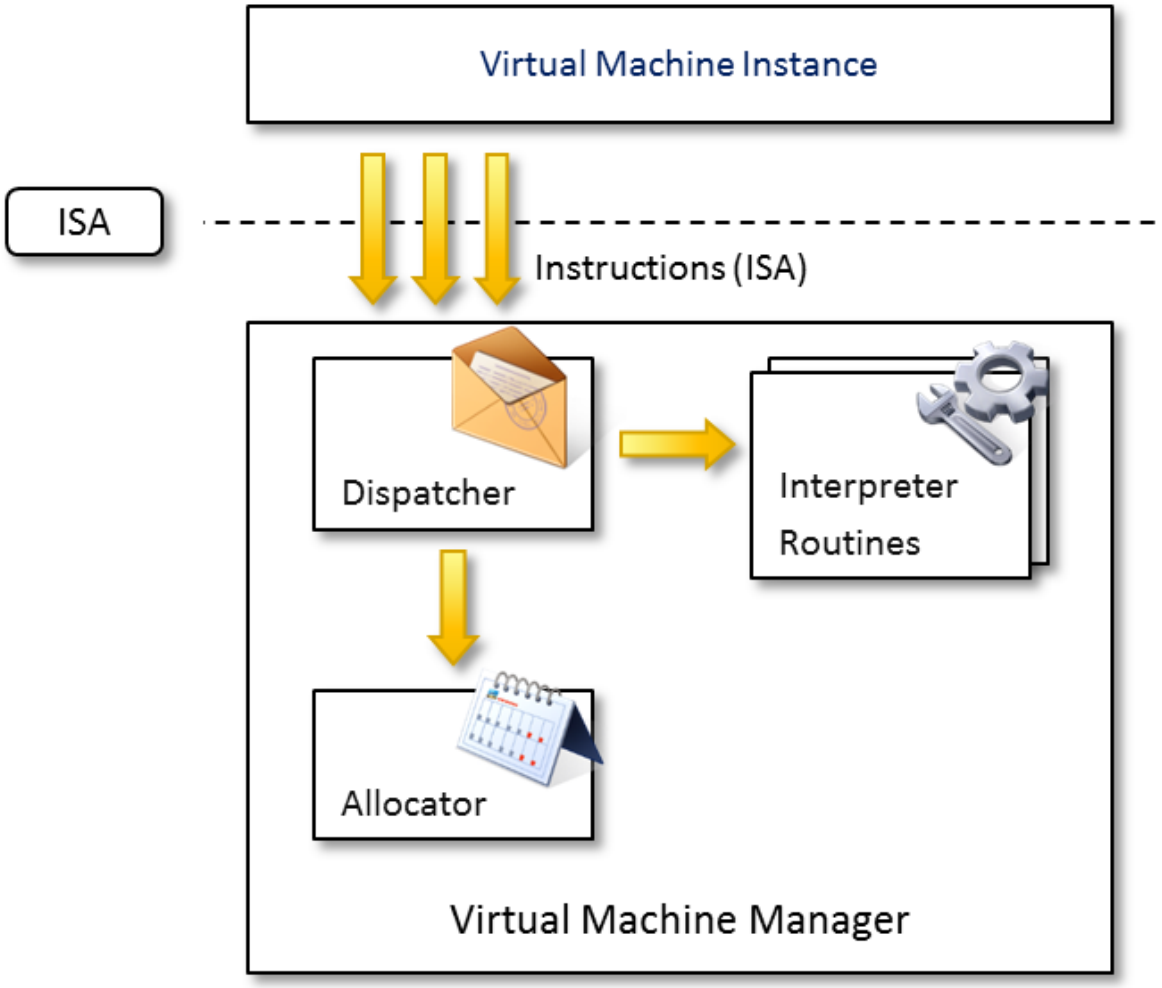
- Also known as *native virtual machine*.

Hypervisor – Type II



- It require the support of an operating system to provide virtualization services.
- Programs managed by the OS.
- Emulate the ISA of virtual h/w.
- Also called hosted virtual machine.

Virtual Machine Manager (VMM)



Criteria of VMM

- **Equivalence** – same behaviour 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.

THEOREM 3.1

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.

Classification of IS

- Privileged Instructions

  Trap if the processor is in user mode
- Control sensitive Instructions
- Behavior sensitive Instructions

Theorems

THEOREM 3.2

A conventional third-generation computer is recursively virtualizable if:

- It is virtualizable and
- A VMM without any timing dependencies can be constructed for it.

Hardware virtualization Techniques

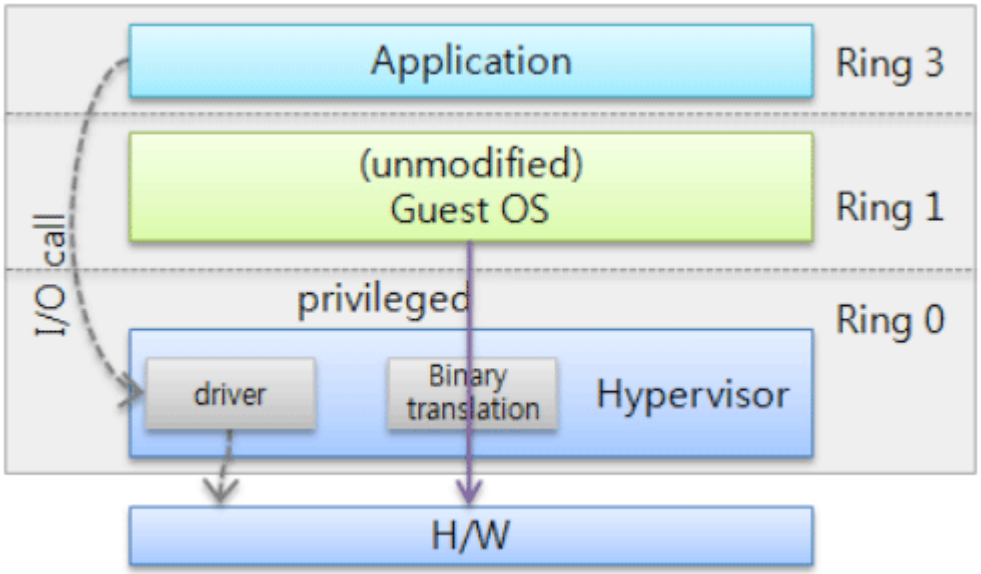
- CPU installed on the host is only one set, but each VM that runs on the host requires their own CPU.
- It means CPU needs to virtualized, done by hypervisor.

Hardware virtualization Techniques

- **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
    - Ease of emulation of different architectures and coexistence
  - ***Key challenge is interception of privileged instructions***

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.

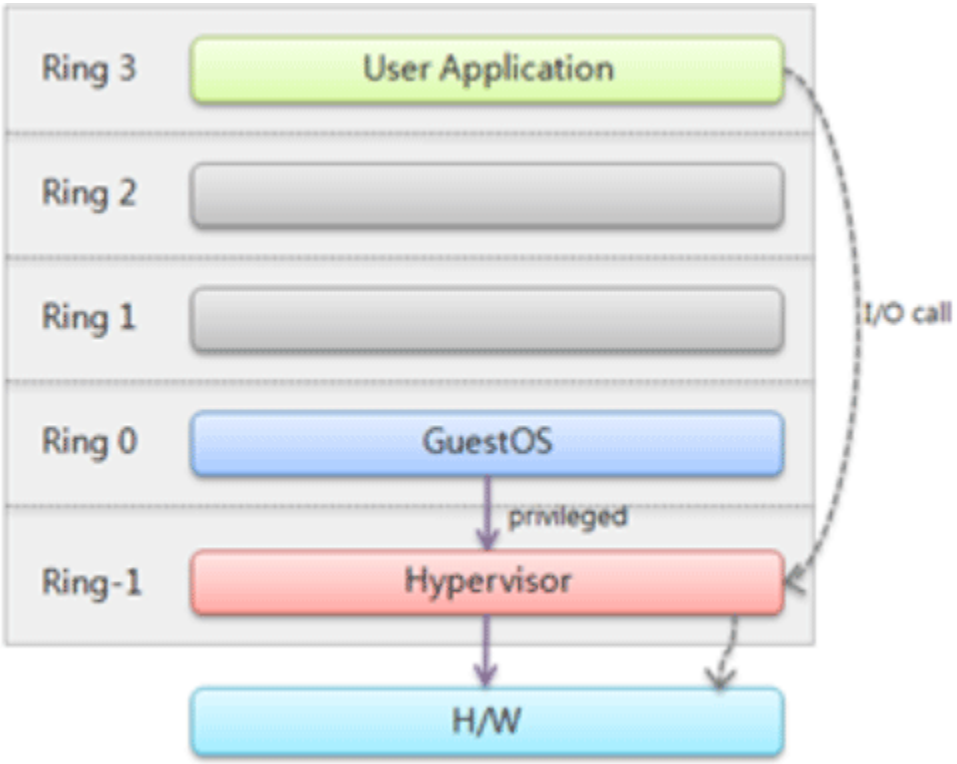


Hardware virtualization Techniques

- **Hardware-assisted virtualization**
  - In this hardware provides architectural support for building a VMM able to run a guest OS in complete isolation.
  - ***Intel VT*** and ***AMD V*** extensions.
  - Early products were using ***binary translation to trap some sensitive instructions*** and provide an emulated version

Hardware-assisted virtualization

- Additional Ring -1
- ***No binary translation*** of privileged instructions
- Commands are executed directly to h/w via the hypervisor

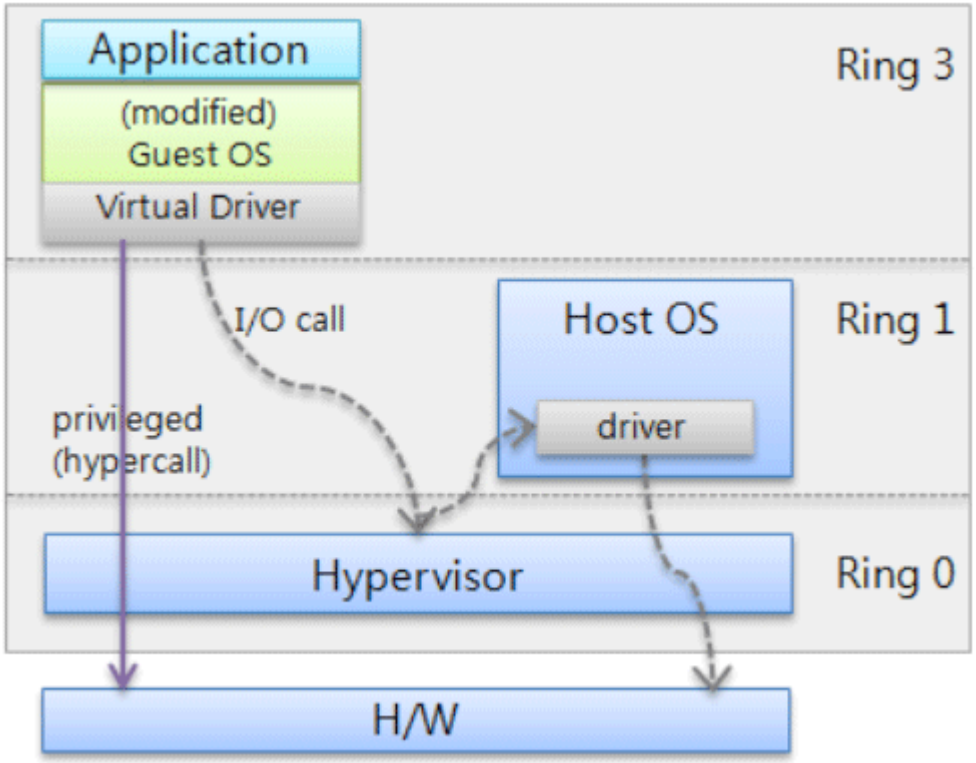


Hardware-assisted virtualization

- **Paravirtualization**
  - Not-transparent virtualization
  - Thin VMM
  - 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.

Paravirtualization

- 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.



Paravirtualization

- **Partial virtualization**
  - Partial emulation of the underlying hardware
  - Not allow complete isolation to guest OS.
  - Address space virtualization is a common feature of comtemporary operating systems.
  - Address space virtualization used in time-sharing system.

Operating system-level virtualization

- It offers the opportunity to create different and ***separated execution environments*** for applications that are managed concurrently.
- No VMM or hypervisor
- Virtualization is in single OS
- OS kernel allows for multiple isolated user space instances
- Good for server consolidation.
- Ex. *chroot , Jails, OpenVZ etc.*

Programming language-level virtualization

- It is mostly used to achieve ***ease of deployment*** of application, ***managed execution*** and ***portability across*** different platform and OS.
- It consists of a virtual machine ***executing the byte code of a program***, which is the result of the ***compilation process***.
- Produce a binary format representing the machine code for an abstract architecture.
- Example
  - Java platform – Java virtual machine (JVM)
  - .NET provides Common Language Infrastructure (CLI)
- They are stack-based virtual machines

Advantage of programming/process-level VM

- Provide ***uniform execution environment*** across different platforms.
- This ***simplifies*** the development and deployment efforts.
- Allow more ***control over the execution*** of programs.
- Security; by filtering the I/O operations
- Easy support for sandboxing

Application-level virtualization

- It is a technique allowing applications to run in ***runtime environments*** that do not ***natively support*** all the features required by such applications.
- In this, applications are not installed in the ***expected runtime environment***.
- This technique is most concerned with :-
  - Partial file system
  - Libraries
  - Operating System component emulation

Strategies for Implementation Application-Level Virtualization

- Two techniques:
  - **Interpretation** -
    - In this every source instruction is ***interpreted*** by an emulator for executing ***native ISA instructions***,
    - ***Minimal*** start up cost but ***huge overhead***.
  - **Binary translation**
    - In this every source insruction is ***converted to native*** instructions with equivalent functions.
    - Block of instructions ***translated*** , ***cached*** and ***reused***.
    - Large ***overhead cost*** , but over time it is subject to ***better performance***.

Different from H/w Virtualization

- In h/w virtualization , it allows the execution of a program ***compiled against a different h/w***.
- In Application level emulation , complete ***h/w environment***.
- Ex:-
  - Wine
  - CrossOver
  - and , many more

Storage virtualization

- It allows decoupling the physical organization of the h/w from its logical representation.
- Using Network based virtualization known as ***storage area network*** (SAN).
- SAN – ***Self Study***

Network virtualization

- It combines h/w appliances and specific software for the creation and management of a virtual n/w.
- It can aggregate ***different physical networks*** into a single logical network.
- VLAN – ***Self Study***

Desktop virtualization

- Abstracts the desktop environment available on a ***personal computer*** in order to provide access to it using a ***client/server approach***.
- Makes accessible a different system - remotely stored on a different host and accessed through a network connection.
- Addresses the problem of making the same desktop environment ***accessible from everywhere***.

Application server virtualization

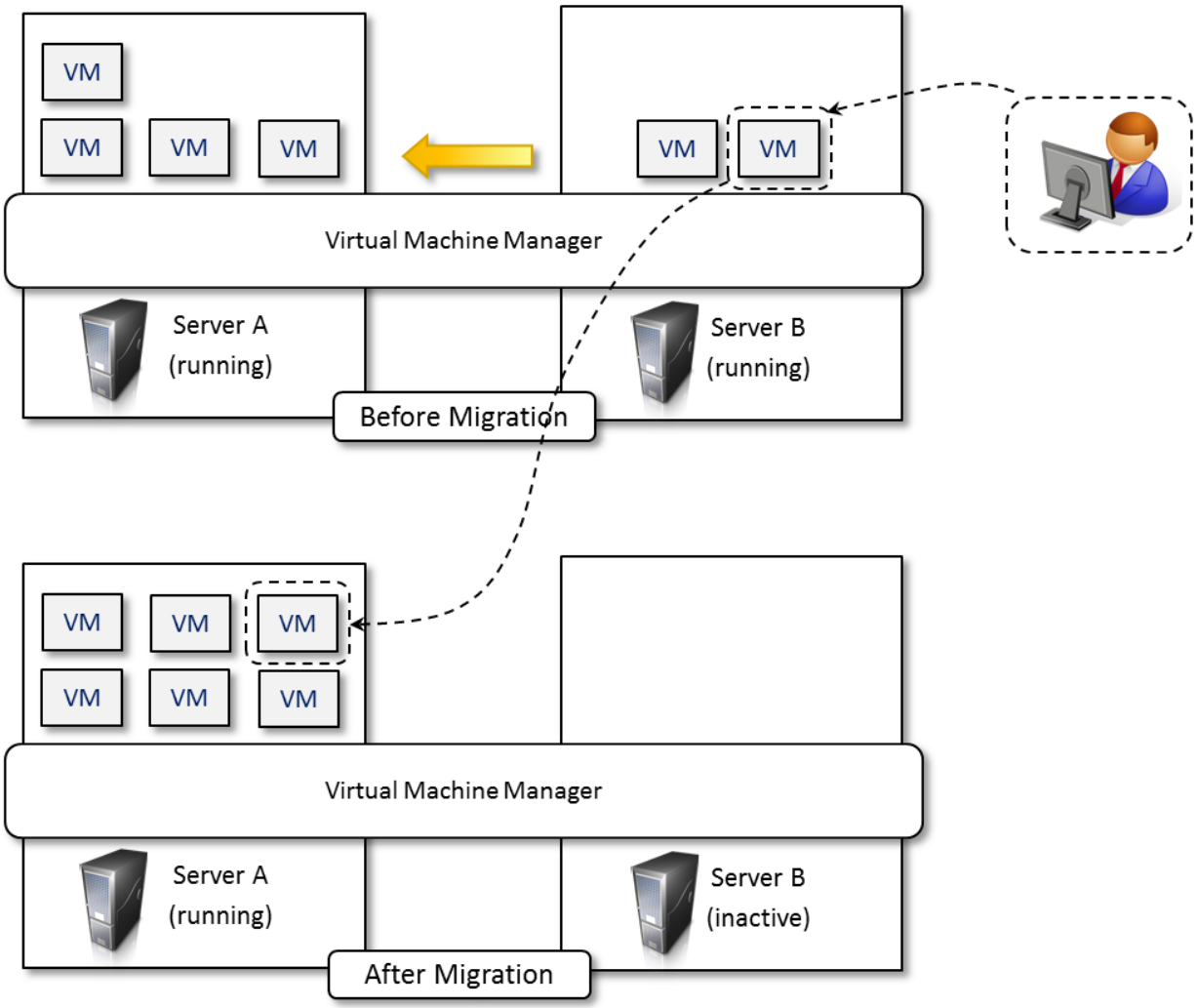
- Abstracts a collection of application servers that provide the same services as a single virtual application server by using load-balancing strategies.
- Provides high-availability infrastructure for the services hosted in the application server.

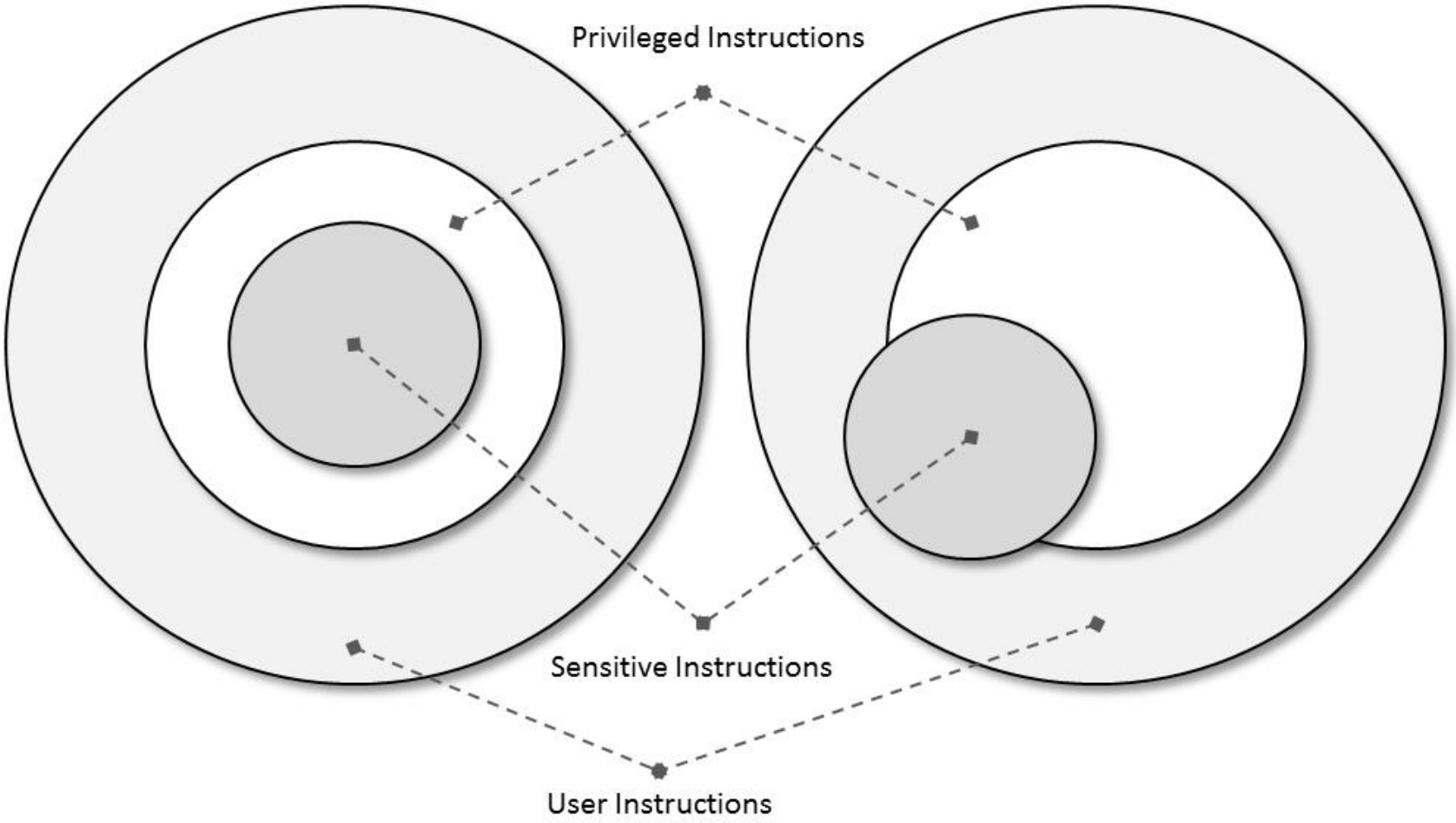
5. VIRTUALIZATION AND CLOUD COMPUTING

Virtualization and cloud computing

- Plays an important role in cloud computing.
- Primarily used to offer configurable computing environments and storage.
- H/w virtualization enabling solution in IaaS
- Programming language virtualization in PaaS.
- Virtualization provides:
  - Consolidating
  - Isolation
  - Controlled environments

Virtual Machine Migration




Privileged Instructions
Sensitive Instructions
User Instructions

Virtualization and cloud computing

- Partition virtual storage services into slices
  - dynamic
  - offer as a service
- Secure and protect the hosting infrastructure
- Recreate the entire computing stack

Pros & Cons of Virtualization

Advantages of virtualization

- Managed execution and isolation
- Portability and self-containment
- More efficient use of resources

Pros & Cons of Virtualization

Disadvantages of virtualization

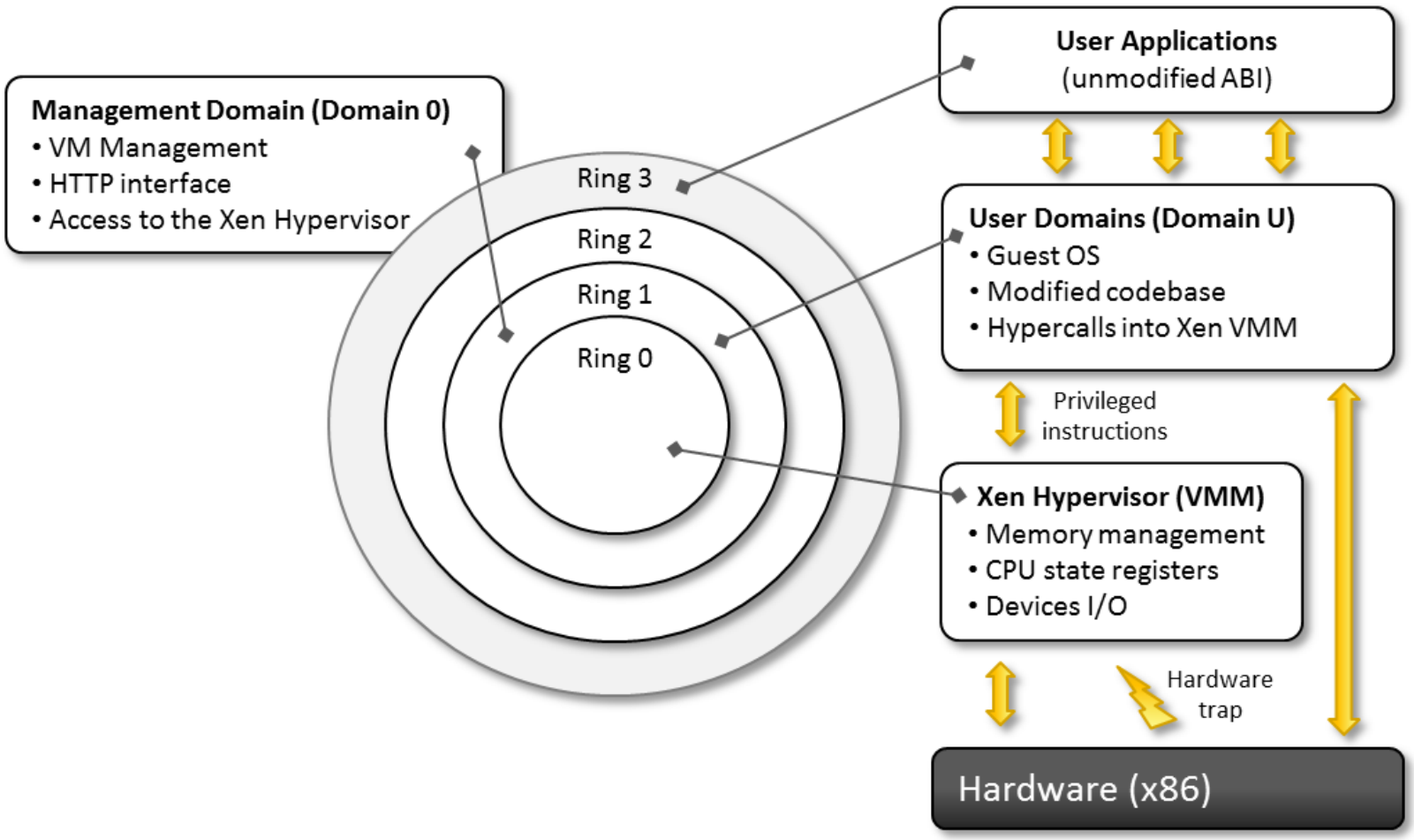
- **Performance degradation** -
  - As it interposes and abstraction layer between guest & host.
- **Inefficiency and degraded user experience** -
  - Some of specific features of the host is unexposed.
- **Security holes and new threats**
  - *Case 1* – emulating a host in a completely transparent manner.
  - *Case 2* - H/w virtualization , malicious programs can preload themselves before the OS and act as a thin VMM.

5. TECHNOLOGY EXAMPLES

Xen: paravirtualization

- Open-source initiative based on paravirtualization.
- Advanced to support full virtualization.
- Commercial solution.
- Desktop/server virtualization.
- Xen Cloud Platform (XCP).

Xen: paravirtualization

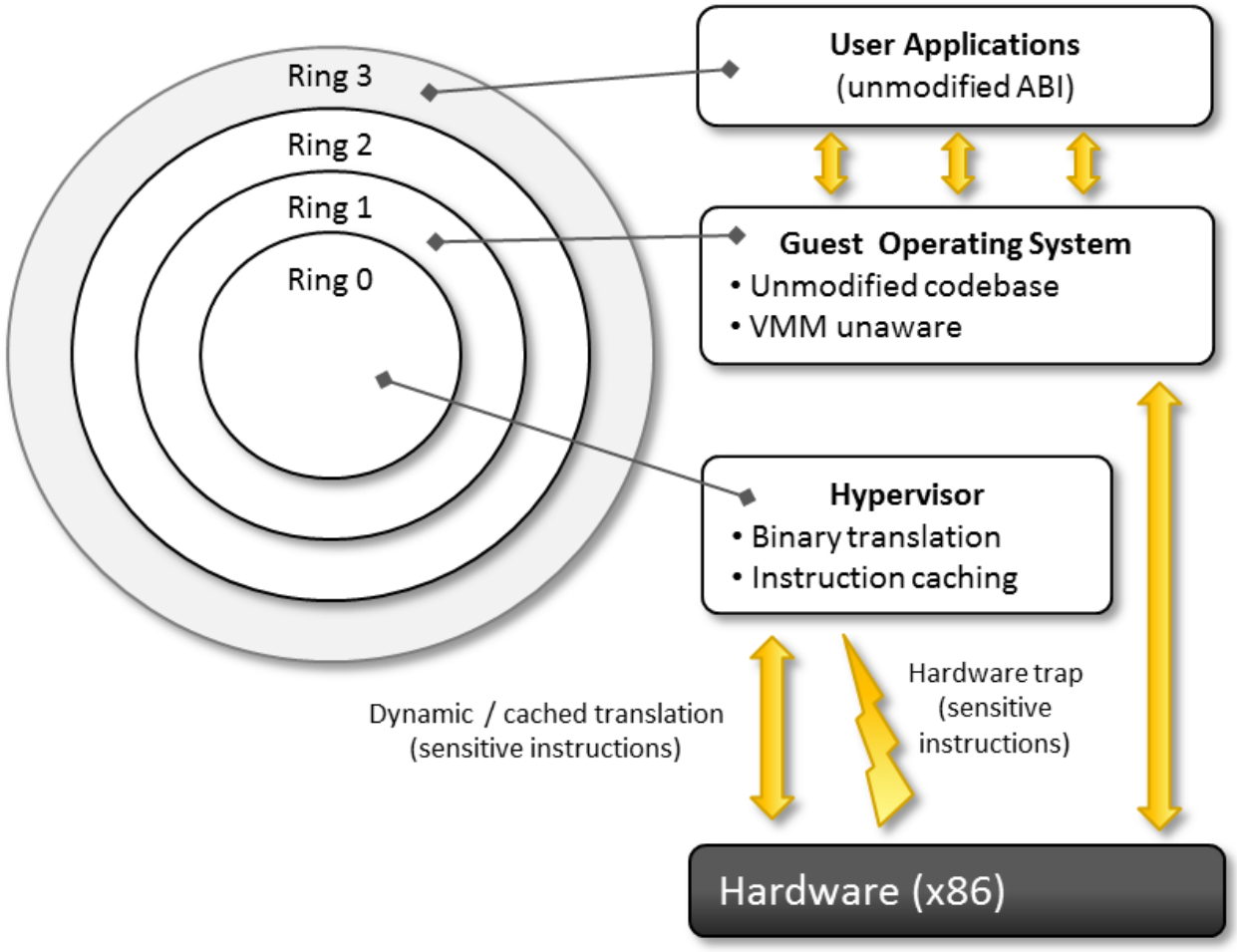


VMware: full virtualization

- Based on the concept of full virtualization.
- Server environment – Type I hypervisors.
- Desktop environment – Type II hypervisors.
- Additional tools and software available.

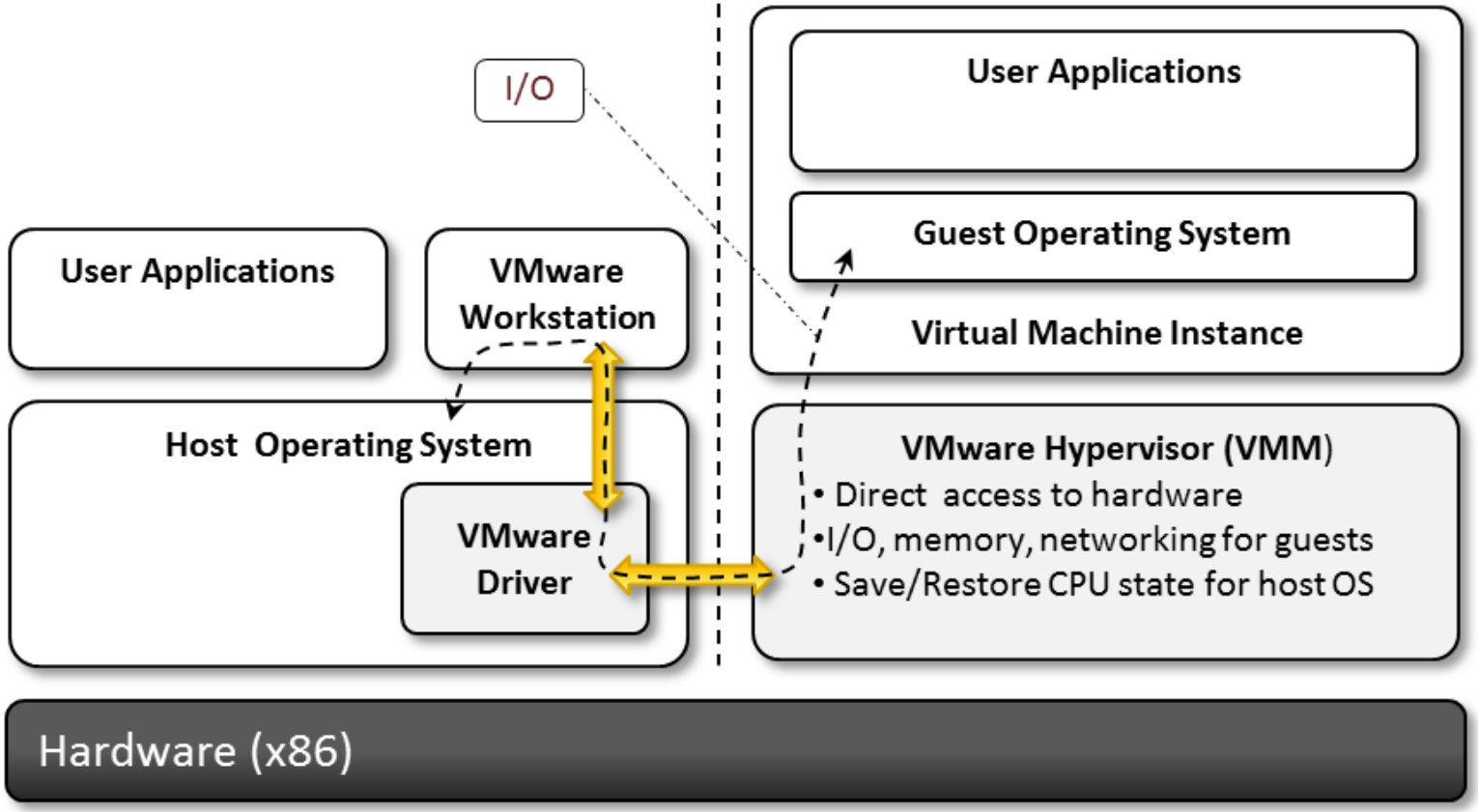
VMware: full virtualization

- Full virtualization and binary translation



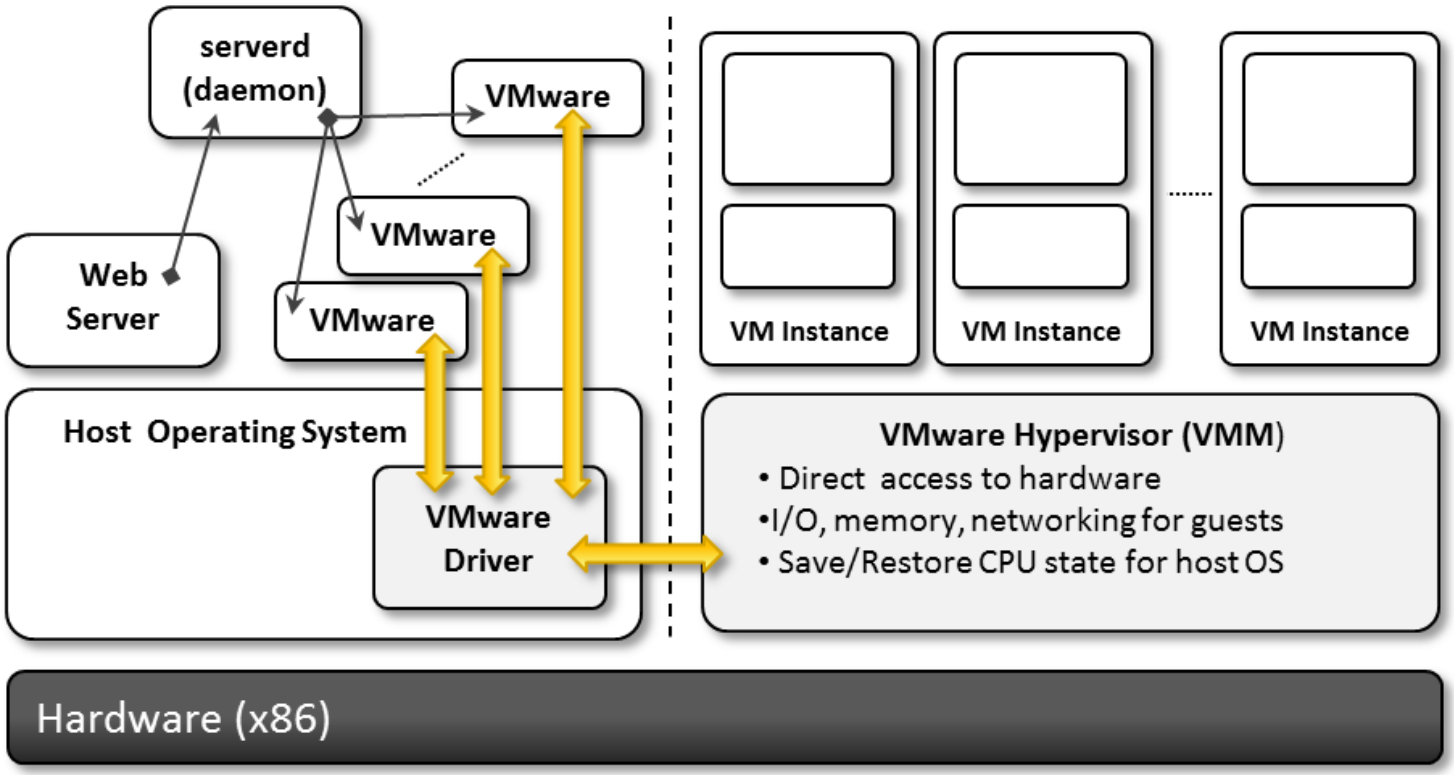
VMware: full virtualization

- Virtualization solutions
  - End-user (desktop) virtualization



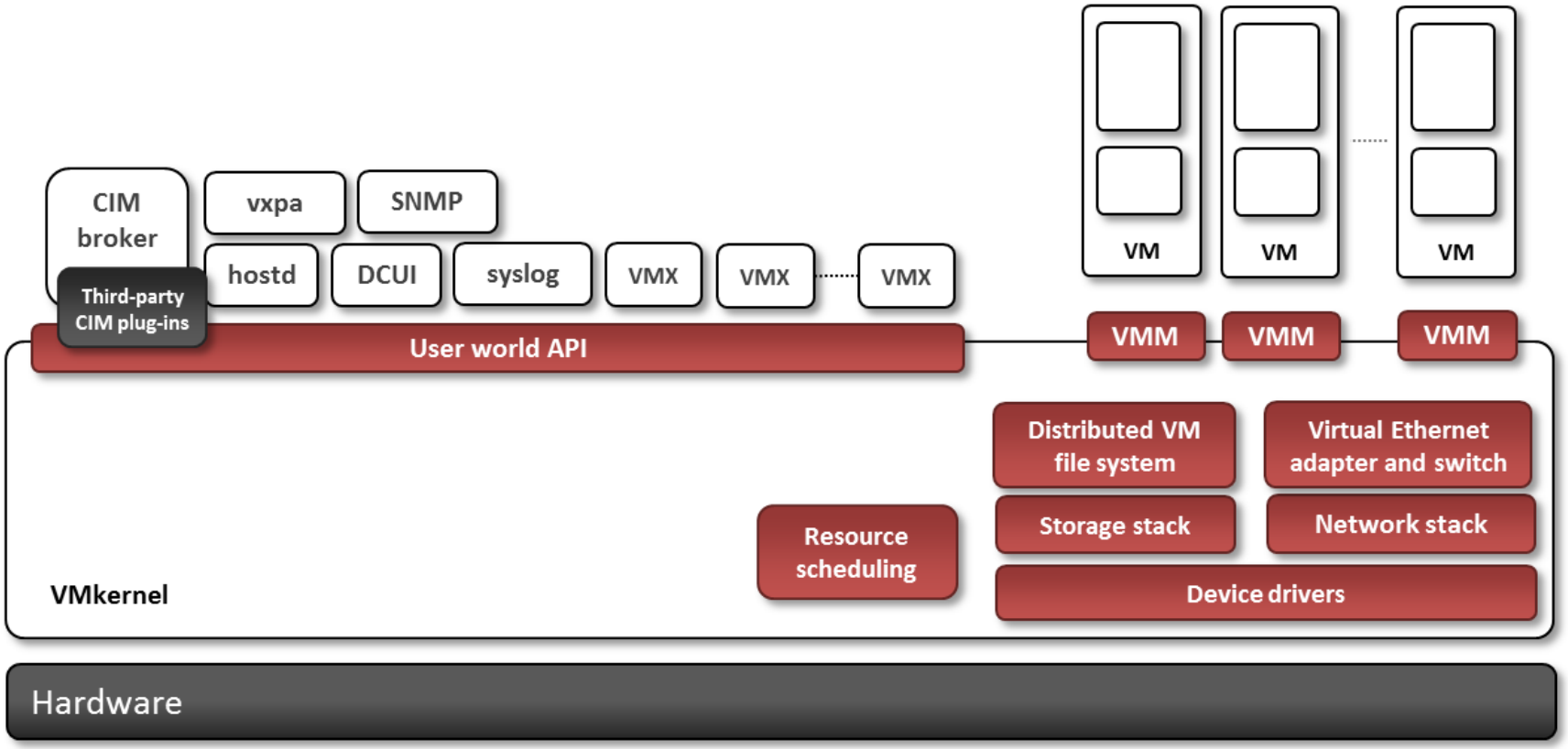
VMware: full virtualization

- Virtualization solutions
  - Server virtualization



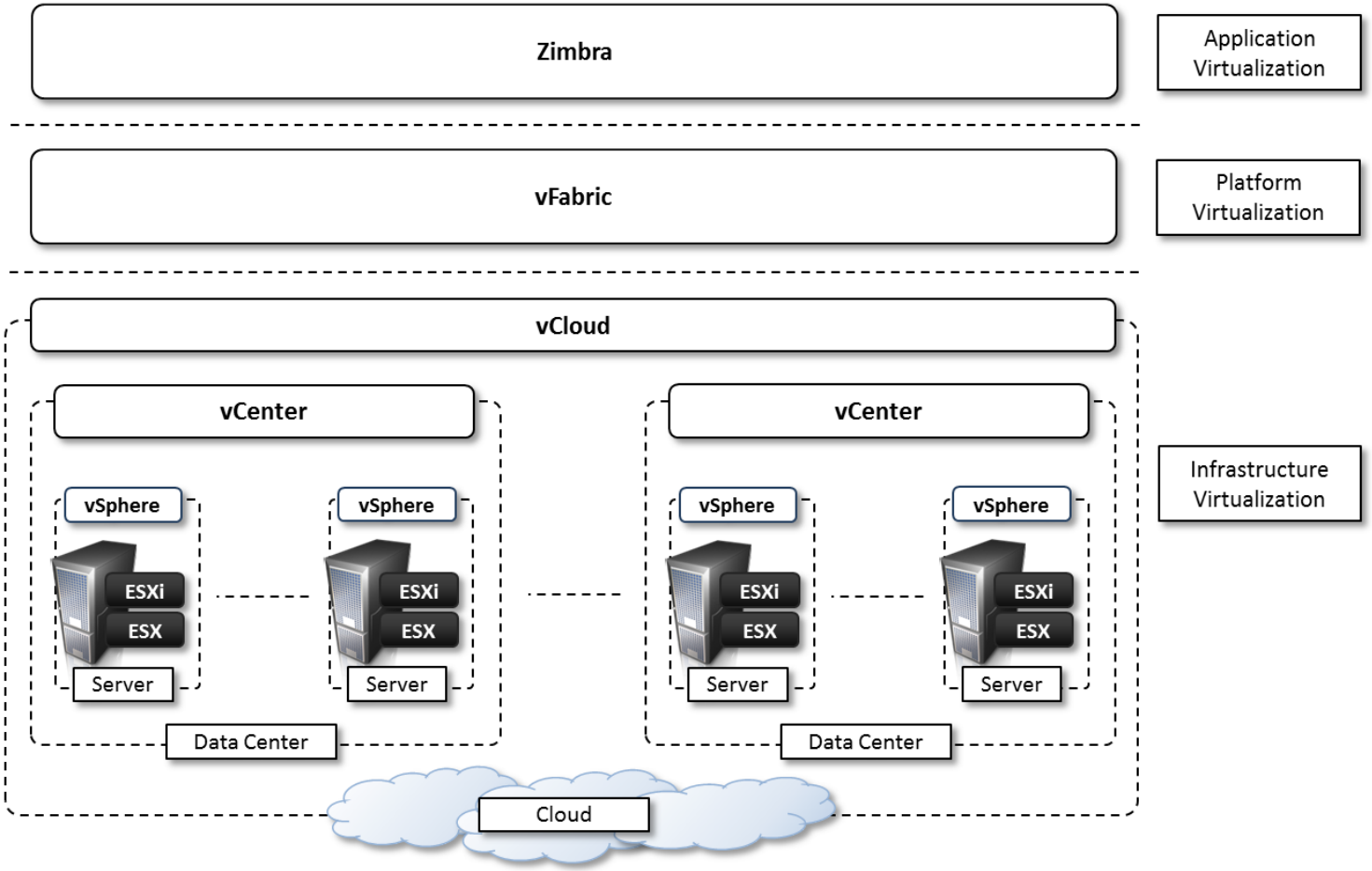
VMware: full virtualization

- Virtualization solutions
  - Server virtualization



VMware: full virtualization

- Virtualization solutions
  - Infrastructure virtualization and cloud computing solutions



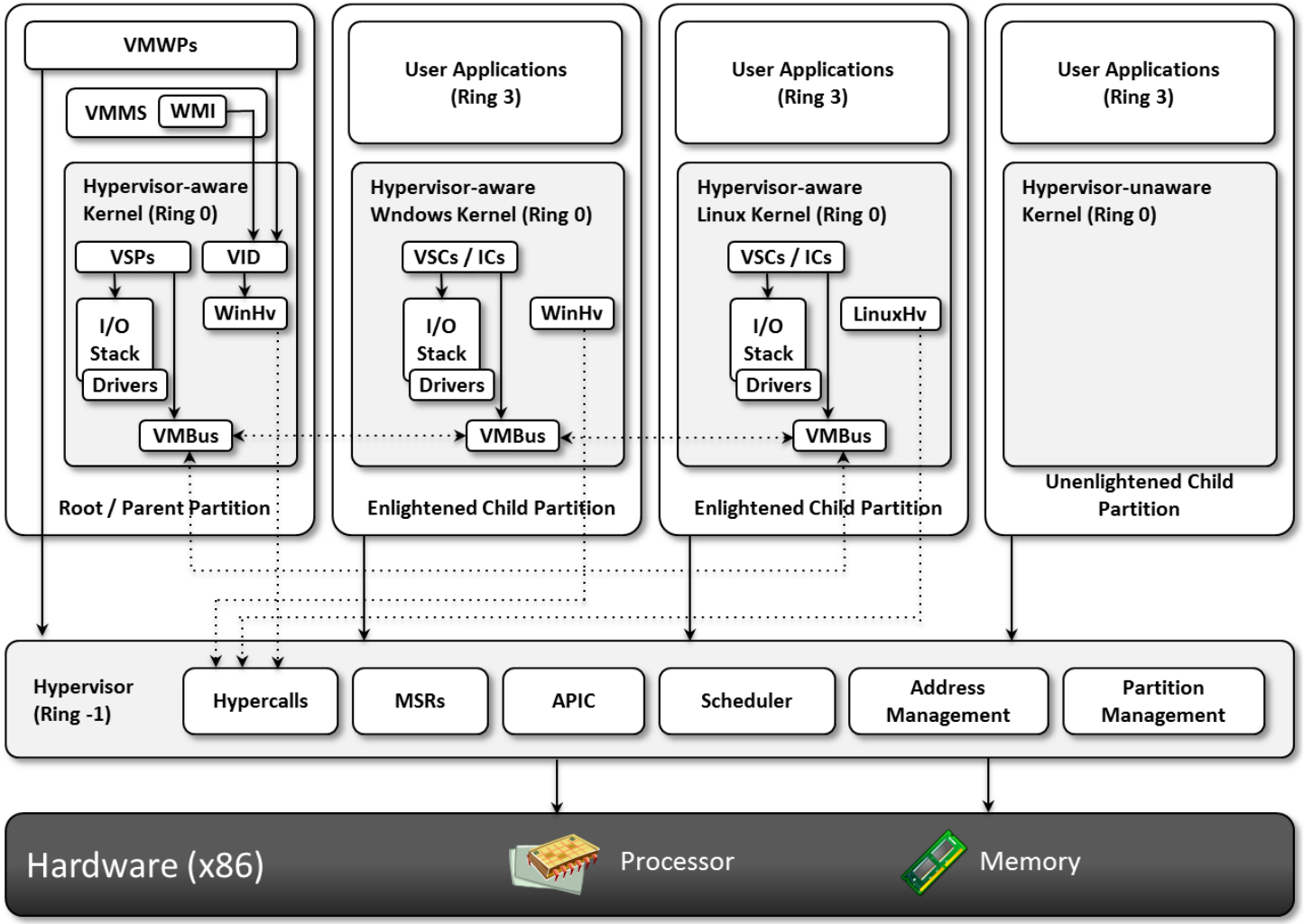
VMware: full virtualization

Observations

- Starts with a solution for fully virtualized x86 hardware.
- Now provides a complete offering for virtualizing hardware, infrastructure, applications, and services, thus covering every segment of the cloud computing market.

Microsoft Hyper-V

- **Architecture**



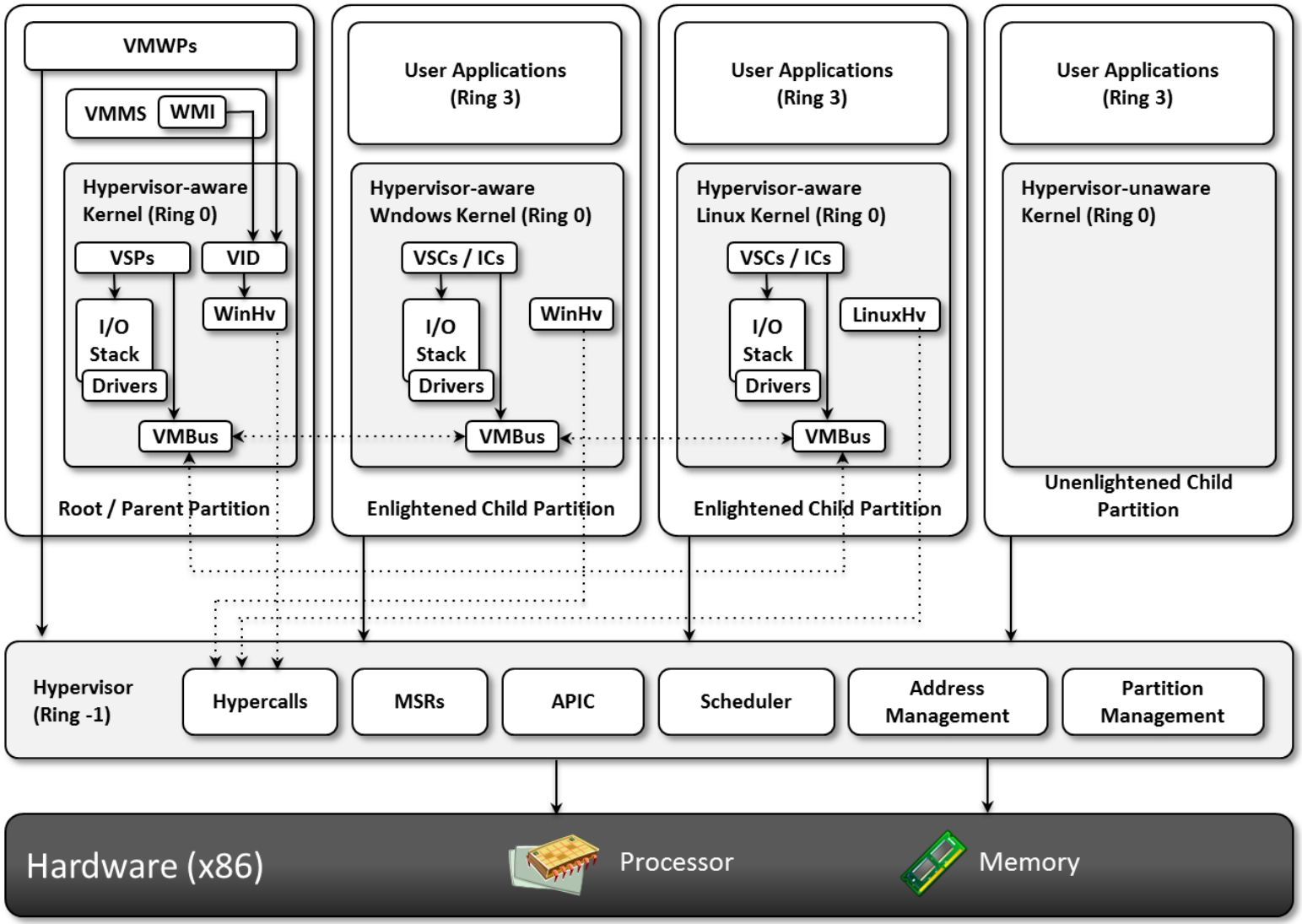
Microsoft Hyper-V

- **Hypervisor**
  - Hypercalls interface
  - Memory service routines(MSRs)
  - Advanced programmable interrupt controller(APIC)
  - Scheduler
  - Address manager
  - Partition manager

Microsoft Hyper-V

- Enlightened I/O and synthetic devices
- Provides an optimized way to perform I/O operations.
- Allows guest operating systems to leverage an interpartition communication channel.

Microsoft Hyper-V



Microsoft Hyper-V

- **Parent partition**
- Executes the host operating system.
- Implements the virtualization stack that complements the activity of the hypervisor.
- Manages the creation, execution, and destruction of child partitions.

Microsoft Hyper-V

- **Child partition**
- Executes guest operating systems.

Types:

- Enlightened
- Unenlightene

Cloud computing and infrastructure management

- Hyper-V constitutes the basic building block of Microsoft virtualization infrastructure.
- Windows Server 2008 (Windows Server Core) - a reduced set of features and a smaller footprint of OS.
- System Center Virtual Machine Manager (SCVMM) 2008:

- Management portal for the creation and management of virtual instances
- Virtual to Virtual (V2V) and Physical to Virtual (P2V) conversions
- Delegated administration
- Library functionality and deep PowerShell integration
- Intelligent placement of virtual machines in the managed environment
- Host capacity management

Observations

- Hyper-V is a hybrid solution - both paravirtualization techniques and full hardware virtualization.
- The basic architecture of the hypervisor is based on paravirtualized architecture.
- Xen hypervisor - installed on bare hardware and filters all the access to the underlying hardware.
- Hyper-V - installed as a role in the existing operating system.

Observations

- Advantages of Hyper-V:
- Flexible virtualization platform supporting a wide range of guest operating systems.
- Disadvantages of Hyper-V:
- Compatibility issue.
- Processor support.
- Installed on an existing OS.