VIRTUALIZATION TECHNIQUES & TYPES

MOHANA MURALI GURUNATHAN

AGENDA

Virtualization

Types of Virtualization

How does Virtualization help Cloud providers

Issues & Challenges

NFV - VNF

VIRTUALIZATION

Foundational technology in cloud computing

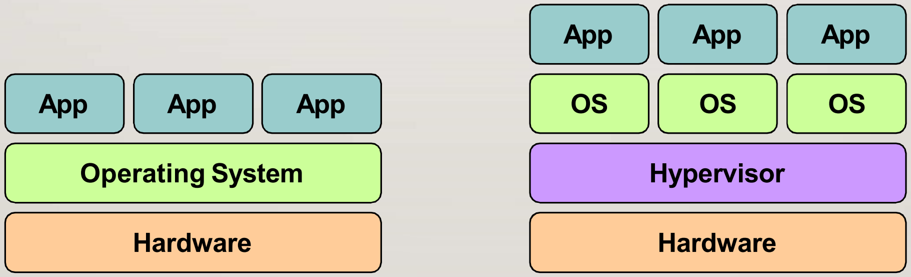
Involves creating a virtual version of something

- Operating System
- Server
- Storage device
- Network resources

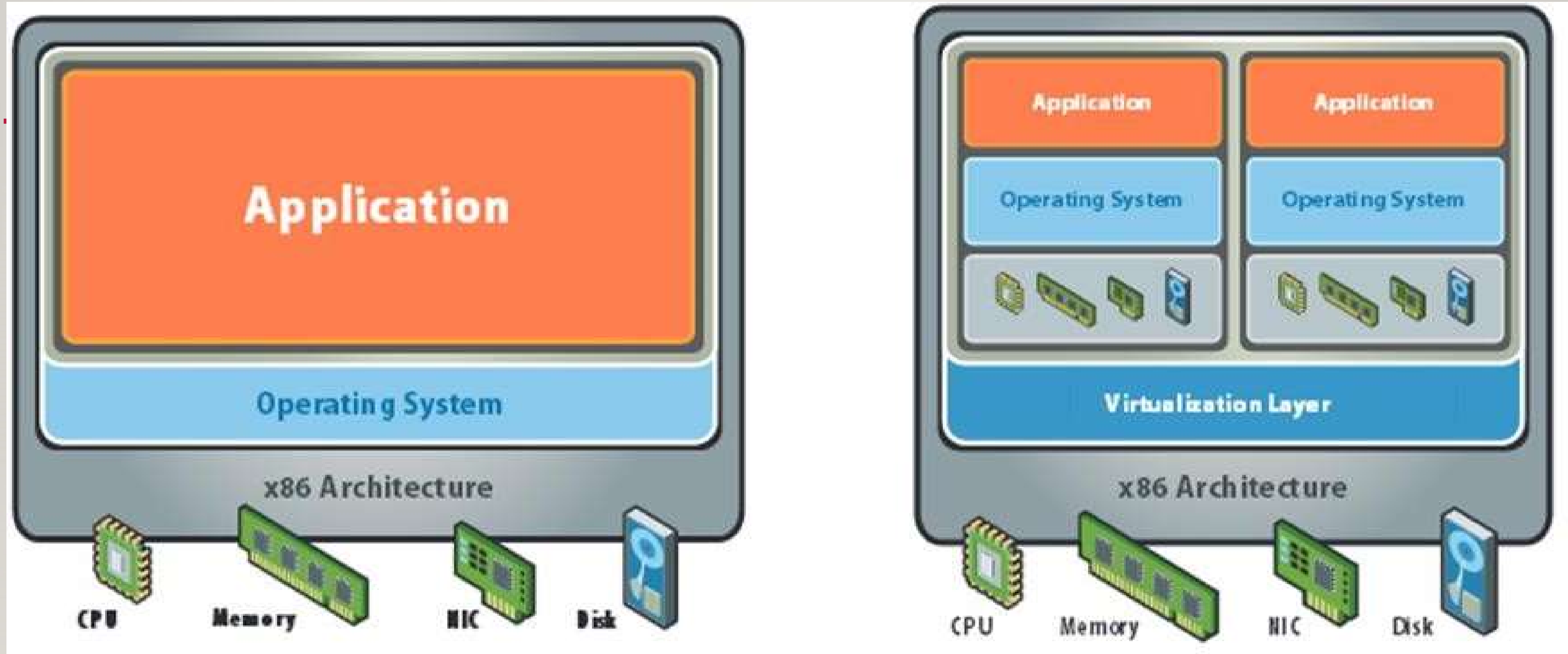
Achieved by using software to simulate hardware functionality and create a virtual computer system.

- Foundation
- Abstraction

Key Technology is Virtualization



Virtualization plays an important role as an enabling technology for datacentre implementation by abstracting compute, network, and storage service platforms from the underlying physical hardware


Application
Operating System
x86 Architecture
CPU
Memory
NIC
Disk
Application
Application
Operating System
Operating System
Virtualization Layer
x86 Architecture
CPU
Memory
NIC
Disk

WHAT DOES VIRTUALIZATION DO?

- Virtualization allows multiple operating system instances to run concurrently on a single computer
- It is a means of separating hardware from a single operating system.
- Each “guest” OS is managed by a Virtual Machine Monitor (VMM) also known as a hypervisor.
- Because the virtualization system sits between the guest and the hardware, it can control the guests’ use of CPU, memory, and storage, even allowing a guest OS to migrate from one machine to another.
- Instead of purchasing and maintaining an entire computer for one application, each application can be given its own operating system, and all those operating systems can reside on a single piece of hardware.
- Virtualization allows an operator to control a guest operating system’s use of CPU, memory, storage, and other resources, so each guest receives only the resources that it needs.

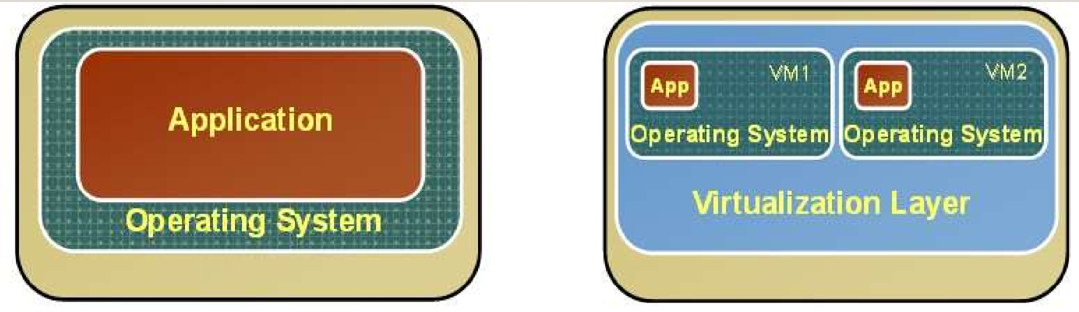
CHANGES AFTER VIRTUALIZATION

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

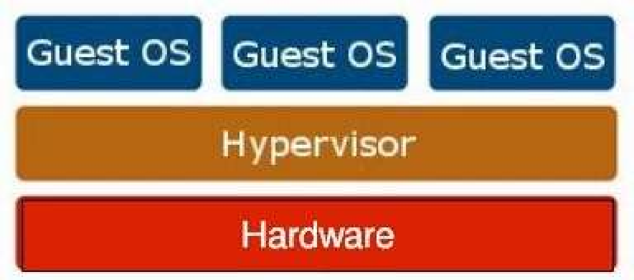
After Virtualization

- 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



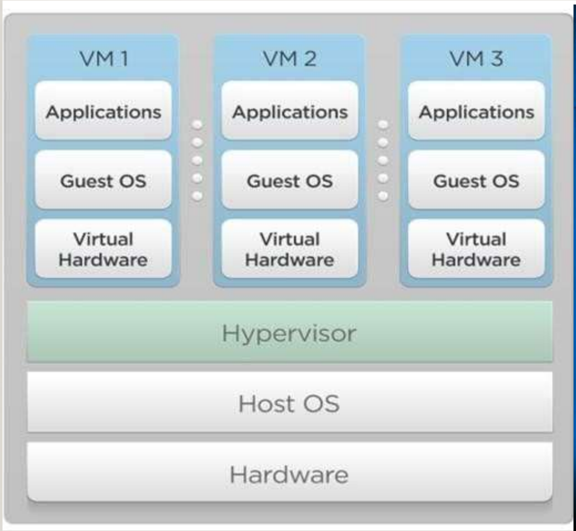
VIRTUALIZATIONARCHITECTURE

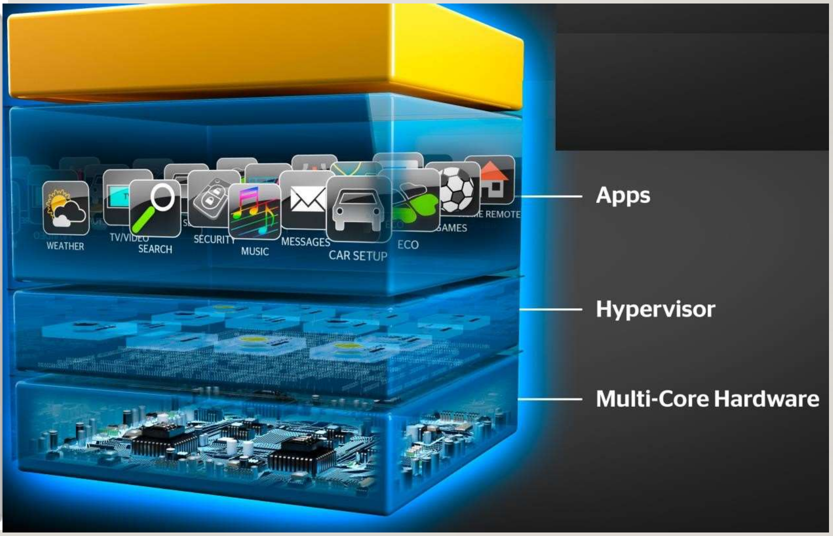
- Guest OS assumes complete control of the underlying hardware.
- Virtualization architecture provides this illusion through a hypervisor/VMM.
- Hypervisor/VMM is a software layer which:
  - Allows multiple Guest OS (Virtual Machines) to run simultaneously on a single physical host
  - Provides hardware abstraction to the running Guest OS' and efficiently multiplexes underlying hardware resources



HYPERVISOR – BARE METAL & HOSTED

Bare-metal hypervisor: Runs directly on the physical hardware without an underlying operating system.
Hosted hypervisor: Runs on top of an operating system, which in turn runs on the physical hardware.

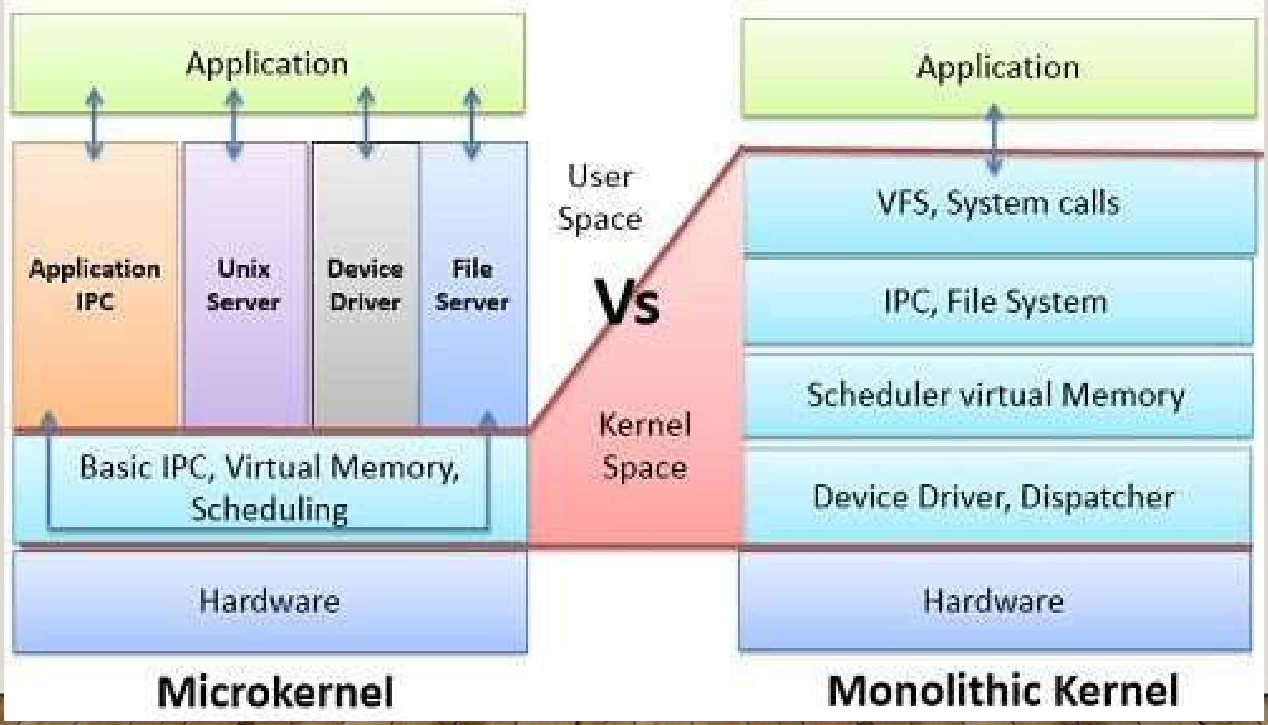




HYPERVISOR DESIGN GOALS

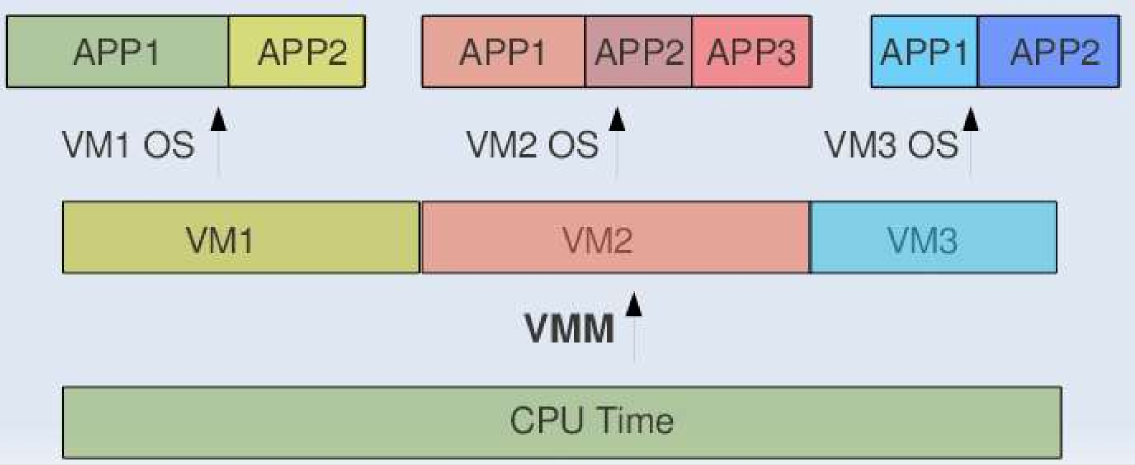
- Isolation
  - Security isolation
  - Fault isolation
  - Resource isolation
- Reliability
  - Minimal code base
  - Strictly layered design
  - Not extensible
- Scalability
  - Scale to large number of cores
  - Large memory systems

HYPERVISOR MONOLITHIC VERSUS MICROKERNELIZED



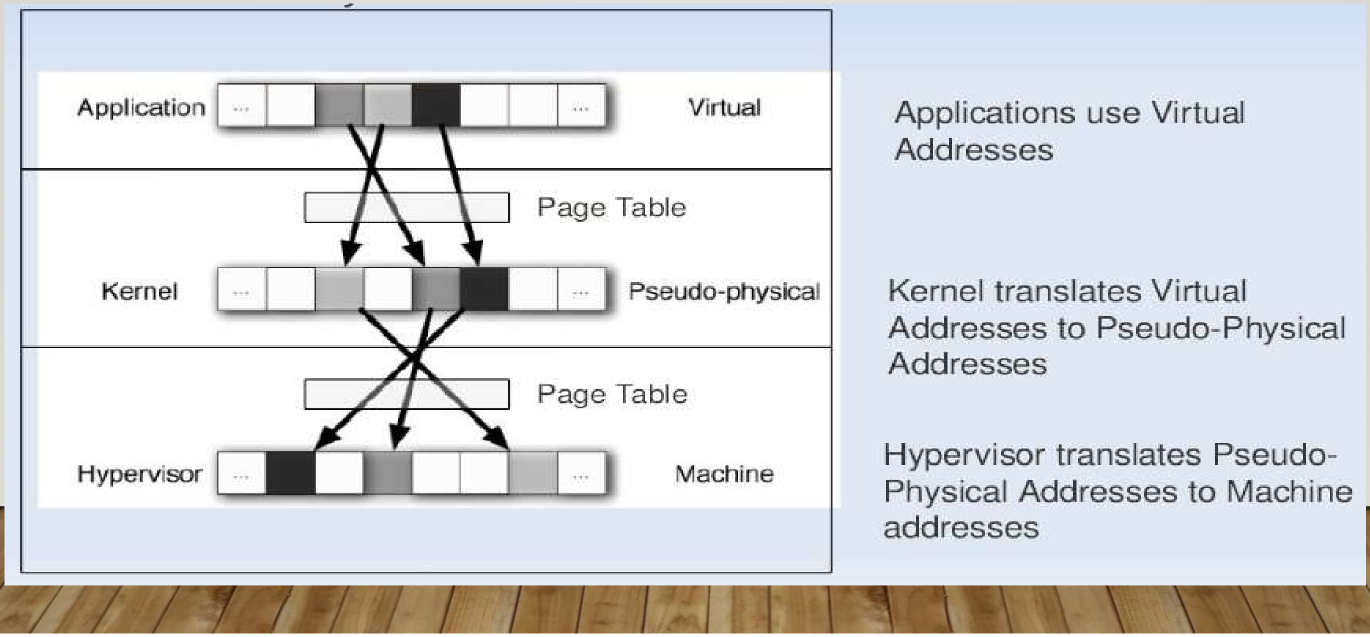
CPU SHARING

- VMM or Hypervisor provides a virtual view of CPU to VMs.
- In multi processing, CPU is alloted to the different processes in form of time slices by the OS.
- Similarly VMM or Hypervisor allots CPU to different VMs.



MEMORY SHARING

- In Multiprogramming there is a single level of indirection maintained by Kernel.
- In case of Virtual Machines there is one more level of indirection maintained by VMM



Applications use Virtual Addresses

Kernel translates Virtual Addresses to Pseudo-Physical Addresses

Hypervisor translates Pseudo-Physical Addresses to Machine addresses

IO SHARING

- Direct I/O (DIO)

Direct access: Allows the guest operating system to access I/O devices directly, bypassing the hypervisor.
Performance: This can improve performance, especially for I/O-intensive workloads.
Security: Requires careful management to prevent security risks

- Pass-through:

Dedicated device: Assigns a physical I/O device exclusively to a single VM.
High performance: Ideal for VMs with specific I/O requirements, like high-performance computing or real-time applications.
Limited flexibility: Reduces the flexibility of resource allocation.

IO SHARING

- Shared I/O

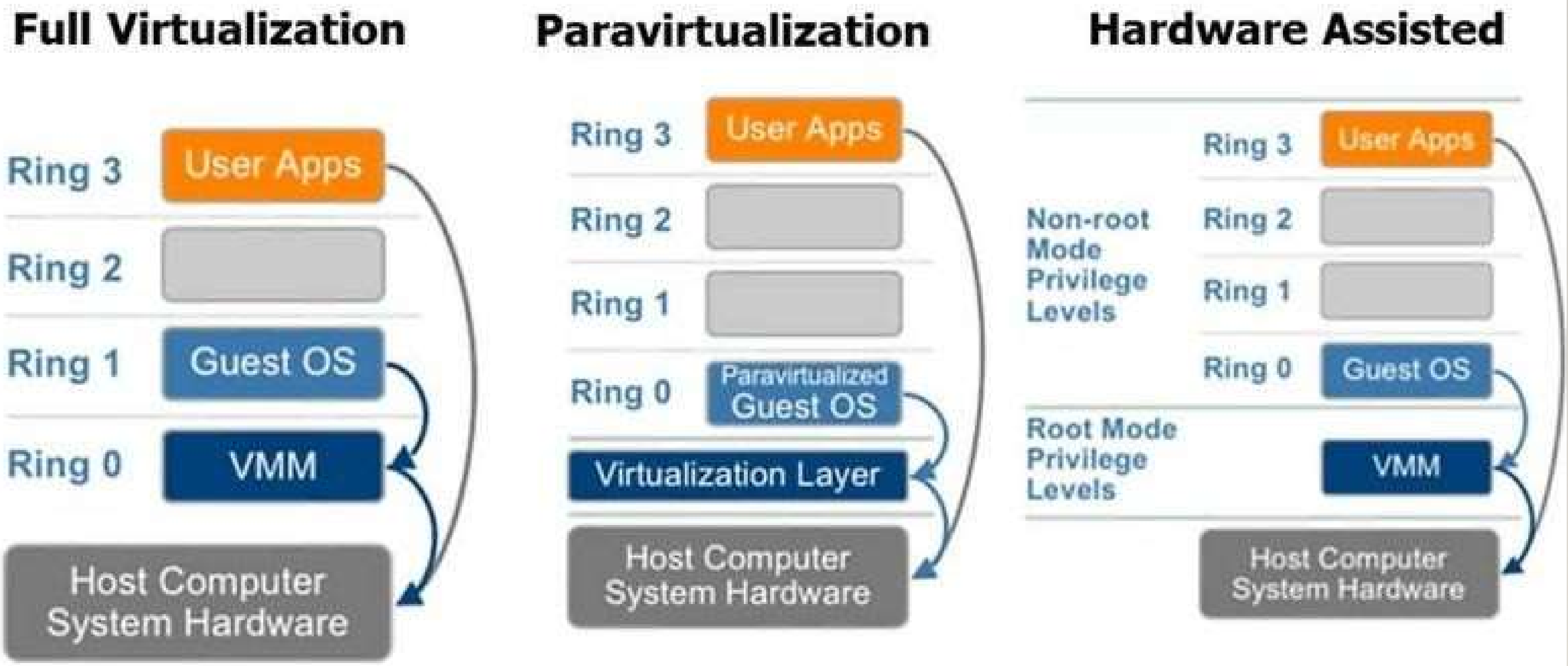
Multiple VMs: Multiple VMs sharing a single I/O device.
Resource management: Hypervisor manages access to the shared device. Ensures fair allocation & conflicts.
Performance trade-offs: Performance overhead when there are resource contentions**.**

- Virtual I/O Device

•**Emulated devices:** Creates virtual I/O devices that are presented to the VMs as physical devices.
•**Flexibility:** Offers greater flexibility in resource allocation and management.
•**Performance:** May have some performance overhead compared to direct I/O

- **Paravirtualization** is virtualization in which the guest operating system (the one being virtualized) is aware that it is a guest and accordingly has drivers that, instead of issuing hardware commands, simply issue commands directly to the host operating system. This also includes memory and thread management as well, which usually require unavailable privileged instructions in the processor.
- **Full Virtualization** is virtualization in which the guest operating system is unaware that it is in a virtualized environment, and therefore hardware is virtualized by the host operating system so that the guest can issue commands to what it thinks is actual hardware, but really are just simulated hardware devices created by the host.
- **Hardware-Assisted Virtualization** is a type of Full Virtualization where the microprocessor architecture has special instructions to aid the virtualization of hardware. These instructions might allow a virtual context to be setup so that the guest can execute privileged instructions directly on the processor without affecting the host. Such a feature set is often called a Hypervisor.

Architectural Comparison



Full Virtualization

Ring 3 User Apps

Ring 2

Ring 1 Guest OS

Ring 0 VMM

Host Computer System Hardware

Paravirtualization

Ring 3 User Apps

Ring 2

Ring 1

Ring 0 Paravirtualized Guest OS

Virtualization Layer

Host Computer System Hardware

Hardware Assisted

Non-root Mode Privilege Levels

Ring 3 User Apps

Ring 2

Ring 1

Ring 0 Guest OS

Root Mode Privilege Levels

VMM

Host Computer System Hardware

HARDWARE & SOFTWARE VIRTUALIZATION

Techniques used to create multiple virtual environments on a single physical system.

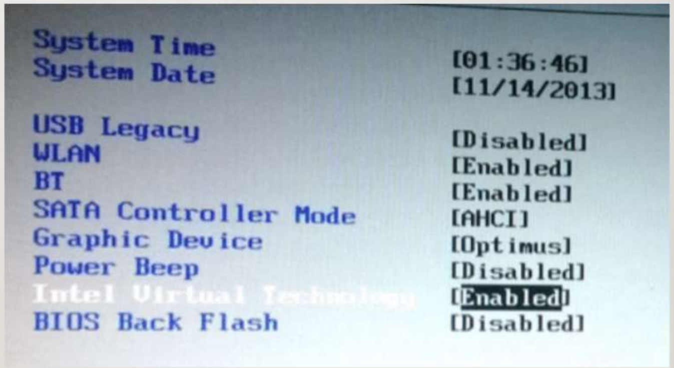
Differ in their underlying mechanisms and applications.

- Mechanism
- Performance
- Flexibility
- Cost

HARDWARE VIRTUALIZATION

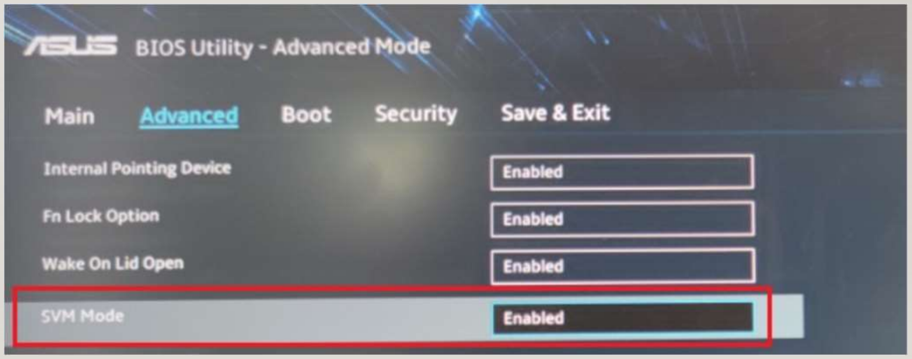
Mechanism: Computer Hardware directly supports the creation of multiple virtual machines. The processor itself provides the capability to run multiple operating systems simultaneously.

Examples: Intel VT-x and AMD-V are examples of hardware virtualization technologies. These technologies allow a physical CPU to emulate multiple virtual CPUs.



```
System Time                              [01:36:46]
System Date                              [11/14/2013]

USB Legacy                               [Disabled]
WLAN                                     [Enabled]
BT                                       [Enabled]
SATA Controller Mode                     [AHCI]
Graphic Device                           [Optimus]
Power Beep                               [Disabled]
Intel Virtual Technology                 [Enabled]
BIOS Back Flash                          [Disabled]
```



```
Internal Pointing Device        Enabled
Fn Lock Option                  Enabled
Wake On Lid Open                Enabled
SVM Mode                        Enabled
```

Many ways to enable the virtualization – Secure Virtual Machine setting or Virtual Tech setting

SOFTWARE VIRTUALIZATION

Mechanism: Software creates the illusion of multiple virtual machines. A hypervisor, a special type of software, manages the allocation of resources like CPU, memory, and storage to each virtual machine.

Example: VMware, VirtualBox, and Hyper-V are popular software virtualization platforms. They use software techniques to divide a physical computer's resources among multiple virtual machines.

HARDWARE & SOFTWARE VIRTUALIZATION

	Hardware Virtualization	Software Virtualization
Mechanism	Hardware-based	Software-based
Performance	Generally faster due to hardware support	Can be slower due to software overhead
Flexibility	Limited by hardware capabilities	More flexible due to software control
Cost	Requires hardware with virtualization support	Can be less expensive as it doesn't require specialized hardware

UseCase

Hardware Virtualization: Server consolidation, running multiple operating systems on a single physical server.

Software Virtualization: Desktop virtualization, providing virtual desktops to users, application testing, and cloud computing.

HOW DOES VIRTUALIZATION HELP CLOUD PROVIDERS?

Efficient Resource Utilization: When a VM is stopped in a Cloud like AWS, its resources, including CPU cores, memory and storage are deallocated.

These resources are then available for other VMs to use.

Preserving the State: While the resources are released, the state of the VM is preserved. This includes the operating system, applications, and data. This allows the VM to be started again quickly without having to reinstall everything.

The stopped VM retains its configuration and state, allowing it to be started again without losing any data.

This approach ensures that stopped VMs do not consume unnecessary resources while still preserving their state for future use.

Preserving the state of a VM is an internal mechanism to store configuration and Data.
This cannot be equated to/considered as image creation

HOW DOES VIRTUALIZATION HELP CLOUD PROVIDERS?

Server Consolidation: Multiple VMs in one single physical server – reduce hardware costs, energy efficiency

Scalable and Flexible

Rapid provisioning : Quick creation and deletion of VMs based on demand
Customization: Wide range of VM configurations

Cost Effectiveness : Pay-as-you-go, Reduced CapEx

Mutli Tenancy, Disaster Recovery (backing up and storing VMs)

List can go further like … virtual environment for Dev Team for dev and test purposes → reduces time to market

ISSUES & CHALLENGES

Performance Overhead: Hypervisor overhead, resource contention

Security Concerns

Management Complexity

Licensing & Costs

NFV & VNF

Network Functions Virtualization : NFV is a framework that enables network functions, traditionally implemented in hardware, to be run as software applications on general-purpose servers. This approach offers greater flexibility, scalability, and cost-effectiveness compared to traditional hardware-based network functions.

Focus: NFV focuses on the overall architecture and framework for deploying and managing virtualized network functions. It involves the separation of network functions from proprietary hardware and their deployment on a virtualized infrastructure.

Virtualized Network Functions : VNFs are individual network functions that have been virtualized. They are software applications that perform specific network functions, such as routing, switching, firewalling, or load balancing.

VNFs are an essential component of NFV. They are the building blocks that are deployed on virtualized infrastructure to create various network services.