SNS COLLEGE OF TECHNOLOGY
(An Autonomous Institution)
Re-accredited by NAAC with A+ grade, Accredited by NBA(CSE, IT, ECE, EEE & Mechanical)
Approvedy by AICTE, New Delhi, Recognized by UGC, Affiliated to Anna University, Chennai

Virtualization Structure

COURSE: **23C**AE717 - Cloud Computing

UNIT II **:** Virtualization

CLASS : II Semester / I MCA

Virtualization Structures

- Before virtualization, the operating system manages the hardware
- After virtualization, a virtualization layer is **inserted between the H/W and OS**
- In such a case, the virtualization layer is responsible for converting portions of the real hardware into virtual hardware
- Depending on the position of the virtualization layer, there are **several classes** of VM architectures

  1. Hypervisor

  2. Para-virtualization (depends on the implementation techniques)

  3. Host based virtualization (depends on the implementation techniques)

Hypervisor Architecture

- Hypervisor (virtualization layer) sits between **real hardware and OS**
- Hypervisor **provides hypercalls** for the guest OS and applications
- Hypervisor can assume a **micro-kernel architecture**
- Micro-kernel hypervisor includes only the basic and unchanging functions

XEN Architecture

- Xen is an **open source hypervisor** program by Cambridge University
- **Completely software based** and requires no special hardware support
- Xen hypervisor implements all the mechanisms, leaving the policy to be handled by Domain 0
- It just provides a mechanism by which a **guest OS can have direct access to the physical devices.**
- VMM, allows users to **dynamically instantiate** an operating system, like **Linux and Windows**
- **Multiple operating systems can run simultaneously and perform different tasks**

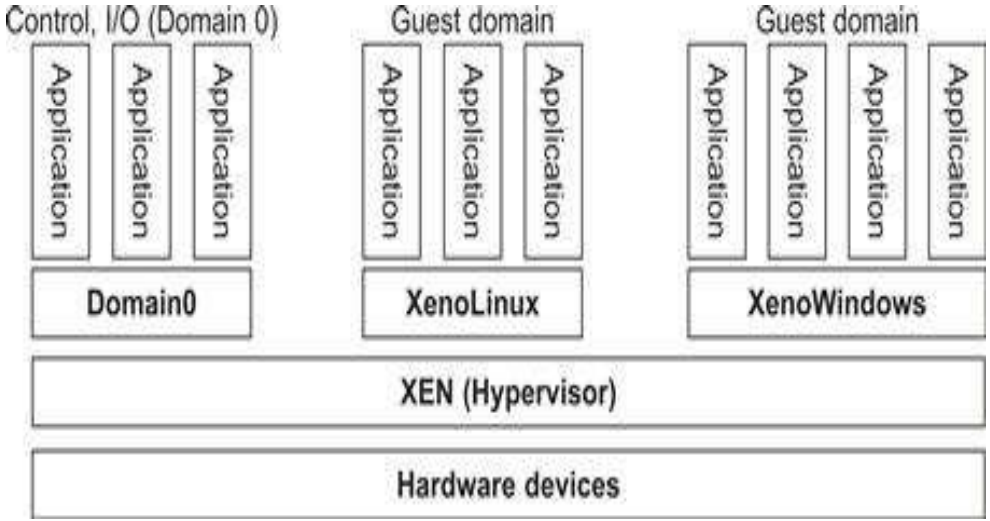
Hardware assisted CPU Virtualization

- Not all guest OSes are created equal, and one in particular controls the others
- Guest OS, **which has control ability, is called Domain 0**, and the others are called Domain
- Domain 0 is a privileged guest OS which is first loaded when Xen boots
- Uses para-virtualization to provide high performance and good resource isolation
  - The guest OS has to be modified to run on the Virtual Machine Monitor.
  - Specifically, the guest OS can no longer execute in ring 0, because that ring is now occupied by the VMM
  - The guest OS has to be modified to run outside of ring 0

XEN Architecture

Core components of a Xen system are

- Hypervisor
- Kernel
- Applications



XEN Architecture

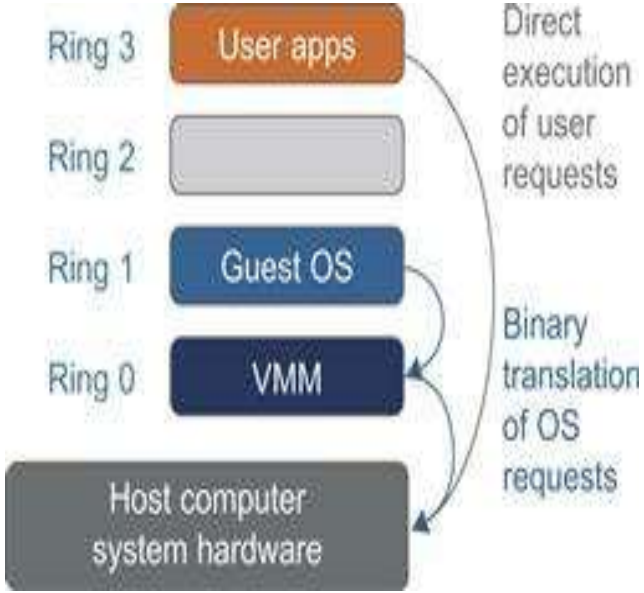
- Domain 0 is designed to **access hardware directly and manage devices.**
- So, one of the responsibilities of Domain 0 is to allocate and map hardware resources for the guest domains
- Domain 0, behaving as a VMM, allows users **to create, copy, save, read, modify, share, migrate, and roll back VMs** as easily as manipulating a file,
- If Domain 0 is compromised, the hacker can control the entire system. So, in the VM system, security policies are needed to improve the security of Domain 0

Binary Translation with Full Virtualization

- Depending on implementation technologies, hardware virtualization may be either full virtualization and host-based virtualization
- Full virtualization does not need to modify the host OS.
- It relies on binary translation to trap and to virtualize the execution of certain sensitive, non-virtualizable instructions
- noncritical instructions run on the hardware directly while critical instructions are discovered and replaced with traps into the VMM to be emulated by software

Host Based Virtualization

- VMM scans instruction stream and identifies the privileged, control and behavior-sensitive instructions
- When these instructions are identified, they are trapped into VMM, which emulates the behavior of these instructions.
- This method used in this emulation is called binary translation

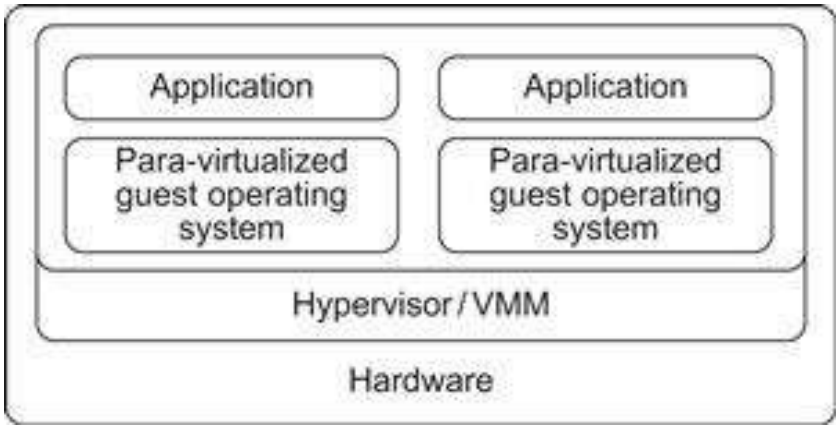


Host Based Virtualization

- Dedicated applications may run on the VMs.
- Certainly, some other applications can also run with the host OS directly
- Host-based architecture has flexibility

Para Virtualization

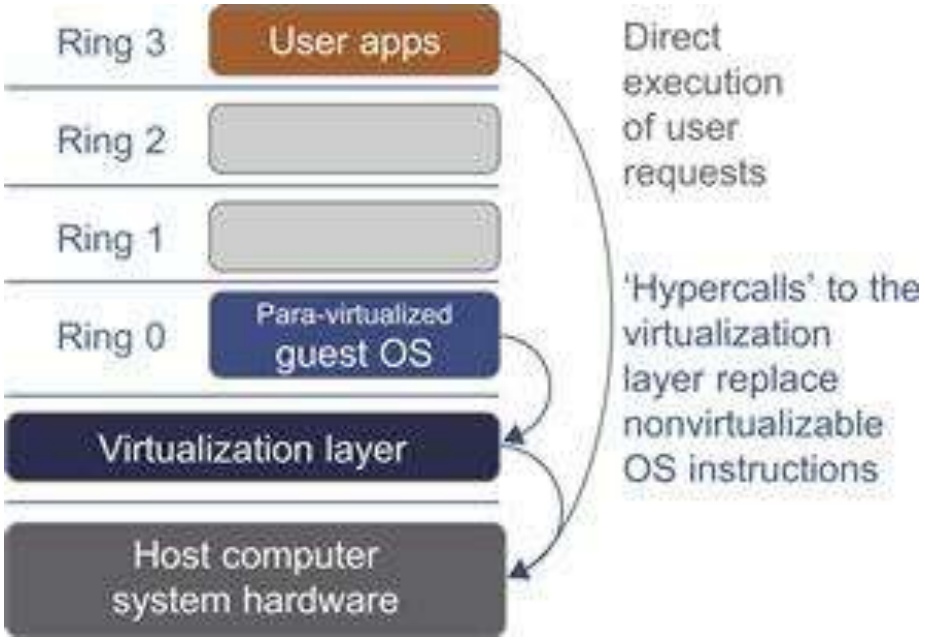
- Needs to modify the guest OS
- Para-virtualization attempts to reduce the virtualization overhead, and thus improve performance by modifying only the guest OS kernel



Para Virtualization

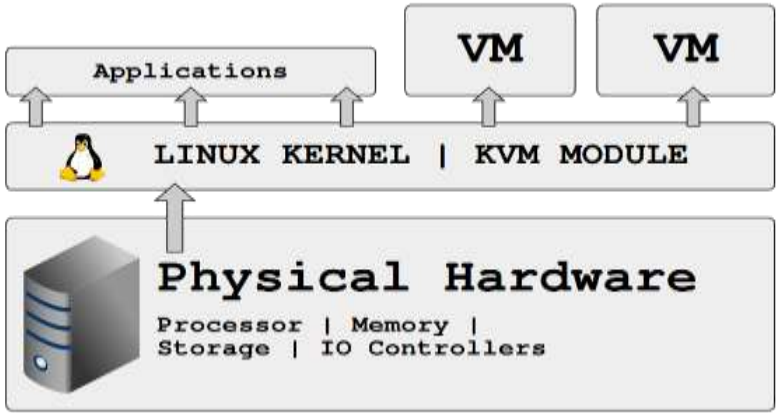
- The guest OSes are para-virtualized. They are assisted by an intelligent compiler to replace the non virtualizable OS instructions by hypercalls as illustrated
- traditional x86 processor offers four instruction execution rings: Rings 0, 1, 2, and 3
- The lower the ring number, the higher the privilege of instruction being executed. The OS is responsible for managing the hardware and the privileged instructions to execute at Ring 0, while user-level applications run at Ring 3

Para Virtualization

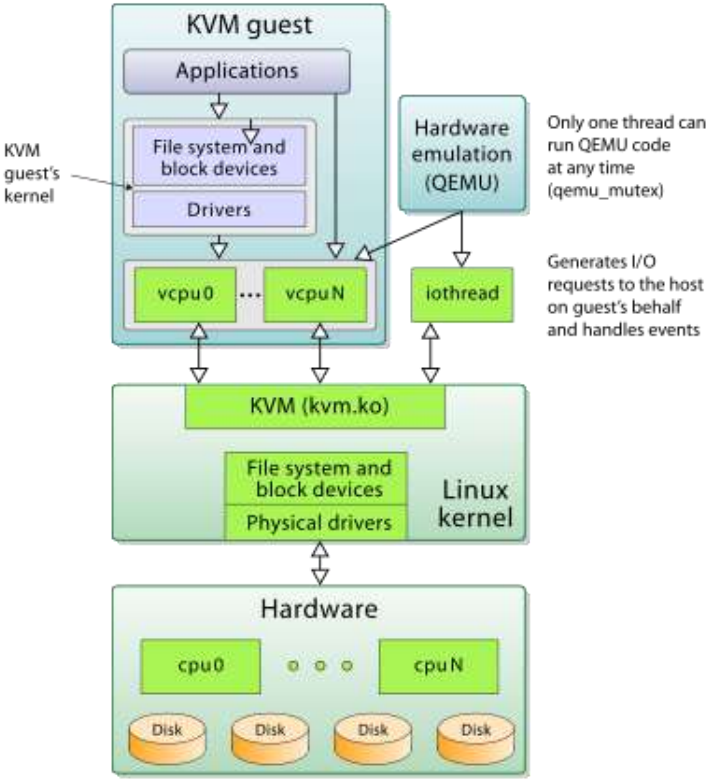


Kernel based Virtualization

- hardware-assisted, Linux para-virtualization system
- Memory management and scheduling activities are carried out by OS kernel
- hypervisor that controls the entire machine



Kernel based Virtualization



Para Virtualization with Compilation Support

- Para-virtualization handles these instructions at compile time.
- The guest OS kernel is modified to replace the privileged and sensitive
- Guest OS running at Ring 1 instead of at R 0.
- It implies that the guest OS may not be able to execute some privileged and sensitive instructions.
- The privileged instructions are implemented by hypercalls to the hypervisor

Para Virtualization with Compilation Support

- After replacing the instructions with hyper calls, the modified guest OS emulates the behavior of the original guest OS
- Drawbacks
  - compatibility and portability may be in doubt
  - maintaining para-virtualized OS is high, because of OS kernel modifications

References

- Kai Hwang, Geoffrey C Fox, Jack G Dongarra, “Distributed and Cloud Computing, From Parallel Processing to the Internet of Things”, Morgan Kaufmann Publishers, 2012
- James E. Smith, Ravi Nair, “Virtual Machines: Versatile Platforms for Systems and Processes”, Elsevier/Morgan Kaufmann, 2005.
- Kumar Saurabh, “Cloud Computing – insights into New-Era Infrastructure”, Wiley India,2011.
- Toby Velte, Anthony Velte, Robert Elsenpeter, “Cloud Computing, A Practical Approach”, TMH, 2009.
- John W.Rittinghouse and James F.Ransome, “Cloud Computing: Implementation, Management, and Security”, CRC Press, 201