Operating Systems

Chapter 6 Virtual Machines

Tien Pham Van, Dr. rer. nat.

Compiled with reference to other presentations

Outlines

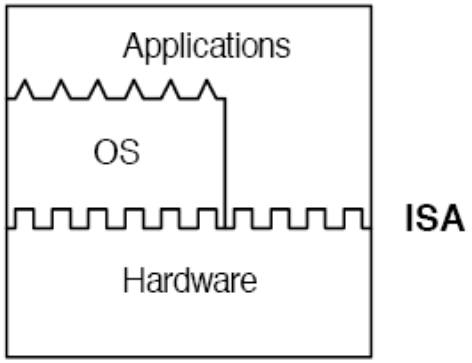
- Introduction
- Virtualization using hardware
- Software-based virtual machine
- Virtualization in clouds

Early Computers

- Hardware designed
  - Software written for hardware
- Each system crafted with own instruction set
  - Software had to made specifically for each instruction set
- Eventually instruction sets became more standardized
  - However, software still requires a certain instruction set architecture and operating system that meets strict standards.

Initial Hardware Model

- All applications access hardware resources (i.e. memory, i/o) through system calls to operating system (priviledge instructions)
- Advantages
  - Design is decoupled (i.e. OS people can develop OS separate of Hardware people developing hardware)
  - Hardware and software can be upgraded without notifying the Application programs
- Disadvantage
  - Application compiled on one ISA will not run on another ISA..
    - Applications compiled for Mac use different operating system calls then application designed for windows.
  - ISA's must support old software
    - Can often be inhibiting in terms of performance
  - Since software is developed separately from hardware.. Software is not necessarily optimized for hardware.



- Virtual machines are “an efficient, isolated duplicate of a real machine”

  -Popek and Goldberg

  Popek and Goldberg introduced conditions for computer architecture to efficiently support system virtualization.

Solution – *Virtual Machine*

- A virtual machine provides interface *identical* to underlying bare hardware
  - I.e., all devices, interrupts, memory, page tables, etc.
- Virtual Machine Operating System creates illusion of multiple processors
  - Each capable of executing independently
  - No sharing, except via network protocols

Virtual Machines

- The resources of the physical computer are shared to create the virtual machines
  - CPU scheduling can create the appearance that each user has own processor
  - Spooling and a file system provide
    - virtual card readers, virtual line printers
  - Disk partitioned to provide virtual disks
  - A normal user time-sharing terminal serves as the virtual machine operator's console

Definitions

- *Host Operating System:*
  - The operating system actually running on the hardware
  - Together with *virtualization layer*, it simulates environment for …
- *Guest Operating System:*
  - The operating system running in the simulated environment
  - E.g., the one we are trying to debug

Virtual Machines

- Virtual-machine concept provides complete protection of system resources
  - Each *virtual machine* is isolated from all other virtual machines.
  - However, no direct sharing of resources
- Virtual-machine system is a good vehicle for operating-systems research and development.
  - System development is done on the virtual machine does not disrupt normal operation
  - Multiple concurrent developers can work at same time
- The virtual machine concept is difficult to implement due to the effort required to provide an *exact duplicate* to the simulated machine

Overview

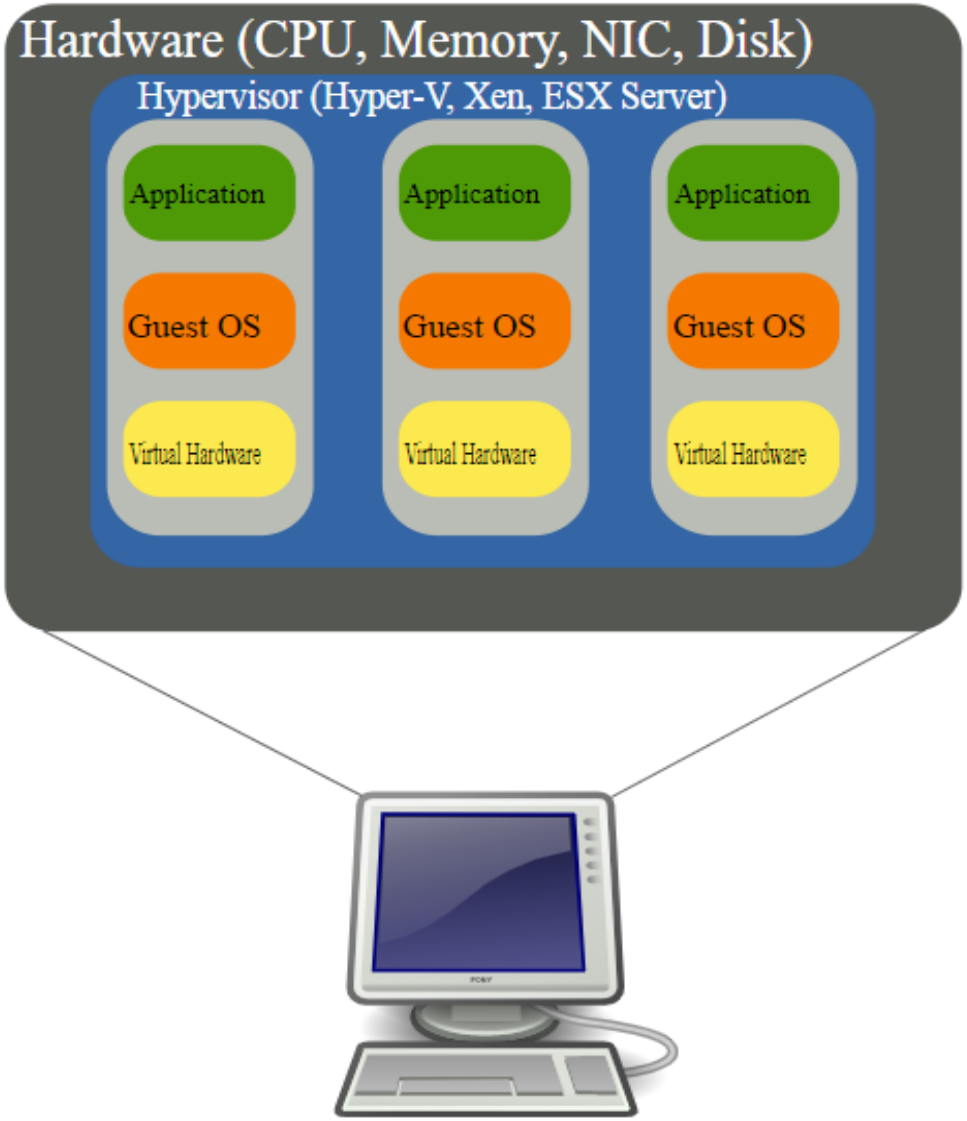
- What is Virtualization? – YouTube

https://www.youtube.com/watch?v=L8A9PHeyRrY

Kinds of VM

- System virtual machines (also termed full virtualization VMs) provide a substitute for a real machine. They provide functionality needed to execute entire operating systems
  - Example: VMWare, QEMU, VirtualBox
- Process virtual machines are designed to execute computer programs in a platform-independent environment
  - Example: Java Virtual Machine

Full Virtualization



Hardware virtualization

- Hardware virtualization is the virtualization of computers as complete hardware platforms, certain logical abstractions of their componentry, or only the functionality required to run various operating systems
- At its origins, the software that controlled virtualization was called a "control program", but the terms "hypervisor" or "virtual machine monitor" became preferred over time

Hardware virtualization

- Virtualization: VM and Hypervisor – YouTube

https://www.youtube.com/watch?v=ISwgVUPH1cs

Hardware-assisted virtualization

- The hardware provides architectural support that facilitates building a virtual machine monitor and allows guest OSs to be run in isolation
- In 2005 and 2006, Intel and AMD provided additional hardware to support virtualization. Sun Microsystems (now Oracle Corporation) added similar features in their UltraSPARC T-Series processors in 2005

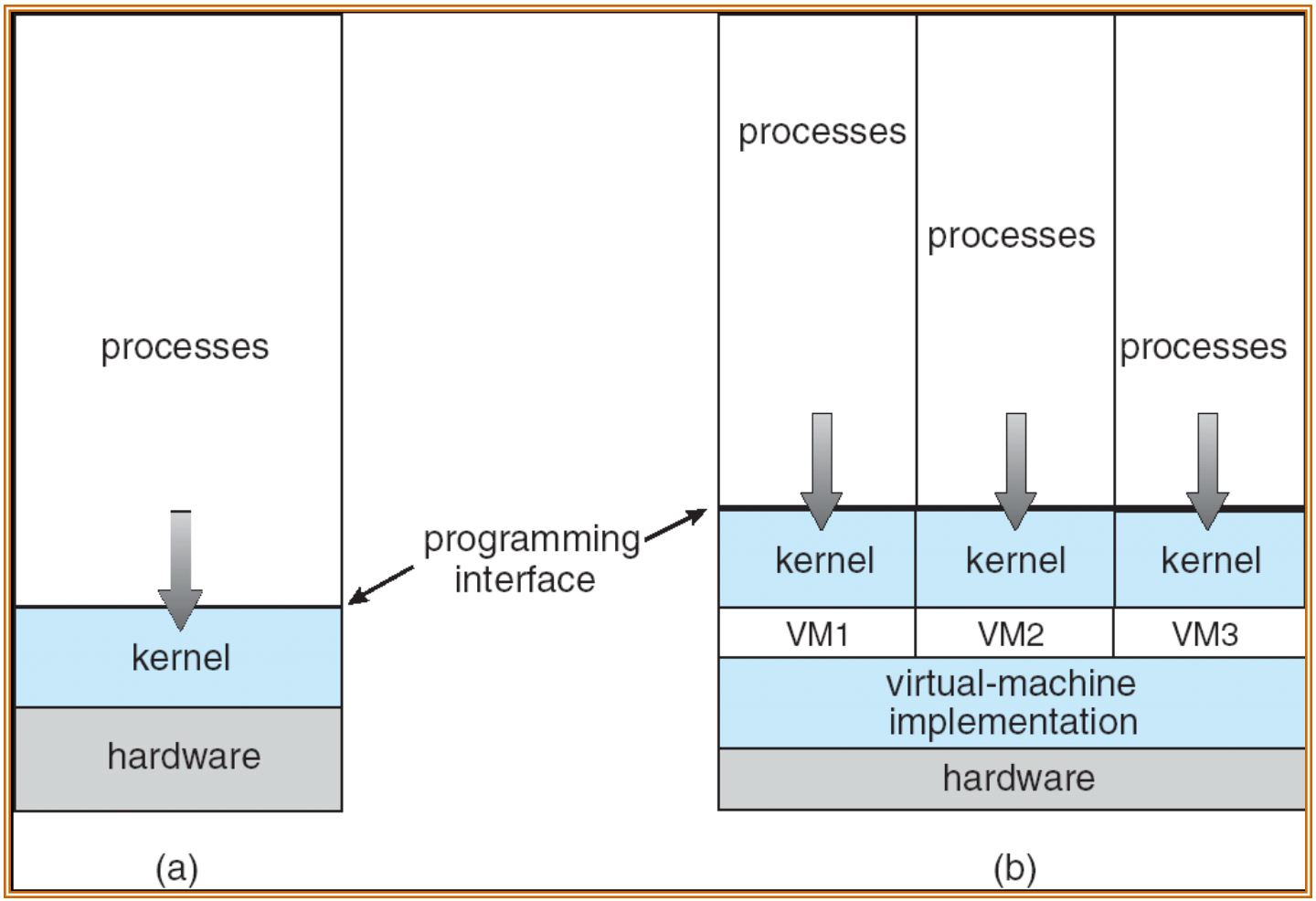
Paravirtualization

- The virtual machine does not necessarily simulate hardware, but offers a special API that can only be used by modifying the "guest" OS.
- It replaces sensitive instructions with calls to VMM APIs (e.g.: "cli" with "vm_handle_cli()"), then re-compiles the OS and use the new binaries

Operating System-level virtualization

- A physical server is virtualized at the operating system level, enabling multiple isolated and secure virtualized servers to run on a single physical server.
- The "guest" OS environments share the same running instance of the operating system as the host system. Thus, the same operating system kernel is also used to implement the "guest" environments, and applications running in a given "guest" environment view it as a stand-alone system.

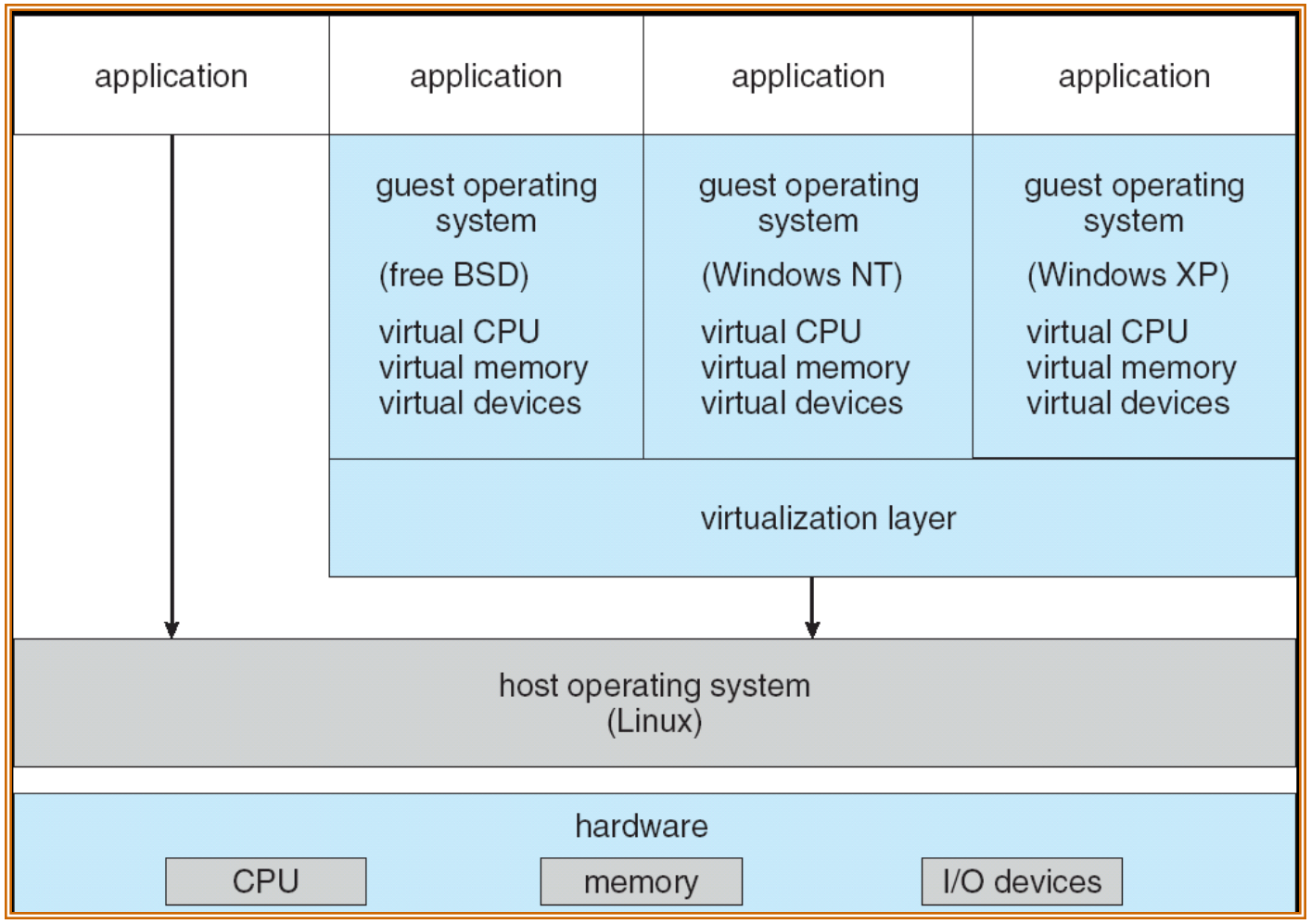
Conventional OS and VM OSs



VMware – Modern Virtual Machine System

- Founded 1998, Mendel Rosenblum *et al.*
  - Research at Stanford University
- *VMware Workstation*
  - Separates *Host OS* from *virtualization layer*
  - Host OS may be Windows, Linux, etc.
  - Wide variety of Guest operating systems
  - < $200

VMware Architecture



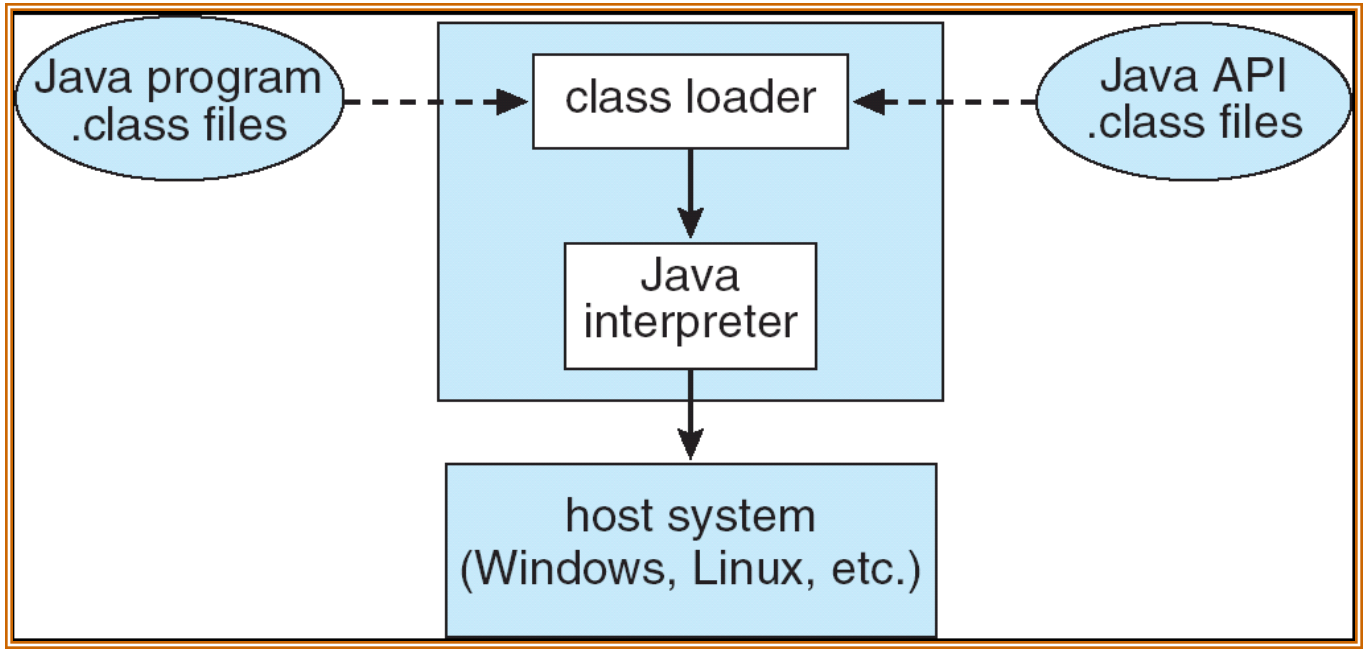
VMware Server

- Free version released in 2006
  - http://www.vmware.com/products/server/
  - Runs on any x86 server hardware and OS
  - Windows Server and Linux Host OS's
- Partition a physical server into multiple virtual server machines
  - Target market – IT centers providing multiple services
  - Allows separate virtual servers to be separately configured for separate IT applications
    - *Provisioning*
  - Portability, replication, etc.

VMware Server ESX

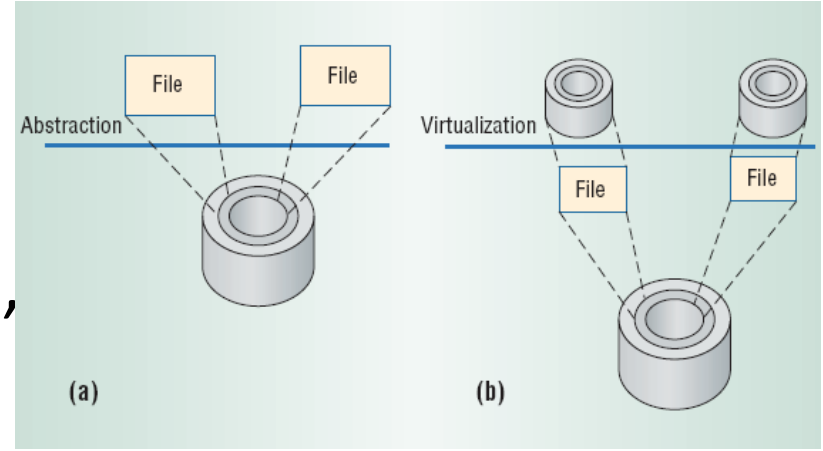
- Total decoupling between hardware and applications
- High-end, high-performance IT applications
  - Oracle, SQL Server, Microsoft Exchange server, SAP, Siebel, Lotus Notes, BEA WebLogic, Apache
- Dynamically move *running* application to different hardware
  - Maintenance, hardware replacement
  - Provisioning new versions, etc.

The Java Virtual Machine



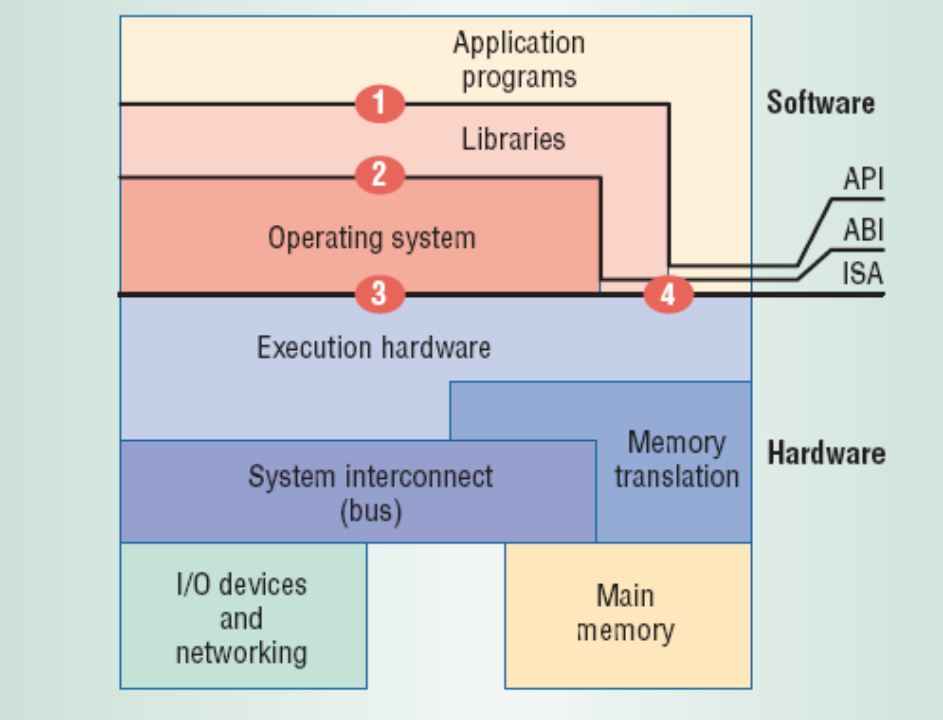
- Own idealized architecture
- Stylized machine language
  - *Byte codes*
- Readily available interpreter

- Computer architecture benefits from Abstraction
  - Well-defined interfaces for hardware and software to use
    - Hard Drives, Networking, I/O devices
  - Limits based on the hardware implementation
- Virtualization
  - Maps interfaces and resources to various hardware, even different architectures

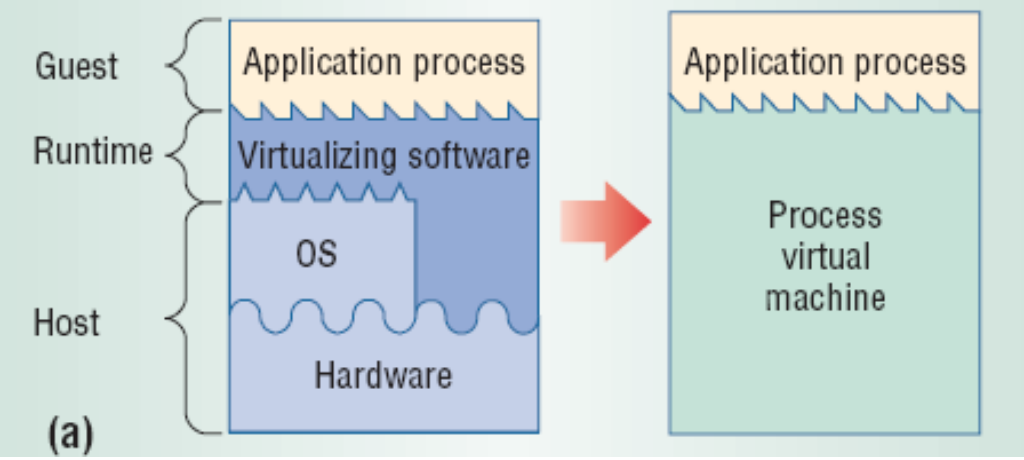


Architecture Interfaces

- Virtualization can take place at these junctures
  - ISA – Instruction Set Architecture
  - ABI – Application Binary Interface
  - API – Application Programming Interface



- Also known as Application VM
- Virtualization below the API or ABI, providing virtual resources to a single process executed on a machine
- Created for the process alone, destroyed when process finishes

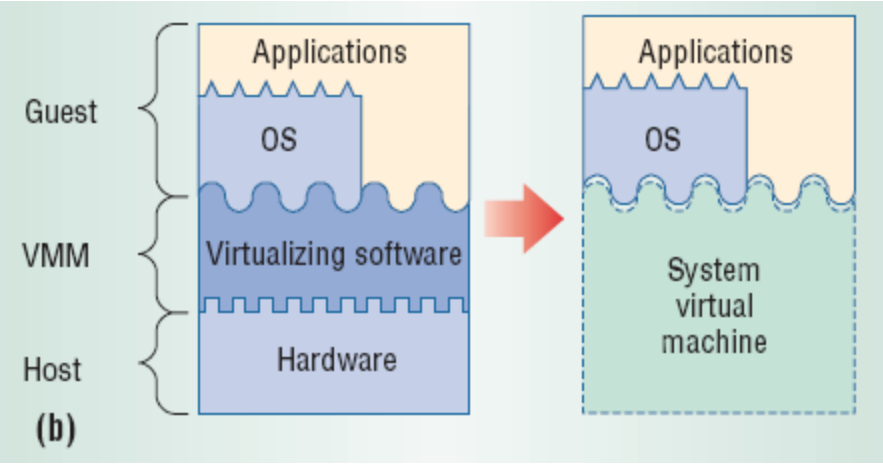


Process VM, continued

- Optimizers, Same ISA
  - Perform code optimization during translation and execution
- High-level-language VM
  - Cross-platform compatibility
  - Programs written for an abstract machine, which is mapped to real hardware through a virtual machine
    - Sun Microsystems Java VM
    - Microsoft Common Language Infrastructure, .NET framework

System Virtual Machines

- Virtualized hardware below the ISA
- Single host can run multiple isolated operating systems
  - Servers running different operating systems
  - Isolation between concurrent systems, security
- Hardware Managed by the VMM – Virtual Machine Manager

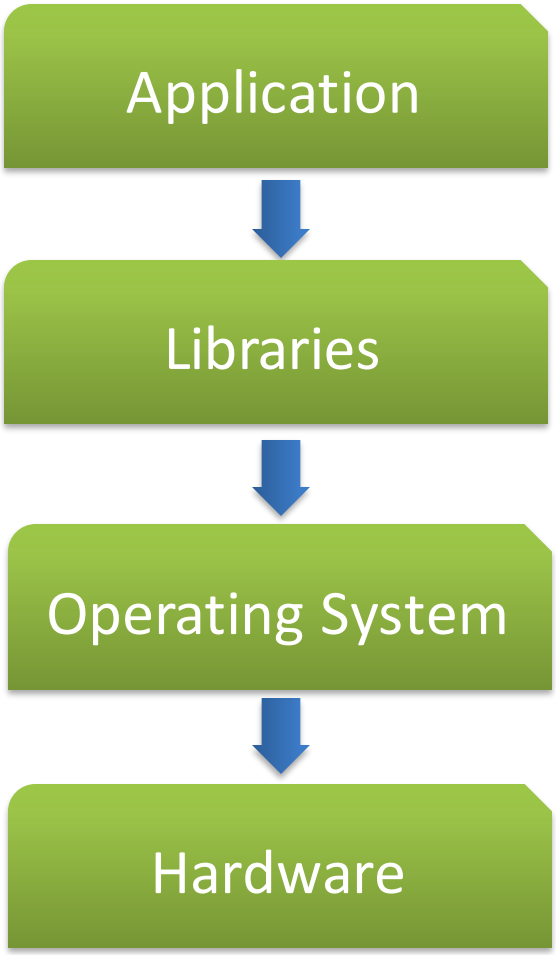


System VM, continued

- Classically, VMM runs on bare hardware, directly interacting with resources,
  - Intercepts and interprets guest OS actions
- Hosted VM
  - Installed application that relies on the OS to access hardware, using same ISA
- Whole System VM
  - Emulate both application and system code for different ISAs
    - Classically: Virtual PC, run windows on old Mac hardware

Virtualization for Cloud

Machine Stack showing virtualization opportunities



- Creation of a virtual version of hardware using software.
- Runs several applications at the same time on a single physical server by hosting each of them inside their own virtual machine.
- By running multiple virtual machines simultaneously, a physical server can be utilized efficiently.

Primary approaches to virtualization

- Platform virtualization Ex : Server
- Resources virtualization Ex : Storage, Network

- Virtualization in Cloud Computing | What is Virtualization | Intellipaat – YouTube

https://www.youtube.com/watch?v=_pPlanX5wQY