Virtualization

Providing a hardware-like view to each process

or

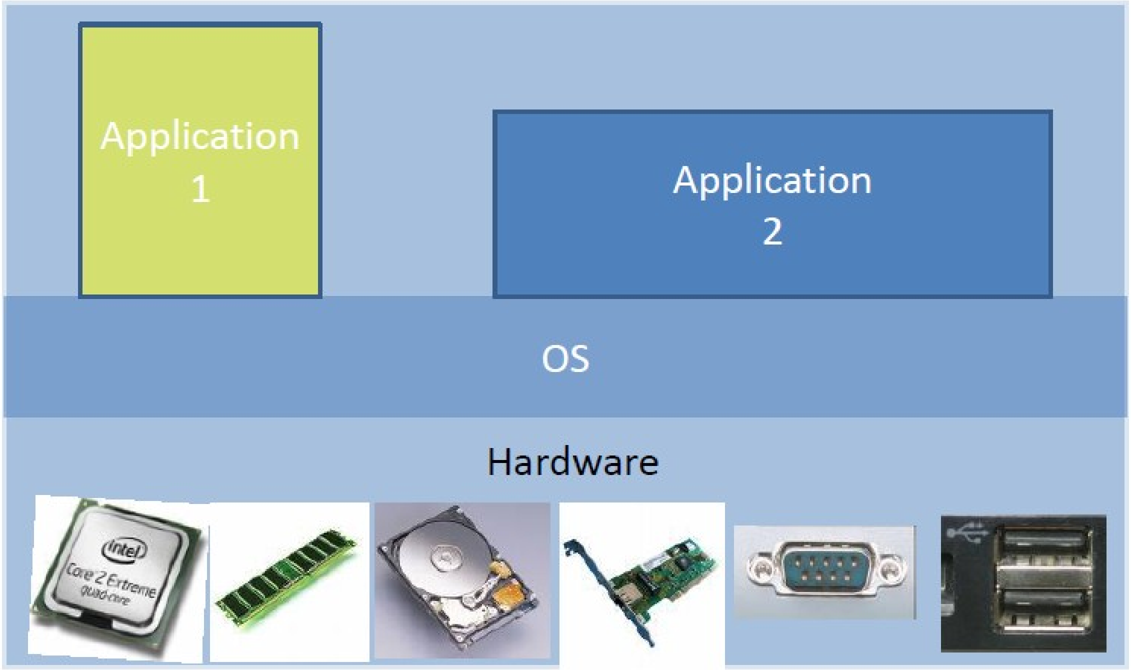
Running an OS inside another OS

or

Running multiple OSes on single physical hardware

Emulating a physical machine in software

Traditional Picture



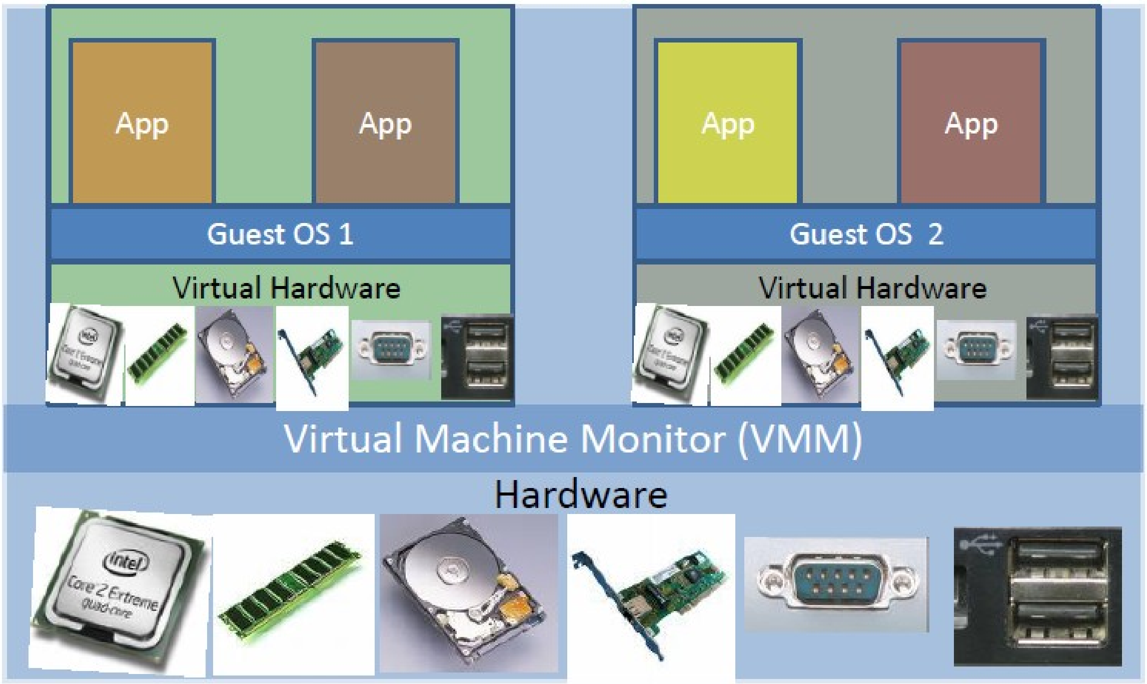
Application 1

Application 2

OS

Hardware

Virtualized Picture



Advantages of Virtualization

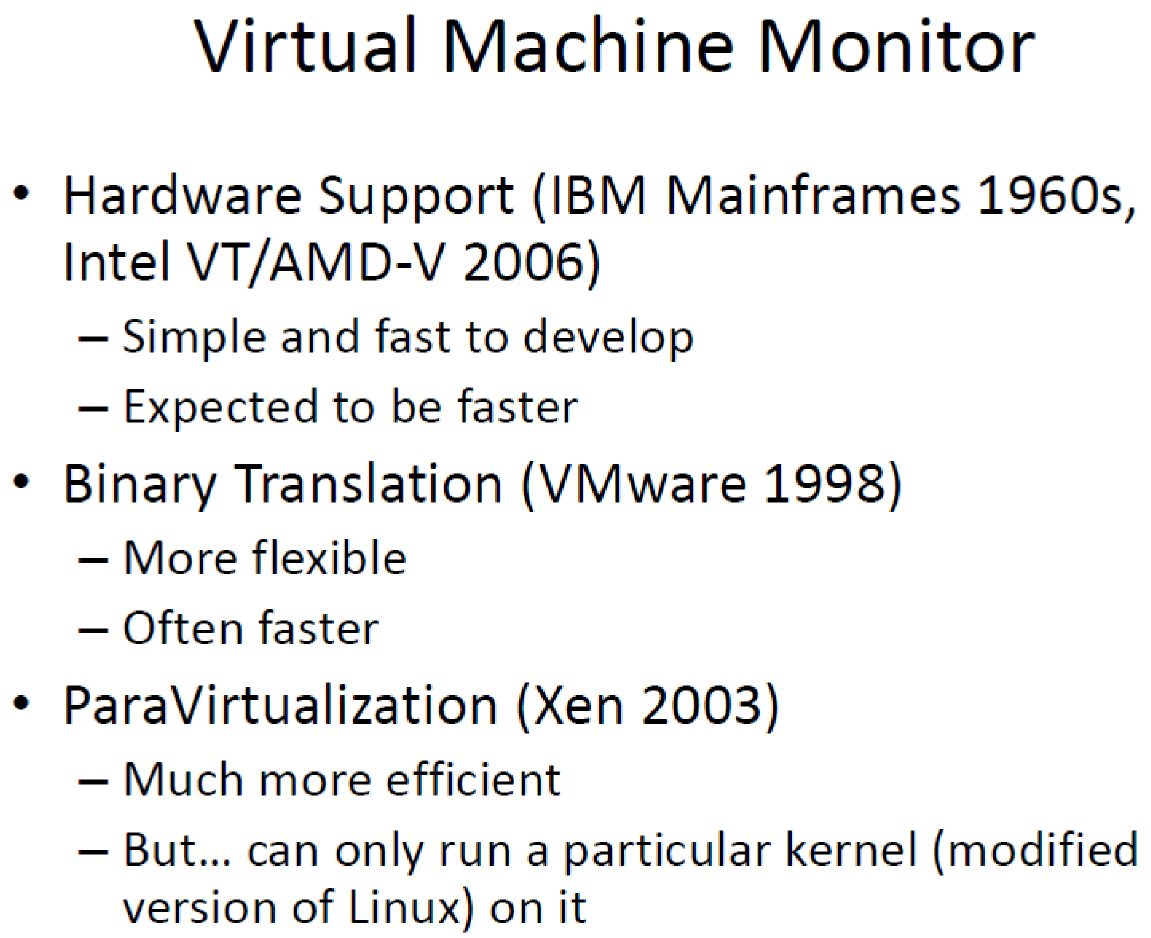
- Server consolidation
- Best of all worlds
  - e.g., run Windows and Linux simultaneously
- Complete isolation between applications
  - e.g., Internet VM and development VM (desktop)
  - e.g., Mail server VM and print server VM (server)
- Encapsulation (a VM is just a file)
  - e.g., snapshotting
- New Applications: Security, Reproducibility, Monitoring, Migration, Legacy systems, …

Virtual Machine Monitors

- [Popek, Goldberg 1974]
  - An architecture is virtualizable if the set of instructions that could affect the correct functioning of the VMM are a subset of the privileged instructions
    - i.e., all sensitive instructions must always pass control to the VMM

- x86 was not designed to be virtualizable
  - VMware Solution
    - Binary translate sensitive instructions to force them to trap into VMM
    - Most instructions execute identically

- Intel VT and AMD-V (2008)
  - Support for virtualization in hardware for x86
  - Obey the principles required to make hardware virtualizable
  - Hence, on modern machines, we no longer require binary translation



Virtual Machine Monitor

- Hardware Support (IBM Mainframes 1960s, Intel VT/AMD-V 2006)
  - Simple and fast to develop
  - Expected to be faster
- Binary Translation (VMware 1998)
  - More flexible
  - Often faster
- ParaVirtualization (Xen 2003)
  - Much more efficient
  - But… can only run a particular kernel (modified version of Linux) on it

Advantages of Virtualization • Server consolidation • Best of all worlds – e.g., run Windows and Linux simultaneously • Complete isolation between applications – e.g., Internet VM and development VM (desktop) – e.g., Mail server VM and print server VM (server) • Encapsulation (a VM is just a file) – e.g., snapshotting • New Applications: Security, Reproducibility, Monitoring, Migration, Legacy systems, …