CMPE 220

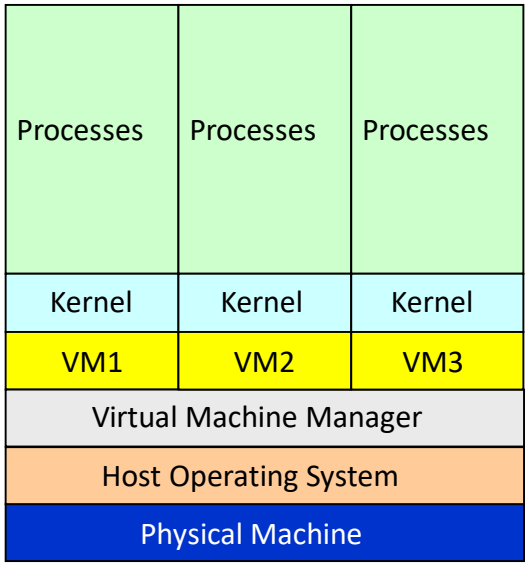
Class 19 – Virtual Systems

Virtual Systems

- A new(?) kind of system software

Virtual Machines

- Abstract the hardware of a single computer system.
- Create several different execution environments.
- Each environment can have its own operating system.
- Each environment believes it has the entire physical system.



Why VMs?

- Allow a user to install and execute software from a different system on their computer
- Allow a users to manage a dedicated server on shared hardware
  - Hosting companies
  - Cloud environments

Types of Virtual Machine Managers, *cont'd*

- Emulators
  - Applications written for one hardware environment (one type of CPU) can run on a very different hardware environment (another type of CPU).

- Application containment
  - Not really virtualization, but segregate applications from the host operating system.
  - Examples: Oracle Solaris Zones, BSD Jails, IBM AIX WPARs

San José State University

Host vs. Guest Operating Systems

- Host (native) operating system
  - The OS running on the physical machine that supports (among its other tasks) a VMM
  - Examples:
    - Linux, Windows, Mac OS X

Host vs. Guest Operating Systems, *cont'd*

- Guest operating system
  - An OS running in a virtual machine under control of a VMM.
  - Example:
    - Debian running under VirtualBox on a Mac
  - If there is enough physical memory and disk space, it is possible to run several guest OSes (and their applications) simultaneously on a single physical machine.

Virtualization Requirements

- Fidelity
  - A VMM provides an environment for programs that is essentially identical to the original machine.
- Performance
  - Programs running within that environment have only minor performance degradation.
- Safety
  - The VMM is in complete control of system resources required by the guest operating systems.

San José State University

Brief History of Virtual Machines

- 1972: Virtual machines first appeared commercially.
  - IBM VM370 on IBM mainframes.
- Late 1990s: Intel 80x86 CPU become popular.
  - Xen and VMware created VMM technologies for that CPU.

Brief History of Virtual Machines, *cont'd*

- Today: Commercial and open-source VMMs run on all common operating systems.
  - Example VMM: VirtualBox runs on Intel x86 and AMD64 CPUs on Windows, Linux, Mac OS X, and Solaris.
  - Example guest OSes: Versions of Windows, Linux, Solaris, BSD, MS-DOS, IBM OS/2

Benefits of Virtual Machines

- Backward compatibility
  - Support earlier OS's
    - IBM 360->270
    - Apple Macintosh
- Sharing
  - Different execution environments can share the same physical hardware resources.
- Security
  - A virus that infects a guest OS is unlikely to affect other guest OSes or the host OS.

Benefits of Virtual Machines, *cont'd*

- Suspend the running of a guest OS.
  - Create a snapshot the state of a suspended guest OS.
  - Resume the execution from the snapshot, possibly on different hardware.

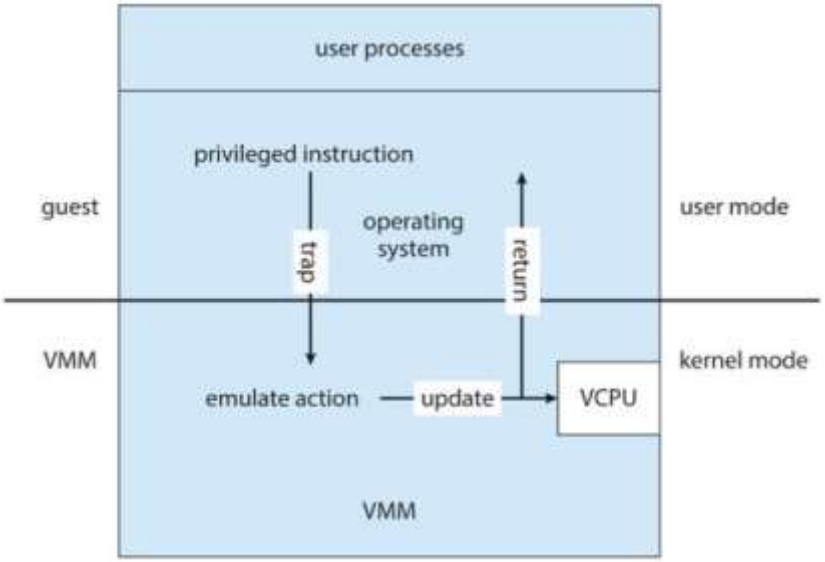
- Live migration: Move a guest from one physical machine to another without interrupting its operations.

Hypervisors or VMMs

- A **hypervisor** is software that creates and runs virtual machines (VMs).
- A hypervisor, sometimes called a virtual machine monitor (VMM), isolates the hypervisor operating system and resources from the virtual machines and enables the creation and management of those VMs.

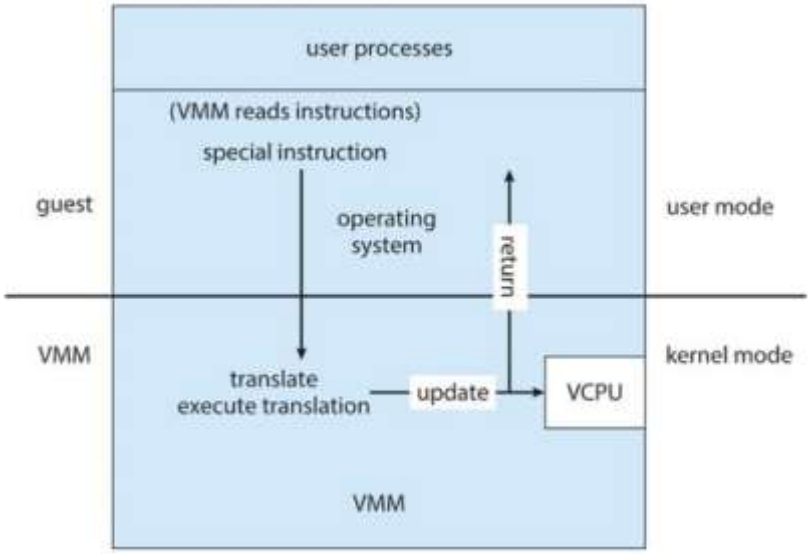
Implementation of Virtual Machines, *cont'd*

- Trap-and-emulate
  - The guest kernel attempts to execute a privileged instruction, such as to do I/O.
  - Causes a trap to the VMM in the real machine.
  - The VMM emulates the privileged operation.
  - Therefore, privileged instructions create extra overhead.
    - The guest will run more slowly.



Implementation of Virtual Machines, *cont'd*

- Binary translation
  - Some x86 instructions ("special instructions") behave differently in user mode vs. kernel mode.
  - The VMM translates special instructions in the guest kernel into a new set of native instructions that accomplish the operations.



Implementation of Virtual Machines, *cont'd*

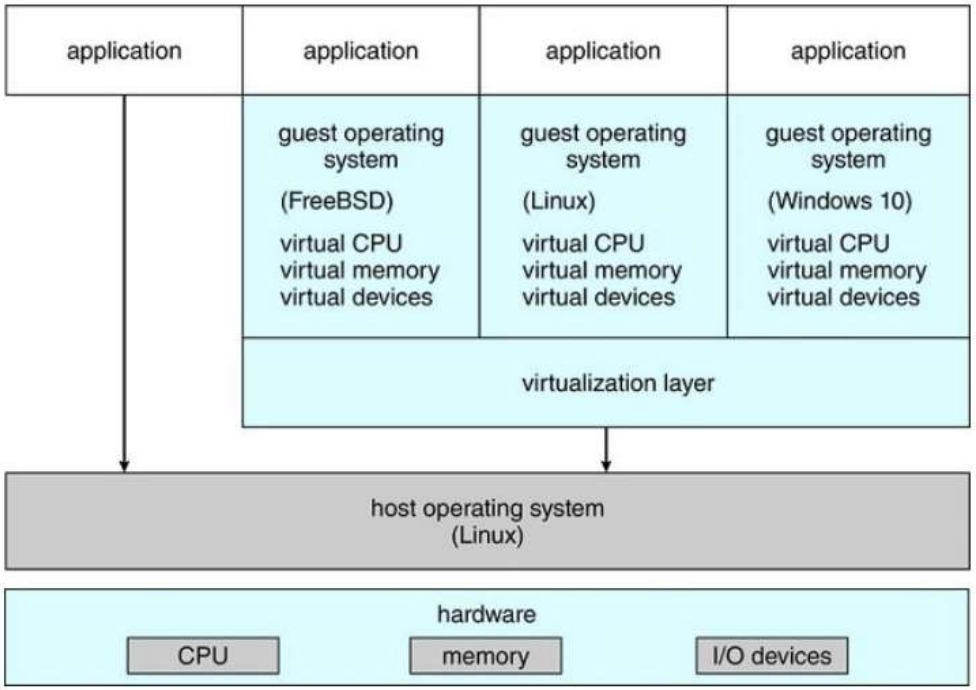
- Binary translation, *cont'd*
  - The new set of instructions can be cached to improve performance.
  - The VMM must also intercept memory paging requests by the guest kernel.
  - The VMM maintains nested page tables (NPTs) to map guest paging operations to physical page table operations.

Implementation of Virtual Machines, *cont'd*

- Hardware assistance
  - Newest CPU chips provide more support for virtualization.
  - 2005: Intel x86 CPU family add VT-x instructions.
    - Binary translation and NPTs no longer needed.
  - 2006: AMD processors support AMD-V technology.
  - CPUs with virtualization hardware assistance can automatically deliver an interrupt destined for a guest to a core that is running a thread of the guest.

Implementation of Virtual Machines, *cont'd*

- The VMM is <u>just another process</u> running on the host.
  - Examples: VMware, VirtualBox
- The host OS doesn't know that virtualization is taking place.



Operating System Concepts, 10th edition
by Abraham Silberschatz, Greg Gagne, and Peter B. Galvin
Wiley, 2018, ISBN 978-1119456339

VMM Examples

- Vmware
- VirtualBox
- Parallels
- QEMU
- Citrix Hypervisor
- Microsoft Hyper-V

Implementation of Virtual Machines, *cont'd*

- The VMM may run as a user application.
  - It might not have the administrative privileges to access the hardware assistance features of modern CPUs.

- No changes are required to the host operating system.
  - Anyone can run VirtualBox to experiment and learn from different guest operating systems.

San José State University

Virtualization Components

- CPU scheduling
  - There may be more virtual CPUs than physical CPUs.
  - The VMM must share the available physical CPUs among the guests.

Virtualization Components, *cont'd*

- Memory management
  - The VMM may overcommit memory among the guests.
  - The VMM determines how much real memory each guest can use.
    - Each guest has the illusion that it has all the memory it wants.
  - The VMM does its own memory page allocation.
    - It works with the host system's memory management.

Virtualization Components, *cont'd*

- I/O management
  - The VMM can dedicate physical I/O devices to guests.
    - Example: Assign a physical CD ROM drive to a guest.
  - The VMM can provide idealized device drivers to guests.
    - The VMM maps guest I/O requests to a device to the actual device driver.

Virtualization Components, *cont'd*

- Storage management
  - The VMM ensures that each guest can only access the disk blocks allocated to it.

- Networking
  - The VMM provides each guest with at least one IP address.
  - The VMM provides routing between the guest and the network.
  - The VMM provides network address translation (NAT).