虛擬化技術
Virtualization Techniques

Introduction to Virtualization Techniques

鍾葉青教授

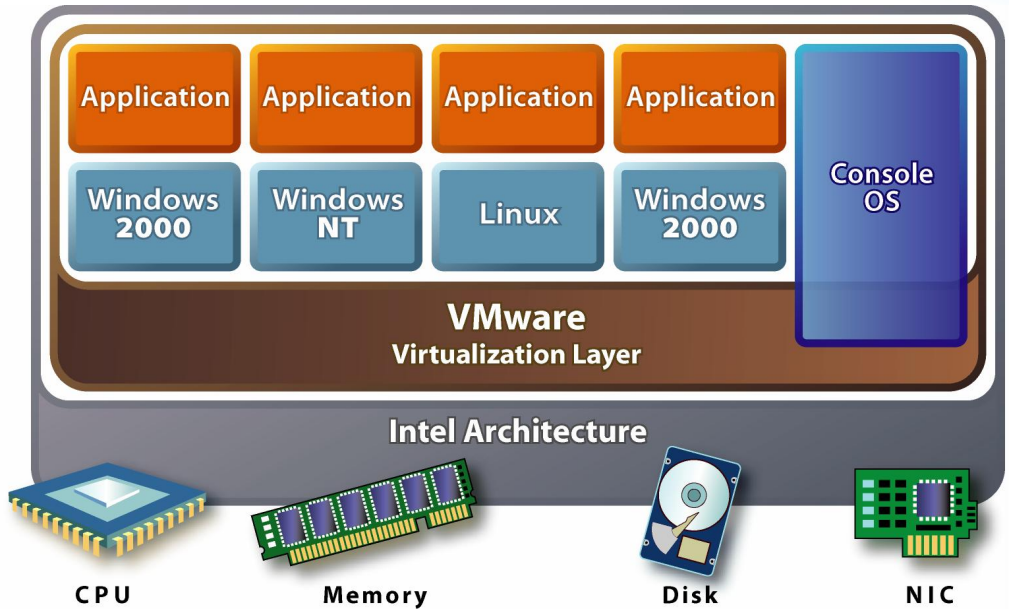
Agenda

- Overview
  - Virtualization Introduction
- Virtualization Techniques
  - System Virtualization
  - Storage Virtualization
  - Network Virtualization
  - GPU Virtualization
  - Software Virtualization
  - Hardware Support Virtualization

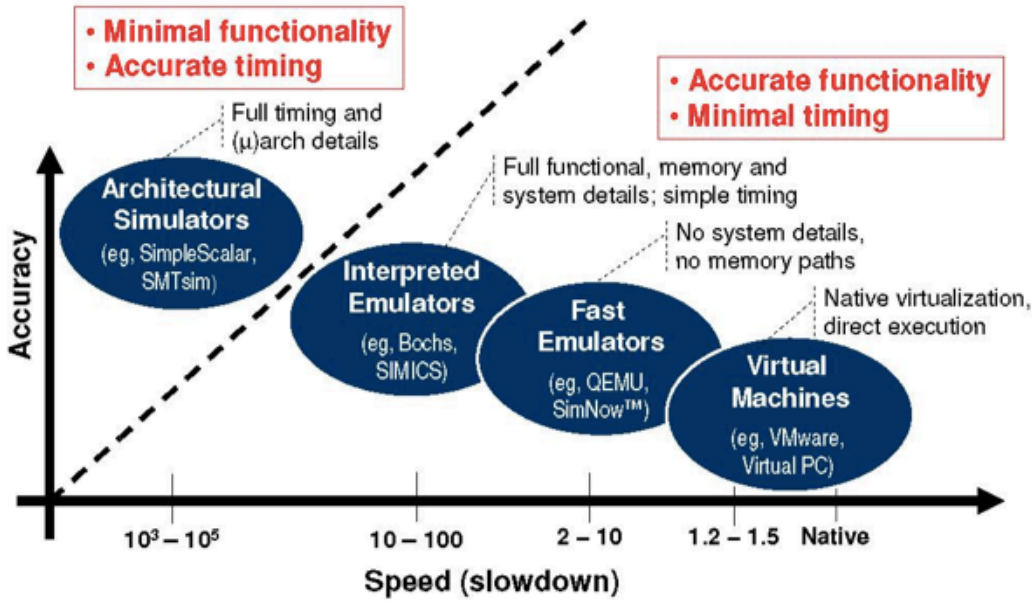
Definition of Virtualization

In computing, virtualization means to create a virtual version of a device or resource, such as a server, storage device, network or even an operating system where **the framework divides the resource into one or more execution environments.**

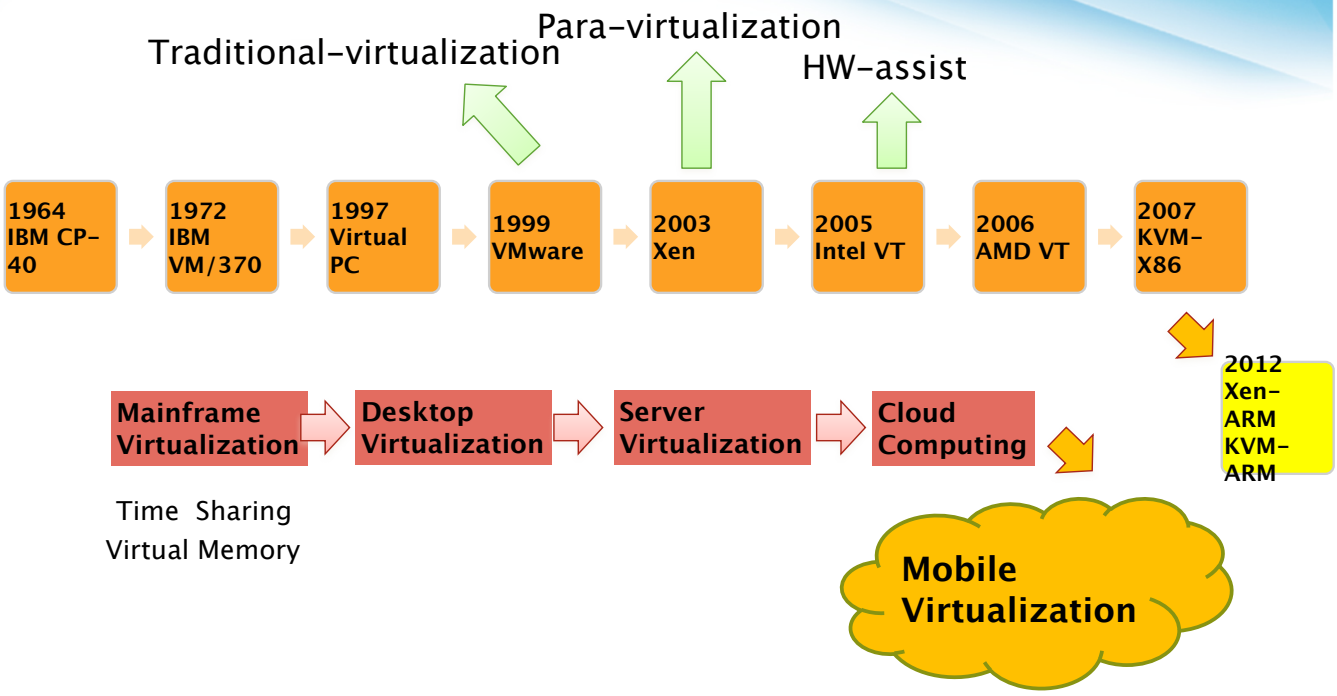
Multiple VMs in One Machine



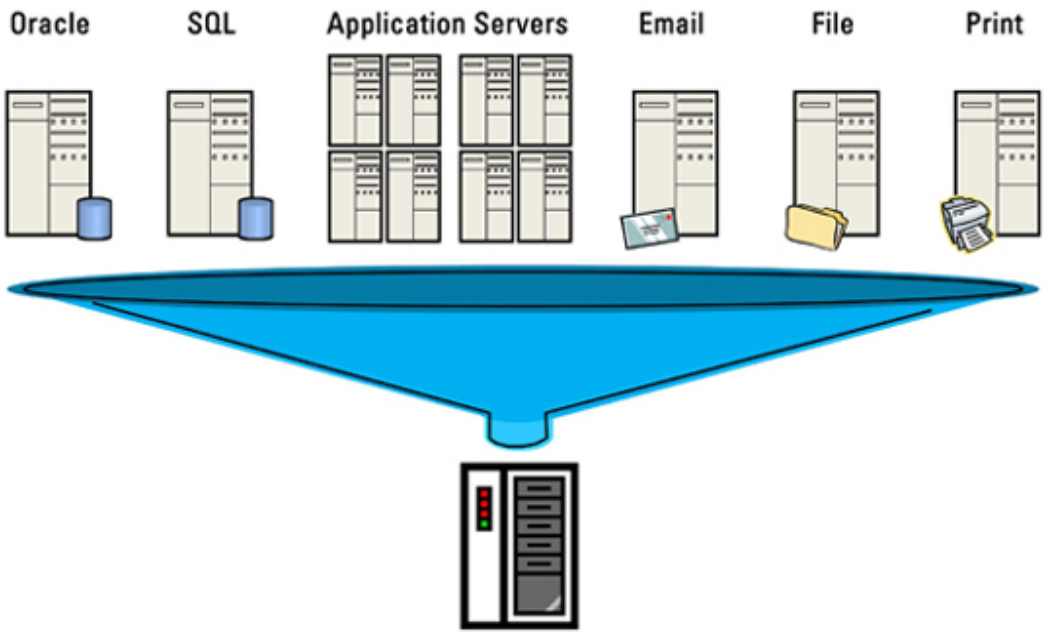
Performance of Virtualizations



History of Virtualization



Example: Server Virtualization



http://www.energystar.gov/index.cfm?c=power_mgt.datacenter_efficiency_virtualization

Benefits of Server Virtualization

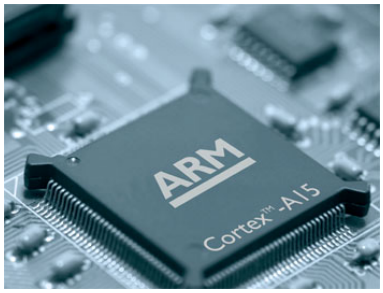
- Virtualization can reduce data center energy expenses by 10%–40%
- Virtualization also improves scalability, reduces downtime, and enables faster deployments.
- Reduce the data center footprint

Example: Mobile Virtualization

VMware MVP

Gartner predict that by 2012, more than 50% of new smart phones shipped will be virtualized

ARM Cortex-A15 enables efficient handling of the complex software environments including full **hardware virtualization**



Benefits of Mobile Virtualization

- Portability
- Multiple OSes on a single chip
- Security
- Dynamic Update of System Software
- Legacy Code re-use
- IP Protection
- Mobile Manageability

Reference : http://en.wikipedia.org/wiki/Embedded_Hypervisor

Virtualization Techniques (1/2)

- System Virtualization
  - CPU Virtualization
  - Memory Virtualization
  - I/O Virtualization
- Storage Virtualization
  - LVM
  - RAID
- Network Virtualization
  - Software Defined Network
  - Open vSwitch
  - InfiniBand Virtualization

Virtualization Techniques (2/2)

- GPU Virtualization
- Software Virtualization
  - Virtual Desktop Infrastructure (VDI)
  - EyeOS
- Hardware Support Virtualization
  - Intel VT
  - ARM
  - SRIOV
  - MRIOV

System Virtualization

Storage Virtualization

Network Virtualization

GPU Virtualization

Software Virtualization

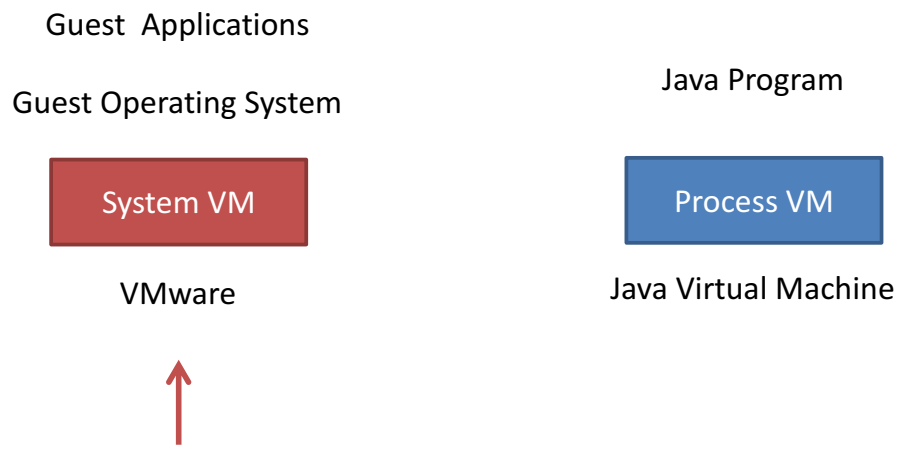
Hardware Support Virtualization

VIRTUALIZATION TECHNIQUES

Virtual Machine (1/2)

- A virtual machine (VM) is a software implementation of a machine that executes programs like a physical machine. Virtual machines are separated into two major classifications:
  - A system virtual machine
    - Which provides a complete system platform which supports the execution of a complete operating system (OS)
  - A process virtual machine
    - Which is designed to run a single program, which means that it supports a single process.

Virtual Machine (2/2)



This course we will focus on the system virtualization

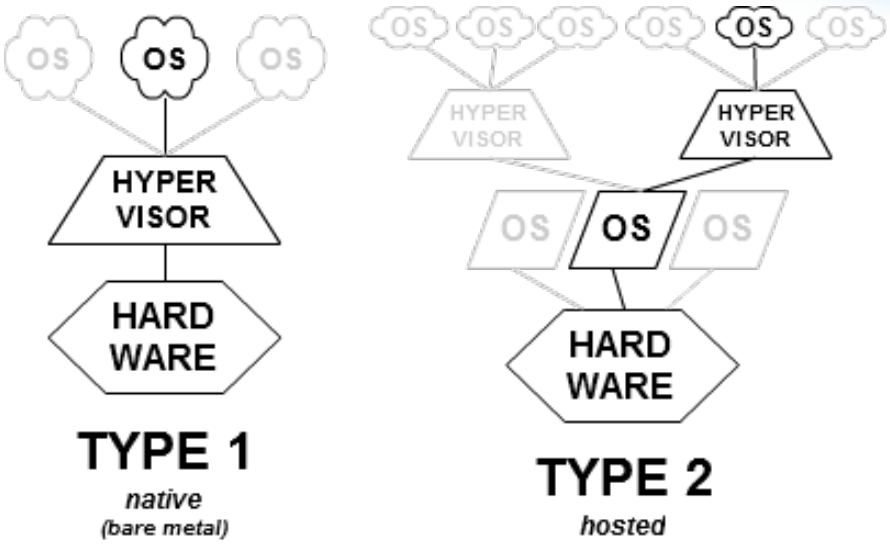
System Virtual Machine

- System virtual machine is controlled by a hypervisor or VMM (Virtual Machine Monitor)
- A hypervisor or VMM is a software to provide a hardware emulation interface including CPU, memory, I/O by multiplexing host resources

Two Types of Hypervisor (1/2)

- In their 1974 article "Formal Requirements for Virtualizable Third Generation Architectures" Gerald J. Popek and Robert P. Goldberg classified two types of hypervisor:
  - Type 1 hypervisor : bare metal type
  - Type 2 hypervisor : hosted type

Two Types of Hypervisor (2/2)



Type 1 (or *native*, bare metal) hypervisors

Type 2 (or *hosted*) hypervisors

http://en.wikipedia.org/wiki/Hypervisor

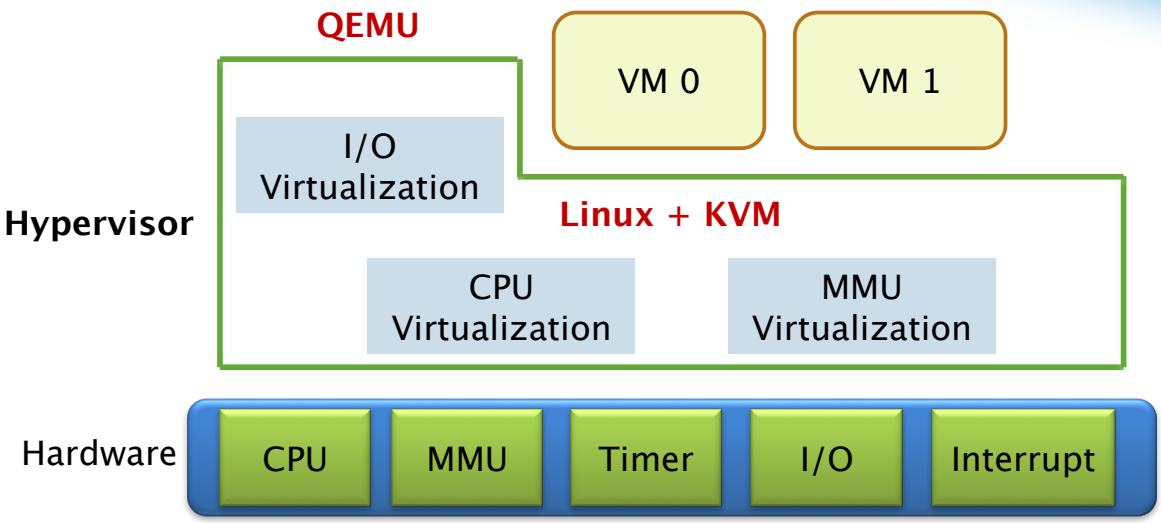
Purposes of Hypervisor

- CPU Virtualization
  - Handle all sensitive instructions by emulation
- Memory Virtualization
  - Allocate guest physical memory
  - Translate guest virtual address to host virtual address
- I/O Virtualization
  - Emulate I/O devices for guest
  - Ex: Keyboard, UART, Storage and Network

Implementations of Hypervisor

- Full Virtualization
  - A wholly emulated virtual machine makes guest operating system binary can be executed directly without modifying guest source code
  - For efficiency, it needs hardware-assisted virtualization
- Para-Virtualization
  - Hypercalls are defined and used in a guest operating system to make a virtual machine abstraction
  - According to literature, it's most efficient way
- Pre-Virtualization
  - By compiling technique, guest operating system binary or source could be compiled for virtualization

Hypervisor Case: KVM

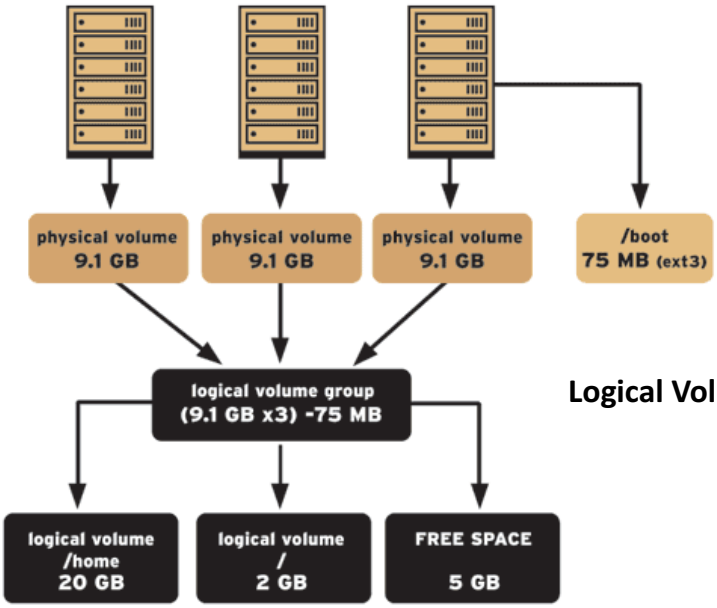


1. CPU and memory virtualizations are handled in the Linux Kernel Space
2. I/O virtualization is handled in the Linux User Space by QEMU
3. It's a type 2 virtual machine
4. It's a full virtualization implementation

System Virtualization
Storage Virtualization
Network Virtualization
GPU Virtualization
Software Virtualization
Hardware Support Virtualization

VIRTUALIZATION TECHNIQUES

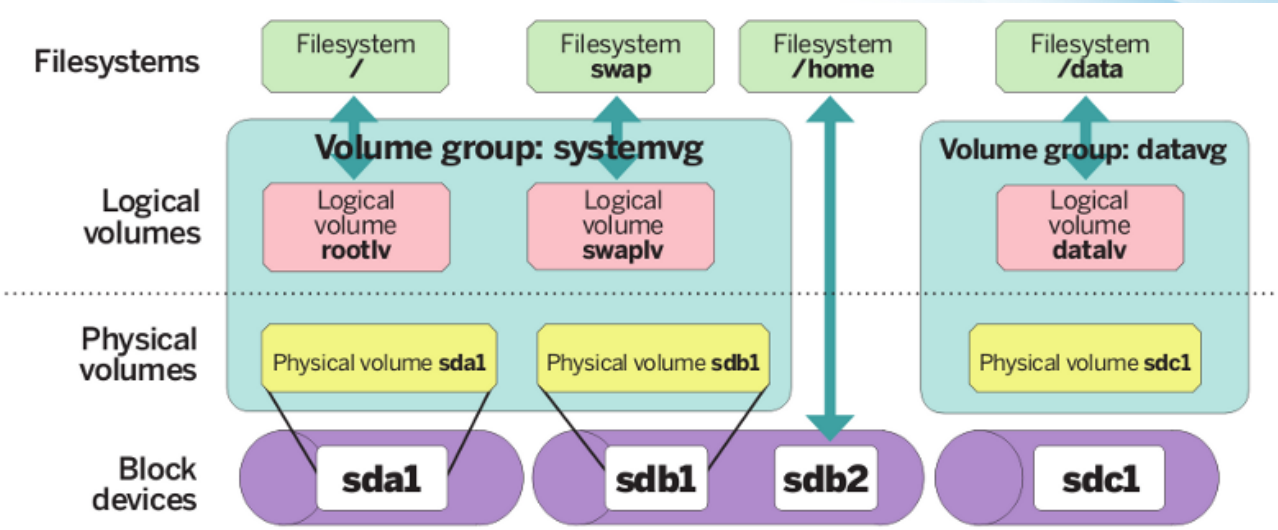
LVM(1/2)



Logical Volume Manager

- **LVM** is a logical volume manager for the Linux kernel; it manages disk drives and similar mass-storage devices.

LVM(2/2) : Example

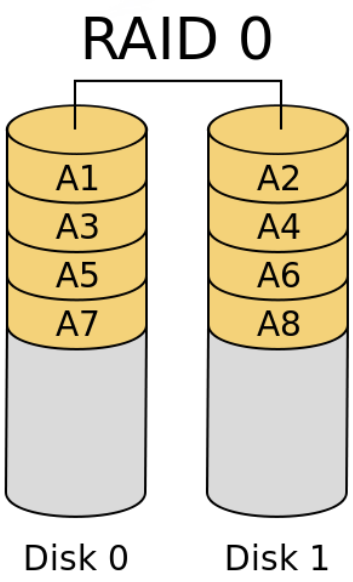


- Disk partition -> physical volumes -> volume group -> logical volumes -> file systems

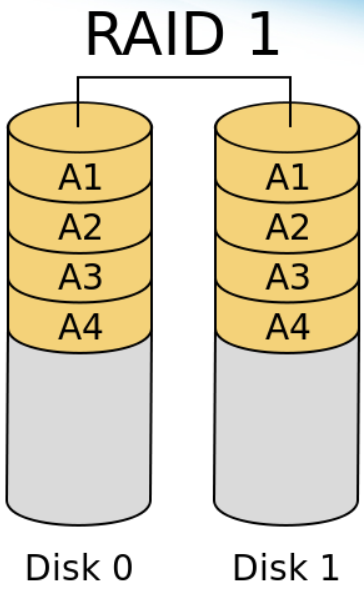
RAID

- **RAID** (**redundant array of independent disks**) is a storage technology that combines multiple disk drive components into a logical unit.
- Data is distributed across the drives in one of several ways called "RAID levels", such as RAID0, RAID1, etc., depending on the level of redundancy and performance required.

Example : RAID 0 and RAID 1



It provides improved performance and additional storage but no fault tolerance (block-level striping without parity or mirroring) .



mirroring without parity or striping

LVM and RIAD for Virtualization

- LVM provides a virtual storage systems which is flexible to partition and allocate logical volumes to virtual machines
- RAID not only improves storage performance but has fault tolerance capability
- Leaning how to configure LVM and RAID in the virtualization system

System Virtualization
Storage Virtualization
Network Virtualization
GPU Virtualization
Software Virtualization
Hardware Support Virtualization

VIRTUALIZATION TECHNIQUES

Software Defined Network (1/2)

- **Software defined networking (SDN)** is an approach to building computer networks that separates and abstracts elements of these systems
- SDN decouples the system that makes decisions about where traffic is sent (the control plane) from the underlying system that forwards traffic to the selected destination (the data plane)

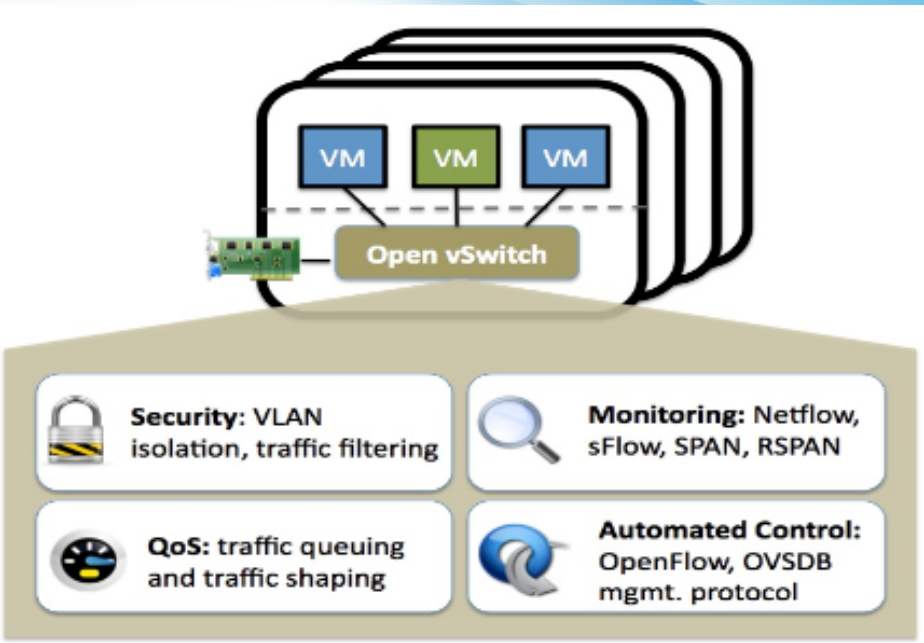
Software Defined Network (2/2)

- The inventors and vendors of these systems claim that this technology simplifies networking and enables new applications, such as
  - network virtualization in which the control plane is separated from the data plane and implemented in a software application.

Open vSwitch (1/2)

- Open vSwitch is a flexible, multi-layer software network switch. **Typically used in virtualization environments as the network switching component in the hypervisor**.
- Open vSwitch maintains the logical state of a virtual machine's network connection across physical hosts when a virtual machine is migrated, and it can be managed and monitored by standard protocols such as: OpenFlow, NetFlow, sFlow, SPAN, RSPAN.

Open vSwitch (2/2)



- When it comes to virtualization, open vSwitch is attractive because it provides the ability for **a single controller to manage your virtual network across all your servers**.

InfiniBand Virtualization

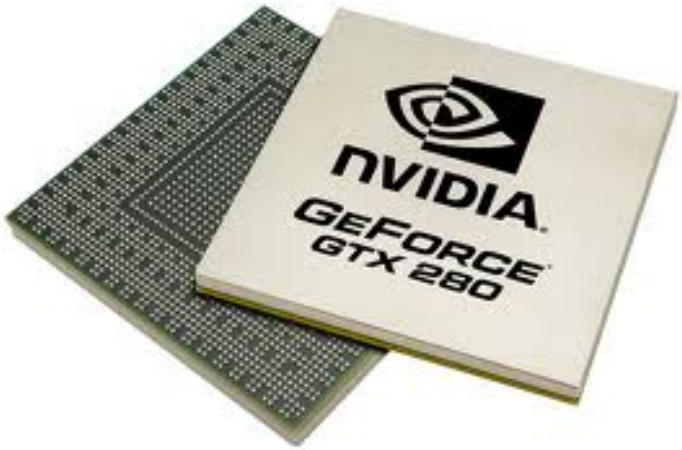
- **InfiniBand** is a switched fabric communications link used in high-performance computing and enterprise data centers.
- It has two key features : low latency and high bandwidth
- ***Virtualization* Using *InfiniBand* Brings Big Benefits to Data Centers**

System Virtualization
Storage Virtualization
Network Virtualization
GPU Virtualization
Software Virtualization
Hardware Support Virtualization

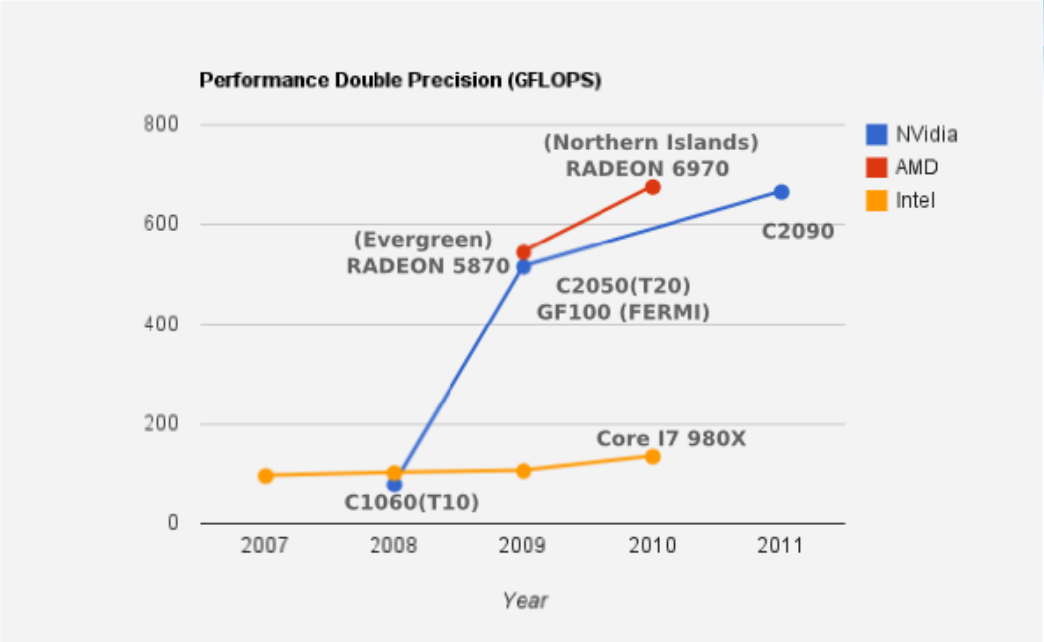
VIRTUALIZATION TECHNIQUES

What's GPU (Graphics processing unit)

- A Graphics Processing Units (GPUs) are high-performance many-core processors capable of very high computation and data throughput.



Performance Comparison: GPU vs. CPU



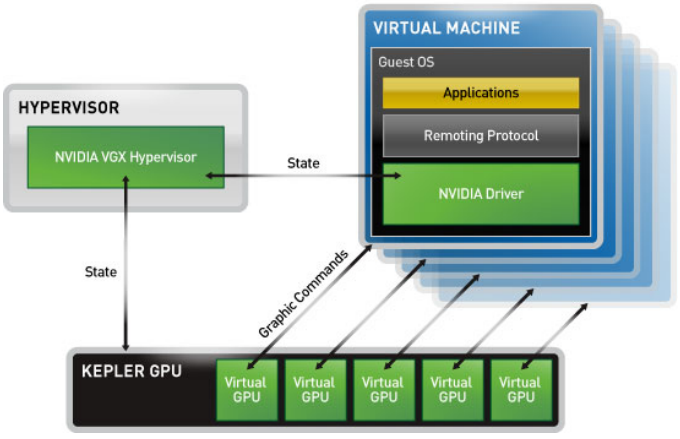
- While the Intel Core I7 980X (extreme edition) gives us around **110GFLOPS**, GPUs such as AMD Radeon 6970 and NVidia C2090 offer more than **660GFLOPS**.

GPGPU

- High performance of modern Graphics Processing Units may be utilized not only for graphics related application but also for general computing.
- Today's GPUs are general-purpose parallel processors with support for accessible programming interfaces and industry-standard languages such as C.
- Developers who port their applications to GPUs often achieve speedups of orders of magnitude vs. optimized CPU implementations.

GPU Virtualization

- GPU virtualization allows multiple virtual machines to interact directly with a GPU and manages the GPU resources so multiple users can share common hardware, while improving user density.



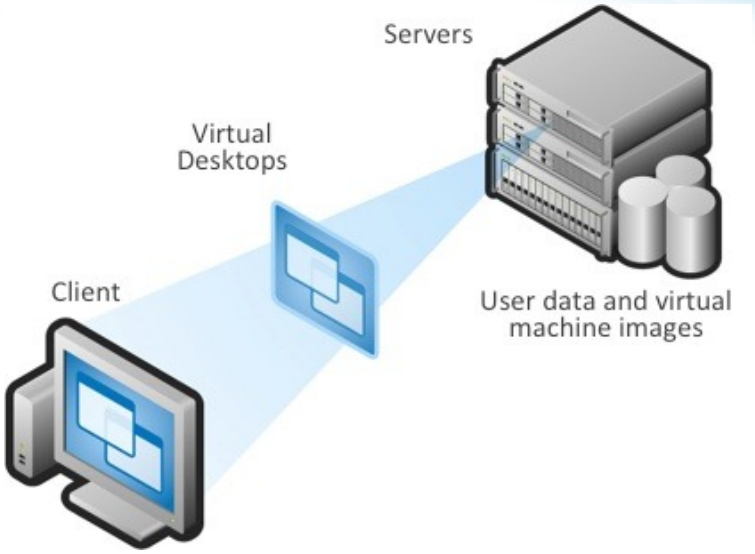
System Virtualization
Storage Virtualization
Network Virtualization
GPU Virtualization
Software Virtualization
Hardware Support Virtualization

VIRTUALIZATION TECHNIQUES

Software Virtualization

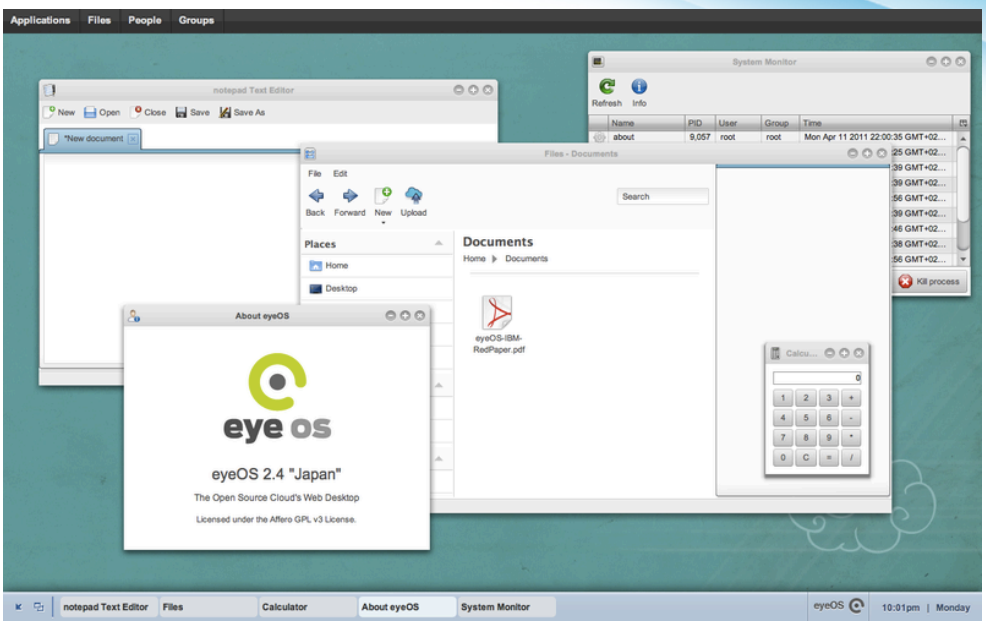
- IT administrators have a lot to deal with in today's corporate infrastructure. With the ever increasing prices of upgrading desktop computers, software virtualization is becoming very appealing.
- It has following features:
  - Ease of Management
  - Security
  - Green
  - Portable

Virtual Desktop Infrastructure (VDI)



- Virtual desktop Infrastructure (VDI) is a desktop-centric service that hosts users desktop environments on remote servers, which are accessed over a network using a remote display protocol.

EyeOS : Web Desktop Virtualization



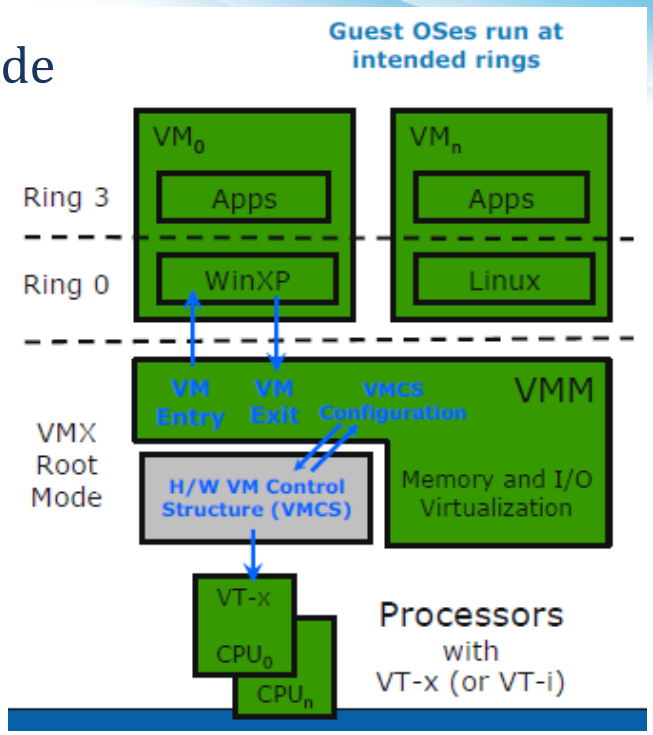
- eyeOS is a web desktop following the cloud computing concept that seeks to enable collaboration and communication among users. It is mainly written in PHP, XML, and JavaScript

System Virtualization
Storage Virtualization
Network Virtualization
GPU Virtualization
Software Virtualization
Hardware Support Virtualization

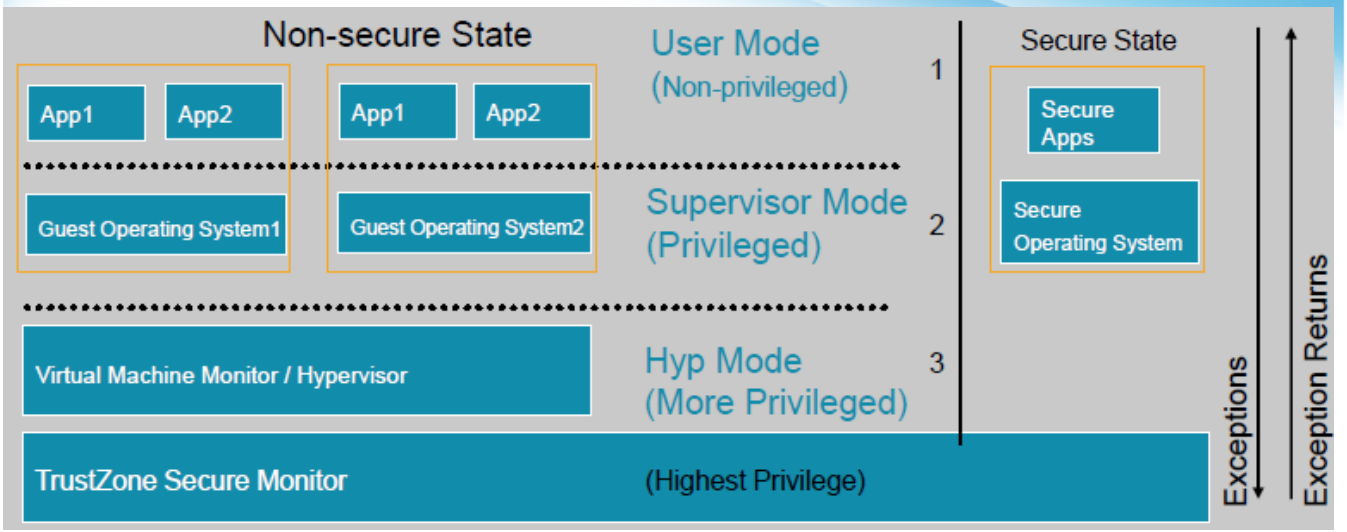
VIRTUALIZATION TECHNIQUES

Intel VT-x

- New CPU Operating Mode
  - VMX Root Operation
  - Non-Root Operation
- New Transitions
  - VM entry to Guest
  - VM exit to VMM
- VM Control Structure
  - Configured by VMM software

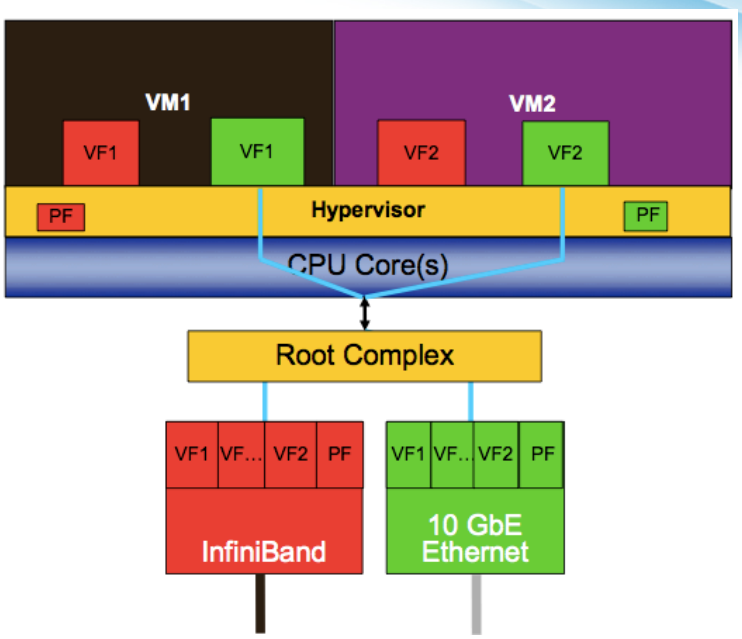


ARM Virtualization Extension



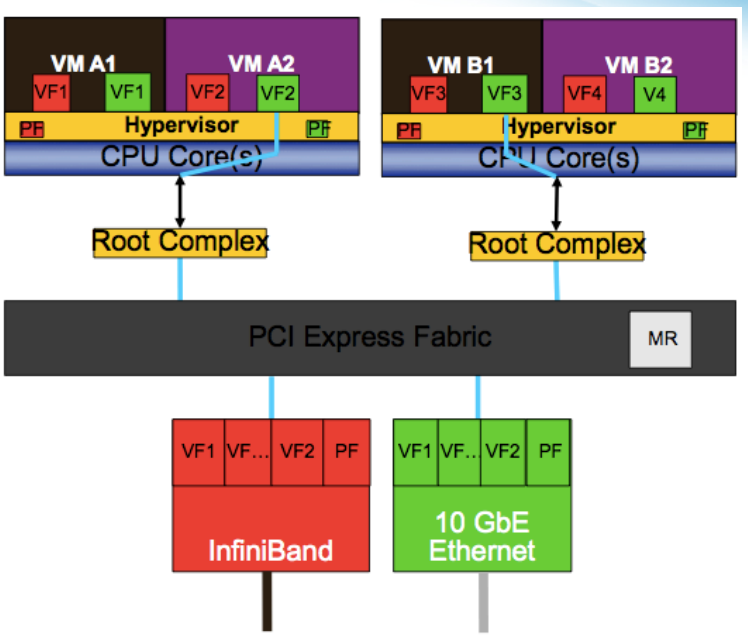
- Secure world supports a single virtual machine
- New Non-secure level of privilege to hold Hypervisor
  - Hypervisor mode applies to normal world
  - Hyp Mode is used by the Hypervisor
  - Guest OS given same kernel/user privilege structure as for a non virtualized environment
- Monitor mode controls transition between worlds

Single-Root I/O Virtualization



- PCI-SIG specifies multiple functional elements addressing performance and security aspects of I/O virtualization
- PCIe devices will have multiple virtual functions (VF's)

Multi-Root I/O Virtualization



- Multiple hardware domains utilizing same IO endpoints
- Virtual functions are dedicated to virtual machines