THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

COMPX527 Lecture 4.1 & 2

Virtualization

craiyon.com

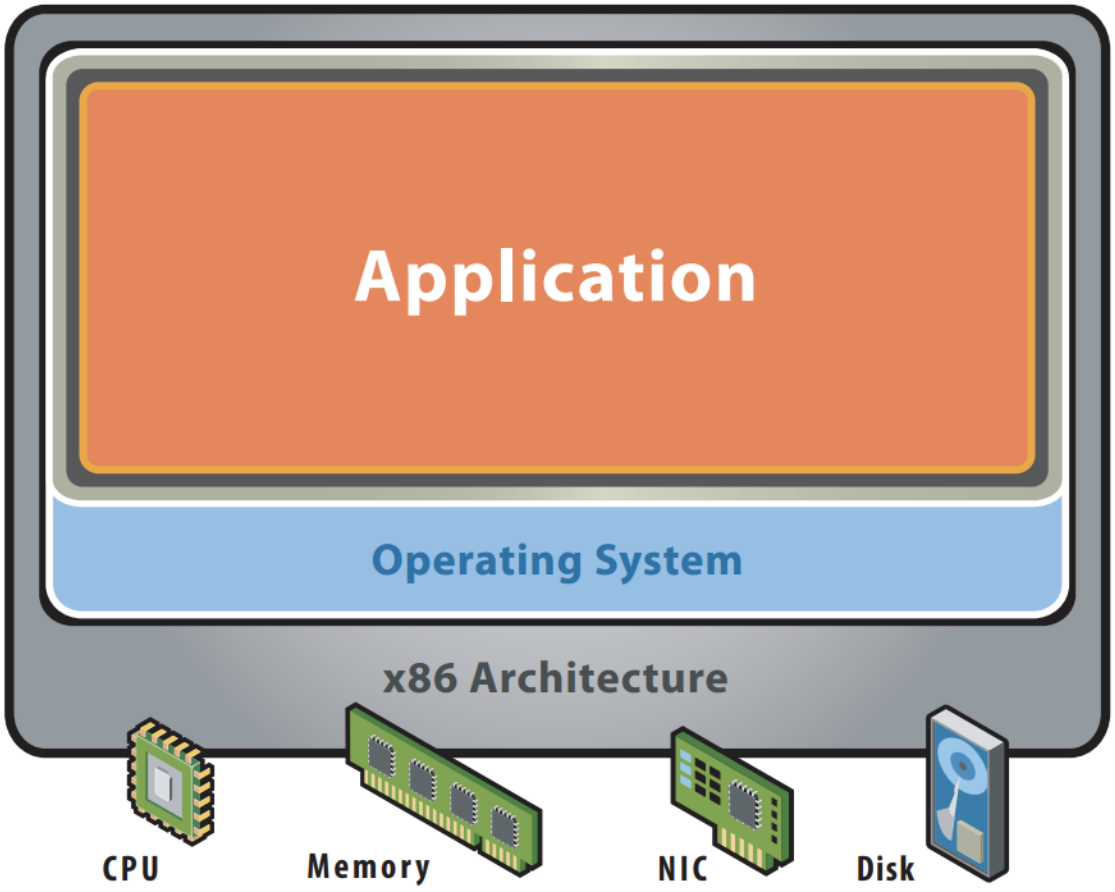
Agenda

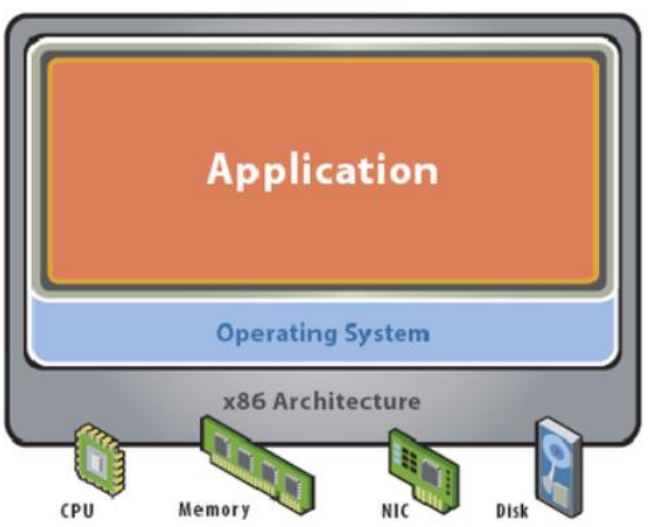
- Virtualisation Overview
- Types of Virtualisation
- Virtualisation Properties
- Virtualisation
  - CPU
  - Network
  - Memory
  - I/O and applications
- Security issues with Virtualisation

Virtualization

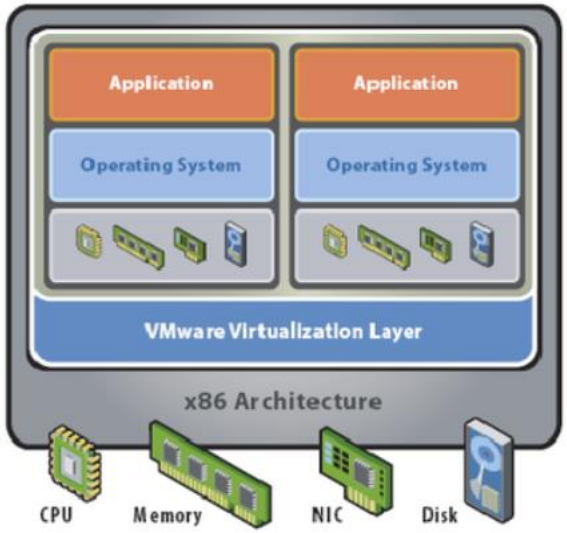
- Virtualization is the separation of a service request from the underlying physical delivery of that service. -VMWare

Computer System





Before Virtualization:

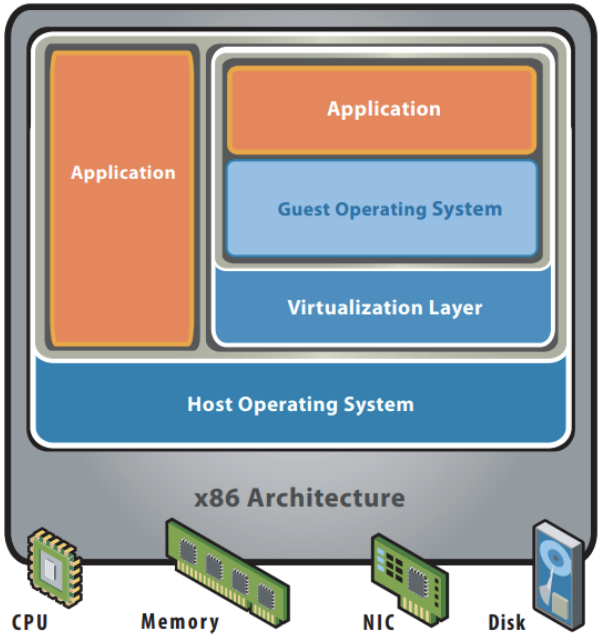


After Virtualization:

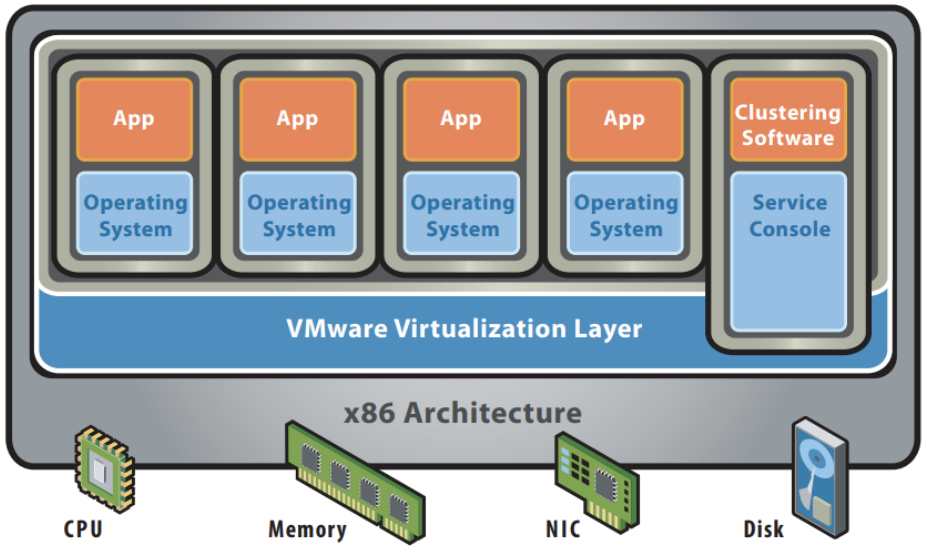
A virtualisation overview VMware Inc, 2008.)

Two types of virtualization

The virtualization layer consists of software that lives in between the hardware, or host, and the virtual machines that it supports.



Hosted



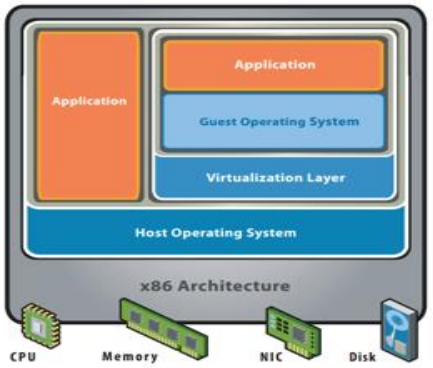
Bare Metal

Hosted Architecture

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

- Installs and runs virtualization layer as an application on top of an operating system.
- Also known as "Type 2"
- User-friendly, ideal for situation where the performance is not utmost concern
- Disadvantage???
- Examples:

  Oracle VirtualBox, Parallel desktops,

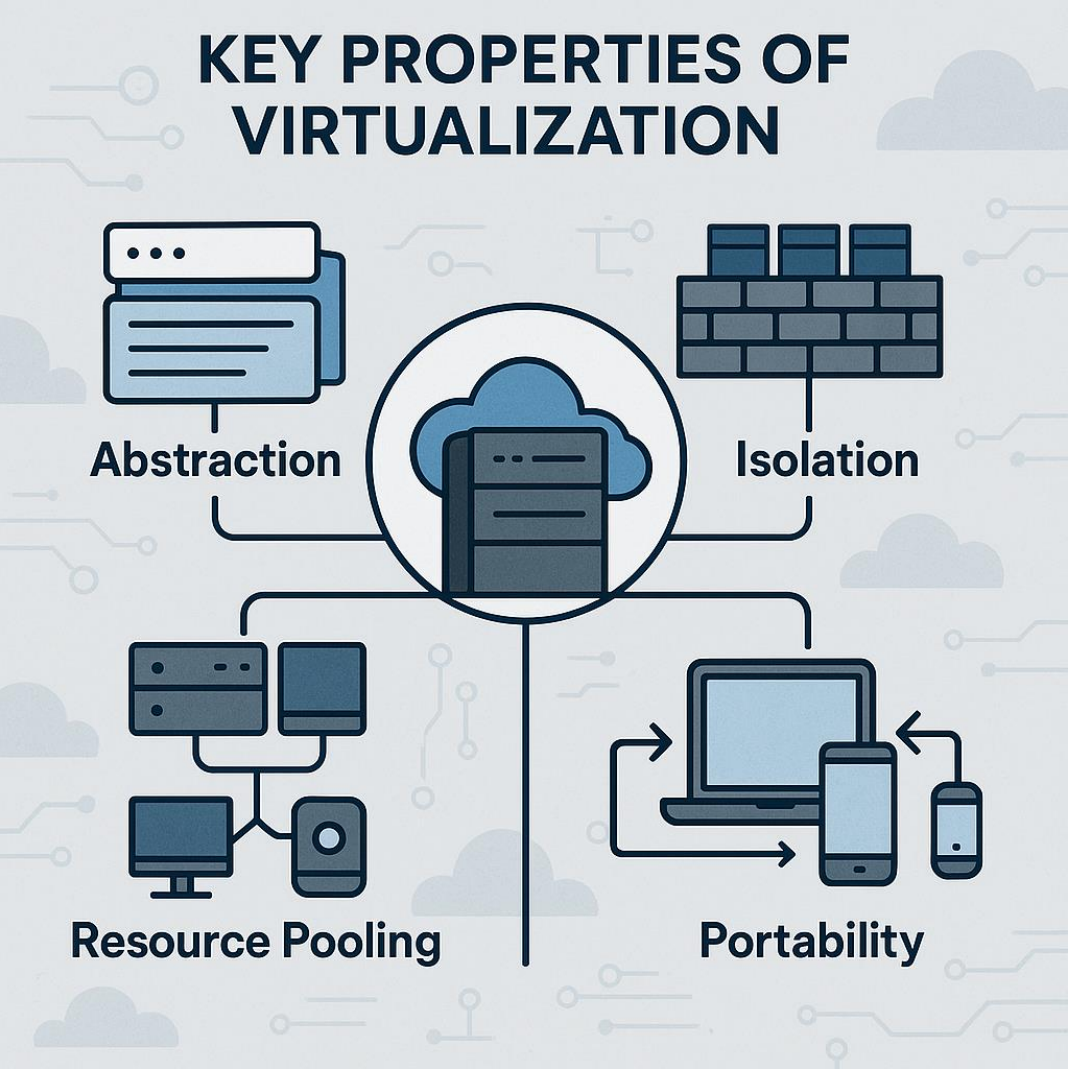


Hosted

Hypervisor (Bare-Metal) Architecture

- Installs virtualization layer directly on a clean x86-based system.
- Also known as "Type 1" architecture.
- Direct access to the hardware resources rather than going through an operating system.
- More efficient than Type 2, and greater scalability, and performance.
- Disadvantages???
- Examples: VMWare ESX Server, etc.

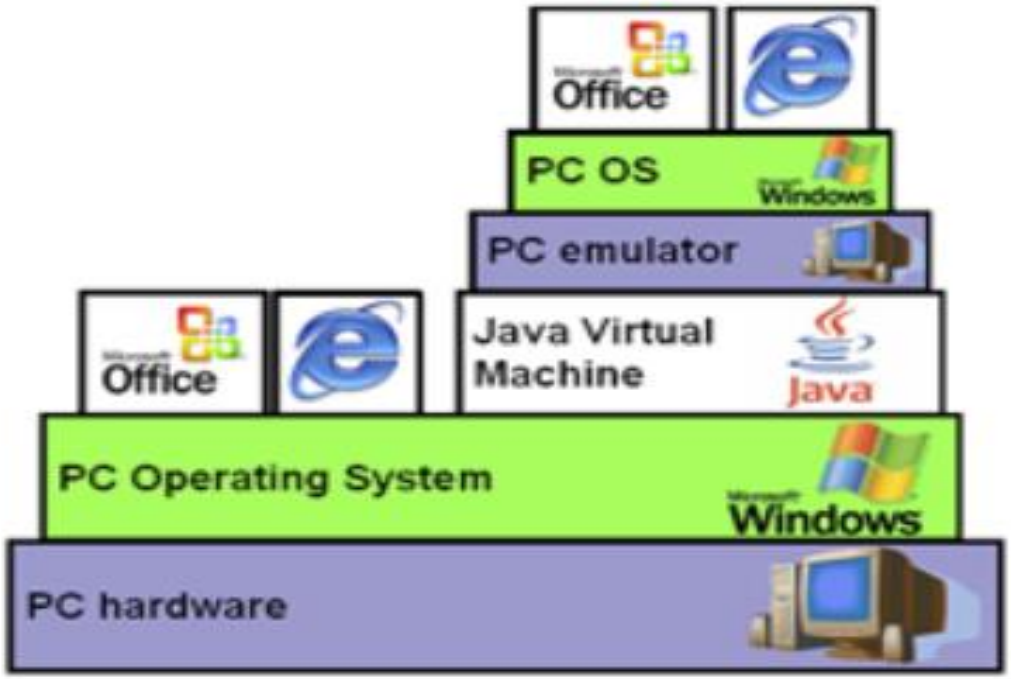
Virtualization Properties



CPU virtualization techniques

- Emulation
- Full Virtualization
- Hardware Assisted Virtualization

Emulation

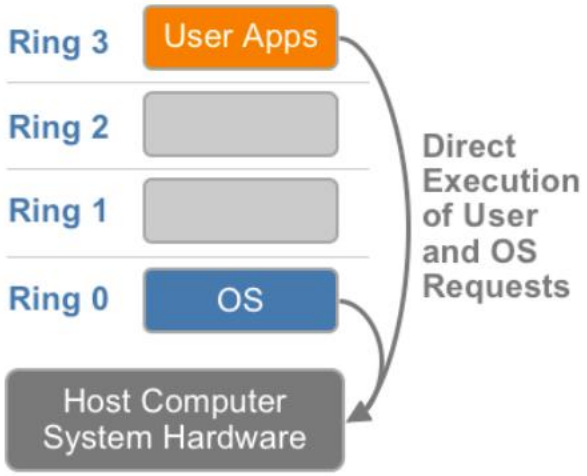


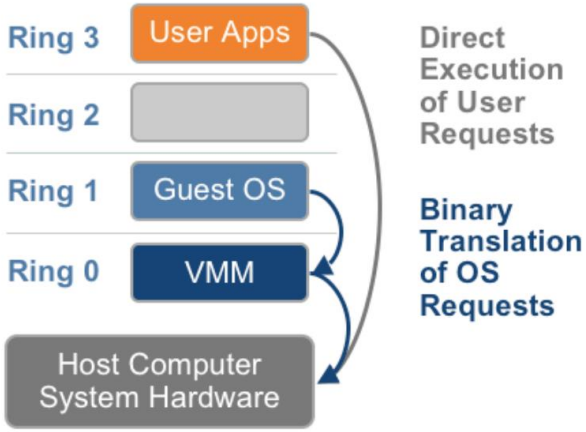
Emulation

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

- The hypervisor emulates the hardware resources in software and presents it to the guest VM
- When the guest VM sends an instruction to the virtual hardware, the hypervisor translates it to the corresponding instruction for the real hardware, executes it and returns the result to the guest VM
- Slow performance
- Example: Boschs

Full virtualization





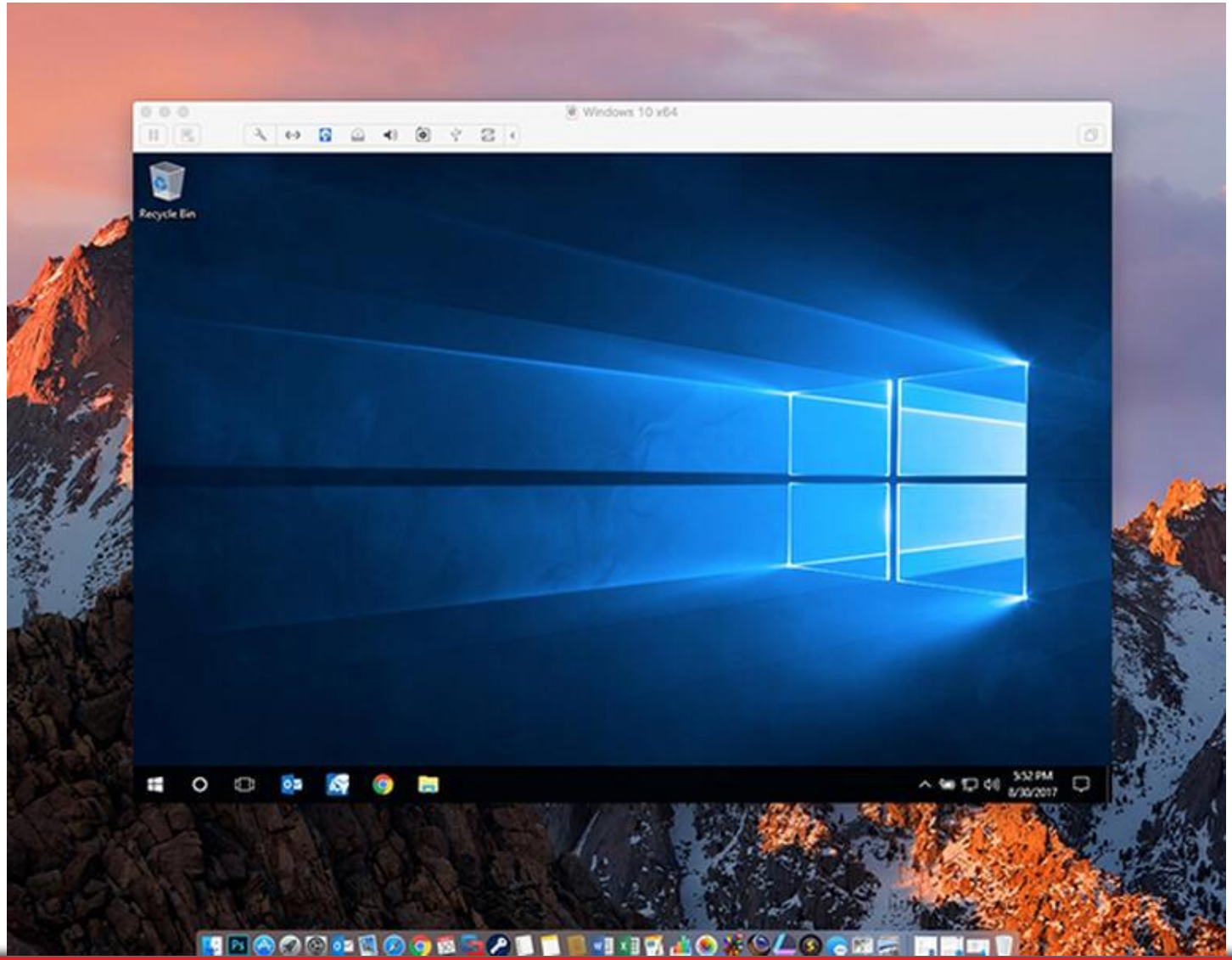
VMM lies between the guest and host OS

Full virtualization

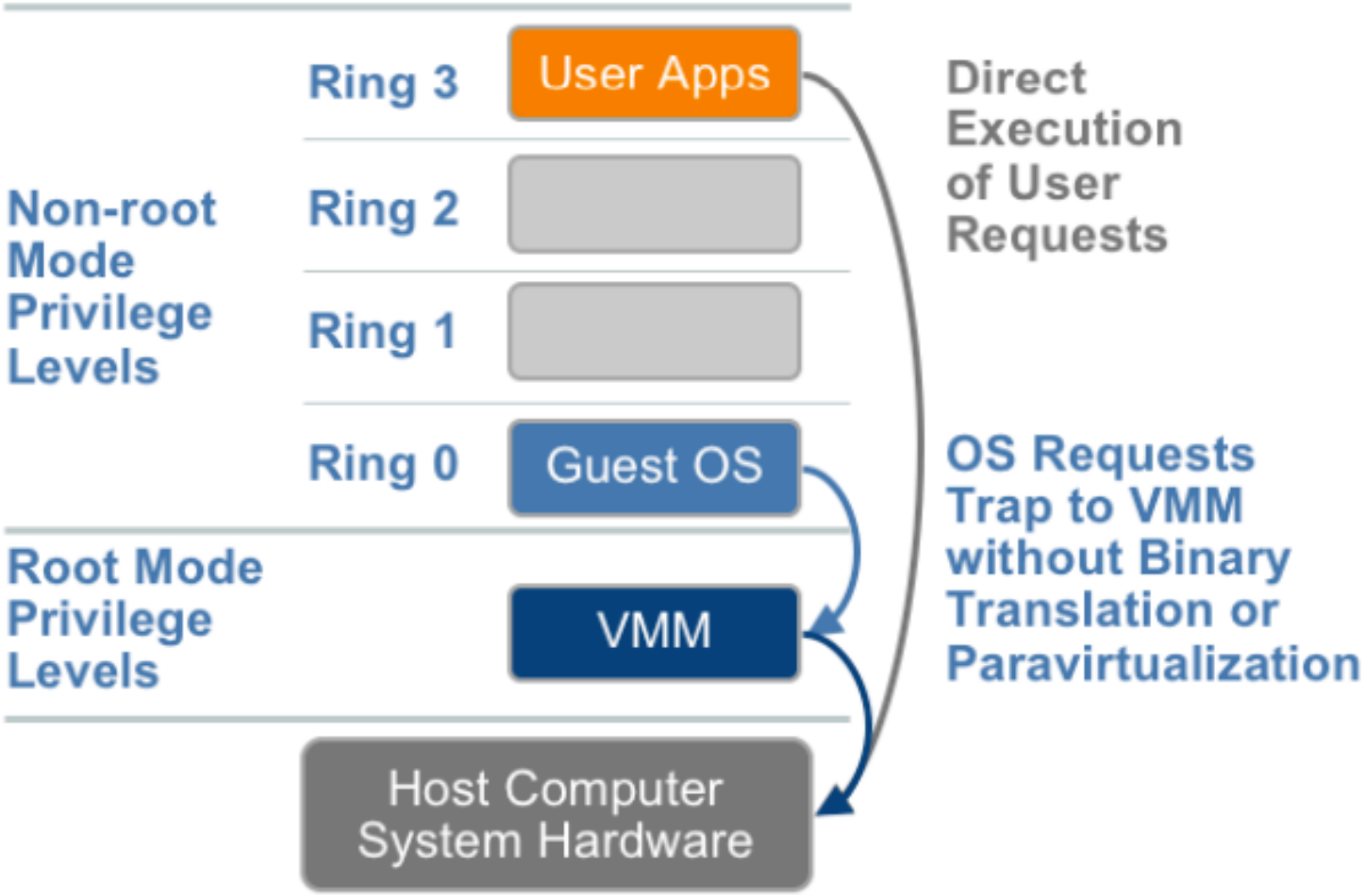
THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

- Each VMM provides each VM with all services of physical system (incl. virtual BIOS, virtual devices, virtualized memory mgmt.)
- Translates kernel code to replace non-virtualizable instructions with new instruction sequences that have the intended effect on the virtual hardware.
- Guest OS is fully decoupled from underlying hardware. Hence FULL virtualization.
- Guest OS unaware that it is actually virtual and hence needs no modification (e.g. Windows 7).
- Hypervisor translates OS instructions on the fly, caches results for future use.
- Best isolation and security for VMs, high portability since the guest OS instance can run on native hardware or virtually.
- Eg.: VMWare, Microsoft Virtual Server, VirtualBox etc.

Example



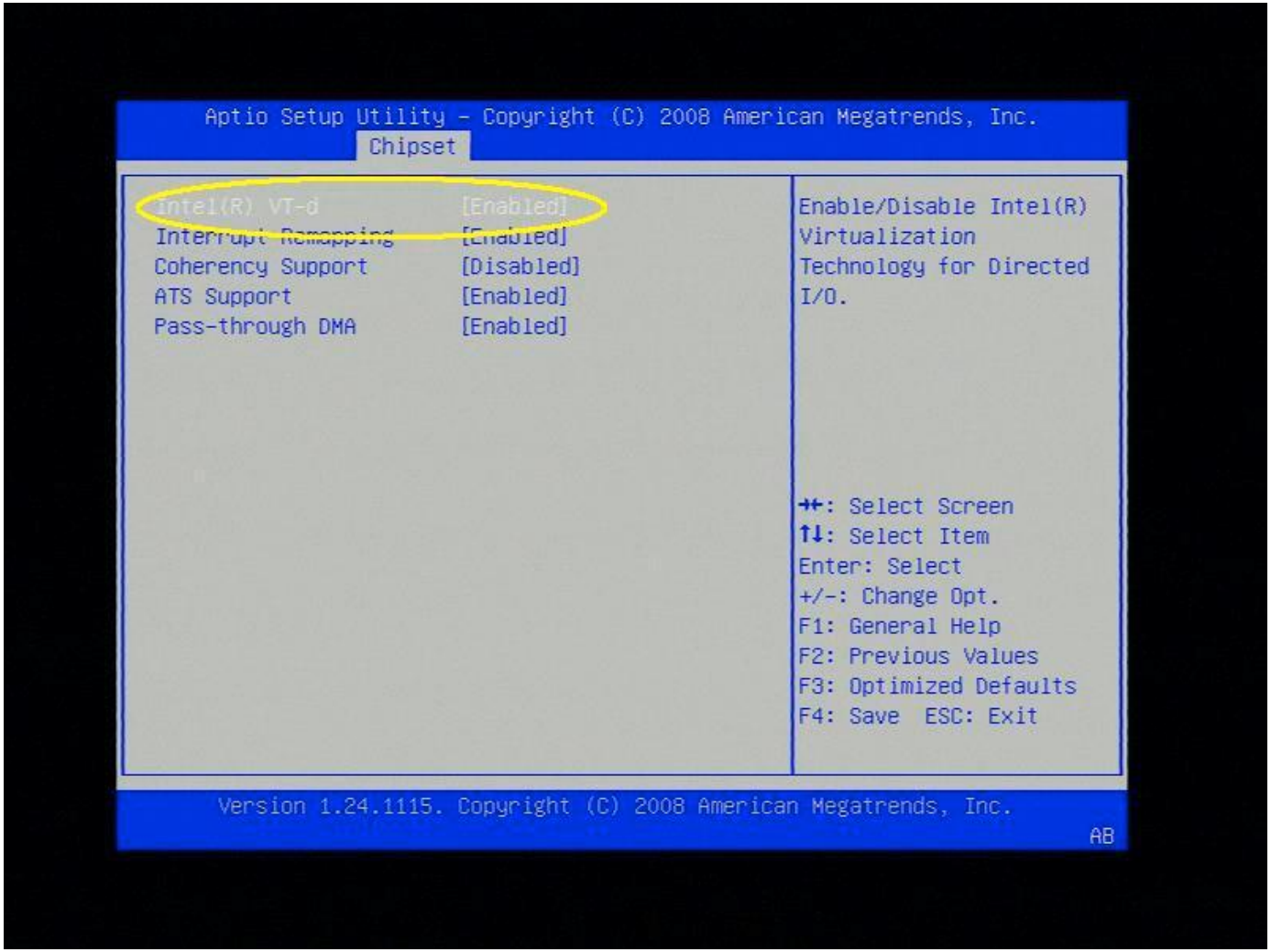
Hardware Assisted Virtualization



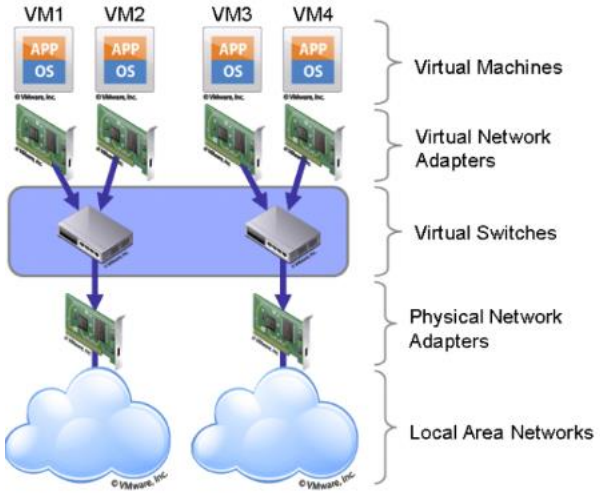
Hardware Assisted Virtualization

- Hardware vendors entering virtualization space, aiming to simplify virtualization techniques.
- "1st generation" enhancement includes:
  - Intel VT-x
  - AMD-V
- Both run under Ring 0 – a new root mode.
  - Automatically trap privileged and sensitive OS calls to the hypervisor
  - Hence, NO need for binary translation.
- Measurement of 'performance' of binary translation vs hardware-assisted depends on circumstances.
- Usually rigid programming models.

Example


Aptio Setup Utility – Copyright (C) 2008 American Megatrends, Inc.
Chipset
Intel(R) VT-d [Enabled]
Interrupt Remapping [Enabled]
Coherency Support [Disabled]
ATS Support [Enabled]
Pass-through DMA [Enabled]
Enable/Disable Intel(R) Virtualization Technology for Directed I/O.
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save ESC: Exit
Version 1.24.1115. Copyright (C) 2008 American Megatrends, Inc.
AB

NETWORK VIRTUALISATION

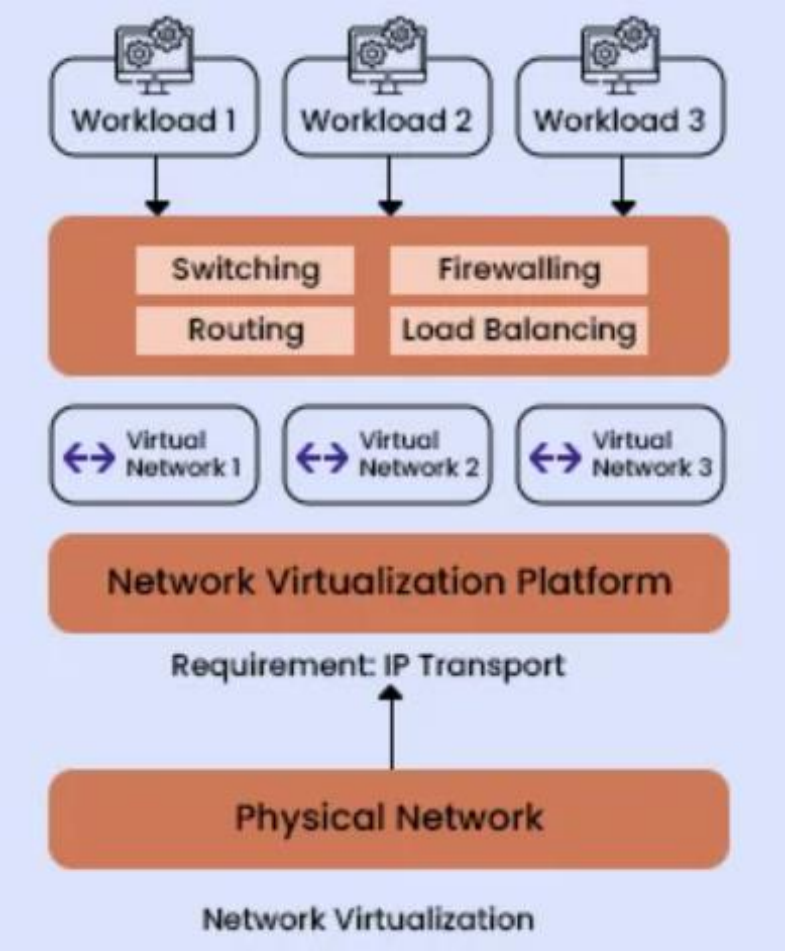


https://tciel.wordpress.com/2015/06/26/network-virtualization/

Network Virtualization (NV) refers to abstracting network resources that were traditionally delivered in hardware to software. (VMware)

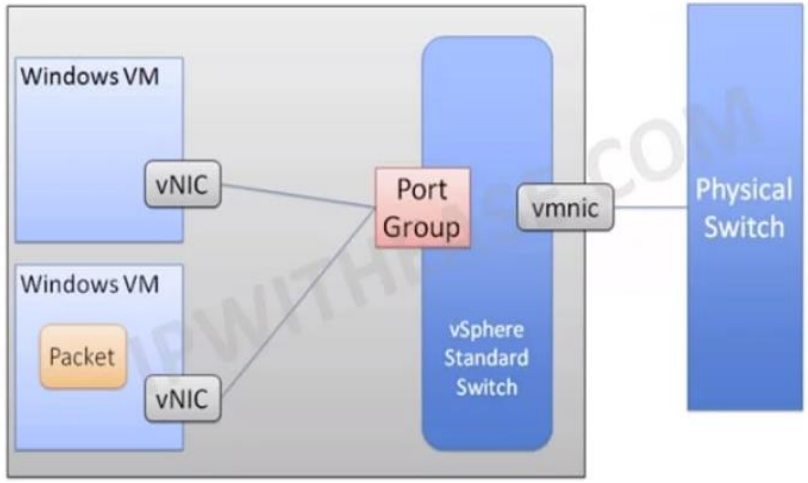
How does network Virtualisation work?

Network virtualization decouples network services from the underlying hardware and allows virtual provisioning of an entire network.



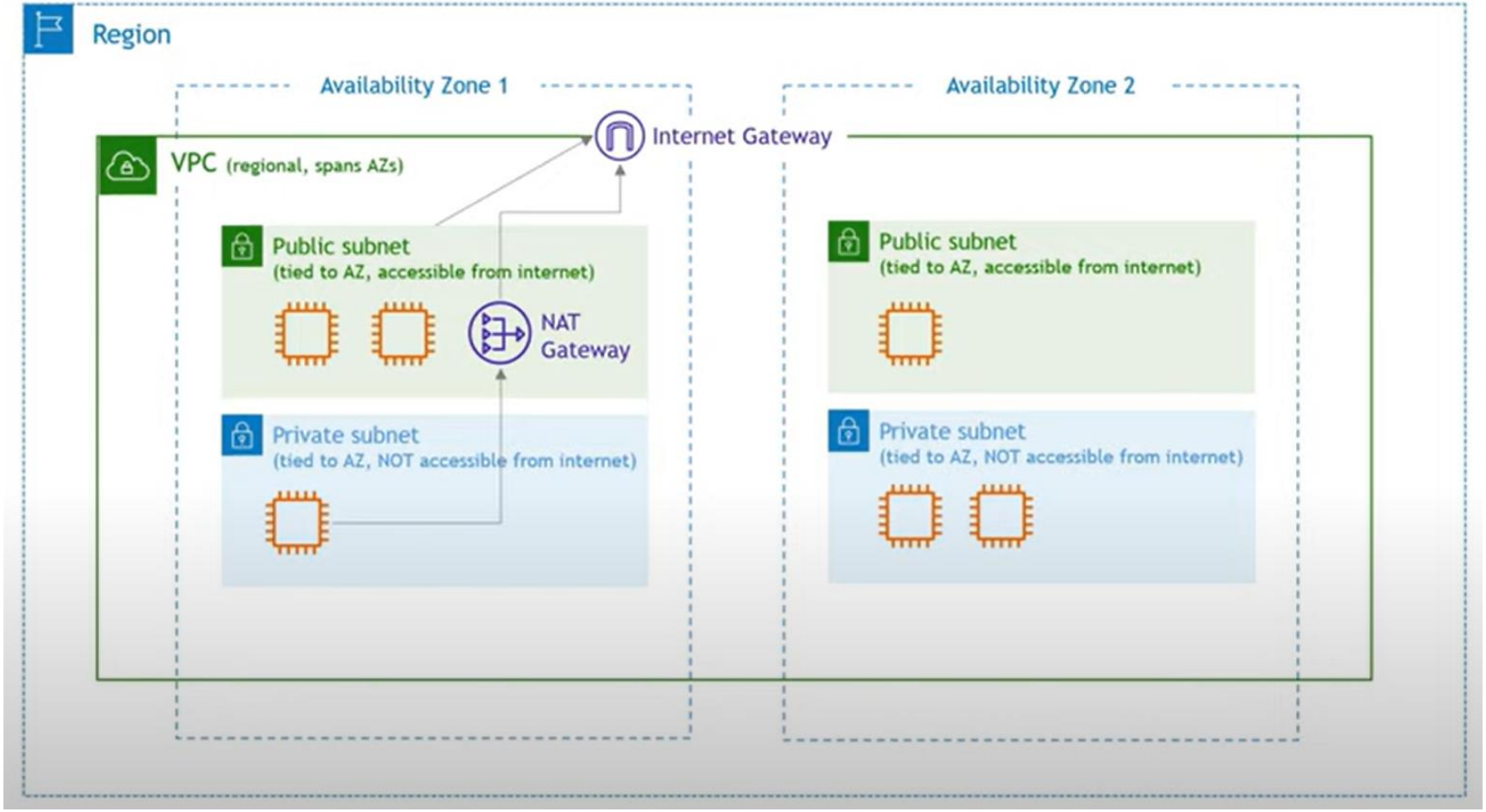
How does network Virtualisation work?

- Virtual machines running applications require network connectivity to other virtual machines (internal virtualization) and the outside world (external virtualization)



https://ipwithease.com/introduction-to-vsphere-standard-switch/

Amazon Virtual Private Cloud (VPC)



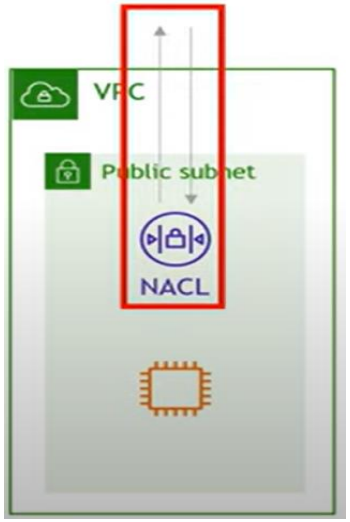
Virtual Private Cloud (VPC)

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

- With Amazon Virtual Private Cloud (Amazon VPC), AWS resources are launched in a logically isolated virtual network.
- In AWS every account will contain a default VPC but you can create your own as well.
- Each VPC has a gateway that connects the VPC to the wider internet
- You can subdivide your network (VPC) into multiple subnets and place services in those subnets
- You can choose to provide or not provide a public IP range to your subnets.
- Service instances in subnets with no public IPs can't communicate outside the cloud

Network Access and Isolation Controls

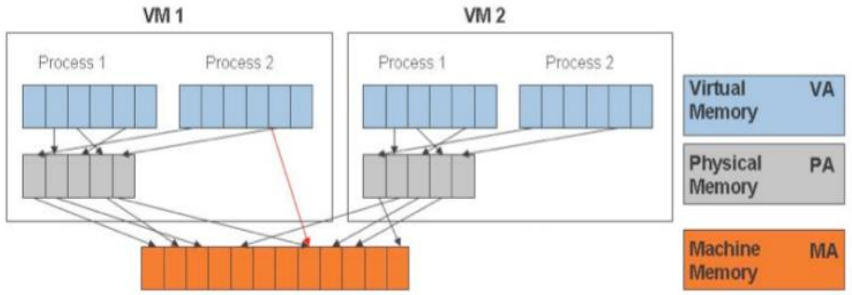
- Security groups
  - A virtual firewall that is attached to every instance
- Network access control lists
  - Operates on subnets
  - Rules defined in a NACL apply to every service instance in the subnet



MEMORY VIRTUALISATION

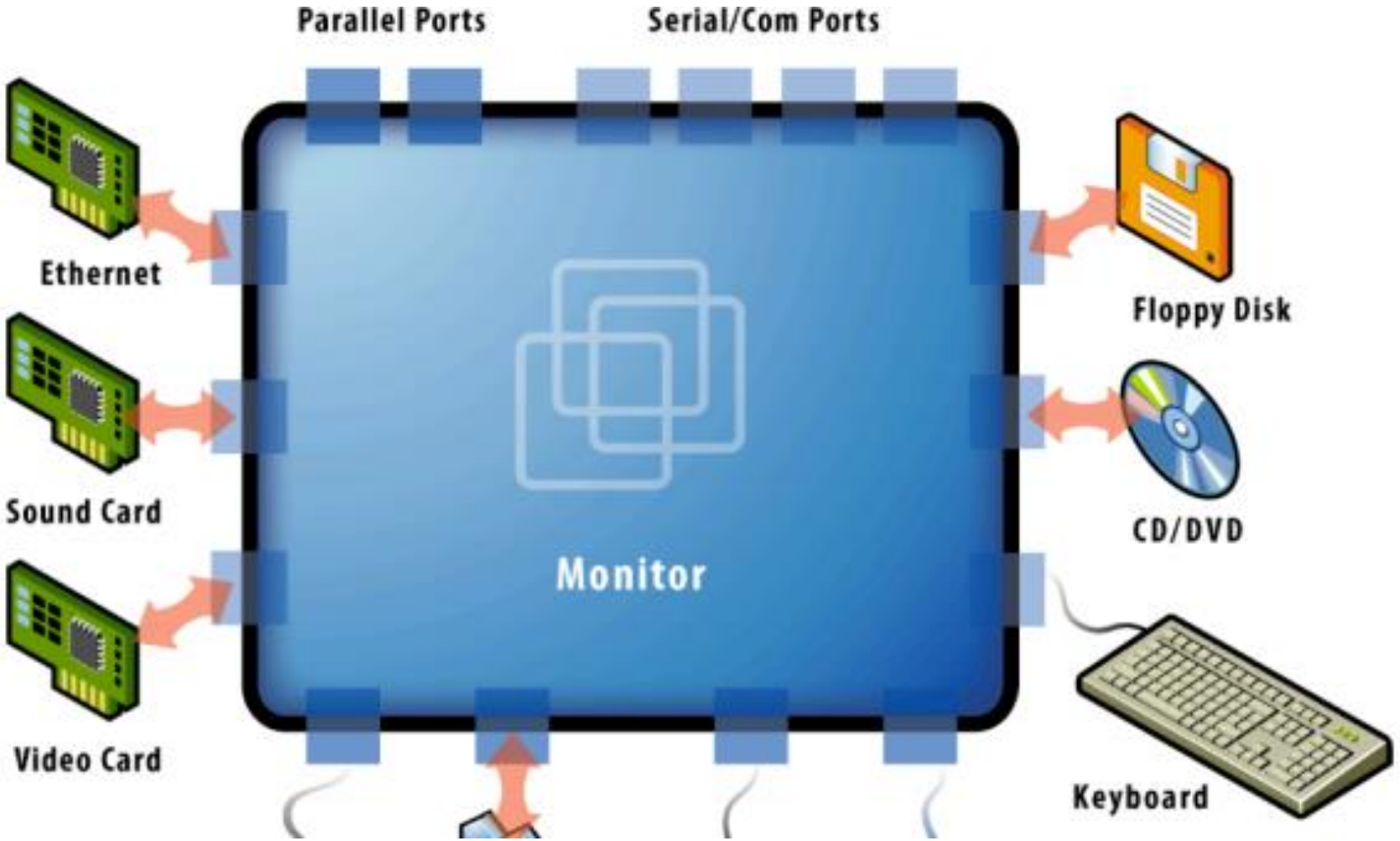
Memory Virtualization

- Sharing physical system memory and dynamically allocating it to the VMs.
- Apps see a contiguous address space that is not necessarily tied to the underlying physical memory.
- OS keeps a mapping of virtual page numbers to physical page numbers stored in page tables.
- Guest OS controls mapping of virtual addresses to guest memory physical addresses but have NO direct access to actual machine memory.



DEVICE & I/O VIRTUALIZATION

Device & I/O Virtualization



Security Issues with Virtualisation

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

- Hypervisor Attacks
- Cross VM Attacks
- Insecure API
- Misconfiguration
- Host OS Compromise
- Insecure VM Migration
- Side-Channel Attacks
- Privilege Escalation

References

- Understanding Full Virtualization, and Hardware Assist, VMWare
- Virtualization Overview, VMWare