Faculty of Engineering
Alexandria University
Electronics and Communication
Engineering department

Microprocessor

Project#4

Intel Virtualization Technology

Name: Eslam omar mohamed
NO : 54
Sec : 3

Intel Virtualization Technology

Intel Virtualization Technology (VT).Formerly known as Vanderpool, this technology enables a CPU to act as if you have several independent computers, in order to enable several operating systems to run at the same time on the same machine.

These operating systems can even be different , you can run Windows in one virtual machine and Linux in another.

virtualization technology is available in two versions:

VT-x for x86 processors

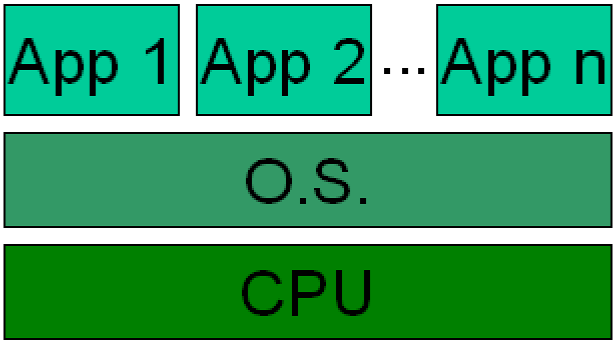
VT-I for x64 processors

-You may confuse virtualization with

Multitasking, **Multi-core,** or **Hyper-Threading.**

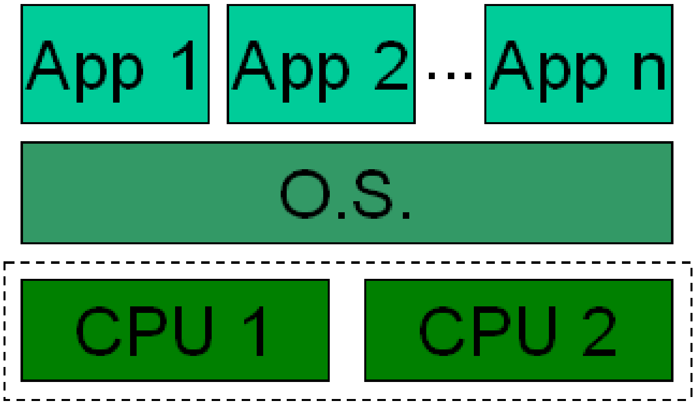
1-Multitasking:

There is a single operating system and several programs running at the same time.



2-Multi-core :

Multi-core technology allows a single processor to have more than one physical processor inside. For example, a computer with one dual-core processor acts as if it were a computer with two CPUs installed, working under a mode called symmetrical multiprocessing (SMP). Even though multi-core CPUs have more than one processor inside, they cannot be used independently. The operating system is run by the first CPU core, and the additional cores the CPU may have must be used by the same operating system.

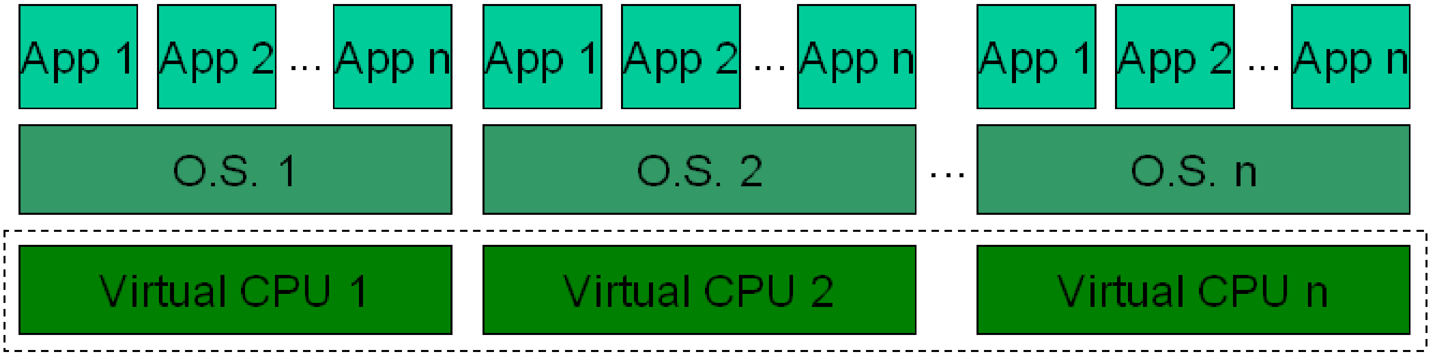


3-Hyper-Threading :

Hyper-Threading technology simulates an additional processor per CPU core. For example, a dual-core CPU with Hyper-Threading technology is seen by the operating system as if it were a quad-core CPU. These additional processors cannot run separate operating systems, so for the operating system the Hyper-Threading technology has the same effect as the multi-core technology.

But With

VIRTUALIZATION, you can have several operating systems running in parallel, each one with several programs running. each operating system thinks it is running on a completely independent COMPUTER.



- Virtualization Technology uses the same idea as the Virtual 8086 (V86) mode, which has been available since the 386 processor. With the V86 mode you can create several virtual 8086 machines to run DOS-based programs at the same time, each one that it is running in a completely independent computer.

- There is software such as VMware that enables virtualization.

- **Why implement Virtualization Technology inside the CPU?**

The advantage is that CPUs with Virtualization Technology have some new instructions to control virtualization. With them, controlling software (called VMM, Virtual Machine Monitor) can be simpler, thus improving performance compared to software-based solutions. When the CPU has support to Virtualization Technology, the virtualization is said to be hardware-based or hardware-assisted.

How It Works !!!

Processors with Virtualization Technology have an extra instruction set called Virtual Machine Extensions or **VMX**.

VMX brings 10 new virtualization-specific instructions to the CPU:

VMPTRLD, VMPTRST, VMCLEAR, VMREAD, VMWRITE, VMCALL, VMLAUNCH, VMRESUME, VMXOFF, and VMXON.

There are two modes to run under virtualization:

-VMX root operation

-VMX non-root operation

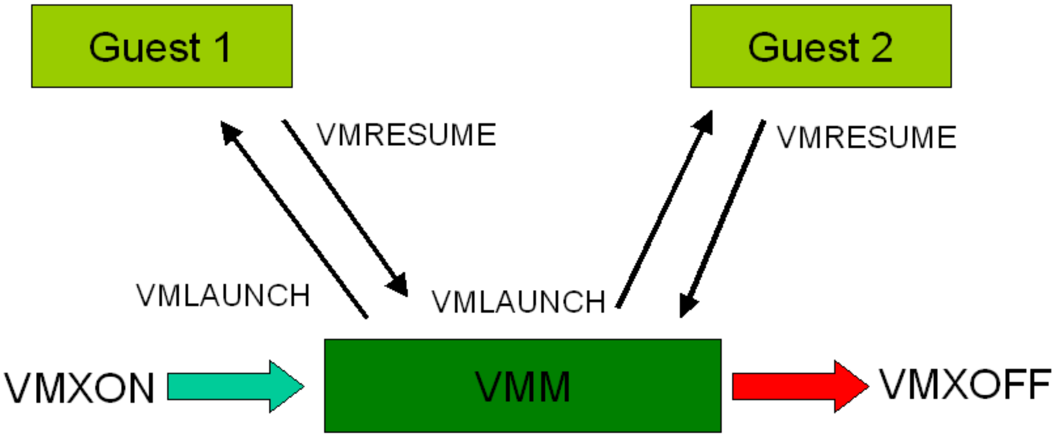
Usually, only the virtualization controlling software, called **Virtual Machine Monitor (VMM)**, runs under **root operation**.

while operating systems running on top of the virtual machines run under **non-root operation.**

→the software should execute the **VMXON** instruction and then call the VMM software.

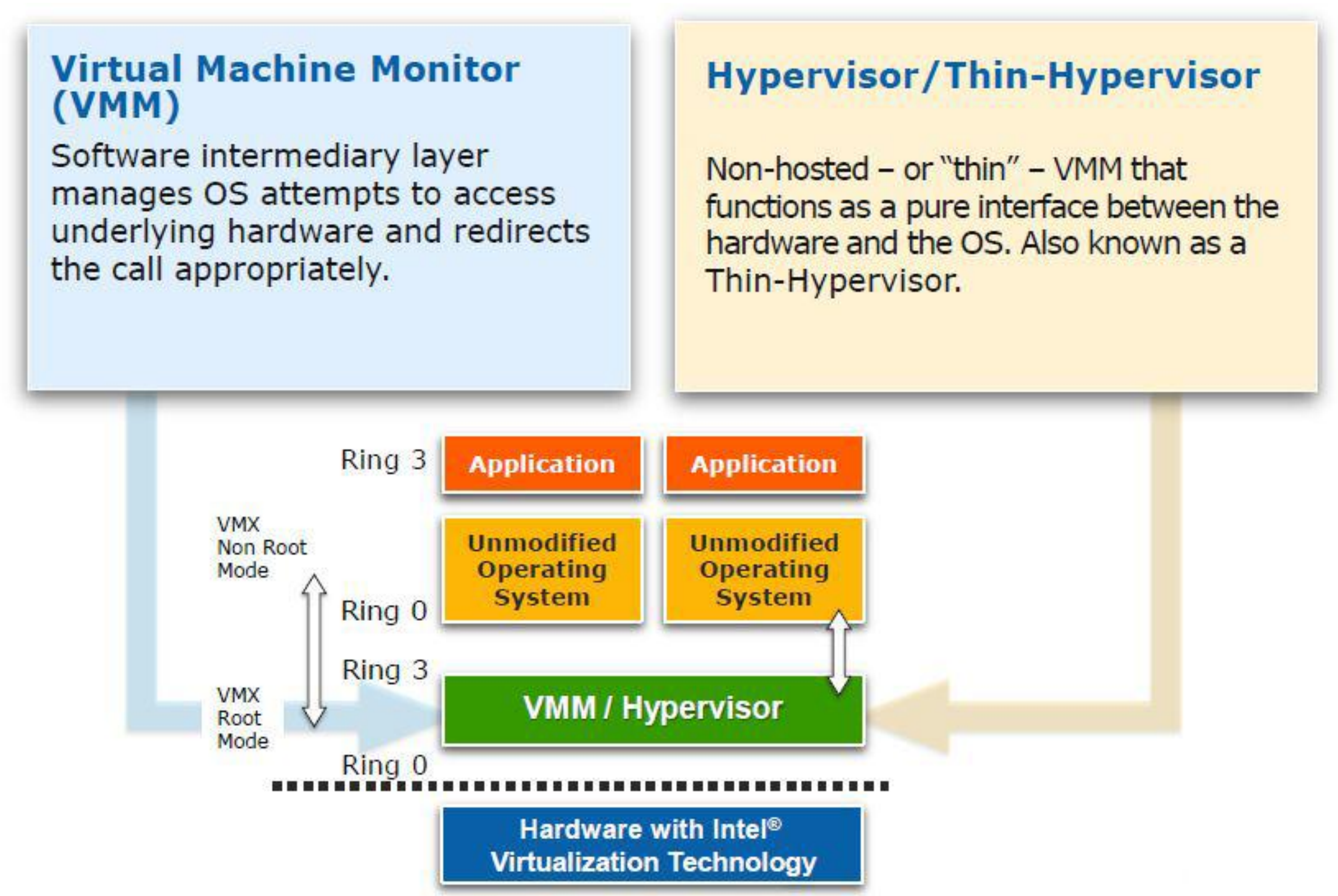
→The VMM software can enter each virtual machine using the **VMLAUNCH** instruction

→exit it by using the VMRESUME instruction. If the VMM wants to shutdown and exit the virtualization mode, it executes the **VMXOFF** instruction



Virtual machine monitor (VMM) and hypervisor

A hypervisor or virtual machine monitor (VMM) is a piece of computer software that creates and runs virtual machines.



Virtual Machine Monitor (VMM)

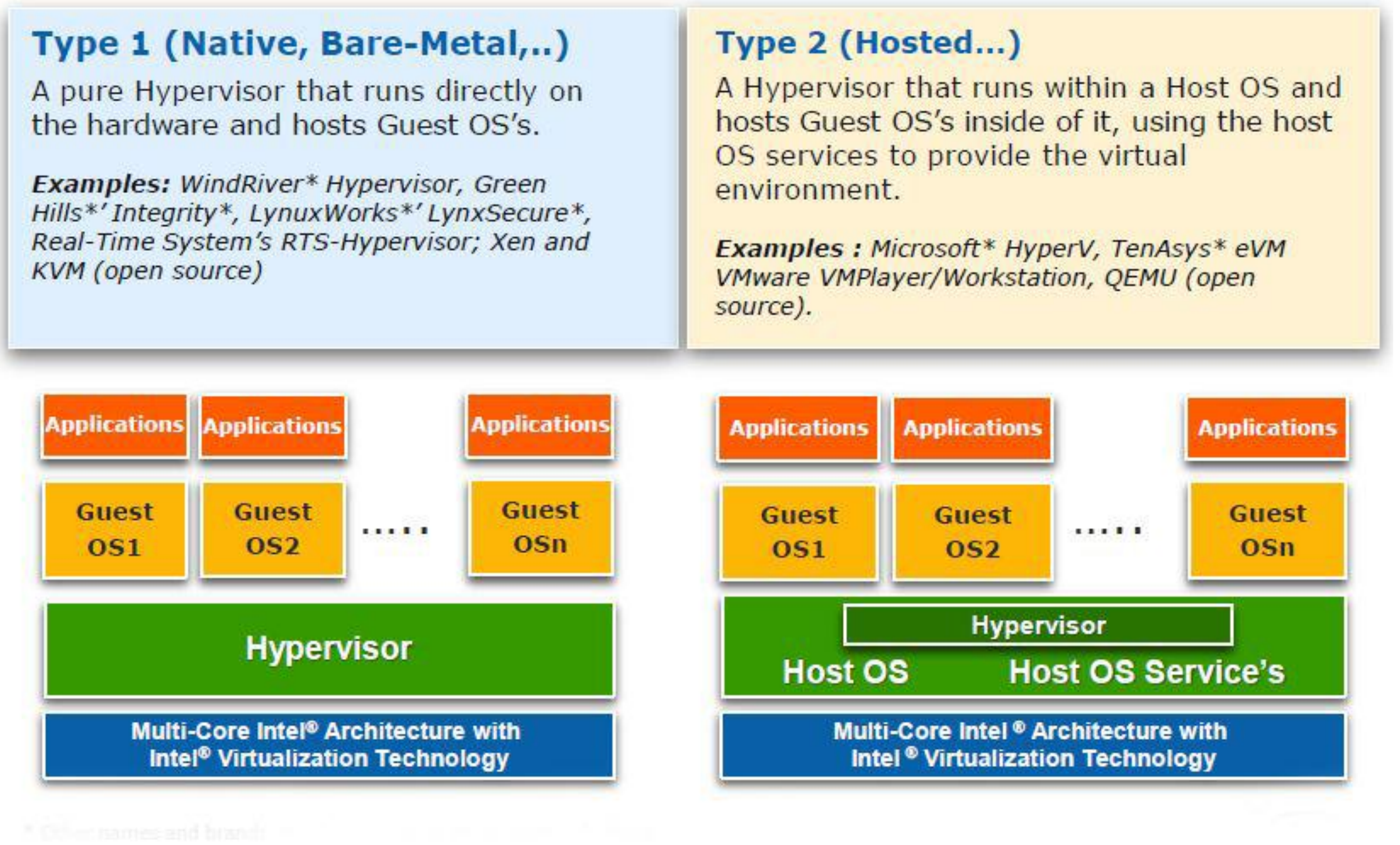
Software intermediary layer manages OS attempts to access underlying hardware and redirects the call appropriately.

Hypervisor/Thin-Hypervisor

Non-hosted – or "thin" – VMM that functions as a pure interface between the hardware and the OS. Also known as a Thin-Hypervisor.

Ring 3
Application
Application
VMX Non Root Mode
Unmodified Operating System
Unmodified Operating System
Ring 0
Ring 3
VMX Root Mode
VMM / Hypervisor
Ring 0
Hardware with Intel® Virtualization Technology

There is two type of hypervisor



Type 1 (Native, Bare-Metal,..)

A pure Hypervisor that runs directly on the hardware and hosts Guest OS's.

Examples: *WindRiver* Hypervisor, Green Hills*' Integrity*, LynuxWorks*' LynxSecure*, Real-Time System's RTS-Hypervisor; Xen and KVM (open source)*

Type 2 (Hosted...)

A Hypervisor that runs within a Host OS and hosts Guest OS's inside of it, using the host OS services to provide the virtual environment.

Examples : *Microsoft* HyperV, TenAsys* eVM VMware VMPlayer/Workstation, QEMU (open source).*

* Other names and brands [illegible]