HARDWARE-ASSISSTED VIRTUALIZATION OVER SOFTWARE-BASED VIRTUALIZATION

BY
MONTDHER ALABADI

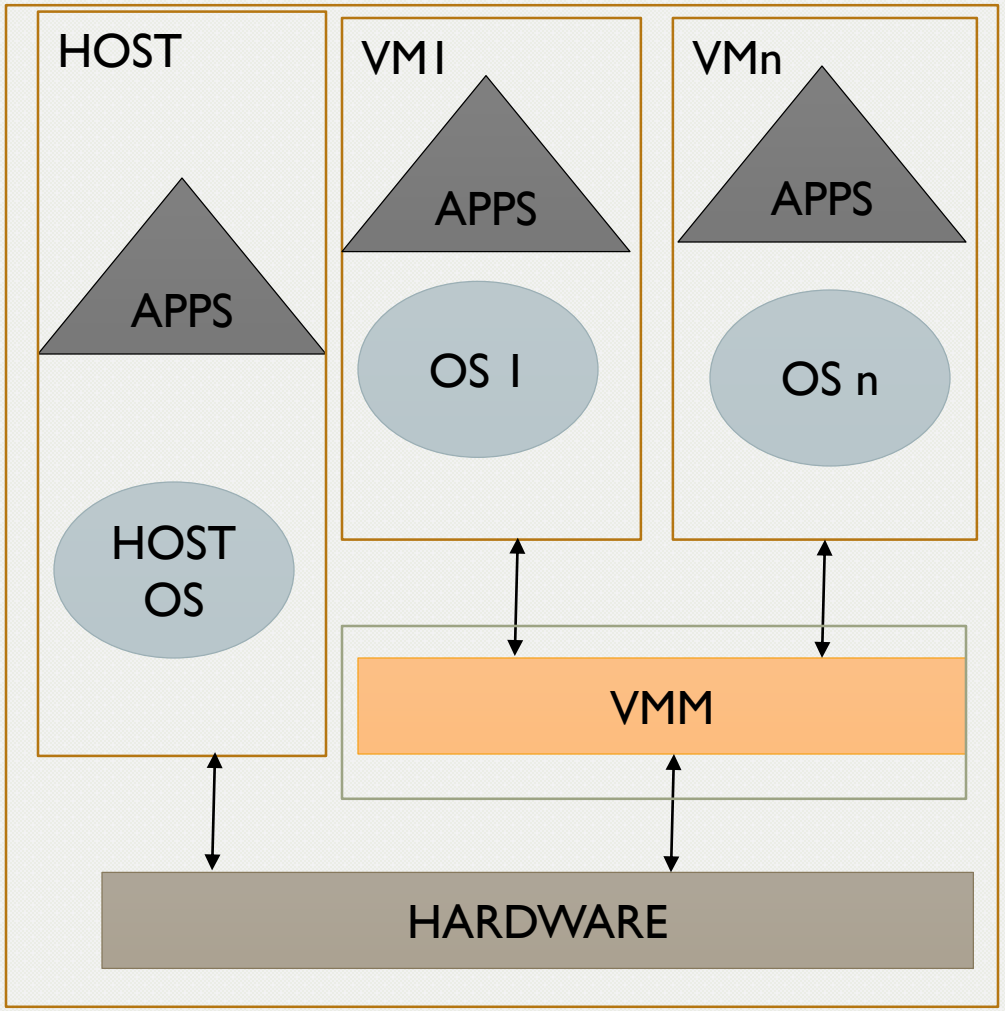
PROBLEMS OF THE PRESENTATION

1. **What is virtualization?**
2. **What is software-based virtualization and what is the problem of it ?**
3. **How intel provide hardware assissted virtualization?**
4. **Benefits of virtualization.**
5. **Another hardware-assissted virtualization approaches.**

1. WHAT IS VIRTUALIZATION?

1. WHAT IS VIRTULAIZATION

- **Virtualization** describes a technology in which an application, guest operating system is abstracted away from the true underlying hardware or software
- A key of the virtualization technology is VMM which is emulate the underlying hardware.

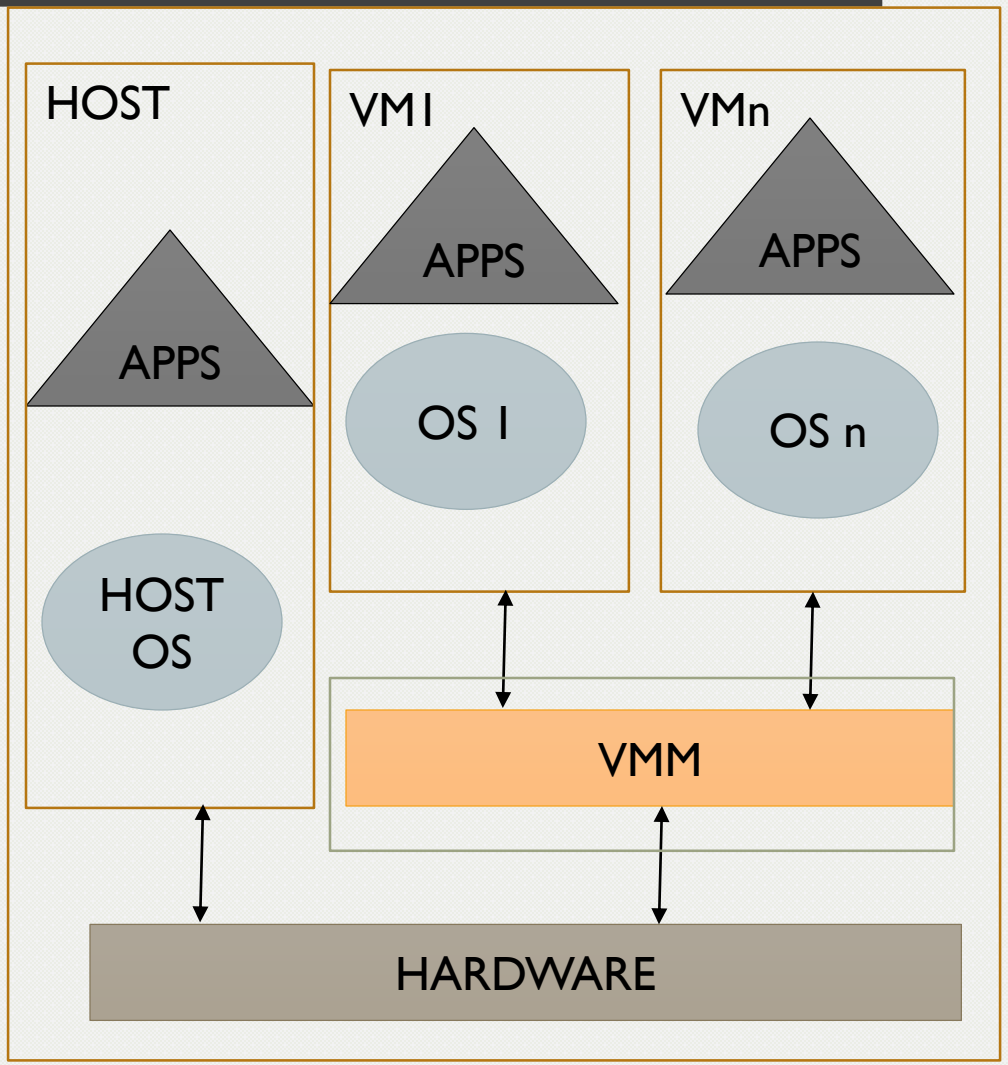


1.WHAT IS VIRTULAIZATION

- **VIRTUAL MACHINE" (VM)** -a tightly isolated software container with an operating system and application inside.
- **VMM(Virtual Machine Monitor)**

- It is the control system at the core of virtualization

- It acts as the control and translation system between the VMs and the hardware.



2.WHAT IS SOFTWARE-BASED VIRTUALIZATION AND WHAT IS THE PROBLEM OF IT ?

2. WHAT IS SOFTWARE-BASED VIRTUALIZATION AND WHAT IS THE PROBLEM OF IT ?

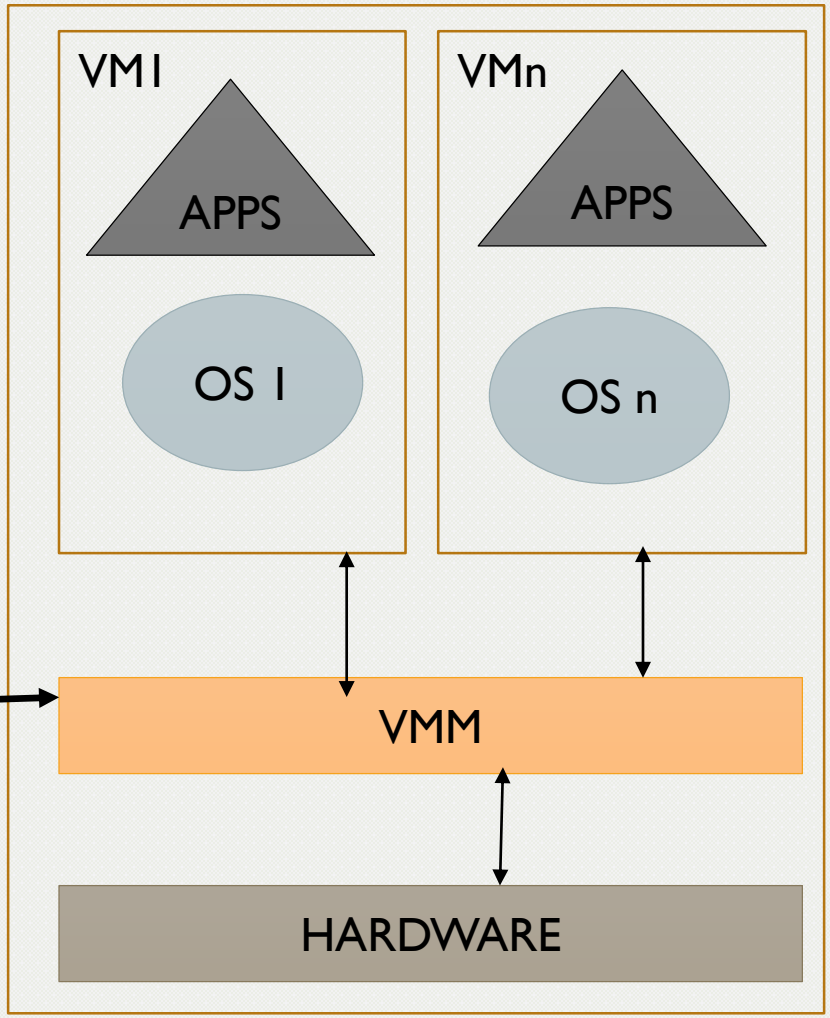
- **SOFTWARE-BASED VIRTUALIZATION:**

- The guest **"normal"** instructions runs directly on the processor

Ex..Add, sub, etc

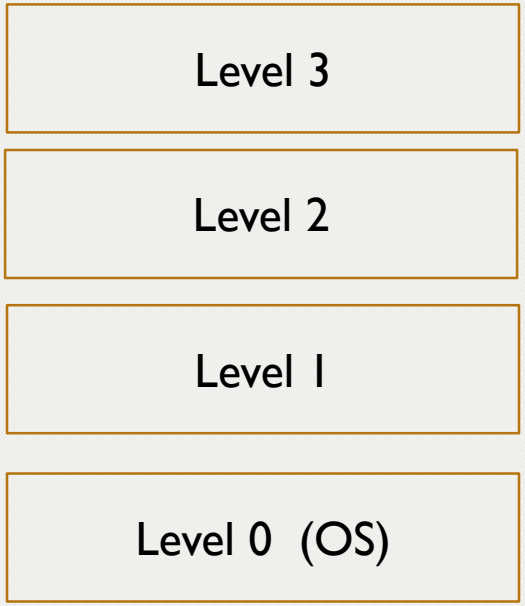
- While the **guest privileged** instruction is translated and the translated instruction executes on the processor.

Ex..System calls, traps, or page table updates .



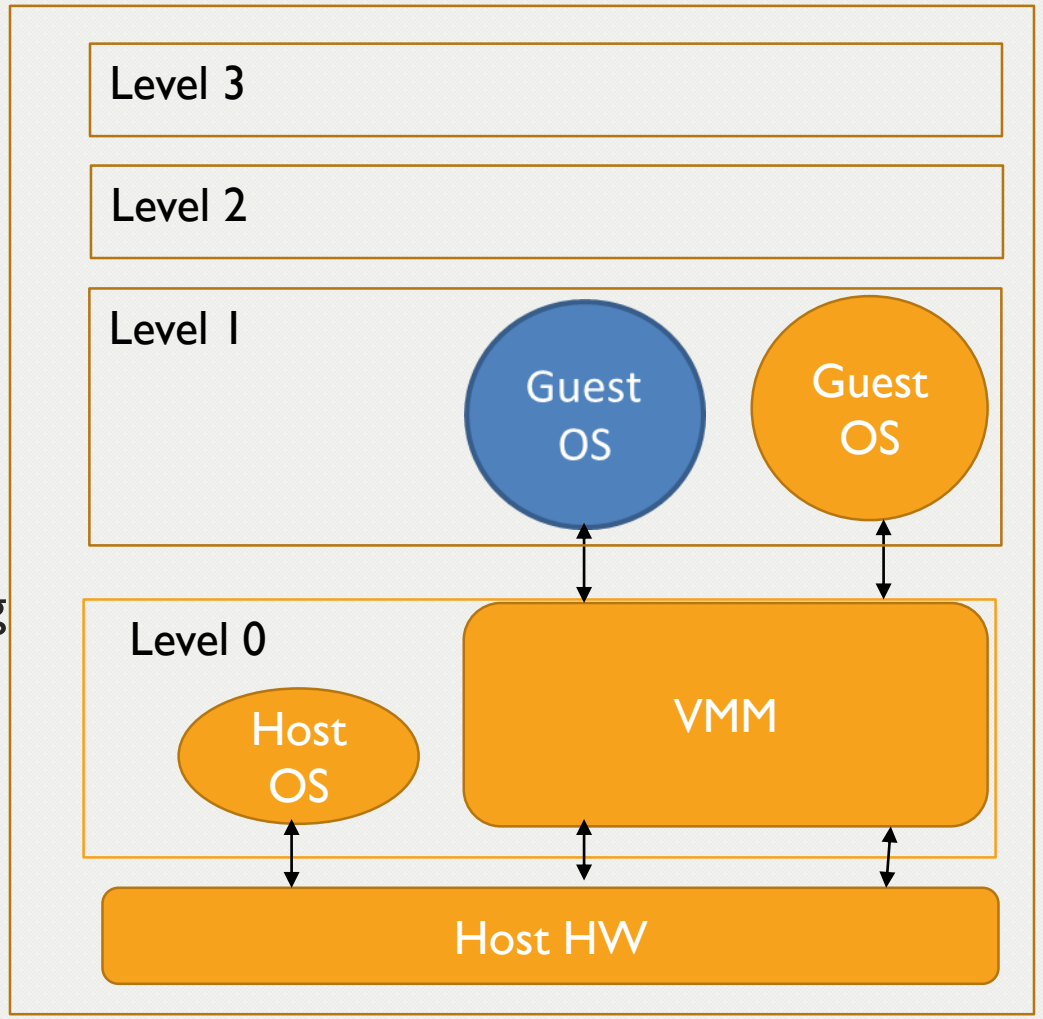
2.WHAT IS SOFTWARE-BASED VIRTUALIZATION AND WHAT IS THE PROBLEM OF IT(PRIVILEGES LEVEL) ?

- There are four privilege levels, numbered 0 (most privileged) to 3 (least privileged).
- At any given time CPU is running in a specific privilege level, which determines what code can and cannot do.
- any attempt to run code outside privilege level cause a general-protection exception.



2.WHAT IS SOFTWARE-BASED VIRTUALIZATION AND WHAT IS THE PROBLEM OF IT ?

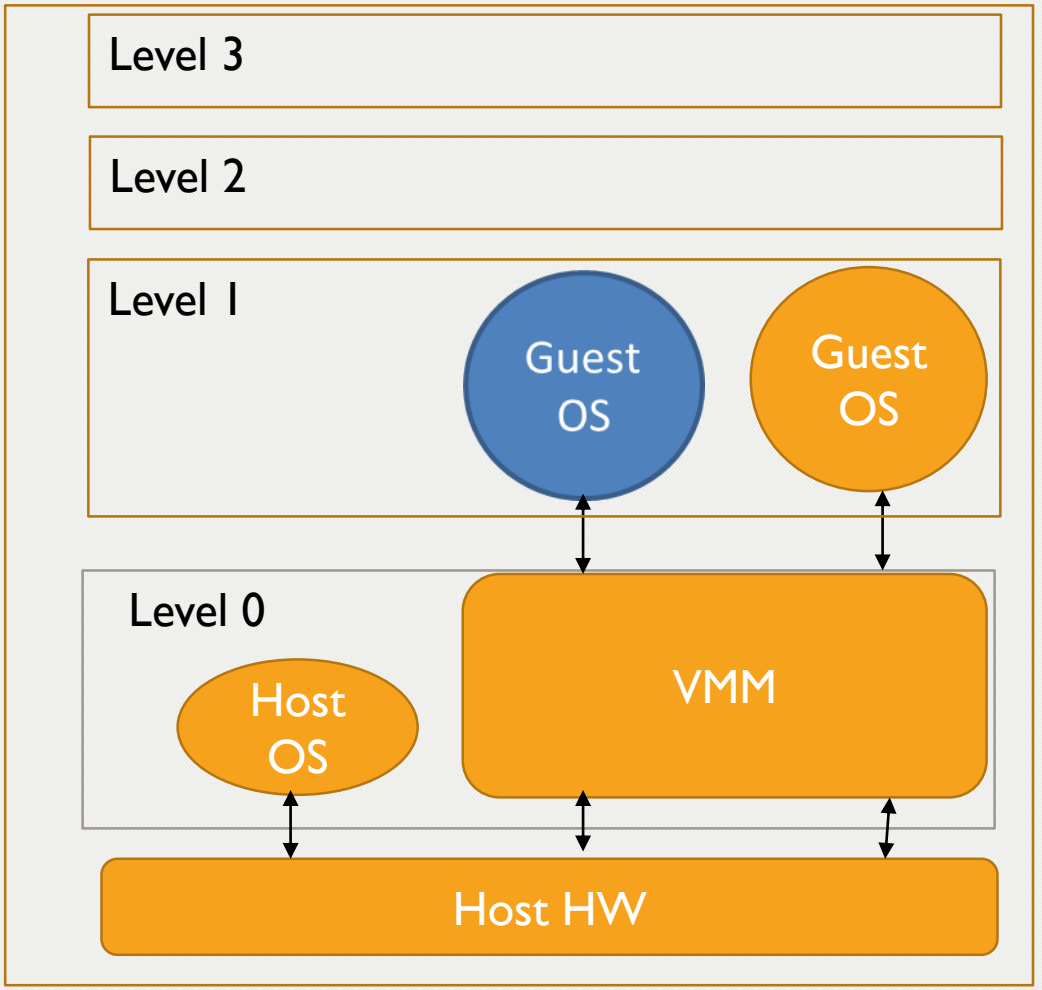
- the host OS and VMM work in Ring 0, the highest privilege level in the system.
- guest OSs are typically designed to also work at privilege level 0
- But the host OS and VMM occupy level 0 and cant share it
- so the guest OSs must operate using a lower privilege level at Ring 1.



2. WHAT IS SOFTWARE-BASED VIRTUALIZATION AND WHAT IS THE PROBLEM OF IT ?

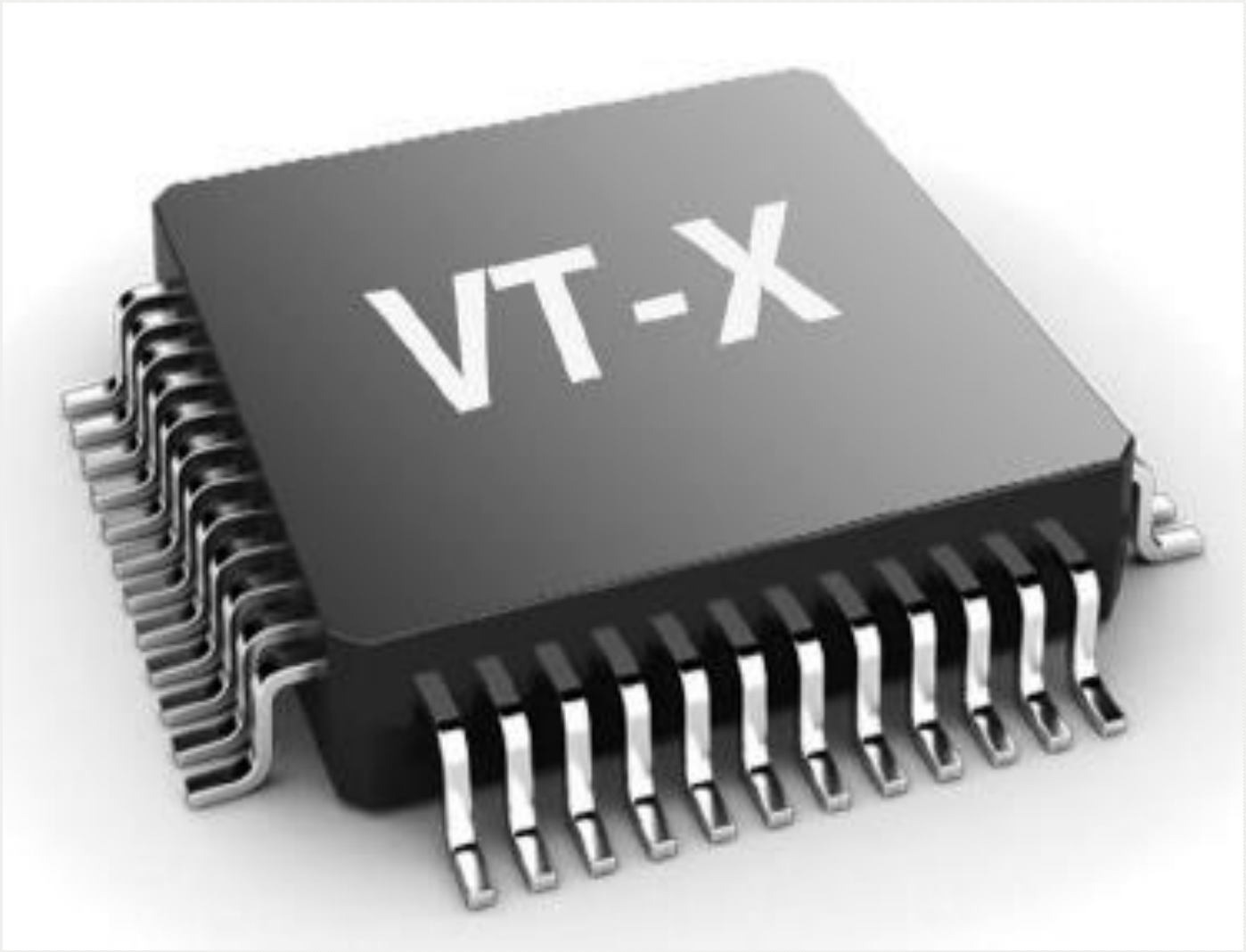
- **PROBLEMS:**

1. Overhead result from translation between the guest OS and the hardware platform.
2. Processor will be intensive because of software-based translations on the calls to hardware resources made by the guest os.
3. This translation consumes processing resources, limiting the performance and scalability of the overall system.



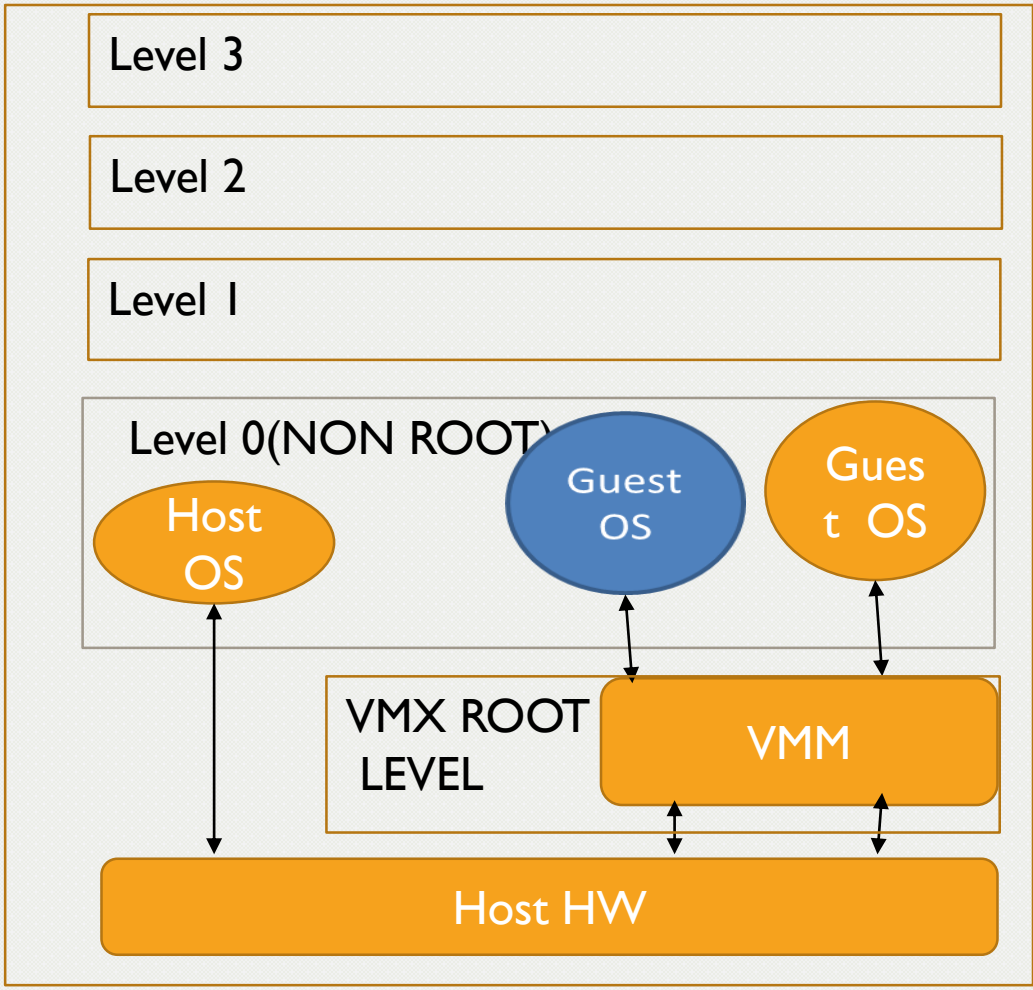
IT IS PRIVILGES PROBLEM

3. HOW INTEL PROVIDE HARDWARE ASSISTED VIRTUALIZATION?


VT-X

3.HOW INTEL PROVIDE HARDWARE ASSISTED VIRTUALIZATION?

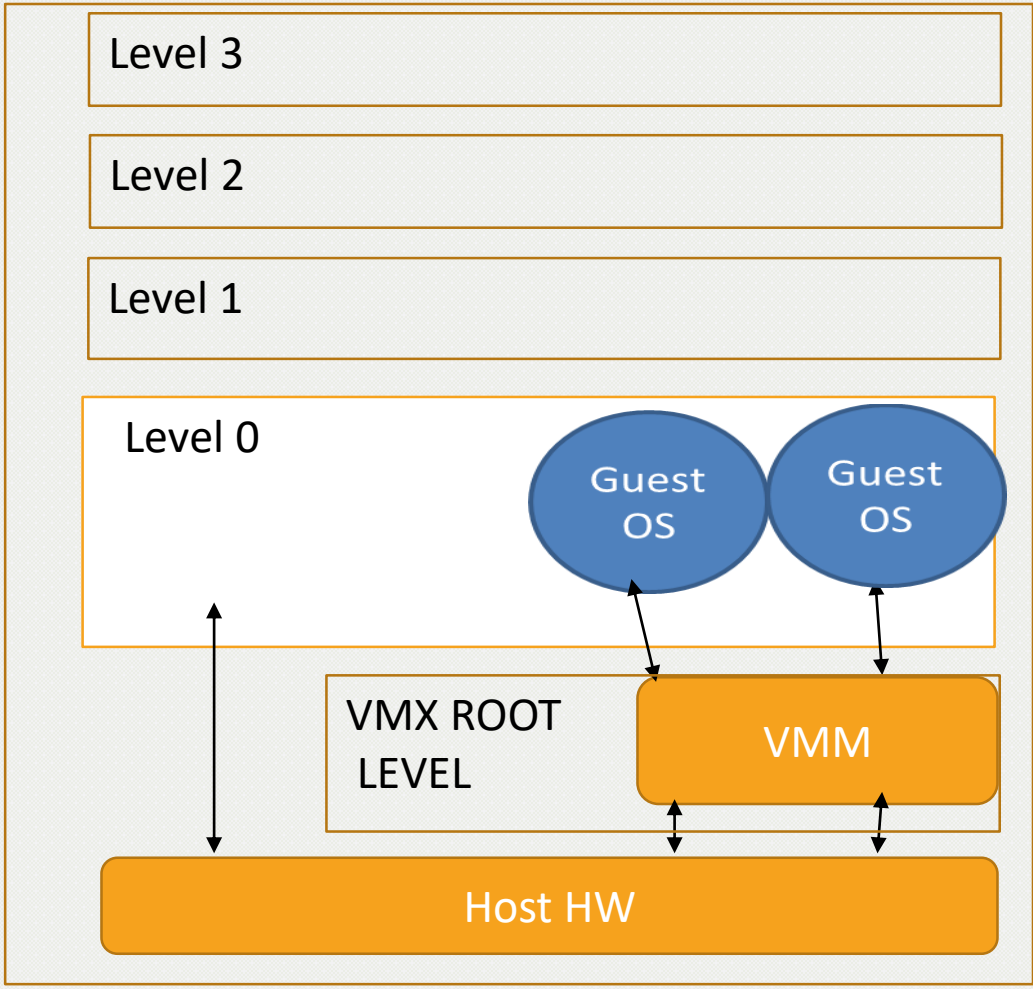
- INTEL (VT-X) - is a hardware assisted virtualization technology embeded in their processors.
- INTEL (VT-X) provides a privilege level known as VMX root specifically for the VMM, leaving ring 0 available for use by guest OS and this level called "VMX NON-ROOT".



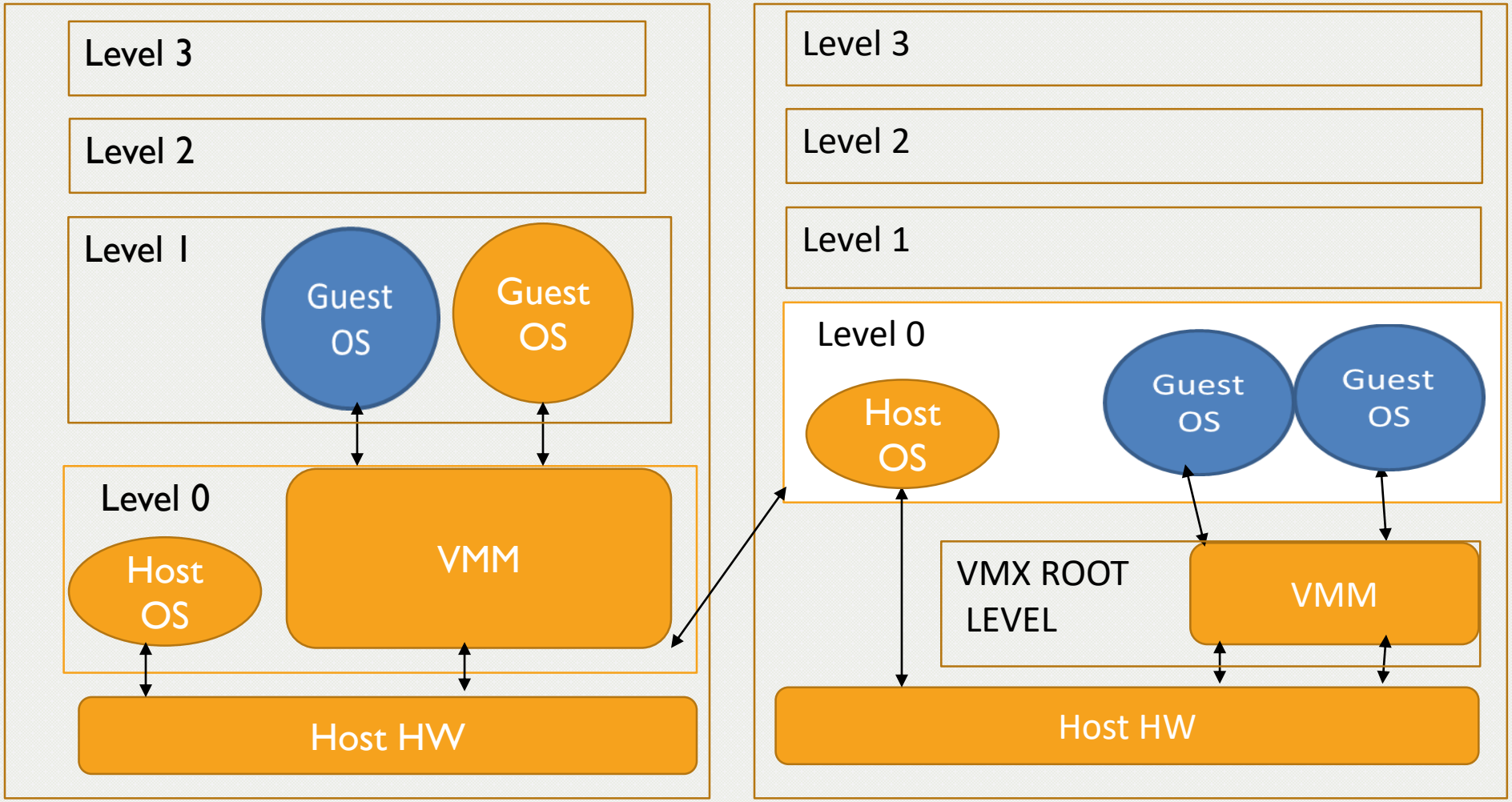
3.HOW INTEL PROVIDE HARDWARE ASSISTED VIRTUALIZATION?

- This technique support :

1. Eliminating processor-intensive software-based translations
2. VMM itself can be smaller and less complex
3. increasing performance
4. No need for guest OSs to be modified for use in a virtualized environment.



3.HOW INTEL PROVIDE HARDWARE ASSISTED VIRTUALIZATION(CONCLUSION)?



4.BENEFITS OF VIRTUALIZATION

4.BENEFITS OF VIRTUALIZATION.

1.Cost-effectiveness – less hardware

- **Multiple virtual machines / operating systems / services on single physical machine (*server consolidation*)**
- **Various forms of computation as a service**

2.Isolation

- **Good for security**
- **Great for reliability and recovery: If VM crashes it can be rebooted, does not affect other services (*fault containment*)**
- **VM migration**

3.Development tool

- **Work on multiple OS in parallel**
- **Develop and debug OS in user mode**
- **Origins of VMware as a tool for developers**

5. ANOTHER HARDWARE-ASSISSTED VIRTUALIZATION APPROACHES.

5. ANOTHER VIRTUALIZATION APPROACHES

- Memory virtualization
- I/O virtualization
- Graphics Virtualization Technology
- Virtualization of Security and Network