Virtualization & Xen's Approach

Feb 23, 2011

Outline

- Virtualization
- Xen

Virtualization?

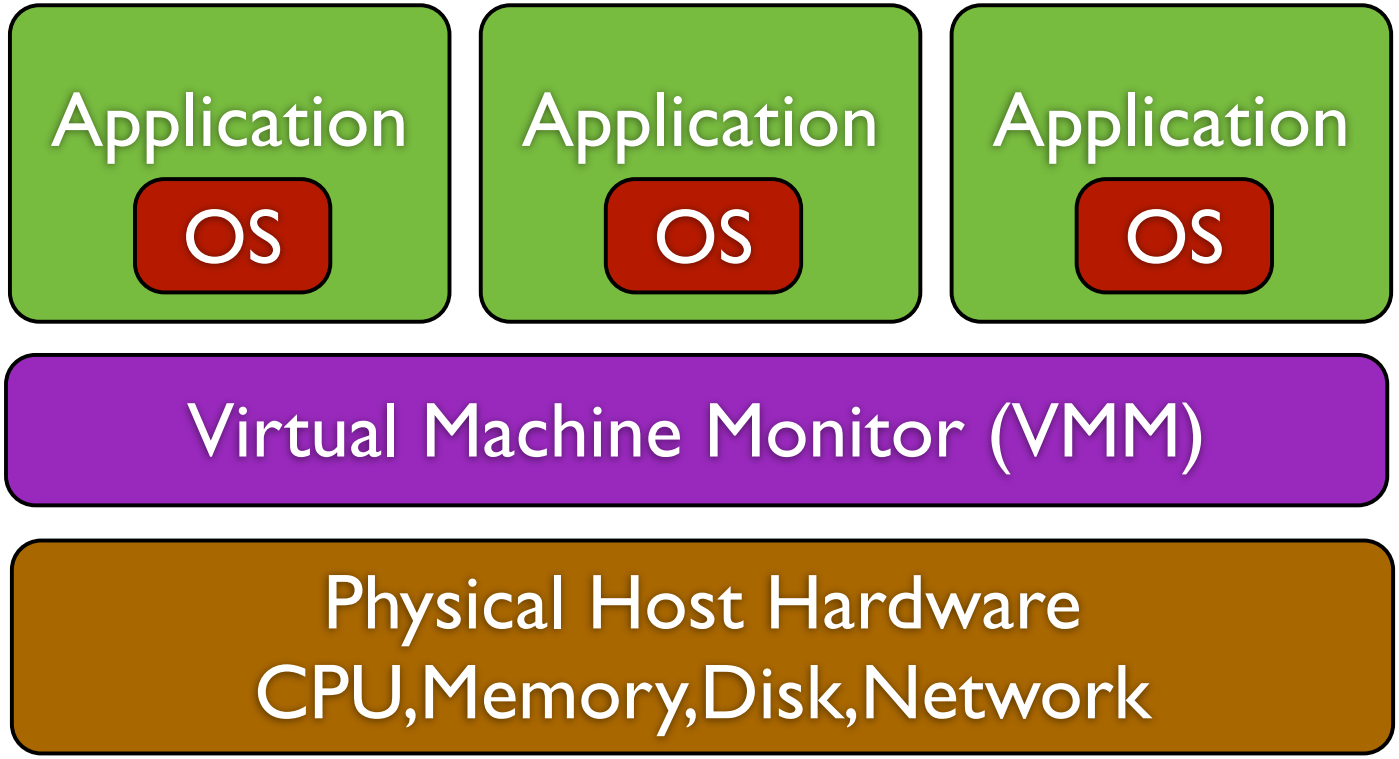
- Inspired by IBM (VM/370) in 1970s
- Multiple OS instances run concurrently on a single computer
- OS instances shares the available common hardware resources

Virtualization?

- Creation of virtual machine that acts like a real computer with an operating system.
- Software executed on these virtual machines are separated from the underlying hardware resources.
- Add a layer of abstraction between the applications and the hardware

From wiki:
http://en.wikipedia.org/wiki/Virtualization

Virtualization?



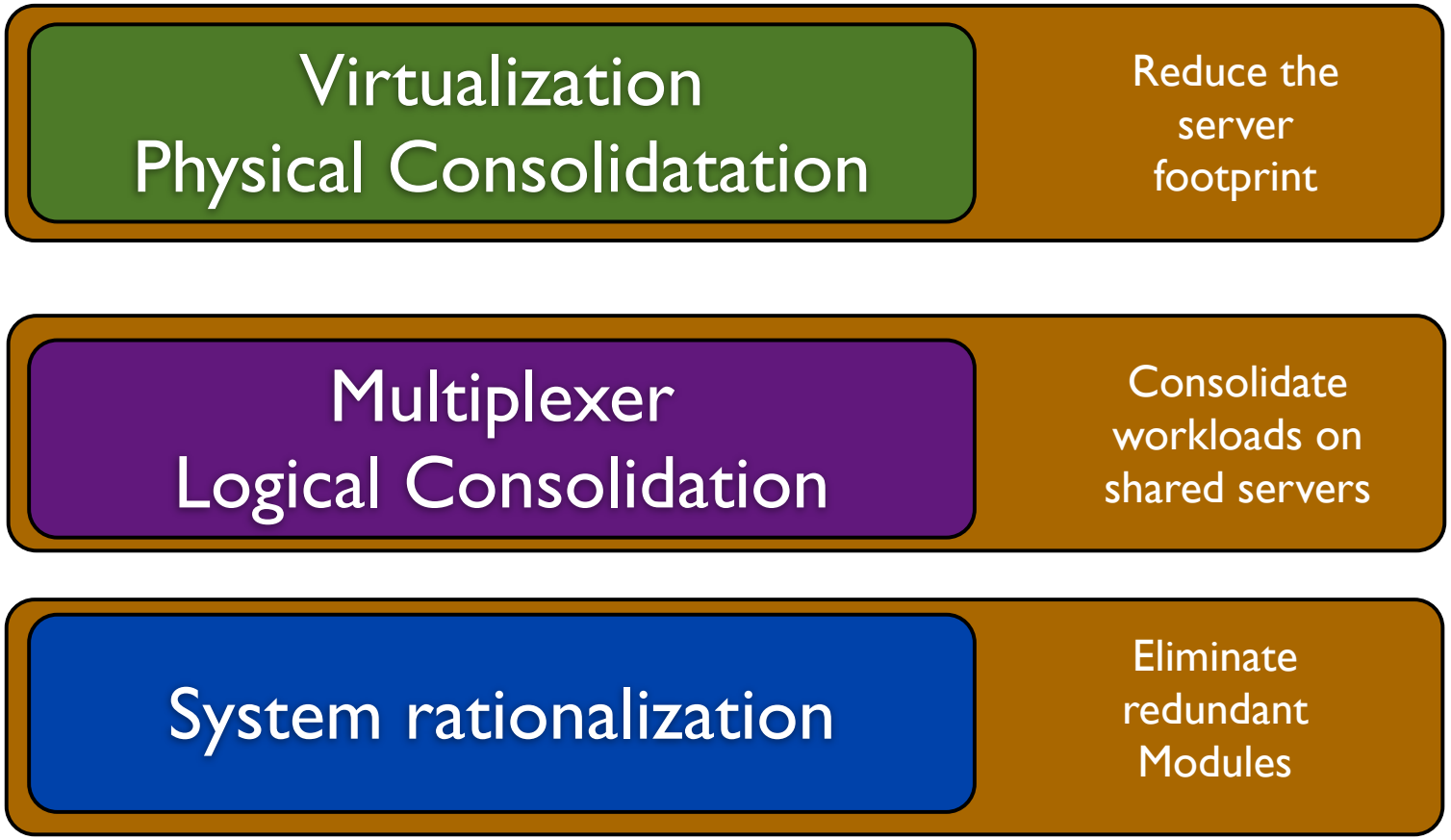
Virtualization?

- Types of Virtualization
  - Full Virtualization
  - Para-Virtualization (Guest OS need modified)

Virtualization?

- Why Virtualization?
  - Increase server utilization
  - Legacy software migration
  - Mixed environments per physical system
  - Isolation (Fault,performance)

Virtualization?



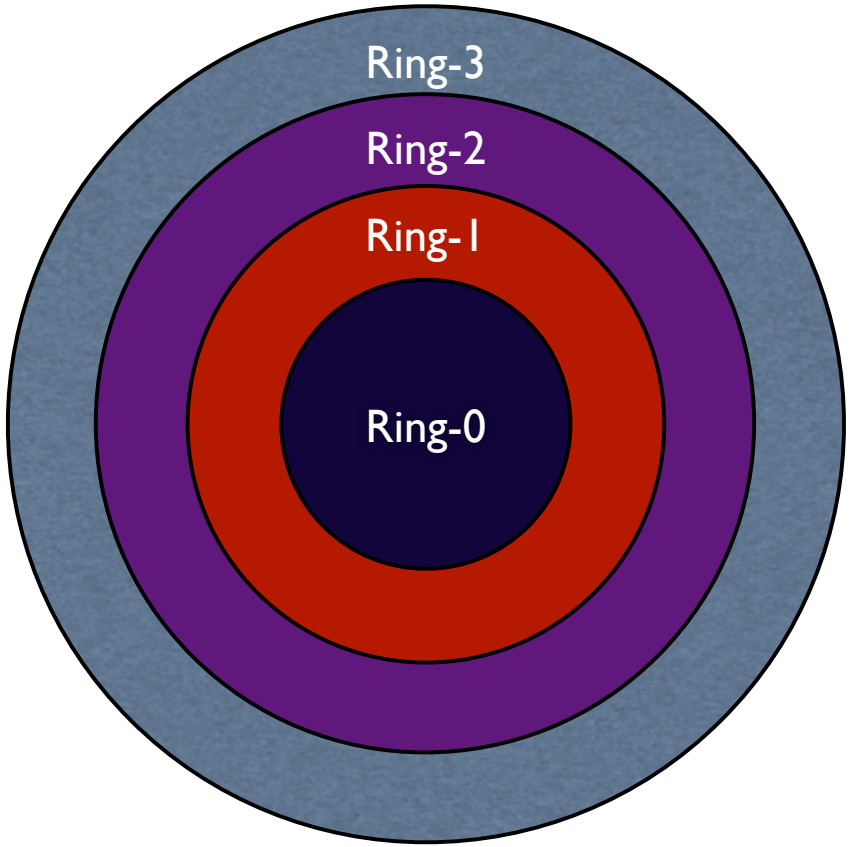
System Optimization

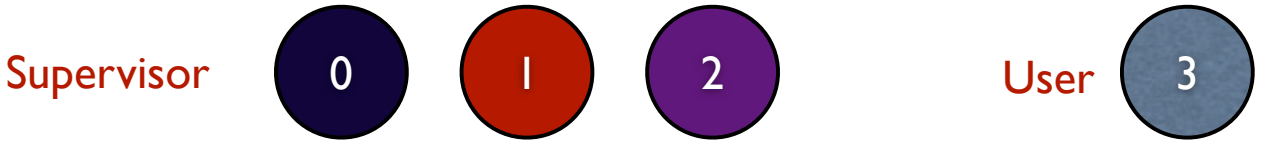
Challenges?

- The Popek and Goldberg Requirements
  - “Formal Requirements for Virtualizable Third Generation Architectures”,1974
  - Equivalence (Fidelity)
  - Resource control (Safety)
  - Efficiency (Performance)

Challenges?

- CPU Architecture
  - Protection rings originated from MULTICS
  - X86's protected mode

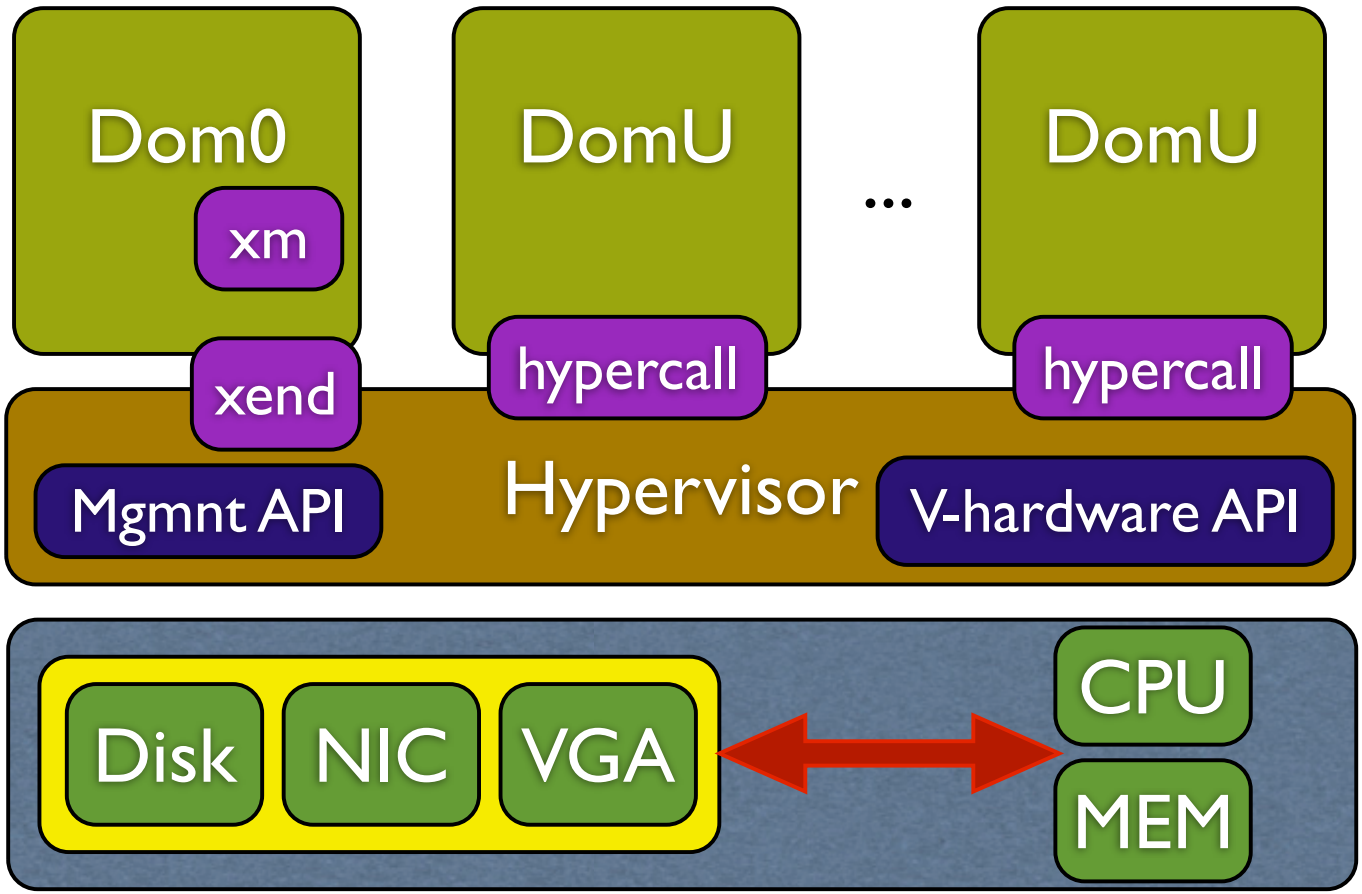




Xen

- Xen is an open-source VMM, or hypervisor, for both 32 and 64-bit processor architectures.
- Runs directly on top of hardware
- Near-native performance
- Live, zero-downtime migration
- Support both para-virtualization and hardware-assisted full virtualization

Xen



- The management VM (Dom0) is responsible for interacting with hypervisor
- Other VMs (DomU) are called guests

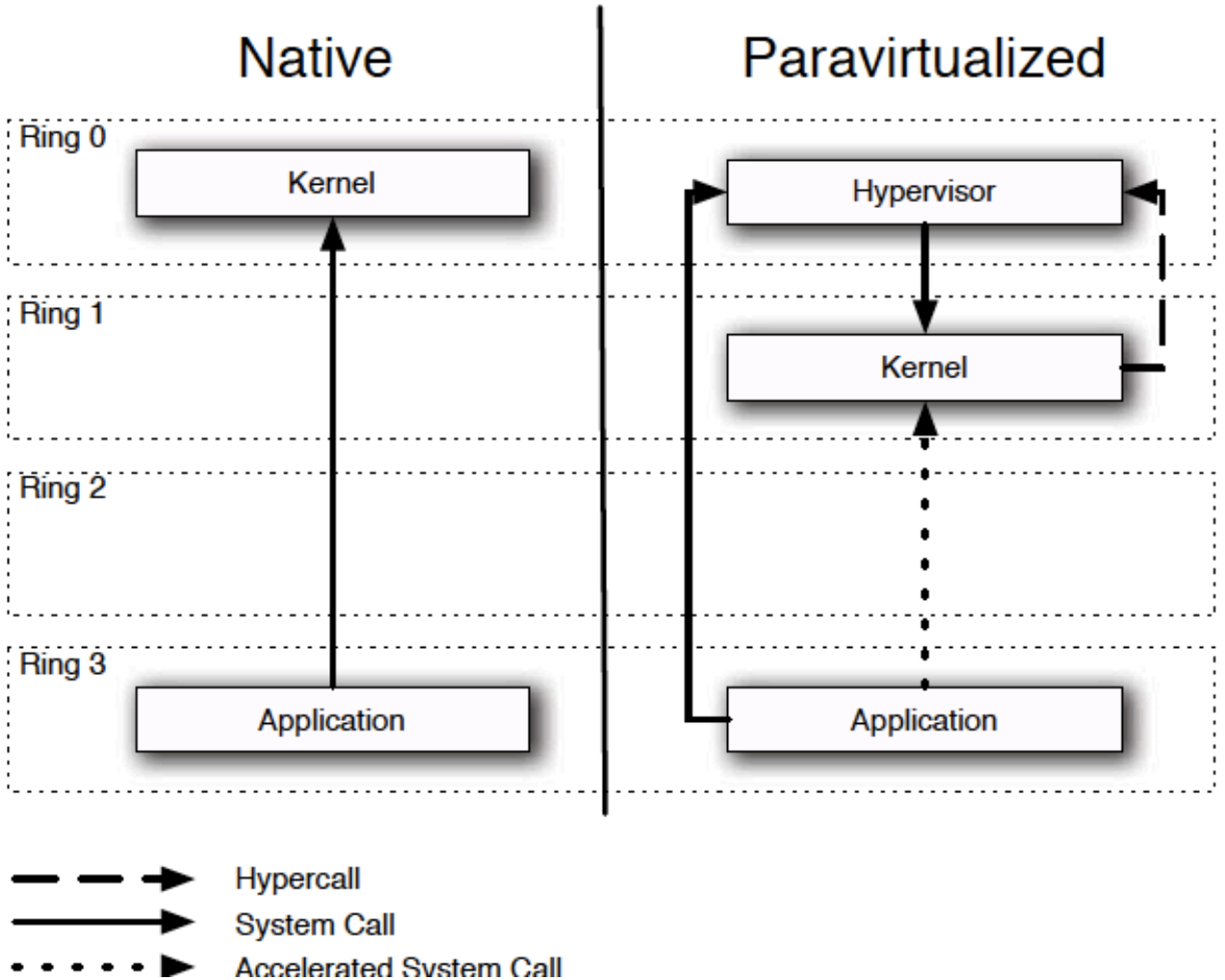
Xen's ParaV

- Other implementations of x86 VMMs place too much burden on the hypervisor.
- Deal with only low-level complexity and leave high-level operations to the guest OS
- Virtualization on CPU, MEM, Device I/O

Xen's ParaV

- CPU Virtualization
  - The guest operating system must run at a more restricted privilege level than Xen
  - The Xen-aware guest operating system registers a table for exception trap handlers.
  - Exceptions are catered to system calls in the guest OS or performed by Xen.

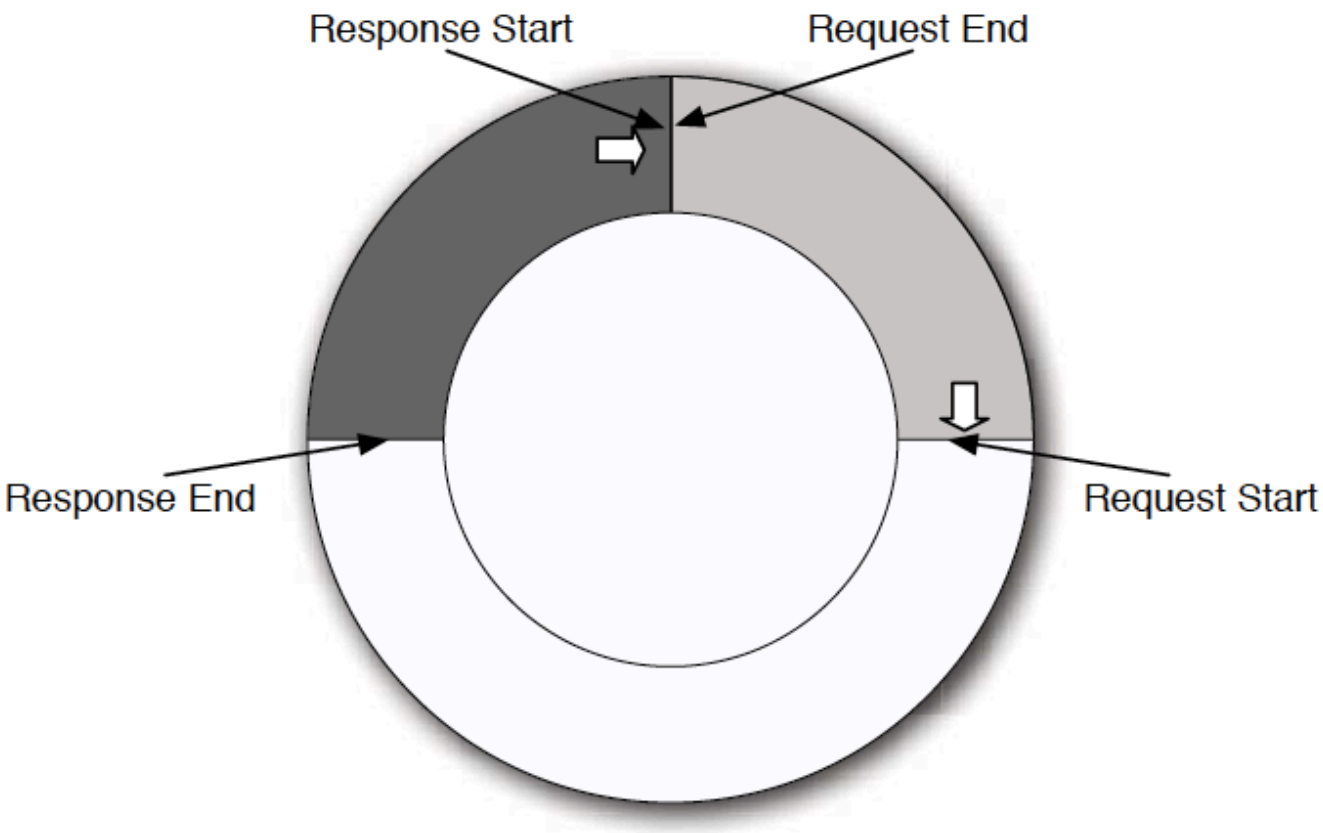
CPU V


Native
Paravirtualized
Ring 0
Ring 1
Ring 2
Ring 3
Kernel
Hypervisor
Kernel
Application
Application
Hypercall
System Call
Accelerated System Call

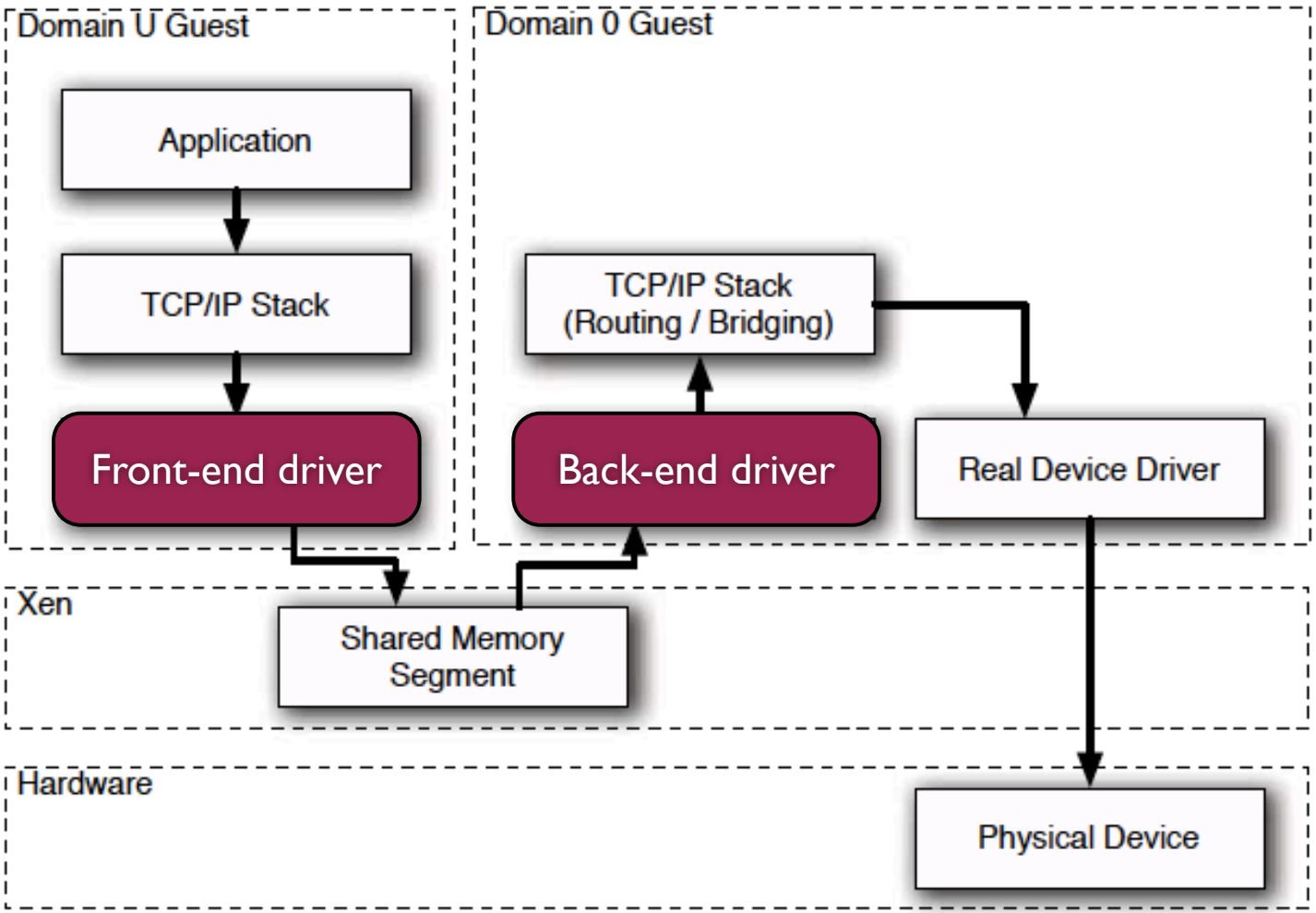
I/O V

- Virtualize I/O devices, such as network interfaces and hard drivers
- Emulation? No. Split Drivers.
- Device I/O rings.

I/O Ring



Split Drivers



Key References

- D.Chisnall. The Definitive Guide to the Xen Hypervisor. Prentice Hall. 2007
- Paul Barham, et.al. Xen and the art of virtualization, SOSP'03