Virtualizing interrupts

OS assumes to be in control of interrupts via the interrupt table

So what happens when an interrupt or trap occurs in a virtual environment?

➡ The VMM handles the interrupt (in kernel mode) using the "virtual" interrupt handler table of the running OS

✓ Some interrupt can be shadowed

Virtualizing memory

OS assumes to be in full control over memory via the page table

But VMM partitions memory among VMs

- VMM needs to assign hardware pages to VMs
- VMM needs to control mappings for isolation
  - Cannot allow an OS to map a virtual page to any hardware page
  - OS can only map to a hardware page given to it by the VMM

Hardware-managed TLBs make this difficult

- When the TLB misses, the hardware automatically walks the page tables in memory
- As a result, VMM needs to control access by OS to page tables