Virtualizing I/O

OSes can no longer interact directly with I/O devices

Types of communication

- Special instruction – in/out
- Memory-mapped I/O
- Interrupts
- DMA

1. Make in/out trap into VMM and use tracing for memory-mapped I/O
2. Run simulation of I/O device
   - Interrupt – tell CPU simulator to generate interrupt
   - DMA – copy data to/from physical memory of virtual machine

Hardware Support

Intel and AMD implement virtualization support in their recent x86 chips (Intel VT-x, AMD-V)

- Goal is to fully virtualize architecture
- Transparent trap-and-emulate approach now feasible
- Echoes hardware support originally implemented by IBM

Execution model

- New execution mode - guest mode
  Direct execution of guest OS code, including some privileged instructions
- Virtual machine control block (VMCB)
  controls what operations trap, records info to handle traps in VMM
- New instruction `vmenter` enters guest mode, runs VM code
- When VM traps, CPU executes new `vmexit` instruction