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

Hardware Support

Memory

- Intel extended page tables (EPT), AMD nested page tables (NPT)
- Original page tables map virtual to (guest) physical pages
  managed by OS in VM, backwards-compatible
- New tables map physical to machine pages
  managed by VMM
- Tagged TLB w/ virtual process identifiers (VPIDs)
  tag VMs with VPID, no need to flush TLB on VM/VMM switch

I/O

- Constrain DMA operations only to page owned by specific VM
- AMD DEV -exclude pages (c.f. Xen memory paravirtualization)
- Intel VT-d IOMMU – address translation support for DMA