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

Virtualizing I/O - Three Models

Xen : modify OS to use low-level I/O interface (hybrid)

- Define generic devices with simple interface: virtual disk, virtual NIC, etc.
- Ring buffer of control descriptors, pass pages back and forth
- Handoff to trusted domain running OS with real drivers

VMware : VMM supports generic devices (hosted)

- E.g. AMD Lance chipset/PCNet Ethernet device
- Load driver into OS in VM, OS uses it normally
- Driver knows about VMM, cooperates to pass the buck to a real device driver
  (e.g., on underlying host OS)

VMware ESX Server: drivers run in VMM (hypervisor)