Virtual Machines
Memory Management

Kai Shen
Dept. of Computer Science, University of Rochester

Memory Virtualization
(protected page table)
- From the VM OS’s view, the page table contains mapping from virtual to VM physical addresses
- For proper operation, the page table hooked up with MMU must map virtual to real machine addresses
- VM OS cannot directly access the page table
  - each page table write is trapped, for a translation (the physical address field is translated from VM physical address to real machine address)
  - each page table read is also trapped for a reverse translation

Memory Virtualization
(shadow page table)
- VM OS maintains virtual to VM physical (V2P) page table
- VM monitor
  - maintains a VM physical to machine (P2M) mapping table
  - combines V2P and P2M table into a virtual to machine mapping table (V2M)
  - supplies the V2M table to the MMU hardware
- Page table updates
  - any VM change on its V2P page table must be trapped by VM monitor
  - VM monitor modifies V2M table appropriately

Memory Virtualization
(hardware support)
- Nested paging (AMD) or extended page tables (Intel)
- VM OS maintains virtual to VM physical (V2P) page table
- hardware maintains a nested VM physical to machine (P2M) mapping table — controlled by VM monitor
- Cost:
  - Consider a four-level page table (48-bit addresses), how many memory references are needed to resolve a TLB miss?

Page walk cache
Virtual Machine Memory Management

- Transparent VM memory size adjustment
  - Ballooning [Waldspurger OSDI2002]
- Transparent VM memory need estimation
  - working set estimation through sampling [Waldspurger OSDI2002]
  - tracing memory accesses through proxy memory management [Pin&Shen USENIX2007]

- Discover and share pages of the same content over multiple VMs.
  - discover: compare hash coding of pages.
  - share: copy-on-write.
- How often do pages have the same content?