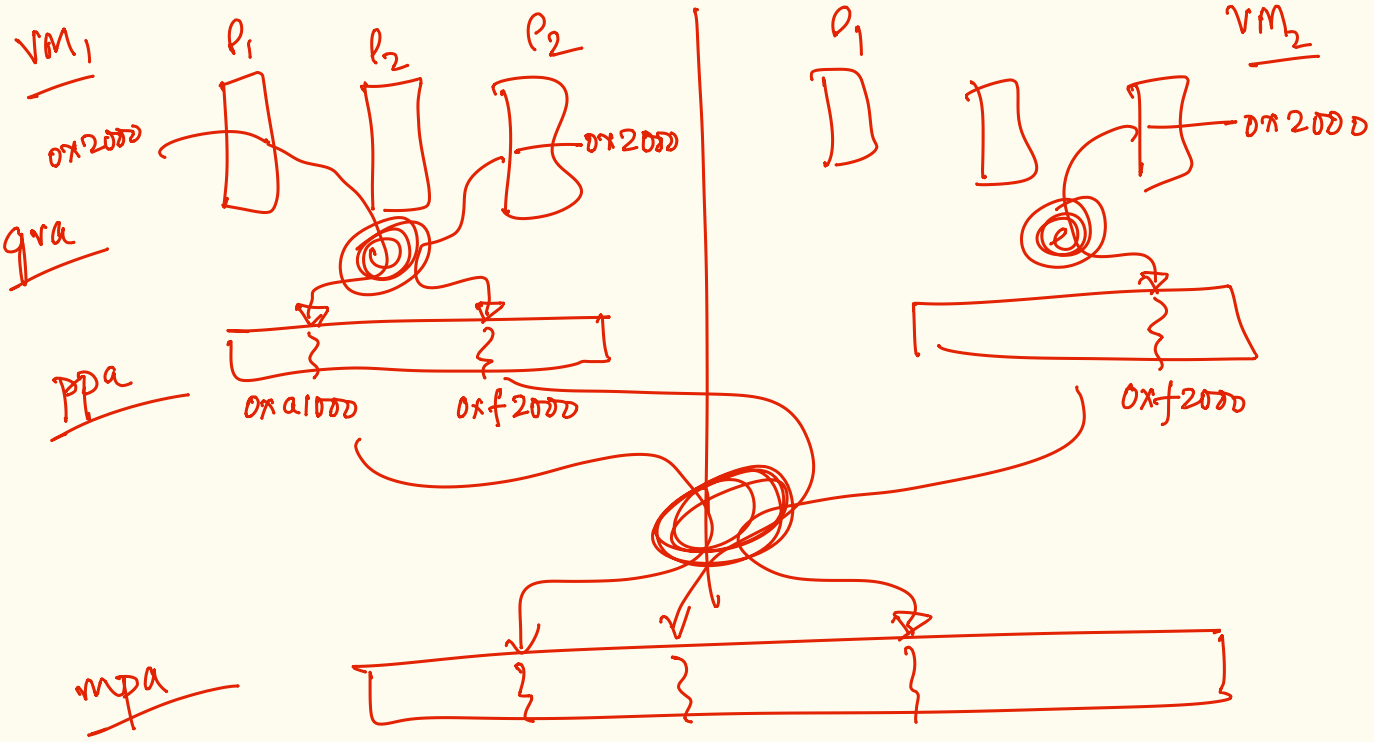
CS695 Lecture 5

- memory virtualization designs for VMs.



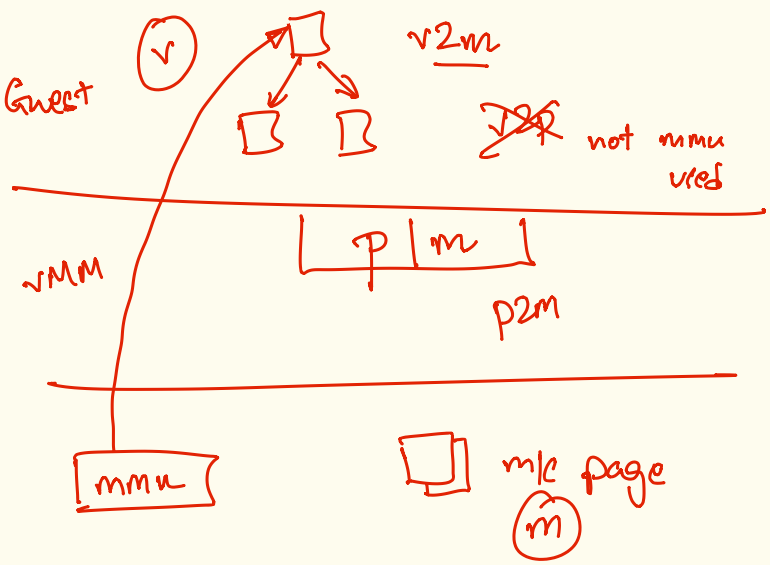
(R) gva —v2p→ ppa —p2m→ mpa

guest OS : v2p
vmm : p2m

- single mapping/translation via the h/w mmu.

Design 1 : Direct Mapping (para-virtualized)

Xen



pagefaults
mem allocation
program loading
} process

va

v2p } OS

(*) guest page tables store v2m ready for m/c page accesses.

(*) how to setup such a table?

(*) lcr3 (ppa) ——— PV ——— hc_update_cr3 (ppa)

1000

vmm

mCR3 ← (mpa)

14000

PV idea:

~ Guest does not direct page table updates/accesses

~ All actions via hypercalls.

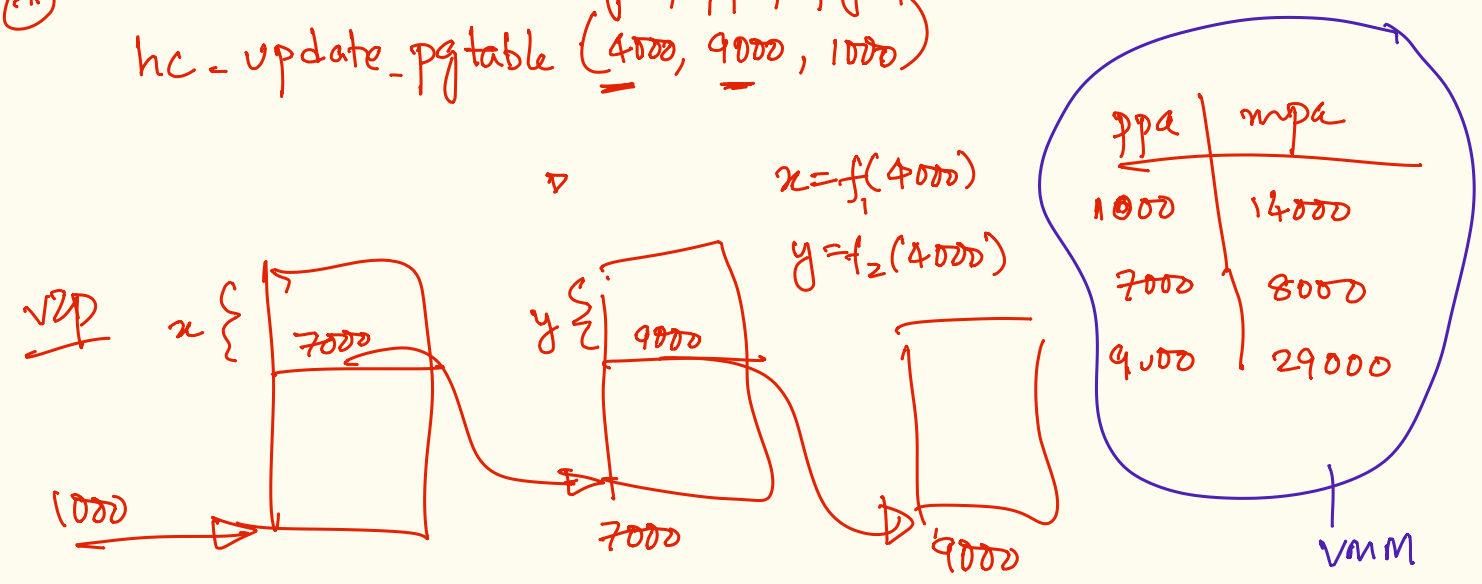
~ vmm uses p2m mapping to maintain a v2m table for mmu.

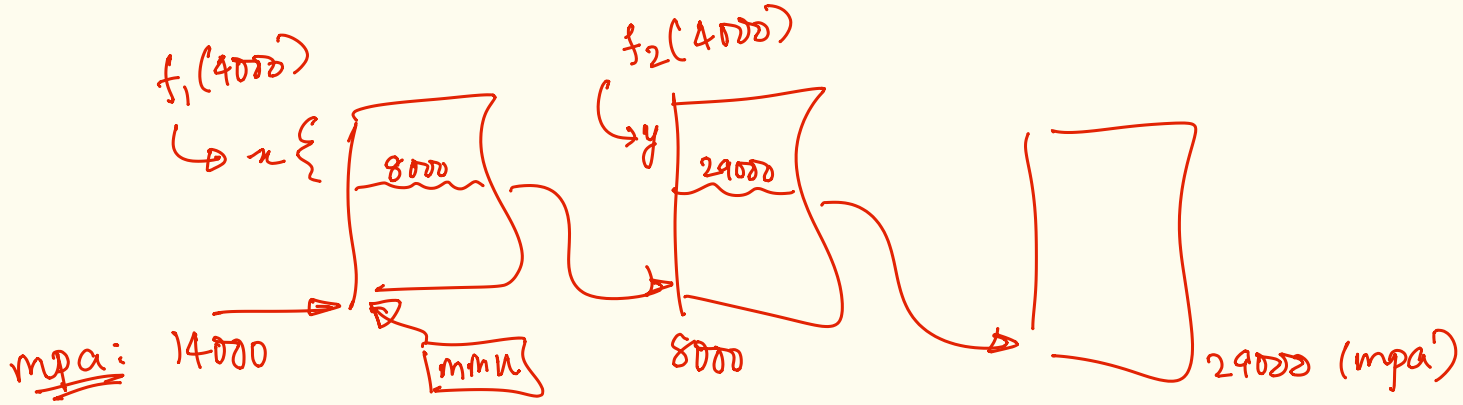
– all guest m/c pages of page tables are write-protected.

(*) hc_update_pgtable (4000, 9000, 1000)

v2p (ppa)

gva, ppa, pgd



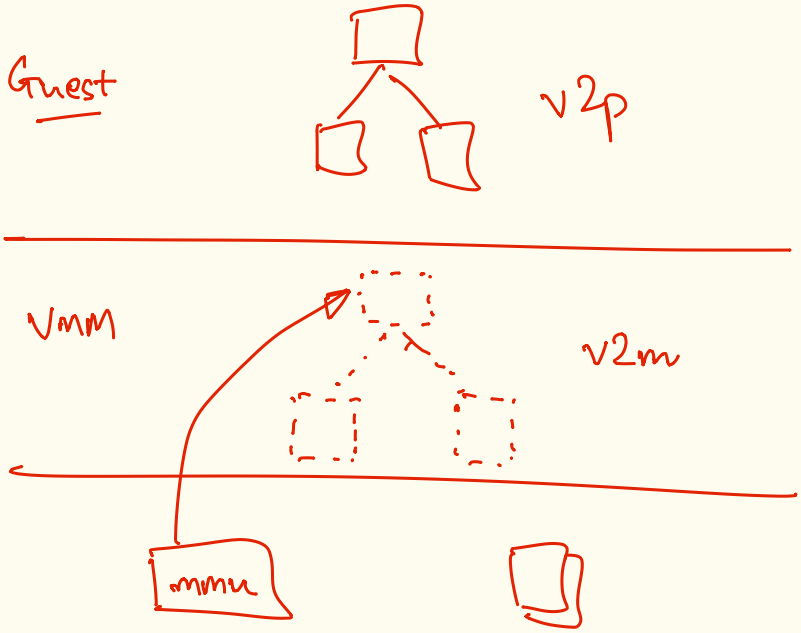


Design 2

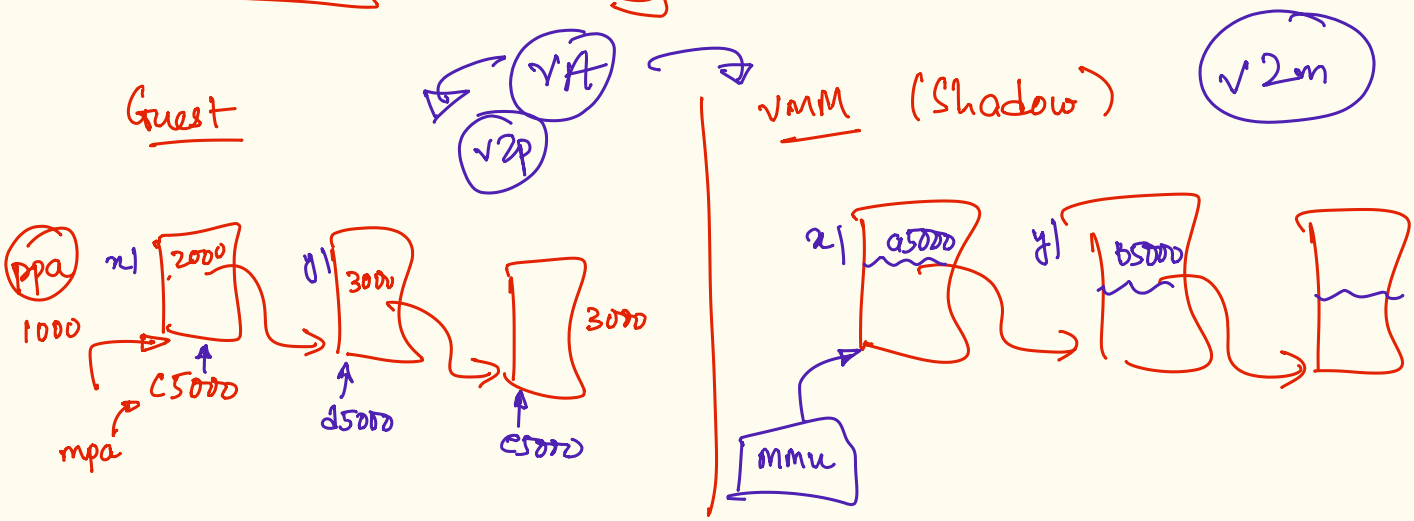
Shadow Paging

Shadow Page Tables

Full virtualization (vmware)



- vmm maintains a separate/second page table / shadow page table which mimics v2p by v2m.



lookup/read (pgd)

read pgd in guest

ppa

read Kva(pgd)

1000

read (c5000)

mmu

v

m

v2m

shadow table