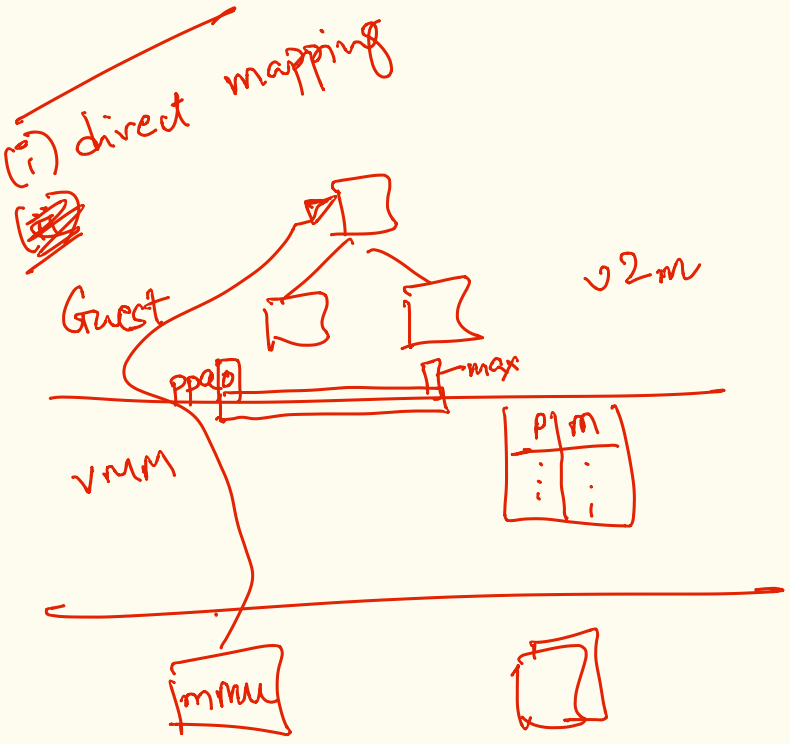
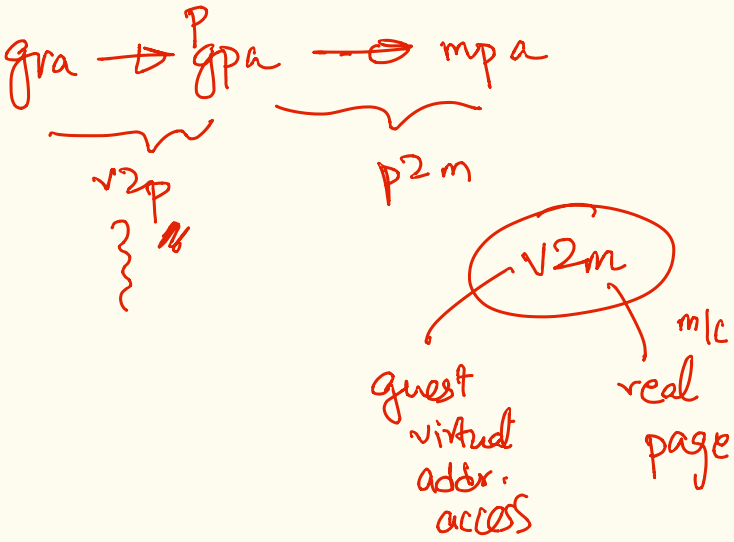
Lecture #7 CS 695 27.1.2023

- interrupt handling (system calls) with VMs & VMM.
- memory virtualization with VMs.
  - (i) direct mapping (PV)
  - (ii) shadow paging (full virtualization, BT) } s/w
  - (iii) nested paging (ept/npt) — h/w-assisted.



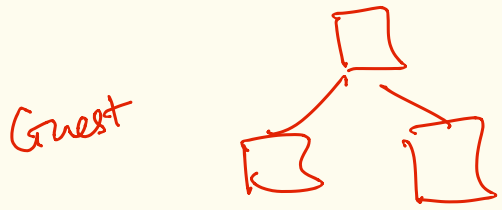




v: ⊗

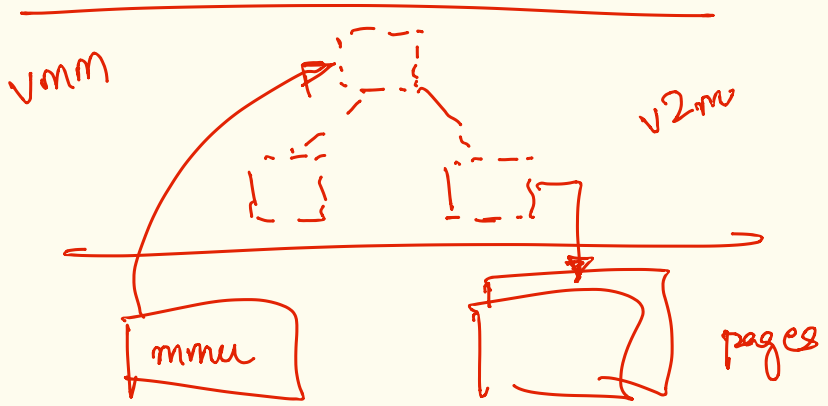
p: 70

m: 10070

(ii) shadow paging (fully virtualization)



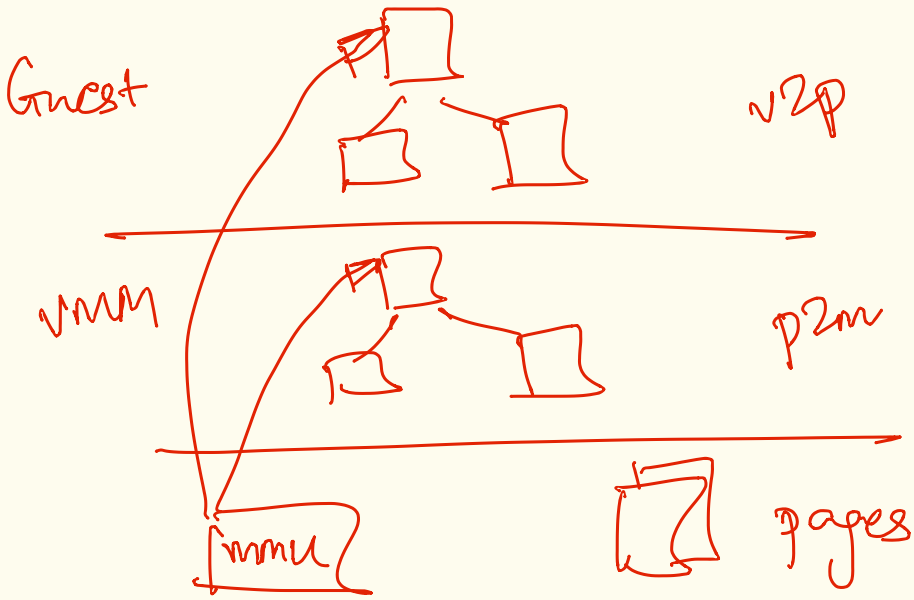

x: 70



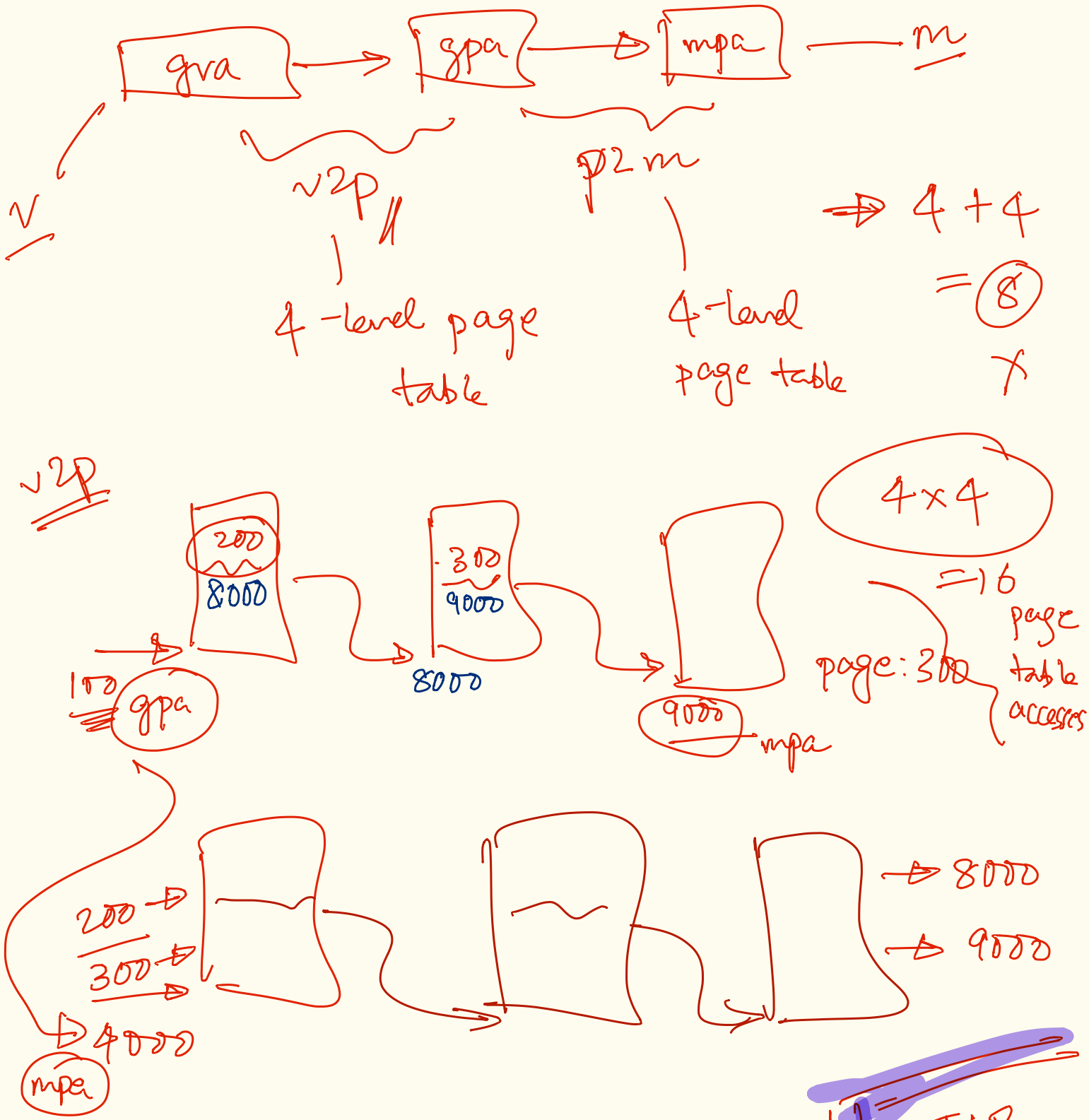

x: 10070

* cr3 is virtualized
- all guest page table pages are write-protected.
- all updates to page tables are via VMM (trap)
- VMM maintains a second (shadow) table w/ v2m mappings.
- every update to a page table ⇒ ~~two~~ updates to two page tables.

(iii) EPT / NPT (hw-assisted)
extended/nested page tables




(v) ~ two level nested walk to resolve from v2m




| v | p | m |
|---|---|---|
| 100 | 1000 | 5000 |
| | X | ? → X |
| 100 → | pg flt (guest) → 2000 | → 8000 |
| 100 → | 2000 | pg flt (VMM) → 10000 X |

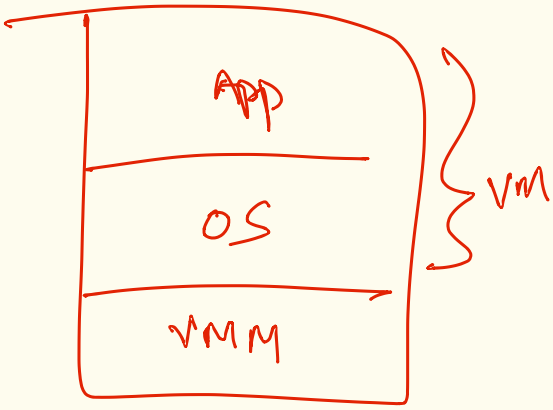
TLB

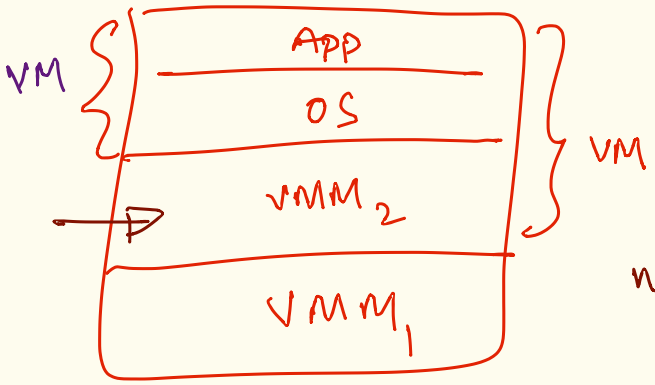
v2m

process centric

Global vs Local

ASID — address space ID




nested virtualization