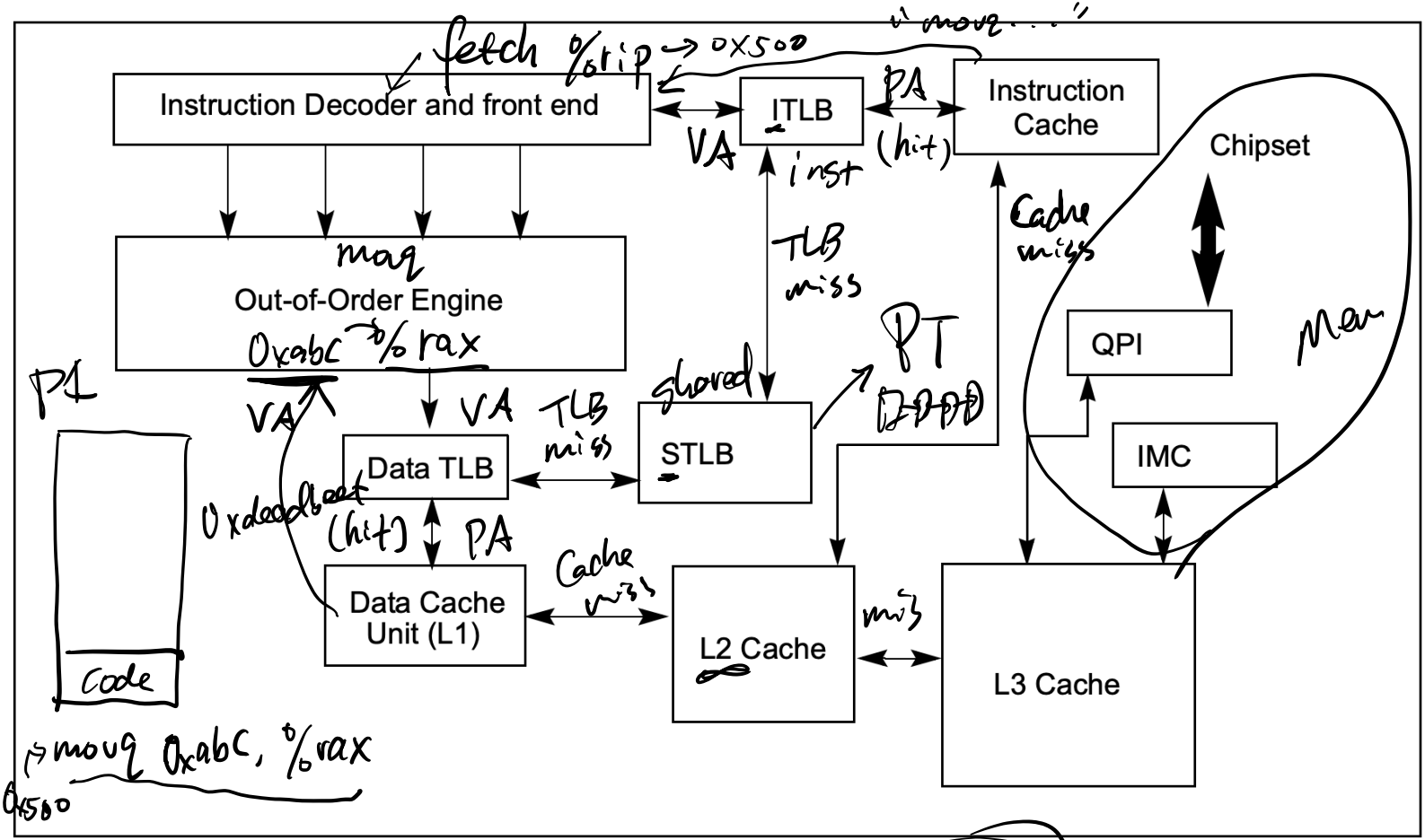
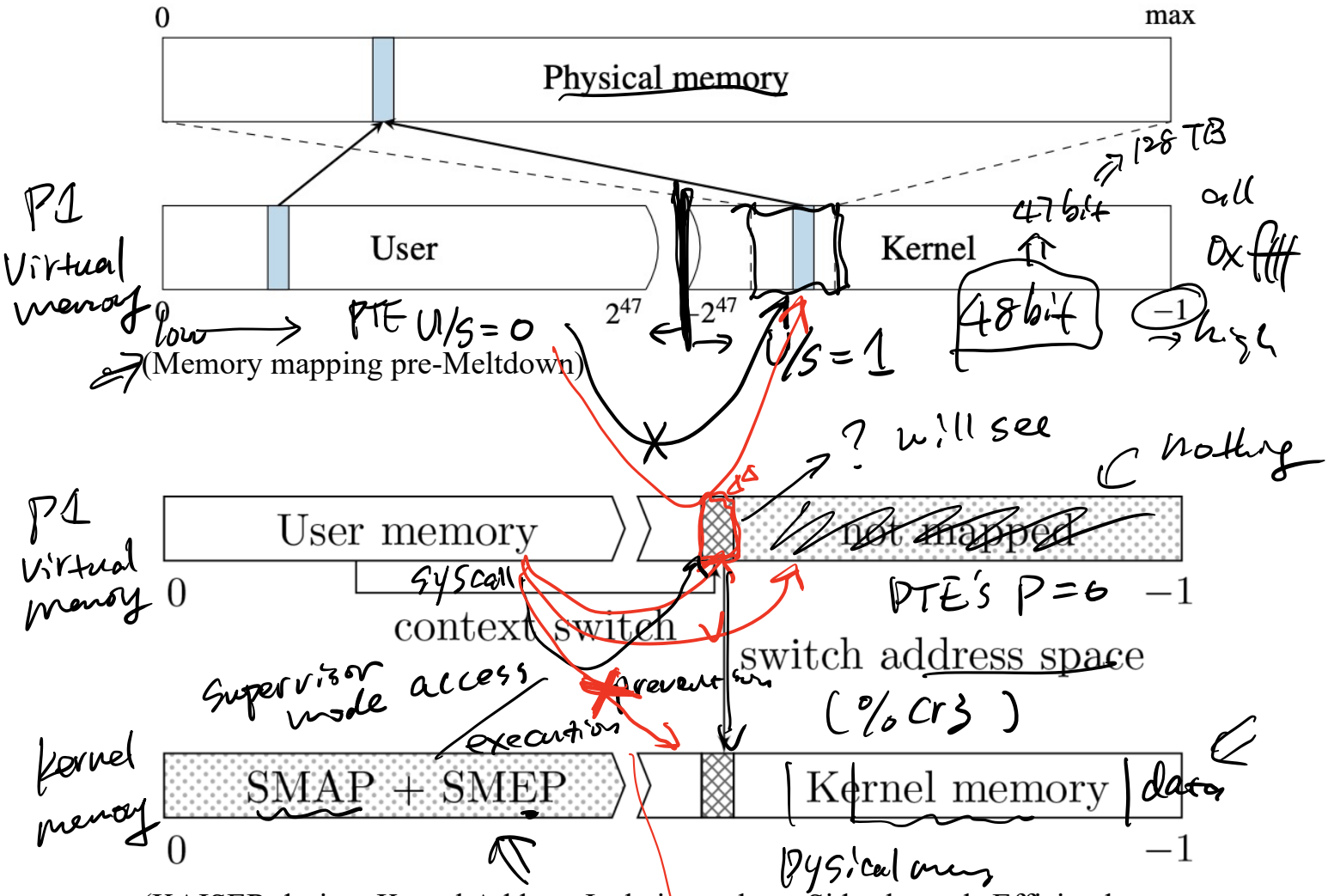


Figure 11-2. Cache Structure of the Intel Core i7 Processors



(KAISER design: Kernel Address Isolation to have Side channels Efficiently Removed)

Figures borrowed from Meltdown and KAISER papers.

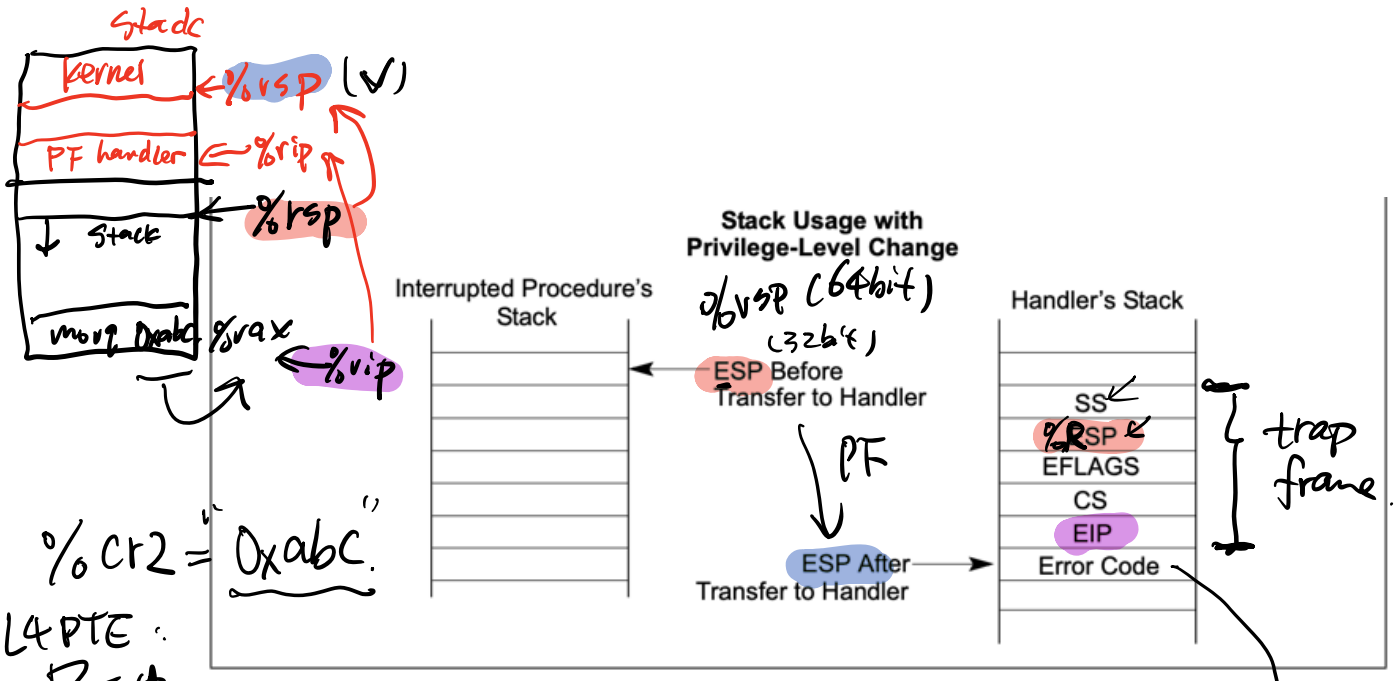


Figure 6-4. Stack Usage on Transfers to Interrupt and Exception-Handling Routines

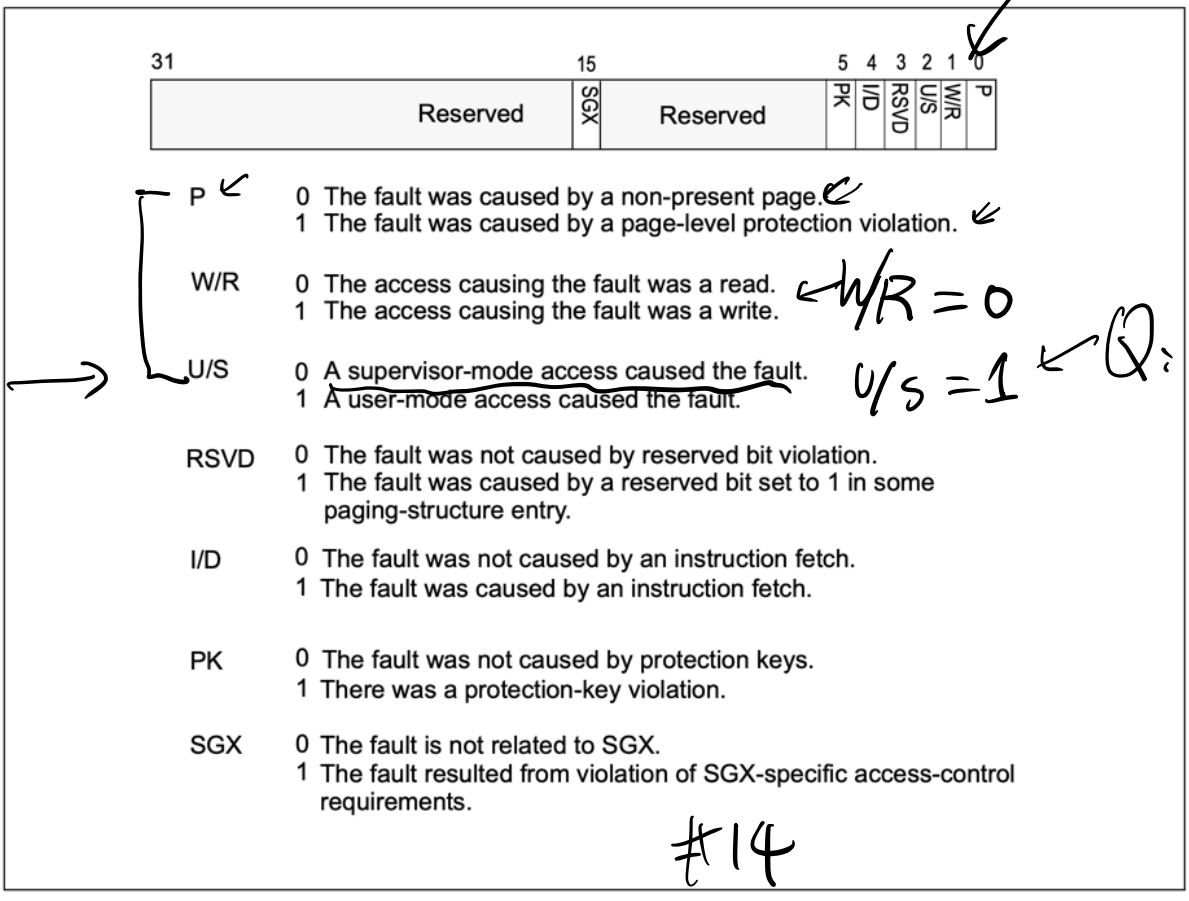


Figure 4-12. Page-Fault Error Code

1. Last time
2. page fault
   - intro
   - usage
   - costs
   - thrashing
3. mmap

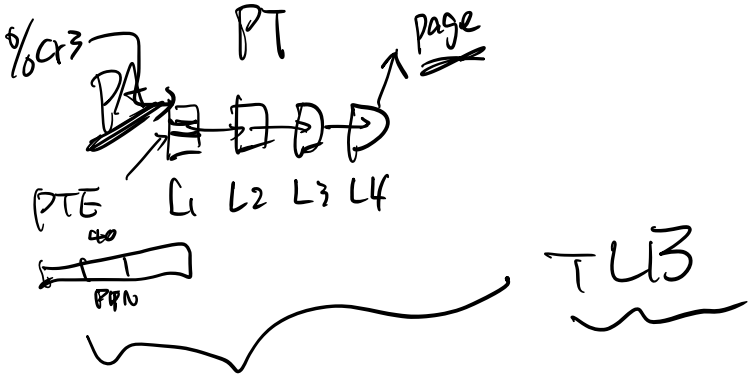
Monitor

KV-Store.

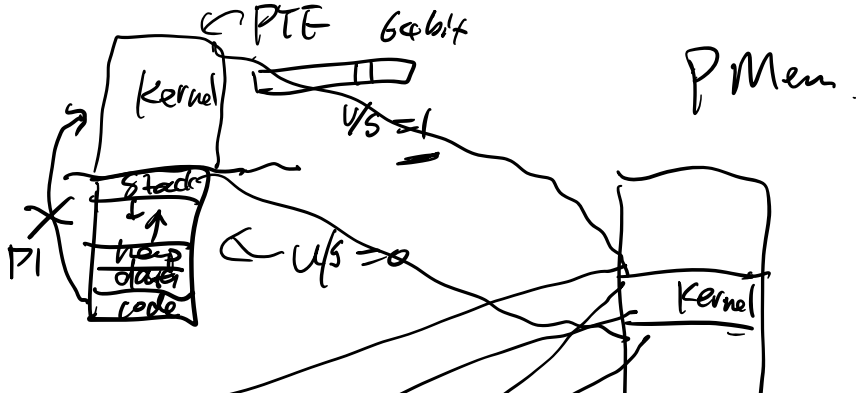
Linearizability

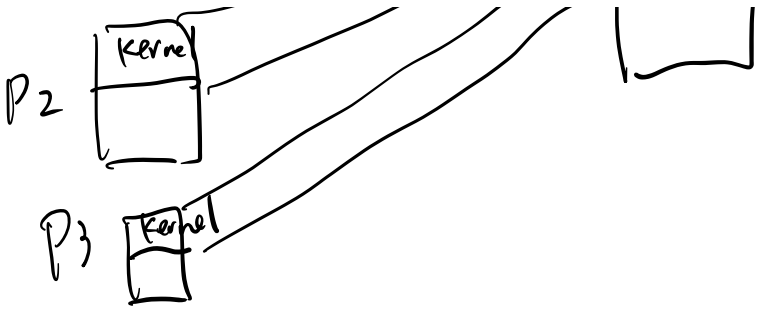
VA → PA

VPN → PPN Q: fetch 1 VA, ⇒ Page



- Where is OS?





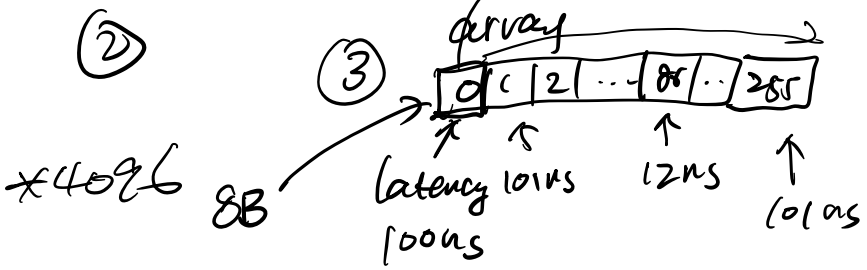
- meltdown / spectre.
  - ↳ OOOExc + side channel
  - ↳ ① Spectuive exec + side channel ②

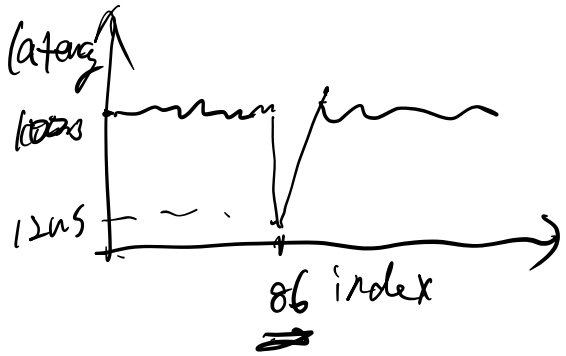
```
if (Cond never True) {
    array [ 8bit (=86) SECRET ];
}
```

① ② ③

array[86] Cached

→ 1 page





- mitigation.

- page faults.

trapping Kernel : syscall / interrupt / exception

→ line1

→ line2

↳ CPU. PF → ① VA → PA PTE (P=0)

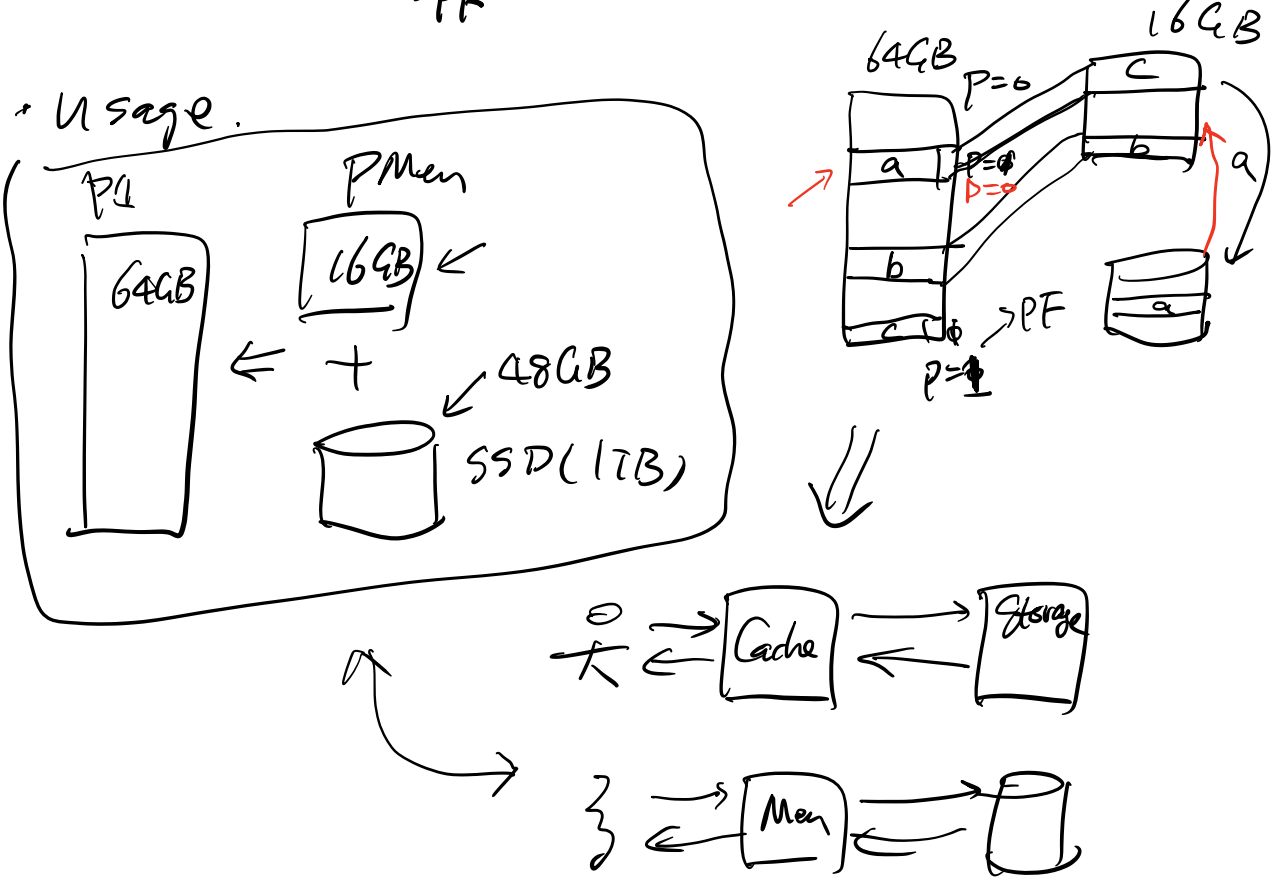
② permission check

e.g. U/S = 1 RO

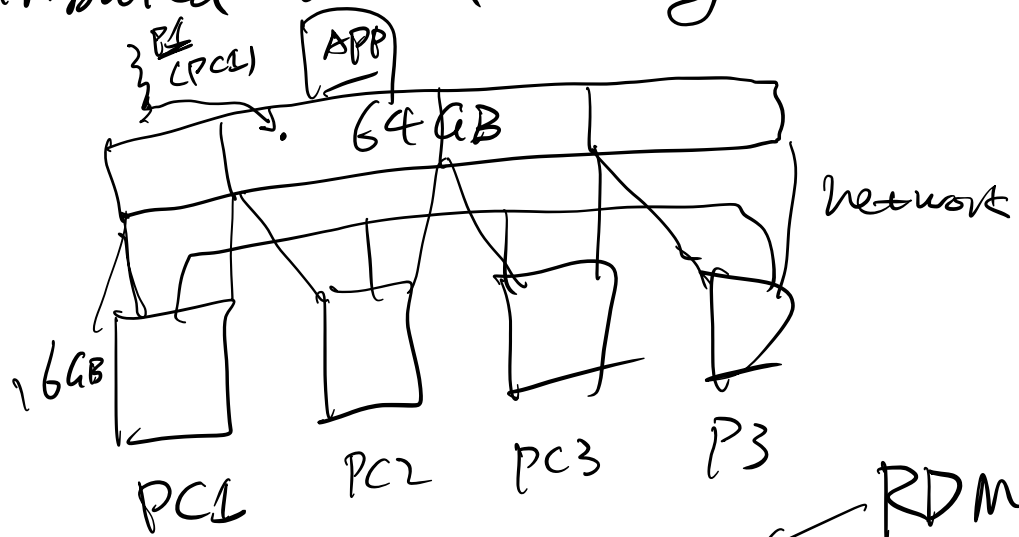
- x86.

movq 0xabc, %rax

↳ PF



- Distributed Shared Memory (DSM)

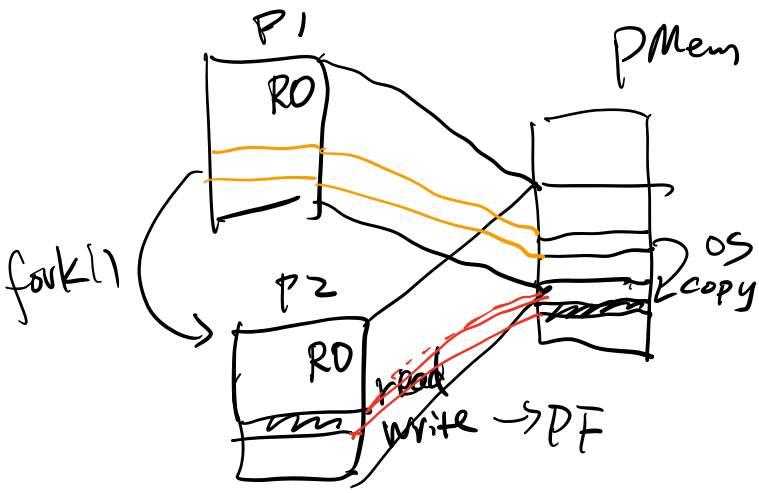


RDMA

100ns vs. 100ms

10^6 x

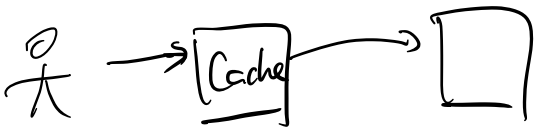
- COW: Copy-on-write



mmap

- GC.

- page replacement policies



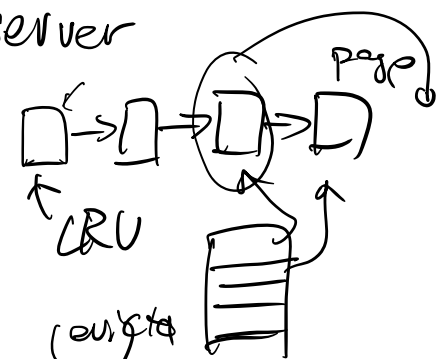
Cache eviction problem

FIFO:

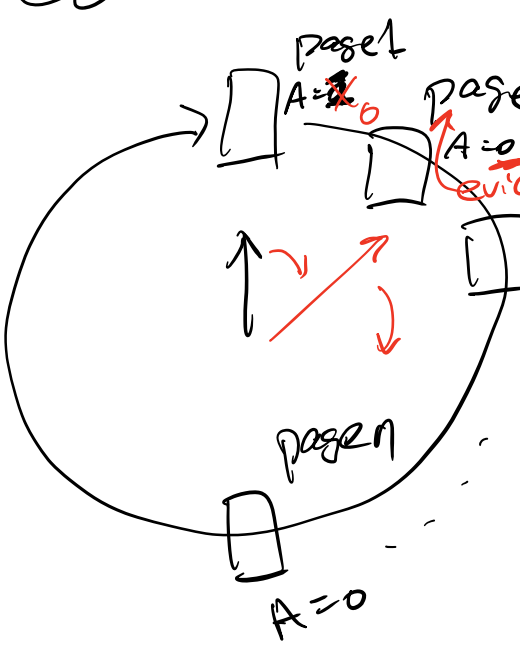
LRU:

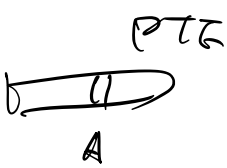
least → rectent used

Web server



clock.





clock ~ LRU ~ OPT

- Thrashing

Program: 50 pages.

PMem: 40 pages. + SSD 10 pages.

Mem: 100ns

SSD: 1 ms.

Q:

$$\text{Avg latency} = \frac{40}{50} \cdot 100\text{ns} + \frac{10}{50} \cdot 10^6\text{ns}$$

$$\simeq 80\text{ns} + 2 \cdot 10^5\text{ns}$$

2000X

50 Page of PMem: 100ns

hailde