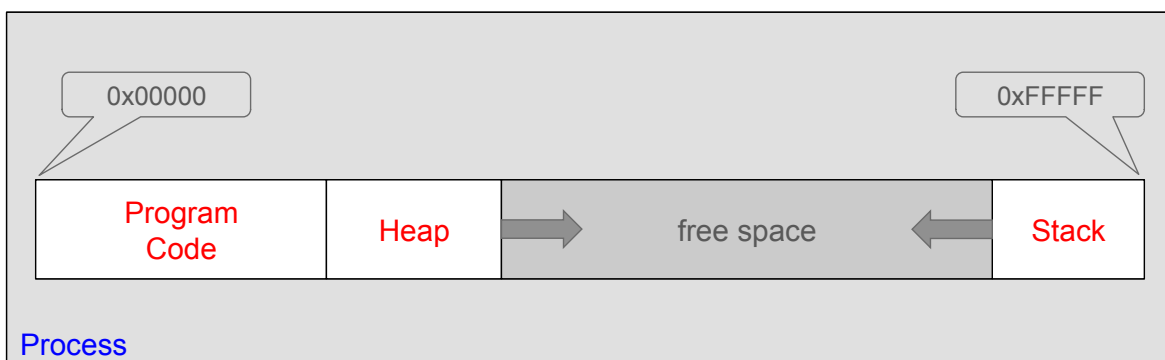


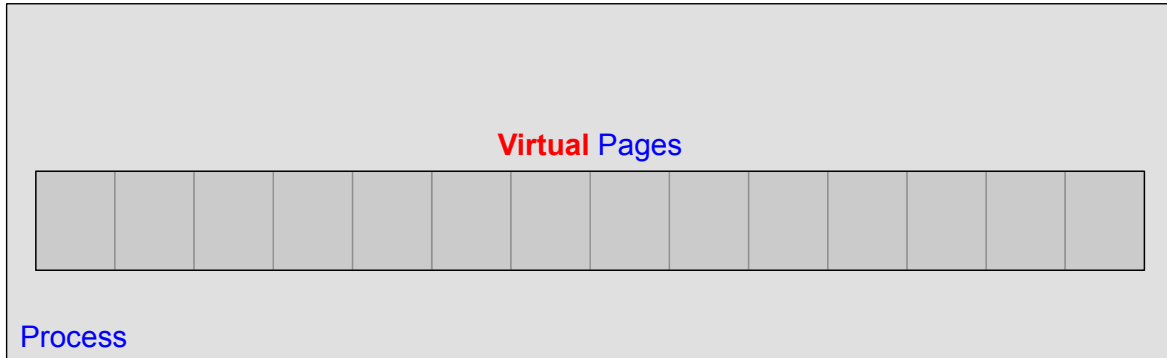
Virtualization – Memory

- Virtual vs. Physical vs. Machine Memory
- Mechanics: Shadow Pages
- Page Replacement: Double Page Faults
- Memory Management: Ballooning

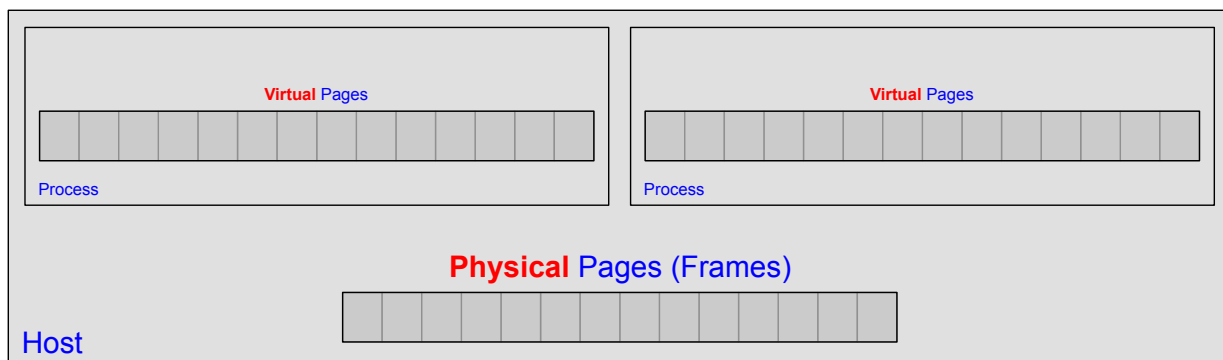
Virtual Address Space



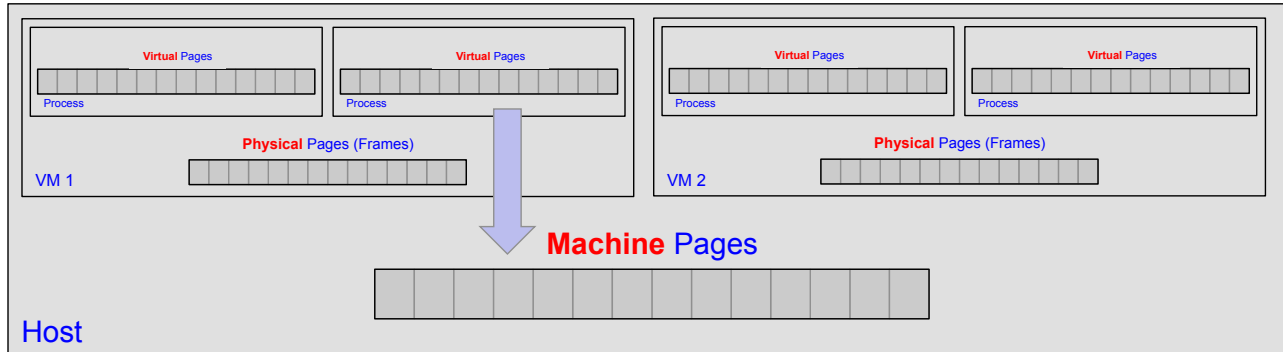
Virtual Address Space



Virtual vs. Physical



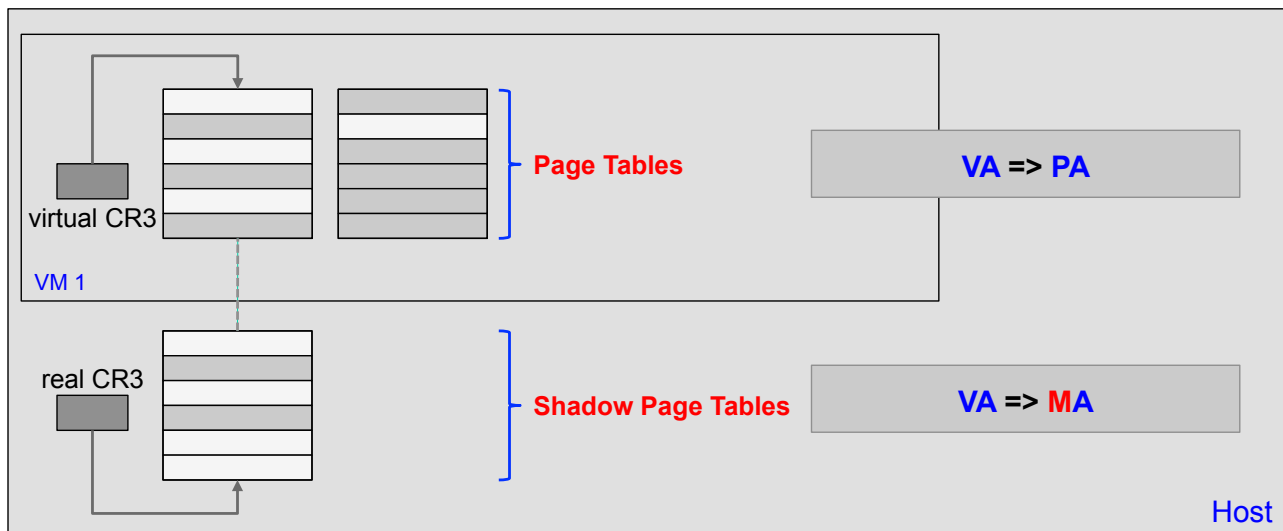
Virtual vs. Physical vs. Machine Memory



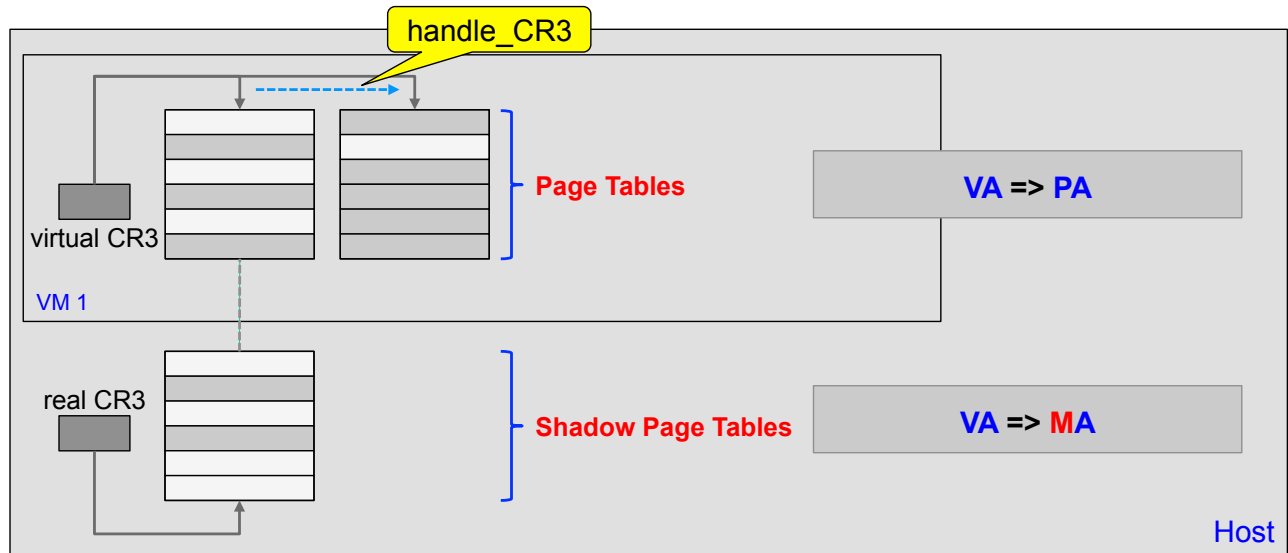
Note1: Guest OS expects zero-based **physical** address space.

Note2: Need to map **Virtual Address** of process to **Machine Address** of host.

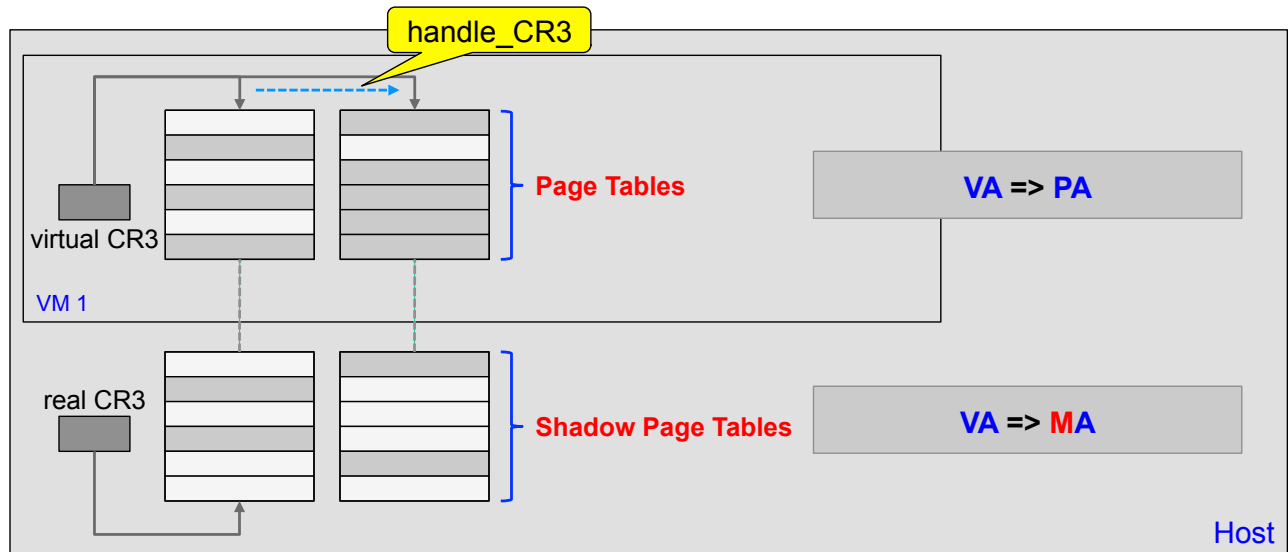
Shadow Page Tables



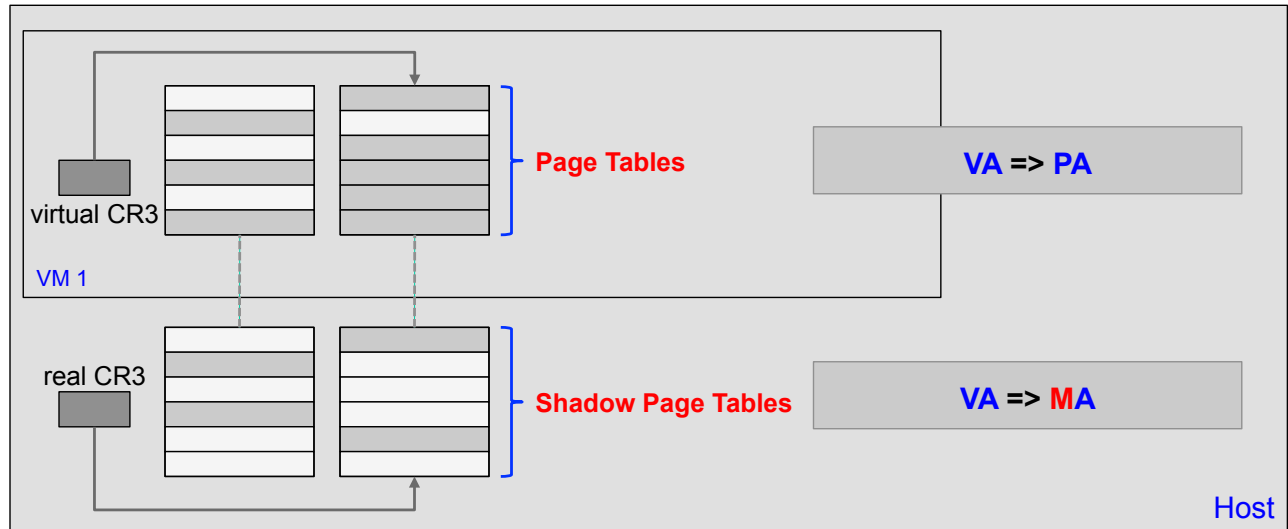
Discover Page Table



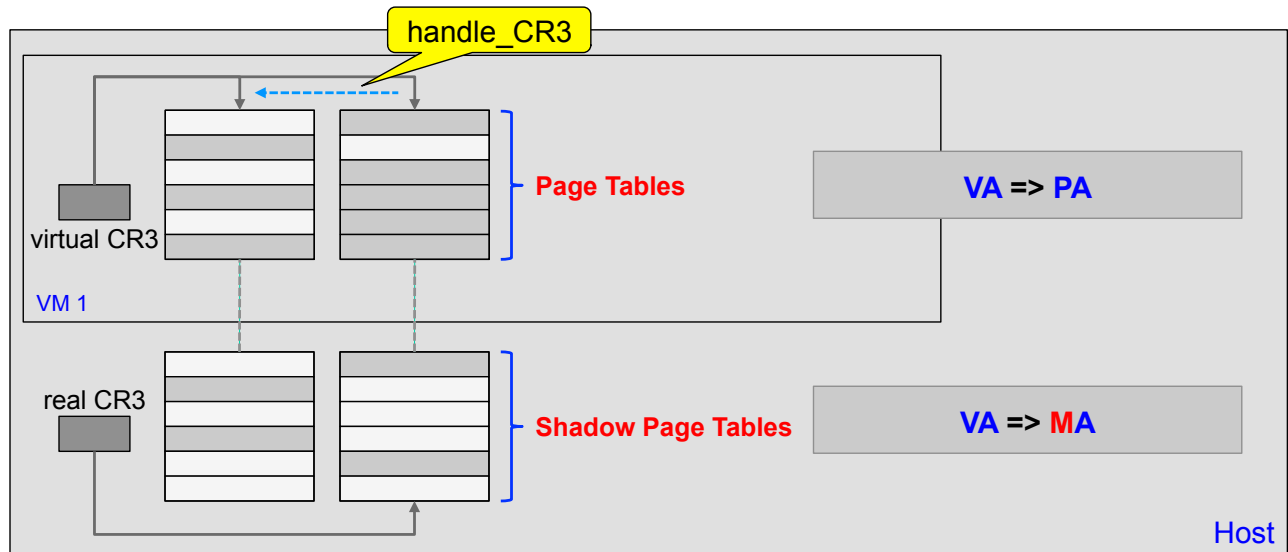
Discover Page Table



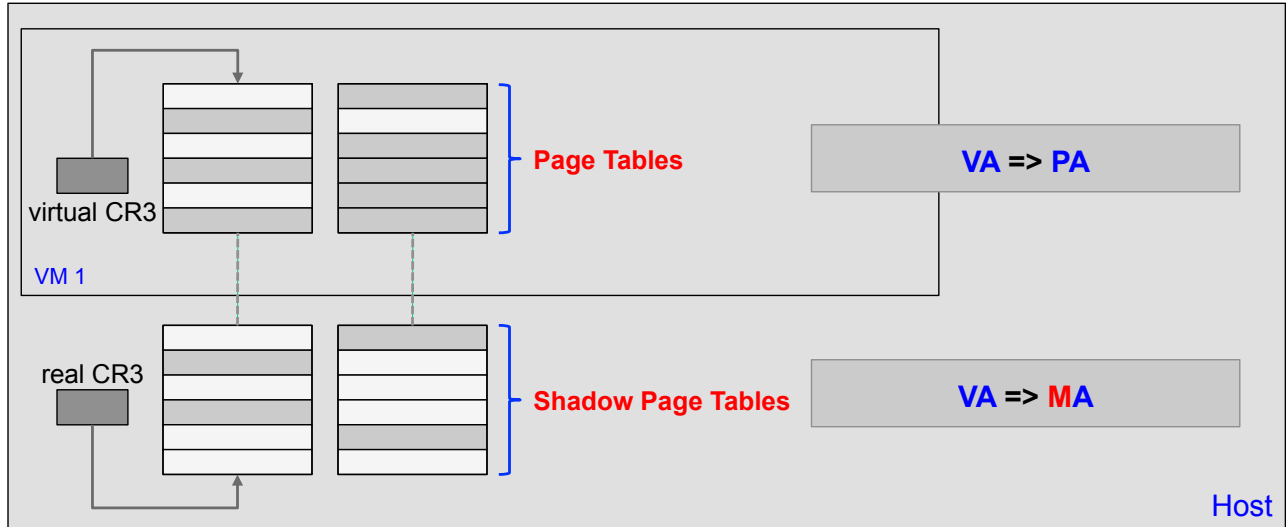
Discover Page Table



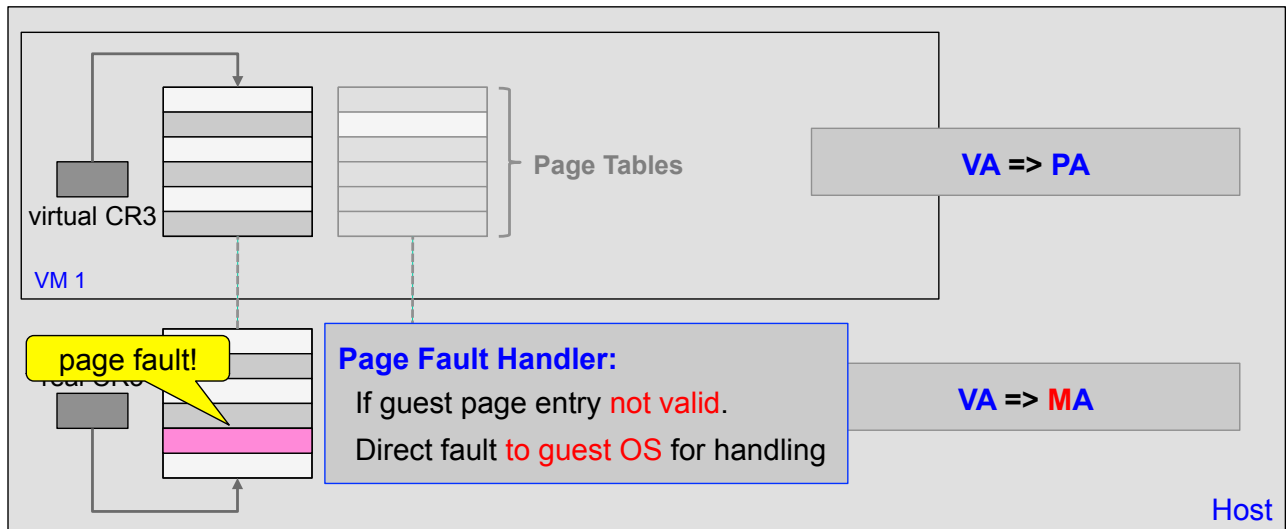
Switch Page Table



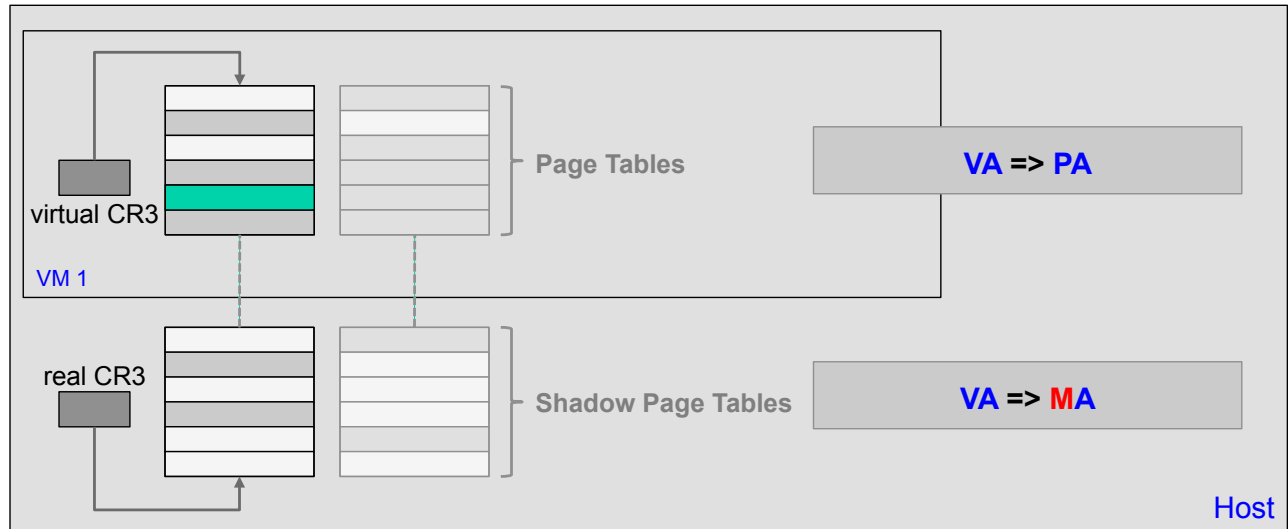
Switch Page Table



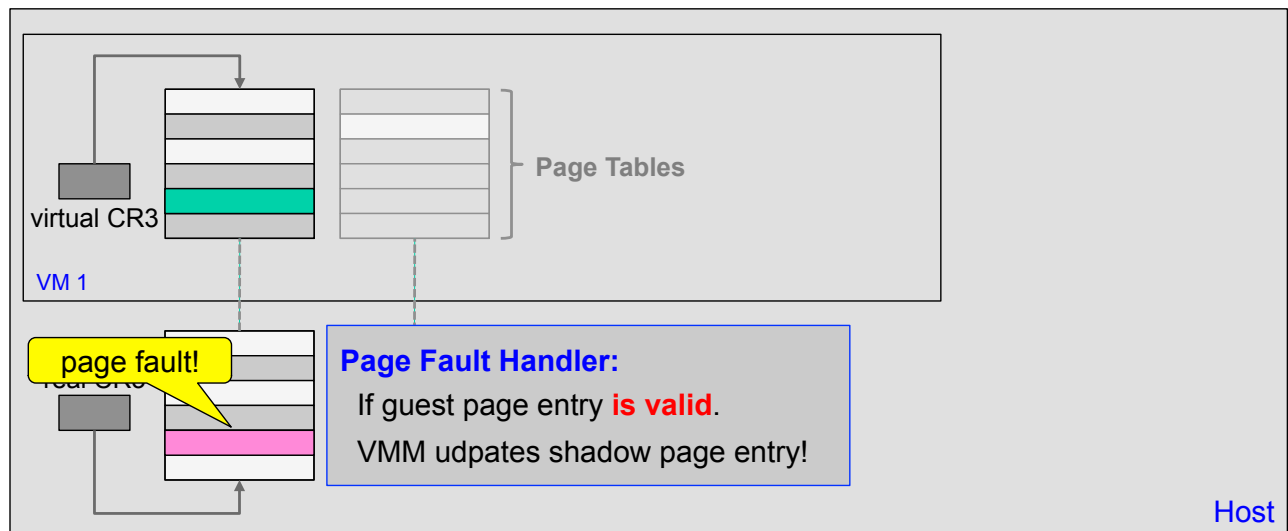
Page Fault



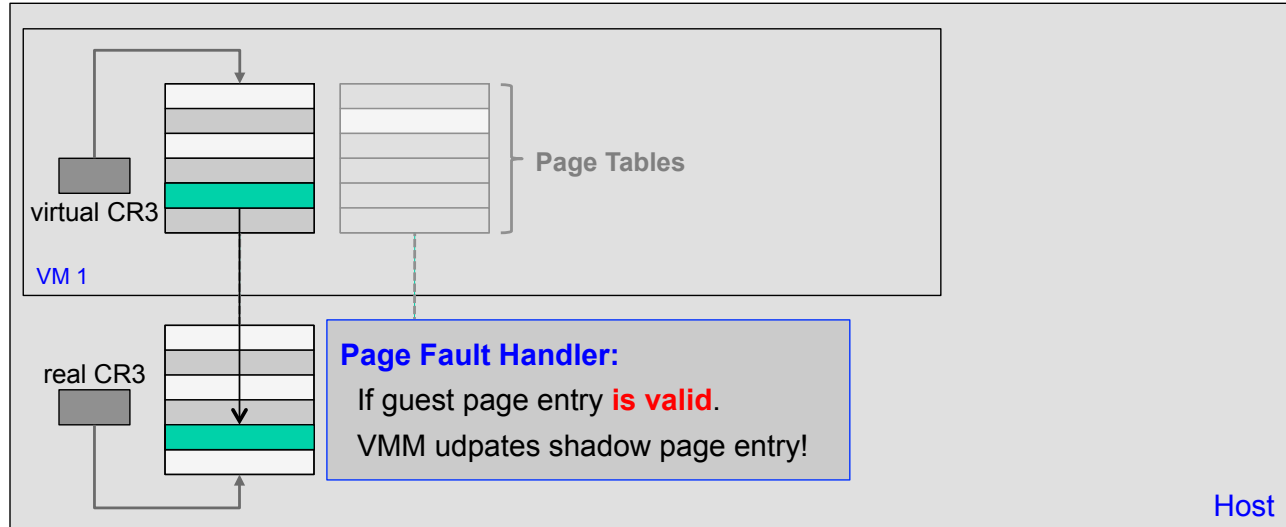
Page Fault



"Shadow Page Fault"



“Shadow Page Fault”



Shadow Page Tables

Pros:

- Eliminates double-bookkeeping (VA->PA and PA->MA)

Cons:

- Every page fault by virtual machine exits into the hypervisor.
- Every page table needs to be duplicated.

Solution approaches:

- Hardware support for memory virtualization
 - AMD nested paging, Intel extended page tables (EPT)
 - TLB maps VA->MA, is aware of VMs

Issues with Page Replacement

Memory Over-commitment: Move some “physical” memory to disk when memory requirement exceed available resources.

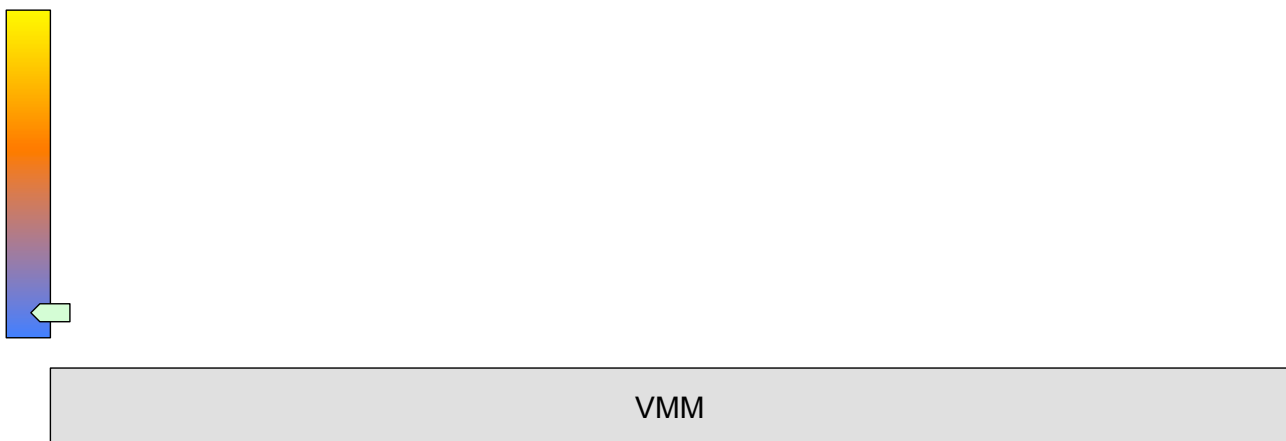
Issue 1: A **page replacement algorithm** now has to pick:

- victim **machine** (ok)
- victim **page** (huh!? What is a good page to replace?!)

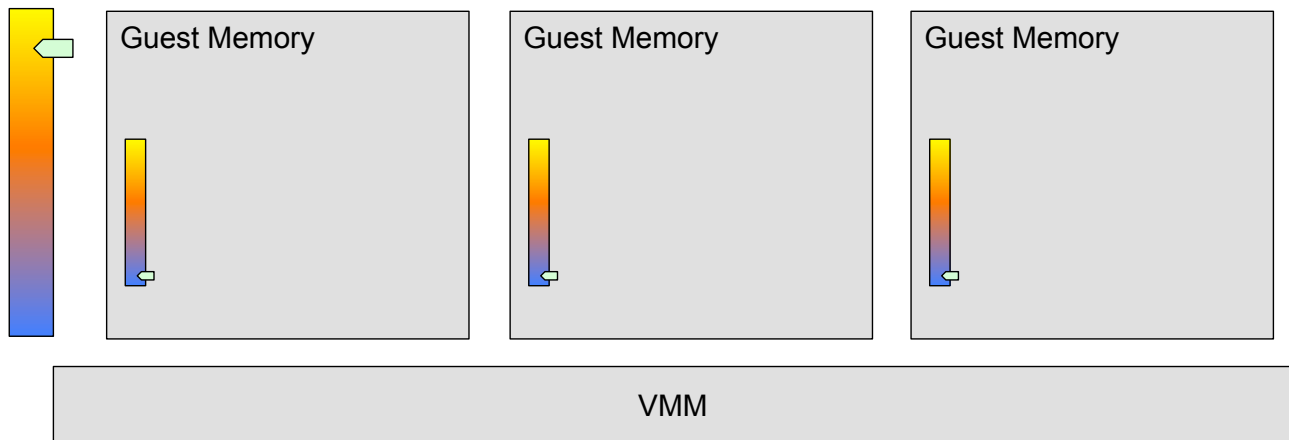
Issue 2: Double-Paging Problem:

- What can happen when we page out a physical page that is on disk?
 - Some time later the guest picks physical page on disk as victim.
 - In order to page out victim, it must first be paged in by VMM beforehand.
- This causes 2 page faults per fault.

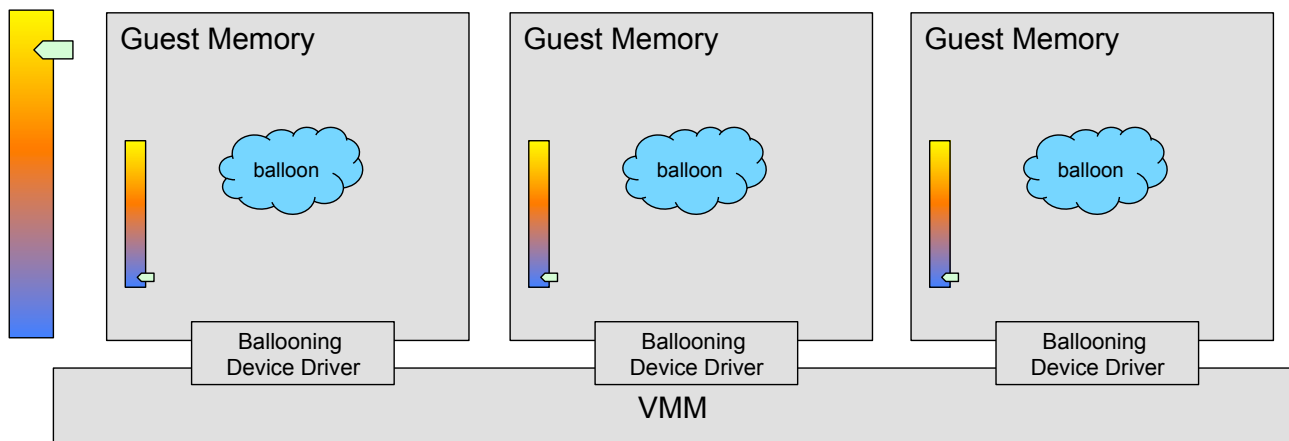
Avoiding paged-out “physical” Pages - Ballooning



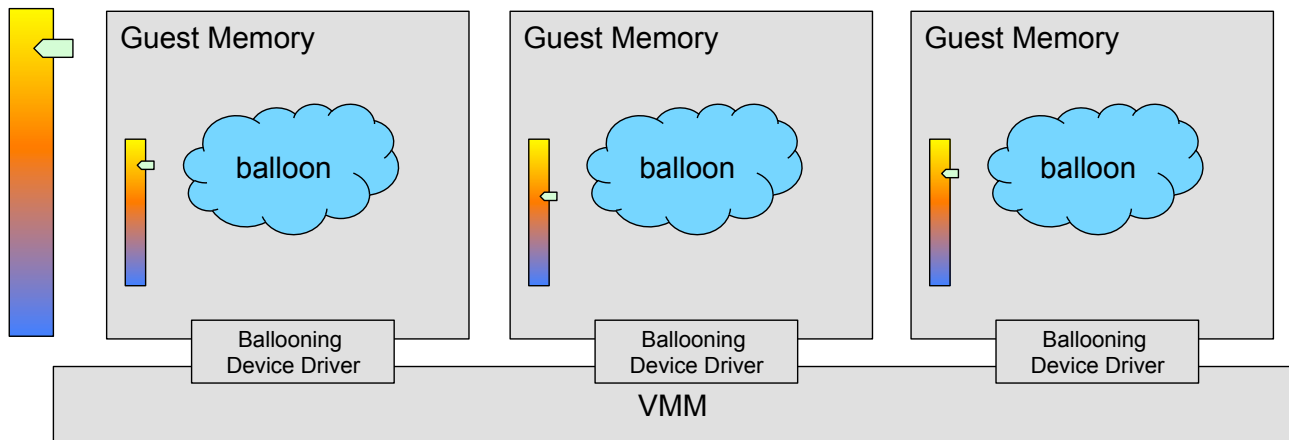
Avoiding paged-out “physical” Pages - Ballooning



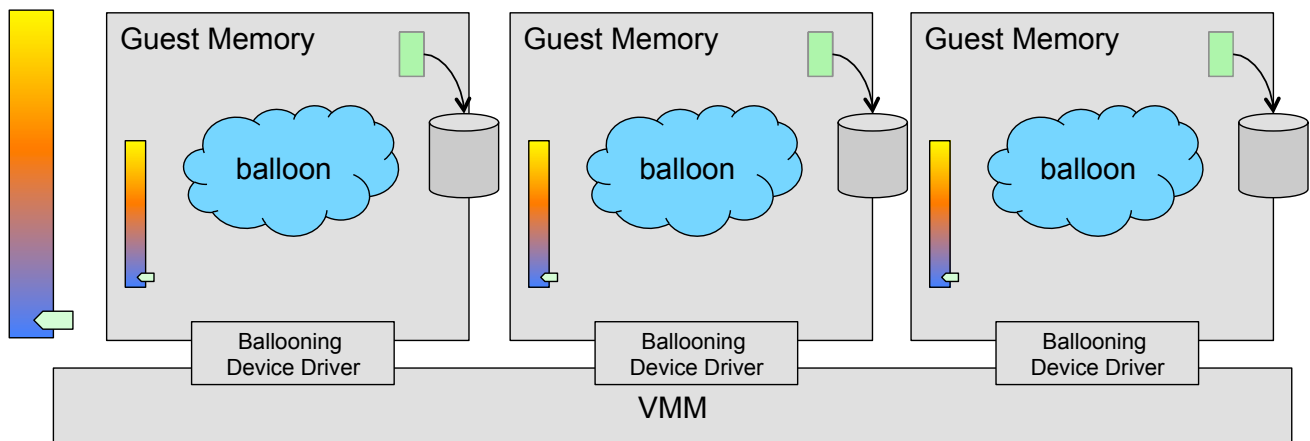
Avoiding paged-out “physical” Pages - Ballooning



Avoiding paged-out “physical” Pages - Ballooning



Avoiding paged-out “physical” Pages - Ballooning



Potential Problems with Ballooning

- Ballooning works fine as long as it works.
 - Ballooning drivers may be **uninstalled**, **disabled explicitly**, **unavailable** during booting.
 - Upper levels on balloon **sizes** may be imposed by guest operating system.
-

Virtualization – Memory Management

- **Virtual** vs. **Physical** vs. **Machine** Memory
 - Mechanics: Shadow Pages
 - Page Replacement: Double Page Faults
 - Memory Management: Ballooning
-