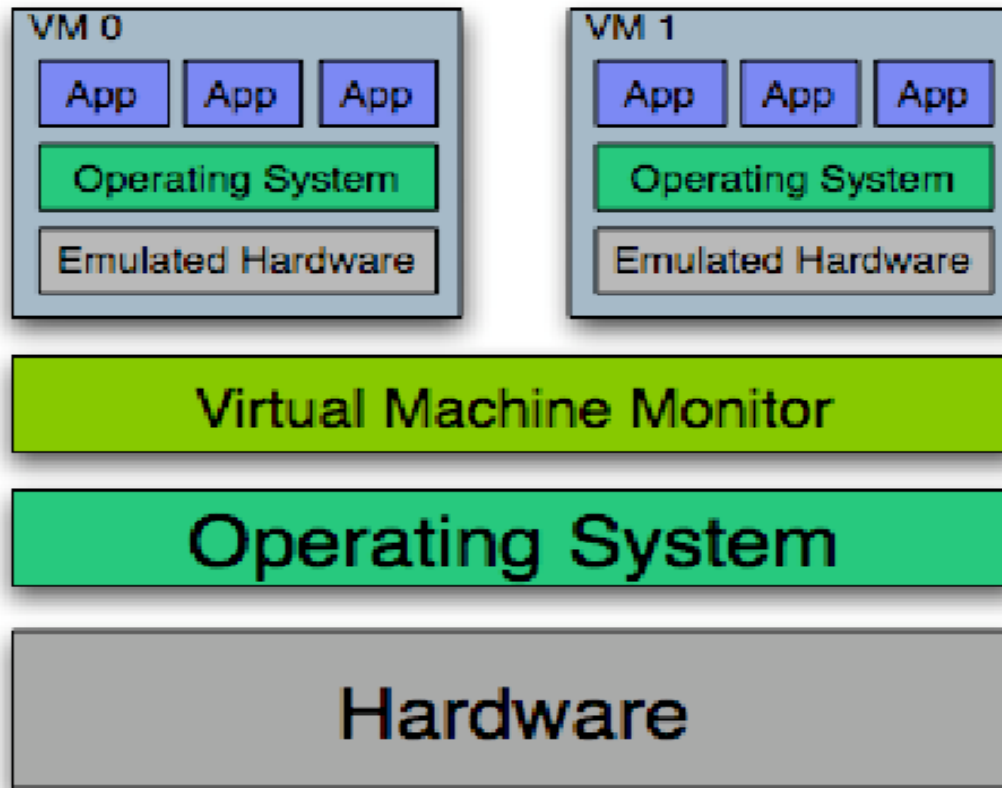
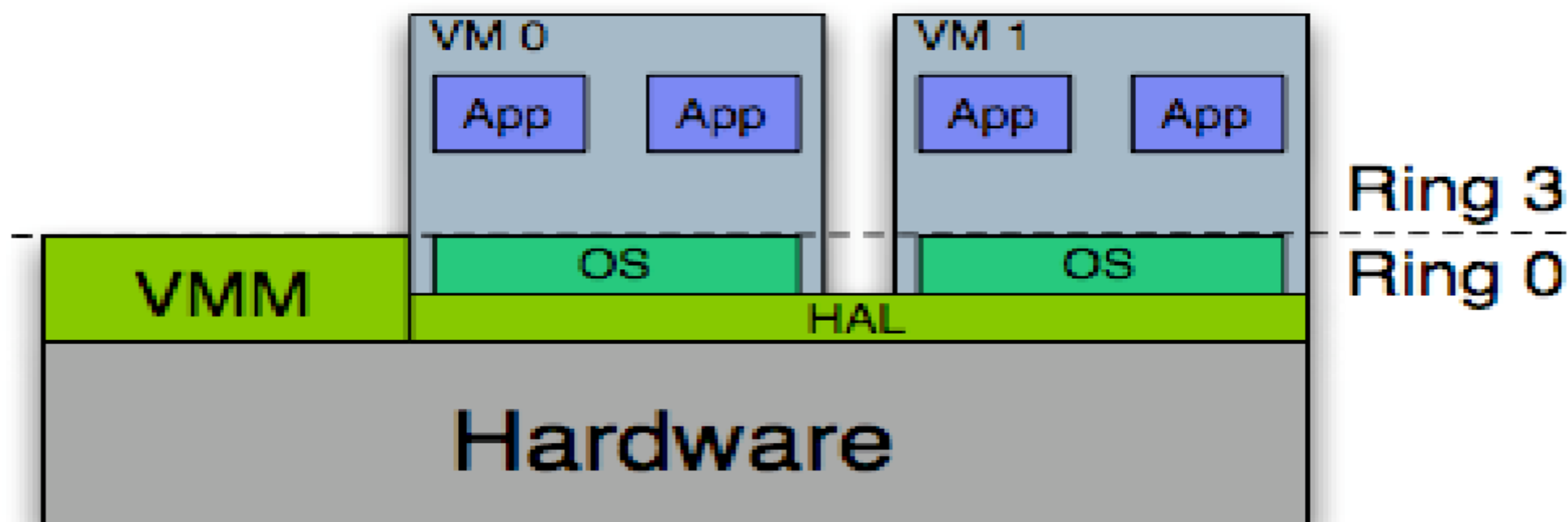


Wirtualizacja wspomagana sprzętowo (architektura x86)



- problemy z wirtualizacją programową
- odpowiednie wsparcie sprzętowe może rozwiązać te problemy



- Architektura x86 nie spełnia założeń twierdzenia Popkego-Goldberga
- Można zbudować na takim komputerze maszynę wirtualną, lecz bez spełnienia warunku wydajności - obsługa tzw. *instrukcji krytycznych*:
 - dynamiczna rekompilacja (*patching*)
 - parawirtualizacja

Nowoczesne metody sprzętowego wspomagania wirtualizacji:

- AMD-V
- Intel-VT
- Itanium VT-i

Intel Virtualization Technology

- Zwany także Vanderpool, IVT, VT-x i VMX
- Dwa rodzaje operacji procesora:
 - główne (*root mode*)
 - niegłówne (*non-root mode*)
- Oba rodzaje operacji mogą wykonywać się we wszystkich trybach uprzywilejowania (Ring 0 - Ring 3)

Intel Virtualization Technology

- Przejścia pomiędzy operacjami głównymi a niegłównymi i vice versa nazywają się (odpowiednio) wejściami i wyjściami maszyny wirtualnej (*VM entries*, *VM exits*)
- W trybie niegłównym wyjścia maszyny wirtualnej zachodzą automatycznie dla niektórych (w pewnym stopniu konfigurowalnych) instrukcji i zdarzeń
- Następuje przesunięcie monitora maszyn wirtualnych z kontekstu gościa do kontekstu gospodarza

Intel Virtualization Technology

- Wejścia i wyjścia maszyny wirtualnej są zarządzane specjalną strukturą danych - *Virtual Machine Control Structure (VMCS)*
- Zawiera obszar stanu gościa i obszar stanu gospodarza (*guest-state area, host-state area*), posiadające pola określające różne aspekty stanu procesora

Intel Virtualization Technology

- Wejście maszyny wirtualnej polega na załadowaniu danych z obszaru stanu gościa
- Wyjście maszyny wirtualnej polega na zapamiętaniu stanu w obszarze stanu gościa i załadowaniu danych z obszaru stanu gospodarza
- VMCS zawiera także pola sterujące obsługą niektórych instrukcji

Intel Virtualization Technology

VMXON/VMXOFF	Enable/Disable VMX operation
VMCLEAR	Initialize VMCS region
VMPTRLD/VMPTRST	Load/Store Current VMCS pointer
VMREAD/VMWRITE	Read or Write VMCS fields
VMLAUNCH/VMRESUME	Launch or resume virtual machine
VMCALL	Issued from virtual machine to call into VMM

Zalety i wady wirtualizacji wspomaganej sprzętowo

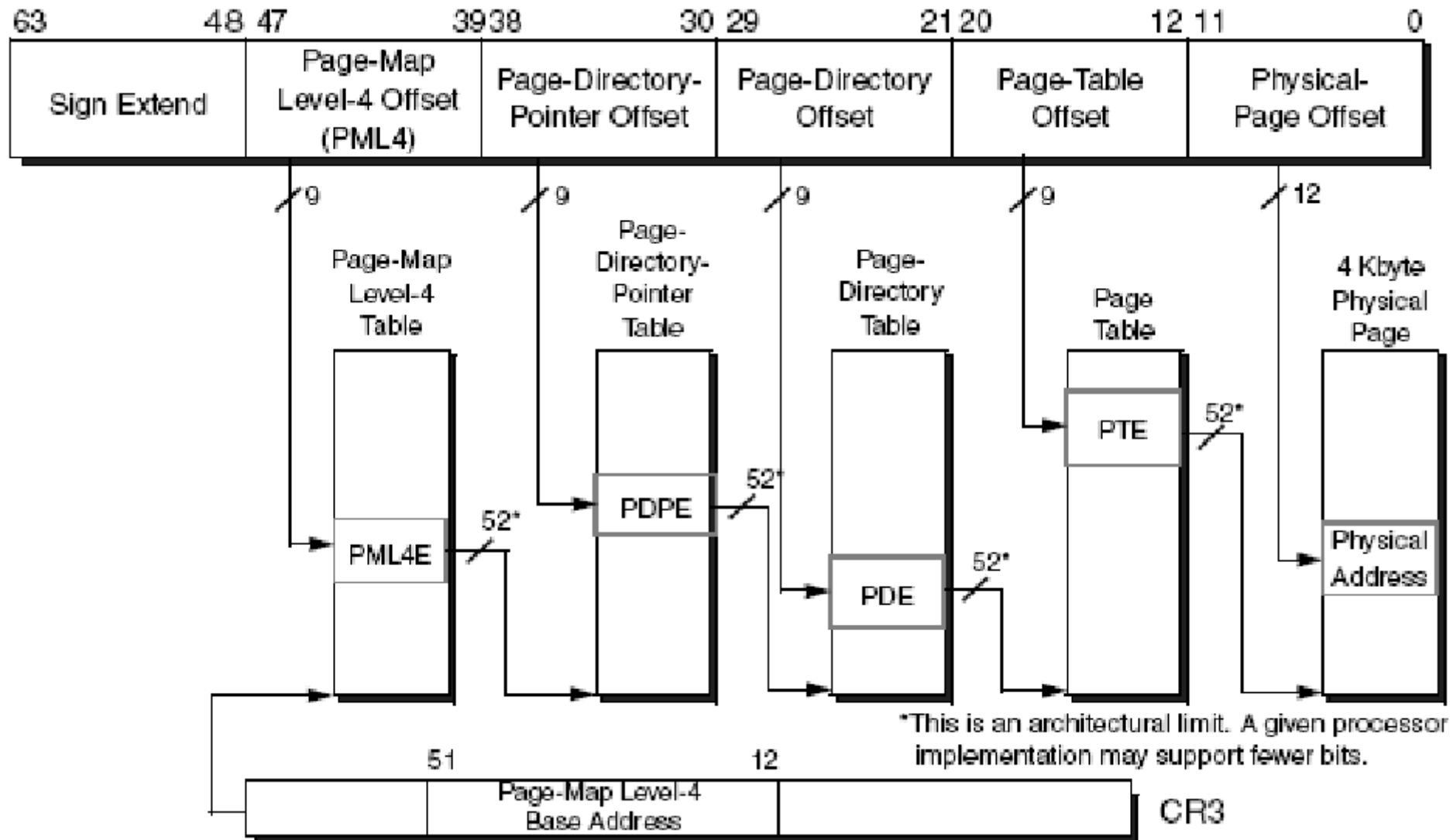
- Zalety:
 - efektywność
 - minimalizuje (idealnie: eliminuje) potrzebę modyfikacji gościnnego oprogramowania
- Wady:
 - musi być
 - problemy z bezpieczeństwem
 - duże użycie procesora => słaba skalowalność

Shadow Page Tables

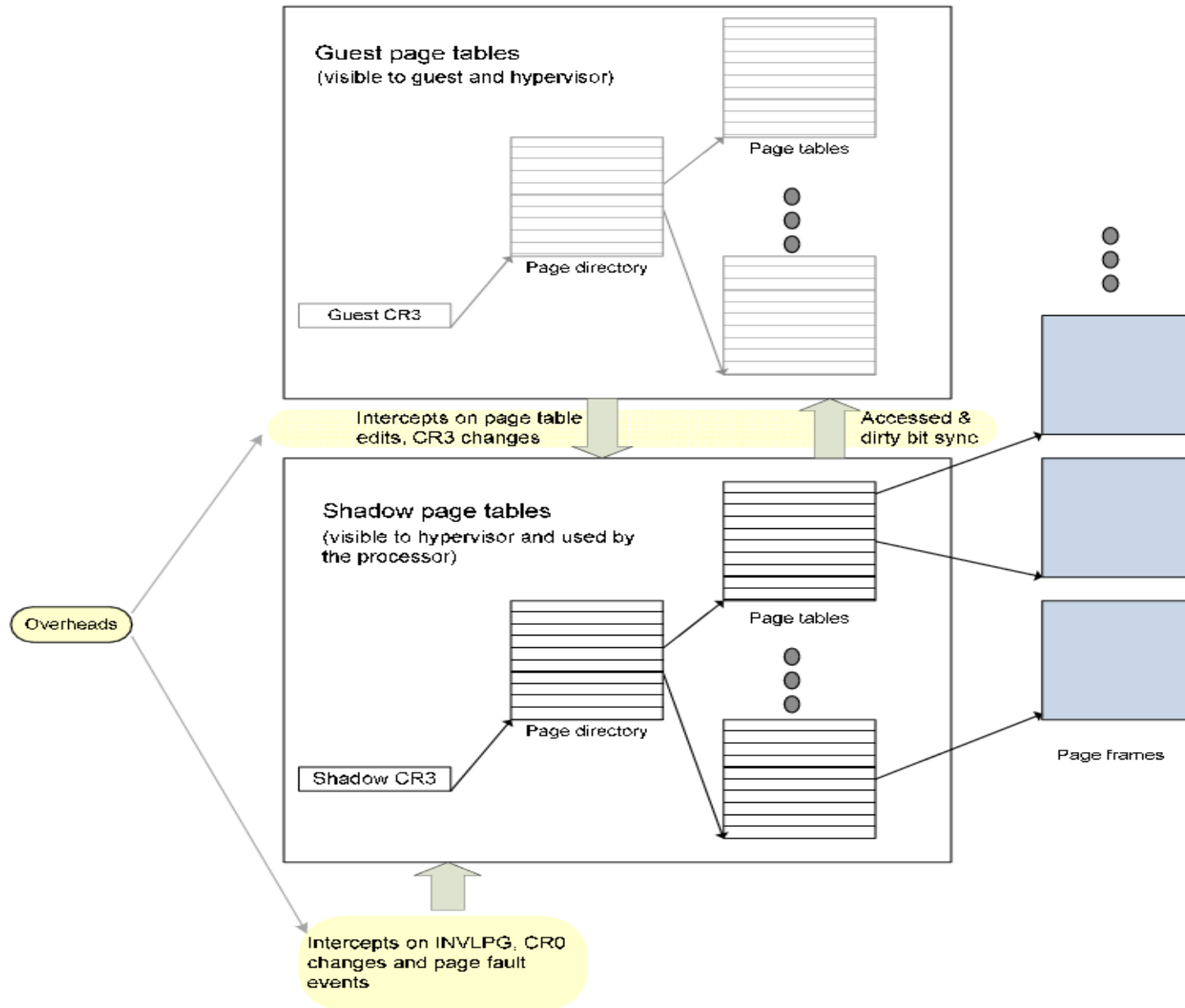
Problem - gościnny OS utrzymuje własne tablice stron.

Rozwiązanie - shadow page tables,
„przykrywające” tablice stron gościa

Shadow Page Tables



Shadow Page Tables



Shadow Page Tables

Wady:

- desynchronizacja pomiędzy tablicami stron gościa a shadow tables i stąd konieczność ich uaktualniania. Techniki:
 - *write-protecting*
 - virtual TLB
- mechanizm programowy, a nie sprzętowy

AMD Nested Paging

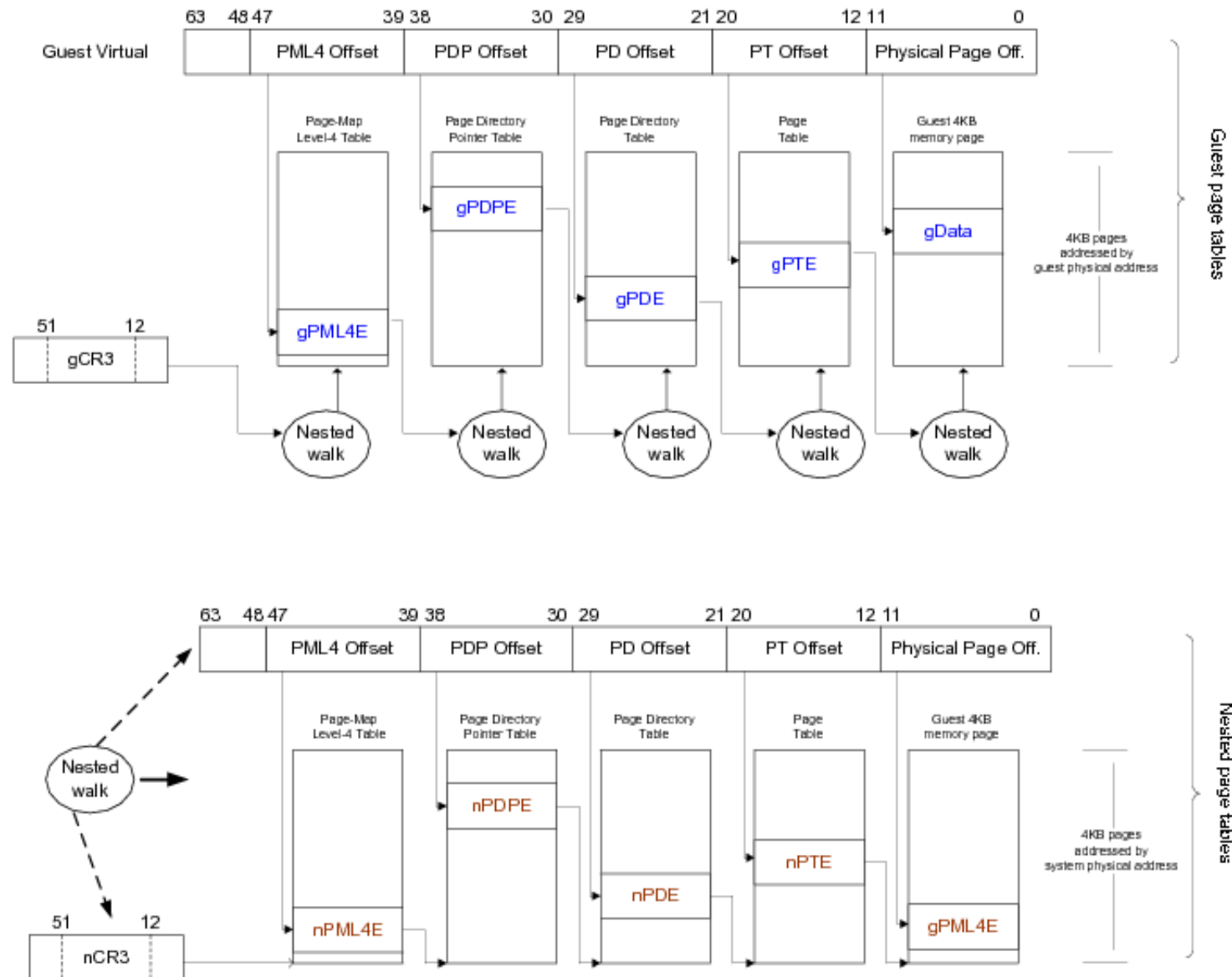
Tłumaczenie adresu jest dwuetapowe:

1. Zmapuj adres wirtualny gościa na adres fizyczny gościa
2. Zmapuj adres fizyczny gościa na adres fizyczny gospodarza

AMD Nested Paging

Translacje adresów zagnieżdżonych są wykrywane i wykonywane przez procesor - utrzymuje on odpowiednie tablice (nested paging tables)

AMD Nested Paging



Intel Extended Page Tables

