Поддержка виртуализации памяти гостевых виртуальных машин

Задачи и методы виртуализации памяти гостевой ВМ

Задачи:

- Изоляция физической памяти всех гостевых ВМ
  guest physical address → host physical address
- Невидимость подмены физической памяти гостя
- Приемлемая производительность в режиме гостя

Методы:

- Механизм перехватов обращений к регистрам MU к в память
- Теневая трансляция адреса (shadow page tables)
- Двухуровневая трансляция адреса (two-dimensional paging)

Перехваты событий MU

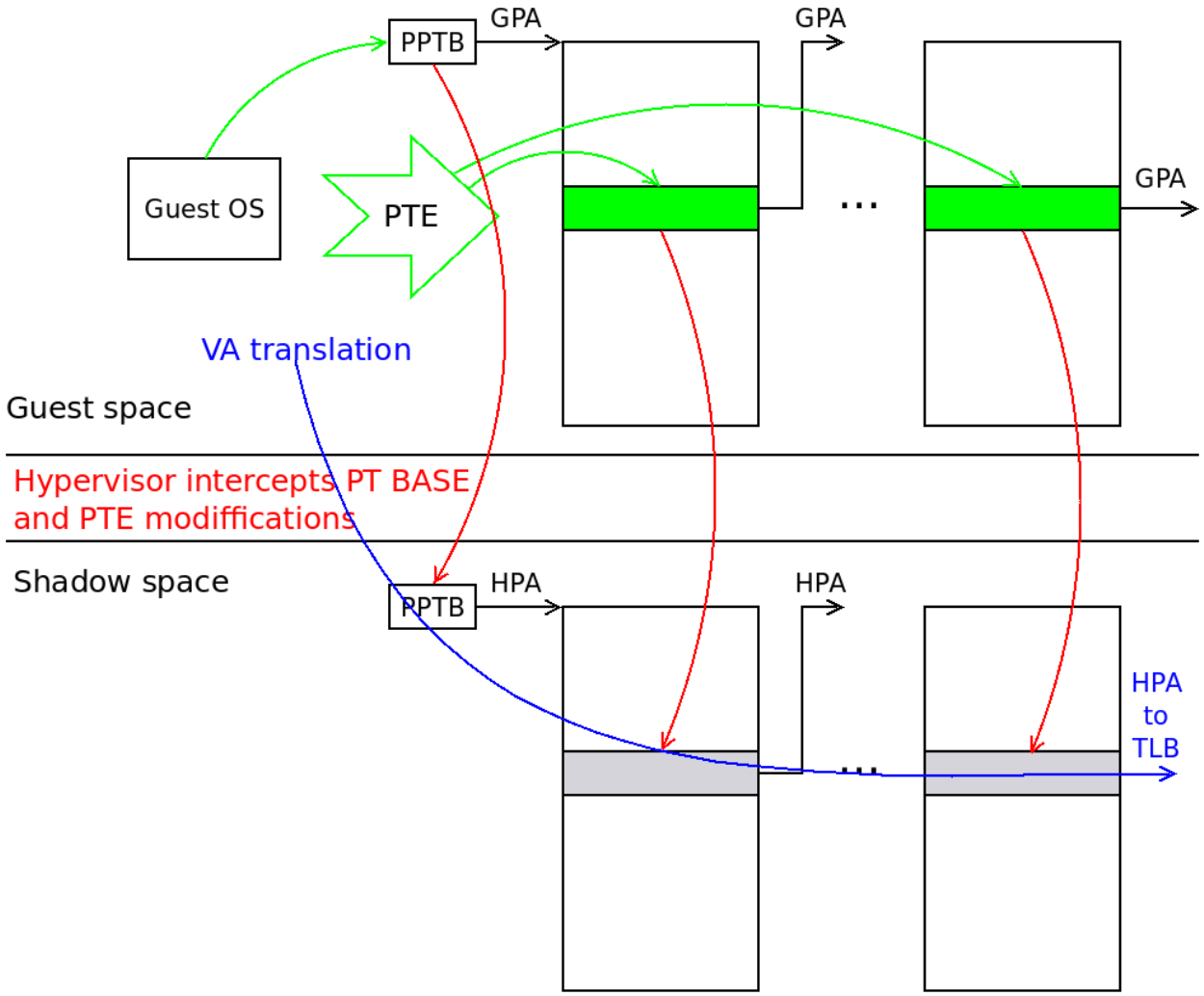
Перехваты следует рассматривать в совокупности с конкретным режимом трансляции адреса, как часть единой концепции, и наоборот.

Две группы перехватов MU:

- Перехваты специальных операций включаются установкой флага в управляющем регистре. Как правило, используются для невидимой подмены результата обращения, например, к регистрам MU.
- Перехваты обычных обращений в память организованы через страничную защиту. Гипервизор анализирует гостевой физической адрес (GPA) и принимает решение, отдавать ли физический ресурс гостю, или нет (например, эмуляция обмена гостя с устройством).

Перехваты не оставляют следов на видимом контексте BM. Из-за отложенного типа перехвата MU пришлось вводить аппаратный механизм перевыполнения прерванных операций.

Теневая трансляция адресов (1)



Теневая трансляция адресов (2)

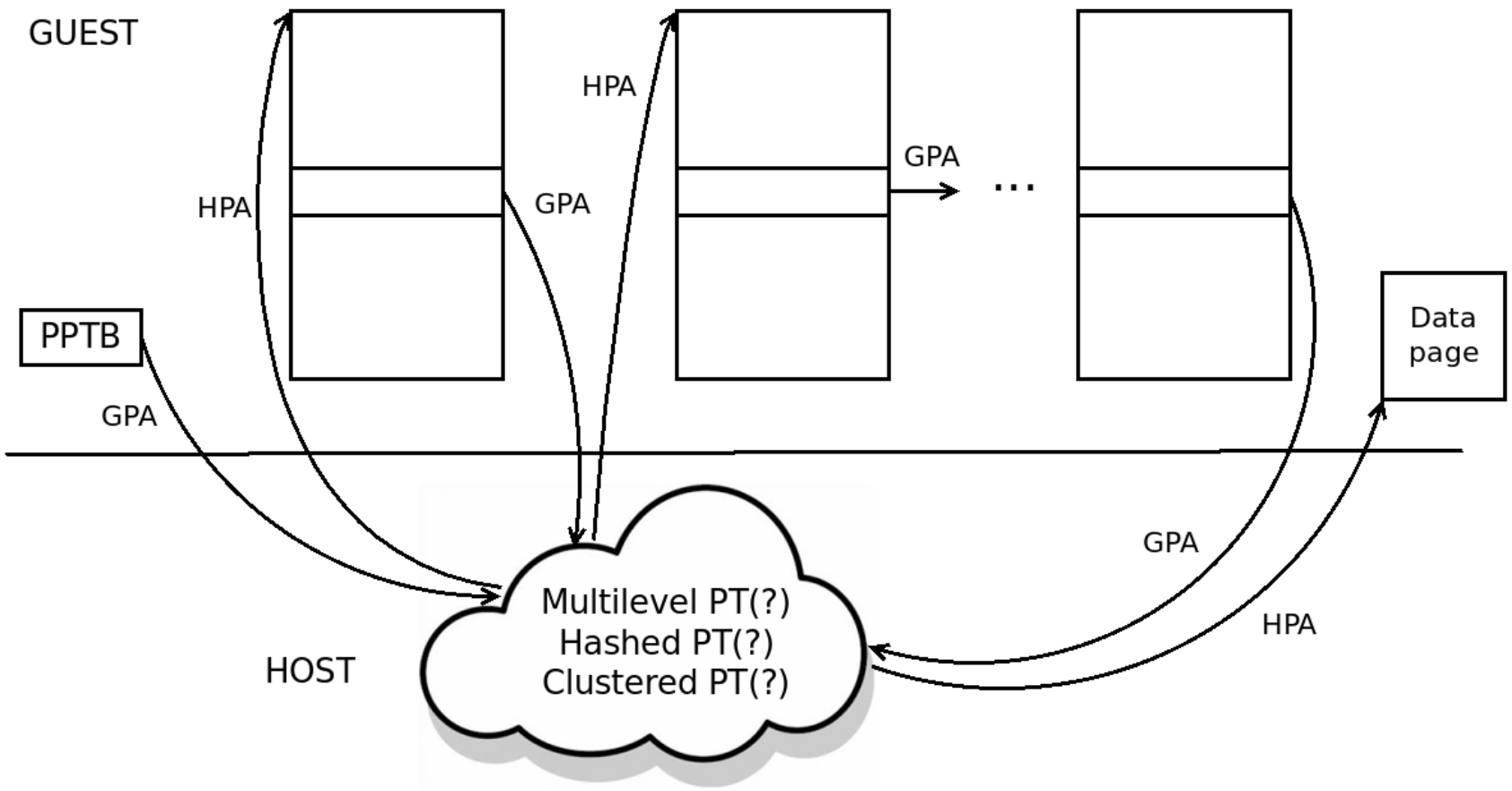
Преимущества:

- Простая реализация в аппаратуре. Алгоритмы прохода по таблице страниц гостя и по теневой таблице идентичны.
- Нет накладных расходов при трансляции адреса.

Недостатки:

- Отсутствует универсальность. Гипервизор обязан знать все детали организации виртуальной памяти гостевой ВМ.
- Накладные расходы на перехват и перенос всех изменений таблицы гостя в теневую таблицу очень велики.

Двухуровневая трансляция (1)



Двухуровневая трансляция (2)

Преимущества:

- Универсальность. Гипервизор ничего не должен знать о гостевой таблице страниц.
- Не нужно следить за таблицей гостя с помощью перехватов — большой выигрыш по сравнению с теневой трансляцией.

Недостатки:

- Сложная реализация в аппаратуре.
- Большой штраф в случае частых промахов в TLB и кэшах TLU.

Двухуровневая трансляция (3)