

簡介

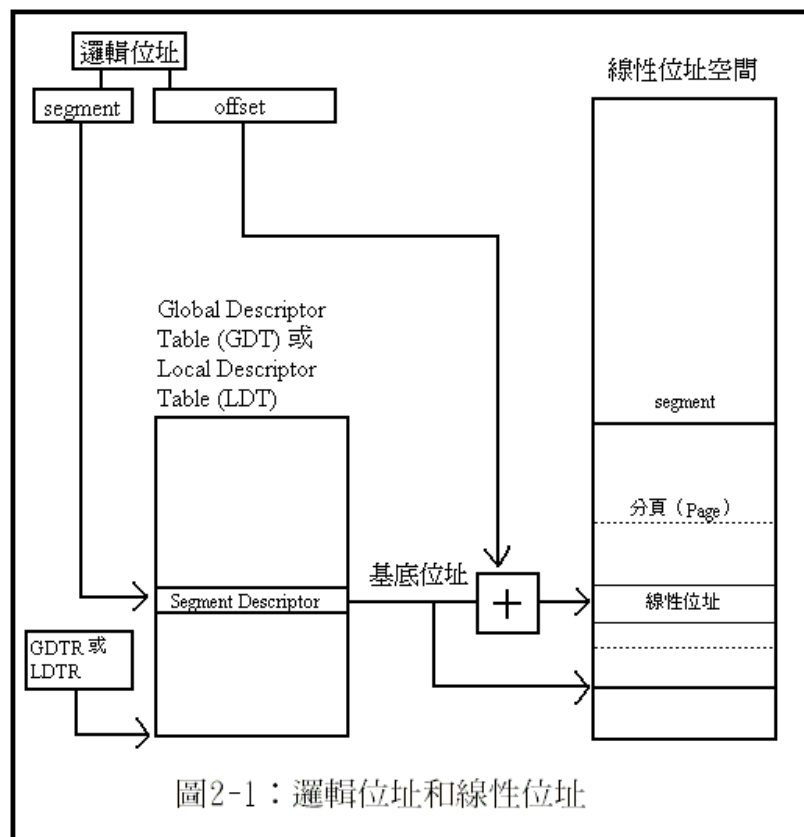
定址方式

在保護模式中，有三種定址方式：邏輯位址（Logical Address）、線性位址（Linear Address）、和實體位址（Physical Address）。對大部分的應用程式而言，幾乎只會用到邏輯位址。線性位址和實體位址在大部分的情形中，只有作業系統會使用。所謂的「實體位址」，就是指系統的記憶體的真正位址，它的範圍由 00000000H 到 FFFFFFFFH，共有 4GB。大部分情形中，系統的 RAM 都是由 00000000H 開始定址（即在最底端），而 ROM 則由 FFFFFFFFH 開始定址（即在最頂端）。這是因為在 RESET 之後，處理器會從定址空間的頂端開始執行，所以把 ROM 定址在頂端才能讓處理器在 RESET 後執行到開機用的程式（如開機自我測試之類的程式）。

在沒有使用分頁（Paging）功能的時候，線性位址是直接對映到實體位址的，也就是說，線性位址就等同於實體位址。不過，在開啟分頁功能之後，一個線性位址可能沒有相對映的實體位址（因為它所對映的記憶體可能被 swap 到硬碟裡了）。所謂的分頁功能，是指把定址空間分割成許多頁，而實際的記憶體可能無法容納這麼多頁，因此有些頁若暫時沒有用到，就可以暫時存放到硬碟（或其它儲存媒體）中，等到需要的時候再取出來。這個功能可以讓系統使用比實際的 RAM 空間更大的記憶體。因此，在這種情形下，一個線性位址所在的頁可能還在硬碟中，因此，要存取這個位址，就要先把 swap 到硬碟中的資料取出，放到實體記憶體中的某個位置中（這時，可能有些頁就得讓開位置，被 swap 到硬碟中了）。

而邏輯位址則和實際模式類似，仍然是 segment:offset 的形式，只不過現在 offset 的大小改成 32 bit 而已，而 segment 仍然是 16 bit。不過，和實際模式不同的是，segment 的地位和過去不同；在保護模式中，segment 的位置不再是固定的，而是可以自由決定的。

Segment 暫存器（稱為 Segment Selector）則是用來選擇想要使用的 segment。同時，在保護模式中，segment 也可以有大小限制，不像在實際模式中，一個 segment 一定是 64KB（雖然 segment 的實際大小可以比 64KB 小，但是處理器並不會檢查存取動作是否超出了 segment 的範圍）。在保護模式中，每一個 segment 都有一個 segment descriptor，描述這個 segment 的位置、大小、型態、存取權限等等資料。Segment 的位置是以「基底位址」來表示，基底位址是一個線性位址。要存取 segment 中的某個位址，需要指定一個 offset 位址，而實際的線性位址則是將 segment 的基底位址加上 offset 就可以得到。下圖顯示出這個記憶體架構的運作方式：



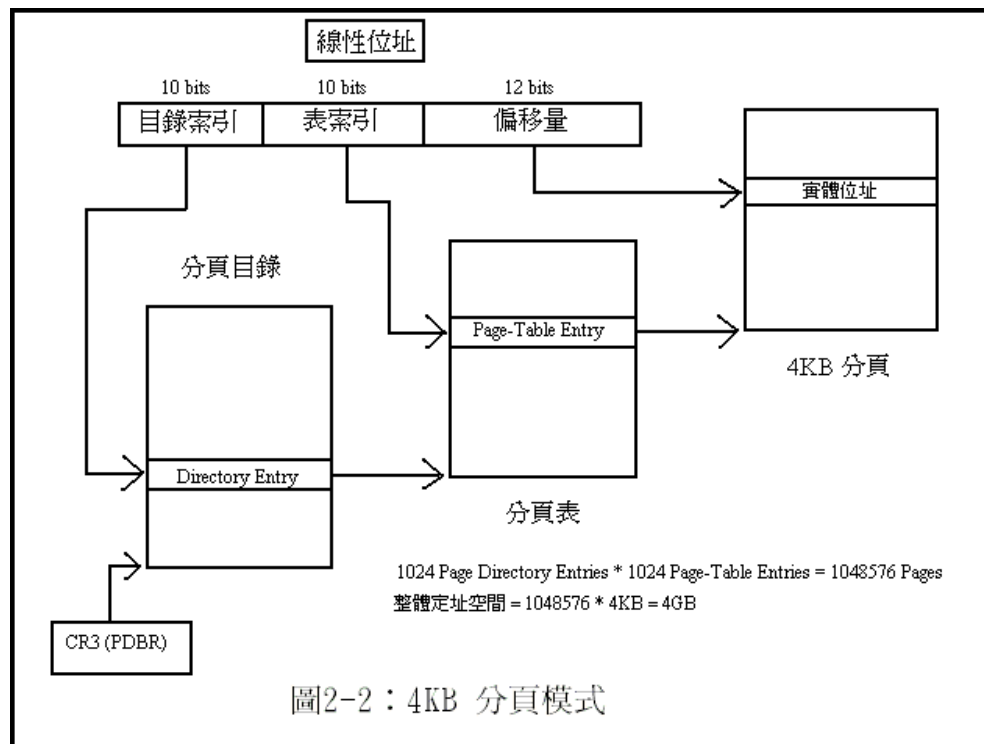
上圖中，顯示出 segment 的 segment descriptor 是存放在 Global Descriptor Table (GDT) 或 Local Descriptor Table (LDT) 中。GDT 和 LDT 都是由 segment descriptor 所組成的陣列。Segment selector 則可以視為這個陣列的 index。GDT 的基底位址存放在 GDTR 中（GDTR 是一個暫存器），而 LDT 的基底位址則放在 LDTR 中（LDTR 也是一個暫存器）。

分段架構可以有效地解決多工環境中，程式和資料的重定位（Reallocation）問題。利用分段架構，為程式和資料分別指定一個 segment，程式和資料都可以從 00000000H 開始取用，而不受程式和資料在記憶體中的位址影響。同時，分段架構也可以避免錯誤的程式意外地存取到不該存取的位址。

分頁架構

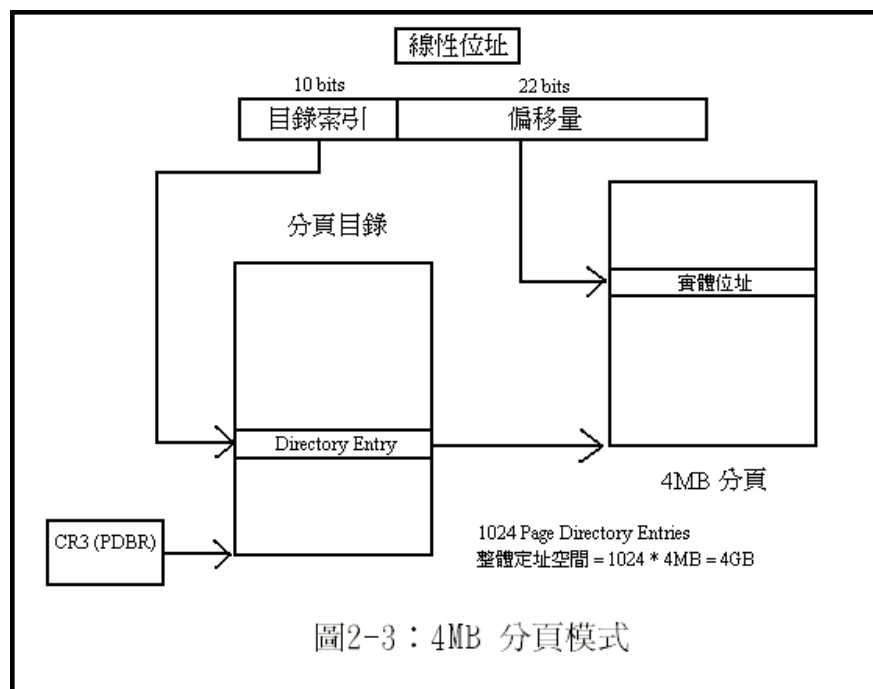
當分頁功能開啟時，線性記憶體就不是直接對映到實體記憶體上了。線性記憶體空間會分割成許多固定大小的頁（Pages），通常是 4KB。在以線性位址存取記憶體時，處理器會找出對映的頁，並把線性位址轉換成相對的實體位址。如果該線性位址所對映的頁現在並不在實體記憶體中，則處理器會發出一個 page-fault 的例外（Exception）。作業系統必須提供一個例外的 handler 來處理這個例外，來取出所需要的頁（例如，作業系統可能會把某一個不需要的頁寫到 swap file 中，再從 swap file 中讀入現在需要的頁）。在處理完這個例外之後，程式就可以從發生例外的地方開始，繼續執行下去。

分頁的大小有兩種：4KB 和 4MB。在 4KB 的模式中，線性位址被分成三個部分：目錄索引（Directory）、表索引（Page Table）、和偏移量（Offset）。如下圖所示：



所有分頁目錄和分頁表中所記載的位址，均為實體位址。在 CR3 中所存放的分頁目錄的基底位址，也是實體位址。分頁目錄的基底位址必須是 4KB 的倍數。

另一個模式是 4MB 分頁模式，即一頁的大小是 4MB。4MB 分頁模式和 4KB 分頁模式很類似，但是在 4MB 分頁模式中，只有分頁目錄，沒有分頁表；即分頁目錄中的 Directory Entry 直接指向分頁的基底位址，而在線性位址中的表索引則和偏移量合併成 22 bits（4MB）的偏移量。如下圖所示：



4MB 分頁模式和 4KB 分頁模式可以共用。例如，在作業系統中，可能會想把整個核心（Kernel）都放在同一頁中，以減少 swap 所產生的額外負擔，而在其它的地方則使用 4KB 的分頁空間。