緒論

Intel Architecture 架構概觀

Intel Architecture 又稱 x86 架構，因為它的第一代處理器的代號是 8086，而其後繼產品依序以 8088、80186、80188、80286……為代號，均為 80x86 的形式；而在 80286 之後，Intel 改以 i386、i486 來命名，因此才被稱為 x86 架構。在 i486 處理器之後，Intel 就不再以 x86 的形式命名，所以在這裡以較正式的 Intel Architecture 來稱呼這個架構（簡稱 IA 架構）。
Intel Architecture 系列的處理器中，最早的 8086 是一 16 bit 的處理器，具有 16 bit 的暫存器和 data bus，並具有 20 bit 的定址能力，能定址最多達 1MB 的記憶體，在當時算是相當大的數目。然而，20 bit 的位址和 16 bit 的暫存器無法相符，因此 Intel 設計了一種 segment:offset 的定址方式，利用兩個 16 bit 暫存器來表示一個 20 bit 的位址。
到了 80286 的時代，1MB 的定址能力已經不敷使用，因此 Intel 為它設計了一個新的「保護模式」（Protected Mode），並將原先 8086 所使用的方式稱為「實際模式」（Real Mode）。80286 具有 24 bit 的定址能力，可以定址 16MB 的記憶體，但是只有在保護模式下才能發揮。在實際模式中，為了維持和 8086 的相容性（這點是 Intel 非常堅持的），還是只能使用 1MB 的記憶體。80286 的保護模式已經有了多工作業的能力，並且可以保護各個節區的資料和程式不被其它程式干擾。IBM 的 OS/2 1.x 和 Microsoft 的 Windows 3.x 都有支援這個模式。
在 i386 出現時，情形有很大的變化。i386 是一個 32 bit 的處理器，並具有 32 bit 的定址能力，可以定址達 4GB 的記憶體。它同時也改進了 80286 不完整的的保護模式，提供了很多新的功能，如虛擬記憶體等等。在這篇文章中所要說明的「保護模式架構」，就是指 i386 的保護模式。

IA-32 的操作模式

在 i386 以後的 Intel Architecture 相容處理器（統稱 IA-32 架構），具有四種操作模式：

- 實際模式（Real Mode）：在這個模式下，處理器就好像是一個超快速的 8086 一般。
- （32 bit 的）保護模式（Protected Mode）：在這個模式下，處理器具有多工、分節保護、分頁等等的能力。
- 虛擬 8086 模式（Virtual-8086 Mode）：這個模式是在一般的保護模式下，模擬一個 8086 的執行環境，可以同時執行多個 8086 程式。
- 系統管理模式（System Management Mode，SMM）：這個模式會使處理器切換到一個獨立的定址空間中執行，通常在電源管理之類的系統工作才會使用這個模式。

而在保護模式中，有四個重要的部分：記憶體管理、保護機制、中斷 / 例外處理、和多工處理。在本文中，會分別針對這四點做詳細的說明。而在 P6 家族（包括 Pentium Pro、Pentium II 等處理器）中所提供的新功能（如延伸定址模式，Extended Addressing）則不在本文範圍之中。

系統暫存器

在處理器中有一些暫存器，是用來控制系統的一些行為的，這些暫存器通常只有作業系統會使用。這些暫存器中，和保護模式有關的，有：

- 在 EFLAGS 中（32 bit 的旗標暫存器）的一些系統旗標和 IOPL 欄位。在保護模式中，只有 CPL 小於或等於 IOPL 的程式才存取 I/O 位址空間，和進行一些其它的操作。
- 控制暫存器（Control Registers），包括 CR0、CR2、CR3、CR4（CR1 保留）。這些暫存器包括一些和保護模式關係密切的內容（例如，是否進入保護模式、是否開啟分頁功能等等）。
- GDTR、LDTR、和 IDTR。這三個暫存器存放三個系統的 descriptor table 的基底位址和邊界（大小）。
- 工作暫存器（Task Register）存放目前工作（task）的 TSS 的基底位址和大小。

在後面的章節中，會分別對這些暫存器做較詳細的說明。