C++ Tricks 2.1 X86 概述

從 farseerfc.wordpress.com 導入

2.1 X86概述

所謂X86體系結構，是指以Intel 8086芯片爲首的芯片所沿襲的CPU結構，一些文檔中又被稱作IA32體系結構。包括的芯片有但不限於:Intel 8086至 80486，奔騰(Pentium)系列處理器1至4，賽揚系列處理器，酷睿系列處理器，以及AMD的相應型號產品。X86體系結構在早期屬於16位處理器，自80386之後擴展爲32位處理器，所以一些文檔中又把80386之後的32位處理器體系稱作I386。自Pentium4後期，AMD的Athlon64開始，I386被進一步擴充爲64位處理器，含有64位尋址能力的X86體系結構被稱作X86-64或IA32-64。總之，市售的個人電腦用CPU，除蘋果的Macintosh之外，全部採用X86體系結構芯片。

在X86早期，16位的尋址能力只支持64KB(2^16=64K)內存，這顯然是不夠的。Intel採用分段尋址的方法，用4位段位+16位偏移量，提供了總共1MB(2^20=1M)的尋址能力。所以在X86的16位編程中，有兩種指針類型：長指針(lp,long pointer)和短指針(sp,short pointer)，長指針(20位)提供整個內存空間尋址能力，短指針(16位)僅支持同一段中的尋址。在“古代”DOS及Win3.x編程過程中，兩種類型的指針，以及總共1MB的內存大小，常常把程序員們折騰得焦頭爛額。

自I386之後，CPU纔開始提供32位的尋址能力。有了整整4GB(2^32=4G)的尋址空間，所有指針統一爲長指針(32位)。時至今日，我們仍可以看到微軟文檔中指針變量的lp前綴。由於內存管理的需要，分段機制被保留下來，但這一次不是因爲地址空間太小，而是因爲地址空間遠大於實際內存容量，從而採用了虛擬內存機制。

在從16位結構向32位結構轉變的過程中，由於向下兼容的歷史原因，曾一度長時間出現硬件32位(I386)、軟件16位(Win3.x)的情況。同樣也是爲了兼容16位軟件，Win9x操作系統(Win95、Win98、WinME)保留了16位代碼和32位代碼。混合代碼的設計使得Win9x及其混亂和不穩定。直到完全32位內核的操作系統WinNT(以及構建於其上的Win2000，WinXP，Win2003)的出現，X86平臺上內存佈局混亂的局面才得以改善。有了從16位至32位移植的經驗和準備，現今的從32位到64位的操作系統移植顯得平穩順利很多。WinXP和WinVista系統都同時發佈了32位版本和64位版本，並且其x86-64系統都實現了對32位軟件的無縫銜接支持。