C++ Tricks 2.1 X86 概述

从 farseerfc.wordpress.com 导入

2.1 X86概述

所谓X86体系结构，是指以Intel 8086芯片为首的芯片所沿袭的CPU结构，一些文档中又被称作IA32体系结构。包括的芯片有但不限于:Intel 8086至 80486，奔腾(Pentium)系列处理器1至4，赛扬系列处理器，酷睿系列处理器，以及AMD的相应型号产品。X86体系结构在早期属于16位处理器，自80386之后扩展为32位处理器，所以一些文档中又把80386之后的32位处理器体系称作I386。自Pentium4后期，AMD的Athlon64开始，I386被进一步扩充为64位处理器，含有64位寻址能力的X86体系结构被称作X86-64或IA32-64。总之，市售的个人电脑用CPU，除苹果的Macintosh之外，全部采用X86体系结构芯片。

在X86早期，16位的寻址能力只支持64KB(2^16=64K)内存，这显然是不够的。Intel采用分段寻址的方法，用4位段位+16位偏移量，提供了总共1MB(2^20=1M)的寻址能力。所以在X86的16位编程中，有两种指针类型：长指针(lp,long pointer)和短指针(sp,short pointer)，长指针(20位)提供整个内存空间寻址能力，短指针(16位)仅支持同一段中的寻址。在“古代”DOS及Win3.x编程过程中，两种类型的指针，以及总共1MB的内存大小，常常把程序员们折腾得焦头烂额。

自I386之后，CPU才开始提供32位的寻址能力。有了整整4GB(2^32=4G)的寻址空间，所有指针统一为长指针(32位)。时至今日，我们仍可以看到微软文档中指针变量的lp前缀。由于内存管理的需要，分段机制被保留下来，但这一次不是因为地址空间太小，而是因为地址空间远大于实际内存容量，从而采用了虚拟内存机制。

在从16位结构向32位结构转变的过程中，由于向下兼容的历史原因，曾一度长时间出现硬件32位(I386)、软件16位(Win3.x)的情况。同样也是为了兼容16位软件，Win9x操作系统(Win95、Win98、WinME)保留了16位代码和32位代码。混合代码的设计使得Win9x及其混乱和不稳定。直到完全32位内核的操作系统WinNT(以及构建于其上的Win2000，WinXP，Win2003)的出现，X86平台上内存布局混乱的局面才得以改善。有了从16位至32位移植的经验和准备，现今的从32位到64位的操作系统移植显得平稳顺利很多。WinXP和WinVista系统都同时发布了32位版本和64位版本，并且其x86-64系统都实现了对32位软件的无缝衔接支持。