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。