保护模式下 Pentium 微处理器的存储管理方案

许精明
(安徽工业大学 计算机学院,安徽 马鞍山 243002)

摘 要:为了解析 Intel Pentium 处理器的先进技术,分析了 Pentium 微处理器的存储管理方案,阐述了保护模式下的分段和分页技术,并指出了存储管理对实现存储保护和虚拟存储提供的优越性,供有关专业人员研究参考。

关键词:保护模式;存储管理;段描述符;逻辑地址;线性地址
中图分类号:TP311.11; TP332 **文献标识码**:A **文章编号**:1005-3751(2003)03-0010-02

Memory Management Scheme of Pentium Microprocessor in Protected Mode

XU Jing-ming
(College of Computer, Anhui Univ. of Techn., Maanshan AH 243002, China)

Abstract: In order to resolve and analyze the advanced technique of Intel Pentium microprocessor, analyzes the memory management scheme of Pentium microprocessor. Elaborates the technology of segmentation and paging in protected mode. Points out that the memory management is of advantage for the memory protection and virtual memory. It can provide the study and reference for professionals.

Key words: protected mode; memory management; segment descriptor; logical address; lineal address

1 引 言

保护模式是 Pentium 系列微处理器最具特色的工作模式之一。在保护模式下,存储管理的功能是进行内存空间的分配和保护,以达到充分利用有限的存储资源和确保代码与数据安全的目的。由于 Pentium 微处理器引进了 32 位结构和大量先进技术,并强调硬件技术与软件技术相结合,使其已成为一种超级微处理器,因此它的存储管理具有复杂性、通用性和代表性。作者对 Pentium 微处理器的存储管理方案进行了详细分析和研究。

2 Pentium 微处理器的存储管理方案

2.1 分段技术

分段是将处理器的可寻址存储空间(即线性地址空间)分成叫做段的较小的保护地址空间。根据段中存放内容的不同,可分为代码段、数据段、堆栈段和系统段,每个段都有一个段描述符。对段中某一字节的访问须通过逻辑地址(又称虚拟地址)进行。逻辑地址由 16 位的段选择符和 32 位的偏移量组成,其中段选择符提供对段描述符的索引,段描述符则指出被访问段的基址、大小、访问权限和特权级。段基址加上偏移量就形成线性地址,再由该线性地址去定位线性地址空间中被访问段中的一个字节。

收稿日期:2002-07-11
作者简介:许精明(1963-),男,安徽桐城人,硕士,研究方向为计算机体系结构,人工智能,CAD/CAM,CIMS 网络。

图 1 为逻辑地址到线性地址的转换示意图。

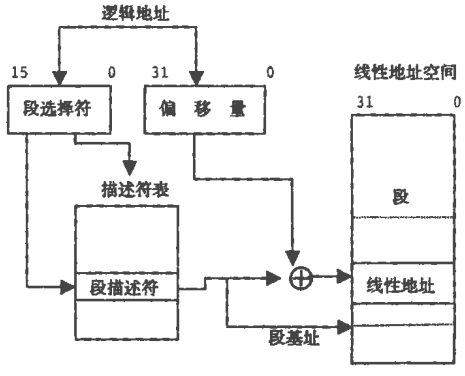

图 1 逻辑地址到线性地址的转换

在保护模式下,Pentium 微处理器的常规地址线为 32 位,可直接寻址的物理地址空间和线性地址空间都是 4GB (2^{32}字节);逻辑地址空间为 64TB ($2^{14} \cdot 2^{32}$字节),其中 2^{14} 为段选择符中高 14 位所确定的可访问的段数,2^{32}为每段的最大地址空间。

(1)段选择符。段选择符是段的 16 位标识符,如图 2 所示。它不直接指向段,而是指向所定义段的段描述符。

对于要访问某个段的程序来说,被访问段的段选择符须事先加载到段寄存器中。段寄存器有两部分组成,一部分用来加载 16 位的段选择符(可见部分),另一部分用来加载由段选择符指向的 64 位段描述符(隐含部分),如图 3 所示。Pentium 微处理器共提供了 6 个段寄存器(CS,SS,DS,ES,FS,GS),每个段寄存器支持特定种类的存储

器访问。

(2)段描述符。段描述符为 64 位,占 8 个字节(两个双字)。它为处理器提供段的基址、大小和段的访问控制及状态信息。段描述符分两类:①代码段与数据段描述符;②系统段描述符。图 4 为段描述符的通用格式。

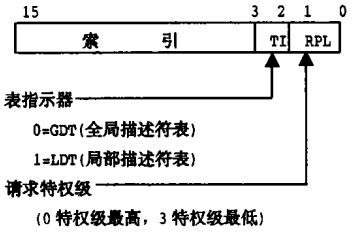

图 2　段选择符

	段选择符	段　描　述　符
CS	16 位段选择符	32 位段基址、20 位段限、12 位访问控制和状态信息
SS		
DS		
ES		
FS		
GS		

图 3　段寄存器

(3)代码段与数据段描述符。当段描述符中的 S(图 4 中第二个双字的第 12 位)标志置位时,描述符既可用于代码段,也可用于与数据段。用段描述符中段类型字段的最高位(图 4 中第二个双字的第 11 位)来确定是用于数据段(该位清零)还是代码段(该位置位)。

对于数据段,段类型字段中的低三位定义为访问(A)、可写(W)和扩展方向(E)。对于代码段,段类型字段中的低三位定义为访问(A)、可读(R)和相容(C)。

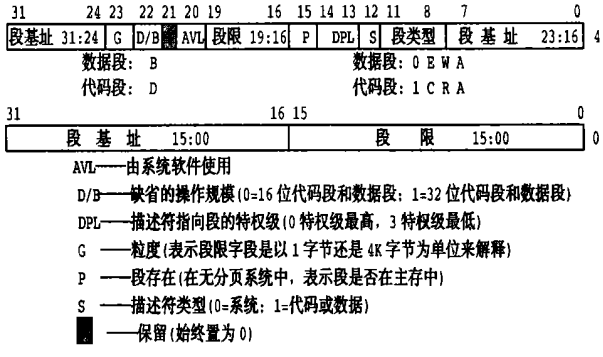

图 4　段描述符

(4)系统描述符。当段描述符中的 S 标志清零时,描述符类型为系统描述符。Pentium 微处理器可识别六种系统描述符:局部描述符表(LDT)描述符、任务状态段(TSS)描述符、调用门描述符、中断门描述符、陷阱门描述符和任务门描述符。这些描述符分为两类:系统段描述符和门描述符。系统段描述符指向系统段(LDT 段和 TSS 段);门描述符(调用门、中断门、陷阱门、任务门)用于在转移过程中增加一级控制,通过门控可以转去执行一般不能直接访问的程序。

2.2　分页技术

分页管理的基本思想是将 4GB 的线性地址空间分成固定大小的页面,这些页面可以映射到物理地址空间和磁盘存储器上。物理地址空间上的固定页面又称为页框。

(1)页目录和页表。分页管理机制使用的四种数据结构是:

•页目录:由最多可达 1024 个的页目录项组成,每个页目录项为 32 位(4 个字节)。页目录可包含在一个 4kB 的页面中。

•页表:由最多可达 1024 个页表项组成,每个页表项为 32 位(4 个字节)。同样,页表也可包含在一个 4kB 的页面中。

•页面:指一个大小固定的、连续的、未分段的平面地址空间,如 4kB、4MB 页面。

•页目录指针表:由 4 个 64 位项组成,每项指向一个页目录。该数据结构只在允许物理地址扩展时使用。

在 4kB 页面规模时,页表中可存放 1024 个页框的基地址,页目录中可存放 1024 个页表的基地址。这样,4GB 的线性地址空间可被分隔成 1024 个页组,每个页组的长度为 4MB;每个页组又包含 1024 个页面,每个页面为 4kB。在页变换过程中,页目录项指向页表,页表项又指向 4kB 页面。图 5 为 4kB 页面和 32 位物理地址时的页目录项与页表项格式。

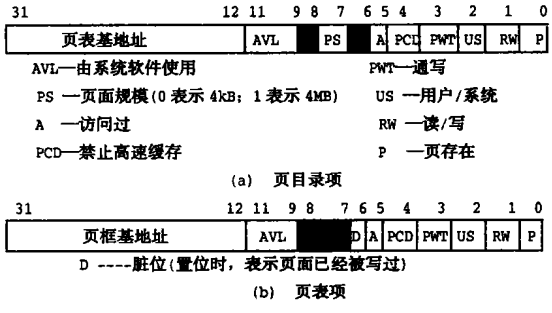

图 5　4kB 页面和 32 位物理地址的页目录项与页表项格式

(2)页变换过程。按页面规模的不同,线性地址的映射可分成 4kB 页面、4MB 页面和 4kB 与 4MB 页面混合三种情况。

①4kB 页面的线性地址转换:CPU 首先获得线性地址,并以控制寄存器 CR3(页目录基址寄存器 PDBR)中的高 20 位作为页目录基地址的高 20 位,隐含的低 12 位为全 0,获得 32 位的页目录基地址;再以线性地址的高 10 位页目录索引(×4)查找页目录,由相应的页目录项得到相应页表的基址;接着以线性地址的中间 10 位页表索引(×4)查找页表,由相应的页表项得到相应的页框基地址,将该页框基地址加上线性地址中的低 12 位页内偏移量就得到最终的 32 位物理地址。图 6 为 Pentium 微处理器 4kB 页面的线性地址转换机制示意图。

②4MB 页面的线性地址转换:当控制寄存器 CR4(含

(下转封三)

NCF FILE 菜单生成新的 AUTOEXEC·NCF 和 STARTUP·NCF 文件。

⑥在一工作站上登录，此时 SUPERVISOR 没有口令，登录后可以看到网络上安装的全部内容，转到原系统(即现在的 SYS1 卷)，在 SYSTEM 目录下找到三个装订库文件：NET $OBJ·SYS，NET $VAL·SYS，NET $PROP·SYS，用 FLAG 命令去掉它们的[H S]属性；用 ATTRIB 去掉其 S 属性，然后将它们的扩展名全部改为·OLD。

⑦在服务器端用 DISMOUNT 命令将 SYS1 和 SYS 卸下，将它们的卷名改回原来的 SYS 和 USER。

⑧重新启动服务器，在工作站上以 SUPERVISOR 登录，由于原装订库已改名，故 SUPERVISOR 没有口令。运行 SYSCON 命令，设置新的 SUPERVISOR 口令；

⑨运行装订库恢复程序 BINDREST·EXE 恢复装订库，这样，SUPERVISOR 即可按新的口令入网。

⑩用 DELETE·EXE 命令将 USER 卷上的系统文件全部删除，然后用 FILER 命令将 USER 卷上被删除的文件彻底删除，最后以 SUPERVISOR 身份将被修改的用户口令全部重新设定。

至此，整个网络已完全恢复到原来的状态。

3 结束语

本文给出了 NOVELL 网络中超级用户口令遗失的五种解决方案，相信还有更好的方案可以供我们去思考和研究。

参考文献：

[1] 李革新·数据通信与计算机网络[M]·北京：高等教育出版社，2000.

[2] 陈明德·NETWARE 网络实际操作一提高篇[M]·北京：人民邮电出版社，1997.

[3] 陈志刚·计算机局域网与 NOVELL 实用教程[M]·长沙：中南工业大学出版社，1993.

[4] 孙 莉·Netware 网络超级用户口令的安全管理[J]·盐城工学院学报，2000，(1)：71—72.

[5] Karanjit S· Netware 4.1 实用管理大全[M]·北京：海洋出版社，1998.

[6] 刘 琳·最新诺顿磁盘管理使用指南[M]·北京：海洋出版社，1993.

(上接第 11 页)

一组允许结构扩展标志的寄存器)中页面规模扩展标志(PSE)置位，且页目录项(PDE)中的页面规模(PS)标志置位时，页面规模大小选定为 4MB。此时，线性地址对 4MB 页面的映射直接由页目录项完成，不经过页表。图 7 为 4MB 页面的线性地址转换示意图。

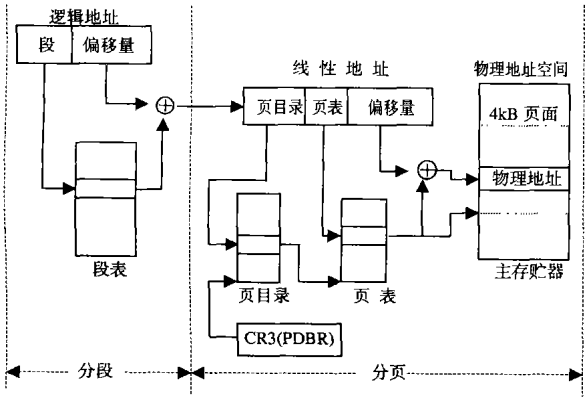

图 6 Pentium 微处理器 4kB 页面的线性地址转换机制

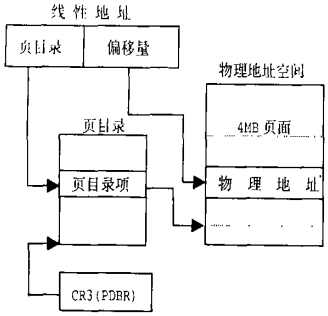

图 7 4MB 页面的线性地址转换

③4kB 页面与 4MB 页面混合的线性地址转换：当控制寄存器 CR4 中页面规模扩展标志(PSE)置位，且页目录项(PDE)中的页面规模(PS)标志清除时，页面规模大小选定为 4kB；若页目录项(PDE)中的页面规模(PS)标志置位，页面规模大小选定为 4MB。因此，当 CR4 中 PSE 标志置位时，通过改变 PDE 中 PS 标志可以使页目录中同时包含 4kB 和 4MB 页面，形成 4kB 与 4MB 页面的混合，它们的线性地址转换分别按 4kB 与 4MB 页面的情况进行。

3 结束语

Pentium 微处理器的地址转换过程看起来很复杂，但实际上这些转换过程都是由 CPU 内部硬件实现的，对用户来说是完全透明的。

由于采用了基于分段和分页技术的存储管理机制，使得 Pentium 微处理器在实现存储保护和虚拟存储以及更方便地进行内存数据与磁盘的交换等许多方面都具备了一定的优越性。

参考文献：

[1] 刘清森，马鸣锦· Pentium Ⅱ/Ⅲ 体系结构及扩展技术[M]·北京：国防工业出版社，2000.

[2] William S· Computer Organization and Architecture (Fifth Edition)[M]· 北京：高等教育出版社，Pearson Education 出版集团(英文影印版)，2001.

[3] 李伯成，侯伯亨· 微型计算机原理及应用[M]· 西安：西安电子科技大学出版社，2000.