保护模式

保护模式是80386处理器的主要工作模式。在此方式下，80386可以寻址4GB的地址空间，同时，保护模式提供了80386先进的多任务、内存分页管理和优先级保护等机制。

在保护模式下，前面32个中断都是保留给CPU异常处理用。

80386处理器的3种工作模式各有特点且相互联系。实模式是80386处理器工作的基础，这时80386当做一个快速的8086处理器工作。在实模式下可以通过指令切换到保护模式，也可以从保护模式退回到实模式。虚拟86模式则以保护模式为基础，在保护模式和虚拟86模式之间可以互相切换，但不能从 实模式直接进入虚拟86模式或从虚拟86模式直接退到实模式。

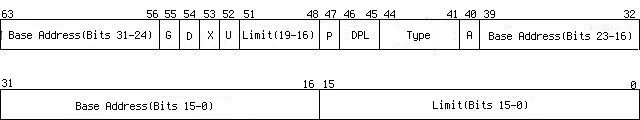
从实模式切换到保护模式是通过修改控制寄存器CR0的控制位PE（位0）来实现的。在这之前还需要建立保护模式必需的一些数据表，如全局描述符 表GDT和中断描述符表IDT等。

描述符

按照描述符所描述的对象来划分，描述符可分为三类：存储段描述符，系统段描述符，门描述符（控制描述符）

存储段描述符

代码和数据描述符的格式



|  |  |
| --- | --- |
| Limit(位 15-0) | 长度的低16位 |
| Base Address(位15-0) | 基地址的低16位 |
| Base Address(位23-16) | 基地址的中8位 |
| A | 存取信息，上一次存取是读(=0)还是写(=1) |
| Type |  |
| 位41 | 对数据/堆栈段而言，可写(=1)；对代码段而言可读(=1) |
| 位42 | 对数据/堆栈段而言表示扩展方向，向下(=1)；对代码段而言confirming(=1) |
| 位43 | 是代码段(=1)还是数据/堆栈段(=0) |
| 位44 | 对代码/数据段必须是1 |
| DPL | 描述符权限级，使用0级内核权限和3级用户权限 |
| P | 段是否存在，本教程中始终是1 |
| Limit(位19-16) | 长度的中8位 |
| U | 用户定义 |
| X | 未使用 |
| D | 指令和数据是32位(=1)还是16位(=0) |
| G | 长度单位是4KB还是1字节 |
| Base Address(位31-24) | 基地址的高8位 |

描述符表有三种类型：GDT(全局描述符表)、LDT(局部描述符表)和IDT(中断描述符表)

系统中只有一个GDT和一个IDT，但每个进程都可以有它们自己的LDT。处理器保留了GDT表的第一条描述符，据手册所述它的值应为零并且不能被使用。

GDT是一个段描述符数组，其中包含所有应用程序都可以使用的基本描述符。

LDT也是段描述符的一个数组。与GDT不同，LDT是一个段，其中存放的是局部的、不需要全局共享的段描述符。 每一个操作系统都必须定义一个GDT，而每一个正在运行的任务都会有一个相应的LDT。每一个描述符的长度是8个字节，

中断描述符会告诉处理器到那里可以找到中断处理程序。和实模式一样，每一个中断都有一个入口，但是这些入口的格式却完全不同。

选择子

选择子的格式



|  |  |
| --- | --- |
| RPL | 请求权限等级 |
| TI | GDT(=0)还是LDT(=1)的索引 |
| Index | 索引值 |

RPL,Requested Privilege Level

TI,Table Indicator

80386 有4个32位控制寄存器，名字分别为CR0、CR1、CR2和CR3。CR1是保留在未来处理器中使用的，在80386中没有定义。CR0包含系统的控制 标志，用于控制处理器的操作模式和状态。CR2和CR3是用于控制分页机制的。在此，我们关注的是CR0寄存器的PE位控制，它负责实模式和保护模式之间 的切换。当PE=1时，说明处理器运行于保护模式之下，其采用的段机制和前面所述的相应内容对应。如果PE=0，那么处理器就工作在实模式之下。

CR0

31 30 ---5 4 3 2 1 0

PG 0 --- 0 ET TS EM MP PE

PE 0：实模式，1：保护模式

PG 0：禁止分页管理，1：分页管理

GDTR

48位，高32位：基地址，低16位：界限。界限是字节单位的，n个描述符的描述符表的界限大小为8\*n-1。

LDTR

IDTR

TR

切换到保护模式，实际就是把PE位置为1。为了把系统切换到保护模式，还要做一些其它的事情。程序必须要对系统的段寄存器和控制寄存器进行初始化。把PE位置1后，还要执行跳转指令。过程简述如下：

1.创建GDT表;

2.通过置PE位为1进入保护模式;

3.执行跳转以清除在实模式下读取的任何指令。

实模式下，cpu指令访问的地址就是物理地址,形式为：段寄存器：偏移

在保护模式下，cpu可以使用分段机制和分页机制。

分段机制下使用的地址就是逻辑地址，形式为：段选择子：偏移

分页机制下使用的地址就是线性地址，形式为：0xXXXXXXXX

无论是逻辑地址还是线性地址，都要被cpu映射成物理地址。

保护模式下必须采用分段机制。在此基础上可采用分页机制。

逻辑地址被转化为线性地址，如果采用分页机制，则该线性地址通过分页机制被映射成物理地址。如果不采用分页机制，则该线性地址就是物理地址。

实模式下的物理地址只能访问1M以下空间，而保护模式下的物理地址可以访问所有32位空间。并且要注意，物理内存空间只是物理地址空间的一个部分而已。