PPT相关内容

1. 什么是实模式，什么是保护模式？

CPU复位(reset)或加电(power on)的时候就是实模式启动

不能实现权限分级，也不能访问20位以上的地址线

在保护模式下，全部32条地址线有效，4G寻址空间

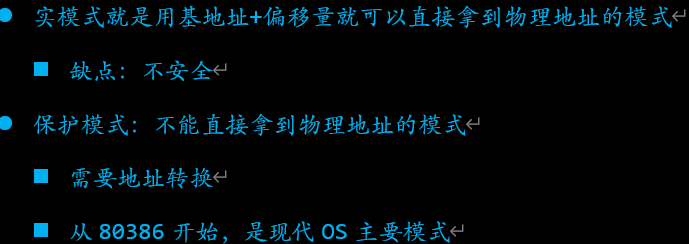
之后一般就是加载OS模块，进入保护模式

保护模式出现的原因是：**\*\*保护进程地址空间\*\***

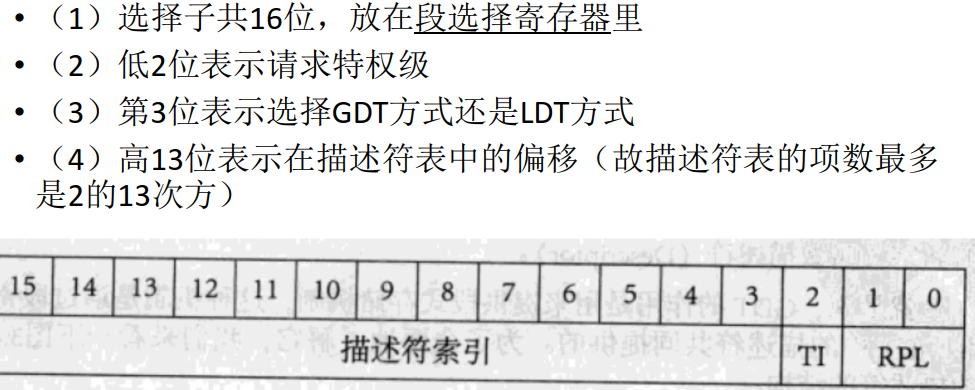
两种模式下的程序寻址方式发生了变化

实模式下，寻址是段+偏移，但是段指向GDT/LDT

GDT定义了段的起始位置、界限、属性等，提供段氏存储机制



1. 什么是选择子？



段选择子，**Selector**

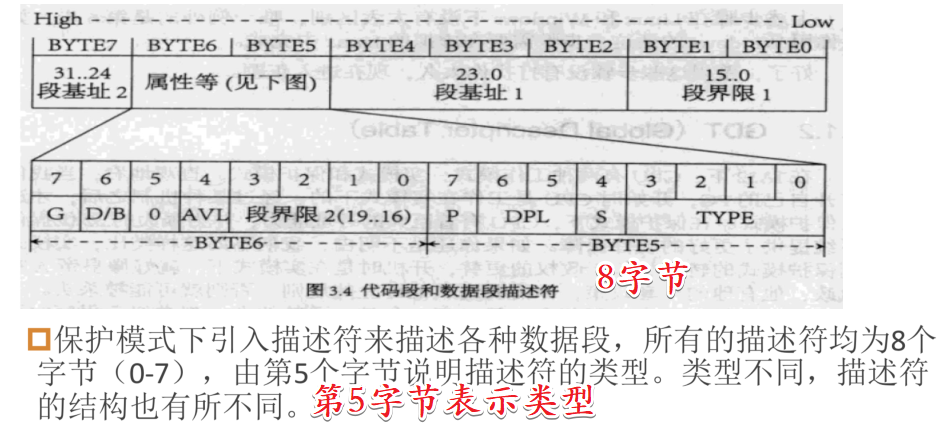
由**GDTR访问GDT是通过“段选择子”（实模式下的段寄存器）来完成的**

段选择子是一个**16位**的寄存器（同实模式下的段寄存器相同）

包括三部分：**描述符索引（index）、TI、请求特权级（RPL）**

* index（描述符索引）：表示所**需要的段的描述符在描述符表的位置**，由这个位置再根据在GDTR中存储的描述符表基址就可以**找到相应的描述符**。然后用描述符表中的段基址加上逻辑地址（SEL:OFFSET）的OFFSET就可以转换成线性地址，
* 段选择子中的TI值只有一位0或1，0代表选择子是在GDT选择，1代表选择子是在LDT选择。
* 请求特权级（RPL）则代表选择子的特权级，共有4个特权级（0级、1级、2级、3级）。

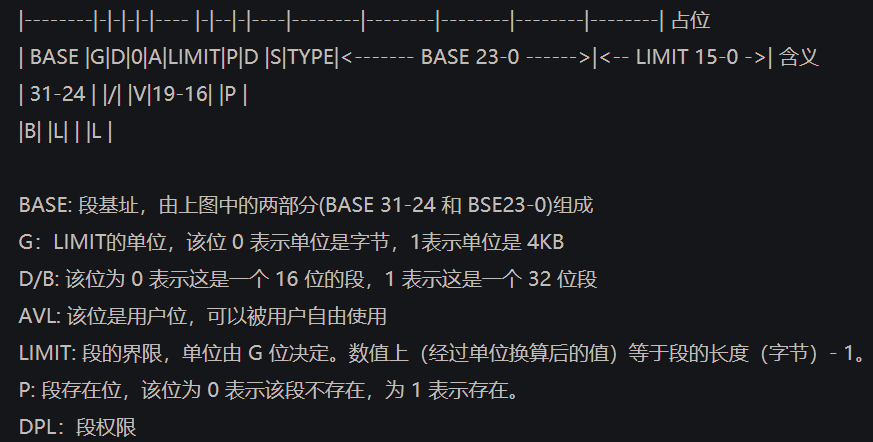
1. 什么是描述符？



段描述符

应该是描述一个段的信息，如段基址、属性等：第5字节类型：数据段、代码段。

**段描述符安装在 GDT 或者 LDT 数组中**



1. 什么是GDT，什么是LDT?



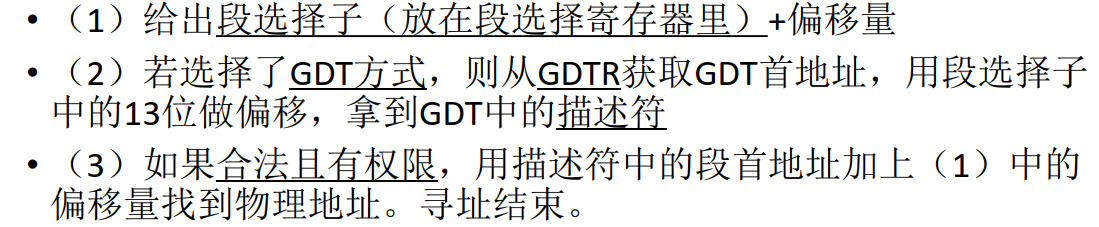
1. 请分别说明GDTR和LDTR的结构。

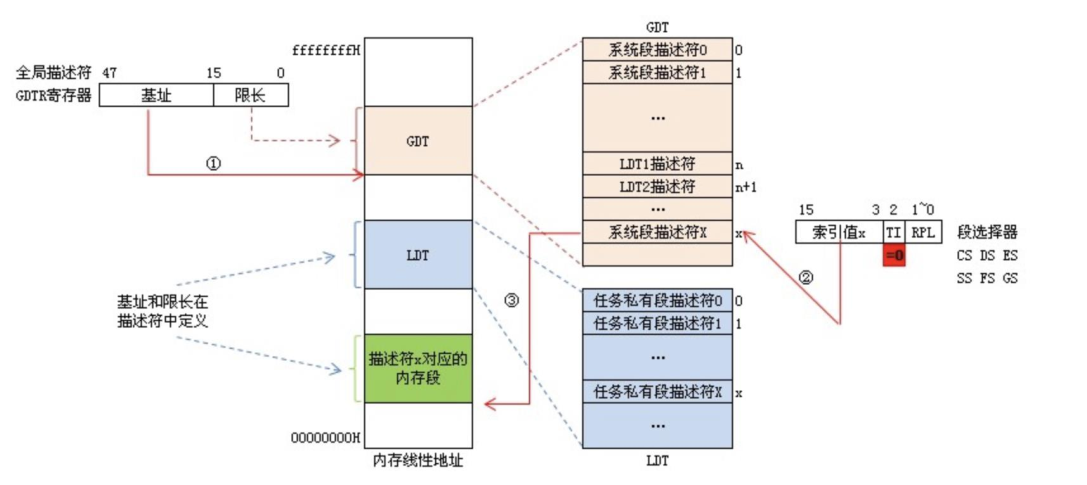
GDTR中存放的是GDT在内存中的基地址和其表长界限。

GDTR：一个寄存器，48位高32地址，低16位长度

LDTR：16位寄存器，存放一个特殊的选择子，用于查找当前进程的LDT首地址

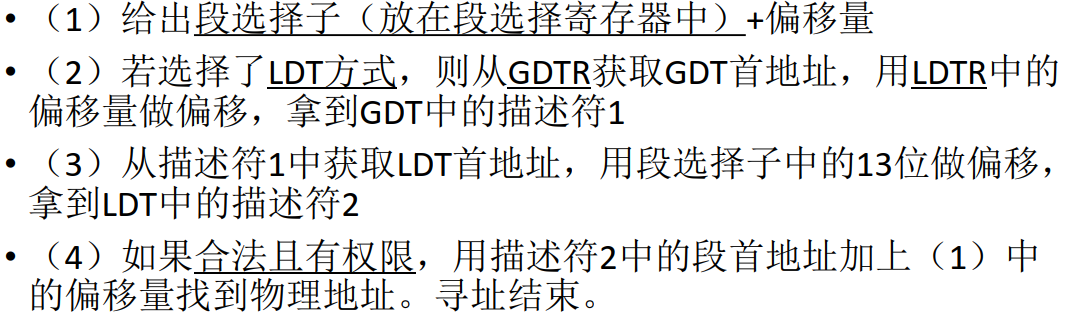
1. 请说明GDT直接查找物理地址的具体步骤。



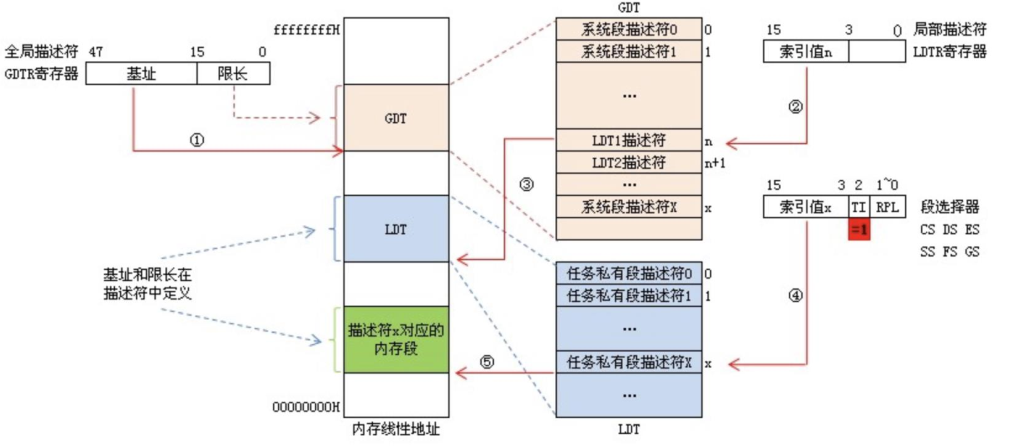




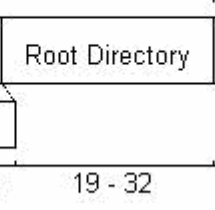
1. 请说明通过LDT查找物理地址的具体步骤。



从GDT拿到的描述符是描述LDT的，拿到其首地址，再用选择子高13位偏移得到真正的描述符L，L+偏移得到物理地址。



1. 根目录区大小一定么？扇区号是多少？为什么？



根目录区：FAT表之后是根目录区，**长度固定**

19-32个扇区，目录表项大小是32位

1. 数据区第一个簇号是多少？为什么？

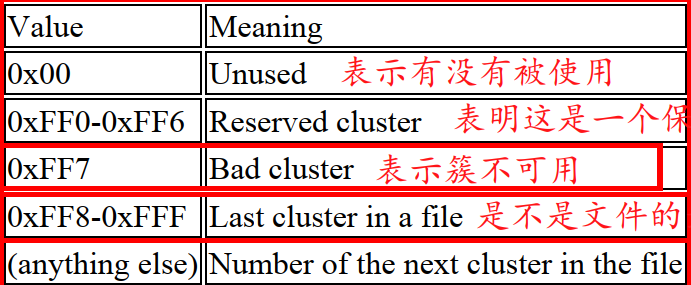
2号，目录项的前3字节被使用，前三字节是固定的：**F0FFFF,** 表示一个**应用在1.44M软盘上的FAT12文件系统**

1. FAT表的作用？

FAT表里面有表项，每个表项12位，每个表项和数据区的一个簇对应，表项序号和簇号也是一一对应的。

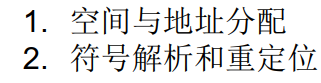
用来寻找簇：

FAT值代表下一个簇号



1. 解释静态链接的过程。

编译阶段直接把静态库加入到可执行文件中去



**静态链接包括两个大部分：一是空间和地址的分配；二是符号解析和重定位**

1. 解释动态链接的过程。

在链接阶段仅仅只加入一些描述信息，而**程序执行时再从系统中把相应动态库加载到内存中去**。



在动态链接程序运行时，除了可执行文件本身，将还有动态链接文件（ELF）与**动态链接器**将被映射到进程的地址空间中，动态链接器被当做普通的共享对象来进行映射，在系统运行可执行文件之前，会将控制权交给动态链接器，由它完成所有的动态链接工作以后再把控制权交给可执行文件。

**Linux的动态链接的实现：**

**1）动态链接器获取自身的符号表和重定位表，以及自身的入口地址**

**（2）将可执行文件和链接器本身的符号表都合并到一个全局符号表中，然后链接器在“.dynamic”段中找到该可执行文件依赖的共享对象，链接器将这些共享对象的名字加入到一个装载集合中**

**3）当所有共享对象加载完毕之后，动态链接器将控制权交回给ELF头中指定的程序入口地址。**

1. 静态链接相关PPT中为什么使用ld链接⽽不是gcc？
2. linux下可执行文件的虚拟地址空间默认从哪里开始分配。

ELF可执行文件默认被加载到内存**0x8048000**这个位置，即从这个位置开始加载。即**从这个位置开始加载。先加载ELF可执行文件的头部信息，再加载代码部分**，但因不同文件头部大小不一样，**第一行代码（即程序的实际入口地址）的位置也会有所不同**

* 实验相关内容

1. BPB指定字段的含义



BPB长度为25字节：

1. 如何进⼊子目录并输出（说明方法调用）

先遍历根目录，拿到一个根目录的目录项，然后解析这个目录项，看第一个逻辑簇的位置在哪里。转到这个逻辑扇区，里面是文件/目录表项

1. 如何获得指定文件的内容，即如何获得数据区的内容（比如使用指针等）

找到文件：

我的是建立一个**文件树**，一开始时遍历整个文件系统得到所有的目录和文件，初始化这个文件树，并且每个文件标有其名字、大小、簇号，

1. 如何进行C代码和汇编之间的参数传递和返回值传递

利用栈，调用函数的时候会将参数压栈，在汇编中取出来即可。

返回值在一个寄存器里面

1. 汇编代码中对I/O的处理方式，说明指定寄存器所存值的含义

汇编颜色：

http://www.tldp.org/HOWTO/Bash-Prompt-HOWTO/x329.html