**1. 什么是实模式，什么是保护模式？**

实模式：基地址+偏移量可以直接获得物理地址的模式

缺点：非常不安全

保护模式：不能直接拿到物理地址

需要进行地址转换

从80286开始，是现代操作系统的主要模式

1. **什么是选择子？**

通过选择子来定位描述符。

是一个2字节的数，最低2位表示RPL（请求特权等级），第三位TI区分LDT和GDT，TI为1时查LDT表。高13位给出描述符的地址。正好足够寻址8K项。

16位地址，段的大小是64KB，每个描述符8个Byte，正好能放8K个描述符。

选择子放在段寄存器中**。**

选择子共16位，放在段选择寄存器里

低2位表示请求特权级

第3位表示选择GDT还是LDT方式

高13位表示在描述符表中的偏移

故描述符表的项数最多是2的13次方

1. **什么是描述符？**

段描述符是GDT和LDT表中的一个数据结构项，用于向处理器提供有关一个段的位置和大小信息以及访问控制的状态信息。

1. **什么是GDT，什么是LDT?**

GDT：全局描述符表，是全局唯一的。

存放一些公用的描述符，和包含各进程局部描述符表首地址的描述符。

LDT：局部描述符表，每个进程都可以有一个。

存放本进程内使用的描述符。

1. **请分别说明GDTR和LDTR的结构。**

GDTR：48位寄存器，高32位放置GDT首地址，低16位放置GDT限长

限长决定了可寻址的大小，注意低16位放的不是选择子

LDTR：16位寄存器，放置一个特殊的选择子，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。**

给出段选择子（放在段选择寄存器里）+ 偏移量

若选择了GDT方式，则从GDTR获取GDT首地址，用段选择子中的13位做偏 移，拿到GDT中的描述符

如果合法且有权限，用描述符中的段首地址加上1.中的偏移量找到物理地址, 寻址结束

1. **请说明通过LDT查找物理地址的具体步骤。**

给出段选择子（放在段选择寄存器中）+ 偏移量

若选择了LDT方式，则从GDTR获取GDT首地址，用LDTR中的偏移量做偏移，拿到GDT中的描述符1

从描述符1中获取LDT首地址，用段选择子中的13位做偏移，拿到LDT中的描述符2

如果合法且有权限，用描述符2中的段首地址加上1.中的偏移量找到物理地址。寻址结束

1. **根目录区大小一定么？扇区号是多少？为什么？**

根目录去长度非固定，需计算。

扇区号19，第一个字节位于偏移19\*512=0x2600处。

（0扇区是引导扇区，1-9放FAT1表，10-18放FAT2表。）

它由若干个目录条目组成，条目最多有BPB\_RootEntnt个，因此其长度大小不固定，依赖于BPB\_RootEntCnt。

1. **数据区第一个簇号是多少？为什么？**

由于FAT表项的序号与簇号一一对应，而FAT表中序号为0和1的表项被设置成了固定值，簇0和簇1就没有存在的意义了，所以数据区起始于簇2.

1. **FAT表的作用？**

FAT表的每一个表项都与数据区中的一个簇相对应，且表项的序号与簇号相对应。

FAT项的值代表文件的下一个簇号，当值>=0xFF8时表示当前簇为本文件的最后一个簇，当值=0xFF7时表示是一个坏簇。

当文件大于512字节时，需要通过FAT表找到所有的簇

1. **解释静态链接的过程。**

空间和地址的分配

重定位和符号解析

**12. 解释动态链接的过程。**

**13. 静态链接相关PPT中为什么使用ld链接⽽不是gcc**

**14. linux下可执行文件的虚拟地址空间默认从哪里开始分配**。

1. BPB指定字段的含义

2. 如何进⼊子目录并输出（说明方法调用）

3. 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）

4. 如何进行C代码和汇编之间的参数传递和返回值传递

5. 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