第13章 保护模式习题

4、sel=0000 0000 1100 1011

5、含义：代码段，已在内存中，包含的是32位指令，该段仅可执行，段基址：01001200H，段限长：FFFFFH。

10、

（1）通过中断门或陷阱门处理中断过程：

根据中断号N，查找IDT，定位到第N项描述符，即为中断门或陷阱门，该门包含选择符X和偏移量Y；

根据选择符X查找GDT/LDT，定位到第X项描述符，即为目标代码段描述符，包含代码段基地址Z和限长L；

由Z+Y得到目标服务程序起始指令地址，即可切换到中断服务程序执行。

（2）通过任务门处理中断过程：

根据中断号N，查找IDT，定位到第N项描述符，即为任务门，该门包含选择符X；

根据选择符X查找GDT，定位到第X项描述符，即为TSS段描述符，包含TSS段基地址Z和限长L；

由Z可访问TSS段，实现任务切换，并取得TSS中的CS值和EIP值，即可定位到目标服务程序起始指令地址，切换到中断服务程序执行。

12、

“CALL r32：偏移量“指令通过任务门实现任务切换的执行过程：

（1）根据r32中的选择符N访问LDT或GDT，定位到N号任务门，该任务门包含选择符X；

（2）根据X访问GDT，定位到第X项描述符，即为TSS段描述符，包含TSS段基地址Z和限长L；

（3）由Z可访问TSS段，实现任务切换，并取得TSS中的CS值和EIP值，即可定位到目标服务程序起始指令地址，切换到中断服务程序执行。