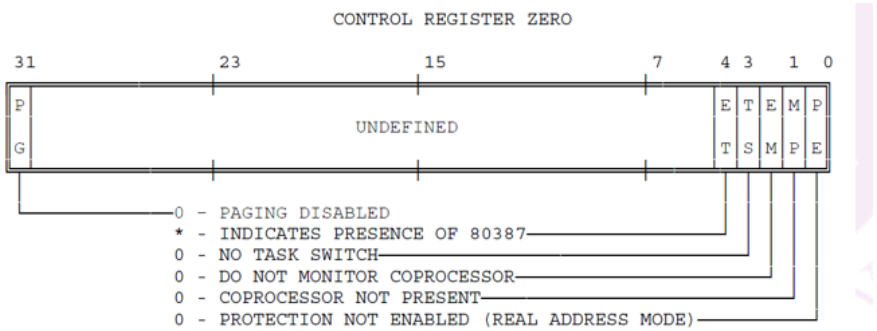
PA3-2 实验报告

191220163 计算机科学与技术系 张木子苗

1. NEMU在什么时候进入了保护模式?

80386的实模式和保护模式由CR0寄存器中的PE位控制。



当PE置为0时，采用实地址模式；当PE置为1时，采用保护地址模式。

在start.S中，我们利用下列语句，将CR0寄存器中的PE位置为1，进入了保护模式

```
# Enable protection
    movl    %cr0, %eax          # %CR0 |= PROTECT_ENABLE_BIT
    orl     $0x1, %eax
    movl    %eax, %cr0
```

2. 在GDTR中保存的段表首地址是虚拟地址、线性地址、还是物理地址？为什么?

线性地址（因为此时还没有开启分页模式，其实也是物理地址);

GDTR 寄存器里面存放的是 GDT 的首地址。lgdt指令的作用是把段表的首地址信息存入GDTR。

这里段表首地址必须是线性地址。因为我们已经开始保护模式，虚拟地址需要经过转换才能成为线性地址；而这个转换需要通过段表；如果在GDTR里面存放虚拟地址，那么“找到段表的前提是找到段表”，显然是一个无限递归，不能得到段表的线性地址。

所以，在GDTR中存放的应该是线性地址。又因为还没有开启分页模式，其实该线性地址也是物理地址。