

PA_3-2 实验报告

计算机科学与技术系 张桓 191220156

1. NEMU 在什么时候进入了保护模式？

答：在 `kernel/start/start.S` 中可以看到，将 `CR0` 寄存器的 `pe` 位从 0 设置为 1，NEMU 就从实地址模式转化为保护模式。相关代码如下：

```
# 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？

答：是线性地址。

因为 `GDTR` 中存放有段表的首地址，在启动保护模式时通过 `lgdt` 命令将段表的首地址给 `GDTR`。开启保护模式后，对于每个逻辑地址必须要依靠段表经过转换后才能得到其线性地址，因此段表首地址必须要以线性地址给出，否则无法确定段表的位置。