

计算机系统基础

实验报告

PA 3

计算机科学与技术系
191220008 陈南瞳

3-2:

1、NEMU 在什么时候进入了保护模式？

NEMU 在刚启动时进入的是实模式。在实模式下，操作系统需要完成初始化段表（如 GDT）和描述符表寄存器（如 GDTR）。在初始化完成后，即当 lgdt 指令把段表的首地址 base 和界限 limit 载入 GDTR 后，操作系统通过将 0 号控制寄存器（CR0）中的 PE 位置为 1 的方式，来通知机器进入保护模式。在此之前，CR0 中的 PE 初始化为 0。

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？

在 GDTR 中保存的段表首地址是线性地址。

lgdt 指令把段表的首地址信息载入 GDTR，在此之后，NEMU 便从实模式进入了保护模式，虚拟地址必须经过转换才能得到线性地址。想要对虚拟地址进行转换，则必须先将各个段寄存器初始化，而初始化过程则需要用到 GDTR 中保存的段表首地址，在保护模式下，GDTR 中保存的地址不能是虚拟地址。同时页目录、页表也未初始化，所以 GDTR 中保存的也不是物理地址。故 GDTR 中保存的是线性地址。