PA 3-2 实验报告

221220085 时昌军

一、实验目的

让NEMU具备现代计算机的内存管理功能。

1、了解逻辑地址，线性地址，物理地址以及段寄存等概念。
2、了解NEMU 的保护模式工作方式。
3、掌握逻辑地址向线性地址转换的方法。

二、实验过程

1. 在`include/config.h`头文件中添加宏定义`IA32_SEG`并`make clean`；
2. 在`CPU_STATE`中添加对`GDTR`、`CR0`的模拟以及在`init_cpu()`中进行初始化为0；
3. 在`CPU_STATE`中添加对6个段寄存器的模拟在`init_cpu()`中进行初始化为0，注意除了要模拟其16位的可见部分，还要模拟其隐藏部分，顺序不能有错；
4. 实现包括`lgdt`、针对控制寄存器和段寄存器的特殊`mov`以及`ljmp`指令；
5. 实现`segment_translate()`、`loag_sreg()`函数，并在`vaddr_read()`和`vaddr_write()`函数中添加保护模式下的虚拟地址向线性地址转换的过程；
6. 通过`make test_pa-3-2`执行并通过各测试用例。

三、思考题

1. NEMU在什么时候进入了保护模式?

答：初始化完成后，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。

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：在GDTR中保存的段表首地址是线性地址。

linear address = base address + offset，若保存的是虚拟地址，则虚拟地址转成线性地址需要存在GDT中的base address,在未转换成功之前是无法根据GDTR访问GDT的，就互相矛盾了。

若不开启分页，则线性地址等于物理地址，若开启分页，除了 cr3 都需要进行线性地址到物理地址的转换，此时线性地址不等于物理地址。而在取 GDTR 的首地址来访问GDT 的过程中，就会进行线性地址向物理地址的转换，此时如果保存的是物理地址，则物理地址转换后出错；若保存的是线性地址，则不会出错。线性地址确保在分页和不分页下均能正确访问GDT。