1. NEMU 在什么时候进入了保护模式？

答：

```
start:
#ifdef IA32_INTR
        cli
#endif
        lgdt    va_to_pa(gdtdesc) # See i386 manual for more information
        movl    %cr0, %eax        # %CR0 |= PROTECT_ENABLE_BIT
        orl     $0x1, %eax
        movl    %eax, %cr0
```

在 start.S 中的这一段代码，将 cr0 放到 eax 中，将 eax 与 0x1 与一下，再传给 cr0，相当于将 cr0 的最低的一位置为 1，即将 pe 置为 1，此时便开启了保护模式。

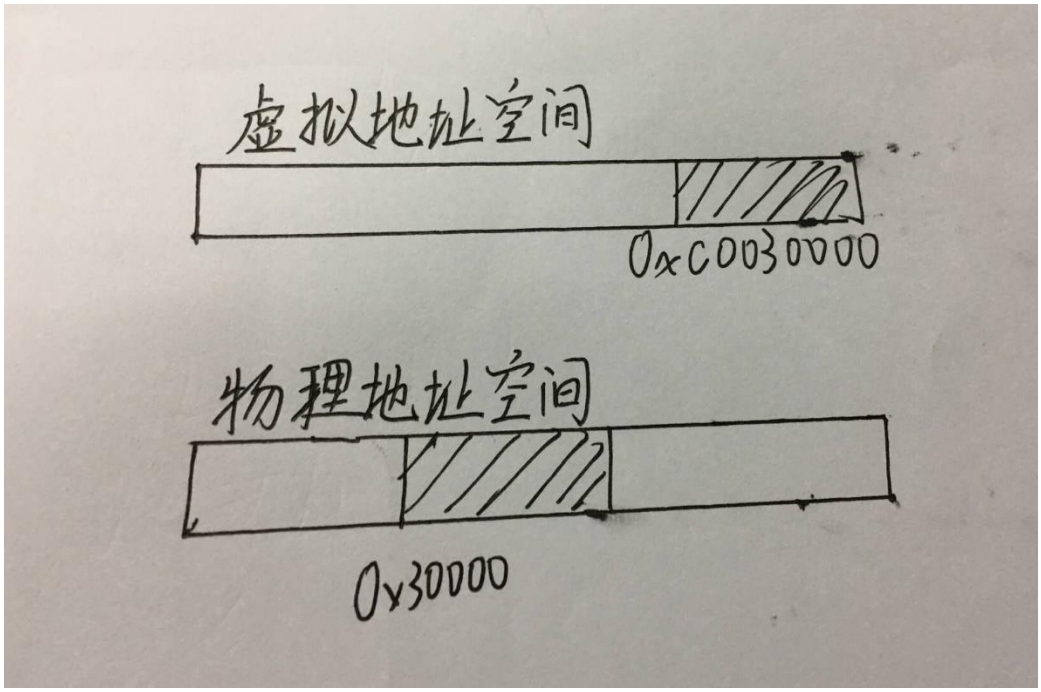
2. 在 GDTR 中保存的段表首地址是虚拟地址、线性地址、还是物理地址？为什么？

答：

是线性地址。段级地址转换的目的是将虚拟地址转换为线性地址，如果段表首地址是虚拟地址，那么这个地址便无法转换为线性地址。如果段表首地址是物理地址，那么分页之前，没有物理地址，是把线性地址直接当做物理地址用的，因此也不是物理地址。因此，只能是线性地址。

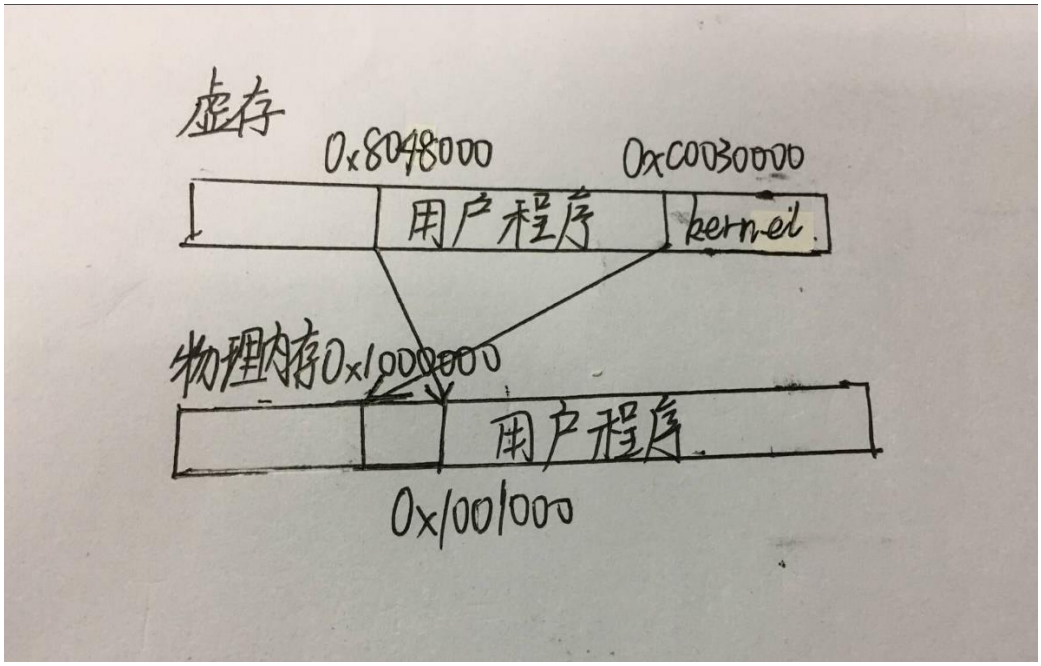
3、Kernel 的虚拟页和物理页的映射关系是什么？请画图说明；

答：



4、以某一个测试用例为例，画图说明用户进程的虚拟页和物理页间映射关系又是怎样的？Kernel 映射为哪一段？你可以在 loader()中通过 Log()输出 mm_malloc 的结果来查看映射关系，并结合 init_mm()中的代码绘出内核映射关系

答：



5、“在 Kernel 完成页表初始化前，程序无法访问全局变量”这一表述是否正确？在init_page()里面我们对全局变量进行了怎样的处理？

答：正确。要先将全局变量的虚拟地址转化为物理地址，在 kernel 完成页表初始化之后才能在物理内存中找到。