gdt最大为多少 由谁决定？段选择子中[描述符索引]那部分 共13位 2^13 \* 2^3 = 2^16 = 64KB

所以这里段表设置为这个最大容量

段表项基本内容：

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 低32 | 31 | 段基地址15~0 | | | | | | | | | | | | | | 16 | 15 | 段界限15~0 | | | | | | | | | | | | | | 0 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 高32 | 段基地址31~24 | | | | | | | | 粒度 | 32 | 64 | 空位 | 段偏移界限 | | | | 存在 | 特权等级 | | 系统 | 段权限 | | | | 段基地址23~16 | | | | | | | |
|  |  |  |  |  |  |  |  |  | 1 | 0 | 0 |  |  |  |  |  |  |  | Yes0 |  |  |  |  |  |  |  |  |  |  |  |  |

保护模式下设置了7个描述符 占用0x7e00~0x7e37 OS中添加新的段表项至少从0x7e38开始

中断描述符表寄存器

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 32位基地址 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | 16位偏移界限 | | | | | | | | | | | | | | | | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |

中断表项基本内容（保护模式下）(调用门也长这样)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 低32 | 31 | 目标代码段描述符选择子 | | | | | | | | | | | | | | 16 | 15 | 中断处理程序的偏移值-低16bit | | | | | | | | | | | | | | 0 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 高32 | 中断处理程序的偏移值高-16bit | | | | | | | | | | | | | | | | 存在 | 特权等级 | | ？ | | | | | ？ | | | 不使用 | | | | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 1 |  |  | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |  |  |  |  |  |

中断表放在全局段表的后面：

中断号有256个 2^8 \* 2^3 = 2^11 = 0x800

0x17E00 + 0x800 = 0x18600

故界限在00x185ff

INTERUPT\_GATE\_DESCRIPTOR{

//从低到高

short 偏移值低16

short 中断程序所在段的选择子（查看引导程序）（0x20）

char dw\_count//什么意思呢 反正是00000000

char 权限 //1000偏移值>>16) & 0x1111

dw\_count = ar低八位

权限 = ar高八位

选择子

}

安装周期性时钟的中断：

set\_intgatedesc（中断表地址 + 周期性时钟中断的终端号，0x20，汇编函数标号[可以起名为refreshtime之类的 或者也可以使用中断号]）

8259芯片的丛片的IR0连接含RTC芯片

含RTC芯片由两部分组成：静态存储模块+RTC电路

哪部分保护现场是硬件默认的？IRETD?

观察0x18180 处的中断门

<bochs:2> xp/2 0x18180

[bochs]:

0x0000000000018180 <bogus+ 0>: 0x0030014b 0x0010008e

翻译回中断门 换算出内存0x0010014b处 中断处理程序

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 低32 | 31 | 目标代码段描述符选择子 | | | | | | | | | | | | | | 16 | 15 | 中断处理程序的偏移值-低16bit | | | | | | | | | | | | | | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| 高32 | 中断处理程序的偏移值高-16bit | | | | | | | | | | | | | | | | 存在 | 特权等级 | | ？ | | | | | ？ | | | 不使用 | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |

objdump 查看中断处理程序的机器码 和中断门指向的内存内容做对比 发现一致

查看中断没有收到的原因