|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 武汉大学国家网络安全学院教学实验报告 | | | | | |
| 课程名称 | 操作系统设计与实践 | | 实验日期 | |  |
| 实验名称 |  | | 实验周次 | |  |
| 姓名 | 学号 | | 专业 | | 班级 |
| 王卓 | 2021302191791 | | 网络空间安全 | | 9班 |
|  |  | |  | |  |
|  |  | |  | |  |
|  |  | |  | |  |
| 1. 实验目的及实验内容   （本次实验所涉及并要求掌握的知识；实验内容；必要的原理分析） | | | | | |
| **实验知识要求：**  **实验内容：**   * 1. **本次实验内容：**  1. 学习中断与异常的机制 2. 调试8259A的编程基本例程 3. 调试时钟中断例程 4. 实现一个自定义的中断向量，功能可自由设想    1. **思考问题：** 5. 什么是中断，什么是异常 6. 8259A的工作原理是怎么样的？怎么给这些中断号的处理向量初始化值 7. 如何建立IDT，如何实现一个自定义的中断 8. 如何控制时钟中断，为什么时钟中断的时候，没有看到int的指令？ 9. 简要解释一下IOPL的作用与基本机理   **原理分析：** | | | | | |
| 1. 实验环境及实验步骤   （本次实验所使用的器件、仪器设备等的情况；具体的实验步骤） | | | | | |
| * 1. **实验环境**   ·虚拟机：VMware Workstation Pro/VMware Workstation 16 player  ·操作系统：Ubuntu 16.04  ·模拟系统软件：Bochs 2.7   * 1. **具体实验步骤**      1. **学习中断与异常的机制**         1. 中断和异常的概念   中断和异常都是软件或者硬件发生了某种情形而通知处理器的行为，都是程序执行过程中的强制性转移，转移到相应的处理程序。每一种中断都对应一个中断向量号，这个向量号通过IDT与对应的中断程序对应起来。    **图\* 中断向量到中断处理程序的对应过程**   * + - * 1. 中断   这里的中断指的是外部中断。中断的引入是为了支持CPU和设备之间的并行操作。中断可以分为可屏蔽中断和不可屏蔽中断。   * 可屏蔽中断：指通过可屏蔽中断请求线INTR向CPU发出中断请求，CPU可以通过在中断控制器中设置响应的屏蔽字来屏蔽他或不屏蔽他，被屏蔽的中断请求将不被送至CPU。 * 不可屏蔽中断：指通过专门的不可屏蔽请求线NMI向CPU发出的中断请求，通常是非常紧急的硬件故障。   注：外部中断是异步的，意思是所有中断来的信号都是记录在中断寄存器中的，当CPU执行完一道指令后，如果是开中断状态，就会检查中断寄存器中有没有中断，如果有中断，就会选择一个中断优先级比较高的中断先处理，等到处理完之后再继续执行；如果是关中断，则不会检查，而直接执行下一条指令。   * + - * 1. 异常   异常也叫内部中断，它不需要硬件支持。异常的引入表示 CPU 执行指令时本身出现的问题。异常可分为以下三种类型：   * Fault：一种可以可以被更正的异常。而且一旦被更正，程序可以不失连续性地继续执行。当一个 fault 发生，处理器会把产生 fault 指令之前的状态保存起来，异常处理程序的返回地址将会是产生 fault 的指令，而不是其后的那条指令。 * Trap：是一种在发生 trap 的指令执行之后立即被报告的异常，它也允许程序或任务不失连续性地继续执行。异常处理程序的返回地址将会是产生 trap 的指令之后的那条指令。 * Abort：是一种不总是报告准确异常发生位置的异常，它不允许程序或者任务继续执行，而是用来报告严重错误的。   注：异常是同步的，这是指异常发生的时候，CPU立即处理本次异常，直到异常处理结束后才能继续进行接下来的任务。   * + - 1. 处理机制          1. 实模式下的中断处理   实模式下，中断转移方法与8086相同，即通过中断向量号直接去中断向量表中找到中断处理程序入口，然后跳转到指定位置执行中断处理程序。  实模式处理  **图\* 实模式中断处理**   * + - * 1. 保护模式下的中断处理   不同于实模式，在保护模式下，中断向量表被IDT代替。IDT的作用是将每一个中断向量和一个描述符对应起来。IDT的描述符有三类：中断门描述符、陷阱门描述符、任务门描述符。   * 中断门和陷阱门  1. 结构   中断门结构  **图\* 中断门和陷阱门结构**  其中灰色部分表示保留，不使用。其中段选择码和偏移用来定位中断处理程序，其余标志该描述符的属性。   1. 处理机制   任务门  **图\* 中断门和陷阱门处理机制**  注意：中断门和陷阱门的区别是对中断允许标志IF位的影响。中断门向量引起中断时会复位IF，此时其他中断干扰会被屏蔽，最终通过iret从堆栈上恢复出IF的原值。   * 任务门  1. 结构   任务门结构  **图\* 任务门结构**  同样，灰色部分表示空闲不使用。任务门不需要提供段内偏移，因为任务门不指向某一个子程序的入口，TSS本身是作为一个段来对待的。   1. 处理机制   任务门  **图\* 任务门处理机制**   * + 1. **调试8259A的编程基本例程**     2. **调试时钟中断例程**     3. **实现一个自定义的中断向量，功能自定** | | | | | |
| 1. 实验过程分析   （实验分工，详细记录实验过程中发生的故障和问题，进行故障分析，说明故障排除的过程及方法。根据具体实验，记录、整理相应的数据表格等） | | | | | |
|  | | | | | |
| 1. 实验结果总结   （对实验结果进行分析，完成思考题目，并提出实验的改进意见） | | | | | |
| * 1. **思考题**      1. **什么是中断，什么是异常**   中断和异常都是程序执行过程中的强制性转移，转移到相应的处理程序。  中断是CPU暂停当前工作，有计划地去处理其他的事情，它的发生一般是可以预知的，处理的过程也是事先制定好的，处理中断时程序是正常运行的；  异常是CPU遇到了无法响应的工作，而后进入一种非正常状态，异常的出现表明程序有缺陷。  每一种中断（异常）都会对应一个中断向量号，而这个向量号通过IDT就与相应的中断处理程序对应起来。   * + 1. **8259A的工作原理是怎么样的？怎么给这些中断号的处理向量初始化值**     2. **如何建立IDT，如何实现一个自定义的中断**     3. **如何控制时钟中断，为什么时钟中断时候，没有看到int的指令**     4. **简要解释一下IOPL的作用与基本原理** * IOPL的作用   IOPL是I/O保护机制的关键之一，位于寄存器eflags的12、13位。  IOPL  **图\* eflags结构**  指令in、ins、out、outs、cli、sti只有在CPL≤IOPL的时候才能执行。前面说的指令被称为I/O敏感指令，如果低特权级的指令试图访问这些I/O敏感指令将会导致常规保护错误（#GP）   * IOPL的基本原理   处理器不限制0特权级程序的I/O访问，它总是允许的。但是，可以限制低特权级程序的I/O访问权限。这是很重要的，操作系统的功能之一是设备管理，它可能不希望应用程序拥有私自访问外设的能力。  可以改变IOPL的指令只有popf和iretd，但只有运行在ring0的程序才能将其改变。运行在低特权级下的程序无法改变IOPL，不过，如果试图那样做的话并不会产生任何异常，只是IOPL不会改变，仍然保持原样。  另一个与I/O操作特权级有关的概念是I/O位图。I/O位图基址是一个以TSS 的地址为基址的偏移，指向的便是I/O许可位图。之所以叫做位图，是因为它的每一位表示一个字节的端口地址是否可用。如果某一位为0，则表示此位对应的端口号可用，为1则不可用。由于每一个任务都可以有单独的TSS，所以每一个任务可以有它单独的I/O许可位图。  I/O位图与IOPL是或的关系，即只用满足一个条件即可。   |  |  |  | | --- | --- | --- | | 指令 | 功能 | 条件 | | cli | 清除IF位 | CPL≤IOPL | | sti | 设置IF位 | CPL≤IOPL | | in | 从I/O读数据 | CPL≤IOPL或I/O位图许可 | | ins | 从I/O读字符串 | CPL≤IOPL或I/O位图许可 | | out | 向I/O写数据 | CPL≤IOPL或I/O位图许可 | | outs | 向I/O写字符串 | CPL≤IOPL或I/O位图许可 |  * 1. **实验改进意见**      1. **王卓**  1. 提供更详细的实验指导：在每个实验步骤中， 提供更详细的指导和说明， 比如预期结果等，这样能帮助我们更好地完成实验。 2. 介绍实验目的和背景：实验开始之前提供实验的目的和背景，解释一下为什么需要进行该实验以及其与操作系统的关系，这能帮助我们更好理解实验的意义和重要性。    * 1. **xxx** | | | | | |
| 1. 各人实验贡献与体会（每人各自撰写） | | | | | |
| * 1. **王卓**      1. **分工**   在本次实验中， 本人完成大部分实验内容， 负责实验内容的第1题、思考题的第1题和第5题的实验报告撰写。   * + 1. **心得体会**   本次实验主要研究保护模式下异常与中断处理机制，整体来说，实验不算过于难。通过对pmtest9a.asm的调试，我掌握了IDT的建立以及保护模式下的中断调用；通过对pmtest9.asm的调试，我知悉了时钟中断的触发机理。除此之外，通过阅读教材，我也掌握了8259A、IDT、中断门的概念及它们在中断处理中的作用、IOPL的作用与运行原理，并最后自己编写了一个中断处理函数。  总的来说，此次实验让我对中断异常的机制和其各种相关知识都有了一定程度的理解和自我的掌握，也进一步锻炼了我的汇编代码的编写。 | | | | | |
| 1. 教师评语 | | | | | |
|  | | | | | |
| **教师评分（请填写好姓名、学号）** | | | | | |
| 姓名 | | 学号 | | 分数 | |
|  | |  | |  | |
|  | |  | |  | |
|  | |  | |  | |
|  | |  | |  | |
| 教师签名：  年 月 日 | | | | | |