

操作系统及安全设计

《操作系统及安全》配套实验
信安系操作系统课程组
2019年11月

1




操作系统设计实验系列（三） 认识保护模式（三）



武汉大学


2

2



一、实验目标


- 理解中断与异常机制的实现机理
- 对应章节：第三章3.4节,3.5节



武汉大学


3

3



二、本次实验内容

1. 理解中断与异常的机制
2. 调试8259A的编程基本例程
3. 调试时钟中断例程
4. 建立IDT，实现一个自定义的中断，功能可自定义，如特定键盘组合触发某个动作、电子钟、自己游走的字符显示、蜂鸣器等
5. 了解IOPL的作用



武汉大学

4

4



三、完成本次实验要回答的问题

- 1.什么是中断，什么是异常
- 2.8259A的工作原理是怎样的？
- 3.如何建立IDT，如何实现一个自定义的中断
- 4.如何控制时钟中断
- 5.IOPL的作用与基本机理



武汉大学

5

5



四、需了解的知识

1.为什么要IDT

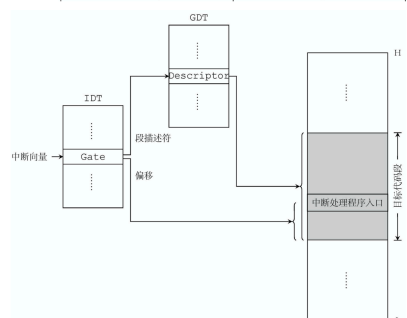
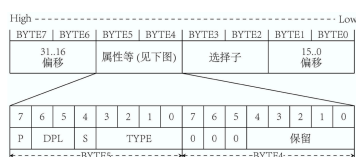
- 实模式：BIOS中断
- 保护模式：IDT机制

2.IDT描述项分类

- 中断门描述符
- 陷阱门描述符
- 任务门描述符

3.IDT的作用与基本流程

- 关联中断向量和描述符



武汉大学

6

6



四、需了解的知识

4.回顾什么是中断和异常

- 同步中断
- 异步中断
- Fault、Trap、Abort的区别

向量号	助记符	描述	类型	出错码	源
0	#DE	除法错	Fault	无	DIV 和 IDIV 指令
1	#DB	调试异常	Fault/Trap	无	任何代码和数据访问
2	---	非屏蔽中断	Interrupt	无	非屏蔽外部中断
3	#BP	调试断点	Trap	无	指令 INT 3
4	#CP	溢出	Trap	无	指令 INCB
5	#RK	越界	Fault	无	指令 BOUND
6	#UD	无效 (未定义的) 操作码	Fault	无	指令 UD2 或者无效指令
7	#NM	设备不可用 (无数学协处理器)	Fault	无	浮点或 WAIT/FWAIT 指令
8	#PF	双重错误	Abort	有 (0)	所有能产生异常或 NMII 或 INTR 的指令
9	---	协处理器段越界 (保留)	Fault	无	浮点指令 C86 之后的 (ASX 处理器不产生此种异常)
10	#TS	无效 TSS	Fault	有	任务切换或访问 TSS 时
11	#NP	段不存在	Fault	有	加载段寄存器或访问系
12	#SS	堆栈段错误	Fault	有	堆栈操作或加载 SS 时
13	#CD	特权保护错误	Fault	有	内存或其他保护校验
14	#PF	页错误	Fault	有	内存访问
15	---	Intel 保留, 未使用			
16	#MF	x87FPU 浮点错 (数字错)	Fault	无	x87FPU 浮点指令或 WAIT/FWAIT 指令
17	#AC	对齐校验	Fault	有 (0)	内存中的数据访问 (486 开始支持)
18	#MC	Machine Check	Abort	无	错误码 (如果有) 和依赖于具体模式 (奔腾 CPU 开始支持)
19	#XF	SIMD 浮点异常	Fault	无	SSR 和 SIMD 浮点指令 (奔腾 3 开始支持)
20~23	---	Intel 保留, 未使用			
24~255	---	用户定义中断	Interrupt		外部中断或 int n 指令



武汉大学

7



四、需了解的知识

5.外部中断



非屏蔽中断

CPU

INT

INTR

主 8295A

从 8295A

- IRQ0 时钟
- IRQ1 键盘
- IRQ2 串行 2
- IRQ3 串行 1
- IRQ5 LPT2
- IRQ6 软盘
- IRQ7 LPT1
- IRQ8 实时时钟
- IRQ9 重定向 IRQ2
- IRQ10 保留
- IRQ11 保留
- IRQ12 PS/2 鼠标
- IRQ13 FPU 异常
- IRQ14 AT 温盘
- IRQ15 保留



武汉大学

8

4



四、需了解的知识

5. 外部中断

- 8259A的编程方式
- 主8259A的端口地址20h, 21h; 从端口A0h, A1h
- 指令格式
 - ICW, 初始化命令字, ICW1—ICW4, 描述详见P92
 - OCW, 操作控制字, OCW1-OCW3
- 编程顺序, **注意不能颠倒!**
 - 向20h或者A0h, 写入ICW1, 主从一致
 - 向21h或者A1h, 写入ICW2, 主从一致
 - 向21h或者A1h, 写入ICW3, 主从不同
 - 向21h或者A1h, 写入ICW4, 主从一致
 - OCW1, 屏蔽中断; OCW2:EOI
- 汇编编程tips:
 - out 端口号, 寄存器
 - 向该端口写入, 对CPU相当于输出。



武汉大学

9

9



谢 谢!



武汉大学

10

10