



LunaixOS

从零开始

自制操作系统

O Brave New Kernel

再论中断：外中断与 APIC

EP 8-1

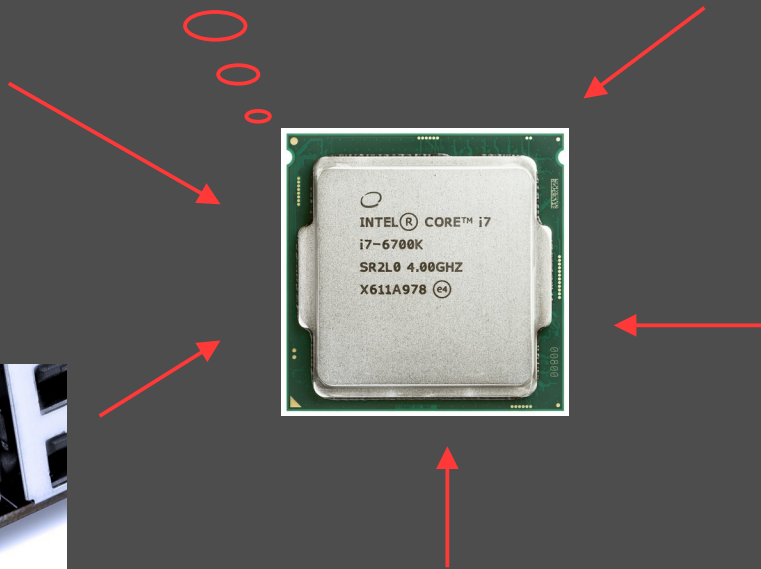
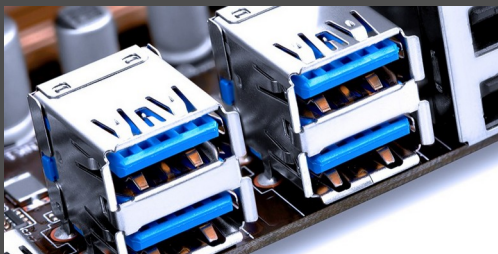
[illegible]



外中断 - CPU 的噩梦



等等外部设备……





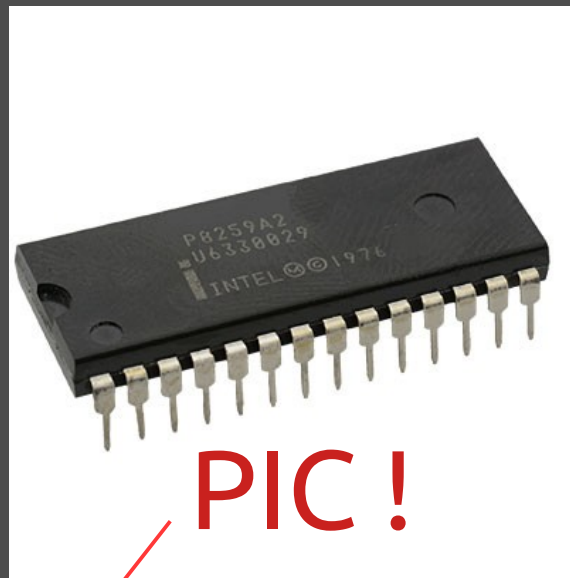
那么，给 CPU 配个秘书吧？

决定 CPU 接下来要处理的中断

帮助 CPU 缓存未处理的中断

拓展 CPU 的中断 Pin

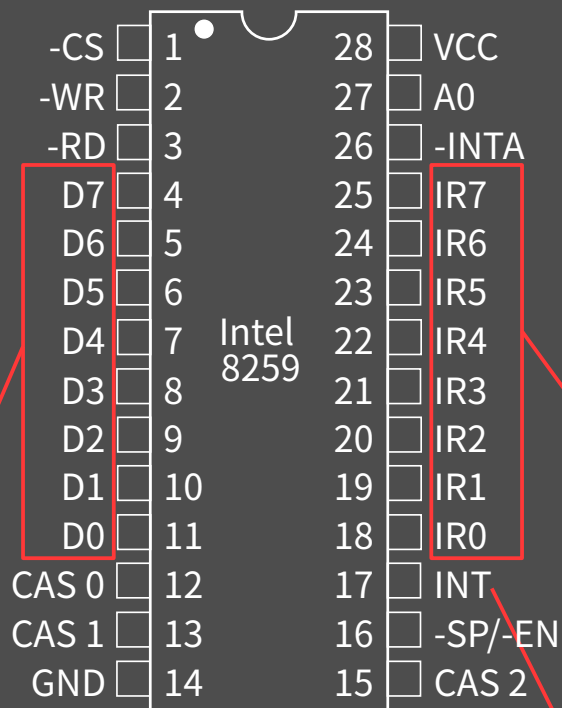
Well, You might guess....



PIC !

可编程中断控制器

(**P**rogrammable Interrupt **C**ontroller)



告诉 CPU 是
几号中断

告诉 CPU 有
中断

外部设备中断

Level	Function
MicroProcessor NMI	Parity or I/O Channel Check
Interrupt Controllers CTLR 1 CTLR 2	
IRQ 0	Timer Output 0
IRQ 1	Keyboard (Output Buffer Full)
IRQ 2	Interrupt from CTLR 2
	Realtime Clock Interrupt
IRQ 8	Software Redirected to INT 0AH (IRQ 2)
IRQ 9	Reserved
IRQ 10	Reserved
IRQ 11	Reserved
IRQ 12	Reserved
IRQ 13	Coprocessor
IRQ 14	Fixed Disk Controller
IRQ 15	Reserved
IRQ 3	Serial Port 2
IRQ 4	Serial Port 1
IRQ 5	Parallel Port 2
IRQ 6	Diskette Controller
IRQ 7	Parallel Port 1

IBM PC/AT

自定义 硬件中断号 → CPU 中断向量的映射



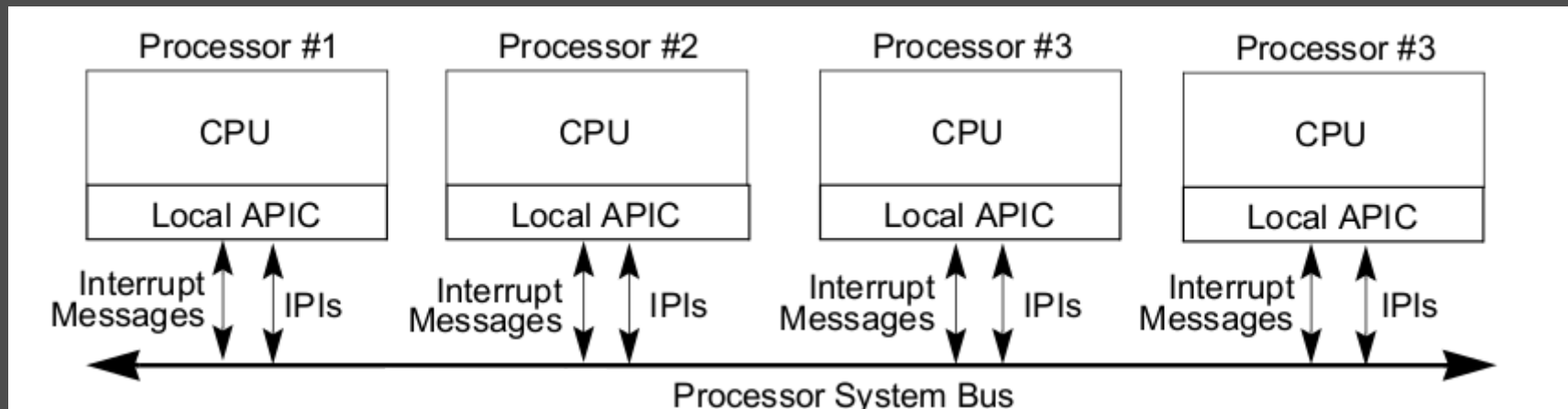
APIC !

高级可编程中断控制器

PIC 继任者，更加的现代！

为多核心处理器打造。

为单个核心指定不同的中断优先级



人人有份，私密独享

本地向量表（Local Vector Table）：
一组 APIC 内置寄存器，定义 **APIC**
本地中断至 CPU 中断向量号的映射

APIC 本地中断：

CMC

APIC 计时器

Thermal Monitor

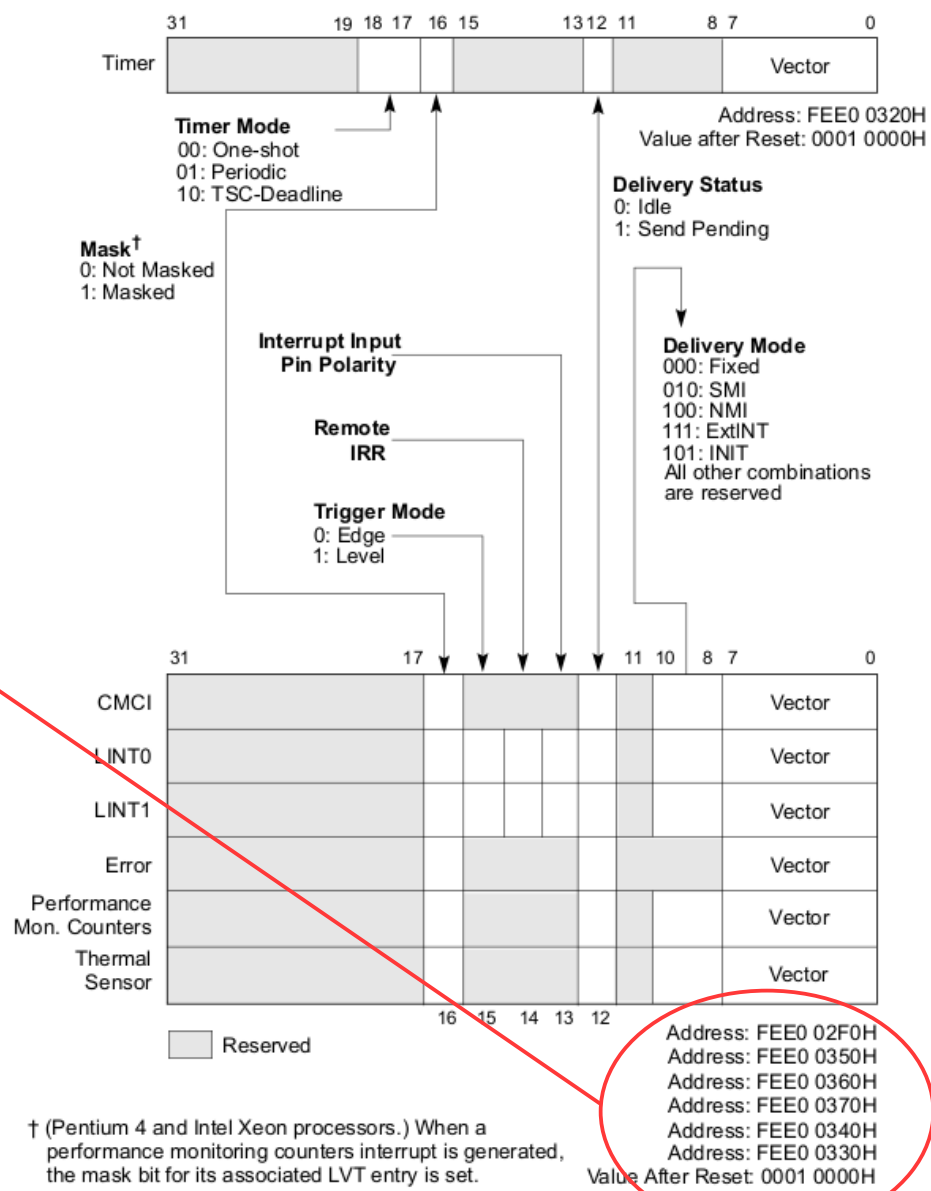
Performance Counter

LINT0 & LINT1

APIC Error

内存映射的 I/O
(MMIO)

不需要 in, out , 平常的
内存读写就可以操控这
些寄存器了！





等等，好像漏了点什么？

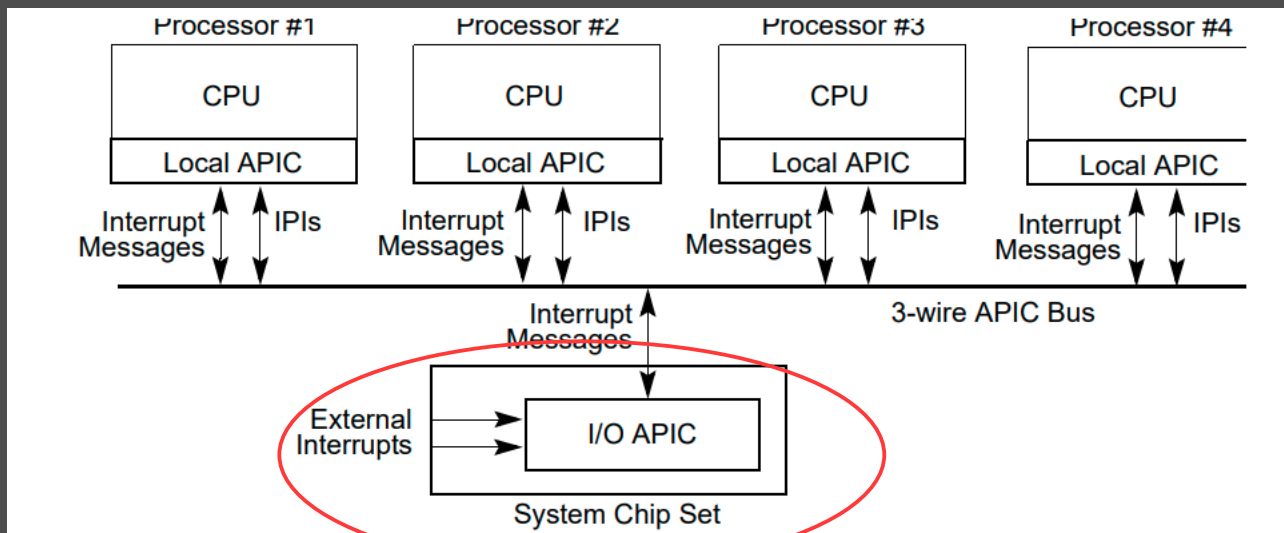
我们的 IR0-7 去哪里了？外部设备的中断们该怎么办？我们怎么映射 IRQ 们？

I/O APIC !

一个拆分出来的 APIC，专用于处理外部设备的中断



I/O APIC 与 Local APIC (LAPIC)



进阶版的 PIC，专职于服务外部中断事件

允许多个 IOAPIC 联级

单个多达 24 个 IRQ！



LunaixOS 将按照以下步骤初始化 APIC

- #0. 禁用中断 (cli)
- #1. 禁用 8259 PIC
- #2. 硬启用 LAPIC
- #3. 初始化 LAPIC
 - #3.1 设置中断优先级
 - #3.2 初始化 LVT
- #4. 软启用 LAPIC
- #5. 初始化 I/O APIC
 - #5.1 映射 IRQ 至自定义的中断号
- #6. 打开中断 (sti)
- #7. Let's party !!

注意：我们只考虑单核情况



使用 APIC 之一：硬启用 Local APIC

从硬件层面上启用 Local APIC

型号相关寄存器 (MSR)，用于操控某些型号相关的功能

一个特殊的寄存器：IA32_APIC_BASE

一旦启用后关闭，不得再次打开！

```
movl $0x1B, %ecx
rdmsr
orl $0x800, %eax
wmsr
```

- When IA32_APIC_BASE[11] is set to 0, processor APICs based on the 3-wire APIC bus cannot be generally re-enabled until a system hardware reset. The 3-wire bus loses track of arbitration that would be necessary for complete re-enabling. Certain APIC functionality can be enabled (for example: performance and thermal monitoring interrupt generation).

Operation `rdmsr`

EDX:EAX := MSR[ECX];

Operation `wrmsr`

MSR[ECX] := EDX:EAX;

1BH	27	IA32_APIC_BASE (APIC_BASE)	This register holds the APIC base address, permitting the relocation of the APIC memory map. See Section 10.4.4, "Local APIC Status and Location" and Section 10.4.5, "Relocating the Local APIC Registers".
	7:0		Reserved
	8		BSP flag (R/W)
	9		Reserved
	10		Enable x2APIC mode.
	11		APIC Global Enable (R/W)
	(MAXPHYADDR - 1):12		APIC Base (R/W)
	63: MAXPHYADDR		Reserved



使用 APIC 之二：禁用 8259 PIC

```
movb $0xff, %al  
outb %al, $0xa1  
outb %al, $0x21
```

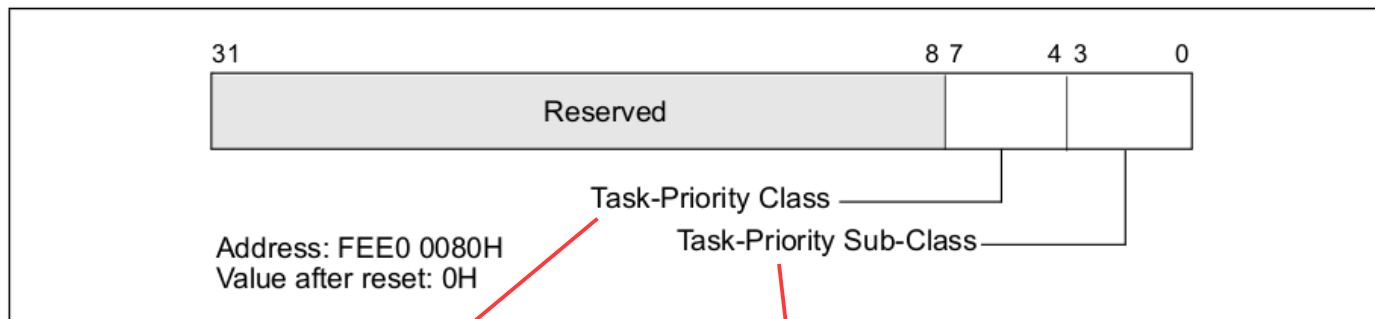
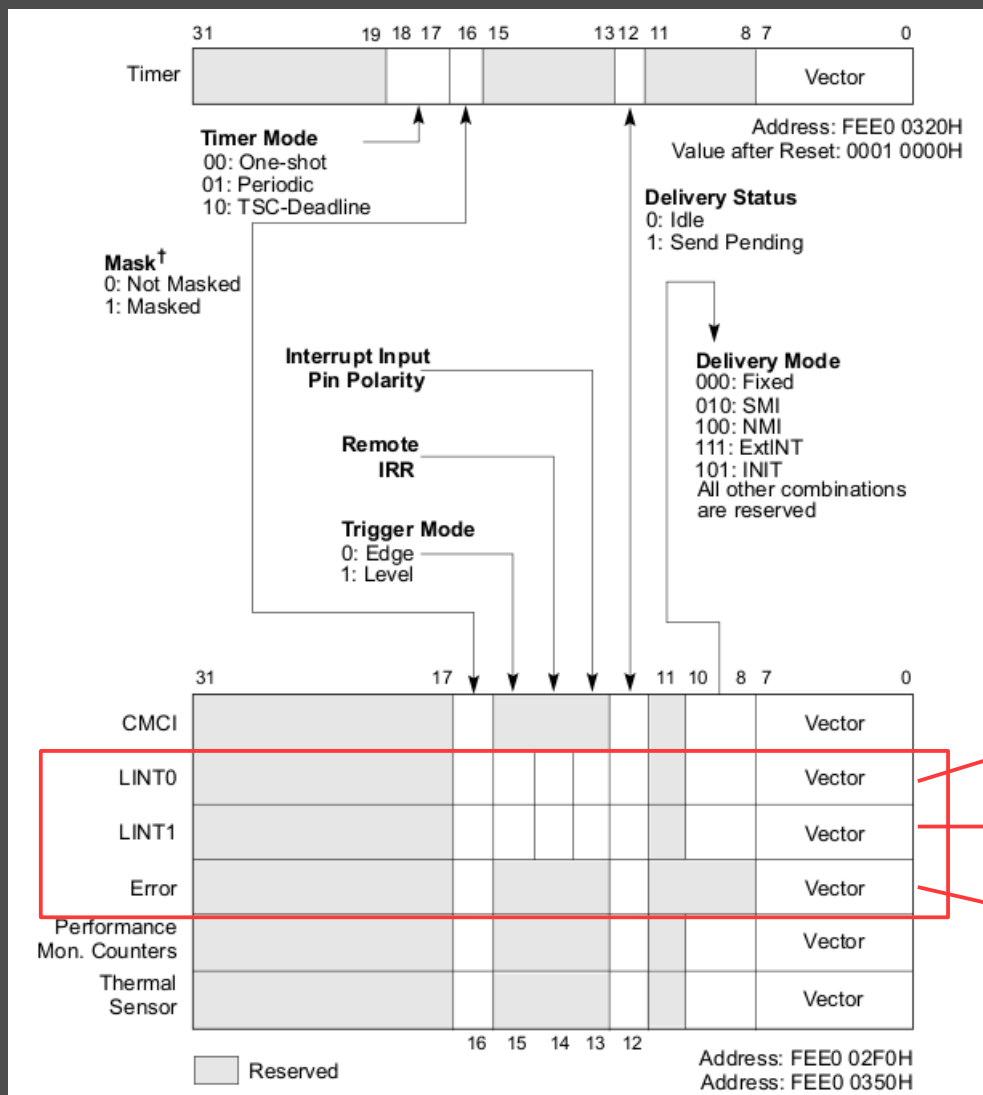


Figure 10-18. Task-Priority Register (TPR)

256 个向量，分 16 个组

每组 16 个

只放行中断号为 $\geq 16 * TC + TSC$ 的中断



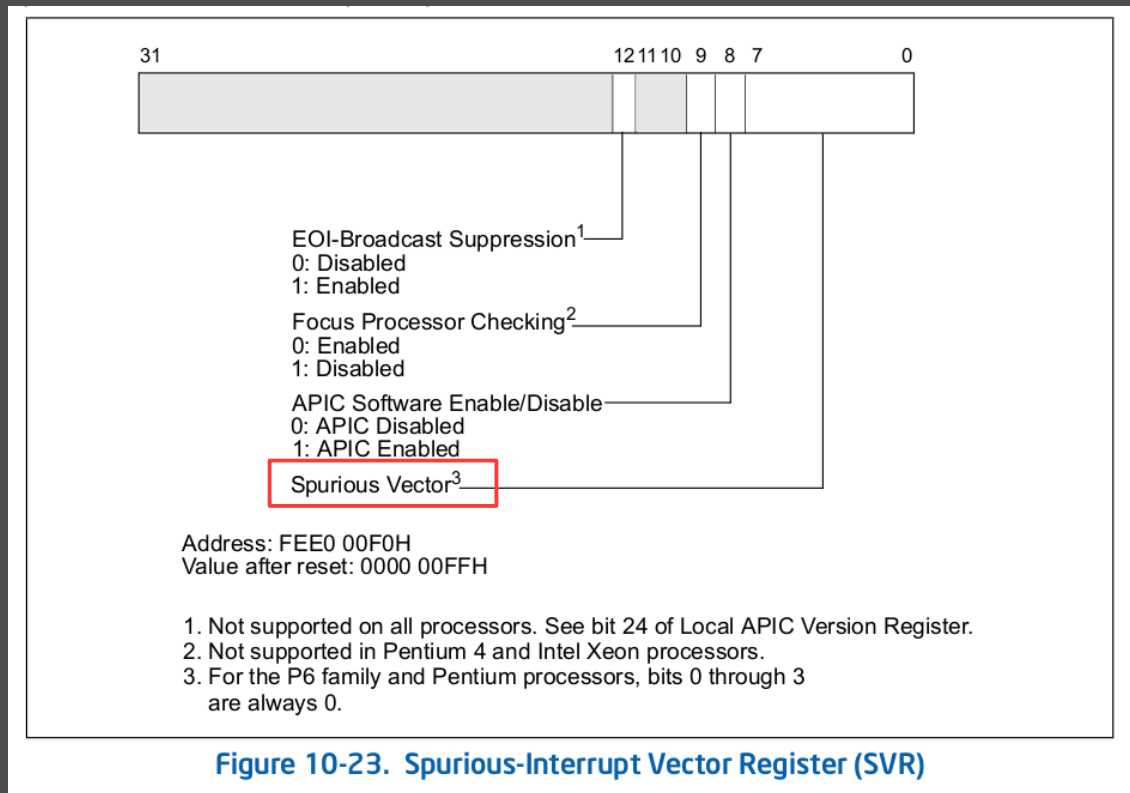
Fixed (#201)

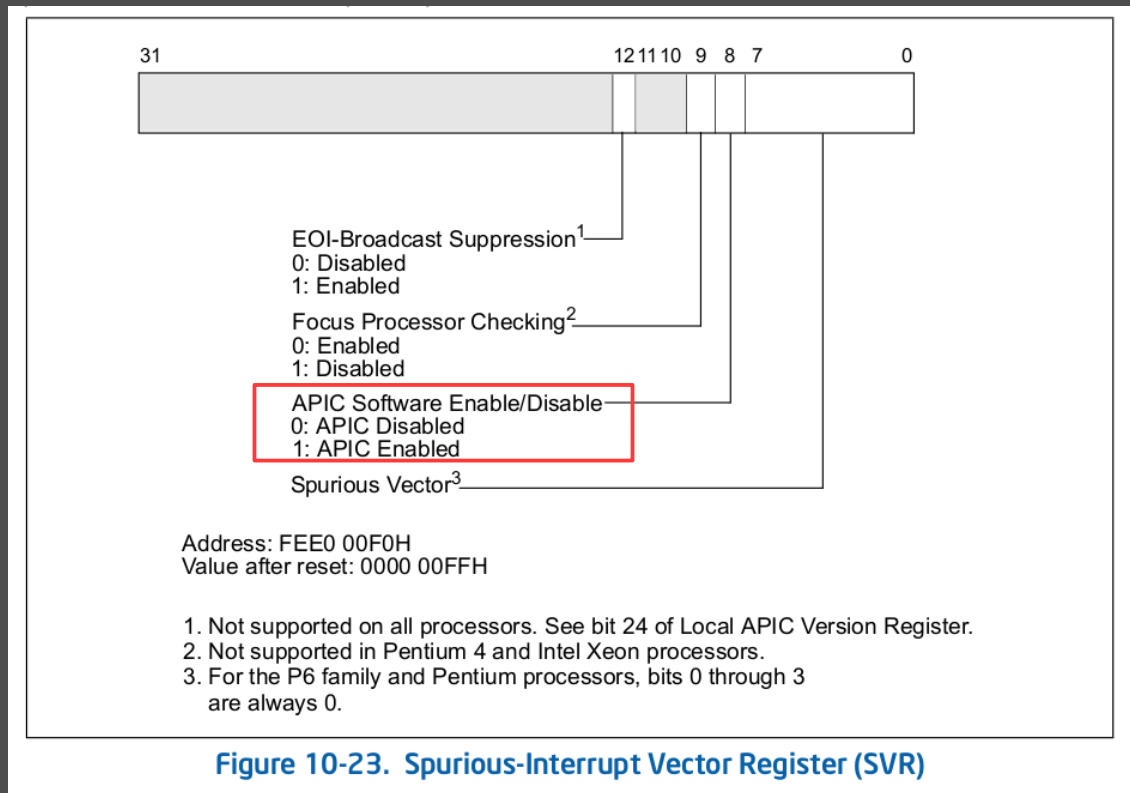
NMI (不考虑)

Fixed (#200)



伪中断（Spurious Interrupt）：用来应对中断引脚上的噪声，用于告诉 CPU 这个是误触发的情况。





Local APIC 的所有寄存器都是映射在内存的 0xFEE00000

I/O APIC 的寄存器也是在内存中的！

但问题是……哪里？

Table 1. Memory Mapped Registers For Accessing IOAPIC Registers

Memory Address	Mnemonic	Register Name	Access	D/I# Signal
FEC0 xy00h	IOREGSEL	I/O Register Select (index)	R/W	0
FEC0 xy10h	IOWIN	I/O Window (data)	R/W	1

NOTES: ???

xy are determined by the x and y fields in the APIC Base Address Relocation Register located in the PIIX3. Range for x = 0-Fh and the range for y = 0,4,8,Ch. WTF??



ACPI

高级配置与电源接口

(**A**dvanced **C**onfiguration & **P**ower **I**nterface)

但这不是本期的重点（下期内容哦 ~）

映射 IRQ 至我们的中断向量

I/O APIC 有 24 个 IRQ 输入

寄存器 IOREDTBL_k 负责 IRQ $\#k$

每个 IOREDTBL_k 为 64bits

写入顺序按照小端序

寄存器地址偏移写入
IOREGSEL

通过 IOWIN 修改 / 读取对
应寄存器的值

3.2.4. IOREDTBL[23:0]—I/O REDIRECTION TABLE REGISTERS

Address Offset:

10–11h (IOREDTBL0)

28–29h (IOREDTBL12)

12–13h (IOREDTBL1)

2A–2Bh (IOREDTBL13)

14–15h (IOREDTBL2)

2C–2Dh (IOREDTBL14)

16–17h (IOREDTBL3)

2E–2Fh (IOREDTBL15)

18–19h (IOREDTBL4)

30–31h (IOREDTBL16)

1A–1Bh (IOREDTBL5)

32–33Fh (IOREDTBL17)

1C–1Dh (IOREDTBL6)

34–35h (IOREDTBL18)

1E–1Fh (IOREDTBL7)

36–37h (IOREDTBL19)

20–21h (IOREDTBL8)

38–39h (IOREDTBL20)

22–23h (IOREDTBL9)

3A–3Bh (IOREDTBL21)

24–25h (IOREDTBL10)

3C–3Dh (IOREDTBL22)

26–27h (IOREDTBL11)

3E–3Fh (IOREDTBL23)

Default Value:

xxx1 xxxx xxxx xxxh

Attribute:

Read/Write

Table 1. Memory Mapped Registers For Accessing IOA

Memory Address	Mnemonic	Register Name
FEC0 xy00h	IOREGSEL	I/O Register Select (index)
FEC0 xy10h	IOWIN	I/O Window (data)



IM: 是否屏蔽

DELMOD: 递送模式 (b000: Fixed , b100 NMI)

INTVEC: 映射的 CPU 中断向量号

DEST: 递送目的地, 我们填 0 就好

DESTMOD: 递送目的地格式, 同样, 填 0 就好

Code Time



Intel® 64 and IA-32 Architectures SDM, Vol 3A, Chapter 10

82093AA I/O APIC Datasheet

8259A PIC (8259A/8259A-2) Datasheet

ACPI Specification v6.4, Section 5.2