第九章 中断技术

张华平 副教授 博士

Email: kevinzhang@bit.edu.cn

Website: http://www.nlpir.org/

@ICTCLAS张华平博士

大数据搜索挖掘实验室（wSMS@BIT）

- （1）【重点讲解】可编程控制器8259
- （2）【重点讲解】保护模式中断和异常的处理过程
- （3）【一般性讲解，概念为主】中断概述及实模式与保护模式的处理过程
- （4）【简单了解，不作要求】高级可编程中断控制器

中断技术

- 中断概述
- 实模式的中断处理
- 保护模式的中断处理
- 可编程中断控制8259
- 高级可编程中断控制器

中断基本原理

- 使CPU中止正在执行的程序而转去处理特殊事件的操作。这些引起中断的事件称为中断源。
- Intel系列微处理器的对外的中断引脚包括两个申请中断的硬件引脚（INTR和NMI），一个响应INTR中断的硬件引脚（INTA）。除此之外微处理器还有软件中断INT，INTO，INT3和BOUND。
- 中断结构中的2个标志位IF（Interrupt Flag，中断标志）和TF（Trap Flag，陷阱标志）和一个特殊的返回指令IRET/IRETD。

中断分类

- CPU把中断分为内部中断和外部中断两大类。为了支持多任务和虚拟存储器等功能，保护模式下，把外部中断称为“中断”（Interrupt），把内部中断称为“异常”（Exception）。通常在两条指令之间响应中断或异常。CPU最多处理256种中断或异常。
- 中断可以分为可屏蔽中断和不可屏蔽中断。
  - ❿ INTR：标志寄存器EFLAGS 中的IF 标志决定是否响应INTR 的中断请求
  - ❿ NMI：不可屏蔽中断

异常

- 异常是CPU在执行指令期间检测到不正常的或非法的操作所引起的。异常是不可屏蔽的，每一种异常类别具有不同的异常号码。
- 软中断指令“INT n”和“INTO”执行时会导致CPU产生异常事件，也属于异常而不称为中断。
- 异常分为故障（Fault）、陷阱（Trap）和中止（Abort）3种。

异常分类

- 故障：故障是在引起异常的指令之前，把异常情况通知给系统的一种情况。故障的特点是可排除。
- 陷阱：陷阱是在引起异常的指令执行之后触发的一种情况。软中断指令“INT n”、单步异常等。
- 终止：系统出现严重的不可恢复的事件时触发的一种异常，产生中止后，正执行的程序不能被恢复执行，系统要重新启动才能恢复正常运行状态。

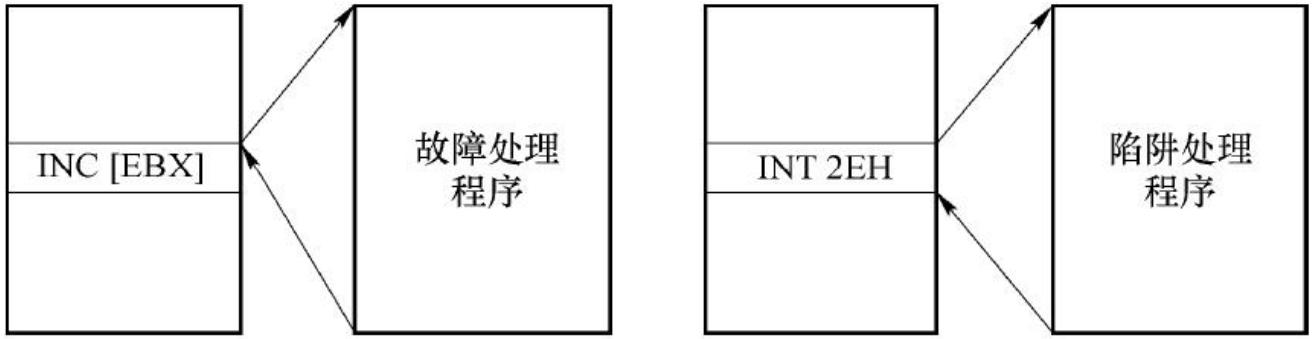

图 9-2　故障和陷阱

异常类型

表 9-1　异常的类型及其向量号

向量号	异常名称	异常类型	出错代码	相关指令
00H	除法出错	故障	无	DIV/IDIV
01H	单步/调试异常	故障/陷阱	无	任何指令
02H	NMI	中断	无	
03H	单字节 INT3	陷阱	无	INT 3
04H	溢出	陷阱	无	INTO
05H	边界检查	故障	无	BOUND
06H	非法操作码	故障	无	非法指令编码或操作数
07H	无浮点处理器	故障	无	浮点指令或 WAIT/FWAIT
08H	双重故障	中止	有	
09H	协处理器段越界	中止	无	访问存储器的浮点指令
0AH	无效 TSS 异常	故障	有	JMP、CALL、IRET 或中断
0BH	段不存在	故障	有	装载段寄存器的指令
0CH	堆栈段异常	故障	有	访问 SS 段的指令
0DH	通用保护异常	故障	有	特权指令、访问存储器的指令
0EH	页异常	故障	有	任何访问存储器的指令
10H	协处理器出错	故障	无	浮点指令或 WAIT/FWAIT
20H～0FFH	软中断 硬件中断	陷阱 中断	无 无	INT n

实模式下中断类型与类型号

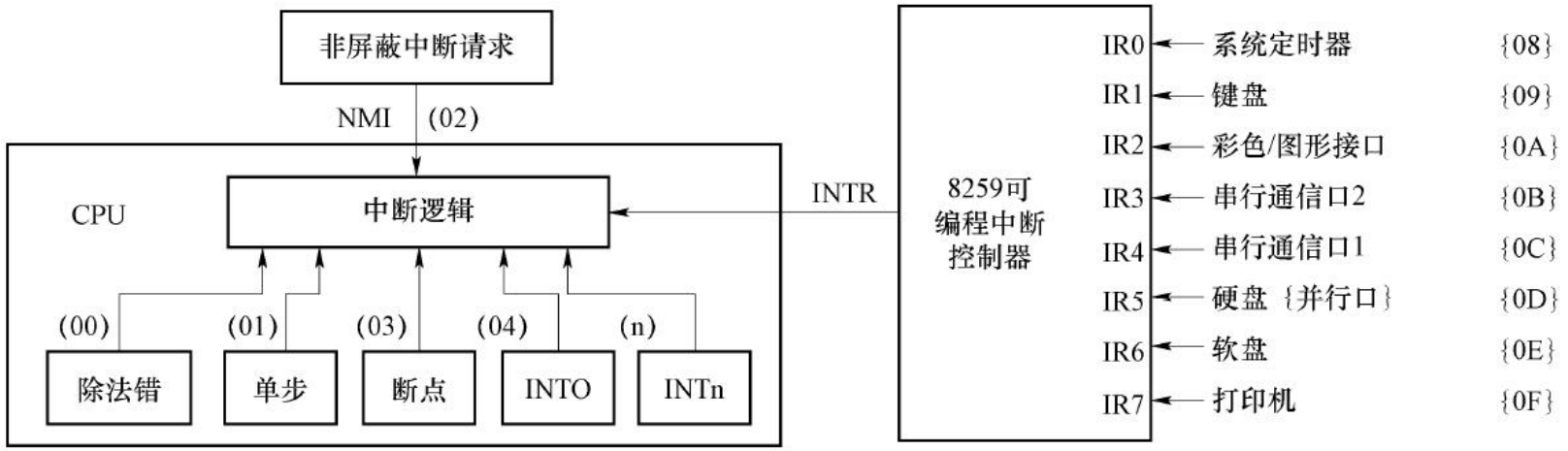

图 9-3　CPU 的中断源

中断服务程序

- CPU响应中断时，CPU暂停当前正在执行的程序转而执行中断服务程序。中断服务程序包括保护现场、处理中断、发送中断结束命令、恢复现场、中断返回几个部分。

9.2 实模式的中断处理

- 中断向量表
- 中断处理过程
- 写中断向量表

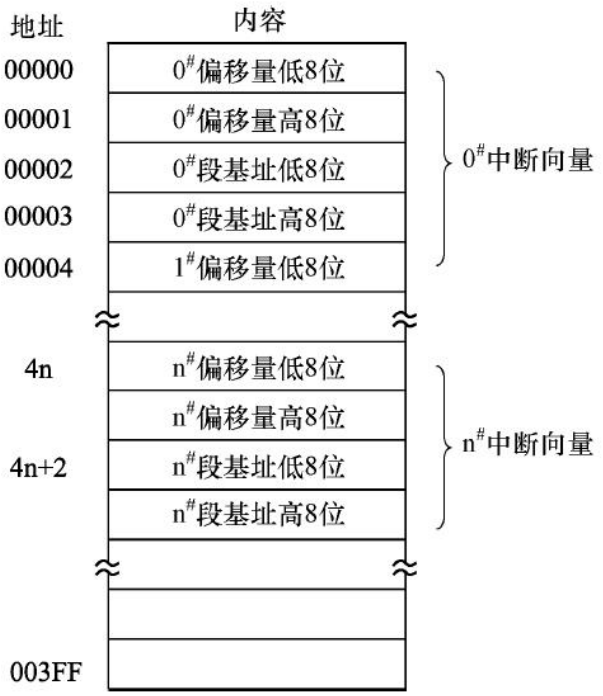

图 3–14　中断向量表

例 9.2　实模式下中断向量表实例。

```
0000:0000    68 10 A7 00 BB 13 73 05 – 16 00 98 03 B1 13 73 05
0000:0010    8B 01 70 00 B9 06 0E 02 – 40 07 0E 02 FF 03 0E 02
0000:0020    46 07 0E 02 0A 04 0E 02 – 3A 00 98 03 54 00 98 03
0000:0030    6E 00 98 03 88 00 98 03 – A2 00 98 03 FF 03 0E 02
INT 8H:    8*4=0020h    020E:0746
```

9.3 保护模式的中断处理

中断描述符表

- 保护模式下响应中断或者处理异常时，CPU根据中断/异常向量号执行对应的处理程序，把中断类型号作为中断描述符表IDT中描述符的索引，取得一个描述符，从中得到中断/异常处理程序的入口地址。
- 每个CPU核具有唯一的一个IDT。IDT的位置不定，中断描述符表寄存器IDTR指示IDT在内存中的位置。

图 9-4　中断门描述符、陷阱门描述符的格式

9.3 保护模式的中断处理

中断和异常响应步骤

- 如果是异常处理，首先根据异常类型确定返回地址（CS:EIP），对于故障，CS:EIP指向引起故障的指令；对于陷阱，CS:EIP指向引起陷阱的指令的下一条指令。
- 判断中断类型号要索引的门描述符是否超出IDT的界限。
- 再从IDT中取得对应的门描述符，分解出选择符、偏移量和属性字节，并进行有关检查。
- 根据门描述符类型，分别转入中断或异常处理程序。

9.3 保护模式的中断处理

跳转到中断服务程序的途径

- 通过中断门或者陷阱门的跳转

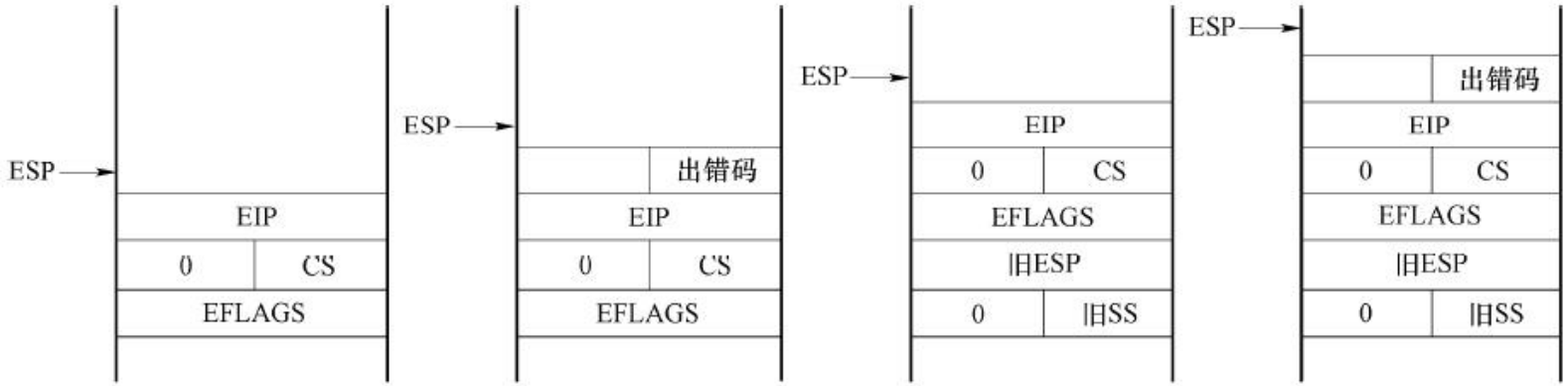

图 9-5　中断或异常后的堆栈

- 通过任务门的跳转
- 两种方式的比较

9.3 保护模式的中断处理

中断或异常处理后的返回

- 中断返回指令IRET用于从中断或异常处理程序中返回。该指令的执行根据任务嵌套标志NT位是否为1分为两种情形。由任务门转入中断或异常处理程序时，NT位被置1；由中断门或陷阱门转入中断或异常处理程序时，NT位被清0。
- NT位为1时，IRET执行的是嵌套任务的返回。
- NT位为0时，IRET执行的是当前任务内的返回。

9.3 保护模式的中断处理

任务切换

图 9-6　任务切换

图 9-7　任务内特权级的变换

图 9-8　任务内相同特权级的转移

9.4 可编程中断控制器8259

- 8259

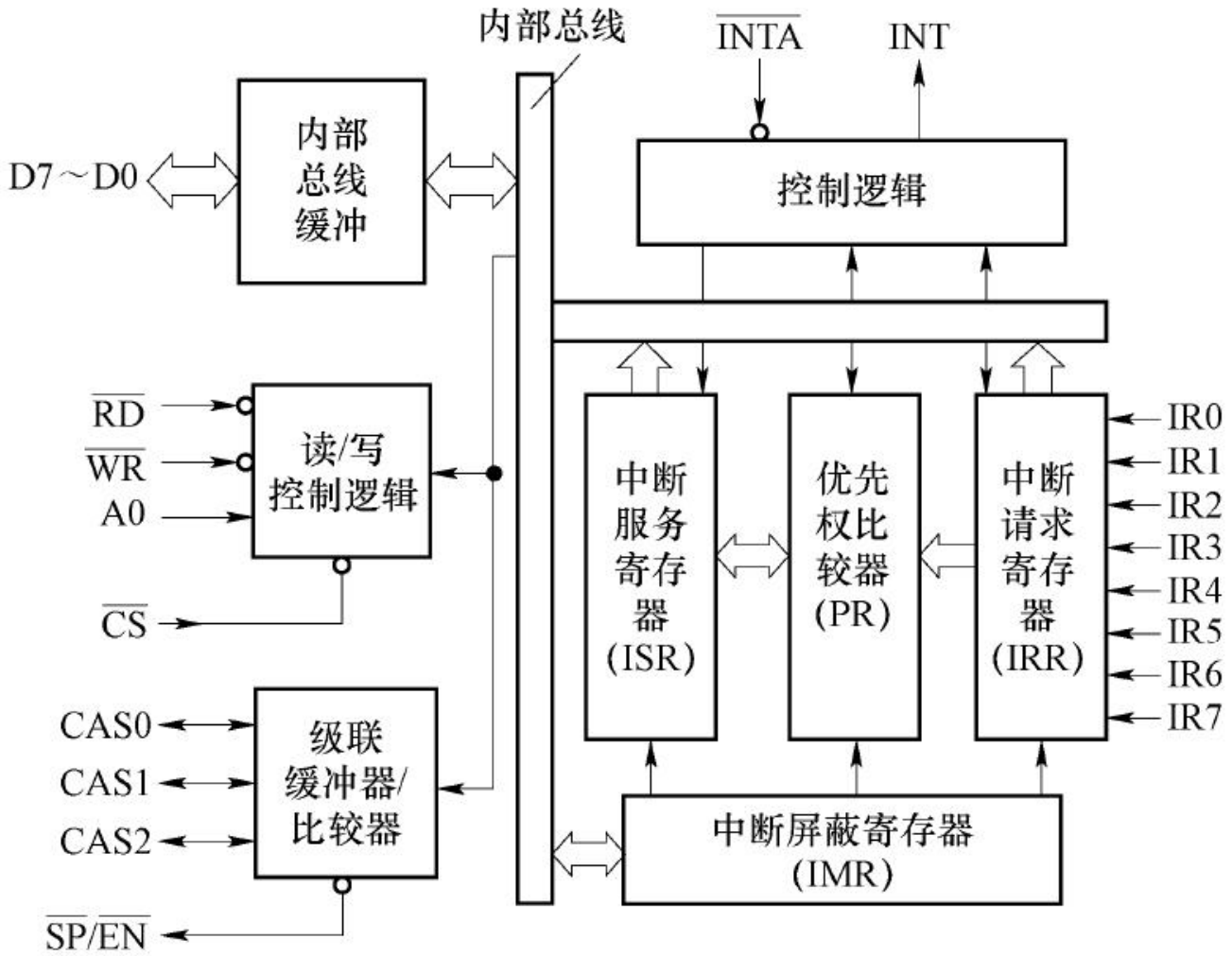

图 9－9　8259 的内部结构

9.4 可编程中断控制器8259

8259中断过程

- 当一条或多条中断请求线IR0～IR7变高时，设置相应的IRR位为1；
- 然后PR对中断优先权和中断屏蔽寄存器的状态进行判断，请求中断服务；
- CPU响应中断时，送出中断响应信号INTA，响应第一个INTA信号时，将当前中断服务寄存器中相应位置位，并把IRR中相应位复位。第二个INTA负脉冲期间，中断类型码被读入CPU。

8259工作流程

- IR2出现中断请求，该引脚的对应的中断屏蔽字相应位为0，即没有被屏蔽。此时由于ISR全为0，没有比它的优先级更高的中断正在执行，IR2的请求被送往CPU。
- CPU响应中断时，8259将ISR的值变为00000100B，标志IR2正在被服务。
- 假定IR7出现中断请求。由于IR2比IR7优先级更高，此请求暂时被忽略。
- 假定IR1出现中断请求。由于IR1比IR2优先级更高，此请求被送往CPU。
- CPU响应中断时，8259将ISR的值变为00000110B，标志IR2被中断，IR1正在被服务。

8259的级联

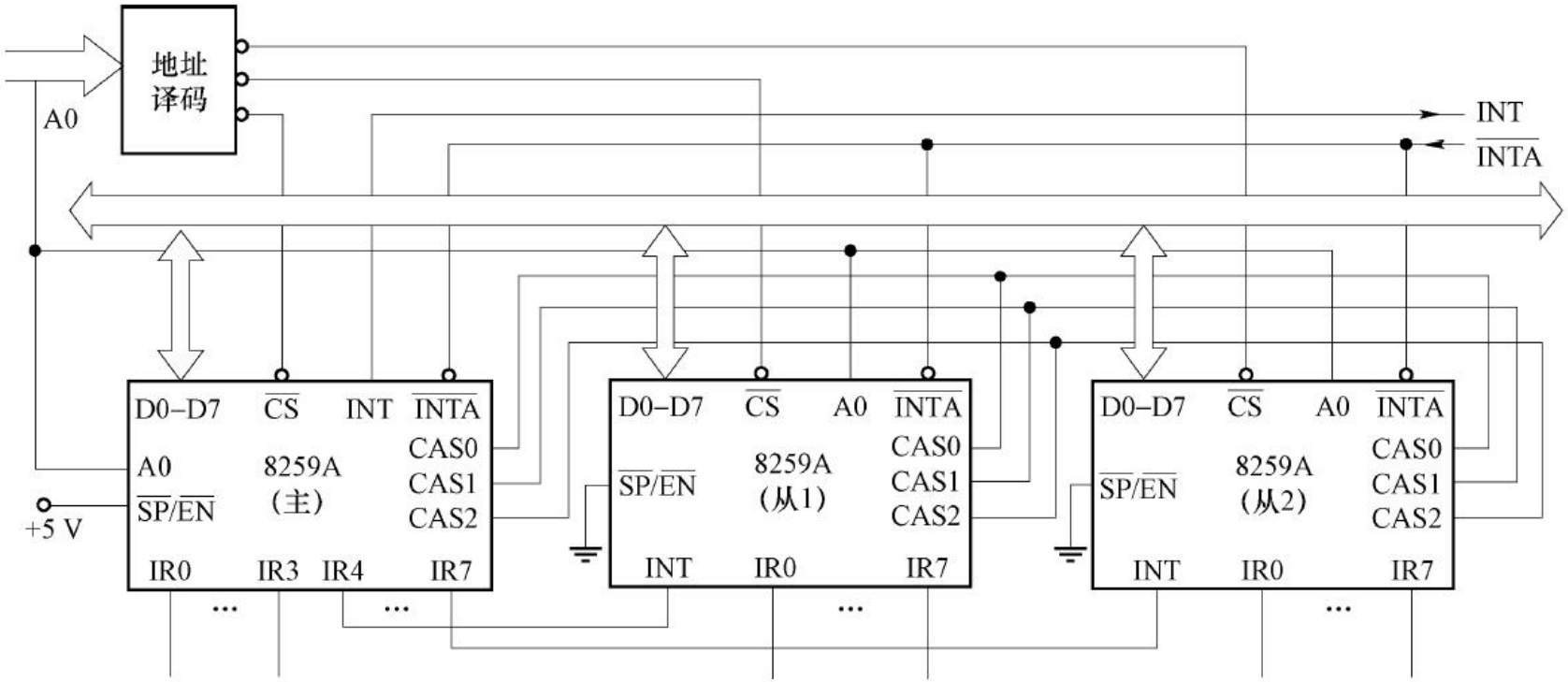

图 9–11　8259 的主从连接

8259的编程

- 命令字分两类：初始化命令字（ICW1～ICW4）和操作命令字（OCW0～OCW4）。
- 初始化命令字在系统启动时，由初始化程序设置，一旦设定，一般在系统工作过程中就不再改变。
- 操作命令字是在计算机系统运行过程中，由CPU利用这些控制字来控制8259执行不同的操作，如中断屏蔽、中断结束、优先权循环和中断状态的读出和查询等。
- OCW可在初始化之后的任何时刻写入8259，并可多次设置。

控制信号操作

- 8259也是依靠CS、A0、RD、WR等信号的组合来实现和CPU 的数据交互的，包括由CPU向8259写入命令字（ICW和OCW）、从8259读出各种状态等。

表 9－2　8259 控制信号对应的操作表

$\overline{CS}$	$\overline{WR}$	$\overline{RD}$	A0	读写操作
0	0	1	0	写 ICW1、OCW2、OCW3
0	0	1	1	写 ICW2、ICW3、ICW4、OCW1
0	1	0	0	读 IRR、ISR、查询字
0	1	0	1	读 IMR

9.4 可编程中断控制器8259

初始化命令字

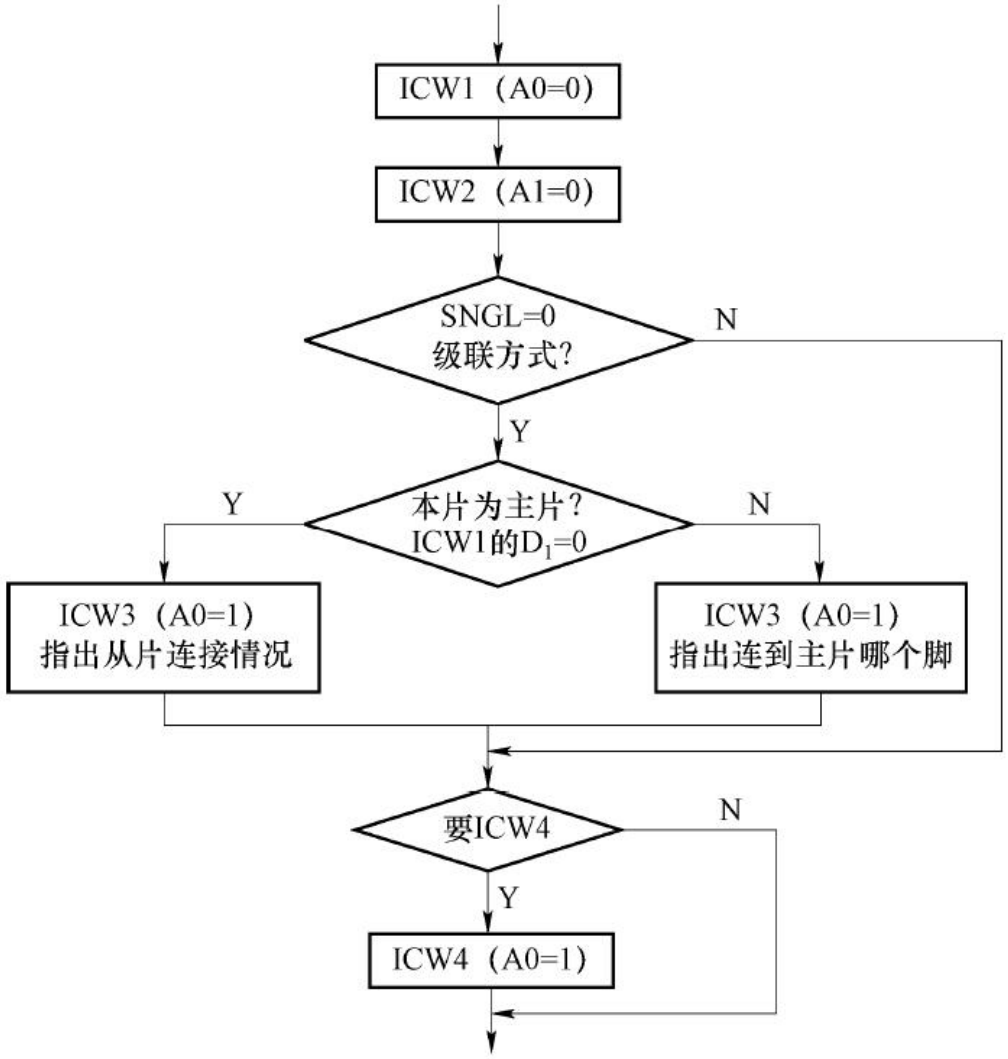

图 9-12 8259 的初始化过程

初始化命令字ICW1

- 例9.6 某系统使用单片8259，中断请求信号为上升沿触发，需要设置ICW4，该片8259的端口地址为20H和21H，则ICW1应为多少？

7	6	5	4	3	2	1	0
D7	D6	D5	1	LTIM	D2	SNGL	IC4

D7～D5	当 8259 与 8086/8088/Pentium 连接时，此位无意义
D4	必须为 1。表示这是一个 ICW1 命令字
LTIM	=0，边沿触发；=1，电平触发
D2	无意义
SNGL	=1，系统中只有 1 片 8259，单片使用；=0，多片 8259 级联使用
IC4	=0，不需要写入 ICW4；=1,需要写入 ICW4

图 9－13　ICW1 的格式

初始化命令字ICW2

- 例9.7 假设系统中使用单片8259，该片8259的端口地址为20H和21H，8个中断源的中断类型码为08H～0FH（00001000B～00001111B），则应如何初始化ICW2？

7	6	5	4	3	2	1	0
T7	T6	T5	T4	T3	0	0	0

T7～T3	中断响应码的高5位

图 9-14 ICW2的格式

初始化命令字ICW3

- 例9.8 系统中，使用两片8259，主片8259的端口地址为20H和21H，从片8259的端口地址为0A0H和0A1H，从片8259的INT连接到主片的IR2上，则应如何初始化ICW3？

7	6	5	4	3	2	1	0
S7	S6	S5	S4	S3	S2	S1	S0

S7～S0	Si 位等于 0 时，IRi 不连接从片；等于 1 时，IRi 连接从片。i=0～7

图 9－15　主片 ICW3 的格式

7	6	5	4	3	2	1	0
0	0	0	0	0	ID2	ID1	ID0

ID2～ID0	从片的标识码（0～7），即从片连接到主片的 IRi。i=0～7

图 9－16　从片 ICW3 的格式

初始化命令字ICW4

- 例9.9 假定包含两片8259。主片地址为20H和21H，从片的地址为AOH和A1H；两片都工作在特殊嵌套方式、非缓冲模式，采用非自动中断结束。写出主片和从片的ICW4初始化程序。

7	6	5	4	3	2	1	0
0	0	0	SFNM	BUF	M/S	AEOI	uPM

SFNM	=0，普通全嵌套方式； =1，特殊全嵌套方式
BUF	=0，非缓冲模式； =1，缓冲模式
M/S	=0，从片； =1，主片。BUF=0 时，此位无意义
AEOI	=0，非自动结束方式； =1，中断自动结束方式
uPM	=0，用于 8080/8085 等 8 位 CPU 系统； =1，用于 8088/8086/Pentium

图 9－17　ICW4 的格式

中断屏蔽操作命令字OCW1

- 例9.10 8259的端口地址为20H和21H，试编写程序屏蔽IR2、IR5两个中断源。

7	6	5	4	3	2	1	0
M7	M6	M5	M4	M3	M2	M1	M0

M7～M0	Mi 位等于 0 时，该中断源 IRi 不会被屏蔽；等于 1 时；IRi 被屏蔽

图 9－18　OCW1 的格式

9.4 可编程中断控制器8259

- 优先级循环方式和中断结束方式操作命令字OCW2
  - 例9.11 8259地址为20H和21H，编写程序完成如下操作：
    ① 清除IR2对应的ISR
    ② 设置IR4为最高优先级

7	6	5	4	3	2	1	0
R	SL	EOI	0	0	L2	L1	L0

R	=1，优先级循环
SL	=1，特定优先级，L2～L0 有效； =0 时，L2～L0 不起作用
EOI	=1，中断结束命令，使中断服务寄存器 ISR 中的某一位清 0
L2～L0	三位二进制编码，代表 0～7 共 8 种中断源

图 9－19 OCW2 的格式

9.4 可编程中断控制器8259

特殊屏蔽方式和中断查询方式操作命令OCW3

例9.12 编写程序段读取8259中IRR和ISR的值。

7	6	5	4	3	2	1	0
0	ESMM	SMM	0	1	P	RR	RIS

ESMM SMM	ESMM=1 且 SMM=0 时，退出特殊屏蔽方式。 ESMM=1 且 SMM=1 时，进入特殊屏蔽方式。 ESMM=0 时，SMM 位无效
P	=1 时，执行中断查询命令
RR	=0 时，RIS 位无效； =1 时，由 RIS 来确定读取 IRR 还是 ISR
RIS	RR=1 且 RIS=0 时，下一次读取的是 IRR(中断请求寄存器)。 RR=1 且 RIS=1 时，下一次读取的是 ISR(中断服务寄存器)

图 9－20 OCW3 的格式

7	6	5	4	3	2	1	0
I	0	0	0	0	W2	W1	W0

I	=0 时，没有中断请求； =1 时，有中断请求
W2W1W0	有效中断请求（IR0～IR7）中优先级最高的中断源的编号

图 9－21 查询字的格式

命令字小结

- 8259一共有7个命令字：ICW1～ICW4、OCW1～OCW3。ICW1、OCW2、OCW3 写入偶地址端口（A0=0）。标志位D4、D3对它们进行区分，

表 9-3　写入偶地址控制字表示

D4	D3	控制字
1	X	ICW1
0	0	OCW2
0	1	OCW3

- 例9.13 8259 初始化举例。
  - 假定两片8259级联使用，从片连接在主片的IR2 引脚，主片端口地址为20H、21H，从片端口地址为A0H、A1H，要求主片中断向量号设置为20H～27H，从片中断向量号设置为28H～2FH。中断向量采用边沿触发的方式，主片采用特殊嵌套方式，从片采用普通嵌套方式，仅仅开启定时中断，屏蔽其他中断。
  - 参考程序P355

9.4 可编程中断控制器8259

- 8259的应用

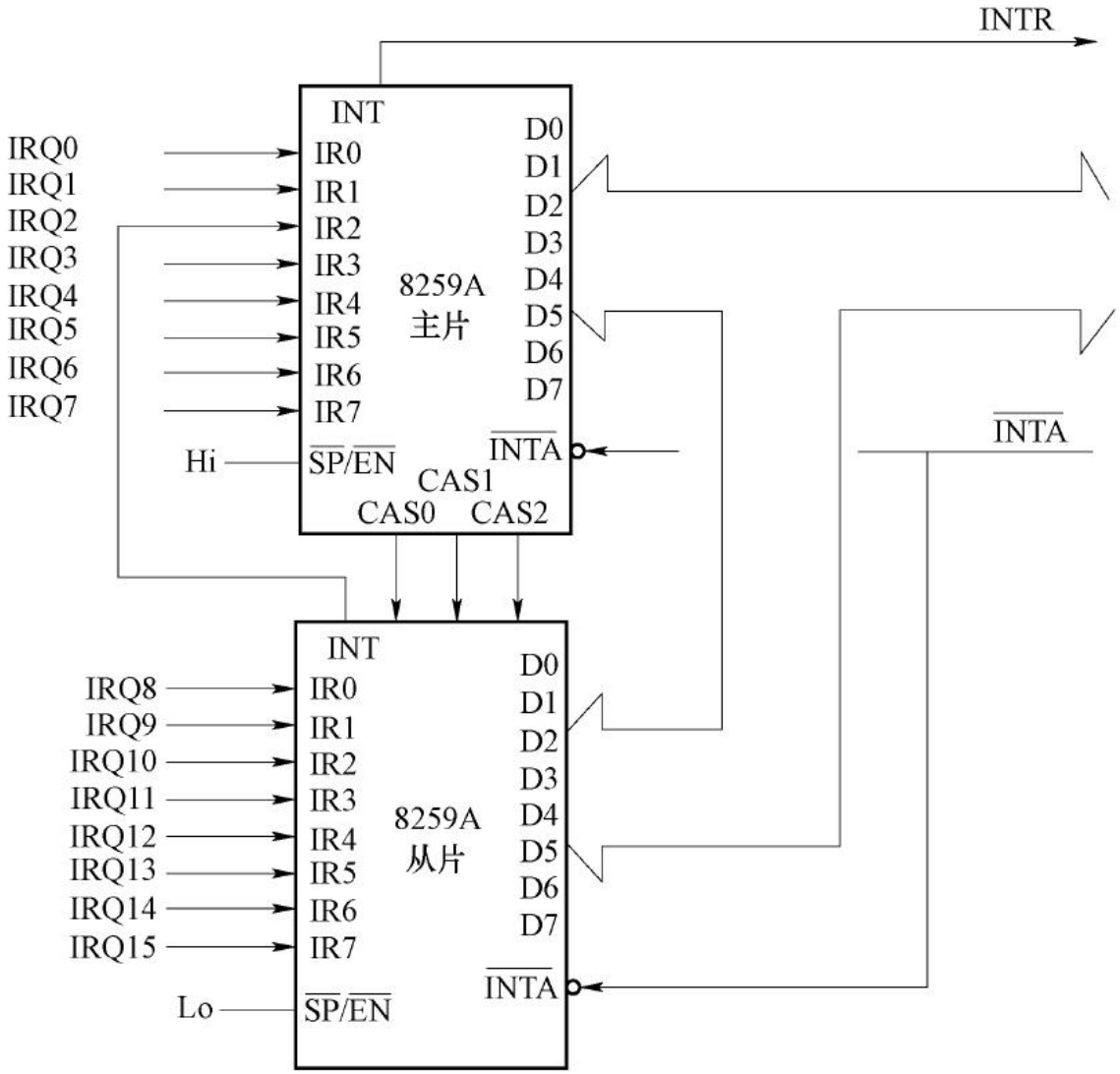

图 9－22　PC 机内 2 片 8259 级联示意

9.5 高级可编程中断控制器

APIC概述

- 标准PC上两片级联的8259提供了理论上15个中断输入源，但实际系统中这些中断源远远不够用。从Pentium 开始，微机系统中引入了高级可编程中断控制器APIC。
- APIC可以用于单CPU和多CPU系统。
- APIC系统可以分为两大部分：LAPIC（Local APIC）和IO APIC。

9.5 高级可编程中断控制器

APIC的组成

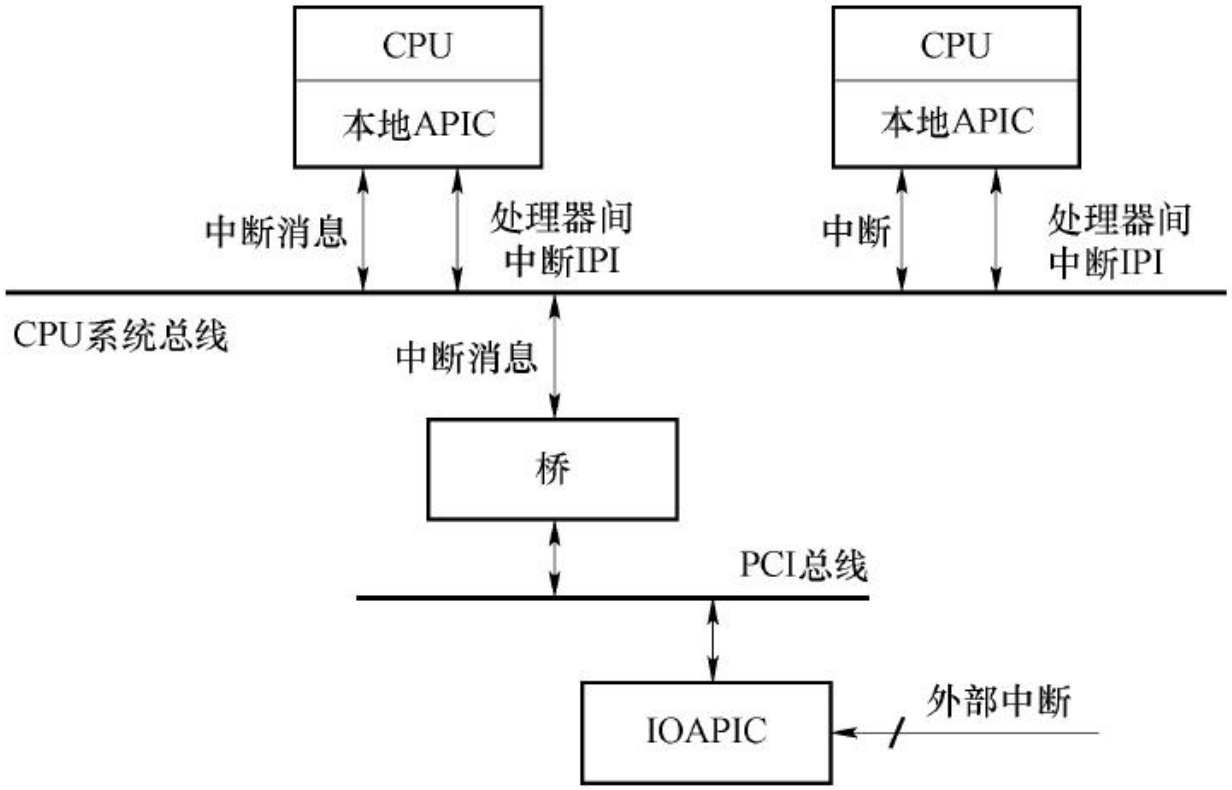

图 9－23　APIC 的组成

9.5 高级可编程中断控制器

- LAPIC：LAPIC（本地APIC）包含了8259和8254的功能。它能响应以下几种中断：
  - 系统中断：IO APIC送来的系统中断请求，由IO APIC 交给中断请求指定的目标处理器处理。
  - 处理器间中断：经APIC 总线（或系统总线）送来的处理器间中断请求（IPI）。
  - 本地中断：本地APIC产生的系统中断请求（计时器、LINT0/LINT1、性能监控、温度传感器、错误）。本地中断只能由该CPU处理。

9.5 高级可编程中断控制器

IO APIC

- IO APIC用来替代传统的8259中断控制器，一般集成在ICH芯片组中。

表 9-7　IO APIC 的 IRQ 源

IRQ	来自 SERIRQ	来自引脚	来自 MSI	说　明	中断向量号
0	No	No	No	8254 计数器 0、高精度定时器 $\overline{\text{HPET0}}$	FFh
1	Yes	No	Yes		B3h
2	No	No	No	用于 8259 级联	FFh
3	Yes	No	Yes		51h
4	Yes	No	Yes		A2h
5	Yes	No	Yes		FFh
6	Yes	No	Yes		FFh
7	Yes	No	Yes		FFh
8	No	No	No	实时钟、高精度定时器 $\overline{\text{HPET1}}$	D1h
9	Yes	No	Yes	系统控制中断 SCI、总体拥有成本控制 TCO	B1h
10	Yes	No	Yes		FFh
11	Yes	No	Yes		FFh

感谢关注聆听！

张华平
Email: kevinzhang@bit.edu.cn
微博：@ICTCLAS张华平博士
实验室官网：
http://www.nlpir.org

大数据千人会