



第2章 80X86微处理器

intel®



Outline

2.1

32位微处理器内部结构

2.2

32位微处理器的工作模式和地址空间

2.3

实模式下,物理地址的形成 (重要)

1. 位和字节

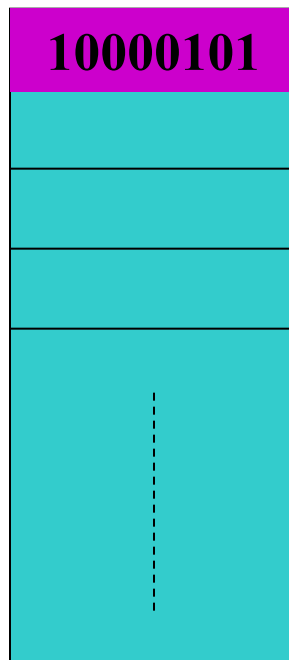
- 位 (bit) 是计算机所能表示的最小最基本的数据单位, 它指的是取值只能为0或1的一个二进制数值位。位作为单位时记作b
- 字节 (byte) 由8个位组成, 通常用作计算存储容量的单位。字节作为单位时记作B

K是kilo的缩写, $1K=1024=2^{10}$;

M是mega的缩写, $1M=1024K=2^{20}$;

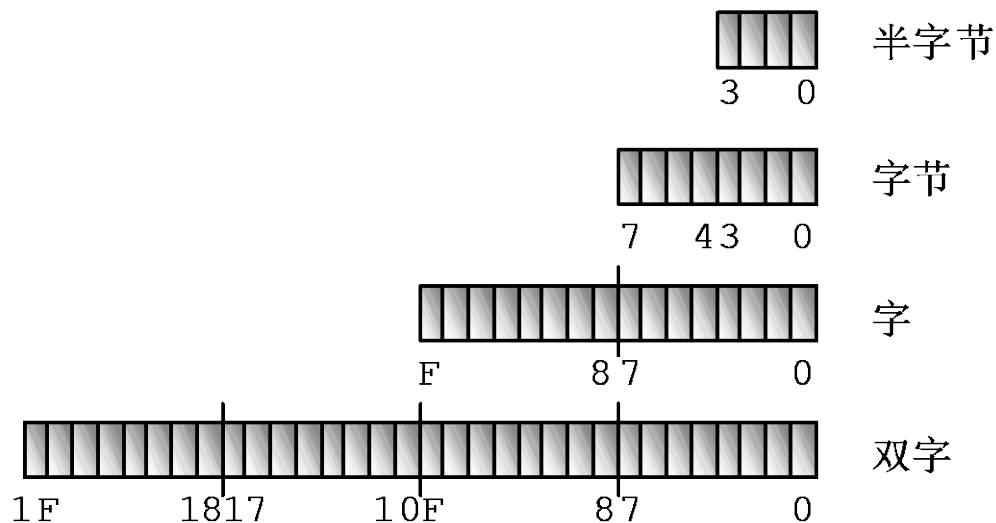
G是Giga的缩写, $1G=1024M=2^{30}$;

T是tera的缩写, $1T=1024G=2^{40}$ 。



2. 字长(数据宽度)

- 字长是微处理器一次可以直接处理的二进制数码的位数，它通常取决于微处理器内部通用寄存器的位数和数据总线的宽度。微处理器的字长有4位、8位、16位、32位和64位等等。



3. 寻址能力

指CPU能直接存取数据的内存地址的范围，它由CPU的地址总线的数目决定。

4. 主频

- ◆ 主频也叫**时钟频率**，用来表示微处理器的运行速度，主频越高表明微处理器运行越快，主频的单位是MHz。**时钟频率类比流水线**

5. MIPS

MIPS是Millions of Instruction Per Second的缩写，用来表示微处理器的性能---**运算速度**，**每秒钟能执行多少百万条指令**。

6. 微处理器的集成度

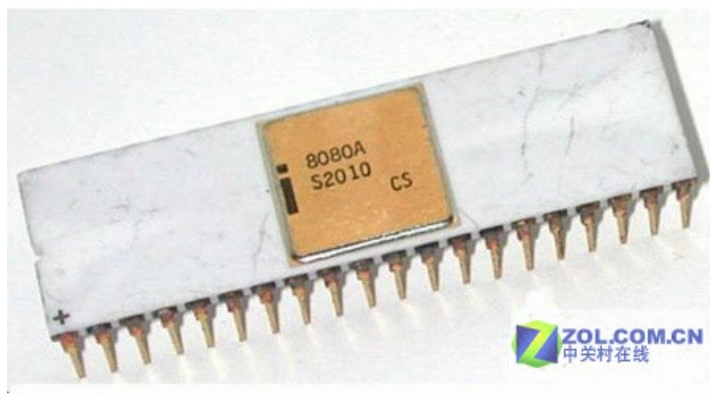
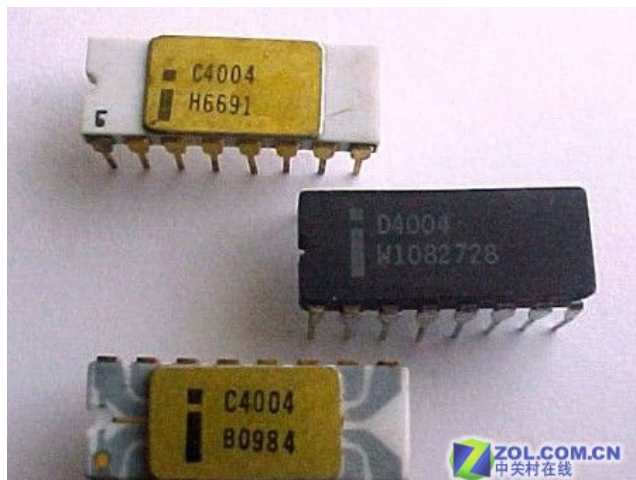
- 指微处理器芯片上集成的晶体管的密度。
- 最早Intel 4004的集成度为2250个晶体管，Pentium III的集成度已经达到750万个晶体管以上，集成度提高了3000多倍。**酷睿系列处理器的集成度以达到亿级别**



80X86 CPU介绍

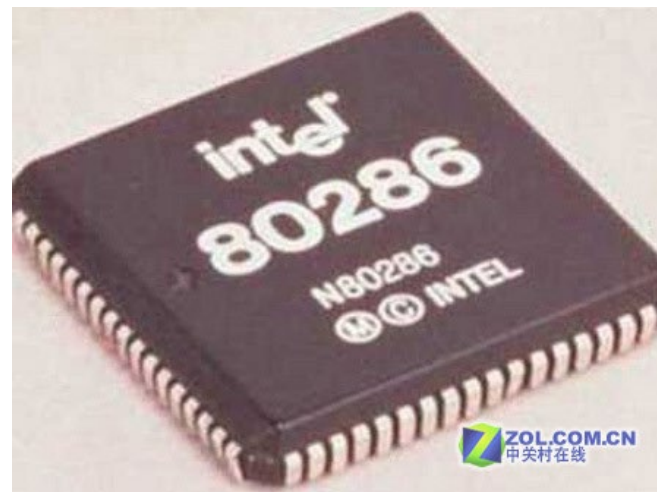
微型计算机原理与接口技术

型号	发布 年分	字长 (位)	晶体管 (万个)	数据总 线宽度	外部总 线宽度	主频	寻址 空间	高速 缓存
8086	1978	16	2.9	16	16	4.77	1M	无
8088	1979	16	2.9	16	8	4.77	1M	无
286	1982	16	13.4	16	16	6~20	16M	无
386	1986	32	27.5	32	32	12~33	4G	有
486	1989	32	120	32	32	25~100	4G	8K
奔腾	1993	32	310	64	64	60~166	4G	8K
奔腾Pro	1995	32	550	64	64	150~ 200	64G	8K 256K
奔2	1997	32	750	64	64	233~333	64G	32K 512K
Itanium	2000	64	2.2亿	64	64	1G以上	64G	6M集 成三级
酷睿2	2006	64	2.91亿	64	64	3.60G	64G	6M集 成三级
Intel I9- 12900k	2022	64	220亿	64	64	5.2G		30M





微型计算机原理与接口技术





微型计算机原理与接口技术







微处理器的基本功能模块:

- 总线接口单元 **BIU**（取指令）
（寄存器组）
- 执行单元 **EU**（执行指令）
（运算器和控制器、寄存器组）



微处理器的功能扩展模块:

- 存储管理(分段和分页部件)
- 指令和数据流水线
- 指令和数据CACHE
- 指令预取
- 浮点处理
- 分支预测
- 并行计算
-



Pentium 采用了多项先进技术:

- CISC和RISC相结合的技术
- 超标量流水线技术
- 分支预测技术



RISC和CISC:

✦ **RISC** (Reduced Instruction Set Computer), **精简指令系统的计算机**

提供数目较少、格式与功能简单、运行高效的指令
追求的是计算机控制器实现简单, 运行高速, 更容易在单块超大规模集成电路的芯片内制做出来

✦ **CISC** (Complex Instruction Set Computer), **复杂指令系统的计算机**

相对于RISC一词而提出来的一种说法

特点: 指令条数多, 格式多样, 寻址方式复杂, 每条指令的功能强。汇编程序设计容易些, 但计算机控制器的实现困难多, 很多指令被使用的机会并不多



流水线:

是一种使多条指令重叠操作的技术,是当代微处理器设计中的关键技术之一。

把一条指令分解成若干个步骤来完成,在流水线上称为级,每级都在一个时钟周期内完成各自的操作。这样每个时钟周期都可以启动一条指令, m 级的流水线上就会有 m 条指令在同时执行。

流水线的性能比非流水线作业几乎提高了 m 倍。

超标量流水线:

标量指单个量,一般的流水计算机因只有一条指令流水线,所以称为标量流水计算机,所谓超标量是指其具有两条以上的指令流水线。

Pentium 有U、V两条整型流水线,一条浮点流水线。

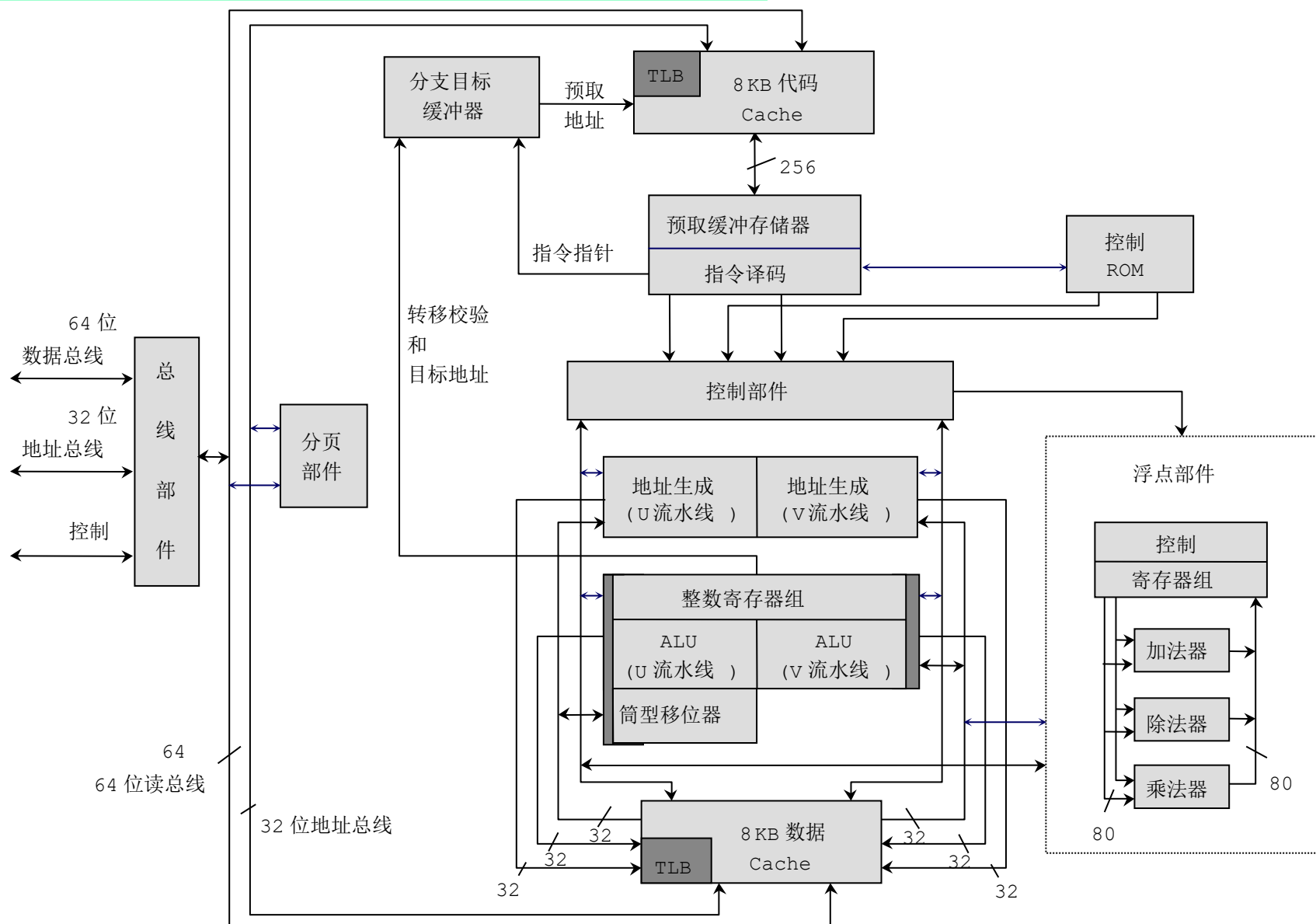


分支预测：

所谓分支预测是指当遇到转移指令、**CALL**调用指令、**RET**返回指令、**INT n**中断指令等跳转指令时，指令预取单元能够较准确地判定是否转移取址。



2.1 32位微处理器内部结构





基本结构寄存器:

486内部寄存器分为4类:

- 基本结构寄存器
- 浮点寄存器
- 系统级寄存器
- 调试测试寄存器

应用程序只能访问基本结构寄存器和浮点寄存器。(我们只介绍基本结构寄存器)



通用寄存器

32位名称		8位名称 16位名称		名称
EAX		AH AX AL		累加器
EBX		BH BX BL		基址寄存器
ECX		CH CX CL		计数器
EDX		DH DX DL		数据寄存器
ESP		SP		堆栈指针
EBP		BP		基址指针
EDI		DI		目的变址寄存器
ESI		SI		源变址寄存器
		32位		
		16位		
EIP		IP		指令指针
EFLAGS		FLAGS		标志

段寄存器

CS	代码
DS	数据
ES	附加
SS	堆栈
FS	
GS	

指令指针 标志寄存器



1.通用寄存器(8个)

32位名称

16位名称

名称

EAX

AX

累加器

EBX

BX

基址寄存器

ECX

CX

计数器

EDX

DX

数据寄存器

ESP

SP

堆栈指针

EBP

BP

基址指针

EDI

DI

目的变址寄存器

ESI

SI

源变址寄存器

- **AX (accumulator)**
- **BX (Base)**
- **CX (Count)**
- **DX (Data)**
- **SP (Stack Pointer)**
- **BP (Base Pointer)**
- **DI (Destination Index)**
- **SI (Source Index)**



32位名称

8位名称

16位名称

名称

EAX		AH AX AL	累加器
EBX		BH BX BL	基址寄存器
ECX		CH CX CL	计数器
EDX		DH DX DL	数据寄存器
ESP		SP	堆栈指针
EBP		BP	基址指针
EDI		DI	目的变址寄存器
ESI		SI	源变址寄存器
EIP		IP	指令指针 IP (Instruction Pointer)

AX、BX、CX、DX 共同特点：

- 既可作为16位寄存器来用又可作为两个8位寄存器（高、低位）来用；
- 都是用于暂存操作数，或是运算的中间结果或其它一些信息。

指令 = 操作码 + 操作数

SP、BP、SI、DI、**IP**：为寻址存贮单元提供偏移地址。



2.段寄存器

CS
DS
ES
SS
FS
GS

代码
数据
附加
堆栈

CS、DS、ES、SS-----4个段寄存器，和偏移地址寄存器一起形成20位存储器物理地址，对存储器中存放的程序、数据、堆栈区域加以区别、寻址。

- 寻址程序(指令): $CS + IP$;
- 寻址数据: $(DS \text{ 或 } ES) + (SI \text{ 或 } DI, BX, BP)$;
- 寻址堆栈: $SS + (SP \text{ 或 } BP)$

具体用法在寻址方式中介绍



3.标志寄存器

EFLAGS**FLAGS**

标志寄存器

标志寄存器**FLAGS**又称为程序状态字**PSW**，为16位寄存器，该寄存器主要有**两个作用**：

- 记录**CPU**运行结果状态标志；
- 提供控制标志。

FLAGS各位含义如下：

15 14 13 12 **11 10 9 8 7 6 5 4 3 2 1 0**

OF DF IF TF SF ZF AF PF CF



根据功能，8086的标志可以分为两类：

状态标志：表示前面的操作执行后，算术逻辑部件处在怎样一种状态，这种状态会像某种先决条件一样影响后面的操作。有**SF**、**ZF**、**PF**、**CF**、**AF**和**OF**。

控制标志：每个控制标志都对某一种特定的功能起控制作用。指令系统中有专门的指令用于控制标志的设置和清除。有**DF**、**IF**、**TF**。



2.2 32位微处理器的工作模式和地址空间

一. 32位微处理器工作模式

- 实地址模式(实模式)
- 保护虚拟地址模式(保护模式)
- 虚拟86模式

1. 实模式的特点

- ①加电、复位之后，486自动工作在实模式，系统在DOS管理下
- ②在实模式下，486只能访问第一个1M内存(00000H~FFFFFH)



- ③ 存储管理部件对存储器只进行分段管理，没有分页功能，每一逻辑段的最大容量为64K。
- ④ 在实模式下，段寄存器中存放段基址。

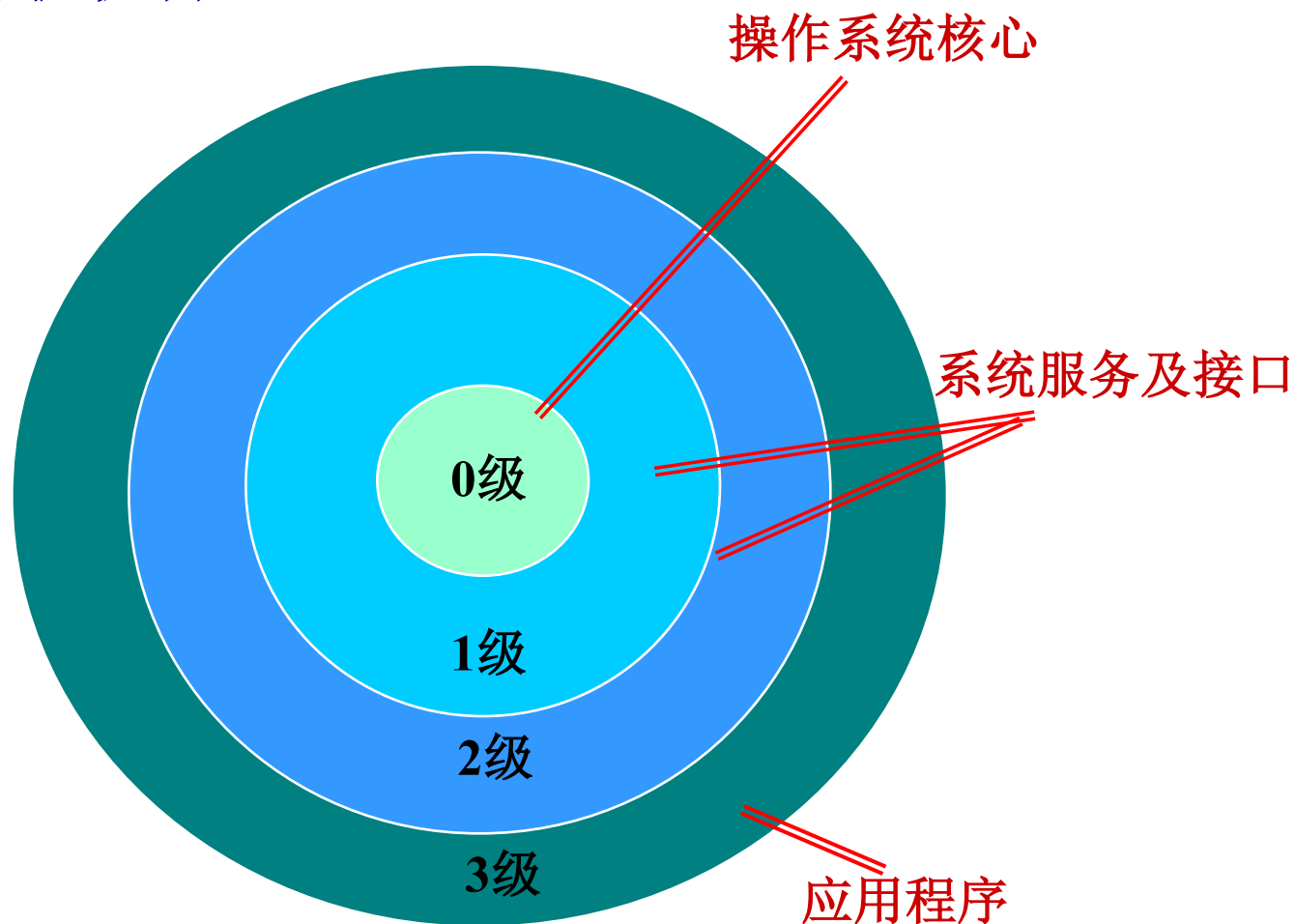
2.保护模式的特点:(仅作了解)

486工作在保护模式下，才能真正发挥它的设计能力。

- ①在保护模式下，486支持多任务操作系统
- ②在保护模式下，486可以访问4G物理存储空间
- ③存储管理部件中，对存储器采用分段和分页管理



□ 关于保护机制：



高级别的程序可以访问同级或低级的数据段，反之则不行



3. 虚拟86模式（仅作了解）：

虚拟86模式是保护模式下的一种特殊工作模式,可运行实模式程序。

在操作系统管理下,486可以分时地运行多个实模式程序。

例如：有3个任务,操作系统为每一个任务分配1ms,每通过1ms就发生一次任务切换,从宏观上看系统是在执行多个任务。

实模式下，一个逻辑段的最大容量是()

- ☐ A 640KB
- ☐ B 1MB
- ☐ C 4GB
- ☒ D 64KB

提交



二、32位微处理器的地址空间（存储地址空间、I/O地址空间）

1. 存储地址空间（物理空间、虚拟空间、线性空间）：

□ **物理空间**（主存储器的实际空间）：

程序的运行空间, 即主存空间

486有32条地址线, 内存最大容量4G。这4G字节称为物理存储器, 每一单元的地址称为**物理地址**, 其地址范围:

0000,0000H~FFFF,FFFFH为物理存储空间。

$$2^{32}=4G$$

物理
地址:

物
理
空
间



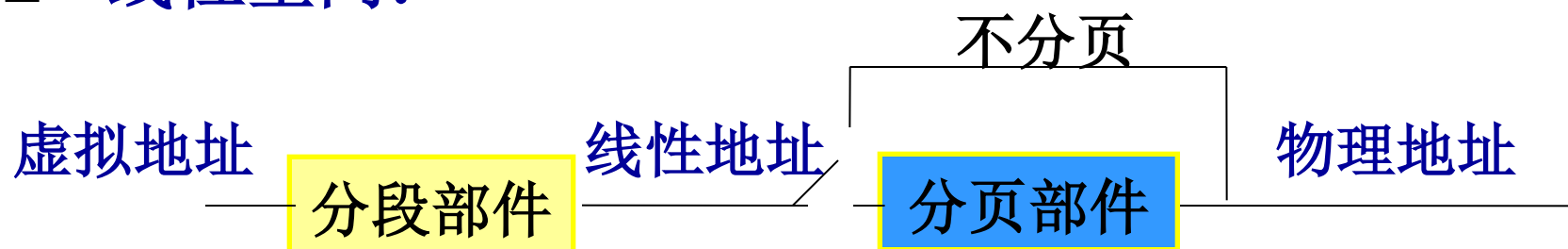
□ 虚拟空间(虚拟存储器地址空间):编程空间

虚拟存储器是一项硬件和软件结合的技术。

存储管理部件把主存(物理存储器)和辅存(磁盘)看作是一个整体,即虚拟存储器。允许编程空间为 $2^{46}=64\text{T}$,程序员可在此地址范围内编程,程序可大大超过物理空间。该空间对应的地址称为**虚拟地址**或**逻辑地址**。运行时,操作系统从虚拟空间取一部分程序载入物理存储器运行。当程序运行需要调用的程序和要访问的数据不在物理存储器时,操作系统再把那一部分调入物理存储器。.....数据的交换极快,程序察觉不到。



□ 线性空间：



当程序从虚拟空间调入物理空间时，要进行地址转换。

分段部件首先把虚拟地址(编程地址)转换为线性地址，

☆ 如果不分页的话，线性地址就是物理地址；

☆ 如果分页的话，则由分页部件把线性地址转换为物理地址。

实模式：存储空间仅分段，而不分页；

保护模式：存储空间先分段，再分页。



2. I/O空间:

486利用低16位地址线访问I/O端口，所以I/O端口最多有 $2^{16}=64\text{K}$ ，I/O地址空间为0000H~FFFFH。

注意:

- I/O地址空间不分段

- I/O地址空间与存储空间不重叠

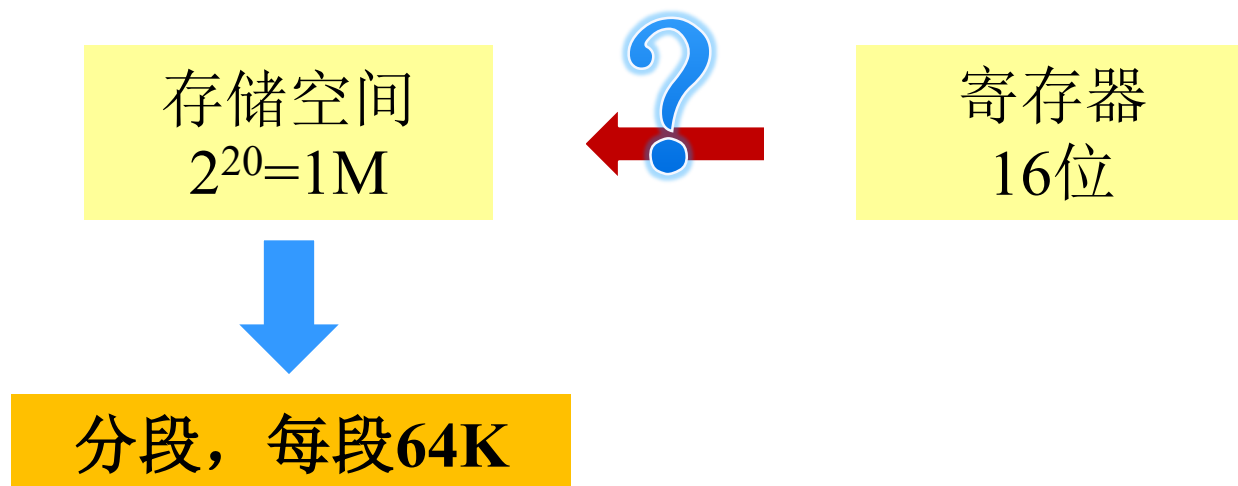
CPU有一条控制线 $\overline{\text{M}/\text{IO}}$ ，在硬件设计上用 $\text{M}/\text{IO}=1$ ，参与存储器寻址，用 $\overline{\text{M}/\text{IO}}=0$ 参与I/O寻址。

- 从PC/XT~Pentium，基于Intel微处理器的系统机，实际上只使用低10位地址线，寻址 $2^{10}=1024$ 个I/O端口。



三. 实模式下, 物理地址的形成 (重要)

1. 存储器的分段管理:



逻辑地址 段基址: 偏移地址
(16位) (16位)

物理地址 = 段基址 $\times 16$ + 偏移地址



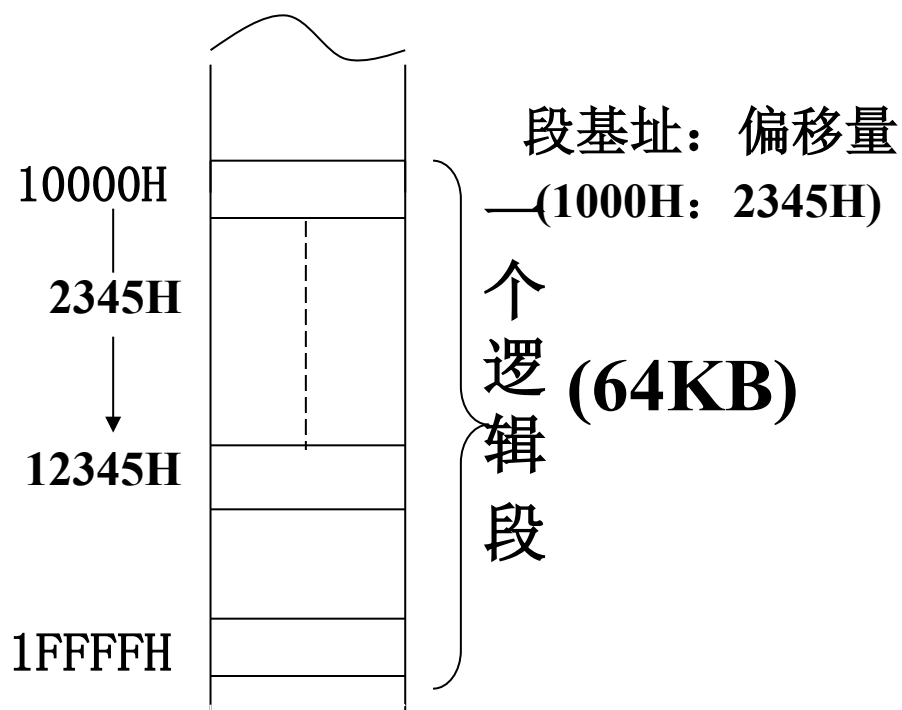
三. 实模式下, 物理地址的形成 (重要)

1. 存储器的分段管理:

例: 设某存储单元, 段基址=1000H, 偏移量=2345H, 求物理地址?

则物理地址为:

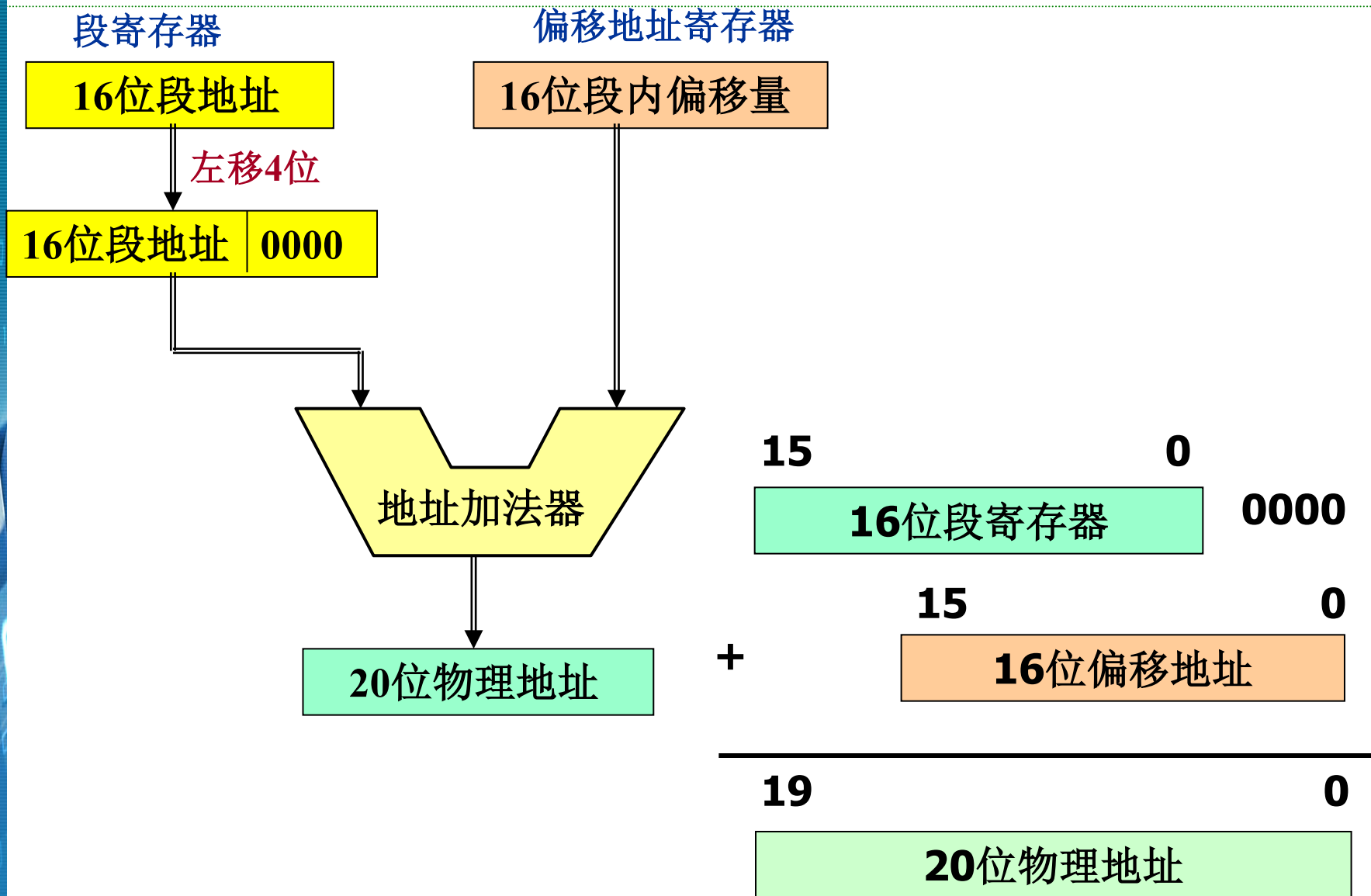
$$\begin{array}{r} 10000\text{H} \\ + 2345\text{H} \\ \hline 12345\text{H} \end{array}$$





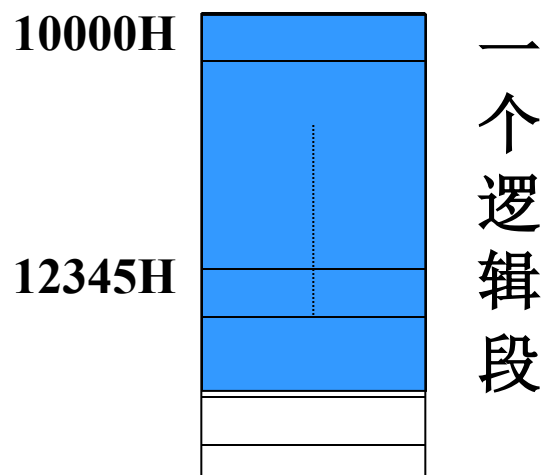
实模式下20位物理地址的形成

微型计算机原理与接口技术





存贮器中的每个存贮单元都可以用两个形式的地址来表示：**物理地址和逻辑地址**。物理地址是指1MB存贮区域中的某一单元地址，地址信息是**20位的二进制代码**，以16进制表示是00000H~FFFFFH中的一个单元，CPU访问存贮器时，地址总线上送出的是物理地址。编制程序，则采用**逻辑地址**。逻辑地址由段基址和偏移量组成。



物理地址为 12345H,

逻辑地址为 1000H:2345H

- 在一个逻辑段中,各单元的**段基址**是相同的
- **偏移地址**是该单元相对于段首的地址偏移量
- 所有段都是起始于16字节的边界。



注意：

物理地址是唯一的，不同的逻辑地址可得到相同的物理地址。 如：

2000H: 0200H —— 20200H

2010H: 0100H —— 20200H

逻辑地址需由程序员在编程时给出

段 基 址：指明由哪个段寄存器给出即可

偏移地址：由程序员在程序中给出具体值

80x86实模式下，逻辑地址2FD0H:100H表示的存储单元的物理地址是 [填空1] H；逻辑地址2F34H:2F6H表示的存储单元的物理地址是 [填空2] H；逻辑地址1234H:5678H表示的存储单元的物理地址是 [填空3] H；逻辑地址576AH:1024H表示的存储单元的物理地址是 [填空4] H。

作答



2.各逻辑段物理地址的形成(以16位寻址为例):

在实模式下, 段寄存器存放相应逻辑段的段基址

逻辑段	段基址存放在.....	偏移地址存放在.....
代码段	CS	IP
堆栈段	SS	SP
数据段	DS	根据不同的寻址方式 选择BX、BP、SI、DI
附加段	ES/FS/GS	

代码段: $CS \times 2^4 + IP$ = 指令单元的物理地址

一条指令的一个字节取出后, IP自动加1, 指向下一字节。

堆栈段: $SS \times 2^4 + SP$ = 栈顶单元的物理地址

数据段: $DS \times 2^4 + \text{偏移地址}$ = 数据单元的物理地址



3. 段寄存器和指针寄存器的初值

CS、IP的初值： 由操作系统赋值

SS、SP的初值： ①由程序员赋值
②由操作系统自动赋值

DS/ES/FS/GS的初值： 由程序员赋值。

BX/SI/DI/BP的初值： 由程序员赋值。



第2章 学习重点

1. 了解X86内部主要功能块的简单作用;
2. 掌握基本结构寄存器中的通用寄存器、段寄存器、指令指针、标志寄存器的结构、名称、汇编助记符;
3. 掌握32位微处理器工作模式中的实模式的特点;
4. 掌握实模式下存储器各个逻辑段的物理地址的形成方法, 以及CS、IP, SS、SP, DS、ES各寄存器初值的赋值原则及特点.