本节主题

x86体系结构

北京大学·慕课

计算机组成

制作人：陆俊林

x86体系结构

体系结构		厂商	微处理器型号	字长	年代
x86	“x86-16” “IA-16”	Intel	**8086**, 8088, 80186, 80188 80286	16位	1978年起
	IA-32	Intel	**80386**, 80486, Pentium, Pentium Pro/II/III/4, Core, Atom	32位	1985年起
		AMD	Am386, Am486, AM5x86, K5, K6, Athlon		
		Others	**Cyrix** 5x86; **VIA** C3/C7 **Transmeta** Crusoe, Efficeon		
	x86-64	AMD	**Opteron**, Athlon 64 Phenom, Phenom II	64位	2003年起
		Intel	Pentium 4 Prescott, Core 2 Core i3/i5/i7		
		Others	**VIA** Nano		

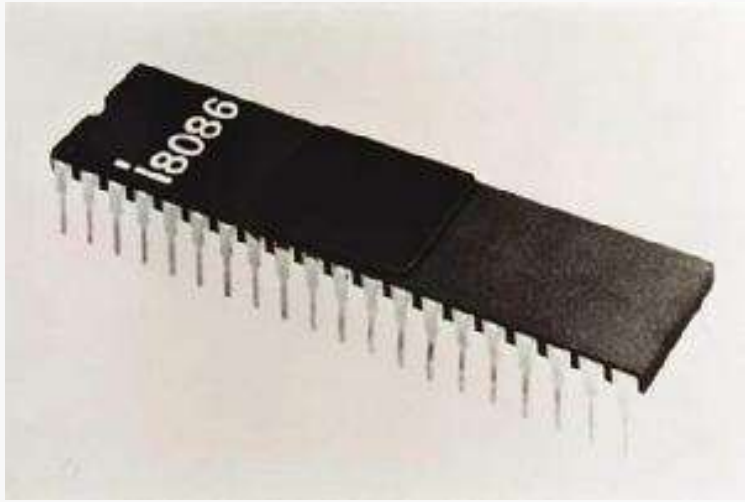
Intel 8086（1978年）

- 8086的主要特点

① 内部的通用寄存器为16位
既能处理16位数据，也能处理8位数据

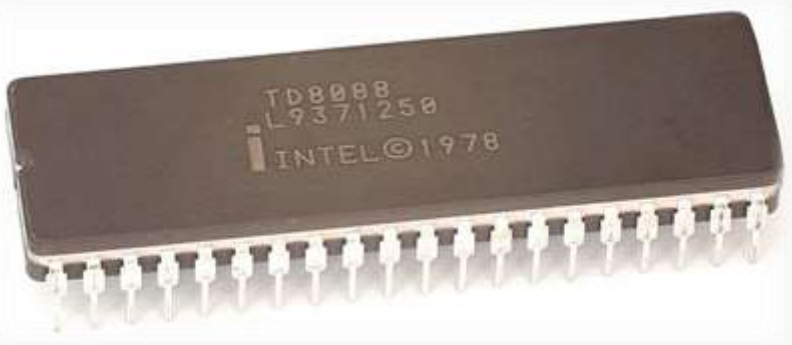
③ 对外有16根数据线和20根地址线
可寻址的内存空间为1MByte（2^{20}）

③ 物理地址的形成采用“段加偏移”的方式



微型计算机的早期代表：IBM PC

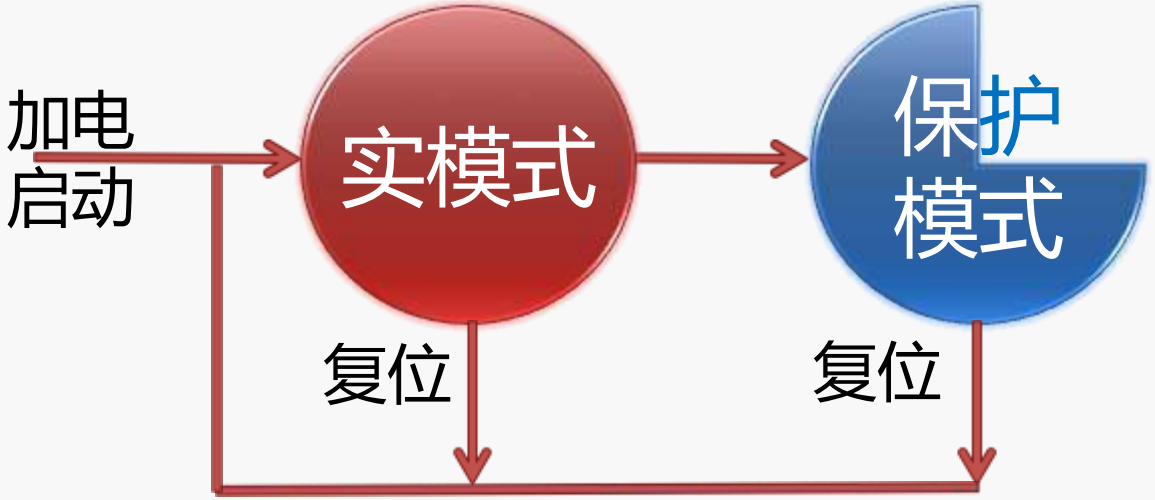
- 1981年，IBM PC 5150诞生
  - 售价约1600美元
  - Intel 8088 CPU，主频4.77MHz，内存16KB
  - 因开放性架构逐渐成为个人计算机的制造标准



Intel 8088 CPU，1979年推出。8088是8086的简化版本，主要区别是数据总线只有8位宽。

Intel 80286（1982年）

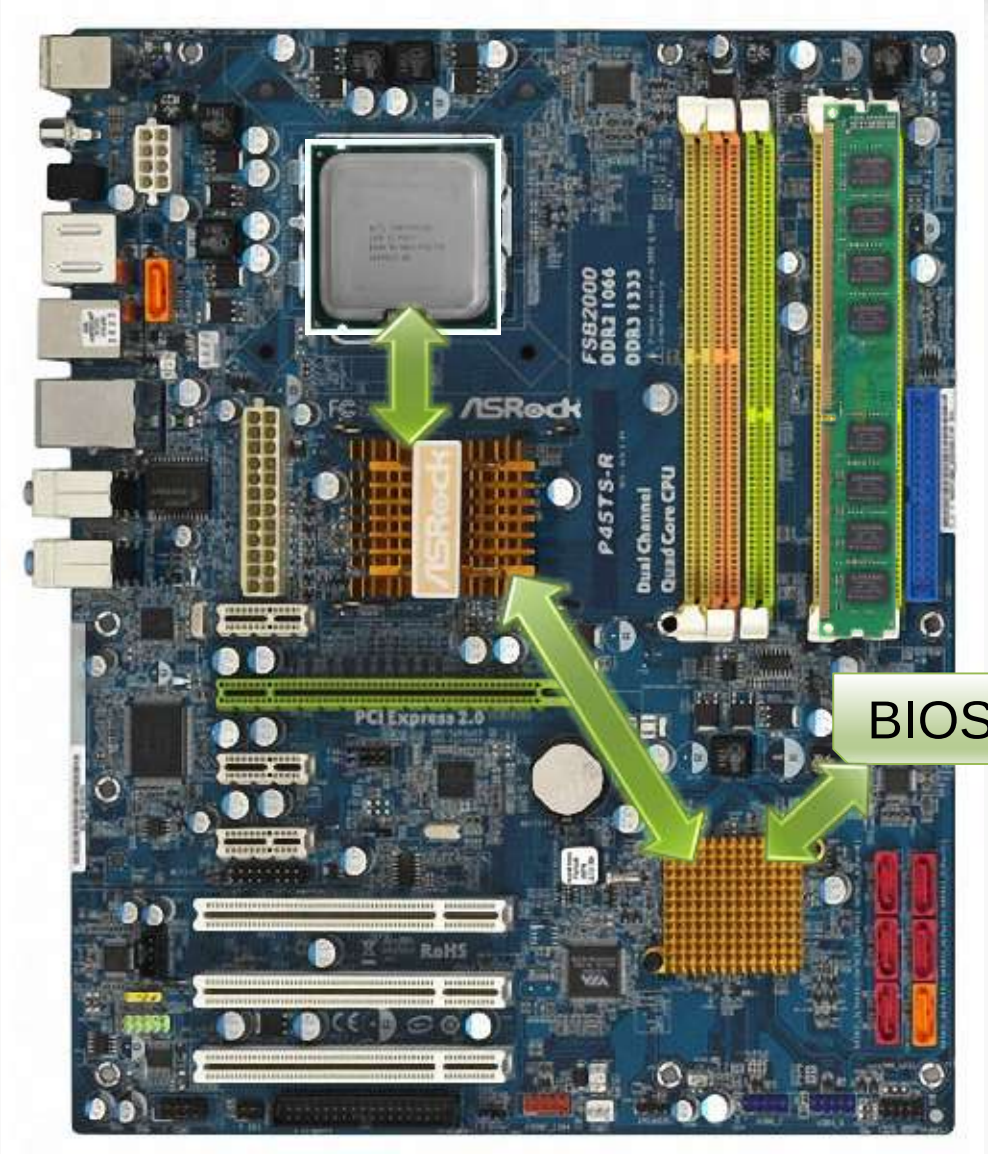
- 80286的主要特点
  - 地址总线扩展到24位，可寻址16MB的内存空间
  - 引入了“保护模式”，但是机制有缺陷
    *例如，每个段仍为64KB，严重限制软件规模
  - 为保持兼容，保留了8086的工作模式，被称为“实模式”



80286
主频6~20MHz
13.4万个晶体管

实模式（Real Mode）

- 实模式，又称“实地址模式”
  - 80286及以上的微处理器采用8086的工作模式，即为**实模式**
  - 运行在实模式下的80x86微处理器像是一个更快的8086
  - 为兼容8086，所有x86处理器在加电或复位后首先进入实模式
  - 系统初始化程序在实模式下运行，为进入保护模式做好准备



x86体系结构

体系结构		厂商	微处理器型号	字长	年代
x86	“x86-16” “IA-16”	Intel	**8086**, 8088, 80186, 80188 80286	16位	1978年起
	IA-32	Intel	**80386**, 80486, Pentium, Pentium Pro/II/III/4, Core, Atom	32位	1985年起
		AMD	Am386, Am486, AM5x86, K5, K6, Athlon		
		Others	**Cyrix** 5x86; **VIA** C3/C7 **Transmeta** Crusoe, Efficeon		
	x86-64	AMD	**Opteron**, Athlon 64 Phenom, Phenom II	64位	2003年起
		Intel	Pentium 4 Prescott, Core 2 Core i3/i5/i7		
		Others	**VIA** Nano		

Intel 80386（1985年）

- 80386的主要特点
  - 80x86系列中的第一款32位微处理器
  - 支持32位的算术和逻辑运算，提供32位的通用寄存器
  - 地址总线扩展到32位，可寻址4GB的内存空间
  - 改进了“保护模式”（例如，段范围可达4GB）
  - 增加了“虚拟8086模式”，可以同时模拟多个8086微处理器

80386
主频12.5~33MHz
27.5万个晶体管

保护模式（Protected Mode）

- 保护模式，可简写为“pmode”
  - 80386及以上的微处理器的主要工作模式
  - 支持多任务
  - 支持设置特权级
  - 支持特权指令的执行
  - 支持访问权限检查
  - 可以访问4GB的物理存储空间
  - 引入了虚拟存储器的概念

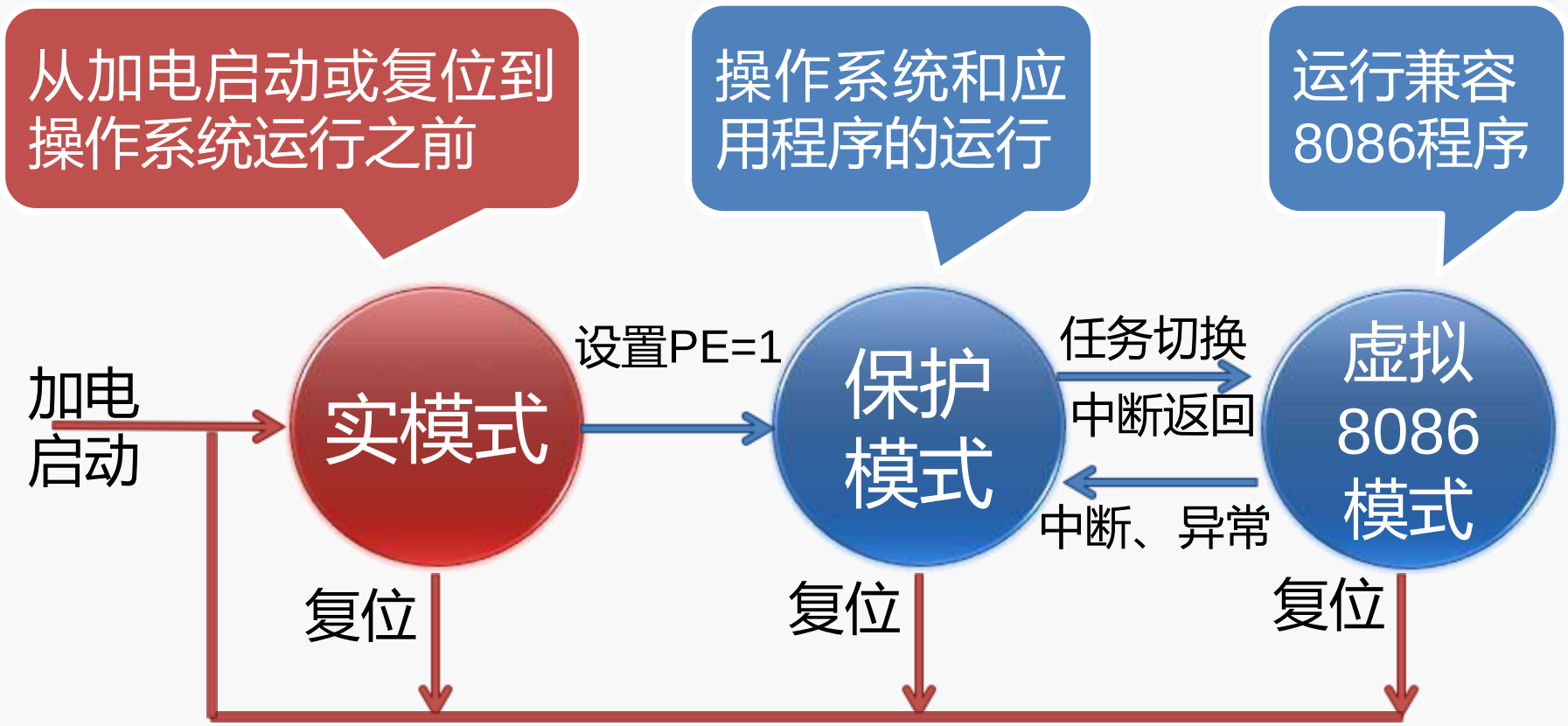
保护模式让操作系统加强了对应用软件的控制，使得系统运行更安全高效

虚拟8086模式（Virtual 8086 Mode）

- 虚拟8086模式，又称“V86模式”
  - V86模式实际上是保护模式下一种特殊工作状态
  - V86模式下的微处理器类似于8086，但不等同

- V86模式 与 实模式 的比较
  - 相同点
    - 可寻址的内存空间为1MB
    - “段加偏移”的寻址方式
  - 不同点
    - 对中断/异常的响应处理

三种工作模式之间的转换



*注：PE即“保护模式允许”，是80x86控制寄存器CR0中的控制位

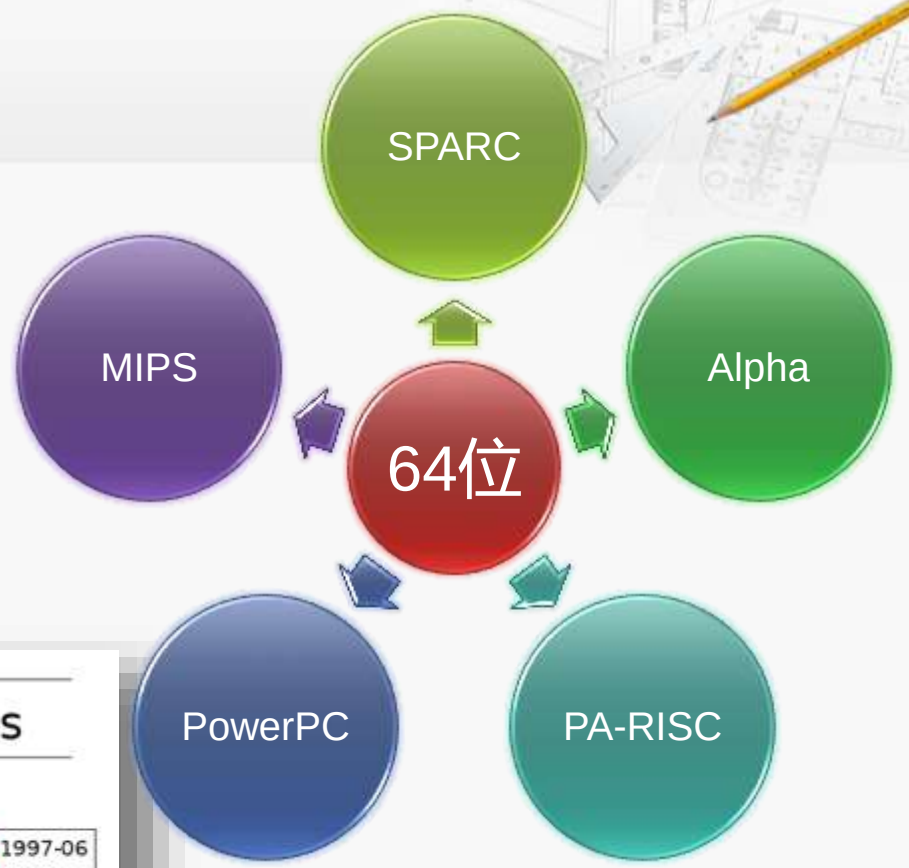
x86体系结构

体系结构		厂商	微处理器型号	字长	年代
x86	“x86-16” “IA-16”	Intel	**8086**, 8088, 80186, 80188 80286	16位	1978年起
	IA-32	Intel	**80386**, 80486, Pentium, Pentium Pro/II/III/4, Core, Atom	32位	1985年起
		AMD	Am386, Am486, AM5x86, K5, K6, Athlon		
		Others	**Cyrix** 5x86; **VIA** C3/C7 **Transmeta** Crusoe, Efficeon		
	x86-64	AMD	**Opteron**, Athlon 64 Phenom, Phenom II	64位	2003年起
		Intel	Pentium 4 Prescott, Core 2 Core i3/i5/i7		
		Others	**VIA** Nano		

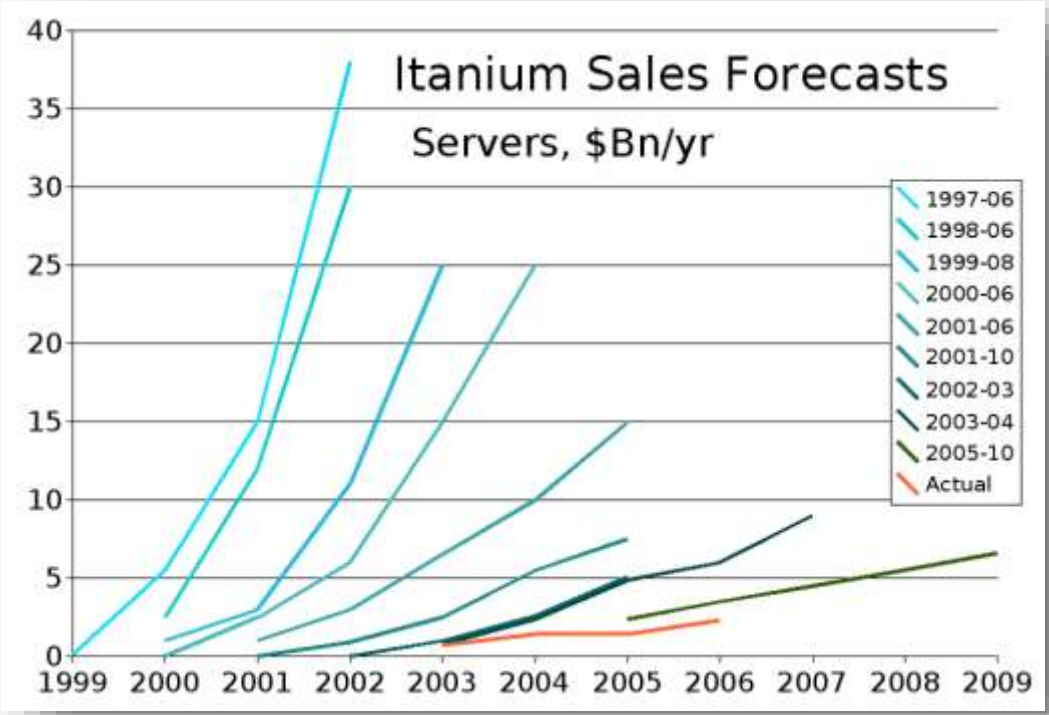
注：Intel提出的IA-64是独立于x86的一种新的体系结构，不兼容IA-32

AMD Opteron（2003年）

- Opteron的主要特点
  - x86扩展到64位的第一款微处理器
  - 可以访问高于4GB的存储器
  - 兼容32位x86程序，且不降低性能



Opteron
主频1.4~3.5GHz
工艺130~32nm



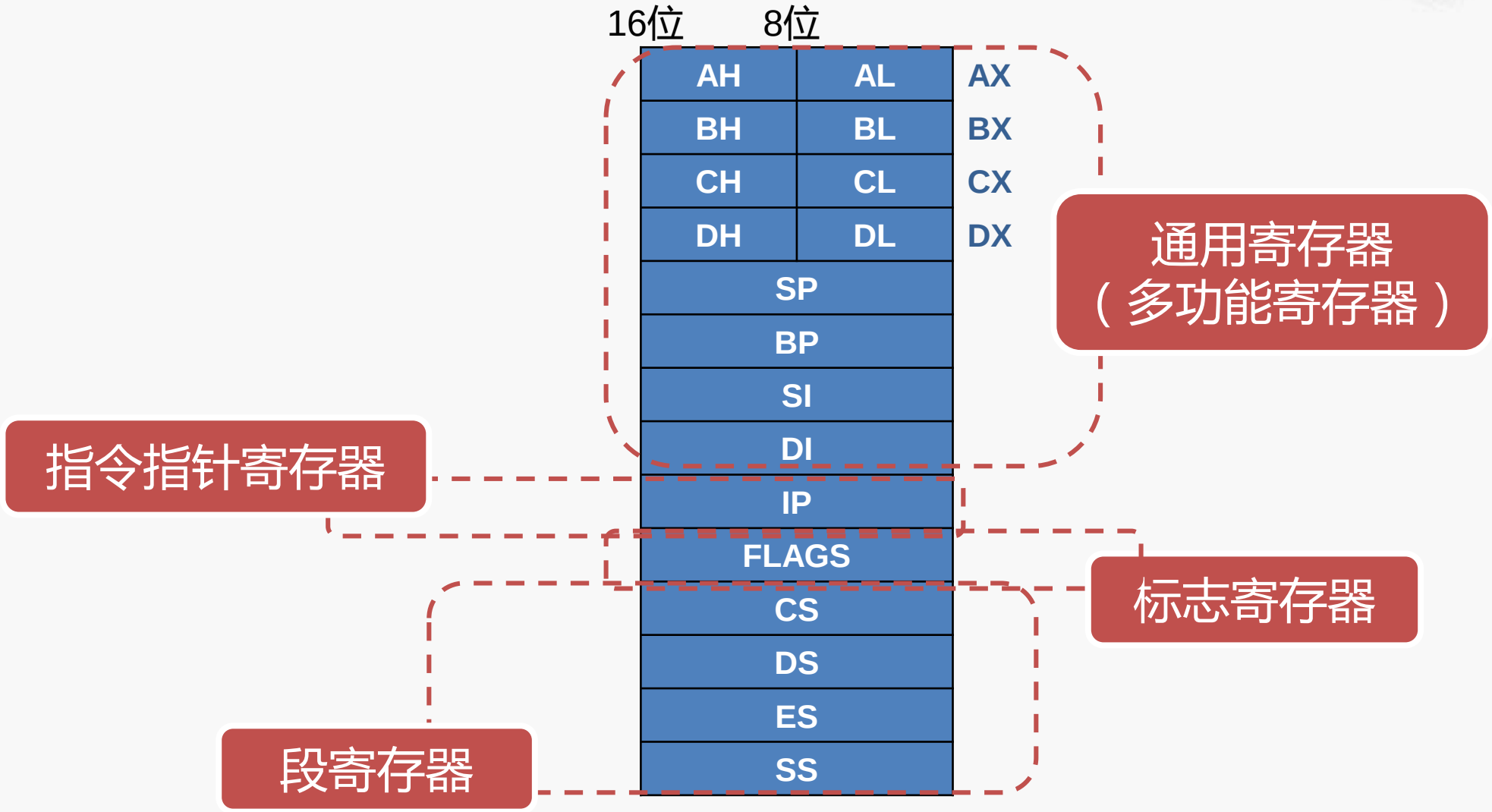
Intel Italium

x86-64的运行模式

运行模式	运行子模式	操作系统	已有程序的支持
长模式 Long mode	64位模式 64-bit mode	64位	需重新编译
	兼容模式 Compatibility mode	64位	不需要重新编译
传统模式 Legacy mode	保护模式 Protected mode	32位或16位	不需要重新编译
	虚拟8086模式 Virtual 8086 mode	32位或16位	不需要重新编译
	实模式 Real mode	16位	不需要重新编译

从16位到64位：x86体系结构的演变

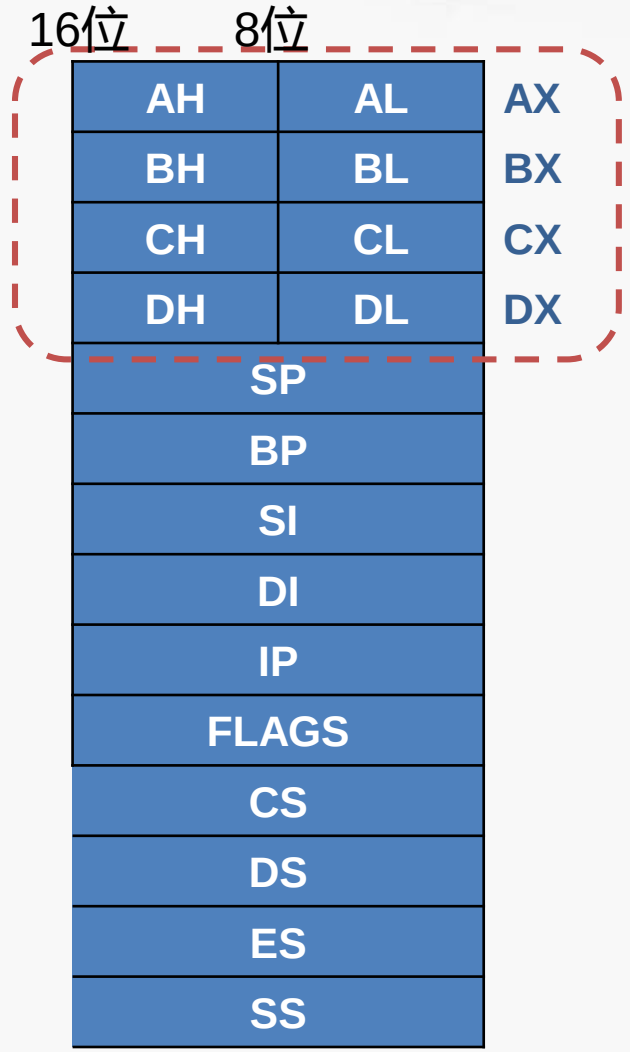
8086的寄存器模型


16位
8位
AH
AL
AX
BH
BL
BX
CH
CL
CX
DH
DL
DX
SP
BP
SI
DI
IP
FLAGS
CS
DS
ES
SS
通用寄存器
（多功能寄存器）
指令指针寄存器
标志寄存器
段寄存器

通用寄存器（多功能寄存器）（1）

- 数据寄存器，共有4个
  - 均为16位寄存器
  - 每个16位寄存器都可分为两个8位寄存器使用
  - 适用大多数算术运算和逻辑运算指令
  - 除存放通用数据外，各有一些专门的用途：

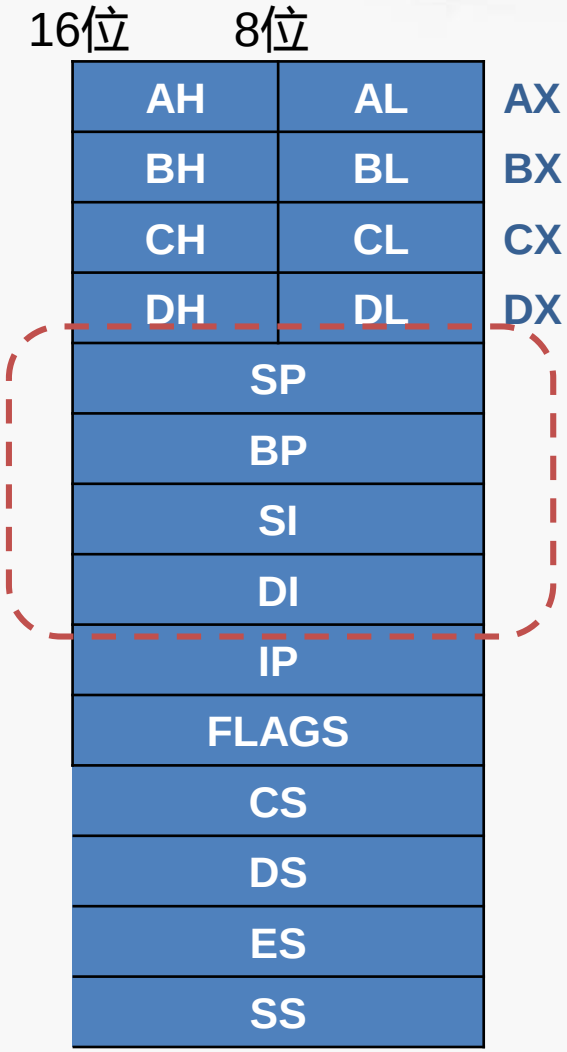
AX	Accumulator	存放乘除等指令的操作数
BX	Base	存放存储单元的偏移地址
CX	Count	存放计数值
DX	Data	乘法运算产生的部分积 除法运算的部分被除数



通用寄存器（多功能寄存器）（2）

- 指针和变址寄存器，共有4个，分为两组
  - 均为16位寄存器
  - SP和BP用于堆栈操作
  - SI和DI用于串操作
  - 都可以作为数据寄存器使用

SP	stack pointer	堆栈指针寄存器
BP	(stack)base pointer	(堆栈)基址指针寄存器
SI	source index	源变址寄存器
DI	destination index	目的变址寄存器

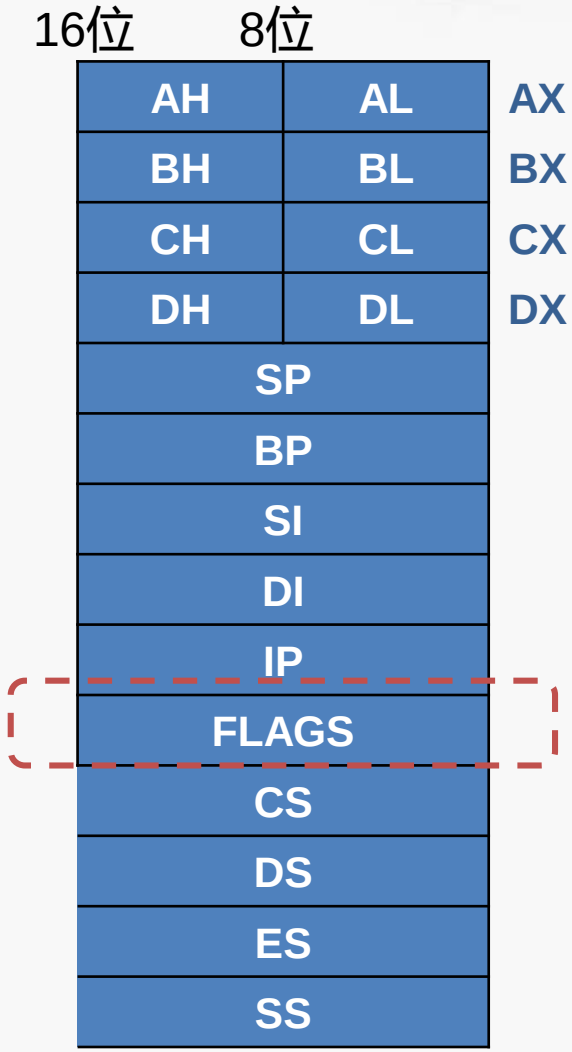


标志寄存器

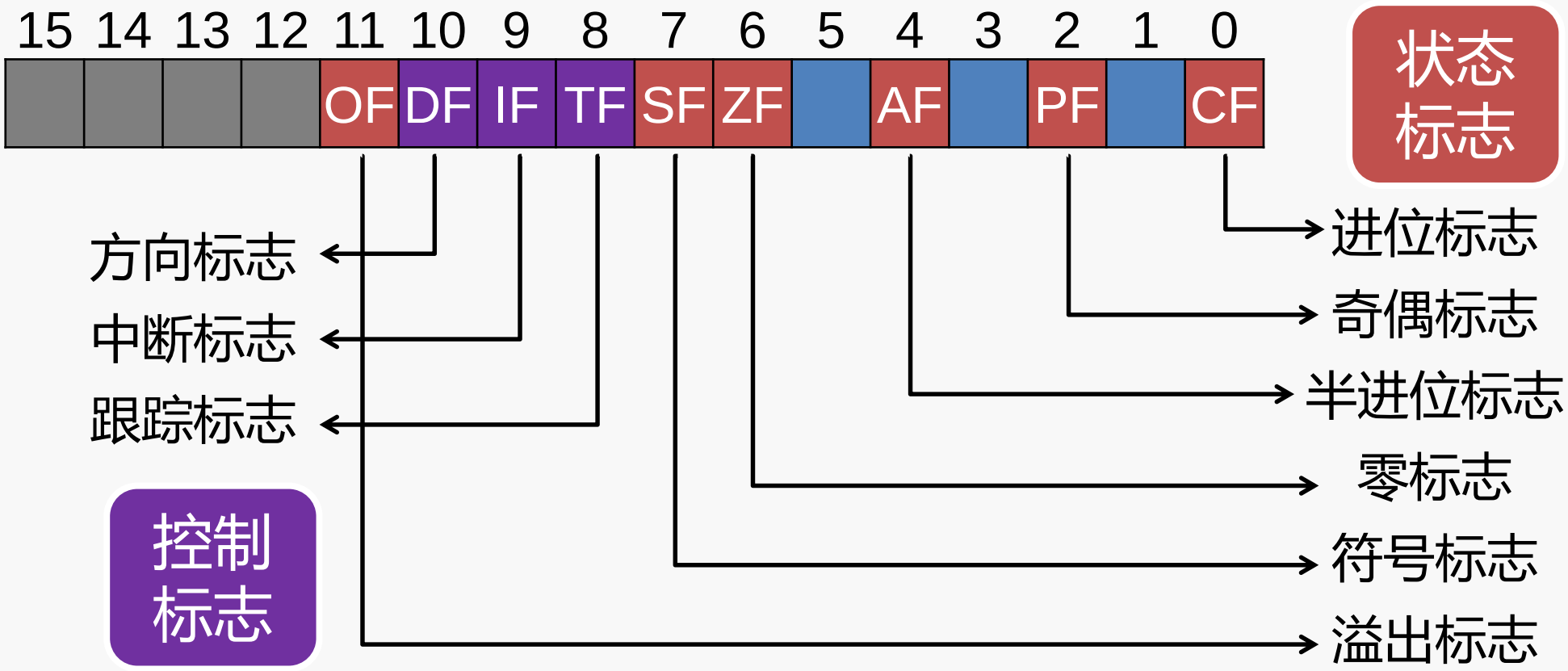
- **标志位**
  - FLAGS寄存器中包含若干标志位
  - 标志位分为两大类：状态标志和控制标志
- **状态标志** 反映CPU的工作状态

  例如：
  - 执行加法运算时是否产生进位
  - 运算结果是否为零
- **控制标志** 对CPU的运行起特定控制作用

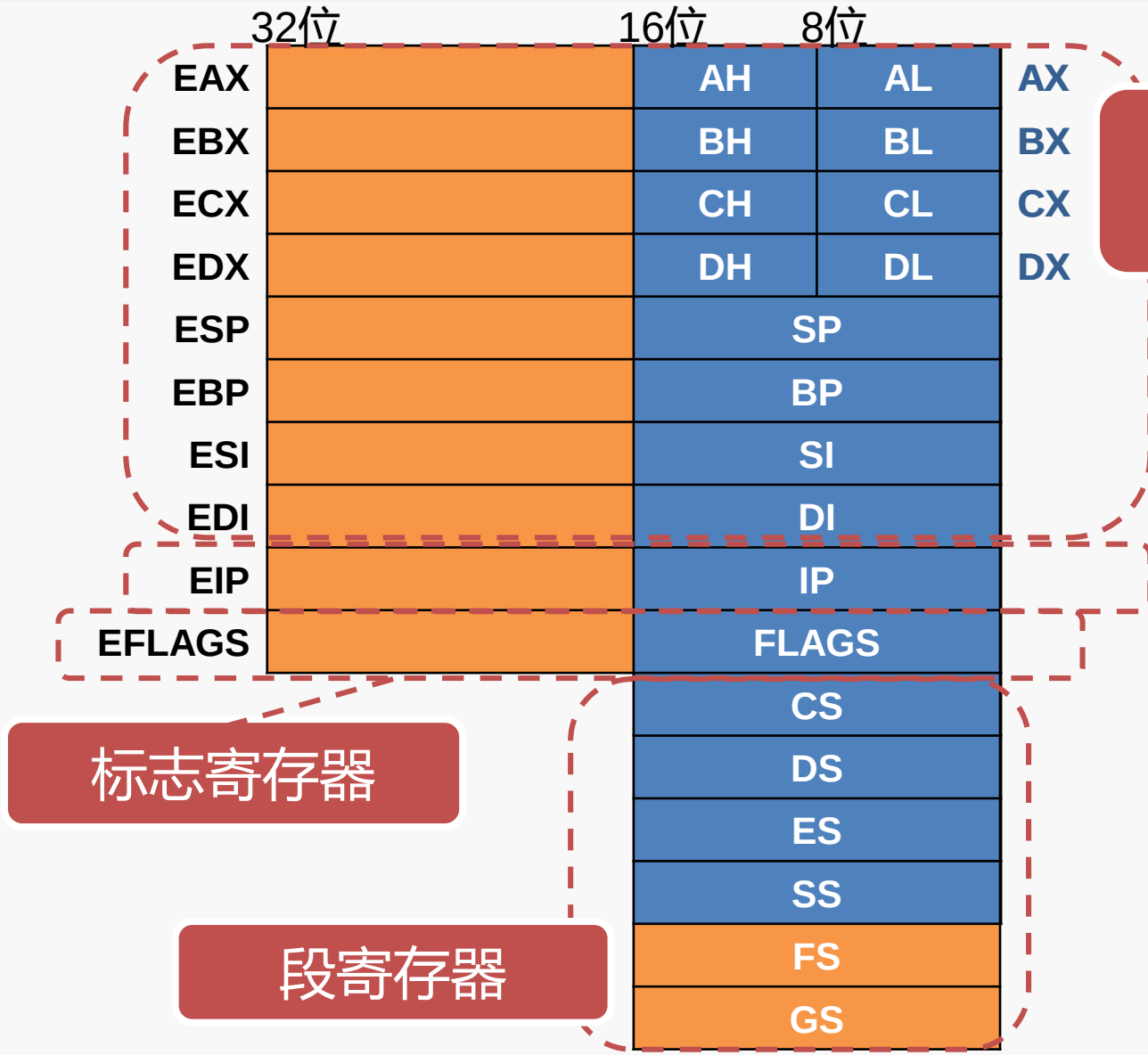
  例如：
  - 以单步方式还是连续方式运行
  - 是否允许响应外部中断请求



8086的标志位


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
状态标志
进位标志
奇偶标志
半进位标志
零标志
符号标志
溢出标志
方向标志
中断标志
跟踪标志
控制标志

IA-32的寄存器模型



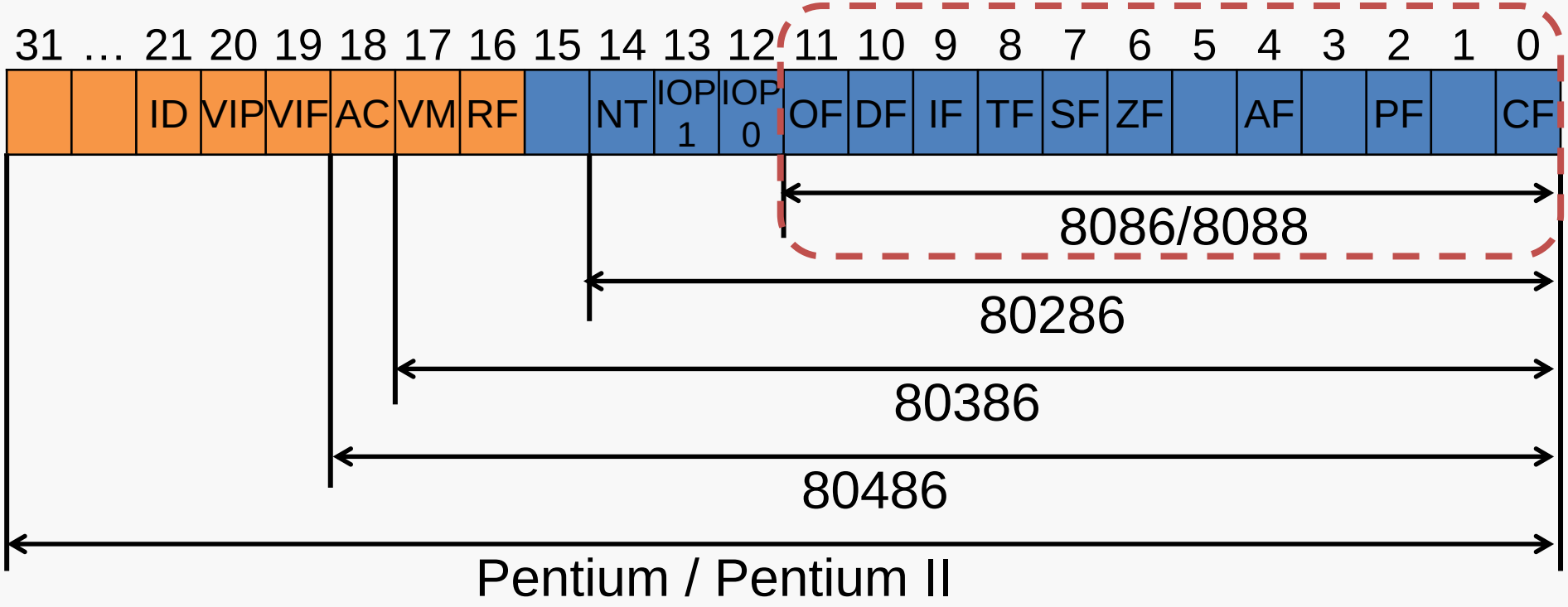
说明

代表IA-32寄存器模型的新增部分

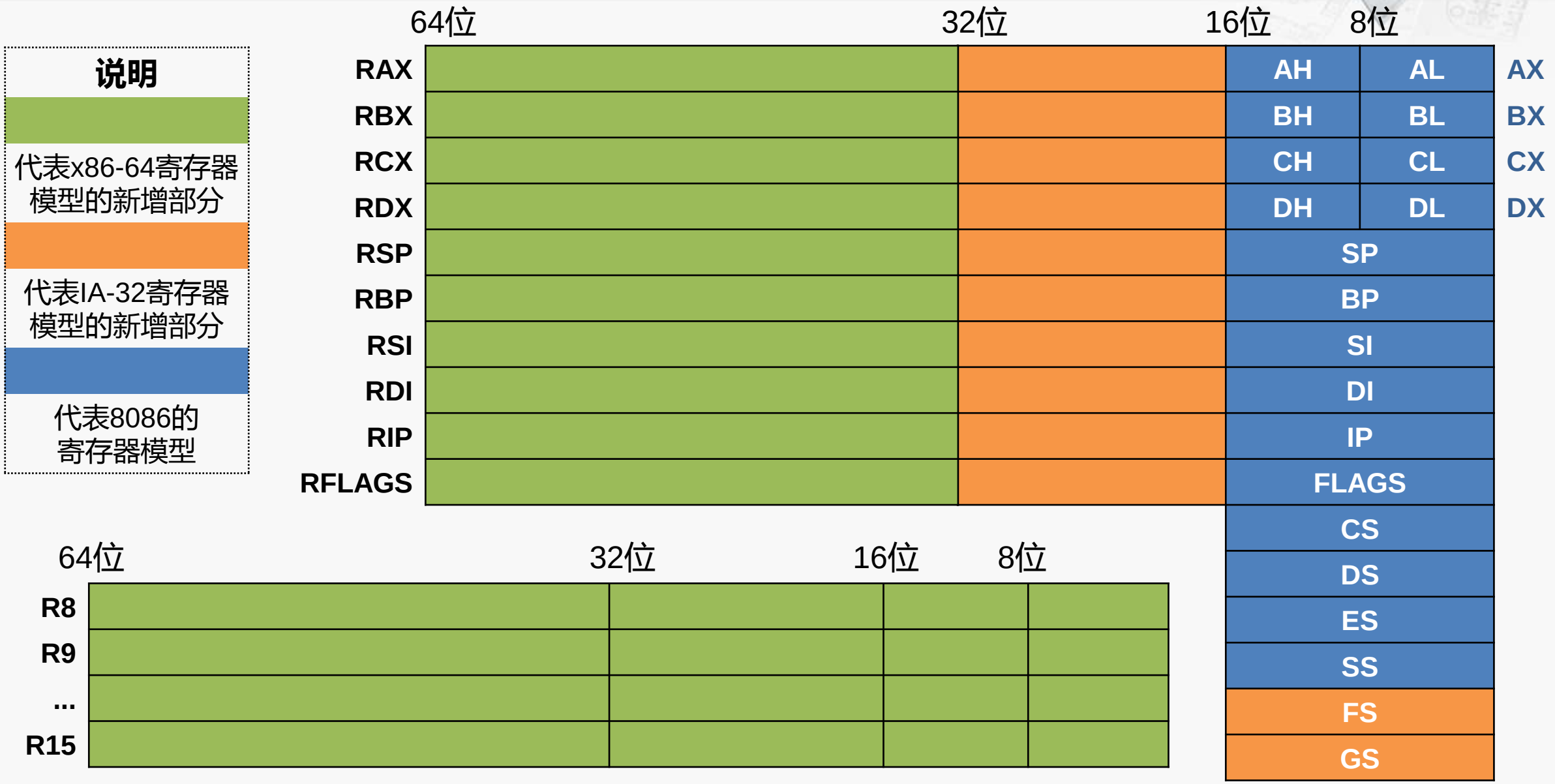
代表8086的寄存器模型

标志寄存器的说明

- 标志寄存器EFLAGS/FLAGS
  - 用于指示微处理器的状态并控制它的操作
  - 标志寄存器的内容在不断扩充



x86-64的寄存器模型



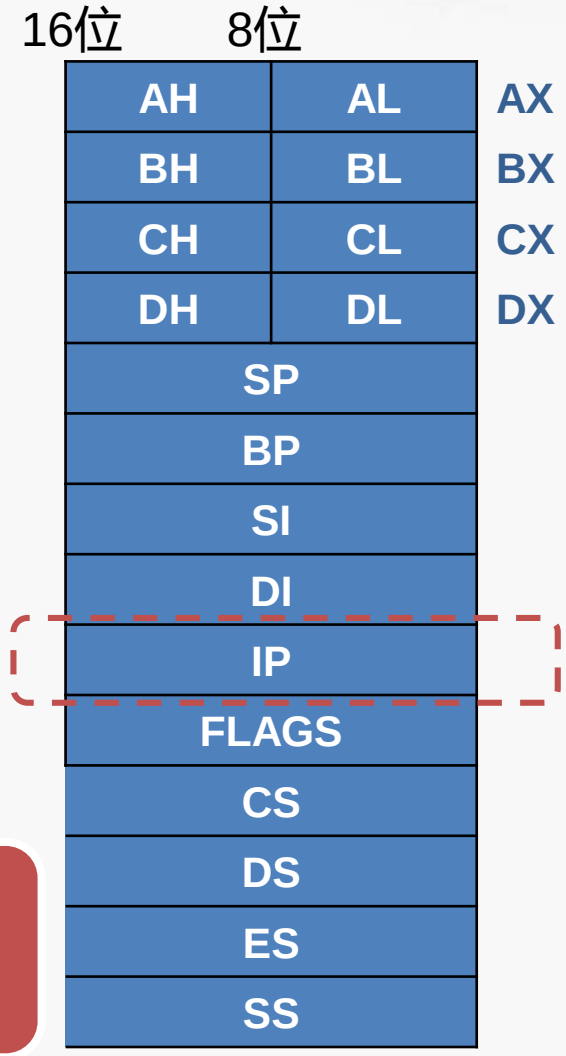
从16位到64位：x86体系结构的演变

寄存器模型

存储器寻址

8086的指令指针寄存器

- 指令指针寄存器 IP（Instruction Pointer）
  - 保存一个内存地址，指向当前需要取出的指令
  - 当CPU从内存中取出一个指令后，IP会自动增加，指向下一指令的地址（注：实际情况会复杂的多）
  - 程序员不能直接对IP进行存取操作
  - 转移指令、过程调用/返回指令等会改变IP的内容



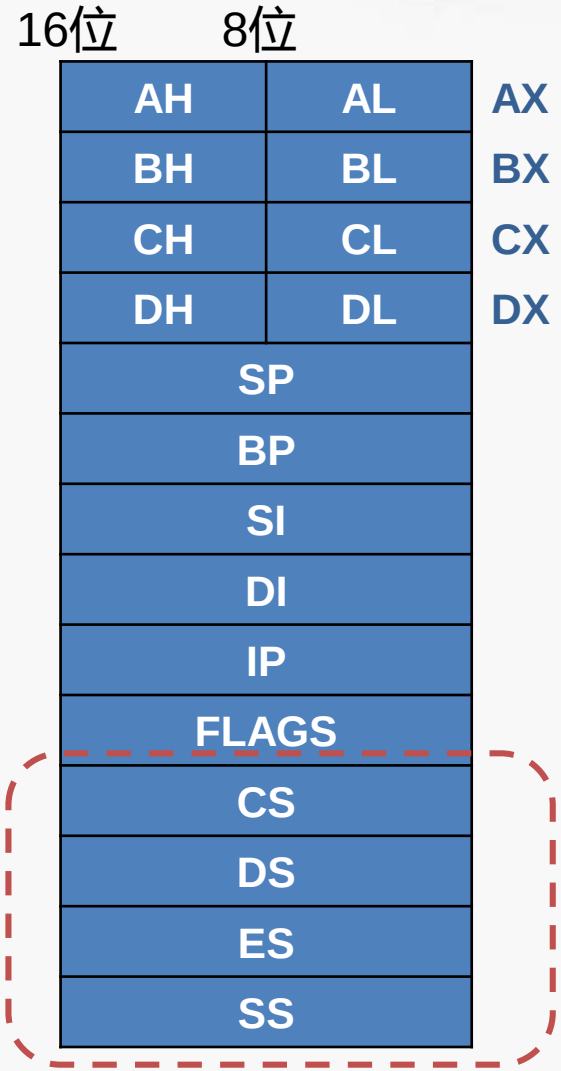
IP寄存器的寻址能力：
2^{16}=65536(64K)字节单元

8086对外有20位地址线
寻址范围：2^{20}=1M字节单元

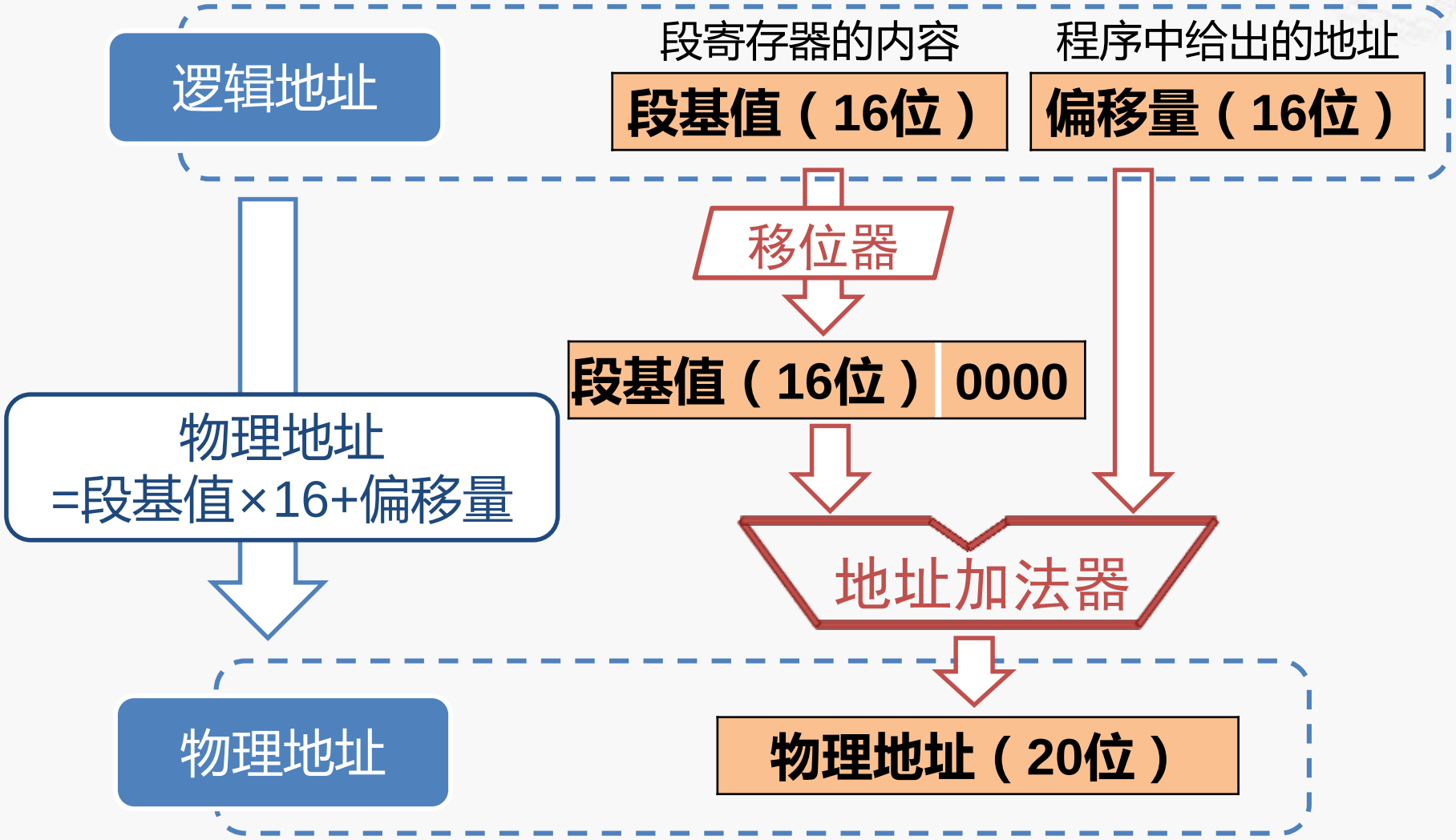
8086的段寄存器

- 段寄存器（Segment Register）
  - 与其它寄存器联合生成存储器地址

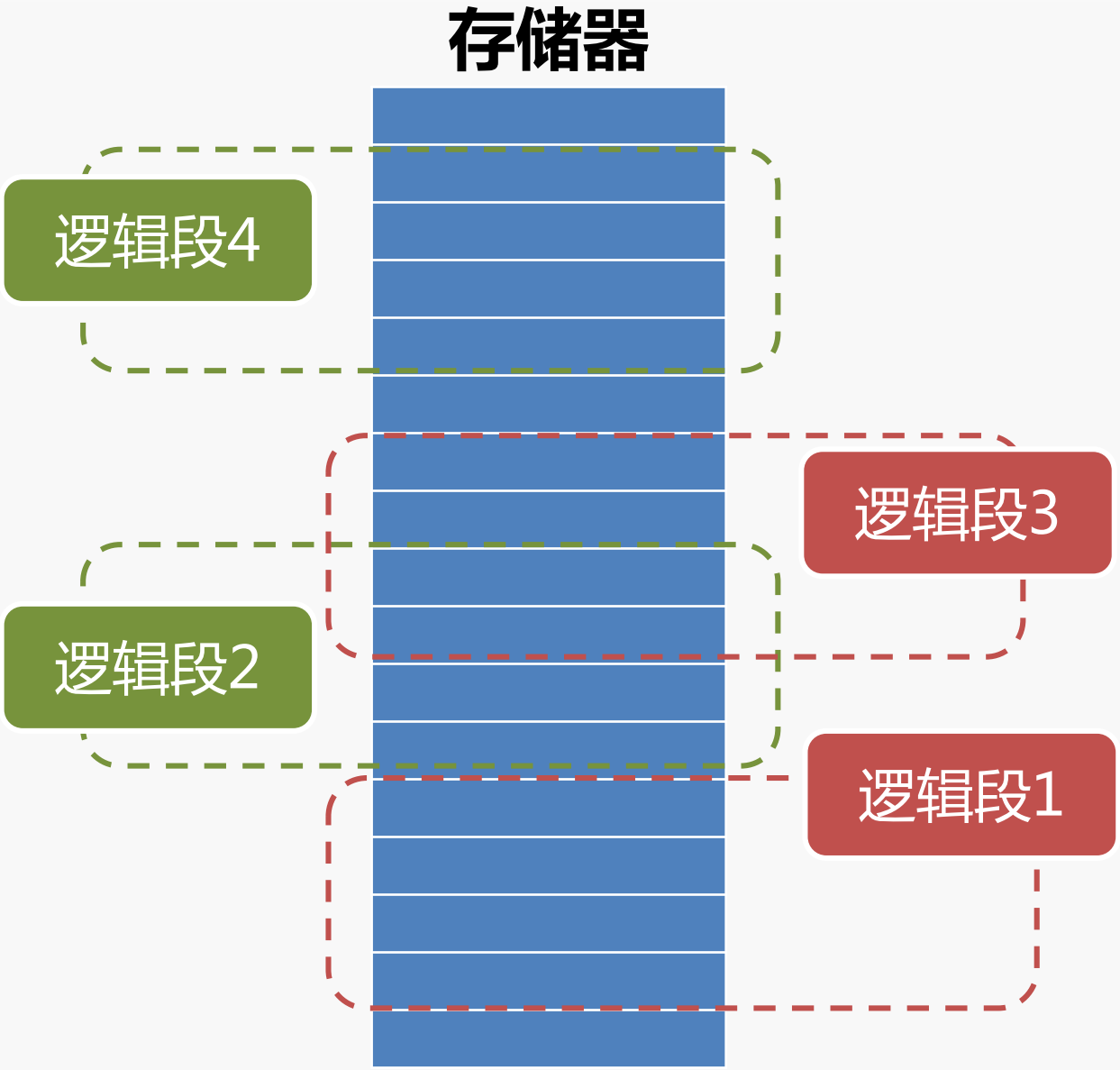
CS	代码段寄存器（Code Segment）
DS	数据段寄存器（Data Segment）
ES	附加段寄存器（Extra Segment）
SS	堆栈段寄存器（Stack Segment）



8086的物理地址生成



逻辑段在物理存储器中的位置

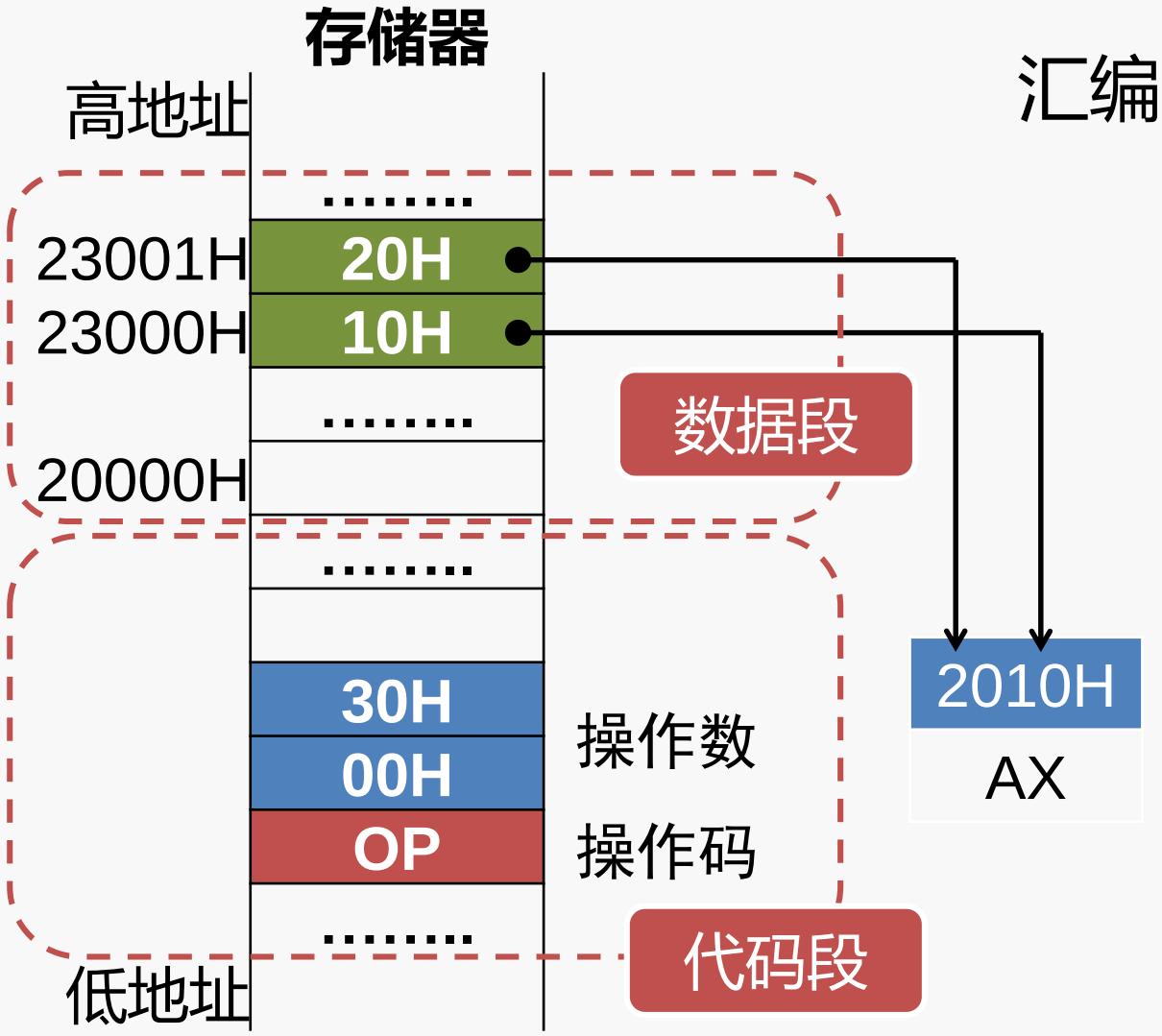


1M字节的存储空间分成许多逻辑段，每段最长64K字节，可以用16位地址进行寻址

编程时使用逻辑地址，不需要知道代码或数据在存储器中的具体物理位置，从而简化存储资源的管理

各个逻辑段在实际存储空间中可以完全分开，也可以部分重叠，甚至完全重叠

“段加偏移”的编程实例



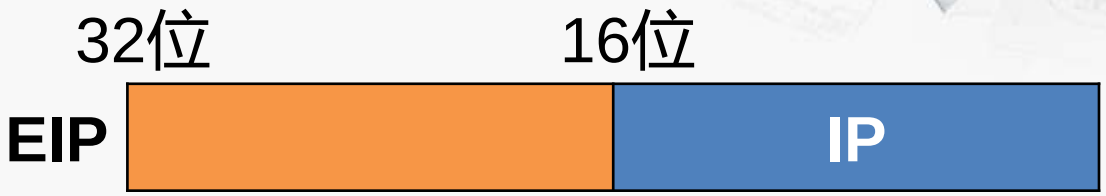
汇编指令 MOV AX, [3000H]

操作数默认存放在DS指向的数据段中，即[3000H]=DS:[3000H]

设：DS=2000H，
则：物理地址
=2000H×16+3000H
=23000H

IA-32的存储器寻址

以指令的寻址为例



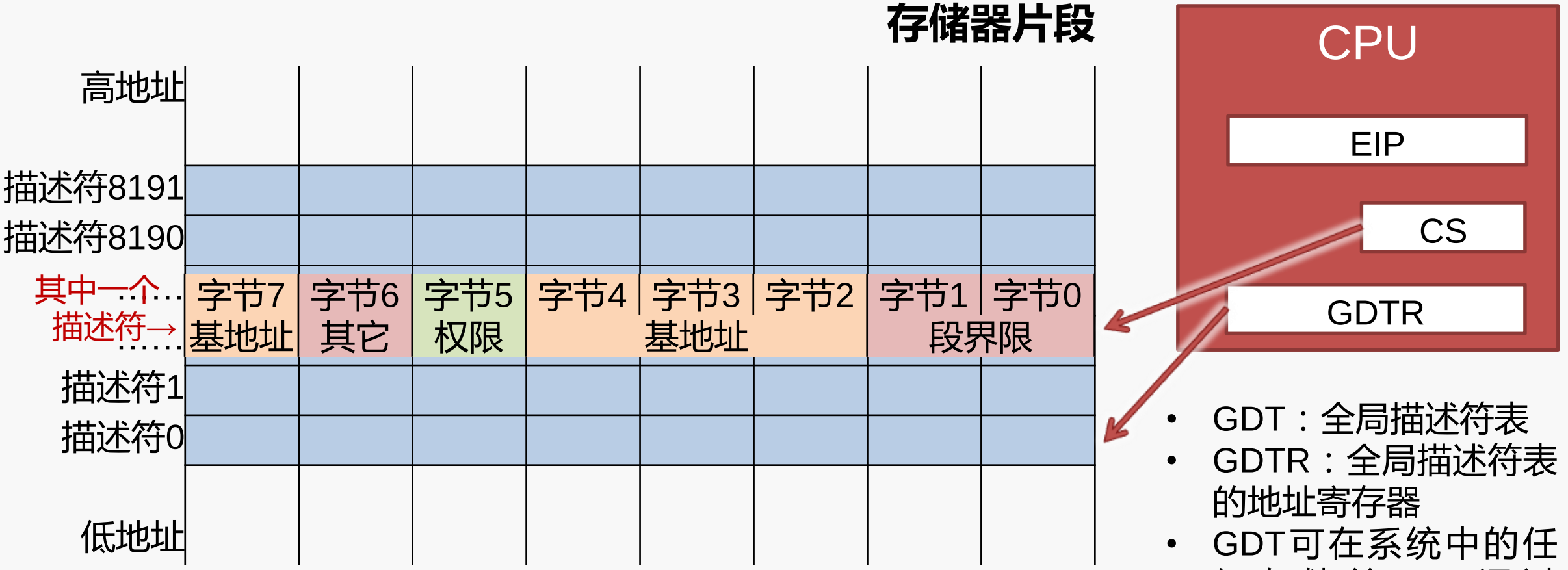
- 实模式 CS:IP
- 保护模式 CS:EIP

EIP寄存器的寻址能力：
2^{32}=4G字节单元

80386对外有32位地址线
寻址范围：2^{32}=4G字节单元

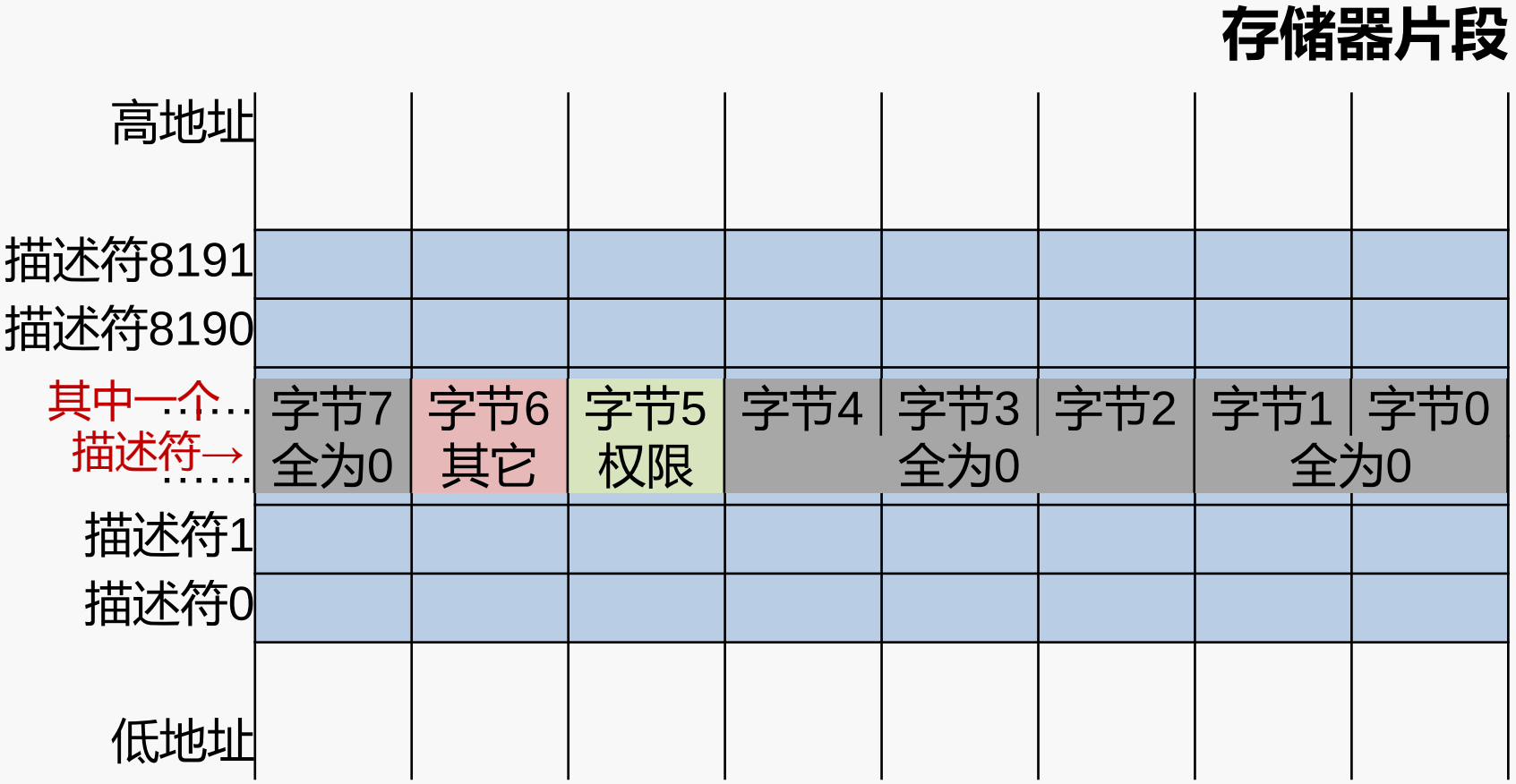
IA-32的存储器寻址

- 保护模式下，段基址不在CS中，而是在内存中



- GDT：全局描述符表
- GDTR：全局描述符表的地址寄存器
- GDT可在系统中的任何存储单元，通过GDTR定位

x86-64的描述符



注：描述符中没有了段基址和段界限，只有访问权限字节和若干控制位。所有的代码段都从地址0开始。

本节小结

x86体系结构

北京大学·慕课
计算机组成
制作人：陆俊林