

本节主题



中断向量表的发展

北京大学·慕课
计算机组成
制作人：陆俊林





实模式下的存储器地址空间

🕒 地址范围：00000H~FFFFFFH，共1M字节

存储器地址	存储器	说明
FFFFFFH		专用区（16字节）：初始化代码区 CPU复位后从地址FFFF0H取出第一条指令，通常是一条无条件转移指令，转移到系统程序的入口处
FFFF0H		
FFFEFH		通用区 用来存储一般的程序指令和数据
00400H		
003FFH		专用区（1 K字节）：中断向量表区 存放256个中断服务程序的入口地址（也称中断向量），每个入口地址占4个字节单元
00000H		



8086的中断向量表

中断用途	类型号	说明
供用户定义的中断 (224个)	类型255	
	
	类型32	
保留的中断 (27个)	类型31	
	
	类型5	
专用的中断 (5个)	类型4	溢出
	类型3	断点
	类型2	非屏蔽
	类型1	单步
	类型0	除法错



80386 ~ Core2的中断向量表

中断用途	类型号	说明	类型号	说明
专用的中断 (19个)	类型9	协处理器段超限		
	类型8	双中断错	类型18	机器检查**
	类型7	协处理器不存在	类型17	对齐检查**
	类型6	未定义的操作码	类型16	协处理器出错*
	类型5	边界	类型15	未分配
	类型4	溢出	类型14	页面出错*
	类型3	断点	类型13	一般性保护
	类型2	非屏蔽	类型12	堆栈段超限
	类型1	单步	类型11	段不存在
	类型0	除法错	类型10	无效任务状态段

中断用途	类型号
供用户定义的中断 (224个)	类型255

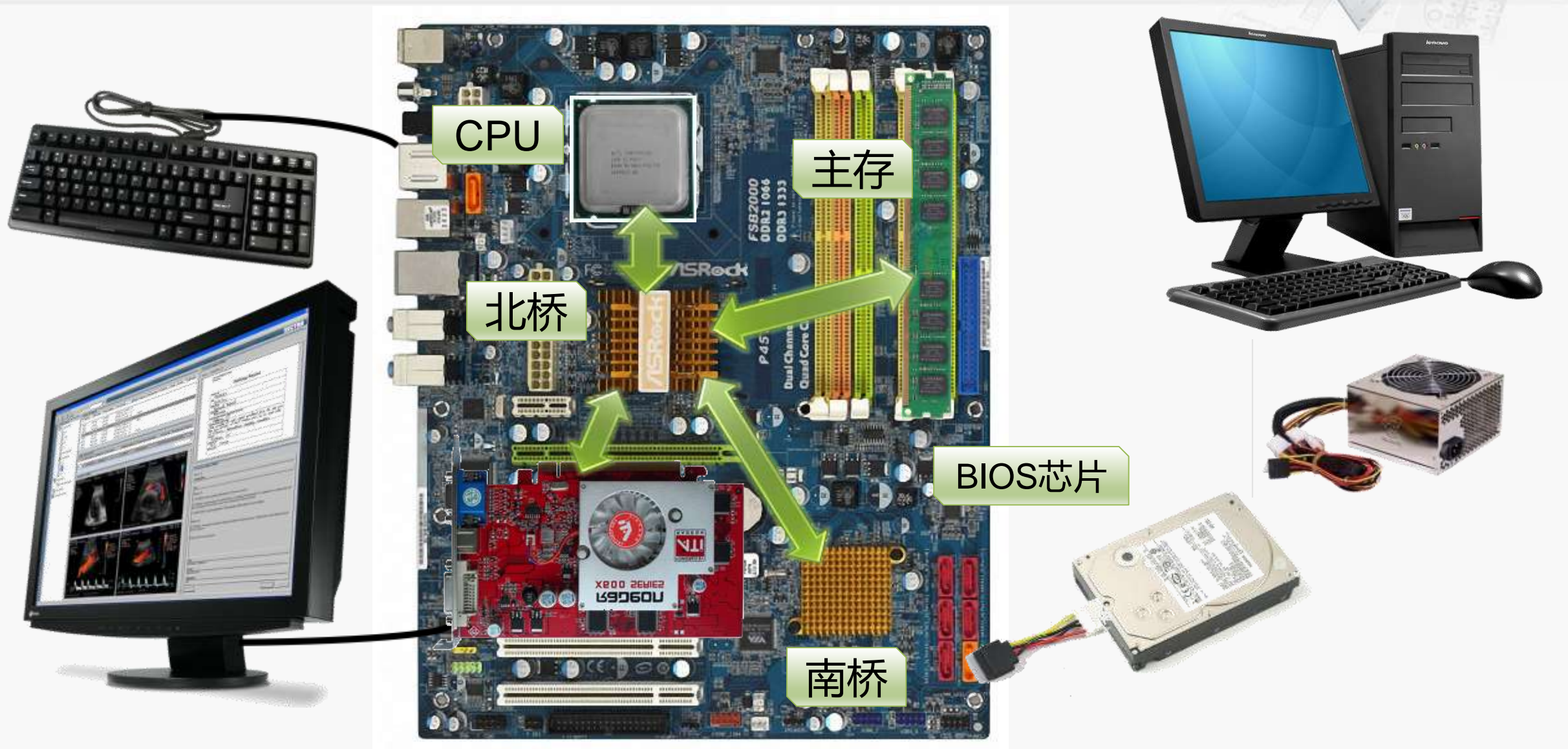
	类型32
保留的中断 (13个)	类型31

	类型19

* 自80386起

**自80486起

中断向量表存放的位置

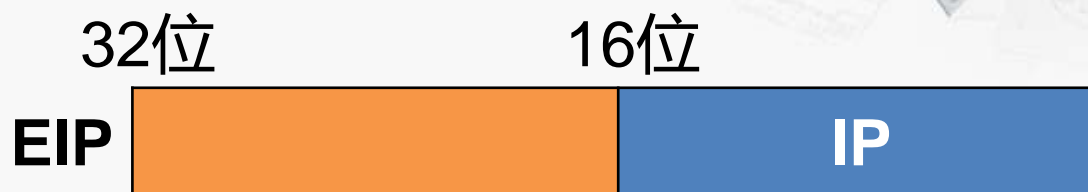


IA-32的存储器寻址

以指令的寻址为例

❶ 实模式 CS:IP

❷ 保护模式 CS:EIP



EIP寄存器的寻址能力：
 $2^{32}=4\text{G}$ 字节单元

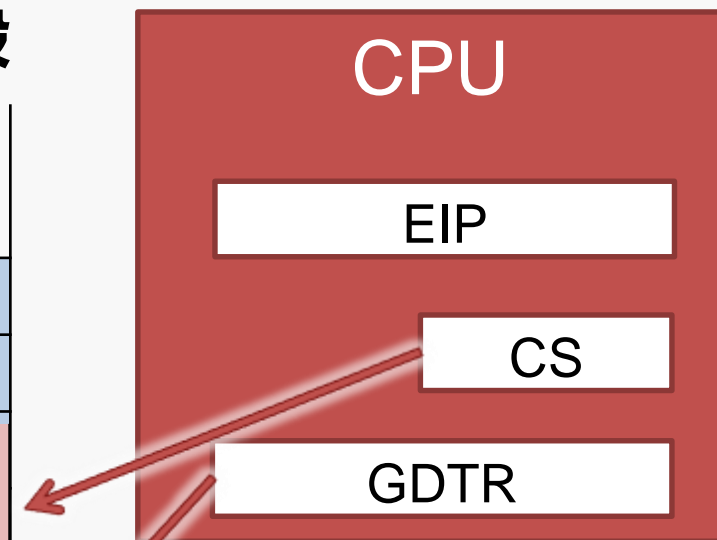
80386起对外有32位地址线
寻址范围： $2^{32}=4\text{G}$ 字节单元

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
存储器片段

CS在这里提供一种索引的功能

高地址								
描述符8191								
描述符8190								
其中一个... 描述符→	字节7 基地址	字节6 其它	字节5 权限	字节4	字节3 基地址	字节2	字节1 段界限	字节0
描述符1								
描述符0								
低地址								



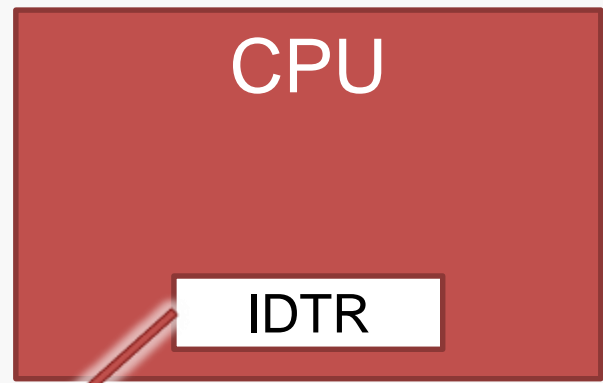
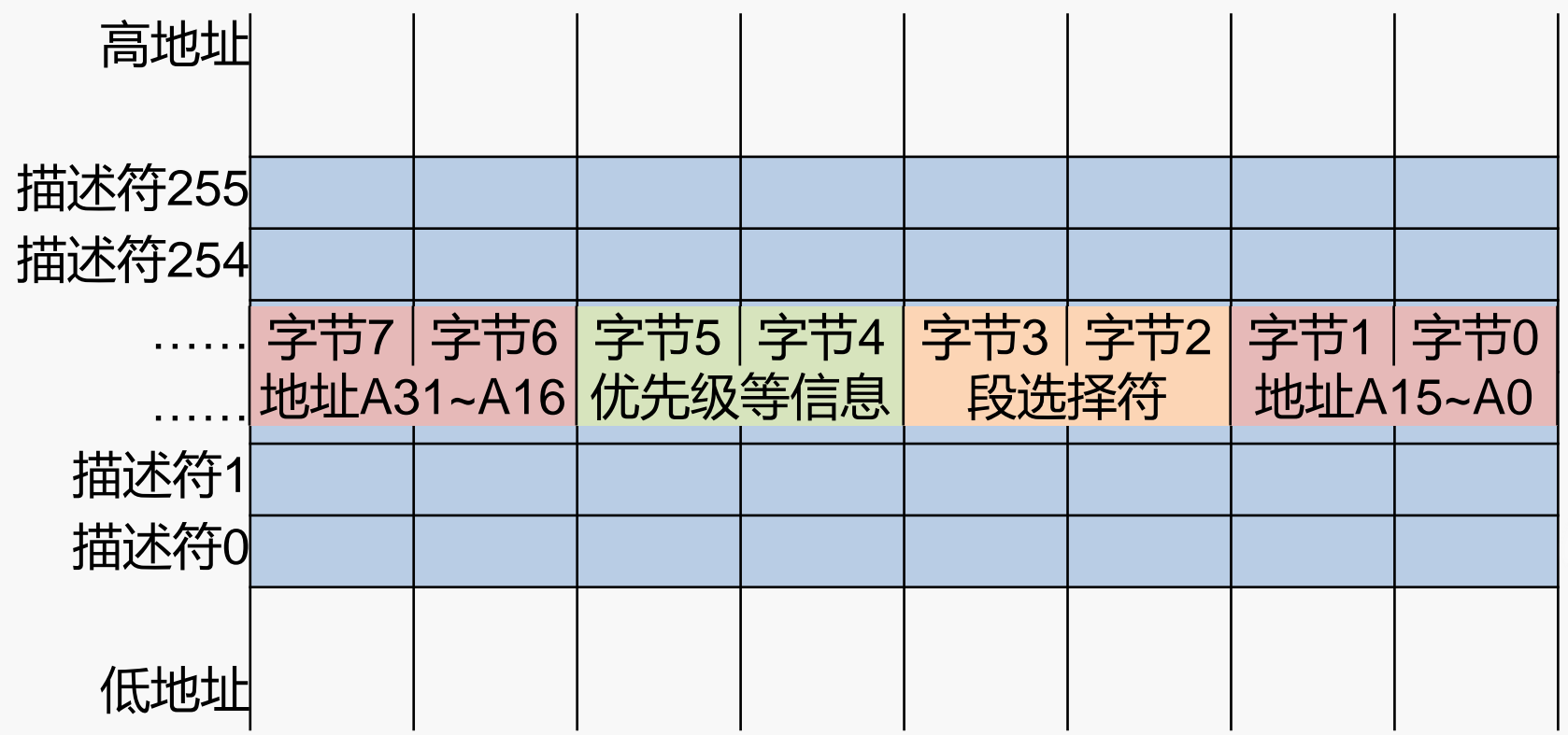
- GDT：全局描述符表
- GDTR：全局描述符表的地址寄存器
- GDT可在系统中的任何存储单元，通过GDTR定位



保护模式的中断操作

中断向量表位置不同，其它操作与实模式类似

存储器片段



IDTR：中断描述符表地址寄存器

IDT可在系统中的任何存储单元，通过IDTR定位

中断描述符表 (interrupt descriptor table , IDT)
每个中断描述符8个字节，256个中断描述符共2K字节

本节小结



中断向量表的发展

北京大学·慕课
计算机组成
制作人：陆俊林

