微型计算机原理与接口技术

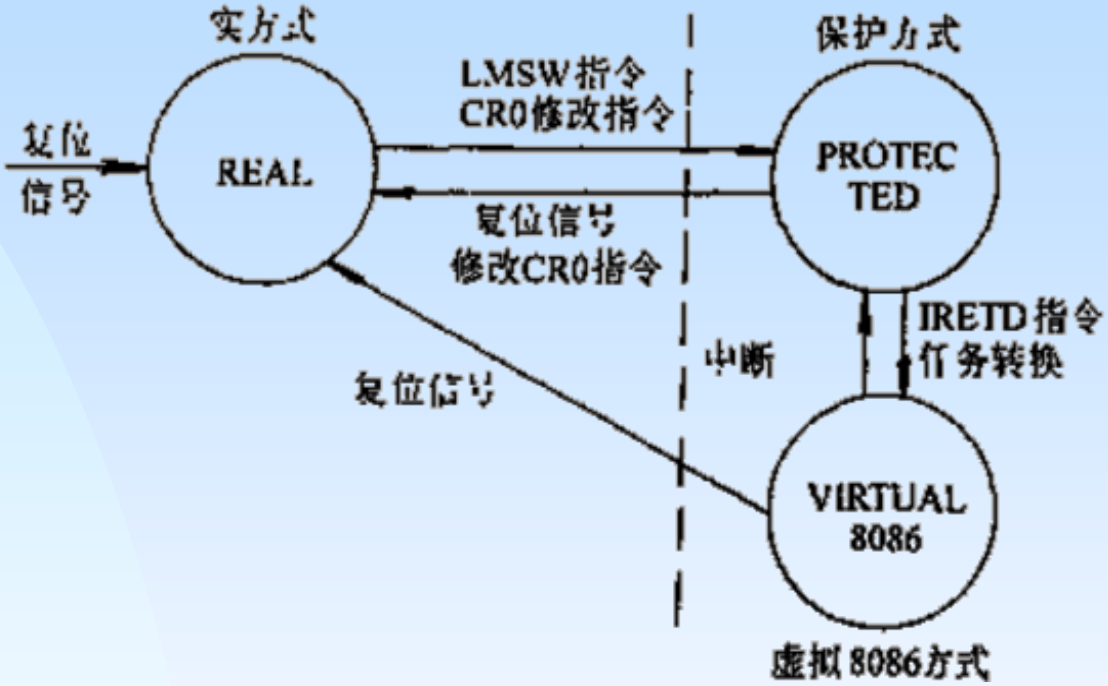
（第九讲）

4.2.3 80386/80486的工作方式

三种工作方式：

- 实地址方式(REAL)：CPU上电或复位后自动工作在实地址方式，与8086工作方式基本相同，只能在1MB范围内寻址，段的最大长度为64KB；
- 保护虚拟地址方式(PROTECTED)：可以访问物理存储器空间为4GB(32位)，程序可用的虚拟地址空间64TB(46位)；MMU由分段部件和分页部件组成，分页功能可选，段的长度为4GB(分页)或1MB(不分页)；每个任务有不同的虚拟空间，不同任务间相互隔离，受到保护；
- 虚拟8086方式(VIRTUAL 8086)：是一种模拟8086方式，可寻址最大存储空间1MB，本质上是在虚拟存储器、保护和多任务操作等概念支持下的一个运行任务的工作方式，允许386/486生成多个8086处理器的映像；

- 三种工作方式在以一定条件下可以相互转换：



① CPU复位后，自动进入实地址方式，启动地址FFFF0H；

② 修改控制寄存器CR_0的机器状态字PE=1（MOV CR_0, Reg，或LMSW）可使CPU进入保护方式；

③ 除复位信号，还可以用修改控制寄存器CR_0状态字的方法，使CPU由保护方式转变为实地址方式；

④ 执行IRETD指令或进行任务转换，可从保护方式转变为虚拟8086方式；

⑤ 虚拟8086任务结束或触发中断时，转变为保护方式；

4.2.4 80386/80486的存储器管理

(1) 保护虚地址方式下存储器的管理：

重点理解三个概念：

- **逻辑地址：程序设计中使用的虚拟地址，46位地址；**

  保护方式下，逻辑地址与虚拟存储器的地址空间相对应；

  逻辑地址（虚地址），由段选择符中14位和32位的偏移量构成；

  CPU在每次访问内存时，都要进行逻辑地址到物理地址的转换。

- **线性地址：用段基址和偏移地址组成的地址，32位地址；**

  保护方式下，不启用分页机制时，线性地址就是物理地址；

- **物理地址：存放操作数的存储单元的实际地址，32位地址；**

  物理地址即经过分段、分页转换后，加在地址线A0~A31的地址；

  保护方式下，启用分页机制时，物理地址不同于线性地址；

  从线性地址到物理地址的F( ) 运算，称为页变换。

分段管理机制：

⇩ 将存储空间分为若干个段，

存储单元的地址为：段基地址(32位) + 段内偏移地址(32位)

其中　段基地址通过指令中的段寄存器间接获取

偏移地址由指令中的寻址方式获取.

如　　MOV　AX，DS: [EBX]

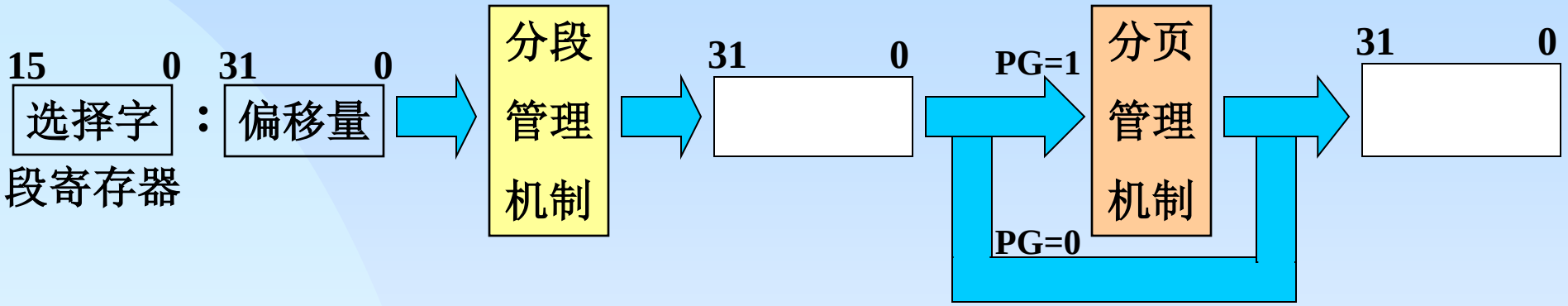
存储单元的段基地址通过DS 寄存器间接获取

偏移地址为EBX寄存器的内容

⇩ 与实方式下不同的是，段基地址不是通过段寄存器直接得到，

保护方式下，段寄存器起到的是索引的作用(称为段选择子)

保护模式下存储器地址的产生



虚拟地址

虚拟地址空间

$2^{13} \times 2^{32} \times 2$

$= 2^{46} = 64T$

线性地址

线性地址空间

2^{32}

物理地址

物理地址空间

最大2^{32}

与实际的配置有关

当PG=0时, 分页管理机制关闭, 线性地址就是物理地址

⇩ 一个任务可以有多个段，
每个段需要一个描述符来描述.

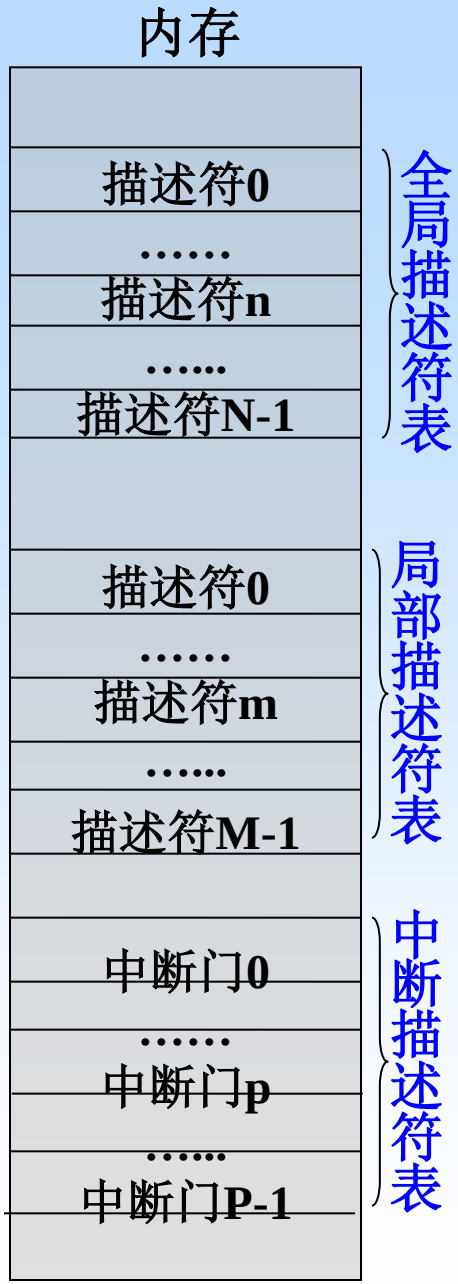
⇩ 为便于组织管理，把描述符组织成线性表，
称为描述符表.

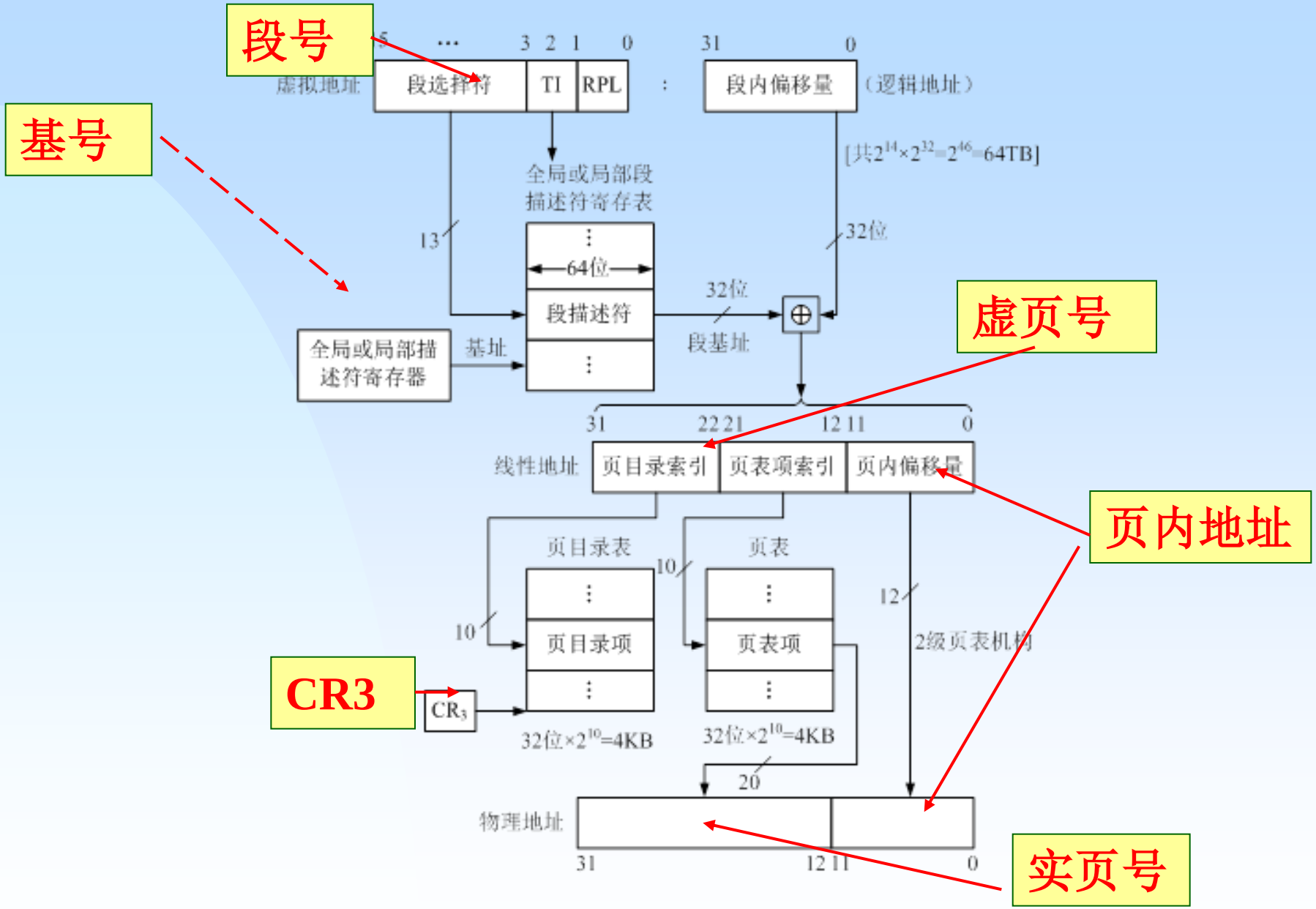
⇩ 有三种类型的描述符表：

1) 全局描述符表GDT
(Global Descriptor Table)

2) 局部描述符表LDT
(Local Descriptor Table)

3) 中断描述符表IDT
(Interrupt Descriptor Table)





参考：《深入分析Linux内核源码》 2.3 段机制和描述符

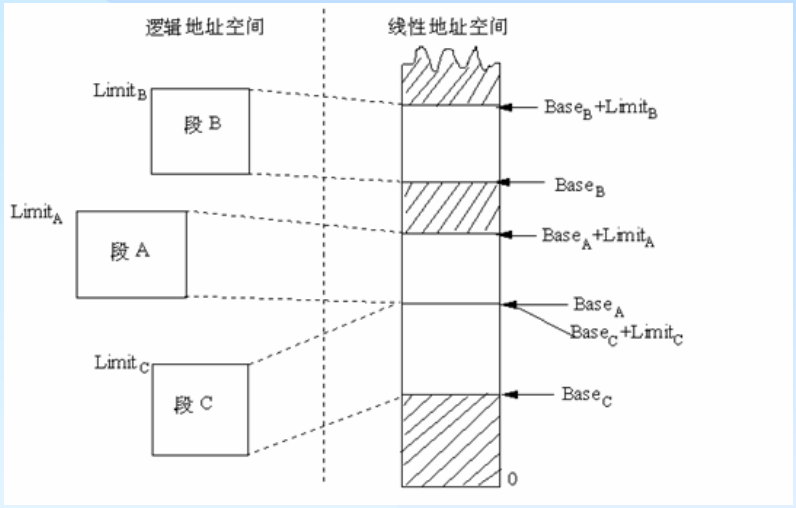


图2.9 逻辑—线性地址转换

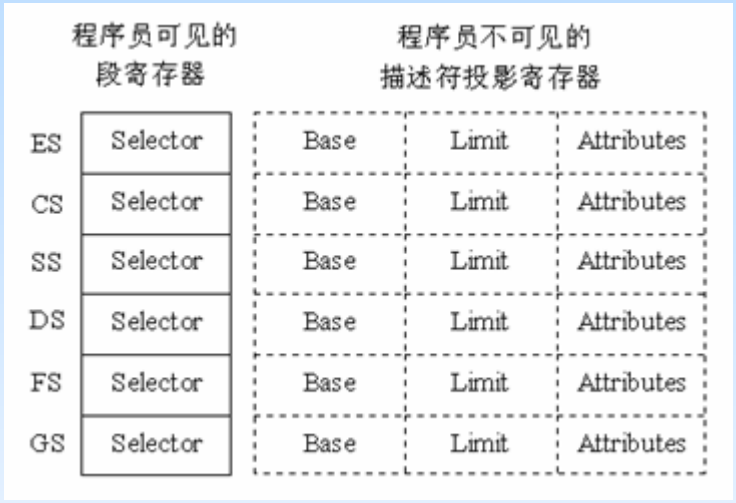


图2.19 六个段寄存器及其投影寄存器

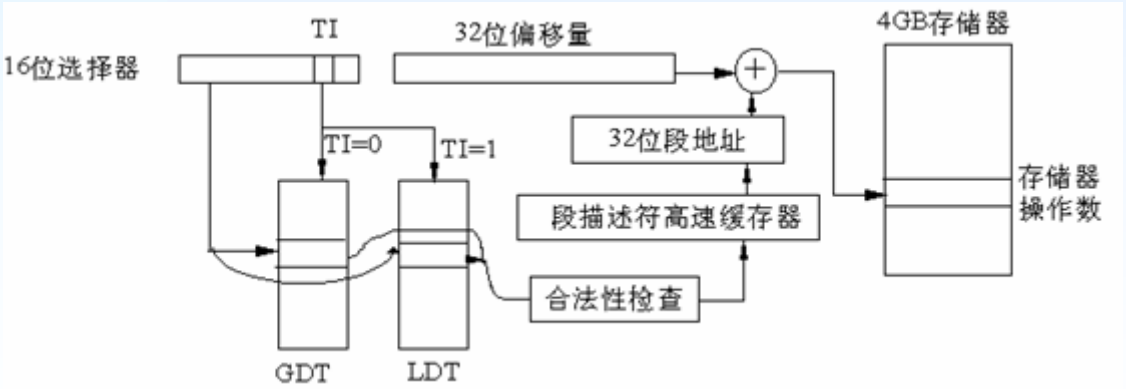


图2.18 寻址过程（分段）

参考：《深入分析Linux内核源码》 2.4 分页机制

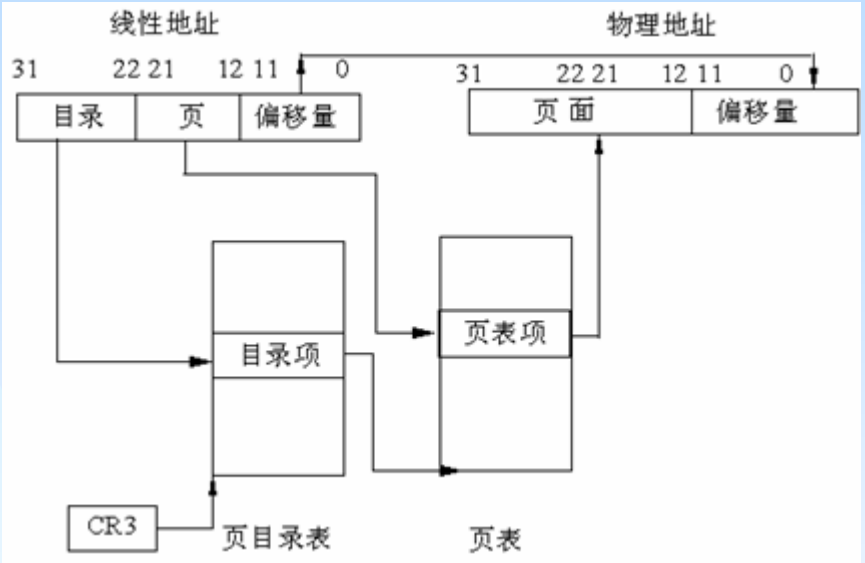


图2.21 两级页表结构

	7	6	5	4	3	2	1	0
7~0位	PSE	0	A	PCD	PWT	U/S	R/W	P
15~8位	3~0位页表地址				OS专用			0
23~16位	11~4位页表地址							
31~24位	19~12位页表地址							

图 2.22的页目录表

	7	6	5	4	3	2	1	0
7~0位	0	D	A	PCD	PWT	U/S	R/W	P
15~8位	3~0位页面地址				OS专用			0
23~16位	11~4位页面地址							
31~24位	19~12位页面地址							

图2.24 页表中的页面项

参考：《深入分析Linux内核源码》 2.4 分页机制

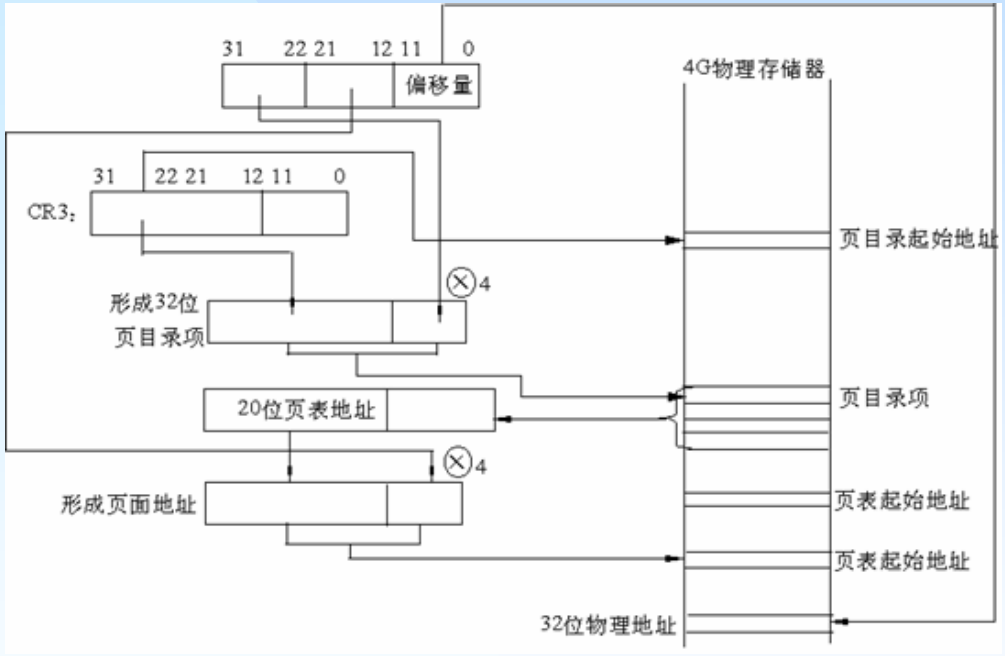


图2.25　32位线性地址到物理地址的转换（分页）

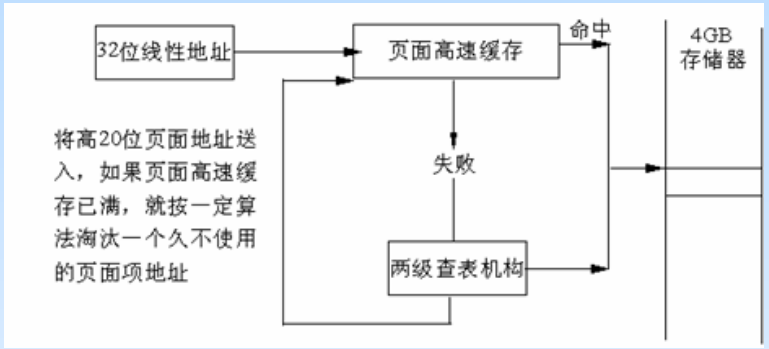


图2.27 子页面高速缓存

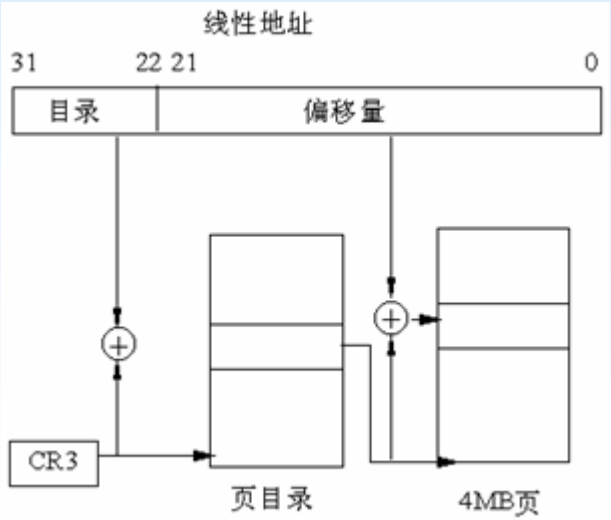


图2.26 奔腾处理器的扩展分页机制

80486 CPU的引脚信号及功能

168条外部引脚：

- 数据总线（32位）
- 地址总线（32位）
- 控制总线
- 总线周期定义信号
- 成组控制信号
- 数据出错报告
- Cache控制
- 中断/复位信号
- A_{20}地址屏蔽信号

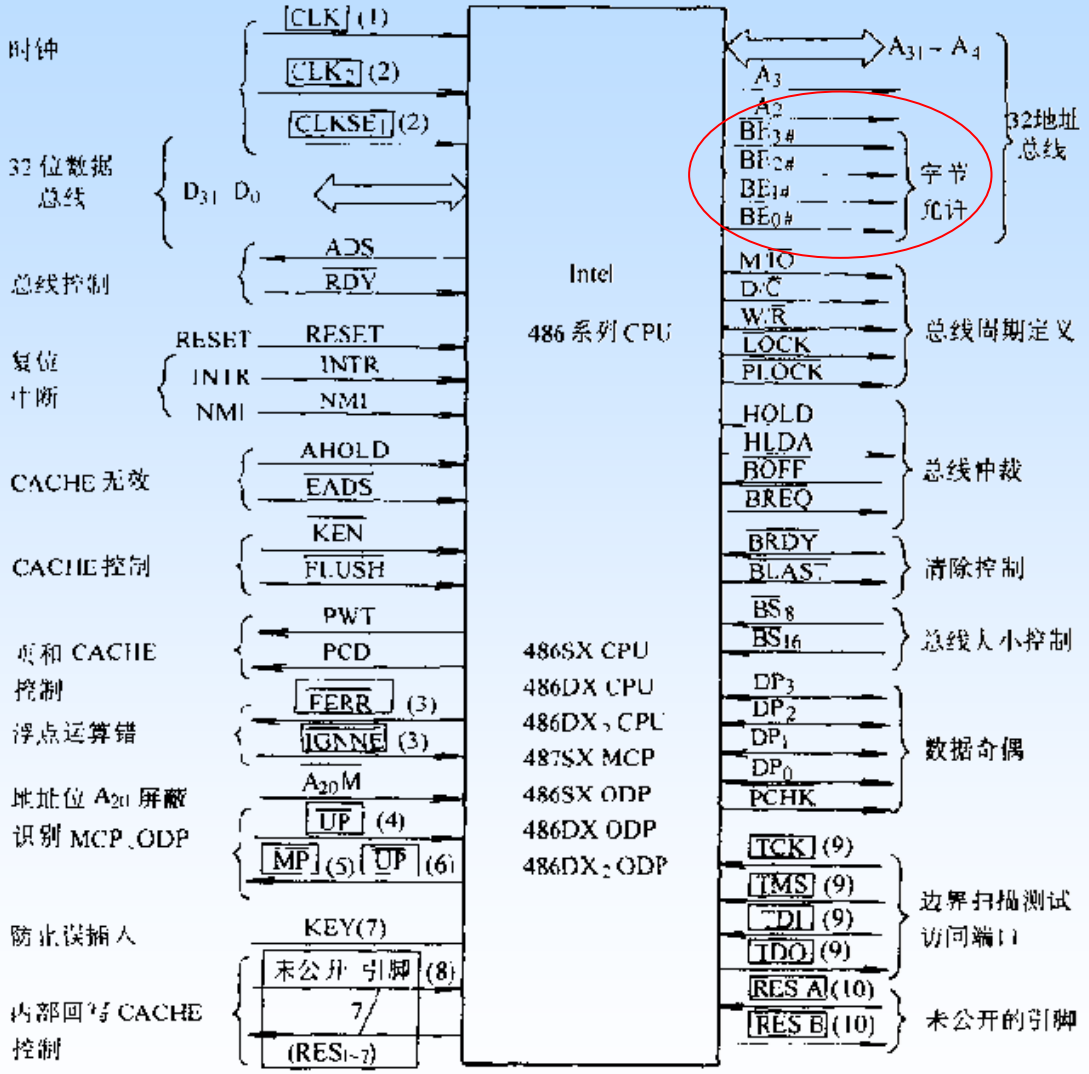
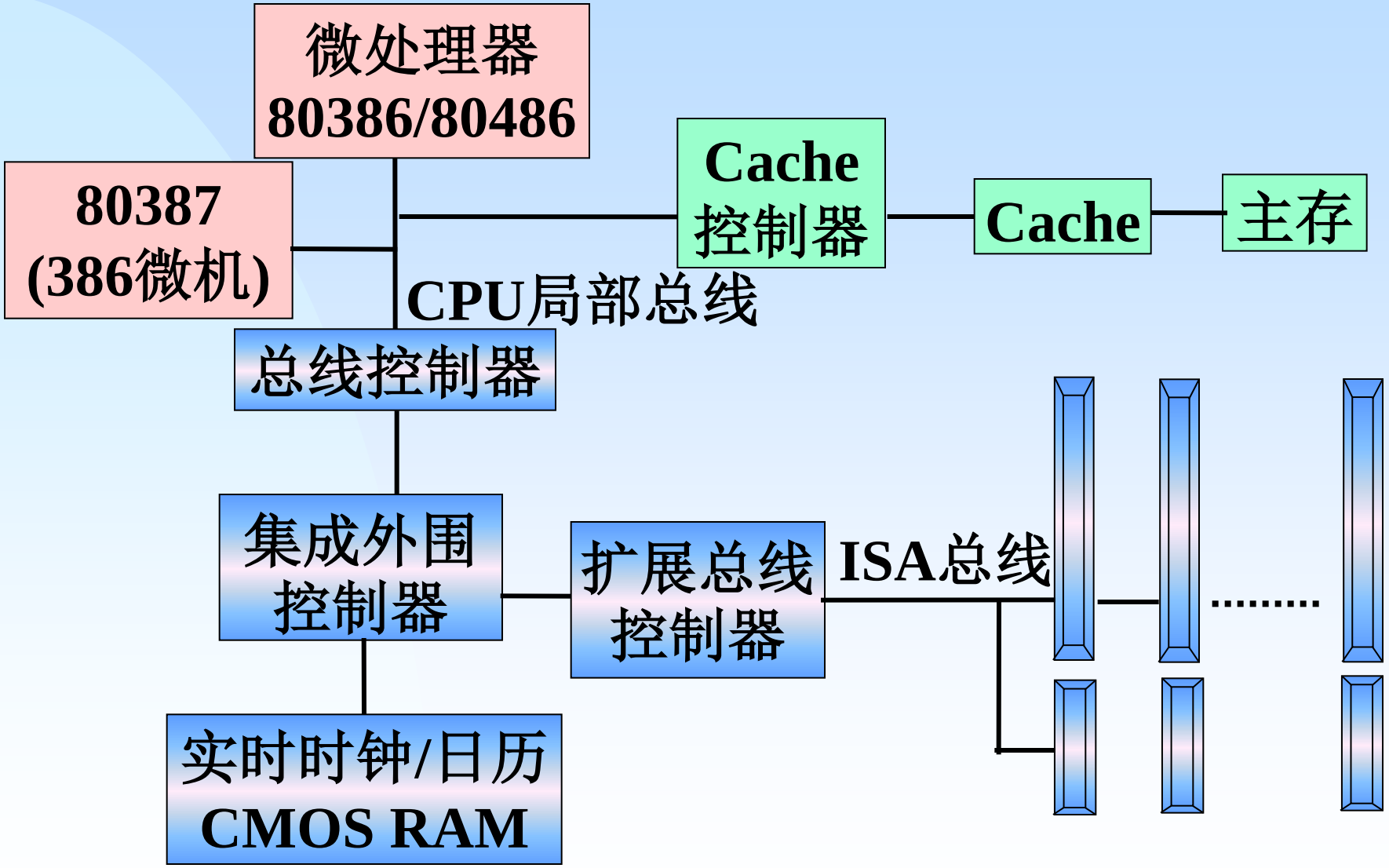


表4-7 字节选通信号与字节数据之间的对应关系

字节选通				要访问的字节数据				自动重复
$\overline{BE_0}$	$\overline{BE_1}$	$\overline{BE_2}$	$\overline{BE_3}$	$D_{31}\sim D_{24}$	$D_{23}\sim D_{16}$	$D_{15}\sim D_8$	$D_7\sim D_0$	
1	1	1	0	-	-	--	$D_7\sim D_0$	N
1	1	0	1	-	--	$D_{15}\sim D_8$	--	N
1	0	1	1		$D_{23}\sim D_{16}$		$D_{23}\sim D_{16}$	Y
0	1	1	1	$D_{31}\sim D_{24}$	-	$D_{31}\sim D_{24}$	—	Y
1	1	0	0	-	--	$D_{15}\sim D_8$	$D_7\sim D_0$	N
1	0	0	1		$D_{23}\sim D_{16}$	$D_{15}\sim D_8$		N
0	0	1	1	$D_{31}\sim D_{24}$	$D_{23}\sim D_{16}$	$D_{31}\sim D_{24}$	$D_{23}\sim D_{16}$	Y
1	0	0	0	---	$D_{23}\sim D_{16}$	$D_{15}\sim D_8$	$D_7\sim D_0$	N
0	0	0	1	$D_{31}\sim D_{24}$	$D_{23}\sim D_{16}$	$D_{15}\sim D_8$	-	N
0	0	0	0	$D_{31}\sim D_{24}$	$D_{23}\sim D_{16}$	$D_{15}\sim D_8$	$D_7\sim D_0$	N

386/486微机的结构:



4.2.5 80386/80486的保护机制与任务转换

80386/80486的保护机制主要有以下几种：

- 段保护：

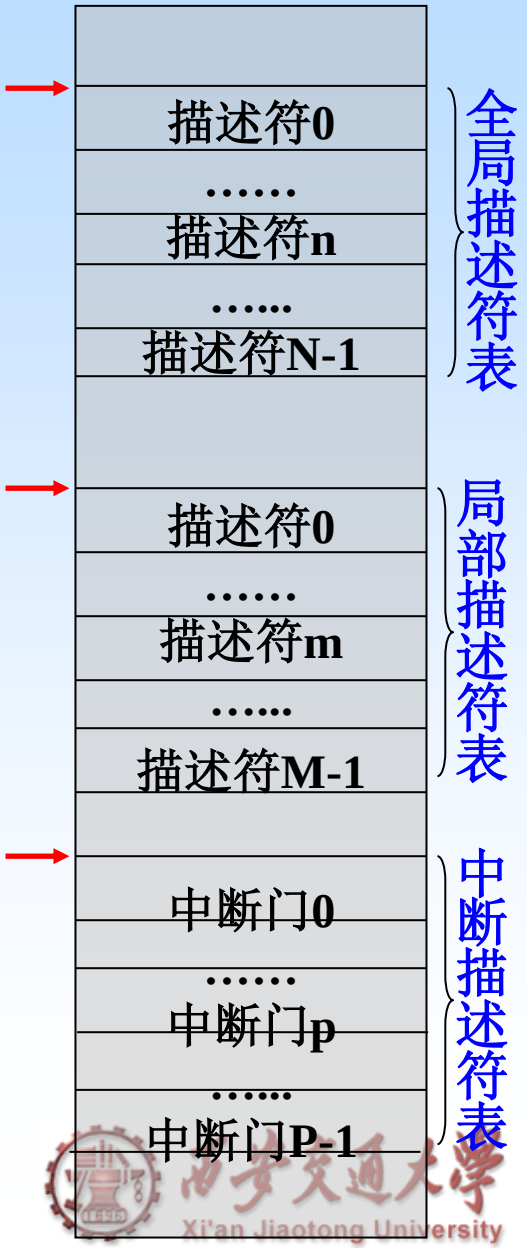
  段存在性检查和越界检查；

- 任务间存储空间的保护：每个任务都有特定的虚拟空间，通过LDT进行隔离和保护；

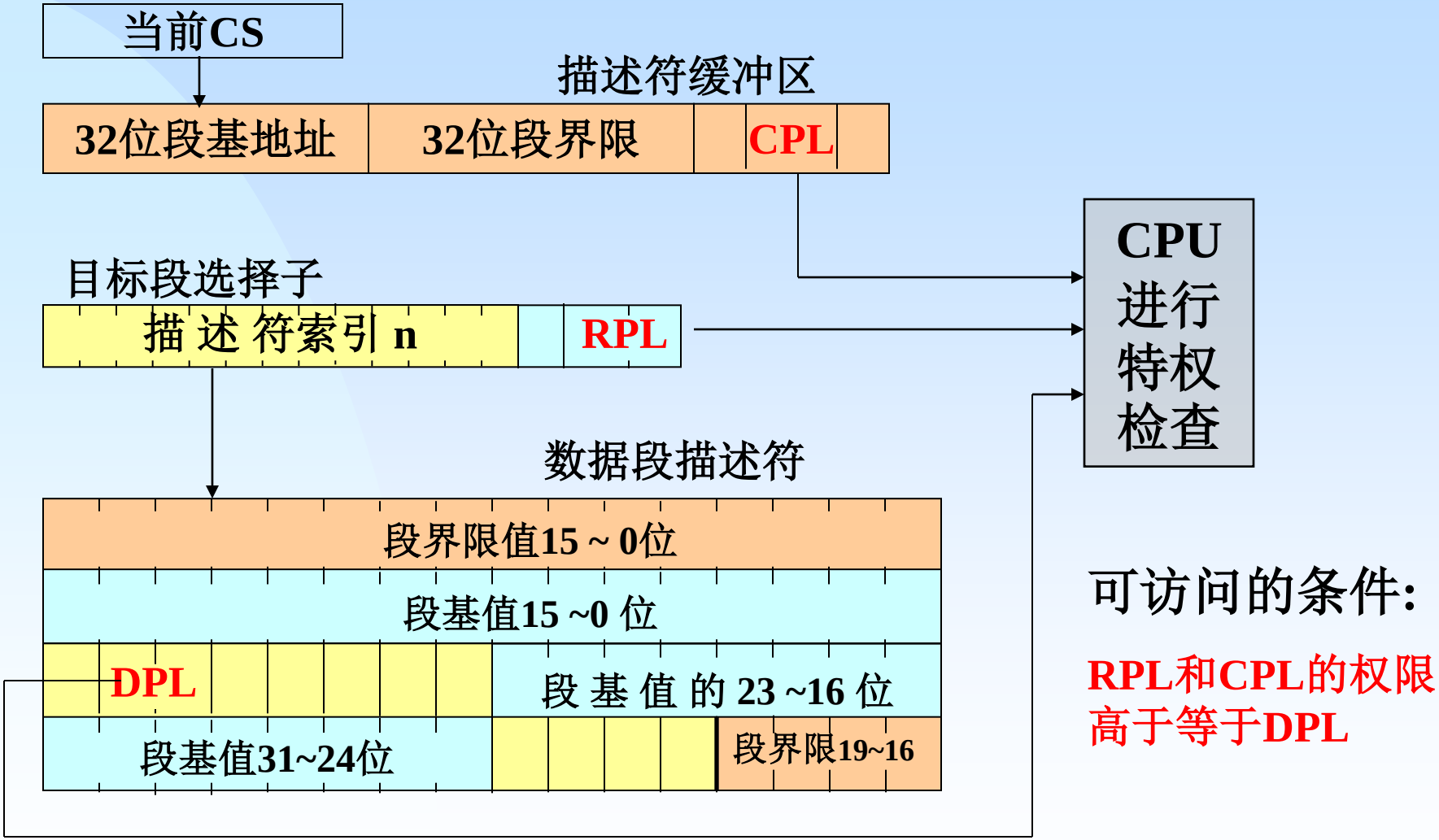
  任何越限和越权的访问都被拒绝执行，并引起异常处理中断

- 特权级保护：
  - 数据段和堆栈段的特权级保护；
  - 代码段的特权级保护；
  - 任务转换；

  程序只能访问同一特权级别或较低级别的数据段，试图访问较高特权级的数据段时，将产生保护异常中断



举例： 数据访问的特权级检查



可访问的条件:

RPL和CPL的权限高于等于DPL

CPL：当前特权级。当前正在执行的代码段所具有的访问特权级，存放在CS的最低两位中。
RPL：请求特权级。是指选择符的特权级，存放在段选择符的最低两位中。
DPL：描述符特权级。这是段被访问的特权级，保存于该段的描述符的DPL位

4.2.5 80386/80486的保护机制与任务转换

- 门（Gate）也是一种描述符，由8字节构成，放置在GDT、LDT或者IDT中供调用；
- 门描述符分为：调用门、中断门、陷阱门、任务门；
- 调用门提供了一个入口地址，可以实现不同特权级的代码之间的转移。

CALL指令可以使用调用门将进程控制转移到一个特权级更高。

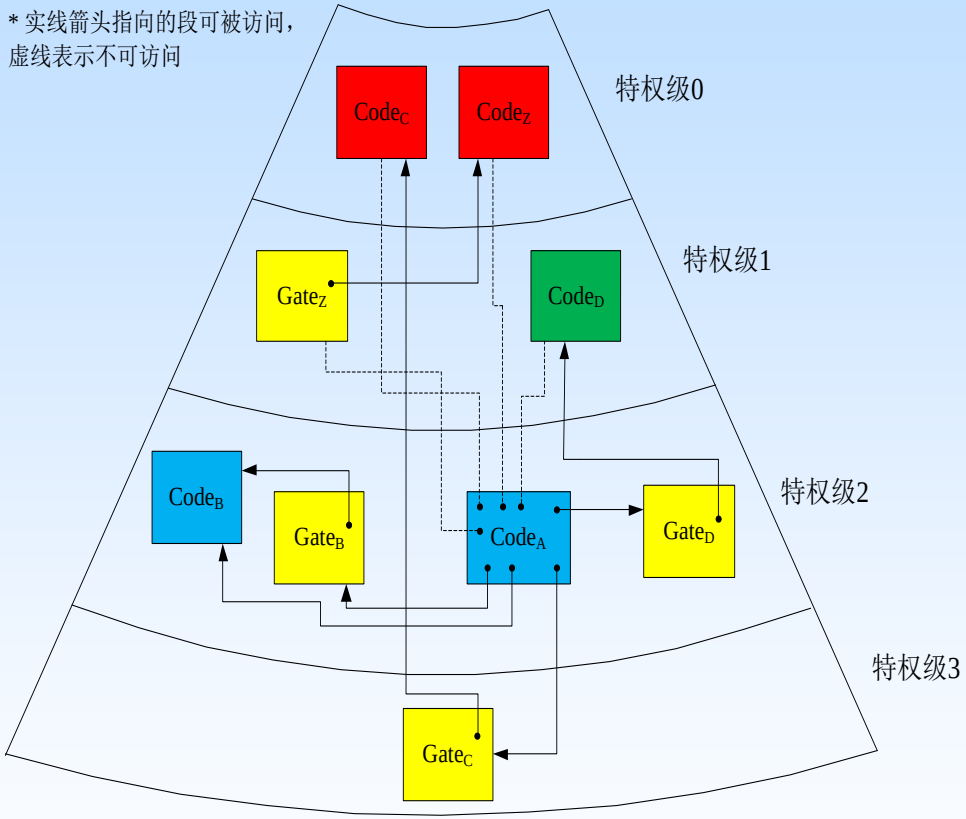


图4-34 特权级和门及其之间的调用

参考：《Linux内核完全剖析—基于0.12内核》
第4章80x86保护模式及其编程

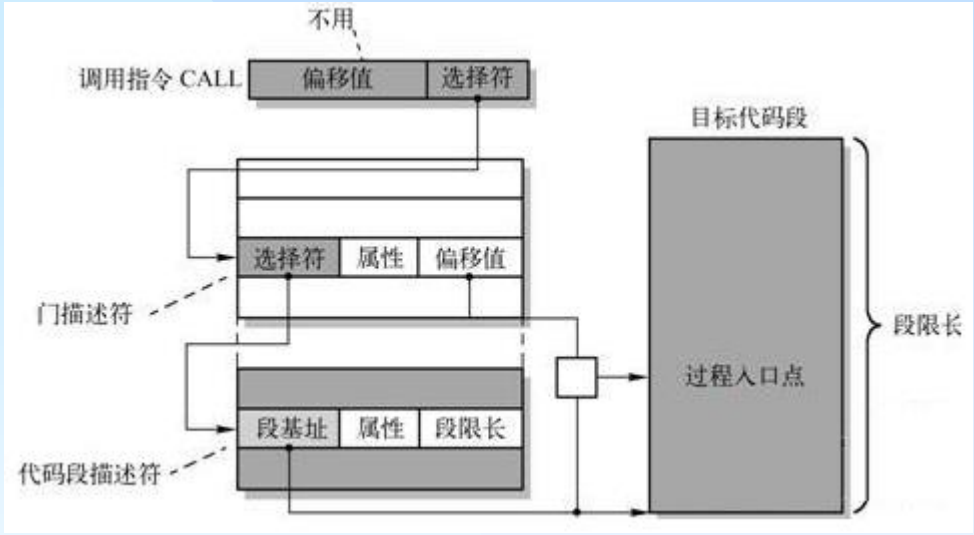


图4-23 门调用操作过程

(1) 为了访问调用门，需要为CALL指令的操作数提供一个远指针，其中的段选择符用于指定调用门。

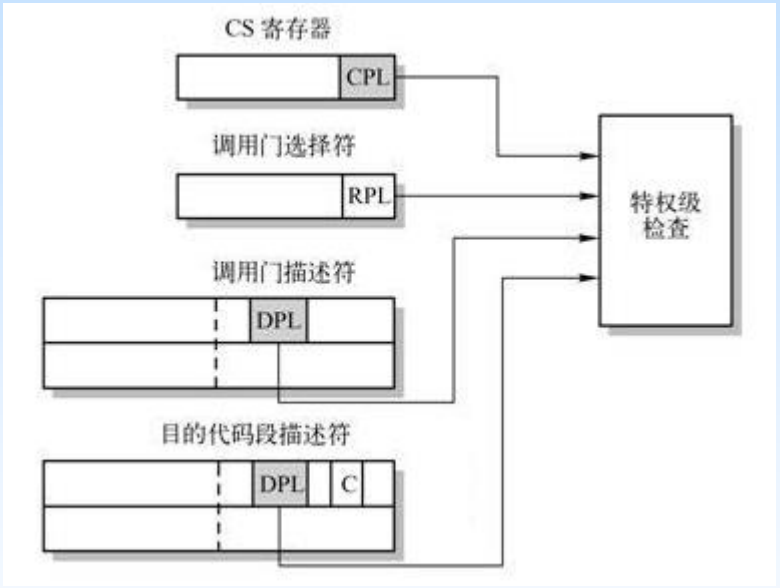


图4-24 通过调用进行控制转移的特权级检查

(2) 通过调用门进行程序控制转移时，CPU会对当前特权级CPL、请求特权级RPL、调用门描述符中的描述符特权级DPL和目的代码段描述符中的DPL进行检查，以确定控制转移的有效性。

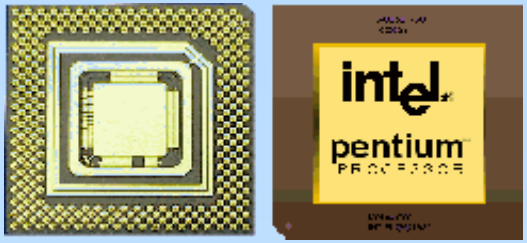
指令	特权级检查规则
CALL	CPL小于或等于调用门的DPL；RPL小于或等于调用门的DPL　访问门的权限 对于一致性和非一致性代码段都只要求DPL小于或等于CPL　访问代码权限

(3) 调用门可以让一个代码段中的过程被不同特权级的程序访问。

4.3 P5、P6、Netburst、Core构架微处理器及迅驰平台

- P5构架微处理器
- P6构架微处理器
- Netburst构架微处理器
- Core构架微处理器
- Intel移动平台迅驰

4.3.1 P5 构架处理器

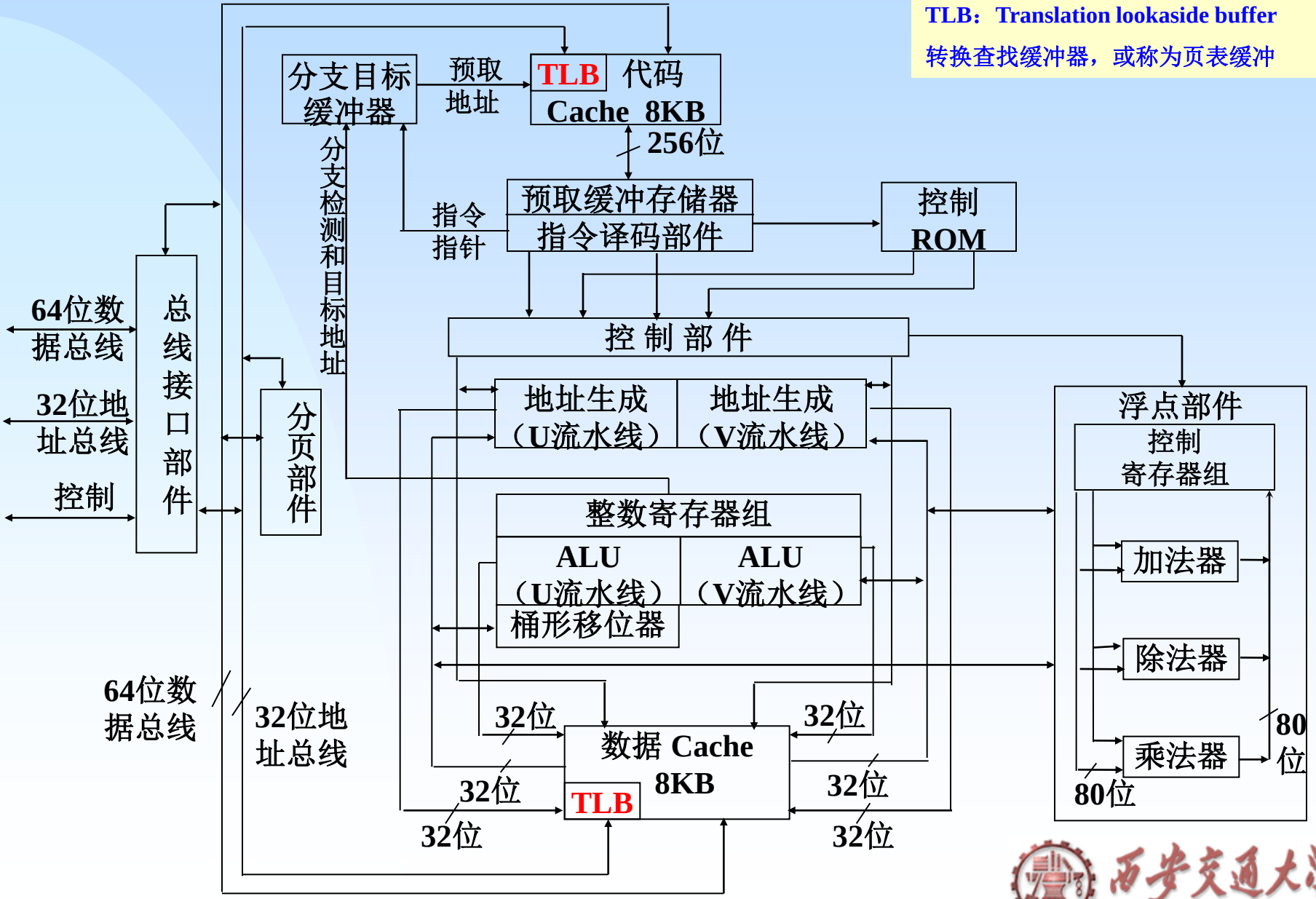


- Pentium处理器是Intel公司于1993年推出的第五代x86系列处理器，该系列微处理器的主要特点如下：
- 32位微处理器：内部ALU和通用寄存器为32位，内部数据总线32位，外部数据总线64位，地址总线32位；
- 超标量流水线：内部采用了超标量流水线，有三个指令执行单元，能够在一个时钟周期内执行多条指令；
- 分离高速缓存：指令和数据分别使用不同的Cache，减少访问主存次数，避免预取指令和数据冲突，提高指令执行速度；
- 分支指令预测：提供分支目标缓冲器BTB，动态预测程序分支路径，消除分支指令之后损失的周期，防止流水线断流；
- 功能自检电路：芯片上电自检，EAX=0表示内部功能正常；

Pentium微处理器内部结构：

TLB：Translation lookaside buffer

转换查找缓冲器，或称为页表缓冲



Pentium的工作模式：

- 实地址模式
  - 1MB空间，分段管理，所有程序全在0级
- 保护模式
  - 存储器采用虚拟地址空间、线性地址空间和物理地址空间三种方式描述
  - 虚拟地址空间64TB（2^{46}）
  - 4级管理，可以使用分页技术
- 虚拟8086模式

	实地址模式	虚拟 8086 模式
内存管理	分段管理	既分段又分页
存储空间	1MB	每个 8086 程序任务寻址 1MB，总寻址空间 4GB
多任务	不支持	支持，虚拟 8086 模式利益是 Pentium 保护模式中多任务的一个任务。

- 系统管理模式
  - 电源管理及为操作系统和正在运行的应用程序提供安全

4.3.2 P6 构架处理器

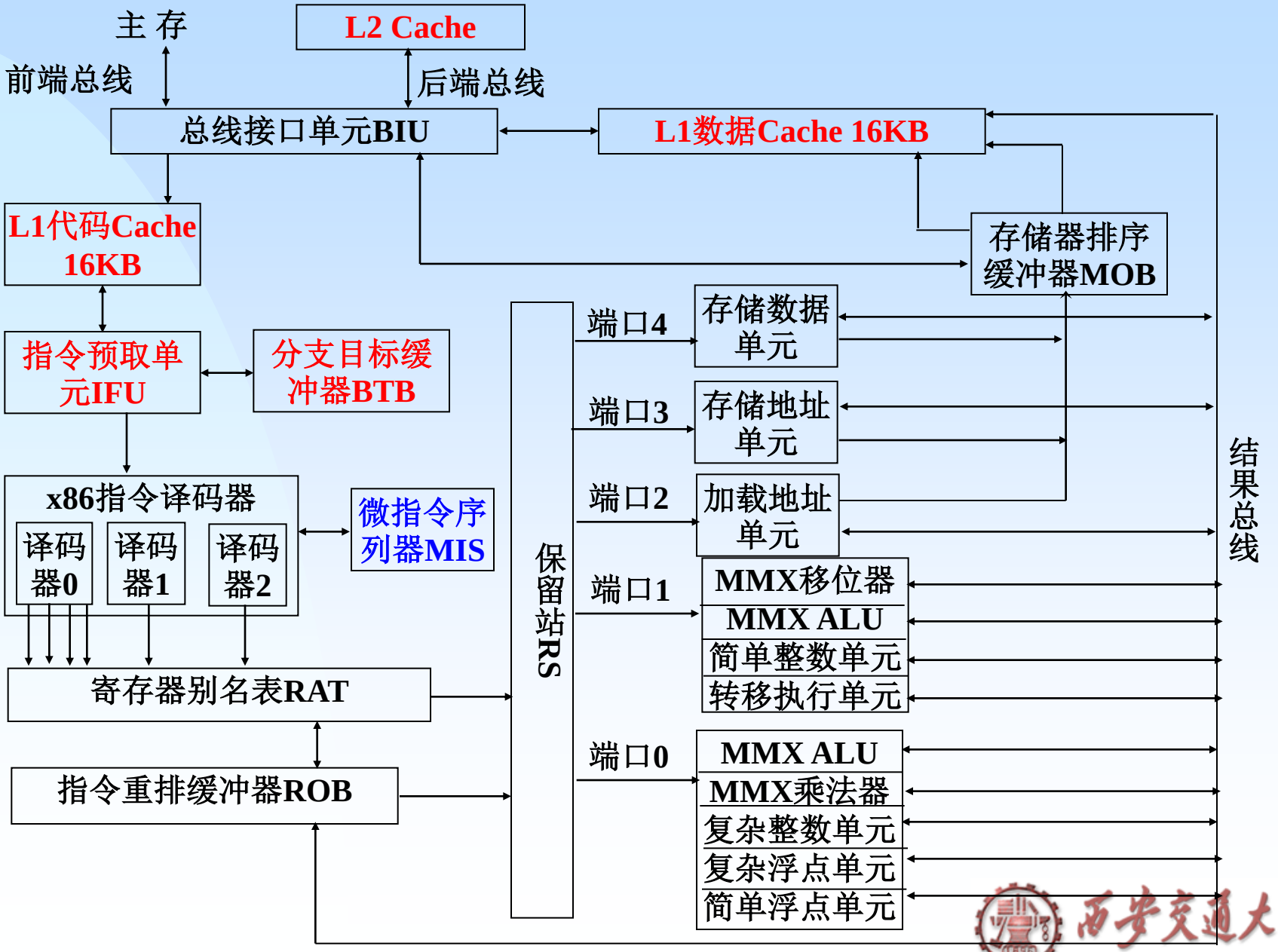
Pentium Pro、II、III属于Intel公司采用P6 构架的第六代微处理器产品。

- **Pentium Pro**：1995年11月推出，可进行36位寻址，最大寻址范围64GB。包含一个CPU核心和一个L2 Cache；
- **Pentium II**：1997年5月推出，对Pentium Pro进行改进并增加了多媒体指令，分为Pentium II 、Pentium II Celeron、Pentium II Xeon 3各系列，其配套440系列芯片组采用南桥/北桥结构；
- **Pentium III**：1999年2月推出，指令流水线为10级，新增70条单指令多数据流扩展（SSE）指令，增强了三维图形和音频、视频处理能力；其配套芯片组810系列，由存储控制中心（MCH）和I/O控制中心（ICH) 和固件中心（FWH）构成；

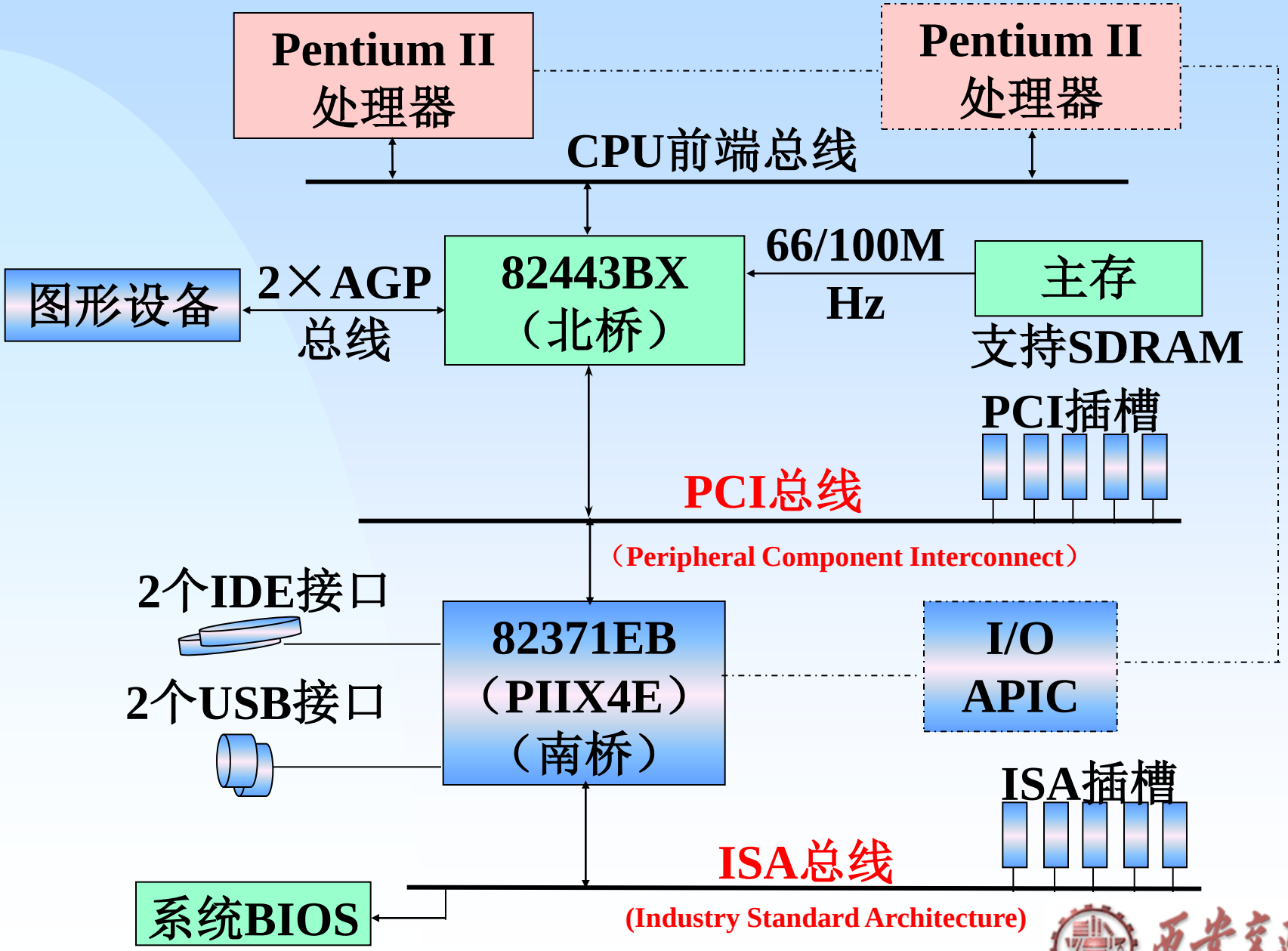
Pentium II 微处理器的特点:

- Pentium Pro核心+MMX
- 双独立总线结构
  - 后端总线连接到L2 Cache上，后来的L2 Cache集成到了CPU芯片中，后端总线用以连接L3 Cache
  - 前端总线FSB主要负责主存储器的信息传送操作
- 借鉴了RISC技术来实现传统的x86指令系统
  - 每一条x86操作都转换成简单的微操作
- 采用动态执行技术和寄存器重命名技术
  - 允许程序的几个分支流向同时在处理器中执行
- 采用了最新的Slot1接口标准

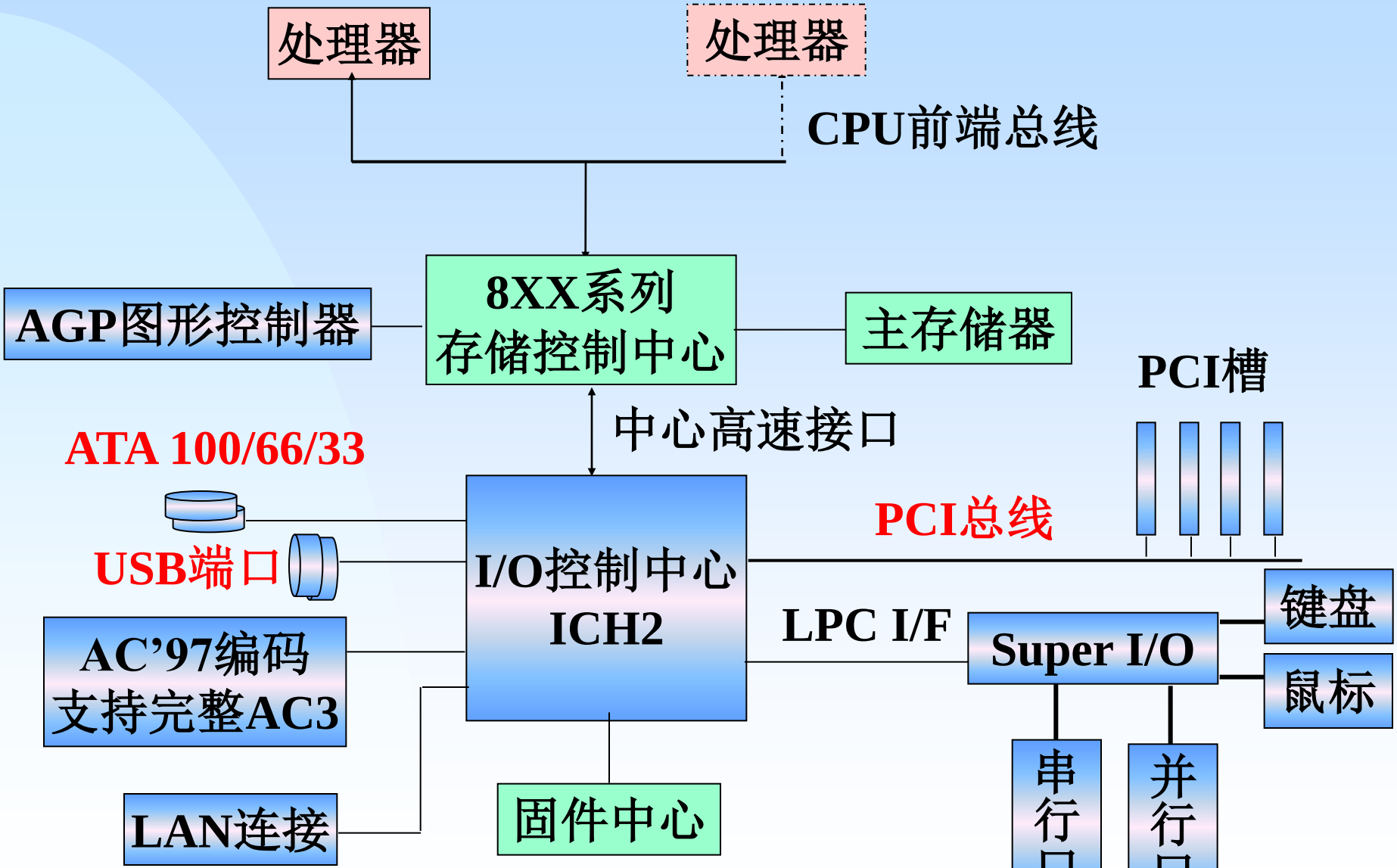
Pentium II 的内部结构



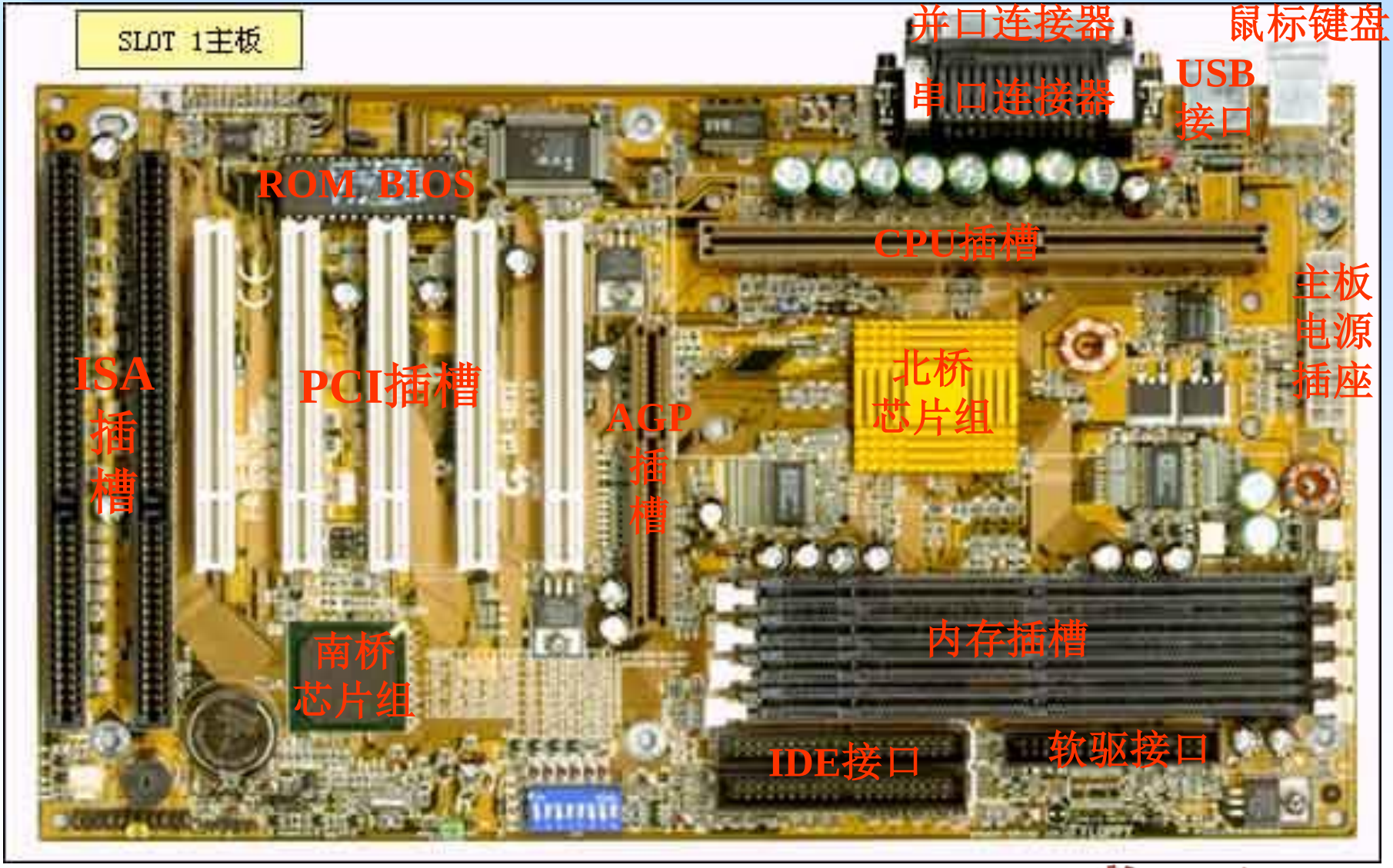
Pentium II微机的基本结构：



Pentium III微机的基本结构：



Pentium III Slot1主板

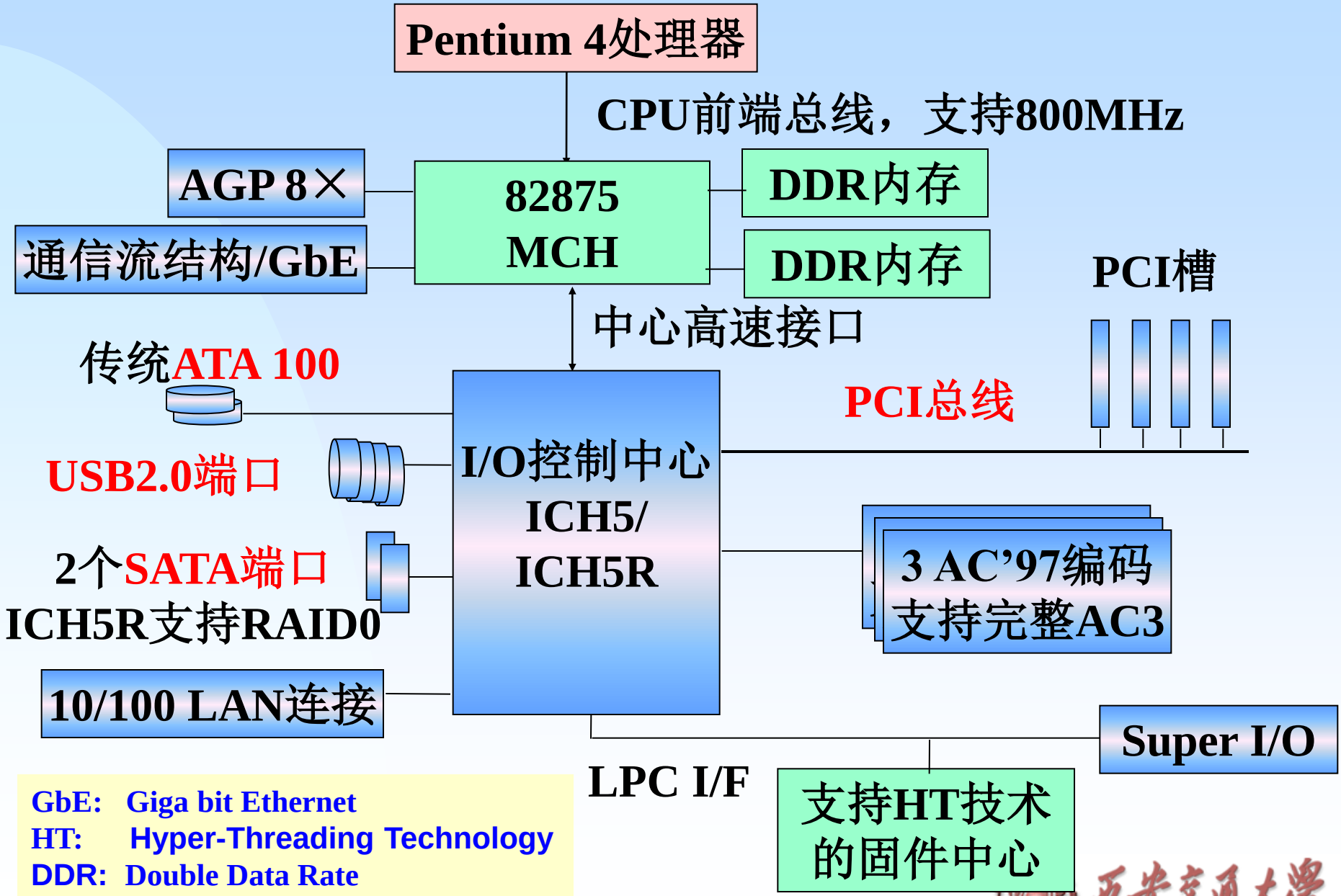


4.3.3 Netburst构架处理器

2000年11月，Intel公司推出了Pentium 4，采用Netburst 微内核结构，特点如下：

- 快速执行引擎 - 简单ALU运行在2倍的处理器核心频率；
- 超级流水线技术 - 具有20/31级超长流水线；
- 高级动态执行 - 改进了分支预测算法，有效降低了失误预测率
- 新的系统总线
  - 前端总线频率可达 800MHz，每周期可传送64位数据；
- 新的缓存体系结构：3级Cache
  - 16KB数据和12KB执行跟踪L1 Cache
  - 1MB或512KB的L2 Cache
  - 2MB L3 Cache
- 硬件指令预取
- 增加了144条SSE2指令和13条SSE3指令

Pentium 4 微机的基本结构：



4.3.4 Core 构架微处理器

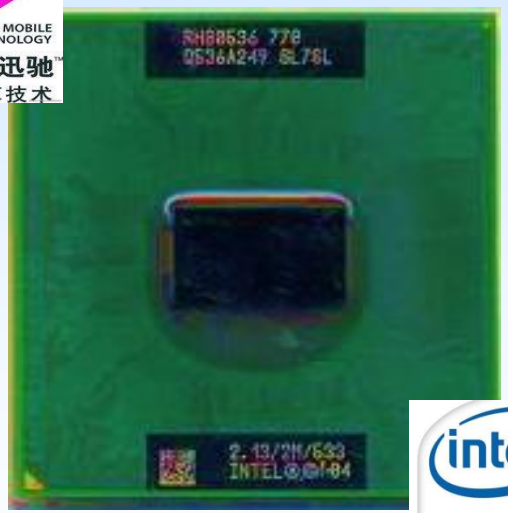
Core（酷睿）构架采用五大新技术：

- 宽位动态执行技术
  - Wide Dynamic Execution
- 智能功率能力技术
  - Intelligent Power Capability
- 高级智能高级缓存技术
  - Advanced Smart Cache
- 智能内存访问技术
  - Smart Memory Access
- 高级数字媒体增强
  - Advanced Digital Media Boost

4.3.5 Intel 移动平台迅驰

迅驰（Centrino）是Intel公司针对便携式电脑提出的无线移动计算解决方案，核心部件包括移动处理器、主板芯片组以及无线网络连接产品；

- 第一代迅驰平台　Carmel
- 第二代迅驰平台　Sonoma
- 第三代迅驰平台　Napa
- 第四代迅驰平台　Santa Rosa
- 第五代迅驰平台　Montevina



4.4 AMD 微处理器

- K5 阶段
  - 动态执行、推测执行、分支预测；
- K6 阶段
  - RISC 86超标量微结构
- K7 阶段
  - Athlon（速龙）、Duron（毒龙）、Sempron（闪龙）
- K8 阶段
  - Opteron（皓龙）、Turion（炫龙）
- K10阶段
  - Phenom （羿龙）

Intel 80x86系列CPU芯片特征小结：

推出年代	CPU芯片	寄存器位数	数据线宽度	地址线宽度	最大主频MHz
1971.11	4004	4	4		0.1
1972.4	8008	8	8	14	0.2
1974.4	8080	8	8	16	2
1978.6	8086	16	16	20	10
1979.6	8088	16	8	20	8
1982.2	80286	16	16	24	16
1985.10	80386	32	32	32	33
1989.4	80486	32	32	32	66
1993.3	Pentium	32	64	32	100
1995.11	Pentium Pro	32	64	36	200
1997.5	Pentium II	32	64	36	450
1999.2	Pentium III	32	64	36	1000
2001	Pentium IV	32	64	36	1300-2400

通　　知：

期中考试时间：10月29日，周六

教学组网址：http://mcp.xjtu.edu.cn

个人主页：http://gr.xjtu.edu.cn/web/ggzhang