实模式与保护模式

操作系统第二次简答题参考资料 王瑞华

1，什么是实模式？什么是保护模式？

- （1）实模式就是用基地址加偏移量就可以直接拿到物理地址的模式。
  - 缺点：实模式非常不安全。

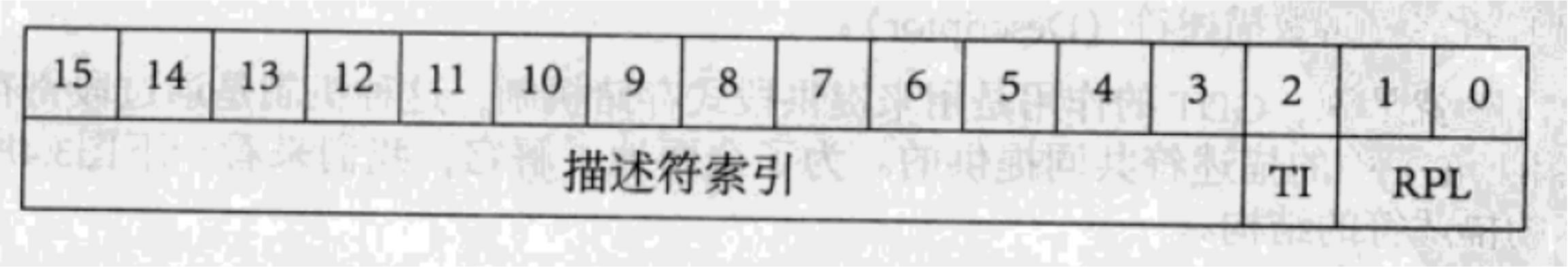
- （2）保护模式就是不能直接拿到物理地址的模式。
  - 需要进行地址转换
  - 从80386开始，是现代操作系统的主要模式

2，保护模式下怎么获取物理地址

- （1）给出段选择子+偏移量
- （2α）若选择了GDT方式，则从GDTR获取GDT首地址，用段选择子中的13位做偏移，拿到GDT中的描述符
- （3α）如果合法且有权限，用描述符中的段首地址加上（1）中的偏移量找到物理地址。寻址结束。
- （2β）若选择了LDT方式，则从GDTR获取GDT首地址，用LDTR中的偏移量做偏移，拿到GDT中的描述符1
- （3β）从描述符1中获取LDT首地址，用段选择子中的13位做偏移，拿到LDT中的描述符2
- （4β）如果合法且有权限，用描述符2中的段首地址加上（1）中的偏移量找到物理地址。寻址结束。

名词解释：选择子

- （1）选择子共16位，放在段选择寄存器里
- （2）低2位表示请求特权级
- （3）第3位表示选择GDT方式还是LDT方式
- （4）高13位表示在描述符表中的偏移（故描述符表的项数最多是2的13次方）



名词解释：描述符

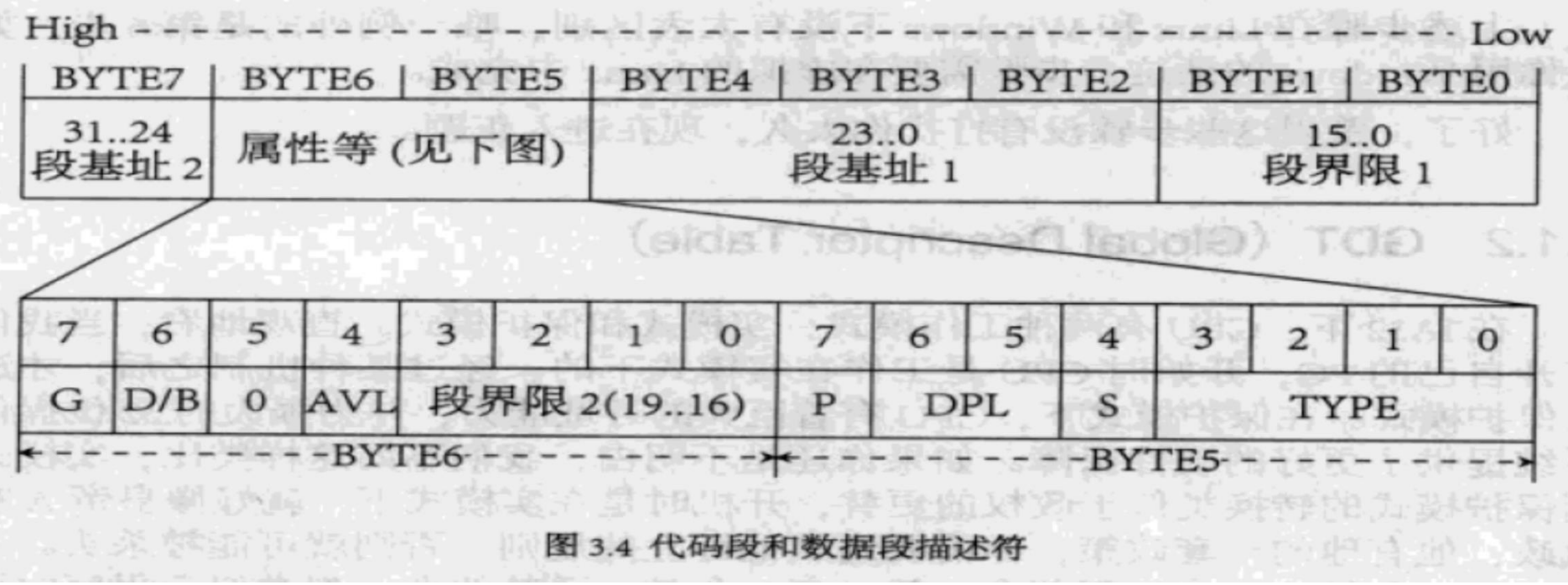


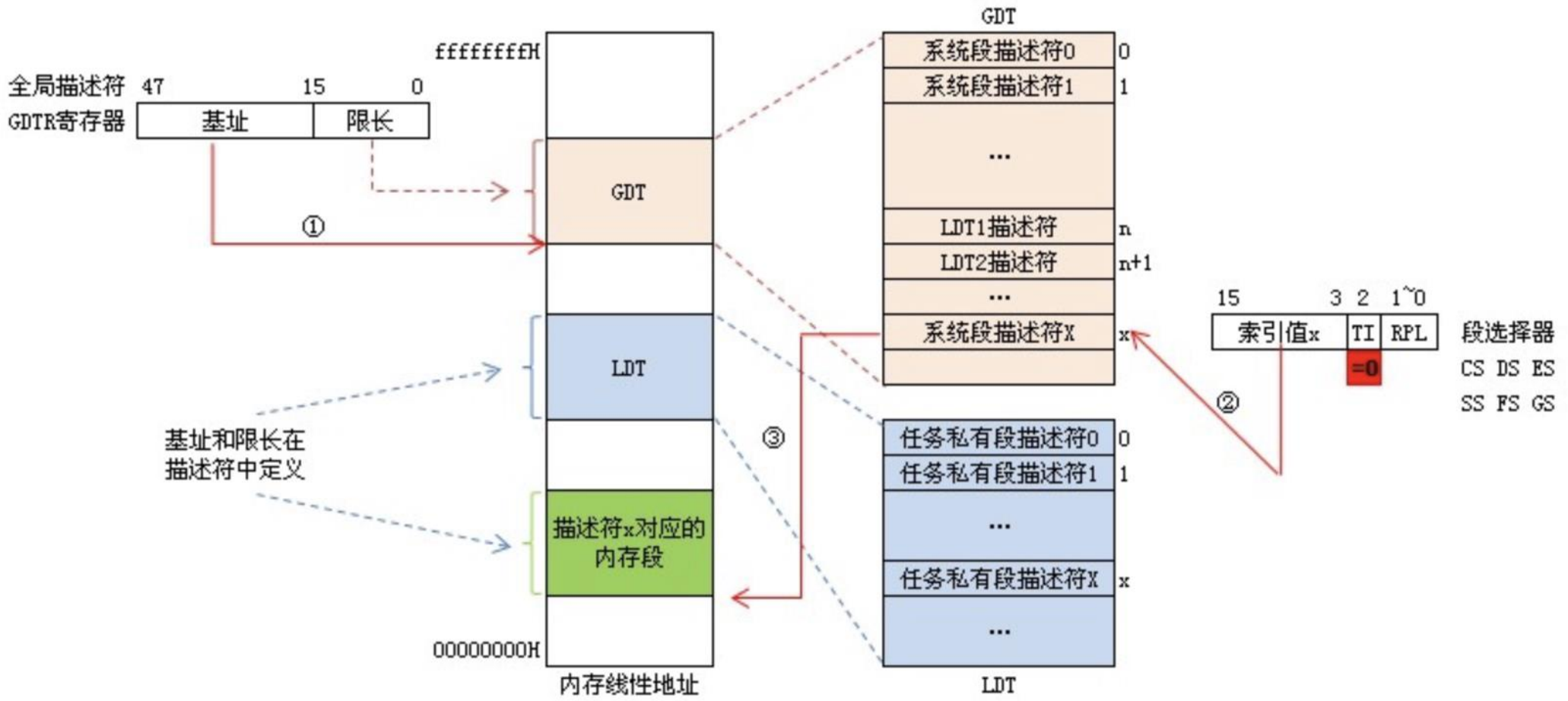
图 3.4 代码段和数据段描述符

- 保护模式下引入描述符来描述各种数据段，所有的描述符均为8个字节（0-7），由第5个字节说明描述符的类型。类型不同，描述符的结构也有所不同。

名词解释：GDT、LDT、GDTR、LDTR

- (1)GDT：全局描述符表，是全局唯一的。存放一些公用的描述符、和包含各进程局部描述符表首地址的描述符。
- (2)LDT：局部描述符表，每个进程都可以有一个。存放本进程内使用的描述符。
- （以上可以理解为二级的表结构）
- (3)GDTR：48位寄存器，高32位放置GDT首地址，低16位放置GDT限长（限长决定了可寻址的大小，注意低16位放的不是选择子）
- (4)LDTR：16位寄存器，放置一个特殊的选择子，用于查找当前进程的LDT首地址。

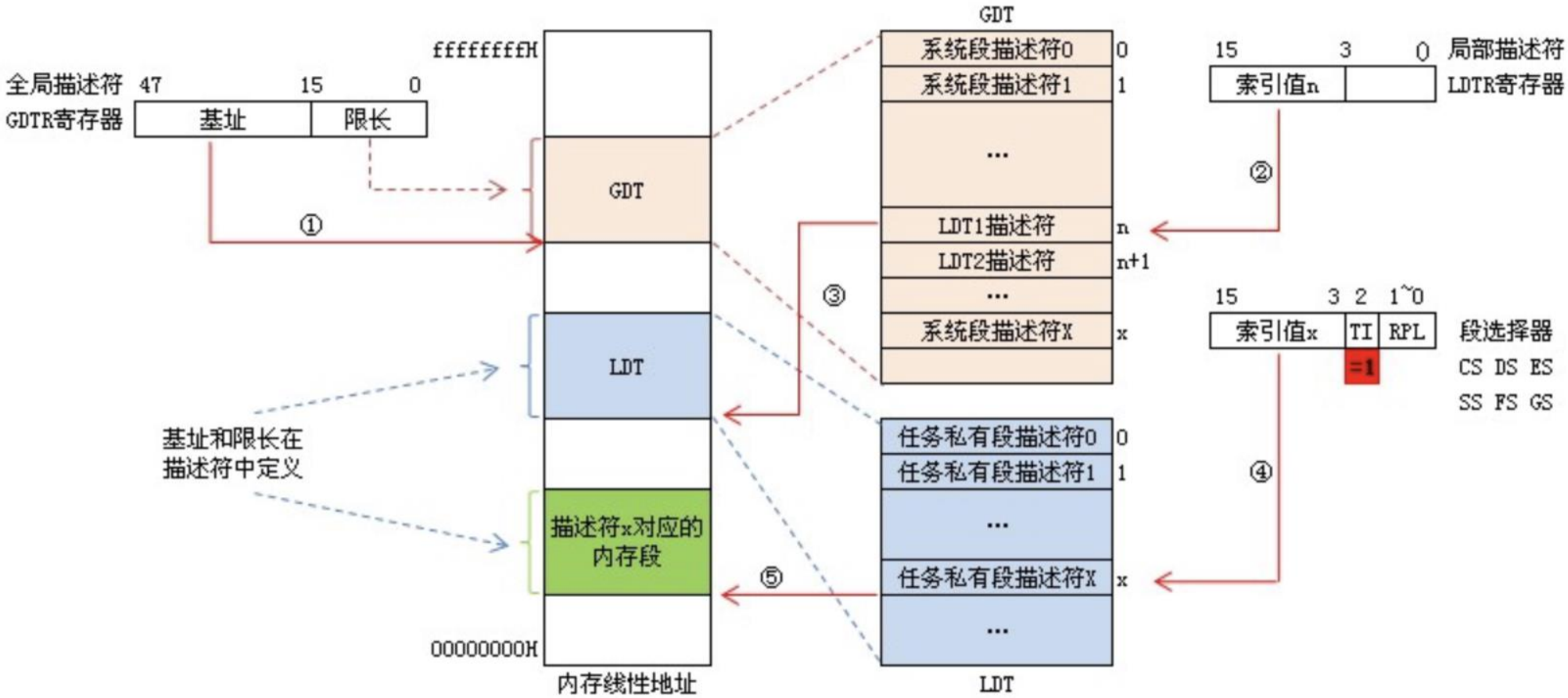
图解：GDT查询物理地址



回顾：GDT查找物理地址的步骤

- （1）给出段选择子（放在段选择寄存器里）+偏移量
- （2）若选择了GDT方式，则从GDTR获取GDT首地址，用段选择子中的13位做偏移，拿到GDT中的描述符
- （3）如果合法且有权限，用描述符中的段首地址加上（1）中的偏移量找到物理地址。寻址结束。

图解：LDT查找物理地址



回顾：LDT查找物理地址的步骤

- （1）给出段选择子（放在段选择寄存器中）+偏移量
- （2）若选择了LDT方式，则从GDTR获取GDT首地址，用LDTR中的偏移量做偏移，拿到GDT中的描述符1
- （3）从描述符1中获取LDT首地址，用段选择子中的13位做偏移，拿到LDT中的描述符2
- （4）如果合法且有权限，用描述符2中的段首地址加上（1）中的偏移量找到物理地址。寻址结束。