



实模式与保护模式

黄婉红 hwh@smail.nju.edu.cn





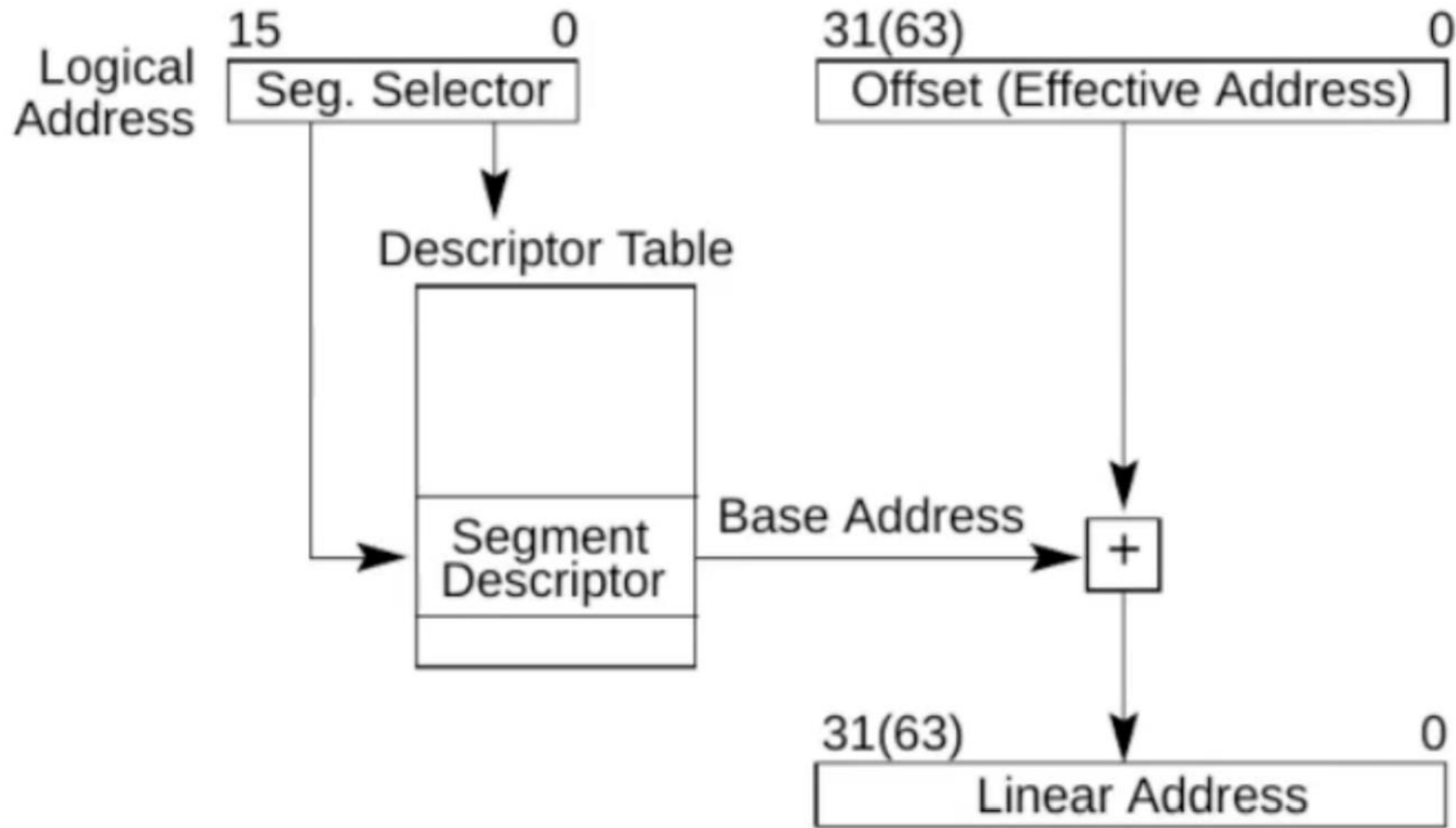
实模式与保护模式

- 实模式：基地址+偏移量可以直接获得物理地址的模式
 - 缺点：非常不安全
- 保护模式：不能直接拿到物理地址
 - 需要进行地址转换
 - 从80286开始，是现代操作系统的主要模式





逻辑地址转线性地址





选择子

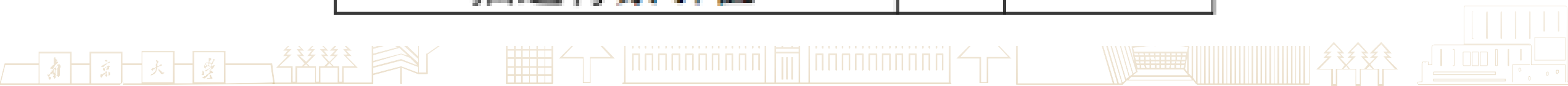
- 选择子共16位，放在段选择寄存器里
- 低2位表示请求特权级
- 第3位表示选择GDT还是LDT方式
- 高13位表示在描述符表中的偏移
 - 故描述符表的项数最多是2的13次方

15

3

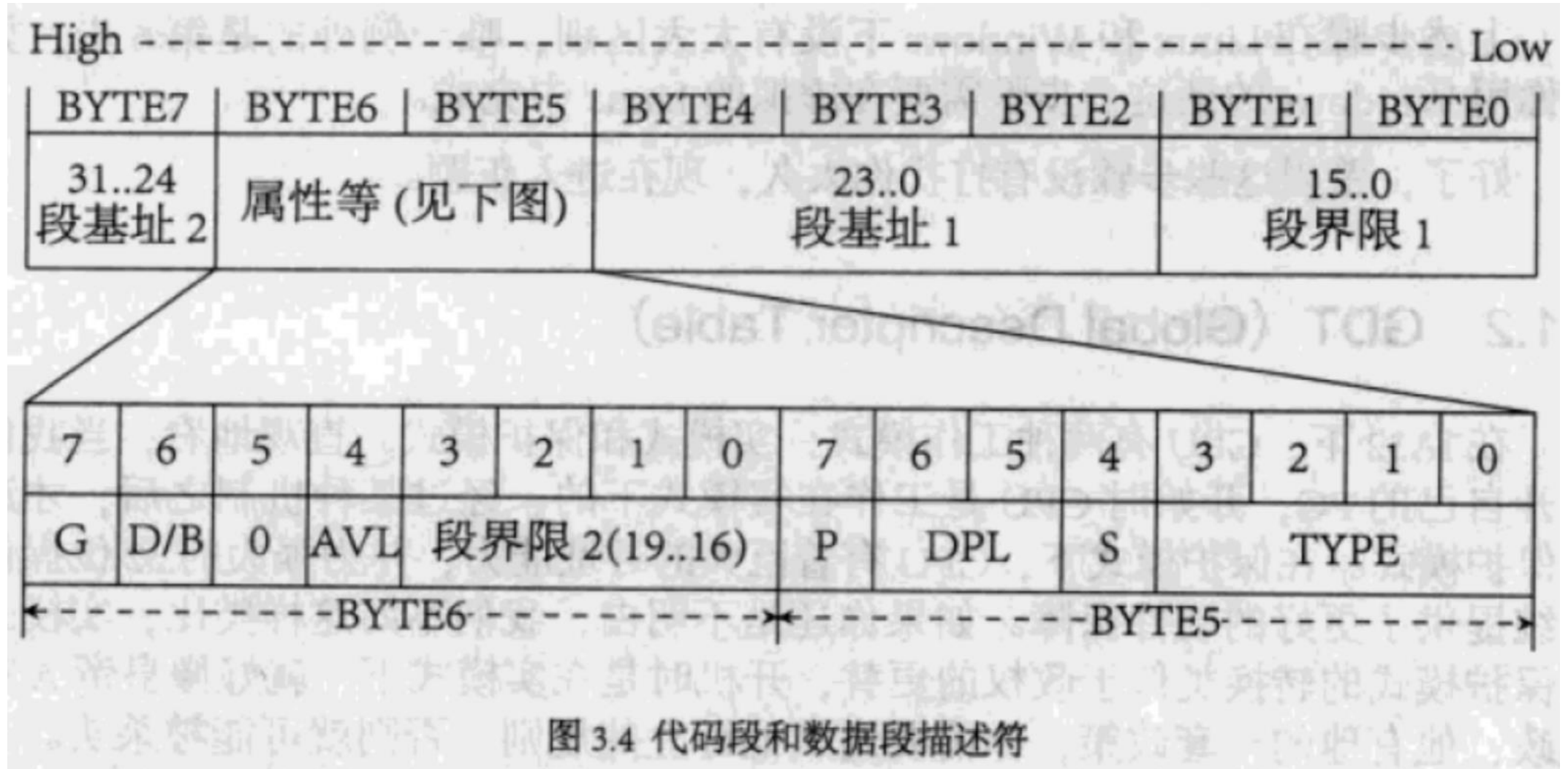
2

0





段描述符





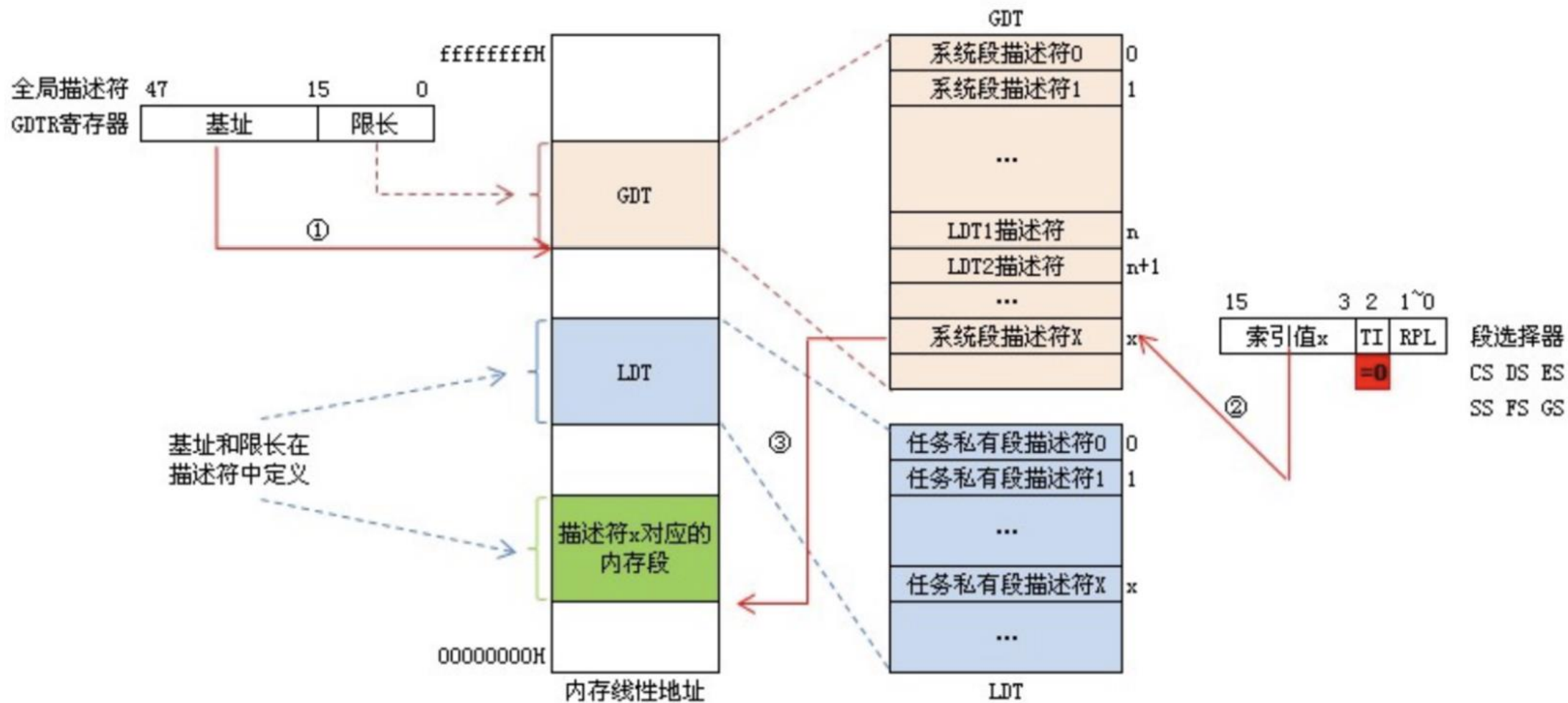
GDT与LDT, GDTR与LDTR

- 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。
- 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。
- 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
- 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。





GDT查询物理地址





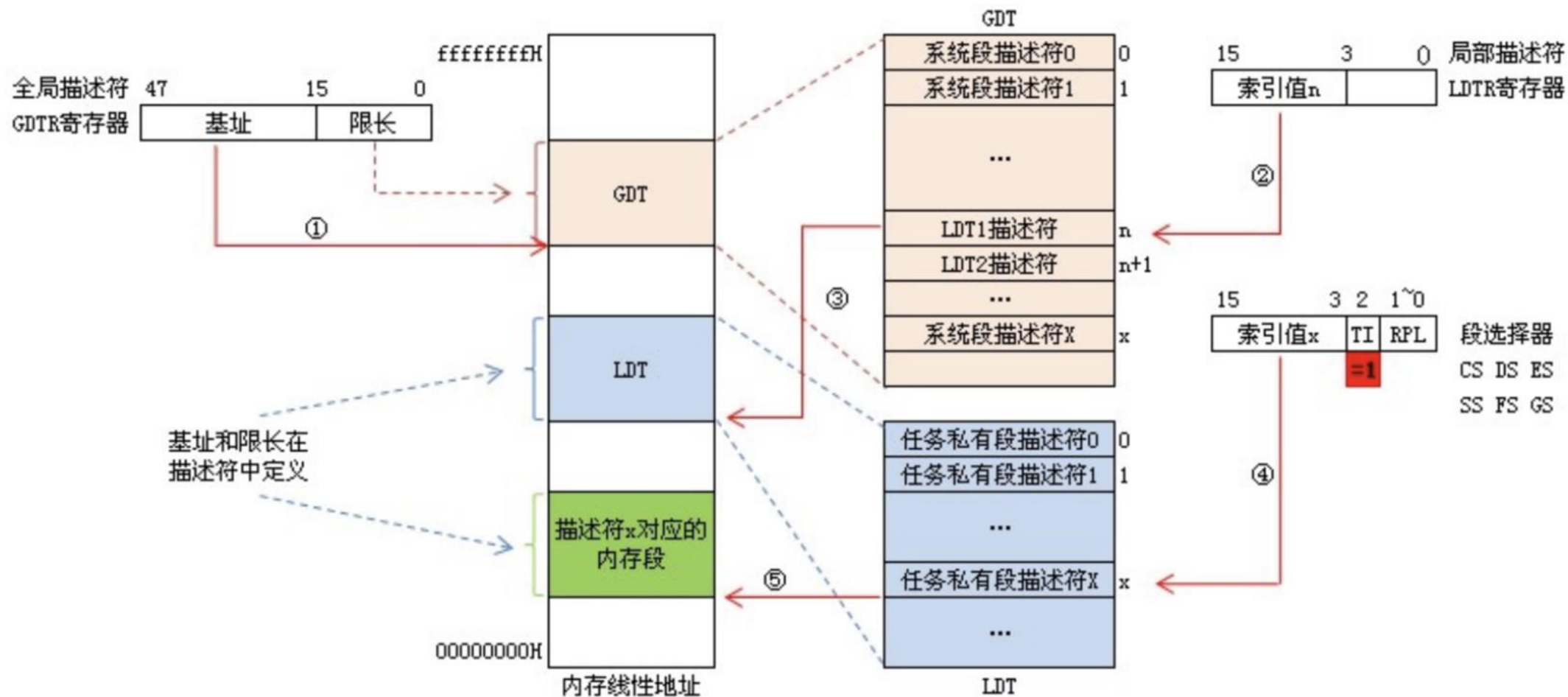
GDT查询物理地址

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





LDT查询物理地址





LDT查询物理地址

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





THANKS

