

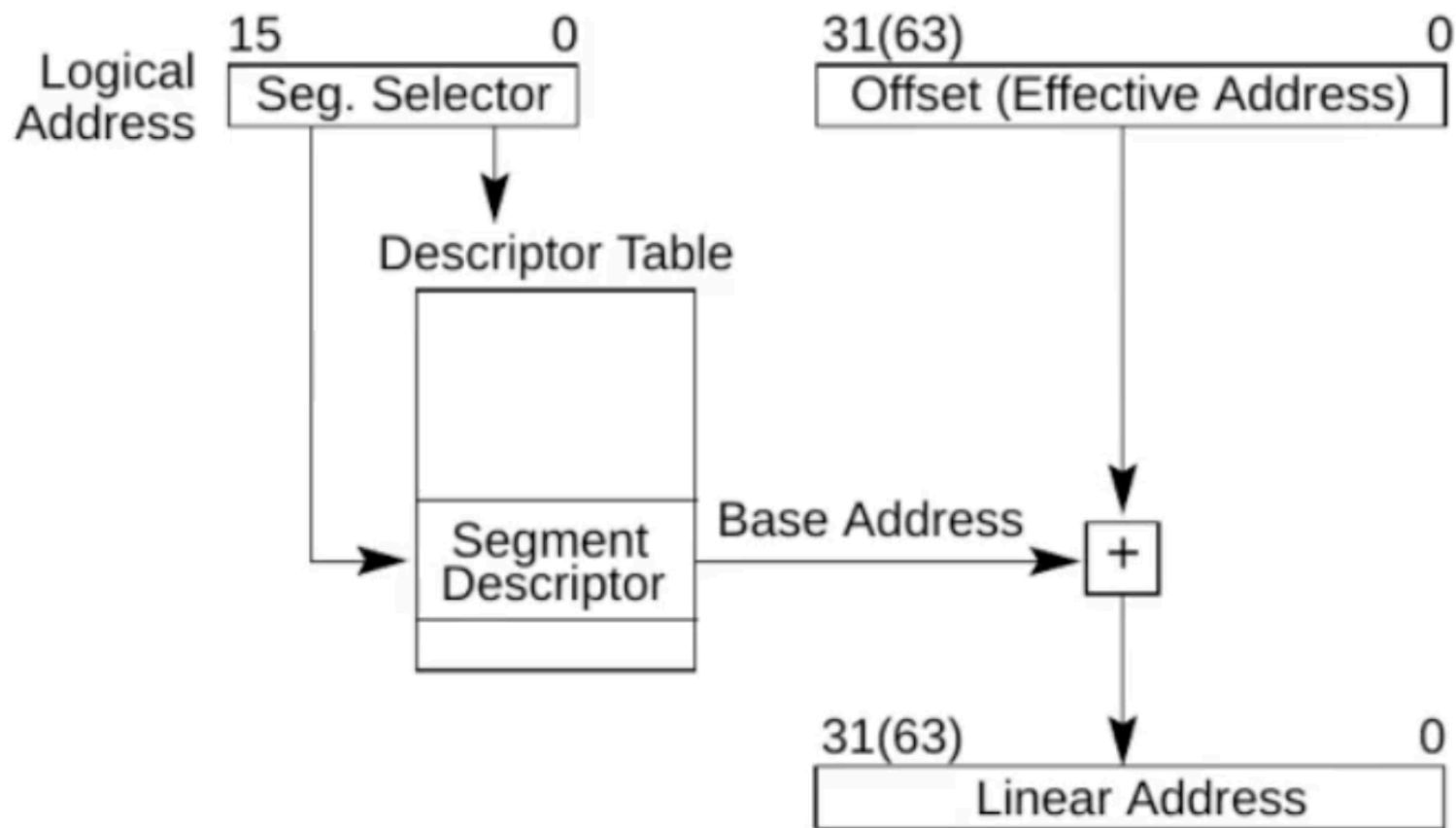
# 实模式与保护模式

陆建杰

# 实模式与保护模式

- 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
- 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

# 逻辑地址转线性地址

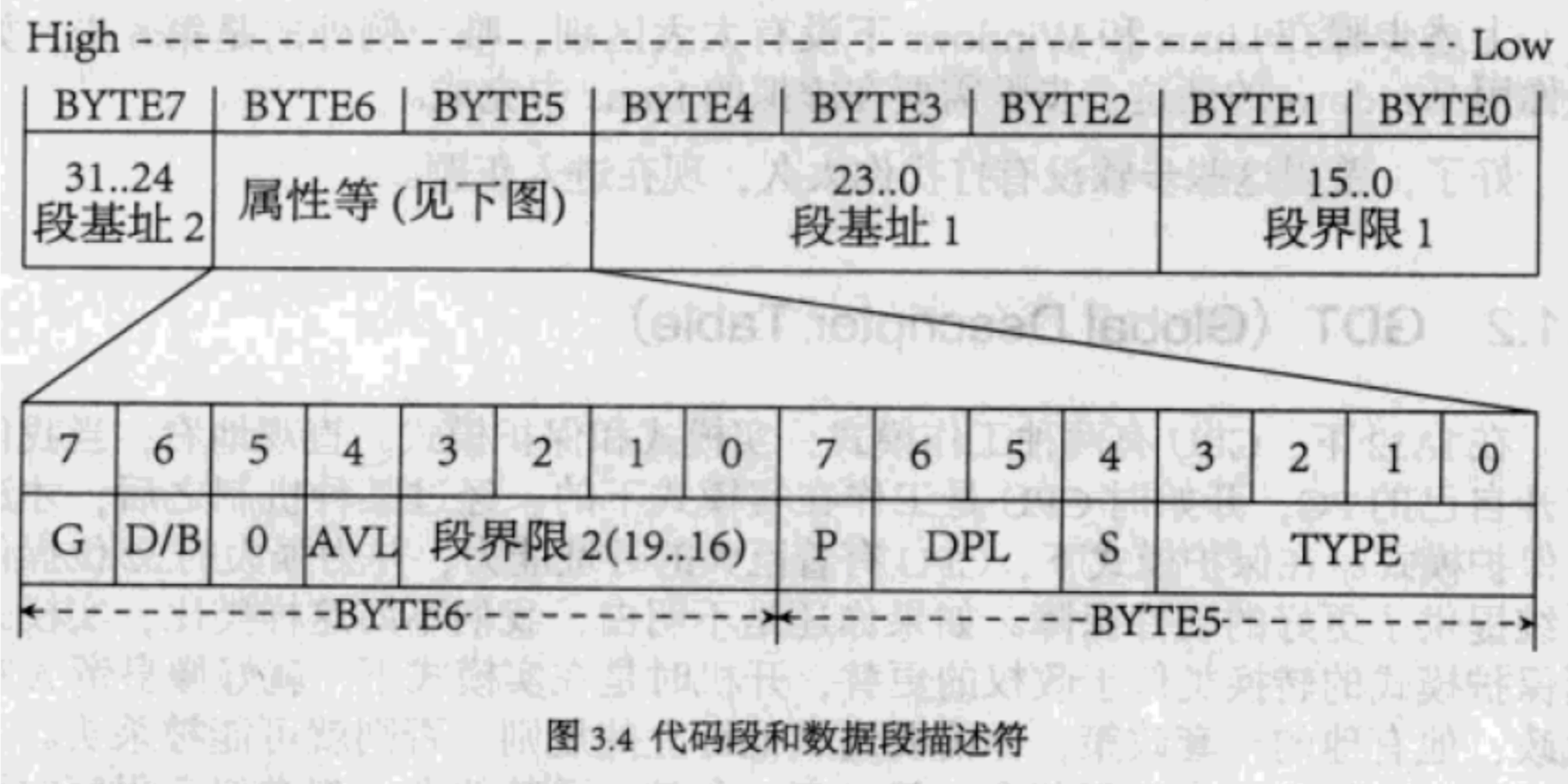


# 选择子

- 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方式还是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	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
描述符索引													TI	RPL	

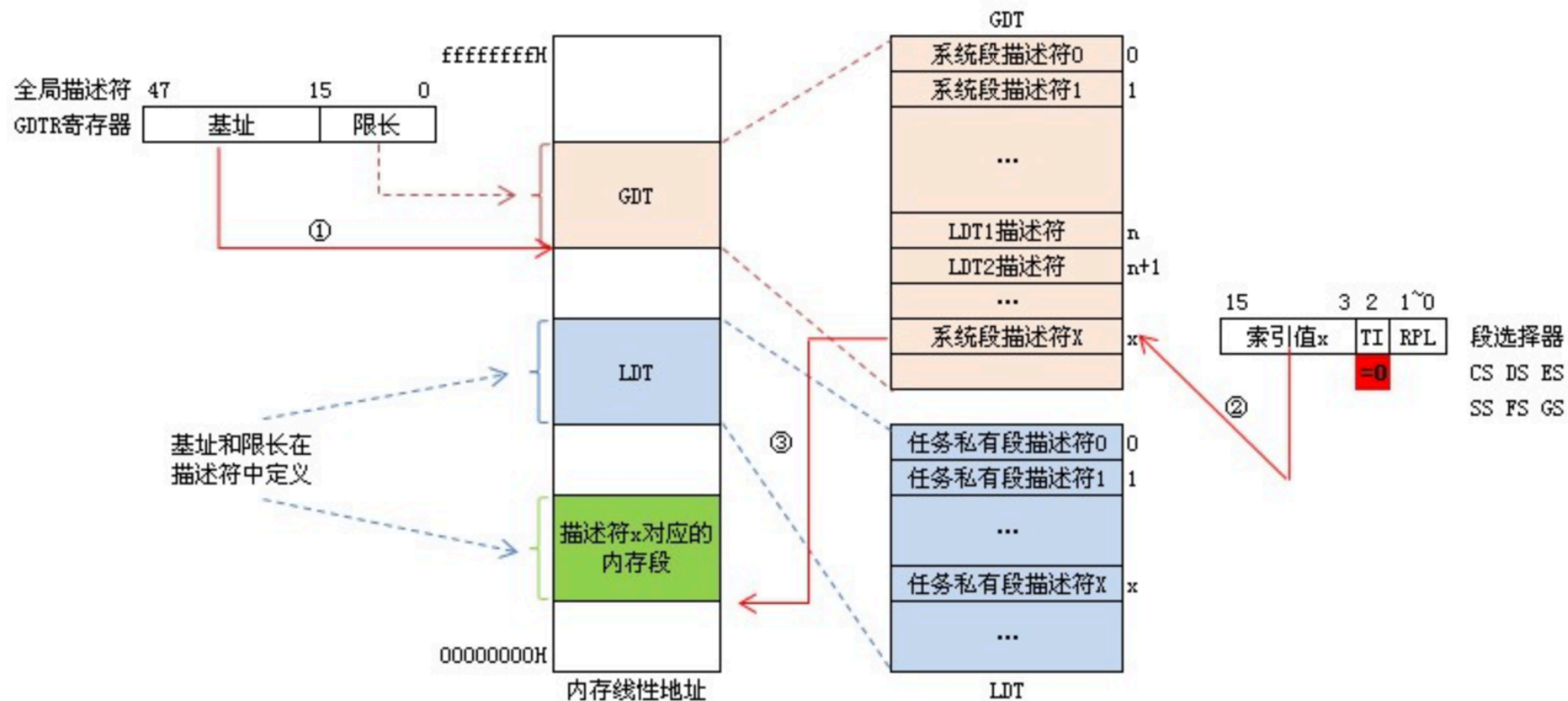
# 描述符



# 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

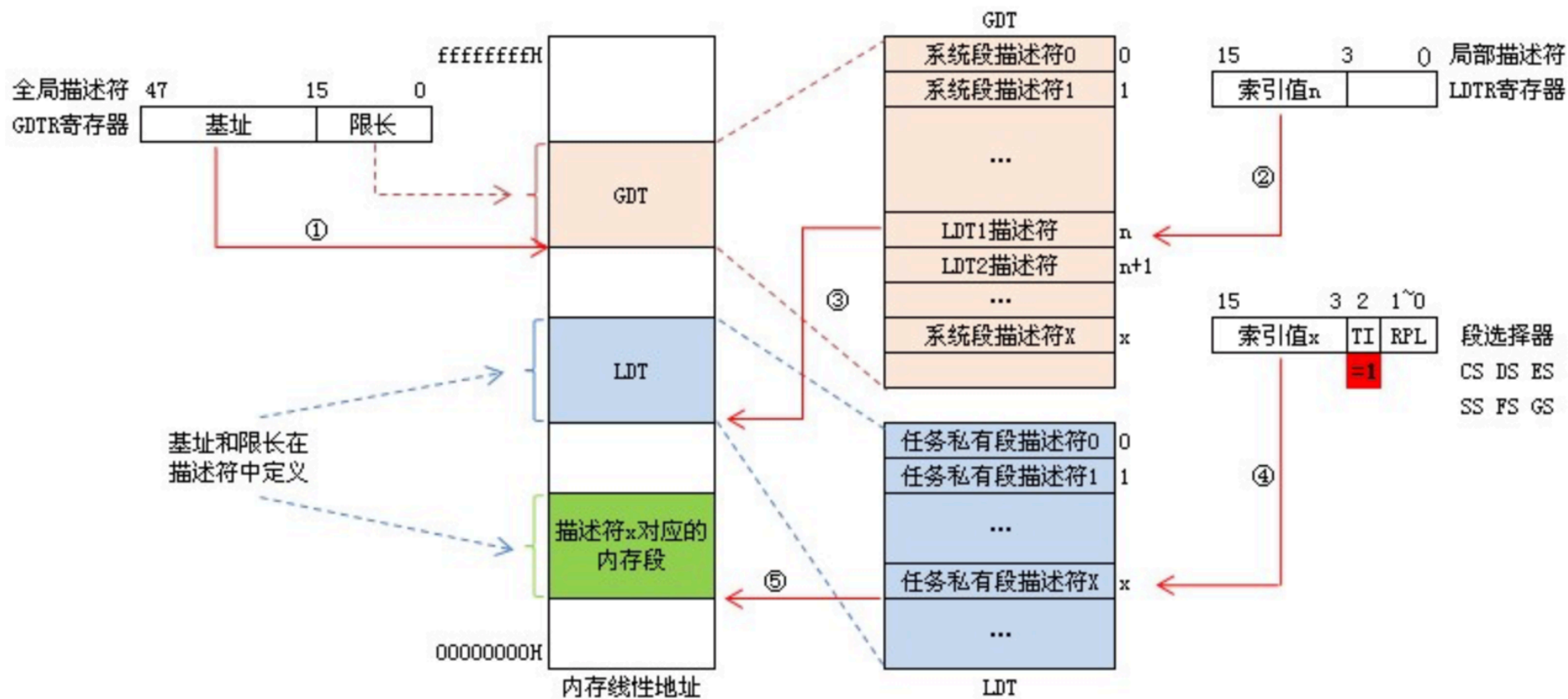


# GDT查询物理地址

- ( 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查找物理地址



# LDT查找物理地址

- ( 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。