实模式与保护模式

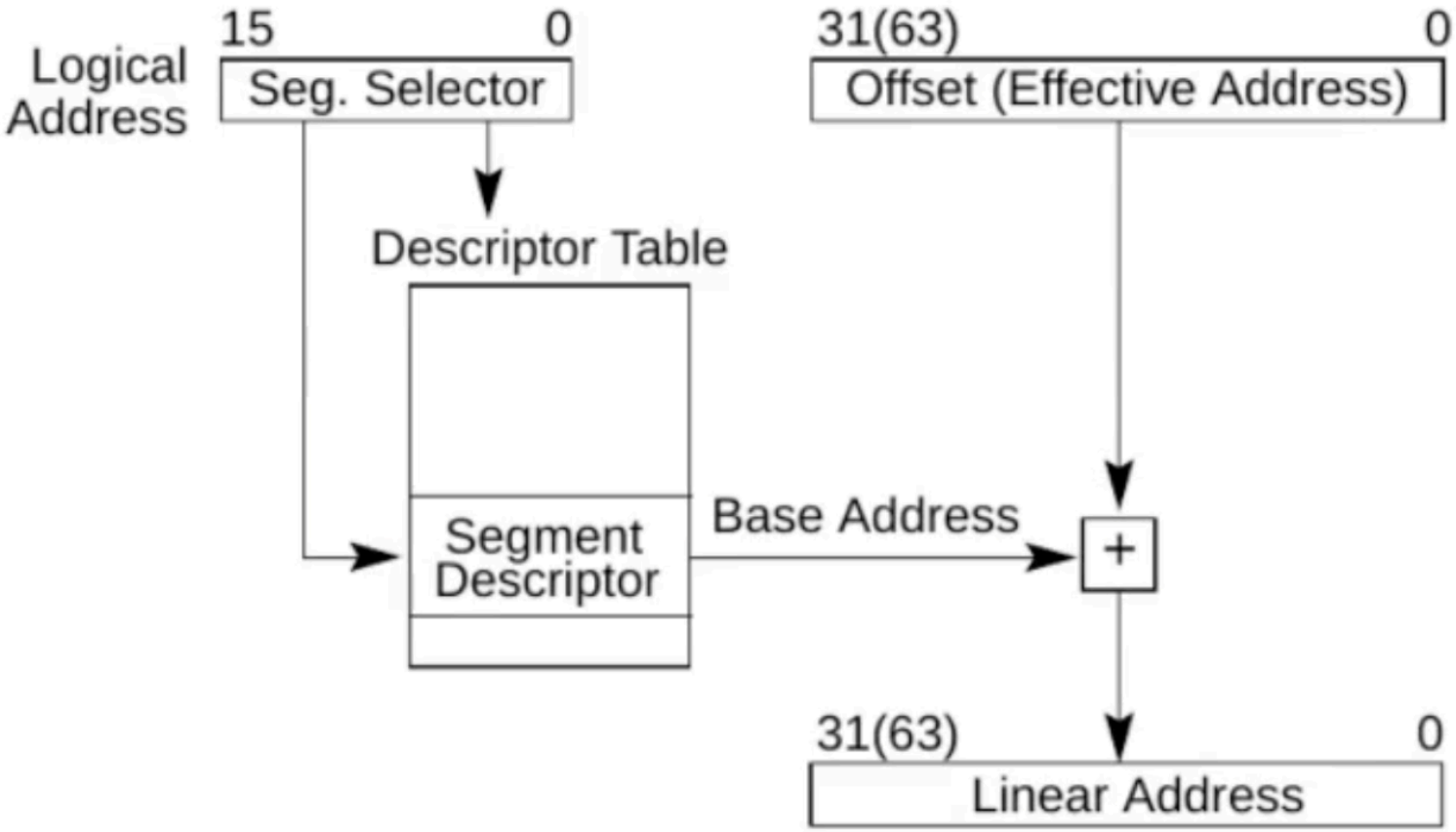
李之豪（zhli@smail.nju.edu.cn）

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

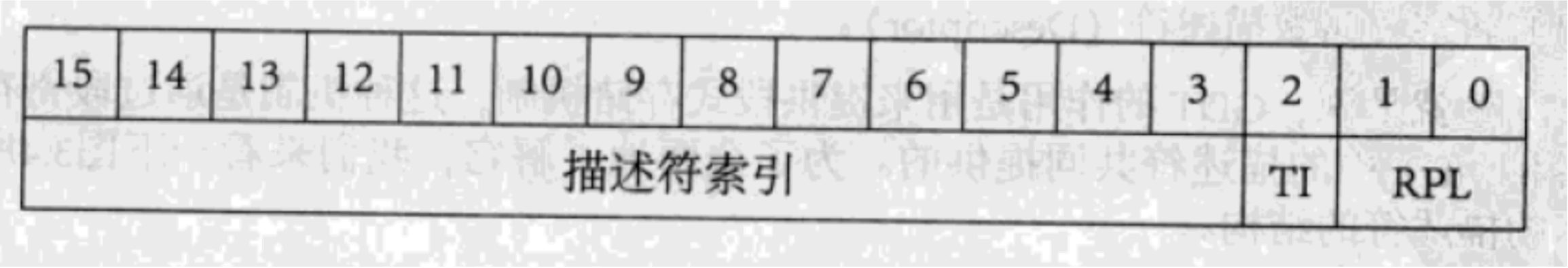
- 保护模式就是不能直接拿到物理地址的模式
  - 需要进行地址转换
  - 从80386开始，是现代操作系统的主要模式

逻辑地址转线性地址


15
0
Logical Address
Seg. Selector
31(63)
0
Offset (Effective Address)
Descriptor Table
Segment Descriptor
Base Address
+
31(63)
0
Linear Address

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）



描述符

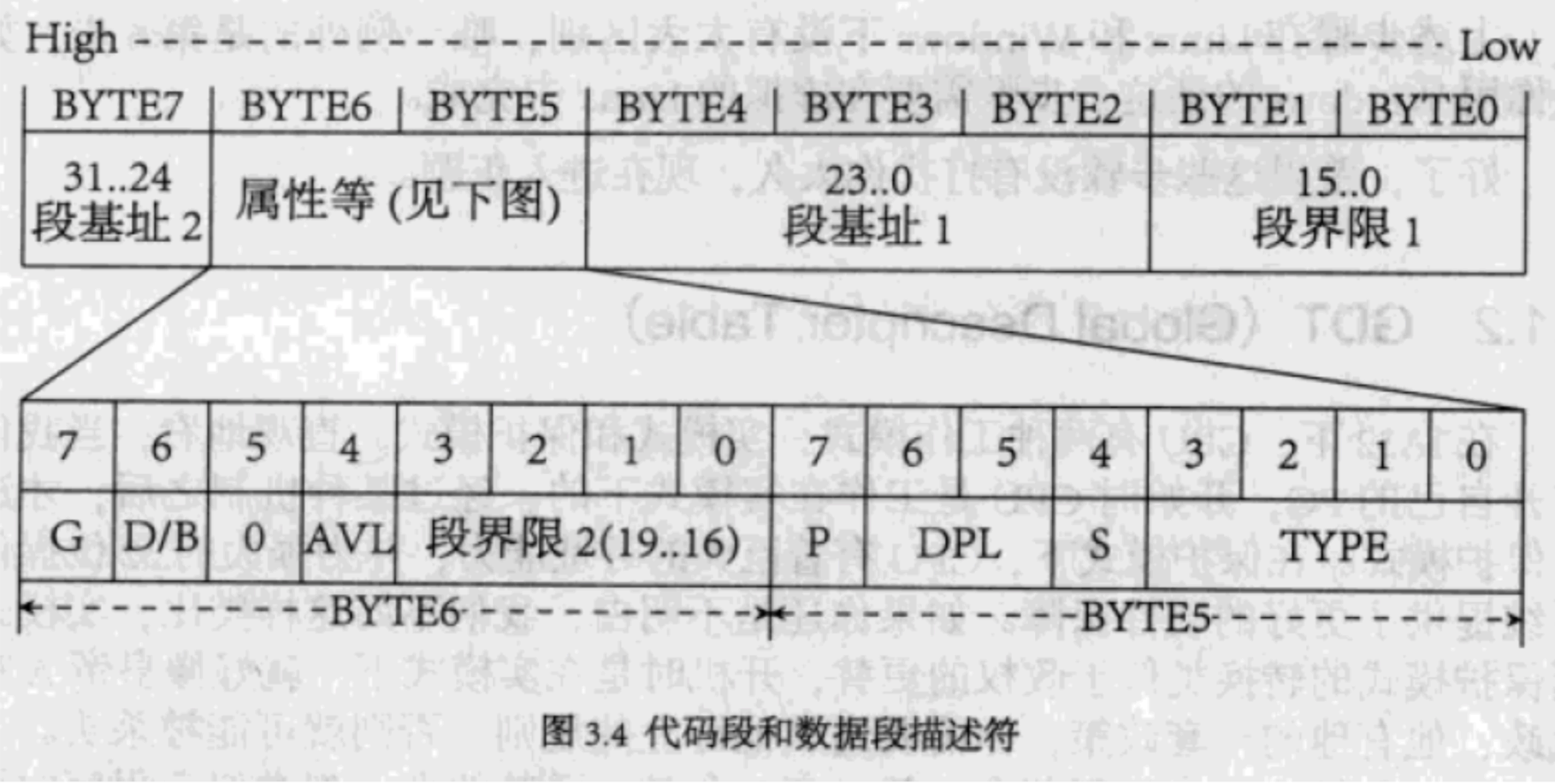


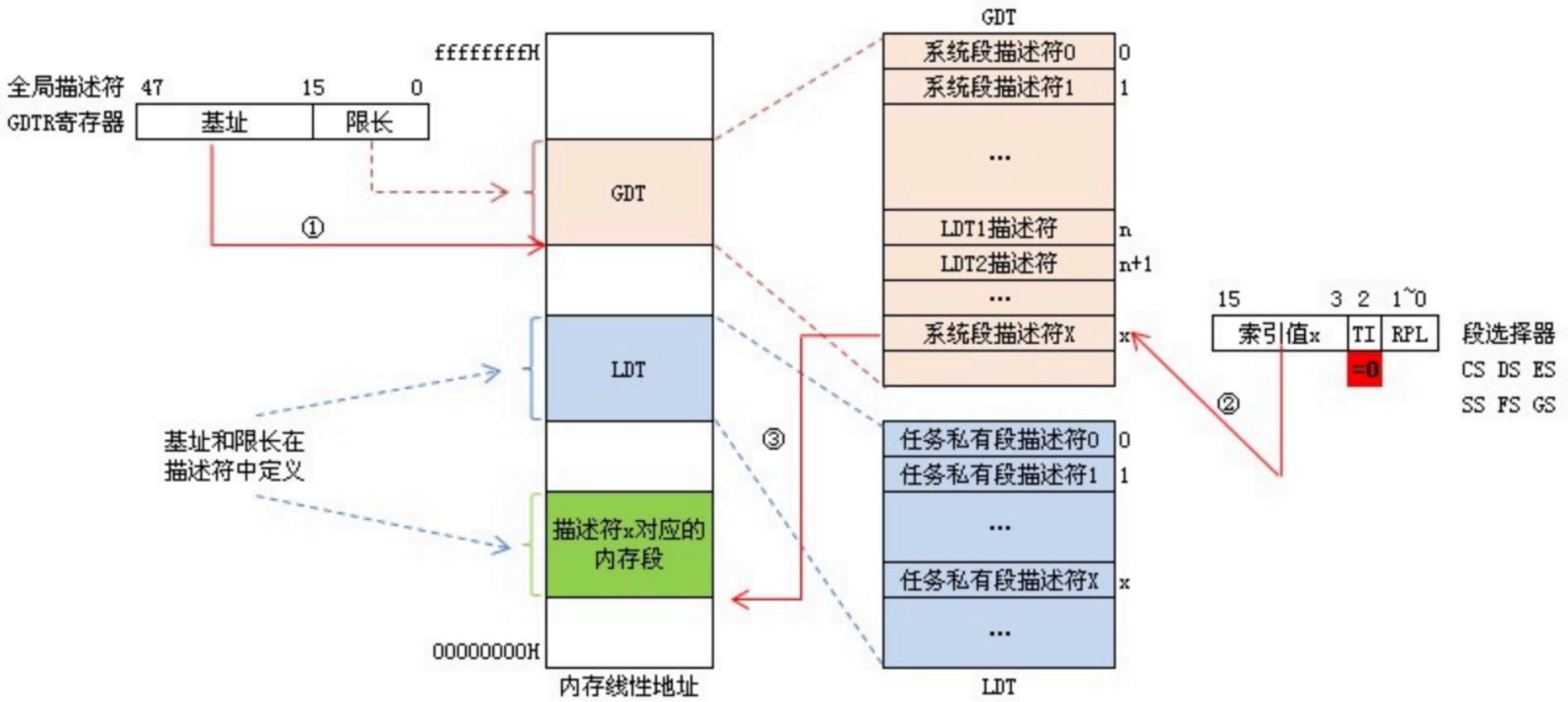
图 3.4 代码段和数据段描述符

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。

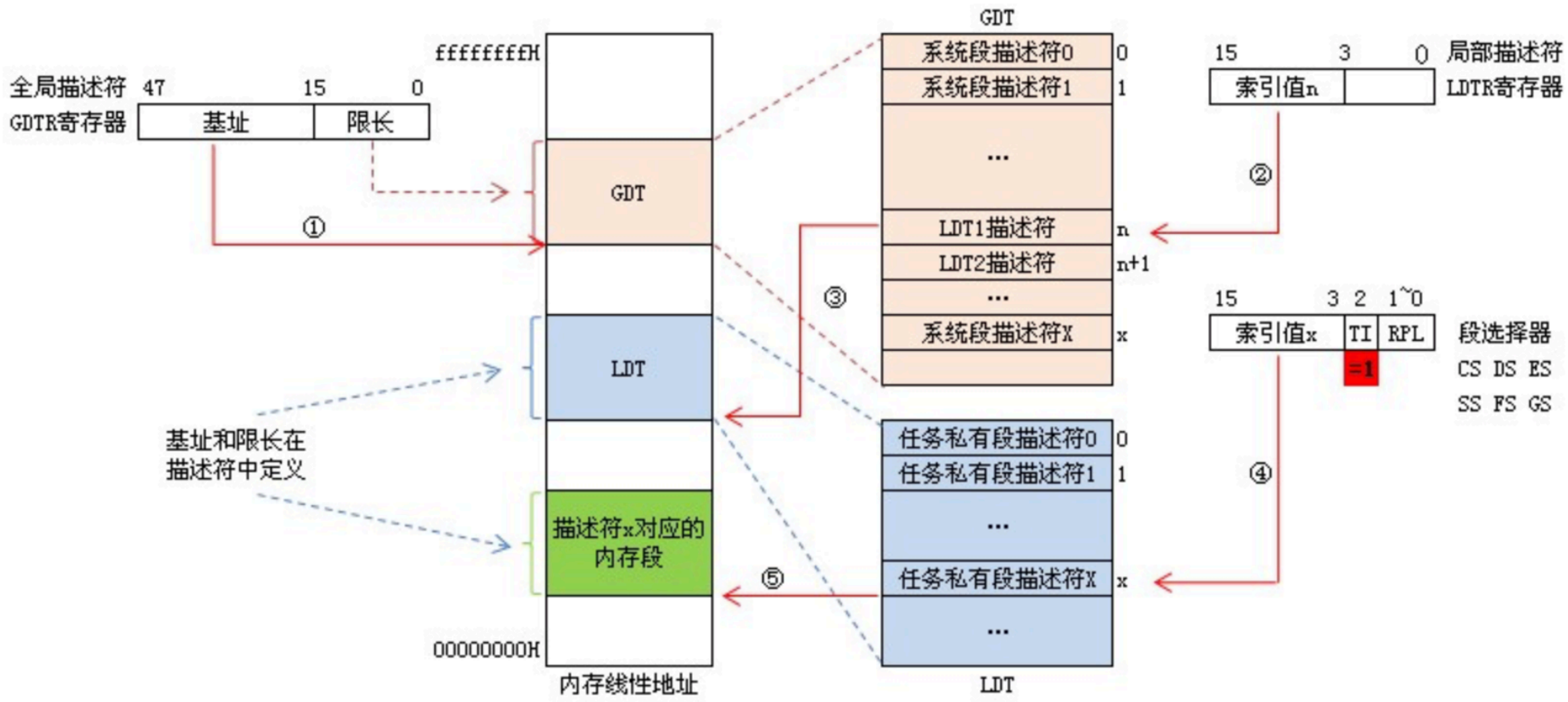
GDT查询物理地址


GDT
ffffffffH
全局描述符
47
15
0
GDTR寄存器
基址
限长
①
GDT
LDT
基址和限长在
描述符中定义
描述符x对应的
内存段
③
00000000H
内存线性地址
系统段描述符0
0
系统段描述符1
1
...
LDT1描述符
n
LDT2描述符
n+1
...
系统段描述符X
x
任务私有段描述符0
0
任务私有段描述符1
1
...
任务私有段描述符X
x
...
LDT
15
3
2
1~0
索引值x
TI
RPL
=0
段选择器
CS DS ES
SS FS GS
②

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


GDT
ffffffffH
全局描述符
GDTR寄存器
47
15
0
基址
限长
GDT
①
LDT
基址和限长在
描述符中定义
描述符x对应的
内存段
00000000H
内存线性地址
系统段描述符0
0
系统段描述符1
1
...
LDT1描述符
n
LDT2描述符
n+1
...
③
系统段描述符X
x
任务私有段描述符0
0
任务私有段描述符1
1
...
⑤
任务私有段描述符X
x
...
LDT
15
3
0
局部描述符
索引值n
LDTR寄存器
②
15
3
2
1~0
索引值x
TI
RPL
=1
段选择器
CS DS ES
SS FS GS
④

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。