|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| CR0 | | | | | | | | | | | | | |
| 31 | 30 | 29 | 。。。 | 18 | 17 | 16 | 。。。 | 5 | 4 | 3 | 2 | 1 | 0 |
| PG | CD | NW |  | AM |  | WP |  | NE | ET | TS | EM | MP | PE |
| PE=0时，CPU运行于实模式。 | | | | | | | | | | | | | |
| PE=1时，CPU运行于保护模式。 | | | | | | | | | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| lgdt [GdtPtr] | | | | | | |
| GdtPtr: | BYTE5 | BYTE4 | BYTE3 | BYTE2 | BYTE1 | BYTE0 |
| 32位基地址 | | | | 16位界限 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 选择子(Selector) | | | | | | | | | | | | | | | |
| BYTE1 | | | | | | | | BYTE0 | | | | | | | |
| 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| 描述符索引 | | | | | | | | | | | | | TI | RPL | |
| TI=0时，系统从当前的GDT中寻找描述符。 | | | | | | | | | | | | | | | |
| TI=1时，系统从当前的LDT中寻找描述符。 | | | | | | | | | | | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 描述符 | | | | | | | | | | | | | | | |
| BYTE7 | | BYTE6 | | BYTE5 | | BYTE4 | | BYTE3 | | BYTE2 | | BYTE1 | | BYTE0 | |
| 段基址2 | | 属性 | | | | 段基址1 | | | | | | 段界限1 | | | |
| BYTE6 | | | | | | | | BYTE5 | | | | | | | |
| 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| G | D/B | 0 | AVL | 段界限2 | | | | P | DPL | | S | TYPE | | | |
| G | | 段界限颗粒度 | | | | G=0时段界限颗粒度为字节 | | | | | | | | | |
| G=1 时段界限颗粒度为4KB | | | | | | | | | |
| D/B | | 在可执行代码段描述符中,  这一位叫D位: | | | | D=0时，在默认情况下使用16位地址及16位或8位操作数。 | | | | | | | | | |
| D=1时，在默认情况下使用32位地址及32位或8位操作数。 | | | | | | | | | |
| 在向下扩展数据段描述符中，这一位叫B位: | | | | B=0时，段的上部界限为64KB。 | | | | | | | | | |
| B=1时，段的上部界限为4GB。 | | | | | | | | | |
| 在描述堆栈段(由ss寄存器指向的段)的描述符中，这一位叫D位 | | | | D=0时，隐式的堆栈访问指令(push,pop,call)使用16位堆栈指针寄存器sp。 | | | | | | | | | |
| D=1时，隐式的堆栈访问指令(push,pop,call)使用32位堆栈指针寄存器sp。 | | | | | | | | | |
| AVL | | 保留 | | | | | | | | | | | | | |
| P | | P＝0时表示段在内存中不存在 | | | | | | | | | | | | | |
| P＝1时表示段在内存中存在 | | | | | | | | | | | | | |
| DPL | | 描述符特权级 | | | | | | | | | | | | | |
| S | | S＝0时表明描述符是系统段/门描述符 | | | | | | | | | | | | | |
| S＝1时表明描述符是数据段/代码段 | | | | | | | | | | | | | |
| TYPE | | 0X | Binary | | | | 数据段和代码段描述符 | | | | | | 系统段和门描述符 | | |
| 0 | 0 | 0 | 0 | 0 | 只读 | | | | | | 《未定义》 | | |
| 1 | 0 | 0 | 0 | 1 | 只读、已访问 | | | | | | 可用286TSS | | |
| 2 | 0 | 0 | 1 | 0 | 读/写 | | | | | | LDT | | |
| 3 | 0 | 0 | 1 | 1 | 读/写、已访问 | | | | | | 忙的286TSS | | |
| 4 | 0 | 1 | 0 | 0 | 只读、向下扩展 | | | | | | 286调用门 | | |
| 5 | 0 | 1 | 0 | 1 | 只读、向下扩展、已访问 | | | | | | 任务门 | | |
| 6 | 0 | 1 | 1 | 0 | 读/写、向下扩展 | | | | | | 286中断门 | | |
| 7 | 0 | 1 | 1 | 1 | 读/写、向下扩展、已访问 | | | | | | 286陷阱门 | | |
| 8 | 1 | 0 | 0 | 0 | 只执行 | | | | | | 《未定义》 | | |
| 9 | 1 | 0 | 0 | 1 | 只执行、已访问 | | | | | | 可用386TSS | | |
| A | 1 | 0 | 1 | 0 | 执行/读 | | | | | | 《未定义》 | | |
| B | 1 | 0 | 1 | 1 | 执行/读、已访问 | | | | | | 忙的386TSS | | |
| C | 1 | 1 | 0 | 0 | 只执行、一致代码段 | | | | | | 386调用门 | | |
| D | 1 | 1 | 0 | 1 | 只执行、一致代码段、已访问 | | | | | | 《未定义》 | | |
| E | 1 | 1 | 1 | 0 | 执行/读、一致代码段 | | | | | | 386中断门 | | |
| F | 1 | 1 | 1 | 1 | 执行/读、一致代码段、已访问 | | | | | | 386陷阱门 | | |

1、用lgdt加载GDTR

lgdt [GdtPtr]

2、关中断

cli

3、打开地址线A20

in al,92h

or al,00000010b

out 92h,al

4、置CR0的PE位

mov eax,cr0

or eax,1

mov cr0,eax

5、跳转

加载LDTR

mov ax,SelectorLDT

lldt ax

特权级 特权级 特权级

低->高 高->低 相同

一致代码段 YES NO YES

非一致代码段 NO NO YES

数据段 NO YES YES

CPL、DPL、RPL

CPL CPL是当前执行的程序或任务的特权级，既当前段寄存器的第0、1位的值。

特殊情况，当遇到一致代码段时。因为一致代码段可以被相同或更低级的代码段访问，所以当处理器访问一个与CPL特权级不同的一致代码段时，CPL不会被改变。

DPL DPL表示段或者门的特权级，既段或者门的DPL位的值。

数据段

DPL规定了可以访问此代码段的最低特权级。比如，一个数据段的DPL是1，那么只有运行在0或者1的程序才有权访问。

非一致代码段(不使用调用门的情况下)

DPL规定了可以访问此代码段的特权级。比如，一个非一致代码段的DPL是0，那么只有CPL为0的程序才有权访问。

调用门

DPL规定了访问此调用门的最低特权级。同数据段。

一致代码段和通过调用门访问的非一致代码段

DPL规定了访问此段的最高特权级。比如一个一致代码段的DPL是2，那吗CPL是0和1的程序将无法访问此段。

TSS

DPL规定了访问TSS的最低特权级。同数据段。

RPL

RPL是段选择子的0，1位的值。

RPL和CPL谁的权限低，则由谁起决定性作用。

调用门的特权级规则 调用门可改变CPL的特权级

call jmp

目标是一致代码段 CPL<=DPL\_G

RPL<=DPL\_G

DPL\_B<=CPL

目标是非一致代码段 CPL<=DPL\_G CPL<=DPL\_G

RPL<=DPL\_G RPL<=DPL\_G

DPL\_B<=CPL DPL\_B=CPL

调用门描述符：

BYTE7 BYTE6 |BYTE5 BYTE4 |BYTE3 BYTE2 |BYTE1 BYTE0

偏移 |属性 |选择子 |偏移

BYTE5 |BYTE4

7 |6 5 |4 |3 2 1 0 |7 |6 |5 |4 3 2 1 0

P |DPL |S |TYPE |0 |0 |0 |ParamCount

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| TSS描述符 | | | | | | |
| BYTE3 | BYTE2 | BYTE1 | BYTE0 | |  |  |
| 0000 0000 | | 链接字段 | | | 00H | 00 |
| ESP0 | | | | | 04H | 04 |
| 0000 0000 | | SS0 | | | 08H | 08 |
| ESP1 | | | | | 0CH | 12 |
| 0000 0000 | | SS1 | | | 10H | 16 |
| ESP2 | | | | | 14H | 20 |
| 0000 0000 | | SS2 | | | 18H | 24 |
| CR3 | | | | | 1CH | 28 |
| EIP | | | | | 20H | 32 |
| EFLAGS | | | | | 24H | 36 |
| EAX | | | | | 28H | 40 |
| ECX | | | | | 2CH | 44 |
| EDX | | | | | 30H | 48 |
| EBX | | | | | 34H | 52 |
| ESP | | | | | 38H | 56 |
| EBP | | | | | 3CH | 60 |
| ESI | | | | | 40H | 64 |
| EDI | | | | | 44H | 68 |
| 0000 0000 | | ES | | | 48H | 72 |
| 0000 0000 | | CS | | | 4CH | 76 |
| 0000 0000 | | SS | | | 50H | 80 |
| 0000 0000 | | DS | | | 54H | 84 |
| 0000 0000 | | FS | | | 58H | 88 |
| 0000 0000 | | GS | | | 5CH | 92 |
| 0000 0000 | | LDT | | | 60H | 96 |
| I/O 许可位图偏移 | | 0000 0000 | | T | 64H | 100 |