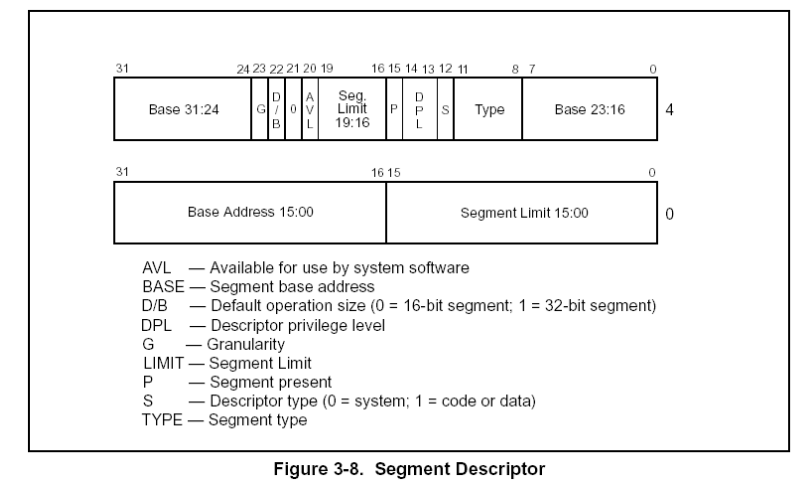
# 一、课后笔记



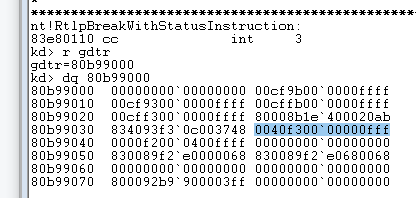
今天讲了 limit, base address, type, p, g，S 这几个位。

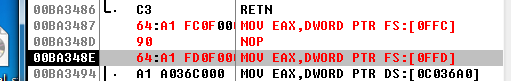
Base是基址，就我目前学到的来说，除了FS的base是随着线程变化以外，其他的段描述符base都是0.所以 比如 ds:[0] 就是逻辑地址0，fs:[0] 就不是了。

Address和base加起来好像就是线性地址了。？不确定。总之寻址的时候要加起来。

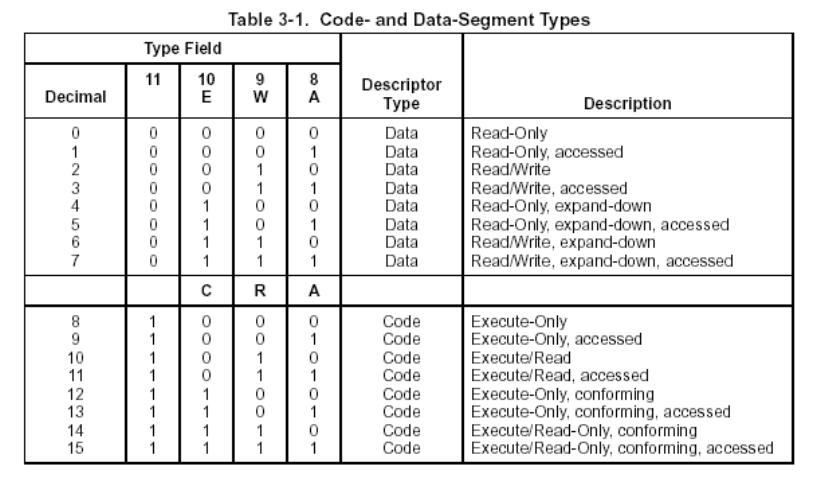
P表示描述符是否有效，1表示有效，0表示无效。

Limit和G放在一起说，G表示粒度，G=1表示页粒度(4KB)，G=0表示字节粒度。LIMIT是限制地址范围的，limit假设是FFFFF，此时如果G=1，地址范围是 (FFFFF+1)\*0X1000-1=0XFFFFFFFF，即4GB；如果G=0，则limit是多少，地址范围就是多少。课上还是以FS举例，FS是3B，对应的段描述符是 0040f300`00000fff,limit就是fff，再看G粒度是0，就是字节粒度，所以FS的范围是FFF，这时候如果dword ptr fs:[0xffc]，是没问题的，但只要再往后一点点，就不行了，超范围了。





S和type应该是要放在一起讲的，S=1就是数据或代码段，然后可以查一个表：



课上以11为例说明，这是表示可读可执行，被访问过的意思。

# 二、作业

拆段描述符。

按照这种格式拆分

limit:fffff 20

base:00000000 基址=0

type:b 11

s:1

DPL:3

P:1 vaild

avl:0

def:0

d/b:1

G:1 页为单位的 zai pc intel amd 1个页是4096个字节 转化为16进制 0x1000

80b99000 00000000`00000000 00cf9b00`0000ffff

80b99010 00cf9300`0000ffff 00cffb00`0000ffff

80b99020 00cff300`0000ffff 80008b1e`400020ab

80b99030 834093f2`cc003748 0040f300`00000fff

80b99040 0000f200`0400ffff 00cf7300`0001ffff

80b99050 830089f2`a0000068 830089f2`a0680068

80b99060 00000000`00000000 00000000`00000000

80b99070 800092b9`900003ff 00000000`00000000

80b99080 00000000`00000000 00000000`00000000

80b99090 00000000`00000000 00000000`00000000

80b990a0 850089d1`d1c00068 00000000`00000000

80b990b0 00000000`00000000 00000000`00000000

80b990c0 00000000`00000000 00000000`00000000

80b990d0 00000000`00000000 00000000`00000000

80b990e0 00000000`80b99100 00009200`0000ffff

80b990f0 830098e3`997003b2 00009200`0000ffff

80b99100 00000000`80b99108 00000000`80b99110

80b99110 00000000`80b99118 00000000`80b99120

80b99120 00000000`80b99128 00000000`80b99130

80b99130 00000000`80b99138 00000000`80b99140

80b99140 00000000`80b99148 00000000`80b99150

80b99150 00000000`80b99158 00000000`80b99160

80b99160 00000000`80b99168 00000000`80b99170

80b99170 00000000`80b99178 00000000`80b99180

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 段描述符 | Limit | Base | Type | P | Dpl | S | G | D/B | DEF(0) | AVL |
| 00000000`00000000 |  |  |  |  |  |  |  |  |  |  |
| 00cf9b00`0000ffff | fffff | 00000000 | b | 1 | 0 | 1 | 1 | 1 | 0 | 0 |
| 00cf9300`0000ffff | fffff | 00000000 | 3 | 1 | 0 | 1 | 1 | 1 | 0 | 0 |
| 00cffb00`0000ffff | fffff | 00000000 | b | 1 | 3 | 1 | 1 | 1 | 0 | 0 |
| 00cff300`0000ffff | fffff | 00000000 | 3 | 1 | 3 | 1 | 1 | 1 | 0 | 0 |
| 80008b1e`400020ab | 020ab | 801e4000 | b | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 834093f2`cc003748 | 03748 | 83f2cc00 | 3 | 1 | 0 | 1 | 0 | 1 | 0 | 0 |
| 0040f300`00000fff | 00fff | 00000000 | 3 | 1 | 3 | 1 | 0 | 1 | 0 | 0 |
| 0000f200`0400ffff | 0ffff | 00000400 | 2 | 1 | 3 | 1 | 0 | 0 | 0 | 0 |
| 00cf7300`0001ffff | fffff | 00000000 | 3 | 0 | 3 | 1 | 1 | 1 | 0 | 0 |
| 830089f2`a0000068 | 00068 | 83f2a000 | 9 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 830089f2`a0680068 | 00068 | 83f2a068 | 9 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 00000000`00000000 |  |  |  |  |  |  |  |  |  |  |
| 00000000`00000000 |  |  |  |  |  |  |  |  |  |  |
| 800092b9`900003ff | 003ff | 80b99000 | 2 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 00000000`00000000 |  |  |  |  |  |  |  |  |  |  |
| 00000000`00000000 |  |  |  |  |  |  |  |  |  |  |
| 00000000`00000000 |  |  |  |  |  |  |  |  |  |  |
| 00000000`00000000 |  |  |  |  |  |  |  |  |  |  |
| 00000000`00000000 |  |  |  |  |  |  |  |  |  |  |
| 850089d1`d1c00068 | 00068 | 85d1d1c0 | 9 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 00000000`00000000 |  |  |  |  |  |  |  |  |  |  |
| 00000000`00000000 |  |  |  |  |  |  |  |  |  |  |
| 00000000`00000000 |  |  |  |  |  |  |  |  |  |  |
| 00000000`00000000 |  |  |  |  |  |  |  |  |  |  |
| 00000000`00000000 |  |  |  |  |  |  |  |  |  |  |
| 00000000`00000000 |  |  |  |  |  |  |  |  |  |  |
| 00000000`00000000 | limit | base | type | p | dpl | s | g | D/b | Def(0) | avl |
| 00000000`80b99100 | 09100 | 000080b9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 00009200`0000ffff | 0ffff | 00000000 | 2 | 1 | 0 | 1 | 0 | 0 | 0 | 0 |
| 830098e3`997003b2 | 003b2 | 83e39970 | 8 | 1 | 0 | 1 | 0 | 0 | 0 | 0 |
| 00009200`0000ffff | 0ffff | 00000000 | 2 | 1 | 0 | 1 | 0 | 0 | 0 | 0 |
| 00000000`80b99108 | 09108 | 000080b9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 00000000`80b99110 | 9110 | 000080b9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 00000000`80b99118 | 9118 | 000080b9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 00000000`80b99120 | 9120 | 000080b9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 00000000`80b99128 | 9128 | 000080b9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 00000000`80b99130 | 9130 | 000080b9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 00000000`80b99138 | 9138 | 000080b9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 00000000`80b99140 | 9140 | 000080b9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 00000000`80b99148 | 9148 | 000080b9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 00000000`80b99150 | 9150 | 000080b9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 00000000`80b99158 | 9158 | 000080b9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 00000000`80b99160 | 9160 | 000080b9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 00000000`80b99168 | 9168 | 000080b9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 00000000`80b99170 | 9170 | 000080b9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 00000000`80b99178 | 9178 | 000080b9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 00000000`80b99180 | 9180 | 000080b9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
|  |  |  |  |  |  |  |  |  |  |  |