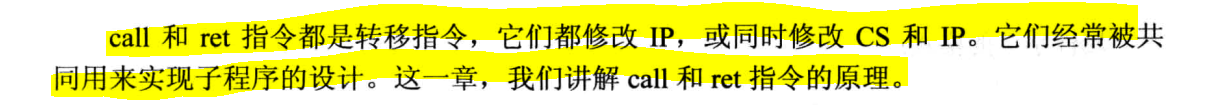
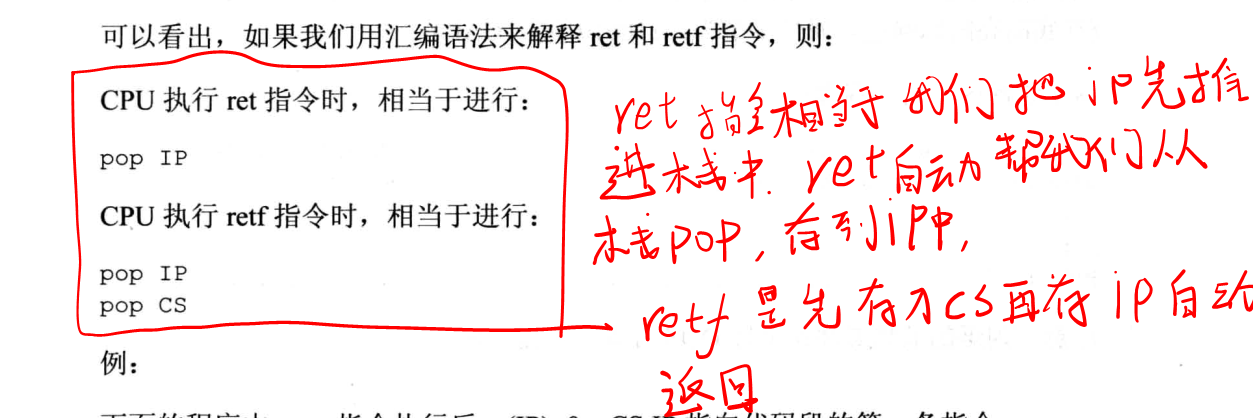


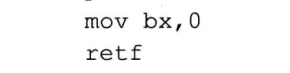
**call和ret**



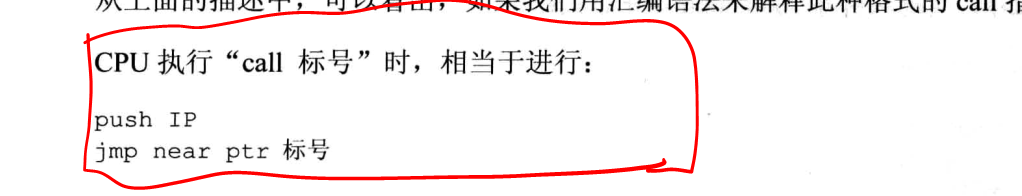
所以这条指令要求我们先推入ip 或者加上cs，所以这个指令不需要我们在后面加上偏移地址等



用法



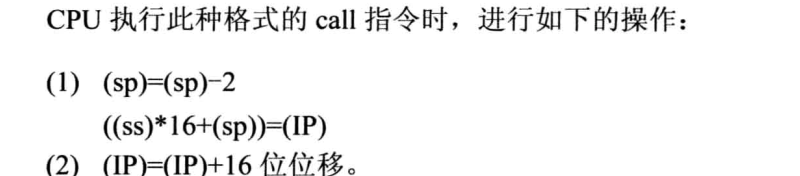
**call**



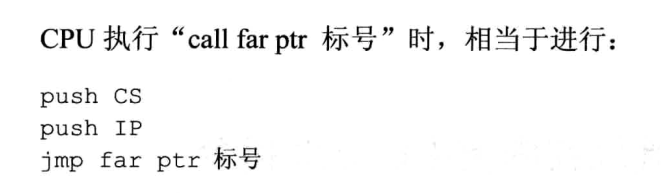
截图.png

通过原理和执行发现，call的命令 ，就是利用栈跳转到

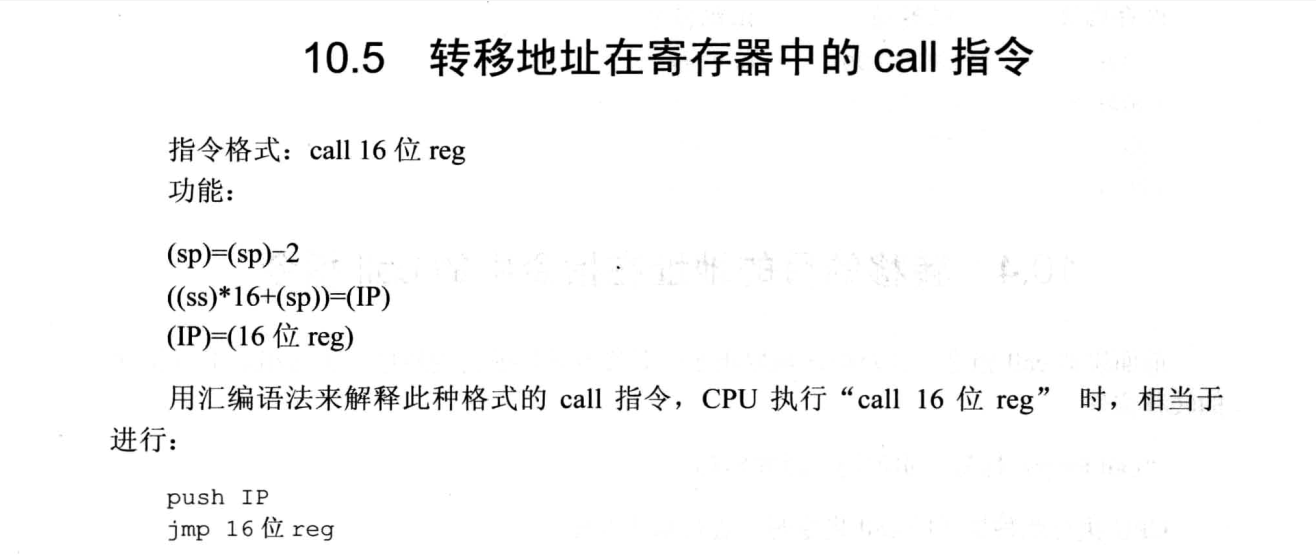
16位偏移量的s位置，这个和 jump near ptr相似，段内偏移



按照上面理解 不用再讲述了原理如下



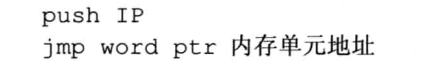
这些指令真的复杂



**我感觉call的本意是存放跳转之前的指令位置，存到堆栈中**

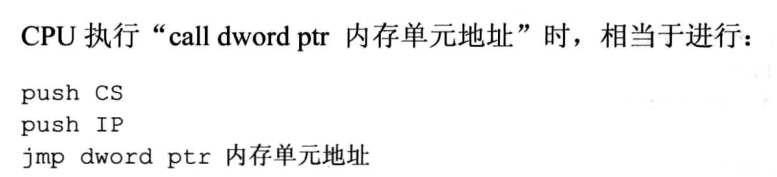
截图.png

**word 16字节，所以存入ip后sp自动加2 ，这个ip存放的是下一条指令的ip**

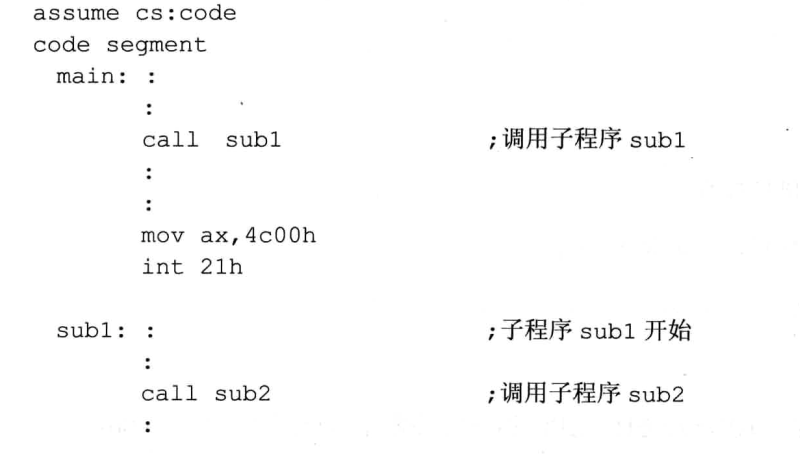


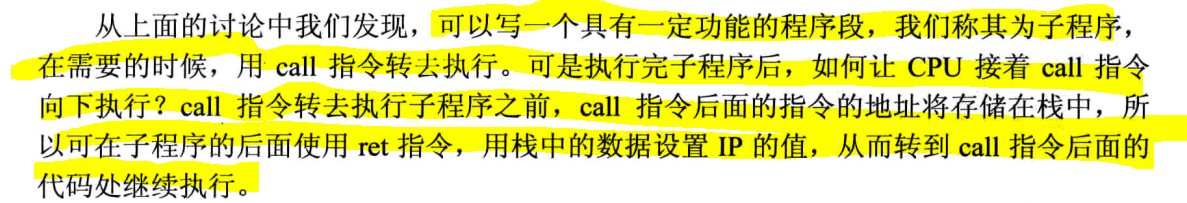
截图.png

**这条指令，dword ptr 是32位的两个字单元，拆分成cs和ip，所以向堆栈中存放时是存放2个字单元，而不是一次sp加4，是分开加两次**



**子程序写法**





**mul指令**

