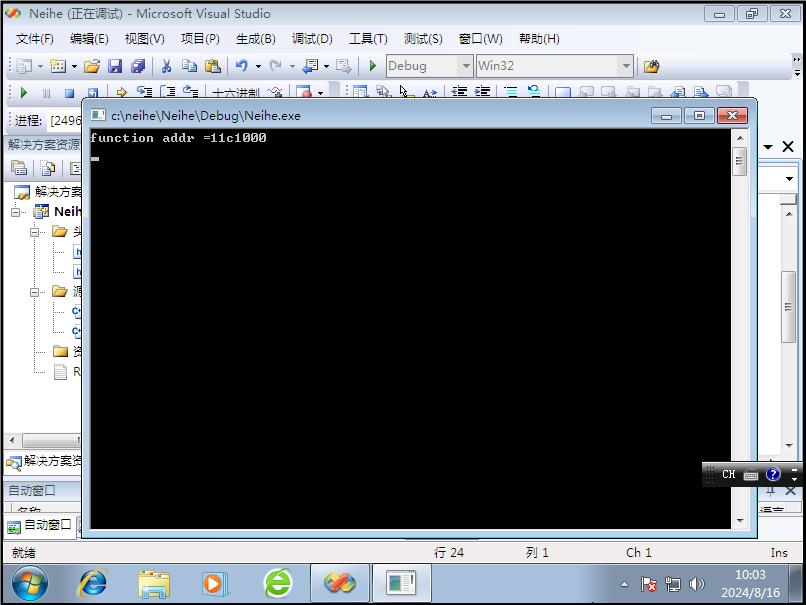
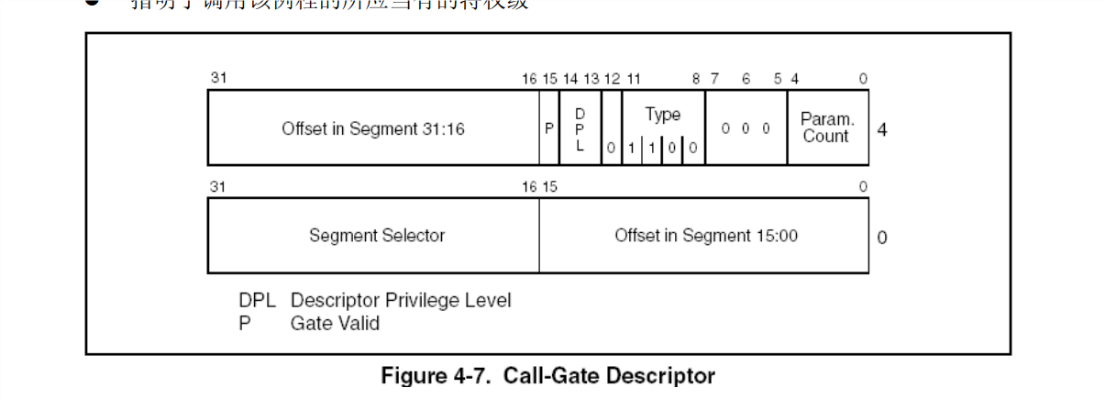
# 环境

环境：win7x86



拿到方法的地址，通过修改段描述符来跳转到这个方法



kd> r cs

cs=00000008

说明R0运行在00000008这个段选择子

需要跳转的地址为011c1000

拼接这个调用门

011cec0000081000

kd> r gdtr

gdtr=80b95000

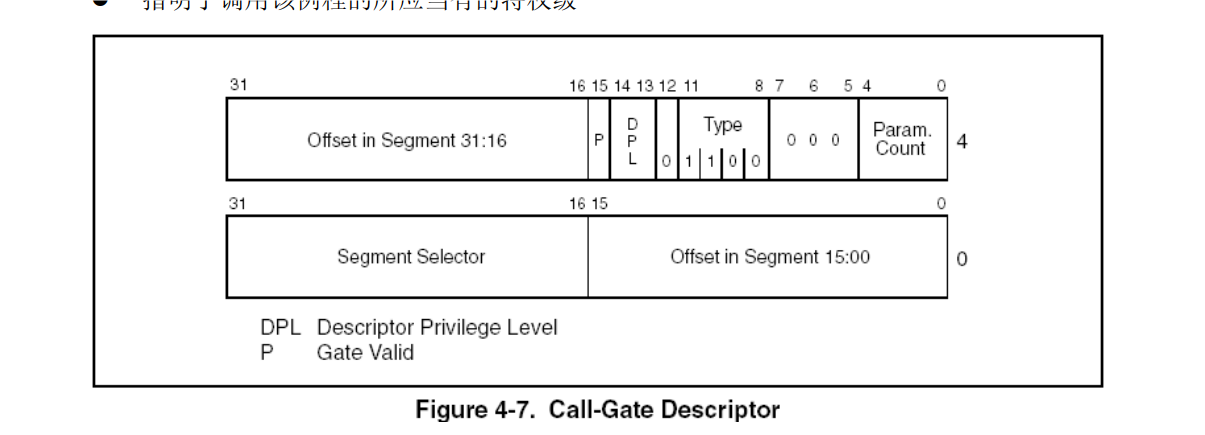
//代码中使用了长跳转 cs=0x48；根据段选择子 01001 000

01001=9

80b95000+9\*8=80B9 5048

eq 80b95048 011cec0000081000

# 资料



S位等于0时， Type的含义 1100为调用门，1110为中断门

