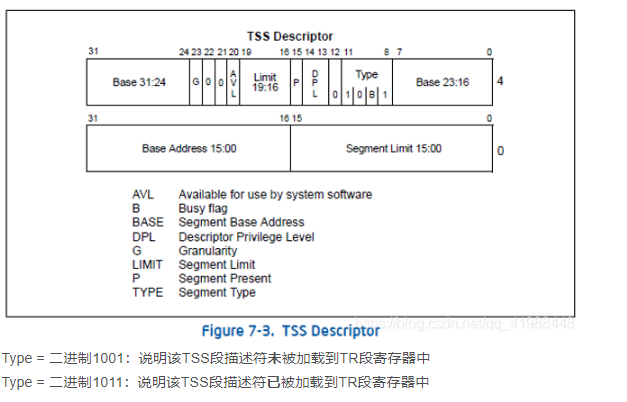
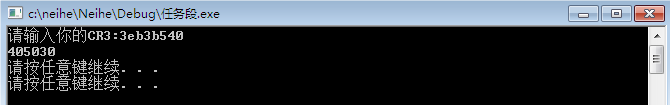
# 环境

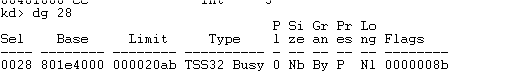
环境：win7x86









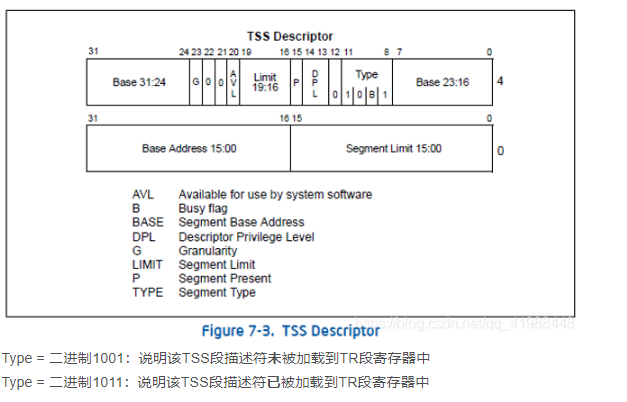




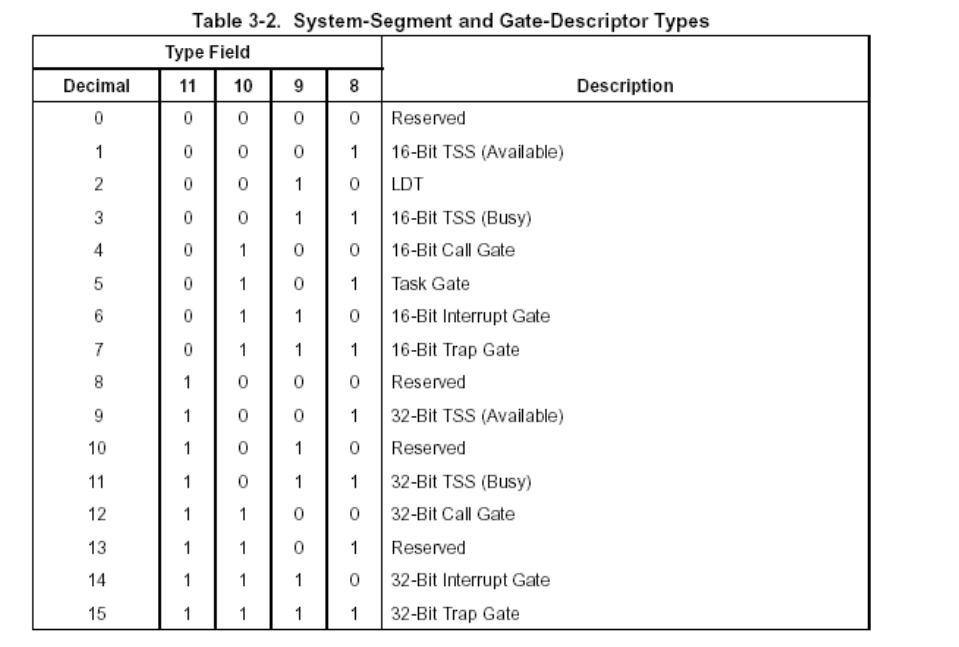
将任务段的地址405030写入gdt+48的位置 base=00405030

0000e940`503020ab :按字节分配20ab的空间 G=0:字节 segment：分配的空间

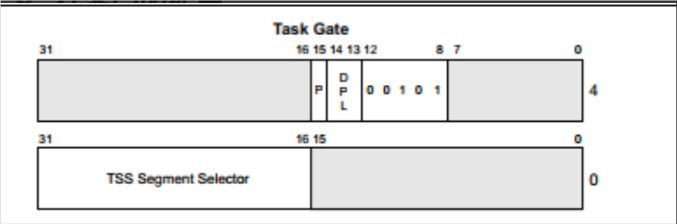
# 资料



S位等于0时， Type的含义 1100为调用门，1110为中断门，1001为空闲任务段，1011为工作任务段



任务门



R0：00008500 XXXX0000

R3：0000E500 XXXX0000