# 分析bootloader进入保护模式的过程。

## 1. 基本知识

在区别I/O空间和内存空间的进程的I/O空间写入数据

outb() I/O上写入8位数据（1字节）；

outw() I/O上写入16位数据（1字节）；

outl() I/O上写入32位数据（1字节）；

inb() I/O上读出8位数据（1字节）；

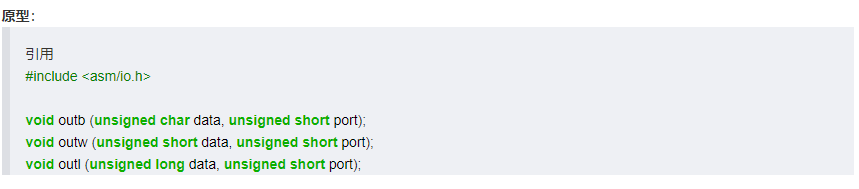
inw() I/O上读出16位数据（1字节）

intl() I/O上读出32位数据（1字节）；

movb 传送8位

movw 传送16位

movl 传送32位



in、out都是对I/O端口进行操作。ioreadb、iowriteb等是对I/O内存操作。

## 2、为何开启A20以及如何开启A20

为了将1M（20位）的寻址空间拓展到4G（32位）的寻址空间。从而得进行相应处理。总共包括开启A20，建立GDT、将CR0的bit0位置成1。其中在开启A20之前，BIOS需要关中断、清除方向标志、将AX、DS、ES、SS置0。

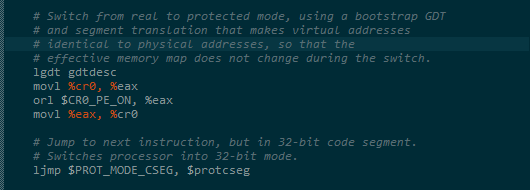




开启A20的两个关键端口port 0x64、port 0x60.

## 3、如何初始化GDT表

## 4、如何使能和进入保护模式



Lgdt gdtdesc 将GDT表的首地址加载到GDTR,剩下三个指令是将CRO寄存器的最低位置一，这标志着系统进入保护模式。跳转指令实现的是跳转到下一个指令的位置，其中$PROT\_MODE\_CSEG代表的是段选择子，也即段的基地址。