电子科技大学

计算机科学与工程学院

标 准 实 验 报 告

（实验）课程名称 计算机操作系统

电子科技大学教务处制表

电 子 科 技 大 学

电 子 科 技 大 学

实　验　报　告

二、实验项目名称：内存地址转换实验

三、实验学时：2 学时

四、实验原理：

在段页式系统中，段标识符加上偏移量就可以得到逻辑地址。

根据段标识符的 T1 字段可以知道段标识符存放在 LDT 还是 GDT 中。寄存器 GDTR 存放 GDT 的地址，LDTR 存放 LDT 在 GDT 的偏移量。若在 LDT 中，则用 GDT 的地址加上 LDT 在 GDT 的偏移量得到 LDT 的地址。LDT 的地址加上 DS 寄存器获取的 DS 段在 LDT 中索引位置，得到段的基址。段的基址加上偏移量就是线性地址。

根据线性地址的划分规则可以知道页目录索引，页表索引，偏移。页目录地址存放在 cr3 寄存器中。因此页目录地址加上页目录索引得到页表地址。页表地址加上页表索引得到页地址。页地址加上偏移得到实际的物理地址。

本次实验划分页目录共有 1024 项，每项占用 4 位，共用了 12 位，因此后 3 个 16 进制数为偏移量，基地址后 3 个 16 进制数为 0。其他同理。

五、实验目的：

（1）掌握计算机的寻址过程
（2）掌握页式地址地址转换过程
（3）掌握计算机各种寄存器的用法

六、实验内容：

本实验运行一个设置了全局变量的循环程序，通过查看段寄存器，LDT 表，GDT 表等信息，经过一系列段、页地址转换，找到程序中该全局变量的物理地址。

七、实验器材（设备、元器件）：

Linux 内核（0.11）+Bochs 虚拟机

八、实验步骤：

1.编写实验源文件

```
#include<stdio.h>
int j=          ;
int main(){
printf("the address of j is 0x%x\n",&j);
while(j);
printf("program terminated normally!\n");
return 0;}
```

2.运行该程序，输出 j 的段内偏移量 0x3004

```
[/usr/root]# gcc -o mytest mytest.c
[/usr/root]# ./mytest
the address of j is 0x3004
```

3.输入 sreg 命令，查看段的具体信息

```
<bochs:2> sreg
es:0x0017, dh=0x10c0f300, dl=0x00003fff, valid=1
        Data segment, base=0x10000000, limit=0x03ffffff, Read/Write, Accessed
cs:0x000f, dh=0x10c0fb00, dl=0x00000002, valid=1
        Code segment, base=0x10000000, limit=0x00002fff, Execute/Read, Accessed,
 32-bit
ss:0x0017, dh=0x10c0f300, dl=0x00003fff, valid=1
        Data segment, base=0x10000000, limit=0x03ffffff, Read/Write, Accessed
ds:0x0017, dh=0x10c0f300, dl=0x00003fff, valid=3
        Data segment, base=0x10000000, limit=0x03ffffff, Read/Write, Accessed
fs:0x0017, dh=0x10c0f300, dl=0x00003fff, valid=1
        Data segment, base=0x10000000, limit=0x03ffffff, Read/Write, Accessed
gs:0x0017, dh=0x10c0f300, dl=0x00003fff, valid=1
        Data segment, base=0x10000000, limit=0x03ffffff, Read/Write, Accessed
ldtr:0x0068, dh=0x000082fa, dl=0xa2d00068, valid=1
tr:0x0060, dh=0x00008bfa, dl=0xa2e80068, valid=1
gdtr:base=0x0000000000005cb8, limit=0x7ff
idtr:base=0x00000000000054b8, limit=0x7ff
```

4.ds 段的段标识符信息是 0x0017（0000 0000 0001 0111）,对应 TI=1，表明段描述符在 LDT 中，右移 3 位之后为 0x02，即表示在局部描述符表 LDT 的偏移量为 2

5.LDTR 寄存器存放了 LDT 在 GDT 的位置,0x0068 对应 TX=0，右移 3 位之后为 0x0D，即在 GTD 中的索引为 13

6.gdtr 存放了 GDT 的起始地址（0x5cb8），加上索引 13，可以得到地址为 0x5cb8+13*8，因为索引对应的描述符占 8 位。查看对应项可以得到 LDT 段描述符

```
<bochs:3> xp /2w 0x00005cb8+13*8
[bochs]:
0x0000000000005d20 <bogus+       0>:    0xa2d00068      0x000082f9
```

7.根据 LDT 段描述符的格式可以得到 LDT 的基址为 0x00f9a2d0

8.LDT 的基址加上 ds 段的偏移量 2 可以得到 ds 段对应的表项地址

0x00f9a2d0+2*8

```
<bochs:4> xp /2w 0x00f9a2d0+2*8
[bochs]:
0x0000000000f9a2e0 <bogus+       0>:    0x00003fff      0x10c0f300
```

9.计算得 ds 基地址为 0x10000000，和 sreg 中 ds 的 base 字段即基地址相同

10.用 ds 基地址加上程序输出的 j 的段内偏移量，得到线性地址 0x10003004，按照线性地址划分的方式，10 位页目录索引为 0x40，10 位页表索引为 0x03，12 位偏移为 0x04

11.页目录表的地址放在 CPU 的 cr3 寄存器中，所以用 creg 查看值，说明页目录表起始地址为 0

```
<bochs:5> creg
CR0=0x8000001b: PG cd nw ac wp ne ET TS em MP PE
CR2=page fault laddr=0x0000000010002fa8
CR3=0x0000000000000000
    PCD=page-level cache disable=0
    PWT=page-level write-through=0
CR4=0x00000000: smep osxsave pcid fsgsbase smx vmx osxmmexcpt osfxsr pce pge mce
 pae pse de tsd pvi vme
EFER=0x00000000: ffxsr nxe lma lme sce
```

12.页目录表起始地址加上页目录索引为 0+0x40*4，查看此地址得到页表基址 0x00fa9000

```
<bochs:7> xp /2w 0x40*4
[bochs]:
0x0000000000000100 <bogus+       0>:    0x00fa9027      0x00000000
```

13.页表基址加上页表索引为 0x00fa9000+0x03*4，查看此地址得到数据页基址 0x00fa7000

```
<bochs:8> xp /w 0x00fa9000+3*4
[bochs]:
0x0000000000fa900c <bogus+       0>:    0x00fa7067
```

14.数据页基址加上偏移为 0x00fa7000+0x04，此为物理地址，查看此地址得到 j 的值

```
<bochs:9> xp /w 0x00fa7000+4
[bochs]:
0x0000000000fa7004 <bogus+       0>:
```

15.设置 j 的数据为 0，程序能够正常退出

```
<bochs:10> setpmem 0x00fa7004 4 0
<bochs:11> xp /w 0x00fa7000+4
[bochs]:
0x0000000000fa7004 <bogus+       0>:    0x00000000
<bochs:12> c
```

```
 Ok.
[/usr/root]# ./mytest
the address of  j is 0x3004
program terminated normally!
[/usr/root]#
```

九、实验数据及结果分析：

成功修改物理地址的数据，程序正常退出。

十、实验结论：

成功理解了段页地址转换，并且成功找到物理地址并修改数据。

十一、总结及心得体会：

深刻理解了段页地址转换的过程，从逻辑地址到线性地址，线性地址到物理地址的转换。

十二、对本实验过程及方法、手段的改进建议：

无。

报告评分：

指导教师签字：