第八章作业

191220008 陈南曈

3、

（1）

程序的功能是在标准输出设备stdout上输出字符串"Hello, world."。

（2）

执行到第16行、第20行的“int $0x80”指令时。

（3）

第 16 行指令调用了 4 号系统调用 write，对应服务例程为 sys_write()函数；第 20 行指令调用了 1 号系统调用 exit, 对应服务例程为 sys_exit()函数。

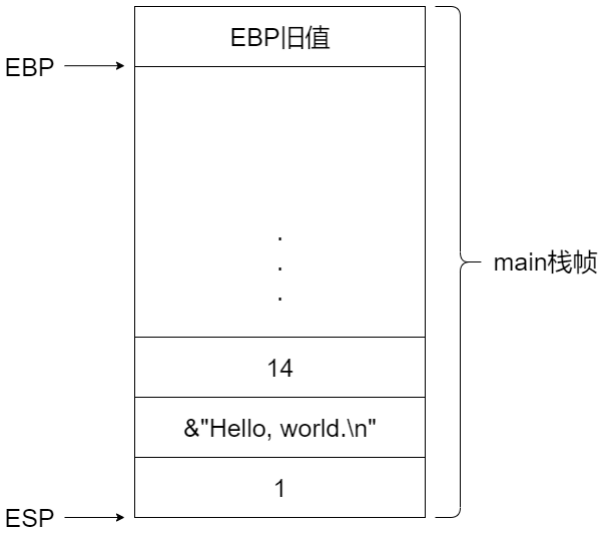
4、

（1）

main 函数在自身栈帧中传递了三个参数：

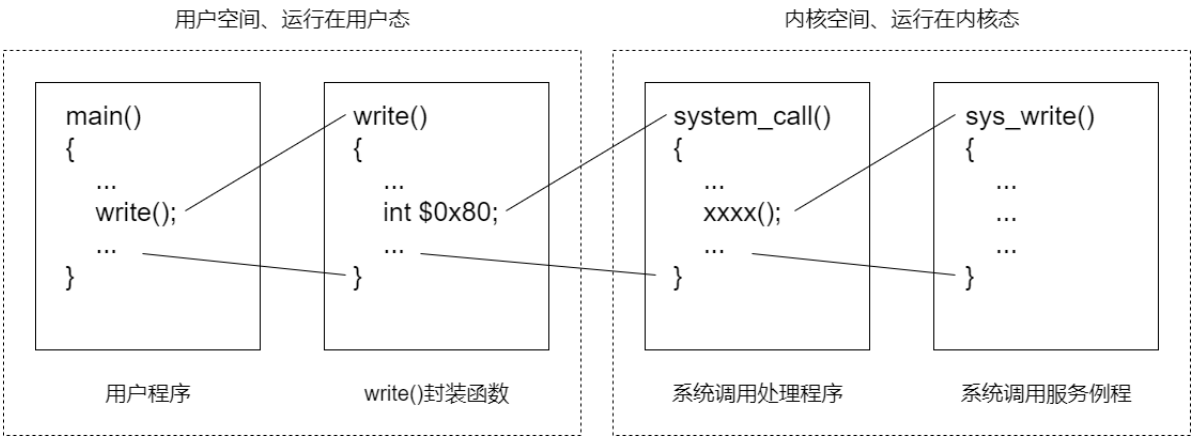
在 R[esp]+8 处存放了 14（第一个参数），R[esp]+4 处存放指向字符串”Hello world.\n” 的指针（第二个参数），最后在 R[esp] 处存放了 1（第三个参数）。

main栈帧示意图如下：



（2）

函数调用关系如下：



（3）

① 第3题的实现方式的便捷性和灵活性都不如本题中的实现方式：第1题采用汇编程序设计方式，若参数发生变化，就需要重新编写不同的指令；而本题采用高级语言程序设计方式，使用封装好的函数，只需要改变实参，就可以完成不同的功能。

② 第3题的实现方式执行性能更好，执行时间更短：第3题使用汇编实现时，省去了高级程序语言中大量的函数调用，节省了大量时间，故执行效率更好，执行时间更短。

5、

（1）

因为 hello.c 中使用了 c 标准库函数 printf()，这个函数的原型说明在 stdio.h 中，所以应该在 main.c 的开头加“#include <stdio.h>”。

因为在 hello.c 的开头加了“#include <stdio.h>”，printf()函数在 stdio.h 中被声明，因此，在预处理后，printf() 函数的原型说明被嵌入到了hello.c 中，使得链接器在进行链接的时候，能够从标准 c 库中得到 printf 模块的信息，完成链接工作。

（2）

需要经过预处理、编译、汇编、链接才能生成可执行文件 hello, 然后通过启动 hello 程序执行。

预处理阶段主要是对带 # 的语句进行处理。

编译阶段主要是将预处理后的源程序文件编译生成汇编语言程序。

汇编阶段主要是将汇编语言源程序转换为可重定位的机器语言目标代码文件。

链接阶段将多个可重定位的机器语言目标代码以及库函数链接起来， 生成最终的可执行文件。

（3）

因为 printf() 函数默认的输出设备为标准输出设备 stdout（即屏幕），所以无需指定字符串的输出目的地。执行了 hello 程序后，自动会在 stdout 设备 （屏幕）上显示字符串。

（4）

根据"Hello, world.\n"字符串中每个字符的ASCII码，可知在机器中的0/1序列（机器码）为：

“48H 65H 6CH 6CH 6FH 2CH 77H 6FH 72H 6CH 64H 0AH 00H”

这个0/1序列存放在hello.o文件的.rodata节中。

这个0/1序列在可执行文件hello的只读数据段中。

（5）

若采用静态链接，printf.o模块所在静态库libc.a中。静态链接后，printf.o 中的代码部分 (.text 节) 被映射到虚拟地址空间的只读代码段中。

若采用动态链接，则函数 printf() 的代码在虚拟地址空间中的共享库映射区。

（6）

```
804f8fa: 53                 push %ebx                    //将被调用者保存寄存器EBX入栈
804f8fb: 86 54 24 10        mov 0x10(%esp), %edx         //将字符串长度14送入EDX
804f8ff: 8b 4c 24 0c        mov 0xc(%esp), %ecx          //将字符串首地址送入ECX
804f903: 8b 5c 24 08        mov 0x8(%esp), %ebx          //将文件描述符fd=1送入EBX
804f907: b8 04 00 00 00     mov $0x4, %eax               //将系统调用号4送入EAX
804f90c: cd 80              int $0x80                    //进入系统调用处理程序
system_call执行
804f90e: 5d                 pop %ebx                     //恢复EBX的旧值
804f90f: 3d 01 f0 ff ff     cmp $0xfffff001, %eax        //将系统调用返回值与
0xfffff001比较
804f914: 0f 83 f6 1f 00 00  jae 8051910<__syscall_error>//大于等于时，转出错处理
804f91a: c3                 ret                          //返回到调用write的过程
```

该Linux系统中系统调用反蝴蝶最大错误号时4095。

因为当返回值大于等于0xfffff001（-4095）时需要进行出错处理，故取负后最大为4095。

（7）

① 第3、4题中的实现方式的便捷性、灵活性不如本题：第3题采用汇编程序设计反射光hi，若参数不一样，就要重新编写汇编语句；第4题直接调用write()函数，只能在支持write系统调用的系统中执行；本题中给出的是C库函数调用，可以在不同的系统中运行。

② 但第3题中的执行性能更好，执行时间更短：采用汇编程序设计方式时，省去了高级语言程序设计中大量的函数调用过程，因而执行性能更好、执行时间更短。

6、

（1）内核的设备驱动程序层

（2）内核的与设备无关软件层

（3）用户I/O软件层

（4）内核的设备驱动程序层和中断服务程序层

（5）内核的设备驱动程序层和中断服务程序层

8、

打印机的数据传输率：6×50行×80字/60s=400字符/s

采用中断方式时，

最长中断申请间隔：1/400=2.5ms

实际中断响应及处理时间：1000×1/500MHz×1000=0.002ms << 2.5ms

所以可以采用中断方式i进行字符打印输出