"操作系统原理与实践"实验报告

基于内核栈切换的进程切换

问题一

% 实验代码

(1) 为什么要加4096?

因为应用程序从用户态进入内核态时,其内核栈必须是一个空栈,即*esp* 必须位于申请到的一页内存的末端 (**高地址**),一页内存为4k,此处的基本单位是 **字节** ,4096 8bit=4k *,正好将*tss *中内核栈的*esp*的值设置到一页内存的末端。应用程序一进入内核,就从一页内存的末端向低地址进行压栈操作。

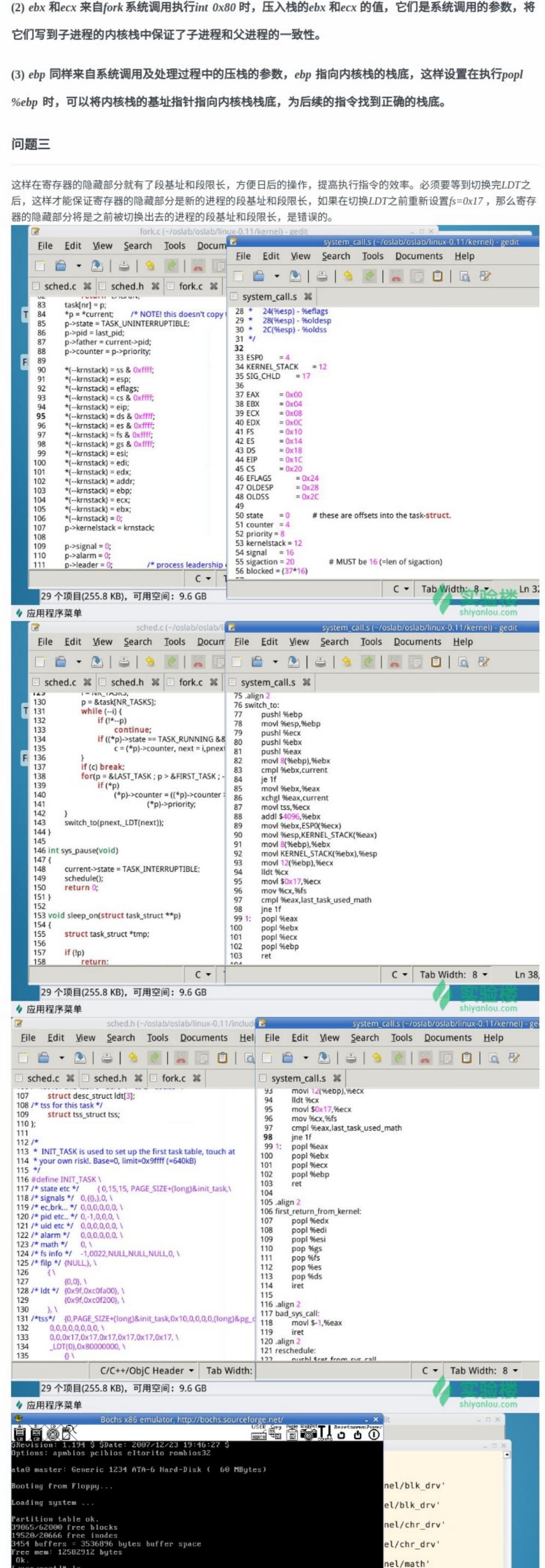
2000 COM (2000 CO 1000 CO 1000

(2) 为什么没有设置ts s 中的s s 0?

因为所有进程都共用 进程o的tss ,而进程o的tss 在初始化时已经设置好了sso ,所以不需要再设置tss 中的sso 了。

问题二

(1) 子进程第一次执行时,eax=0。这样fork()函数就可以通过返回值区分子进程和父进程。在fork.c 中的copy_process() 函数中语句*(--krnstack)=0 做了这个工作。



₽0