CS302: Lab6 Report

Name：陆荻芸 SID：12011537

Answer 1

从内核态到用户态的转变需要中断的发生。我们通过`kernel_execve`中的 ebreak 进入 trap 处理中并且把 a7 寄存器的值设为 0 表示非正常中断。在`do_execve`中为用户态分配了新资源，并且在`load_icode`中，先将进程中断帧的 epc 寄存器内写入了可执行文件的程序入口，然后把 sstatus 的 SPP 设成 0，中断处理结束后 sret 会因为 0 而返回 Umode。

Answer 2

在用户态有被封装好的标准库可供调用。而这些标准库中调用了 ecall，可以让系统产生一个 trap，进入 S mode。然后在 S 态的 trap 中进行系统调用。

Answer 3

用户进程执行结束之后，调用`do_exit`退出。首先会切换到内核的页表上，让用户进程在内核的虚拟地址空间上执行，并进行状态判断后开始回收。回收后会开启中断，执行 schedule 函数，选择新的进程执行结束后模式会切换到 S 态。

Answer 4

当子进程比父进程早结束，但是父进程没有进行回收时会产生僵尸进程。进程等待回收时会被设置成`PROC_ZOMBIE`。