Week10 Report

姓名：Yitong WANG(王奕童) 11910104@mail.sustech.edu.cn

学号：11910104

实验课时段：周五5-6节

实验课教师：Yun SHEN(沈昀) sheny@mail.sustech.edu.cn

实验课SA:

- Yining TANG(汤怡宁) 11811237@mail.sustech.edu.cn
- Yushan WANG(王宇杉) 11813002@mail.sustech.edu.cn

Q1 S->U

1. user_main执行exec()和load_icode()，替换进程资源
2. 更改status的SPP位为0，使得返回至Umode
3. 设置epc的值为新程序入口，使得sret的时候返回跳转执行新程序
4. 中断处理结束，trapret恢复上下文
5. 执行sret，切换至用户态

Q2 用户进程调用系统调用

用户进程：用户态运行

系统进程：内核态运行

调用：

- 封装对应的系统调用函数，作为用户程序调用的接口，供用户调用
- 系统调用函数中，通过内联汇编和引起trap进行ecall环境调用
- CPU的特权级切换，由U态进入S态

以代码中cprintf做示例：

- cprintf()不能直接sbi_console_putchar()，需要经过sys_putc()
- 内联汇编与ecall环境调用

- 产生trap，实现系统调用

Q3 进程结束后模式切换

进程结束后，OS需要释放进程对应的资源，需要相关的系统调用支持。

而系统调用结束后，CPU寄存器需要从内核态恢复原先的用户态，然后切换为用户空间，因此进程结束时需要有模式切换的过程。

Q4 僵尸进程

僵尸进程的形成：一个进程结束，但是父进程没有等待它，那么此时子进程的相关信息就保存在系统进程表中，就形成了僵尸进程。

Q5 load_icode()

load_icode()是在do_execve()函数中被调用，主要功能是将新的程序加载到当前进程，为用户进程分配新的资源，比如说MM，页表，用户栈等等。