CS302 OS Lab05 - Report

Name: 刘仁杰
SID: 11911808

Answers

1.总结执行`ebreak`后，我们的操作系统是如何进行断点中断处理的

- `ebreak`中断触发后，cpu会寻找`stvec`寄存器中的值，然后跳转到这个位置进行中断处理
- 在中断处理初始化函数中，把`stvec`设置成所有中断都要跳到 trapentry.S 进行处理
- 在trapentry.S中，`__alltraps`函数作为中断入口点执行
- `__alltraps`中先通过`SAVE_ALL`来保存上下文，具体操作是保存所有36个寄存器到栈顶
- 然后`move  a0, sp`来传递参数，`jal trap`跳转到`trap.c`里面的`trap`函数，`a0`寄存器作为参数
- 在`trap`中断处理函数中，根据`scause`将异常处理的工作分发给了`interrupt_handler()`和`exception_handler()`，再根据类型作不同处理，`ebreak`会给`exception_handler`进行处理，打印错误信息并对`sepc`进行加2操作，防止重复调用
- 中断处理完成后，跳转回`trapentry.S`，执行`__trapret`里面的内容
- `RESTORE_ALL`恢复上下文，从栈顶反向写入36个寄存器，最后再恢复栈顶指针
- 最后执行`sret`，从S 态中断返回到 U 态，实际作用为pc←sepc

2.触发一条非法指令异常（ILLEGAL_INSTRUCTION），在`kern/trap/trap.c`的异常处理函数中捕获，并对其进行处理，简单输出异常类型和指令即可。

```c
int kern_init(void)
{
    extern char edata[], end[];
    memset(edata, 0, end - edata);

    const char *message = "os is loading ...\n";
    cputs(message);

    // ----------start------------

    idt_init();
    intr_enable();
    asm volatile("ebreak" ::);
    asm volatile("mret" ::);

    // -----------end-------------

    while (1)
        ;
}
```

```
lrj11911808@lrj-Precision-3630-Tower: ~/2022_os/lab/lab05/lab5_code
lrj11911808@lrj-Precision-3630-Tower:~/2022_os/lab/lab05/lab5_code$ make qemu
+ cc kern/trap/trap.c
+ ld bin/kernel
riscv64-unknown-elf-objcopy bin/kernel --strip-all -O binary bin/ucore.bin

OpenSBI v0.6
   ____                    _____ ____ _____
  / __ \                  / ____|  _ \_   _|
 | |  | |_ __   ___ _ __ | (___ | |_) || |
 | |  | | '_ \ / _ \ '_ \ \___ \|  _ < | |
 | |__| | |_) |  __/ | | |____) | |_) || |_
  \____/| .__/ \___|_| |_|_____/|____/_____|
        | |
        |_|

Platform Name          : QEMU Virt Machine
Platform HART Features : RV64ACDFIMSU
Platform Max HARTs     : 8
Current Hart           : 0
Firmware Base          : 0x80000000
Firmware Size          : 120 KB
Runtime SBI Version    : 0.2

MIDELEG : 0x0000000000000222
MEDELEG : 0x000000000000b109
PMP0    : 0x0000000080000000-0x000000008001ffff (A)
PMP1    : 0x0000000000000000-0xffffffffffffffff (A,R,W,X)
os is loading ...

ebreak caught at 0x000000008020003a
illegal instruction caught at 0x000000008020003c
```