Chapter 4

王拓为 2018011917

一、实现

对于 `sys_get_time` 和 `sys_task_info` 函数：

实现了对指针中地址在虚存机制中的转换和数据的拷贝。

对于 `mmap` 和 `munmap` 函数：

实现了申请和释放内存的系统调用，同时可以针对可能的错误做中断处理。

二、问答

1. SV39 分页模式下页表项组成如下所示：

63 — 54	53 — 28	27 — 19	18 — 10	9 — 8	7	6	5	4	3	2	1	0
Reserved	PPN[2]	PPN[1]	PPN[0]	RSW	D	A	G	U	X	W	R	V
10	26	9	9	2	1	1	1	1	1	1	1	1

   其中 $[63:54]$ 为预留区域，$[53:10]$ 为物理页号，$[9:8]$ 为特权级软件预留区域，$[7:0]$ 为标志位。

   标识位的作用如下：

   - D（Dirty）：页表项这一位上次被清零后，页表项对应虚拟页面是否被修改过；
   - A（Accessed）：页表项这一位上次被清零后，页表项对应虚拟页面是否被访问过；
   - G（Global）：页表项对应映射是否在所有地址空间中存在；
   - U（User）：页表项对应页面是否在 CPU 处于 U 特权级下允许被访问；
   - X（eXecute）：页表项对应页面是否允许执行；
   - W（Write）：页表项对应页面是否允许写；
   - R（Read）：页表项对应页面是否允许读；
   - V（Valid）：页表项是否合法；

2. 可能是缺页导致的异常有：

   - Instruction page fault
   - Load page fault
   - Store/AMO page fault

   与缺页相关的 CSR 寄存器的值及含义

   - scause：记录中断异常信息；
   - sstatus：记录处理器当前状态；
   - stvec：记录处理 trap 的入口地址；
   - sscratch：交换上下文时临时中转寄存器；
   - sepc：记录发生中断/异常指令的下一条指令的地址；
   - stval：记录处理 trap 的相关信息；

   Lazy 策略的好处是：

Lazy 策略可能可以提升性能。因为有的页面可能被加载后没有被访问就被释放或者替代了，Lazy 策略可以避免无用的加载。

10GB 连续的内存页面，对应的 SV39 页表大致占用内存大小为：20MB

Lazy 策略的实现及缺页处理是：

分配内存时先不实际分配，当访问缺页时出发缺页异常，在处理异常时再分配对应内存。

页面失效在页表项（PTE）上的表现是：

标识位 V 会被置为 0。

3. 单页表下，置换页表的方式可以和双页表切换页表的方式相同；

   单页表下，可以通过将内核页面的页表项的标志位 U 置为 0；

   单页表的一个优势是在用户态和内核态切换时不需要更换页表；

   双页表下用户态和内核态切换时以及用户态应用程序切换时都需要切换页表，

   单页表下不同用户线程切换时需要切换页表。