## 实验概述

### 1. 重写 sys_get_time 和 sys_task_info

基本逻辑和lab3一样，但是lab4必须使用微秒计算运行时长，否则有精度问题。系统调用拿到的是用户空间的地址，使用 translated_byte_buffer 拿到对应的物理地址，然后将结构体转成u8数组，按结构体大小复制byte即可。

### 2. mmap 和 munmap 匿名映射

mmap 检查完基本参数后，找出当前任务所属的task，然后检查 task 中 memory_set 是否已经有申请过当前地址段的虚拟地址，如果有则失败。如果没有，则使用 insert_framed_area 插入新的 MemoryArea 即可，需要注意要修改这些辅助函数，不能忽略内存不够等异常情况。

munmap 参数有两个，start 和 len，而不是像C语言free()函数只有ptr一个参数，由系统根据指针的额外信息释放上次malloc()的全部内存。因此如果要完全根据len来释放空间会比较麻烦且对具体行为需要更清晰的描述。为了简单，这里根据 start 和 len 按 mmap 的方式计算出页号范围，然后在当前任务中找到范围完全一致的 MemoryArea 才算参数有效，将该 MemoryArea 调用 unmap() 之后从 MemorySet 移除该范围即可。

## 问答作业

### 1

```
SV39 页表页表项一共64位，[63 : 54] 为保留字段，[53 : 10] 是44位物理页号。

第0位是 V 标志位，仅当位 V 为 1 时，页表项才是合法的。

第1位是 R 标志位，表示该页面是否可读。

第2位是 W 标志位，表示该页面是否可写 。

第3位是 X 标志位，表示该页面是否可执行 。

第4位是 U 标志位，表示该页面是否能在用户态访问 。

第6位是 A 标志位，处理器记录自从页表项上的这一位被清零之后，页表项的对应虚拟页面是否被访问过。

第7位是 D 标志位，处理器记录自从页表项上的这一位被清零之后，页表项的对应虚拟页面是否被修改过。
```

### 2

a.

```
页表项有多个标志位，因此缺页可能是不满足某个条件，由此引发指令缺页异常或读写缺页异常。
```

b.

假设在用户态发生缺页异常

pc 会跳转到 stvec 所保存的位置(Direct模式).

sp 加载 sscratch 中的值，即内核栈顶

sstatus 中的 SPP 字段给出 Trap 发生之前 CPU 处在哪个特权级（S/U).

sepc 记录缺页发生前执行的最后一条指令

scause 给出缺页的具体原因，比如12是指令缺页

stval 保存缺页的虚拟地址

c.

Lazy 策略可以减少程序运行前的准备时间，且减少内存消耗。

d.

10G 连续的内存页面共需 10G / 4K = 2.5M个页表项，每个页表项8byte，共需20M空间作为页表的叶子节点，这20M空间还需要二级页表来索引，但数量较小，总内存占用在20M多一点。

e.

实现Lazy策略需要页表项多加一位表示是否为Lazy页，当发生缺页后如果Lazy标志位为1，则按需加载该页内存后继续执行上一条指令即可。

f.

页面失效时，V位为0

**3.**

a.

单页表由用户态进入内核态不需要更换页表，不同用户程序之间切换才需要更换页表

b.

设置U标志位为0，禁止用户程序访问

c.

发起系统调用不需要刷新TLB，提升性能

d.

双页表在切换用户程序或用户程序进入内核态都需要更换页表。单页表只需要在切换用户程序时更换页表。

## 荣誉准则

1. 在完成本次实验的过程（含此前学习的过程）中，我曾分别与 **以下各位** 就（与本次实验相关的）以下方面做过交流，还在代码中对应的位置以注释形式记录了具体的交流对象及内容：

   > 无

2. 此外，我也参考了 **以下资料** ，还在代码中对应的位置以注释形式记录了具体的参考来源及内容：

   > https://pdos.csail.mit.edu/6.828/2019/lec/l-usingvm.pdf 了解 stval 寄存器在缺页时的值
   >
   > https://lwn.net/Articles/738975/ 了解单页表的基本情况

3. 我独立完成了本次实验除以上方面之外的所有工作，包括代码与文档。 我清楚地知道，从以上方面获得的信息在一定程度上降低了实验难度，可能会影响起评分。
4. 我从未使用过他人的代码，不管是原封不动地复制，还是经过了某些等价转换。 我未曾也不会向他人（含此后各届同学）复制或公开我的实验代码，我有义务妥善保管好它们。 我提交至本实验的评测系统的代码，均无意于破坏或妨碍任何计算机系统的正常运转。 我清楚地知道，以上情况均为本课程纪律所禁止，若违反，对应的实验成绩将按“-100”分计。