思考题5

1. Copy-On-Write (COW) 配置页表描述符的字段：

    1. 访问权限（AP 位）: 页表描述符的位[7:6]，设置为只读（Read-Only），以防止子进程直接写入共享页面
    2. 访问标志（AF 位）: 页表描述符的位[10]，设置为已访问（Accessed），表示页面已被访问
    3. 用户/内核位（UXN/SXN 位）: 页表描述符的位[54]和[53]，根据需要设置为用户可访问（User-Accessible）或内核可访问（Kernel-Accessible）
    4. 共享位（SH 位）: 页表描述符的位[9]，设置为共享（Inner Shareable），以允许多个进程共享该页面

2. 页错误时的处理流程：

    1. 捕获页错误异常：当子进程尝试写入只读页面时，CPU 会触发页错误异常，并跳转到内核的页错误处理程序
    2. 确认错误类型：页错误处理程序首先确认这是一个写入导致的页错误
    3. 分配新页面：内核为子进程分配一个新的物理页面
    4. 复制页面内容：将父进程的共享页面内容复制到新分配的页面中
    5. 更新页表：修改子进程的页表，将该虚拟地址映射到新分配的物理页面，并将访问权限设置为可读写
    6. 刷新 TLB：确保新的页表映射生效，可能需要刷新相关的 TLB 条目
    7. 返回用户态：页错误处理完成后，内核返回到子进程的用户态，继续执行写操作

思考题6

没有为内核页表使用细粒度的映射的问题：

1. 权限控制问题：可能将所有内存设置为相同的权限，无法区分不同内存区域的访问权限，增加了安全风险。
2. 内存安全问题：细粒度映射可以防止非法访问特定内存区域，缺乏细粒度映射可能导致内存泄漏或数据损坏。
3. 内存浪费：映射整个1GB内存区域可能导致大量未使用的内存被映射