**系统虚拟化作业1**

1. 假设在Virtualizable硬件上使用Trap-and-Emulate方法实现CPU虚拟化。1）请描述VM内的用户态进程执行System Call被VM内核处理并返回的全过程。2）进程内执行Fork Bomb是否会大量增加VMM的线程并大量消耗VMM的资源？

2. 假设有一台支持Intel VT-x和8个物理CPU的服务器，在其上运行1个VMM和10个VM，每个虚拟机有4个vCPU。若该VMM使用了VT-x硬件虚拟化，需要创建多少线程为这些VM服务（只考虑CPU虚拟化）？总共需要创建多少个VMCS？请解释原因。

3. ARM v8.0的硬件虚拟化机制为Type-1 VMM所设计，当直接在EL2内运行Type-2 VMM（如KVM）时会存在一些问题。请具体解释会造成哪些问题？为此，KVM/ARM提出了什么样的解决方案？该方案是否存在VM Exit处理路径上的性能问题？

4. 假设使用影子页表机制实现内存虚拟化。现有10个虚拟机，每个虚拟机内有10个进程，VMM总共需要创建多少个影子页表？