进程切换

1，thread->esp0始终指向进程内核栈为空时的栈顶，而thread->esp随着push和pop指令而改变。

2，

Copy\_page\_tables函数的入参是一个源线性地址，一个目的线性地址以及长度，从而复制这一块线性地址空间的页目录和页表项，这导致目的线性地址指向的物理页和源是相同的，从而实现页面共享。页面共享状态下页表被设置为只读，此时当共享的其中一个进程出现写操作，则触发写时复制。写时复制的处理中，首先申请一个内存页，并将原来共享的页面内容拷贝到新页面，然后刷新页表项，并且将内存引用数减一。而另一个共享进程出现写操作时同样会触发页面异常，此时当系统发现内存引用数为1，即无内存共享时，则直接修改只读属性为读写属性即可。从而实现，进程拥有独立内存的结果。