APC

1.线程是不能被“杀掉”、“挂起、“恢复”的，线程在执行的时候自己占据着cpu，别人怎么可能控制它呢？所以说线程如果想死，一定是自己执行代码把自己杀死，不存在他杀的情况

那如果想改变一个线程的行为该如何？

可以给他提供一个函数，让他自己去调用，这个函数就是APC，即一部过程调用

2.APC队列

将上图保存到下图的链表中

3.APC函数何时被执行

KiServiceExit函数：

这个函数是系统调用、异常或中断返回用户空间的必经之路

KiDeliverApc函数

负责执行APC函数

4.SaveApcState的意义

防止进程切换时CR3　产生改变，导致线程APC地址发生混乱，即进程发生切换时保存APCstate的备用APC队列

5.挂靠环境下ApcState的意义

在挂靠的环境下，也是可以先线程APC队列插入APC的，那这种情况下，使用的时哪个APC队列呢

ApcQueueable用于表示是否可以向线程的APC队列中插入APC。

当线程正在执行退出的代码时，会将这个值设置为0，如果此时执行插入APC的代码(KeInsertQueueApc 后面会讲),在插入函数中会判断这个值的状态，如果为0，则插入失败。