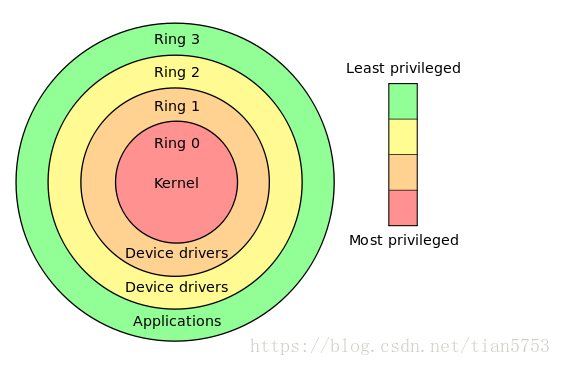
Intel将CPU的特权级别分为4个级别：RING0、RING1、RING2、RING3.

Windows只是用其中两个级别RING0和RING3，RING0只给操作系统用，RING3谁都能用。如果普通应用程序企图执行RING0指令，则Windows会显示“非法指令”错误信息。

RING0是指CPU的运行级别，RING0是最高级别，以下次之。那linux+86来说，操作系统（内核）运行的代码在最高运行级别RING0上，可以使用特权指令，控制中断、修改页表、访问设备等。应用程序的代码运行在最低运行级别RING3上，不能做受控操作。如果要做，比如需要访问磁盘，写文件。那就要通过执行系统调用（函数），执行系统调用的时候，CPU的运行级别会发生从RING3到RING0的切换，并跳转到系统调用对应的内核代码位置执行，这样内核就为你完成了设备访问，完成之后再回到RING3.这个过程就叫做用户态和内核态的切换。



RING设计的初衷是将系统权限与程序分离出来，使之能够让OS更好的管理当前系统资源，也使得系统更加稳定。举个RING权限的最简单的例子：一个停止响应的应用程序，它运行在比RING0更高（如RING3）的指令环上，你不必大费周章的想着如何使系统恢复运作，这期间，只需要启动任务管理器便能轻松终止它，因为它运行在比程序更低的RING0指令环中，拥有更高的权限，可以直接影响到RING0以上运行的程序，当然有利就有弊，RING保证了系统稳定运行的同时，也产生了一些麻烦的问题。