1、描述符特权级DPL、当前特权级CPL和请求特权级RPL的含义是什么？在哪些寄存器中这些字段？对应的访问条件是什么？

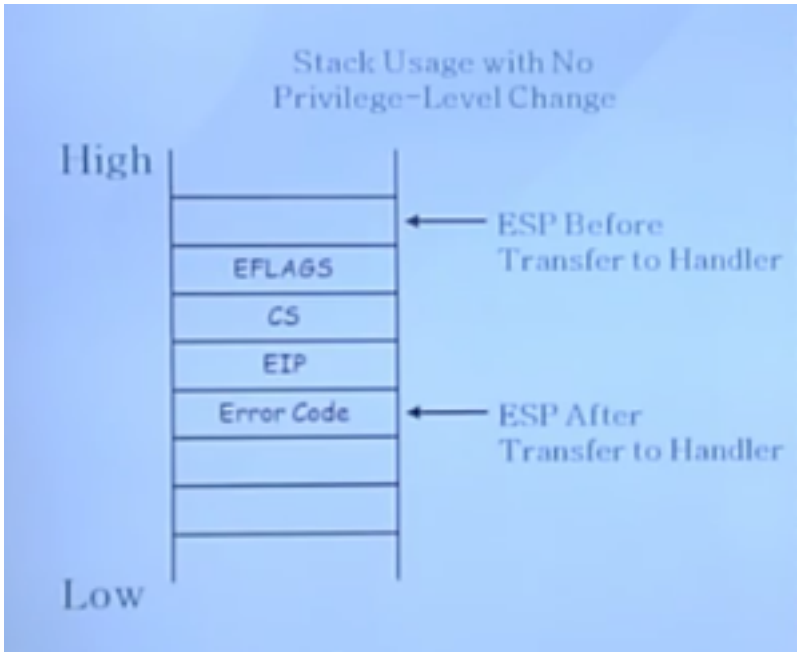
答：
CPL是当前进程的权限级别，是当前正在执行的代码所在的段的特权级，存在于CS寄存器的低两位。

RPL说明的是进程对段访问的请求权限，是段选择子里面的bit 0和bit 1位组合所得的值，是对于段选择子而言的，每个段选择子有自己的RPL，它说明的是进程对段访问的请求权限。而且RPL对每个段来说不是固定的，两次访问同一段时的RPL可以不同。

DPL存储在段描述符中，规定访问该段的权限级别，每个段的DPL固定。

当进程访问一个段时，需要进行进程特权级检查，一般要求DPL >= max {CPL, RPL}。所以RPL对CPL有削弱作用，当RPL大于CPL时，特权级检查以RPL为准，例如，当DPL=2，CPL=1，RPL=3时，特权级检查是不通过的，即进程不能访问该段。

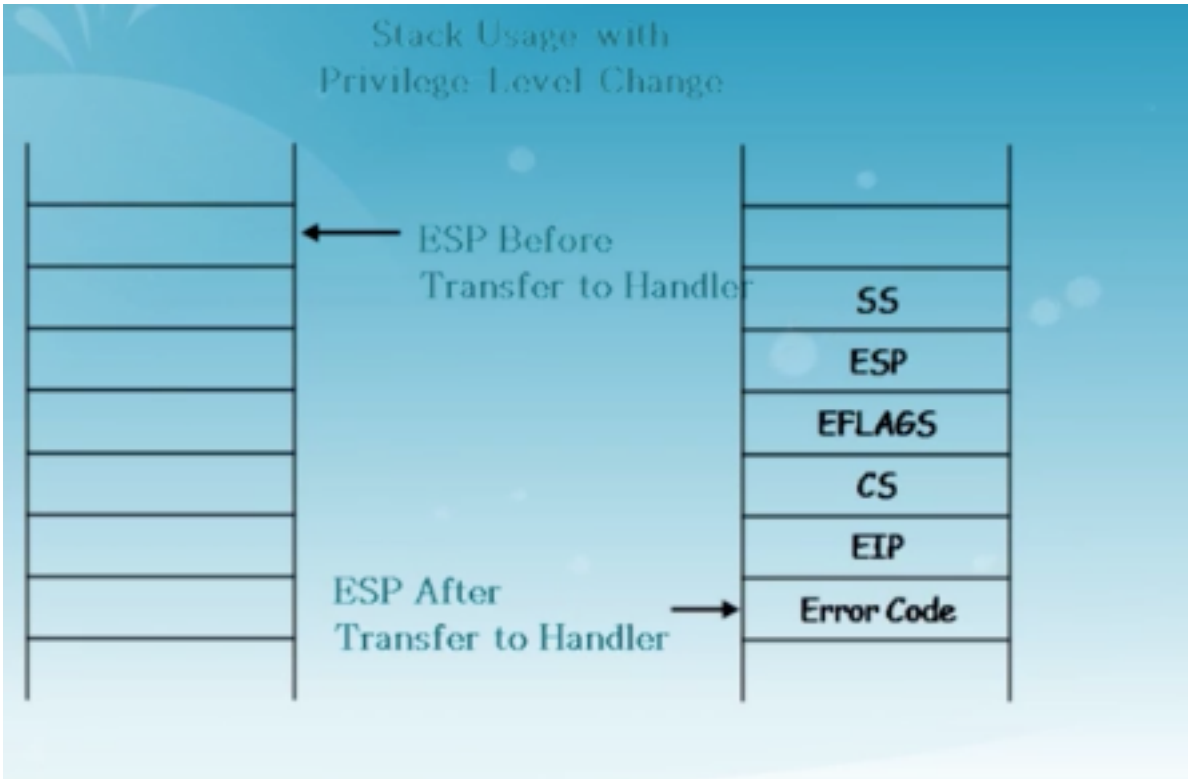
2、不同特权级状态下的堆栈变化：
在内核态时产生中断：



首先将Error Code压入栈，然后是EIP、CS和EFLAGS，使用同一个栈。

在用户态产生中断：

首先要新开一个内核态的堆栈，除了之前的情形需要压入栈的内容之外，还需要将用户态堆栈的地址（SS和ESP）压入栈以便于iret时返回原来的用户态堆栈去执行。


Stack Usage with
Privilege Level Change
ESP Before
Transfer to Handler
SS
ESP
EFLAGS
CS
EIP
Error Code
ESP After
Transfer to Handler