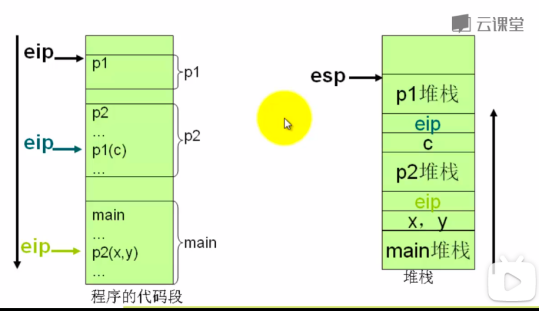
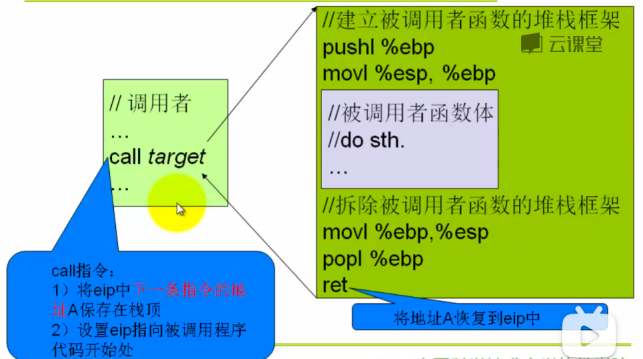
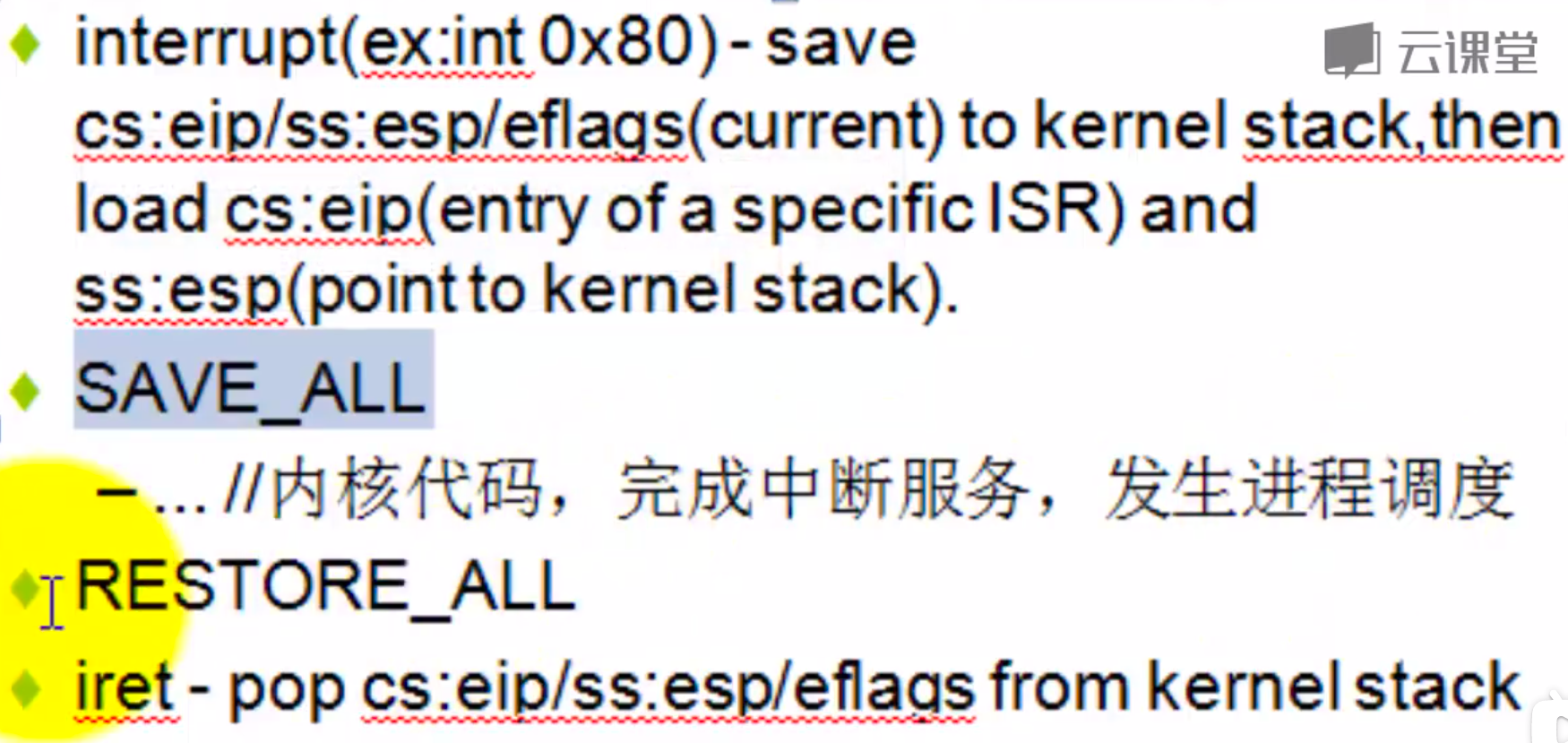
1. 堆栈是c语言程序运行时必须的一个记录调用路径和参数的空间：①函数调用框架；②传递参数；③保存返回地址；④提供局部变量空间；
2. c语言编译器对堆栈的使用有一套规则，
3. ebp基址指针在c语言中用作记录当前函数调用基址，每个函数的ebp是不同的；
4. CS:EIP总是指向下一条指令，call和ret指令会修改EIP；其中CS是代码段，如果程序短只有一个代码段可以省略；





1. 早期编译器要求必须把变量的声明放在函数头部，就是为了计算需要分配多少栈空间；现在编译器可以扫描整个函数来确定；

6）中断处理过程