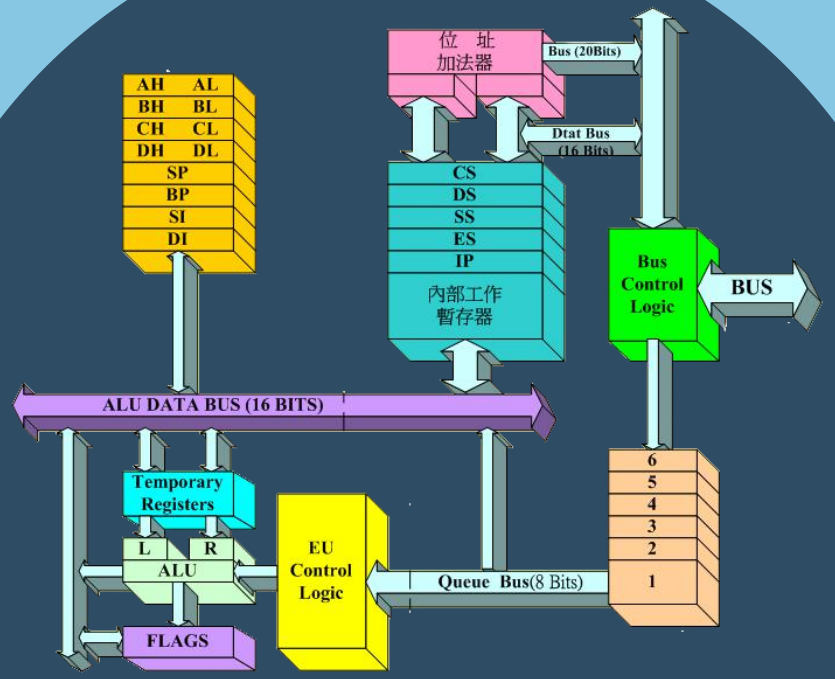
jmp指令

贺利坚　主讲



汇编语言程序设计

Assembly Language

修改CS、IP的指令

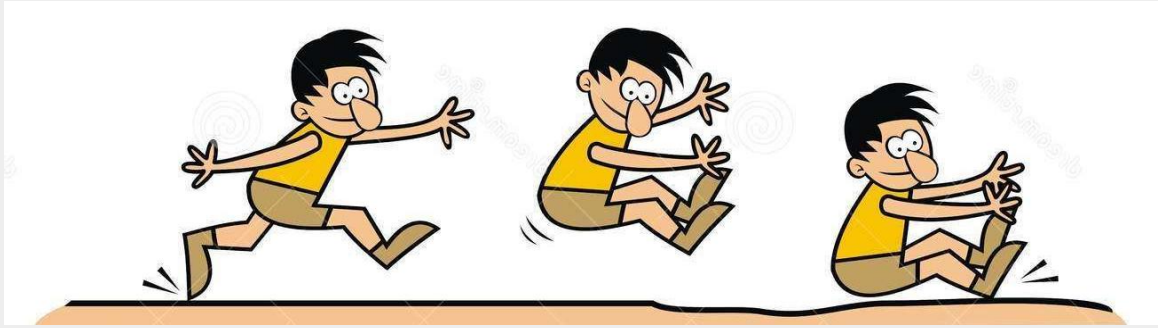
- 事实：执行何处的指令，取决于CS:IP
- 应用：可以通过改变CS、IP中的内容，来控制CPU要执行的目标指令
- 问题：如何改变CS、IP的值？
- 方法1：Debug 中的 R 命令可以改变寄存器的值——rcs, rip
  - Debug是调试手段，并非程序方式！
- 方法2：用指令修改

```
mov cs, 2000H
mov ip, 0000H
```

8086CPU不提供对CS和IP修改的指令！

- 方法3：转移指令 jmp

转移指令 jmp



- 同时修改CS、IP的内容

  jmp 段地址：偏移地址

  jmp 2AE3:3

  jmp 3:0B16

  功能：用指令中给出的段地址修改CS，偏移地址修改IP。

- 仅修改IP的内容

  jmp 某一合法寄存器

  jmp ax （类似于 mov IP, ax）

  jmp bx

  功能：用寄存器中的值修改IP。

问题分析

从20000H开始，执行的序列是：

（1）mov ax,6622

（2）jmp 1000:3

（3）mov ax,0000

（4）mov bx,ax

（5）jmp bx

（6）mov ax,0123H

（7）转到第（3）步执行

CS	2000	IP	0000		
AX		BX		CX	