巧设寄存器重设思科路由器密码 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/271/2021_2022__E5_B7_A7_E8_AE_BE_E5_AF_84_E5_c101_271546.htm 在Cisco路由器中有一个配置注册码，即Configuration register value，使用show version命令后，在最后一行可以看到它的值，它是由4个16进制数组成，如0x2102，用二进制表示就是0010000100000010，它的后四位称为Boot field，路由器根据Boot field的值决定从哪里启动IOS系统，具体规定如表所示。它的第六位（有下划线的位）一般为“ 0 ”，如果是“ 1 ”则表示让路由器启动的时候绕过配置文件进入到Startup模式，这时没有口令提示就直接进入特权配置模式，于是通过修改第六位的值就可以实现恢复口令的目的。 Boot field 字段的值 启动方式 0x0-（0000）直接进入Rommon>方式，此方式可以修改Configuration register 的值 0x1-（0001） 从ROM中自动引导IOS 0x2-0xF（0010-1111） 如果没有Boot system命令，将安装Flash中的IOS，失败的话以广播的方式在TFTP服务器上寻找IOS，如果再次失败，从ROM中安装IOS. 如果有Boot system命令，则查看Boot system命令来决定用什么方式安装IOS. 首先，准备一台装有Windows9x/2000/xp操作系统的计算机，使用路由器所带的console线连接PC的com口和路由器的console 口，然后进入PC，进入“ 开始→程序→附件→通讯→超级终端 ”，建立一个新连接，使用COM串口，端口设置为：每秒位数9600bps、数据位8位、奇偶检验无、停止位1、数据流控制无。然后打开路由器电源，键入回车键即可显示路由器启动信息。 然后，需要修改启动路由器的配置注册码（Configuration register

value）。在路由器启动的第一个60秒内按下CTRL BREAK键，这时会终止路由器的启动，进入ROMMON模式下，即ROMMON 1>，输入下面的命令： Rommon 1 > confreg 0x2142 （针对1600、2600系列路由器） Rommon 2 > reset （重新启动路由器） 如果是1500、2500系列路由器，输入“ o/r 0x2142 ”命令，0x2142中的“ 4 ”，用二进制表示就是0100，把配置注册码的第6位设置为“ 1 ”，也就是0010000101000010，这使得路由器启动的时候绕过配置文件进入到Startup模式。路由器启动后进入Startup模式，显示系统配置对话，提示是否进入初始配置时，输入“ N ”不进行配置，然后在用户模式下（User mode）输入enable命令直接进入特权模式（Privileged mode），这时没有提示输入口令。 这时进入路由器的特权配置模式，使用#show running-config命令可以发现没有任何配置，使用#show startup-config命令可以看到原来配置的参数，使用下面的命令进行参数恢复。Router#copy startup-config running-configDestination filename [running-config]? 键入回车567 bytes copied in 0.761 secs 最后，修改密码和配置注册码（Configuration register value）后，保存配置并重新启动路由器就可以了。Router#config terminalEnter configuration commands, one per line. End with CNTL/Z.Router(config)#enable secret 123456 （重新设置口令）Router(config)#line vty 0 4Router(config-line)#password 123456 (设置远端登录口令)Router(config-line)#exitRouter(config)#config-register 0x2102 （修改配置注册码为0x2102）Router(config)#exit 100Test 下载频道开通，各类考试题目直接下载。详细请访问