

总结: Cisco路由器的口令恢复技巧 PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/142/2021\\_2022\\_\\_E6\\_80\\_BB\\_E7\\_BB\\_93\\_Cis\\_c101\\_142468.htm](https://www.100test.com/kao_ti2020/142/2021_2022__E6_80_BB_E7_BB_93_Cis_c101_142468.htm) 为保障网络安全，设置路由器口令是必要的，但是如果路由器口令忘记了，对管理员来讲是一个不小的损失。笔者经过研究并实践，找到了对Cisco路由器口令的恢复方法，此方法对1500、1600、1700、2500、2600、3600等系列Cisco路由器均适用，下面笔者以2610路由器为例。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。首先，准备一台装有Windows 9x/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 通信 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原配置参数的恢复：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。100Test 下载频道开通，各类考试题目直接下载。详细请访问 [www.100test.com](http://www.100test.com)