神奇恢复Cisco路由器口令 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__E7_A5_9E_E5_A5_87_E6_81_A2_E5_c101_142368.htm 一、Cisco 路由器口令类别 1．有效密码口令（enabled secret password）：是一种安全级别最高的加密口令，适用于Cisco IOS 10.3 (2) 以后的版本，在路由器的配置表中以密码的形式出现。 2．有效口令（enabled password）：安全级别次高的非加密口令。当有效密码口令没设置时，使用该口令。 3．终端口令（console password）：用于防止非法或未授权用户修改路由器配置，在用户通过主控终端对路由器进行设置时，使用该口令。 二、口令恢复原理 1．内部内存种类（以2500系列为例）。Cisco 路由器保存了几种不同的配置参数，并存放在不同的内存模块中。 Cisco2500系列路由器的内存：ROM、闪存（flash memory）、不可变RAM（NVRAM）、RAM和动态内存（DRAM）等五种。作用如下：内 存 类 别 作 用 ROM 存放系统的引导程序。类似PC机的BIOS，是一种只读存储器，系统掉电程序不会丢失。 闪存 存放Cisco IOS的镜像，类似PC机的硬盘，是一种可擦写、可编程的ROM, 系统掉电数据不会丢失。 NVRAM 存放配置文件（即Startup-config） RAM 存放当前系统使用配置（即Running-config） DRAM 主要包含路由表、ARP缓存、fast-switch缓存、数据包缓存等，也包含正在执行的配置文件。系统掉电该内存数据回丢失。 一般地，路由器启动时，首先运行ROM中的程序，进行系统自检及引导，然后运行FLASH中的IOS，并在NVRAM中寻找路由器配置，并装入DRAM中。 2．口令恢复的关键在于对配置登记码

（Configuration Register Value）进行修改，从而让路由器从不同的内存中调用不同的参数表进行启动。有效口令存放在NVRAM 中，因此修改口令的实质是将登记码进行修改，从而让路由器跳过NVRAM 中的配置表，直接进入ROM 模式，然后对有效口令和终端口令进行修改或者重新设置有效加密口令(因为有效加密口令为加密乱码，无法 进行恢复，只可以删掉或改写），完成后再将登记码恢复(如忘记恢复路由器重起后修改的配置可能回丢失)。 Configuration Register Value及其含义 Configuration Register Value 含 义 0x2102 缺省设置 bit13=0x2000 Flash引导失败5次后，自动从Rom引导 bit8=0x0100 关闭Break键 Boot field=0x2 从Flash中引导正常运行模式 0x2101 bit13=0x2000 Flash引导失败5次后，自动从Rom引导 bit8=0x0100 关闭Break键 Boot field=0x1 进入Boot Rom运行模式。 Router(boot)> 0x142 bit8=0x0040 进入 Rom Monitor运行模式。> 或 ROMMON> Boot field=0x2 从Flash中引导正常运行模式。 三、口令恢复步骤 1．用Cisco随机配备的线将路由器console口连接到PC机的串口（如COM1或COM2）上； 2．启动Win95/98 的超级终端，并配置为9600波特率、8 个数据位、无奇偶校验、2 位停止位； 3．在“ > ”提示符下，用show version 命令查看登记码（Configuration register），一般为0x2102或0x102；一定记住此登记码，在第9步要将此登记码还原。 4．通过查看登记码，如果中断屏蔽（即登记码的第4 位为1），则重启路由器， 并在开机后30 秒 内按Ctrl Break 键；如果中断未屏蔽，则发送中断(Cisco公司提供的技术手册是开机后60秒内按Break键)。 5. 如路由器是2000、2500、3000、680x0 based 4000、7000系列，IOS版本为10.0以下；

或出现“ > ”提示符 如路由器是1003、1004、3600、4500、4700、72xx、75xx系列；或出现“ ROMMOM> ” 1) > o/r 0x42 1)ROMMON> confreg 0x42 2) > i 2)ROMMON> reset 6. 当提示是否进入对话配置时（Would you like to enter the initial configuration dialog? [yes]:），回答“ NO ”（如误输入“ YES ”，立刻按Ctrl-C退出）；出现“ Press RETURN to get started! ”，按回车，进入ROM 模式 Router > 。 7．键入enable 命令进入EXEC 状态, 键入Router#show config查看原路由器配置和未加密口令，建议立刻做一文本备份文件，以免误操作将原路由器配置丢失；再键入Router#configuration memory, 将NVRAM模式中的参数表装入内存。 8．键入Router#configure terminal 命令进行配置，从配置表中找出忘记的有效口令或改写；更改完毕注意一定要写入NVRAM中，否则路由器原配置会丢失以及改写口令无效。 Router#write memory(copy running-config startup-config)。 9．将第3步查到的登记码还原，一般为0x2102（即从闪存正常启动，并屏蔽中断），并激活所有端口（系统会将所有端口自动shutdown）。 Router#config-register 0x2102 Router(config)#interface xx Router(config-if)#no shutdown 10. Router#Ctrl-Z 11．重新启动路由器：Router# reload 经过以上步骤，既不会丢失原来的路由器配置，又可以找到或更改口令。 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