思科系列丛书

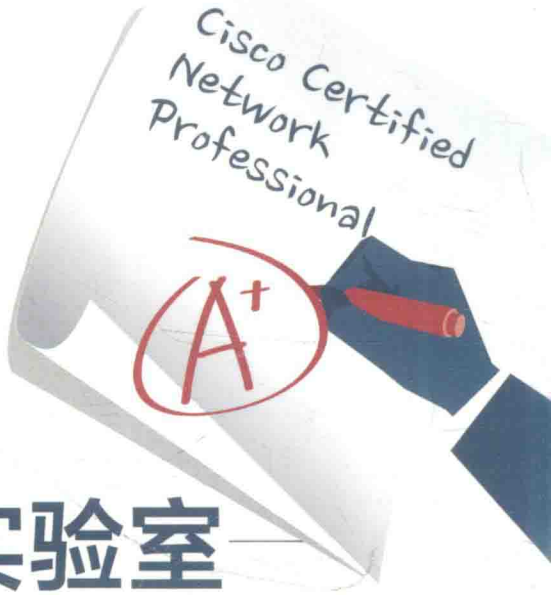
思科网络实验室

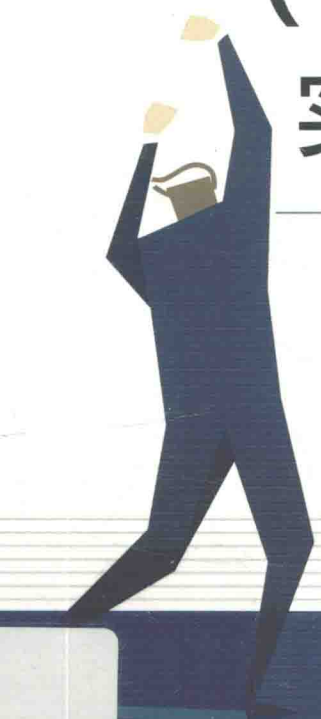
CCNP

（交换技术）

实验指南（第2版）

◆ 王隆杰　梁广民　编著





中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

思科系列丛书

思科网络实验室 CCNP（交换技术）实验指南

（第 2 版）

王隆杰　梁广民　编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书旨在帮助正在学习 CCNP 的读者提高 CCNP 交换方面的动手技能。全书共 6 章，主要内容包括交换机基本配置，VLAN、Trunk、VTP 与链路汇聚，STP，VLAN 间路由，高可用性，交换机的安全。本书的重点是实验，希望能通过实验有效地帮助读者掌握技术原理及其使用场合。本书采用 Catalyst 3560 V2 作为硬件平台（IOS 版本为 15.0）。

本书适合想要通过 CCNP 认证考试的网络技术人员，以及那些希望获得实际经验以轻松应付日常工作的专业人员阅读，本书既可以作为思科网络技术学院的实验教材，也可以作为电子和计算机等专业网络集成类课程的教材或者实验指导书，还可以作为相关企业员工的培训教材；同时也是一本不可多得的很有实用价值的技术参考书。

图书在版编目（CIP）数据

思科网络实验室 CCNP（交换技术）实验指南 / 王隆杰，梁广民编著. —2 版. —北京：电子工业出版社，2018.4
（思科系列丛书）
ISBN 978-7-121-33845-8

Ⅰ. ①思… Ⅱ. ①王… ②梁… Ⅲ. ①计算机网络－信息交换机－实验－指南 Ⅳ. ①TN915.05-33

中国版本图书馆 CIP 数据核字(2018)第 048230 号

策划编辑：宋　梅
责任编辑：宋　梅
印　　刷：三河市双峰印刷装订有限公司
装　　订：三河市双峰印刷装订有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1092　1/16　印张：15.25　字数：390 千字
版　　次：2012 年 5 月第 1 版
　　2018 年 4 月第 2 版
印　　次：2018 年 4 月第 1 次印刷
定　　价：68.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：mariams@phei.com.cn。

前　言

CCNP 涉及交换的内容不是很多，然而网络工程师在实际工作中和交换机打交道的机会往往比路由器多。作者一直很推崇理论与实验相结合的学习方法，这是作者多年从事教学的经验，也是编写本书的原因。也许理论与工作实践相结合更好，可是又有多少人会有这样的机会呢？会有几个企业允许你在实际的生产环境中实践一下呢？那就让我们先在实验室做实验吧，哪怕你失败也没有关系，实验室中的失败是为了不在实际工程中失败。

本书针对 CCNP 交换部分的考试（代码 300-115）所需的知识精心规划了 37 个实验，这些实验将有助于读者在动手过程中掌握相关的理论。值得一提的是，本书的绝大多数实验可以使用同一网络拓扑实现，这将大大减少读者反复搭建实验台的时间。作者非常期望能通过这些实验帮助读者了解这些技术在什么场合可以使用，将产生什么效果。

全书共 6 章，第 1 章介绍实验台的拓扑以及如何配置访问服务器方便读者进行实验；第 2 章介绍交换的基本配置、VLAN 操作、中继和链路汇聚、VTP，以及私有 VLAN；第 3 章详细介绍各种 STP 技术，包括标准的 STP、PVST、RSTP 和 MSTP，还介绍了 STP 的保护，以及在某些场合可以替代 STP 的 Flex Link 技术；第 4 章介绍使用单臂路由或者三层交换实现 VLAN 间路由的技术，还补充了进程交换、快速交换和 CEF 的区别方面的内容；第 5 章介绍保证局域网高可用性的技术，包括思科私有的 HSRP 和标准化的 VRRP、网关负载均衡和服务器负载均衡，以及如何使用日志服务或 SNMP 监控交换机的运行情况；第 6 章介绍交换机上的各种安全措施，包括基本的端口安全、DHCP 监听、动态 ARP 检测、源 IP 保护、防止 VLAN 跳跃攻击，以及使用 AAA 实现 dot1x 认证和交换机上的各种 ACL。

本书由王隆杰（CCIE#14676 R/S，Security）和梁广民（CCIE#14496 R/S，Security）组织编写及统稿，参加编写的还有刘平、张立涓、石光华、邹润生、石淑华、杨名川和杨旭。编著者虽然已尽全力，书中难免还有错误之处，请发邮件到 wanglongjie@szpt.edu.cn 指正。

编　著　者

2018 年 2 月于深圳

目　录

第 1 章　交换机基本配置

本章将首先介绍本书中始终要用到的实验台的拓扑，该拓扑能够灵活地把不同数量的路由器和交换机进行组合，组成各种拓扑以满足不同实验的要求。随后将详细介绍如何配置访问服务器，以便同时控制多个路由器或者交换机。最后，本章还将介绍交换机的密码恢复以及 IOS 恢复过程。

1.1　实验台配置

1.1.1　本书实验台拓扑

为了完成本书的各个实验，需要构建不同的拓扑，如果每次都临时进行拓扑的搭建会花费大量的时间。我们设计了一个功能强大的网络拓扑，如图 1-1 和图 1-2 所示（图中不包含访问服务器和它们的连接），本书绝大多数的实验可以使用该拓扑完成；该拓扑还可以满足 CCNA 以及 CCIE 的部分实验。拓扑中的路由器和交换机均通过访问服务器来进行控制，该拓扑可以让 1～7 人共同操作。

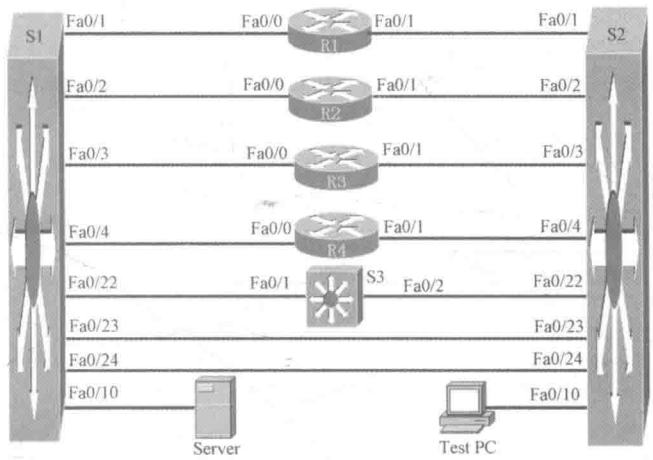


图 1-1　本书实验拓扑（以太网连接部分）

在图 1-1 拓扑中，4 台路由器均为 CISCO2911 路由器，IOS 采用 c2900-universalk9-mz.SPA.157-3.M.bin；3 台三层交换机为 Catalyst 3560 V2，IOS 采用 c3560-ipservicesk9-mz.150-2.SE11.bin 。所有路由器的 GigabitEthernet0/0 以太网端口与交换机 S1 进行连接；GigabitEthernet0/1 以太网接口则与交换机 S2 进行连接。交换机 S1 和 S2 之间通过 FastEthernet0/23 和 FastEthernet0/24 进行连接；交换机 S3 的 FastEthernet0/1 端口连接到 S1 的 FastEthernet0/22 上，FastEthernet0/2 端口连接到 S2 的 FastEthernet0/22 上。为了便于测试，

在图 1-1 中还连接了一台服务器和一台 PC。

4 台路由器之间通过串行链路进行连接，如图 1-2 拓扑所示。

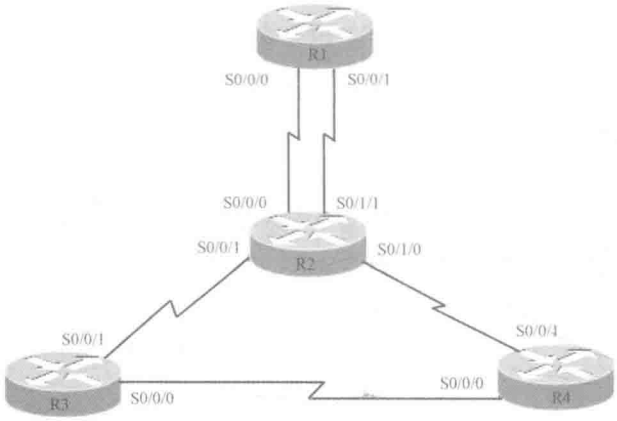


图 1-2　本书实验拓扑（广域网连接部分）

1.1.2　访问服务器

稍微复杂一点的实验就会用到多台路由器或者交换机，如果通过计算机的 COM 口和它们的 Console 口连接，由于一个 COM 口只能连接一台设备，就需要多台计算机或者经常拔插 Console 线，非常不方便。访问服务器可以解决这个问题，访问服务器和网络设备的连接方法如图 1-3 所示。访问服务器可以是一台插有 8 个（NM-8A 模块）或者 16 个（NM-16A 模块）异步口的路由器，从它引出多条连接线到各个路由器上（被控设备）的 Console 口。在使用时，用户首先 Telnet 到访问服务器，然后再从访问服务器访问各个路由器和交换机等被控设备，这样就能同时控制多台设备。

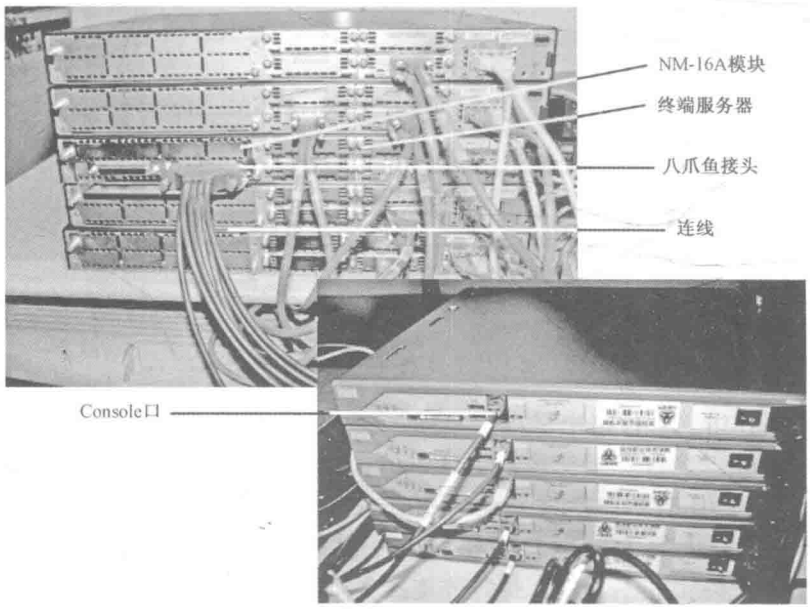


图 1-3　访问服务器和网络设备的连接方法

1.2　实验 1：配置访问服务器

使用访问服务器（就是插有异步模块 NM-8A 或者 NM-16A 的路由器）可以避免在同时配置多台路由器时频繁拔插 Console 线，为了方便使用访问服务器，可以制作一个简单的菜单。

1. 实验目的

通过本实验可以掌握：

① 访问服务器的配置方法并制作一个简单的菜单。

② 访问服务器和交换机的使用方法。

2. 实验拓扑

访问服务器与各路由器和交换机连接实验拓扑如图 1-4 所示。

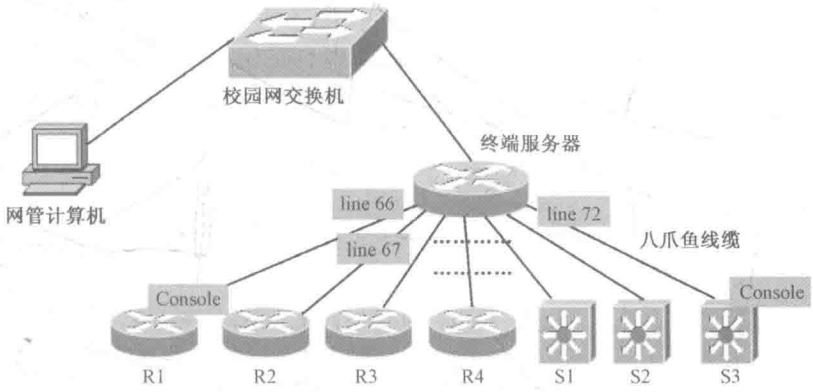


图 1-4　访问服务器与各路由器和交换机连接实验拓扑

3. 实验步骤

（1）访问服务器的基本配置

```
Router(config)#hostname Terminal-Server   //配置访问服务器的主机名
Terminal-Server(config)#enable secret CISCO
//配置进入特权模式的密码，防止他人修改访问服务器的配置
Terminal-Server(config)#no ip domain-lookup
//禁止路由器查找 DNS 服务器，防止输入错误命令时的长时间等待
Terminal-Server(config)#line vty 0 ?
  <1-15>   Last Line number
  <cr>
//查看该路由器支持多少 vty 虚拟终端，可以看到支持 0～988 个。路由器支持多少 vty 和路由器的 IOS 有关
Terminal-Server(config)#line vty 0 15
Terminal-Server(config-line)#login
```

```
Terminal-Server(config-line)#password CISCO
Terminal-Server(config-line)#logging synchronous
Terminal-Server(config-line)#exec-timeout 0 0
Terminal-Server(config-line)#exit
//以上配置 Telnet 该访问服务器时需要输入的密码，并且配置长时间不输入命令也不会自动 Logout 出来
Terminal-Server#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
Terminal-Server(config)#interface fastEthernet 0/0
Terminal-Server(config-if)#ip address 10.3.24.31 255.255.255.0
Terminal-Server(config-if)#no shutdown
Terminal-Server(config-if)#exit
//配置以太网端口的 IP 地址并打开端口
Terminal-Server(config)#no ip routing
//由于访问服务器不需要路由功能，所以关闭路由功能，这时访问服务器相当于一台计算机
Terminal-Server(config)#ip default-gateway 10.3.24.254
//配置网关，允许他人从别的网段 Telnet 该访问服务器
```

（2）配置线路，制作简易菜单

```
Terminal-Server#show line
    Tty Line Typ      Tx/Rx      A Modem  Roty AccO AccI  Uses  Noise  Overruns   Int
*     0    0 CTY                   -    -    -    -    -     4      0     0/0      -
      1    1 AUX      9600/9600    -    -    -    -    -     0      0     0/0      -
*   1/0   66 TTY     9600/9600    -    -    -    -    -    14      1     0/0      -
*   1/1   67 TTY     9600/9600    -    -    -    -    -    13   2790     0/0      -
*   1/2   68 TTY     9600/9600    -    -    -    -    -    12      7     4/16     -
    1/3   69 TTY     9600/9600    -    -    -    -    -    12      2     0/0      -
*   1/4   70 TTY     9600/9600    -    -    -    -    -     4     55     0/0      -
（省略部分输出）
   1/14   80 TTY     9600/9600    -    -    -    -    -     0      0     0/0      -
   1/15   81 TTY     9600/9600    -    -    -    -    -     0      0     0/0      -
*   514  514 VTY                  -    -    -    -    -    21      0     0/0      -
（省略部分输出）
   520  520 VTY                   -    -    -    -    -     6      0     0/0      -
```

以上是查看访问服务器上异步模块的各异步口所在的线路编号，TTY 表示的就是异步模块，该访问服务器模块有 16 个端口，线路编号为 66～81，这里实际上只用了 66～72。记住线路的编号，后面须要根据这些编号进行配置。

```
Terminal-Server#configure terminal
Terminal-Server(config)#line 66 81
Terminal-Server(config-line)#transport input all
//进入线路模式，线路允许所有进入，实际上只允许 Telnet 进入即可
Terminal-Server(config-line)#no exec
//不允许该 line 接受一个 exec 会话，即只能被反向 Telnet
Terminal-Server(config-line)#exec-timeout 0 0
```

```
//以上配置超时时间为 0
Terminal-Server(config-line)#logging synchronous
Terminal-Server(config-line)#exit
Terminal-Server(config)#interface loopback0
Terminal-Server(config-if)#ip address 1.1.1.1 255.255.255.255
```

创建一个环回口并配置 loopback0 端口的 IP 地址，loopback 端口是一个逻辑上的端口，路由器上可以任意创建几乎无穷多的 loopback 端口，该端口可以永远是 UP 的。loopback 端口经常用于测试等。

```
Terminal-Server(config)#ip host R1 2066 1.1.1.1
Terminal-Server(config)#ip host R2 2067 1.1.1.1
Terminal-Server(config)#ip host R3 2068 1.1.1.1
Terminal-Server(config)#ip host R4 2069 1.1.1.1
Terminal-Server(config)#ip host S1 2070 1.1.1.1
Terminal-Server(config)#ip host S2 2071 1.1.1.1
Terminal-Server(config)#ip host S3 2072 1.1.1.1
```

从访问服务器上控制各路由器是通过反向 Telnet 实现的，此时 Telnet 的端口号为线路编号加上 2000，例如，line 66，其端口号为 2066，如果要控制 line 66 线路上连接的路由器，可以采用“**telnet 1.1.1.1 2066**”命令。然而这样命令很长，为了方便，使用“**ip host**”命令定义一系列的主机名，这样可以直接输入“R1”控制 line 66 线路上连接的路由器了。

```
Terminal-Server(config)#alias exec cr1 clear line 66
Terminal-Server(config)#alias exec cr2 clear line 67
Terminal-Server(config)#alias exec cr3 clear line 68
Terminal-Server(config)#alias exec cr4 clear line 69
Terminal-Server(config)#alias exec cs1 clear line 70
Terminal-Server(config)#alias exec cs2 clear line 71
Terminal-Server(config)#alias exec cs3 clear line 72
```

//定义了一系列的命令别名，例如，“cr1”=“**clear line 66**”，“**clear line**”命令的作用是清除线路，有时候会出现无法连接到被控设备的情形，需要把线路清除一下

```
Terminal-Server(config)#privilege exec level 0 clear line
Terminal-Server(config)#privilege exec level 0 clear
//在用户模式下也能使用“clear line”和“clear”命令
Terminal-Server(config)#banner motd @
Enter TEXT message.  End with the character '@'.
        ************************************
        R1------R1      cr1-----clear line 66
        R2------R2      cr2-----clear line 67
        R3------R3      cr3-----clear line 68
        R4------R4      cr4-----clear line 69
        S1------s1      cs1-----clear line 70
        S2------s2      cs2-----clear line 71
        S3------s3      cs3-----clear line 72
        ************************************
@
```

以上命令完成了一个简单的菜单，提醒用户：要控制路由器 R1 可以使用“R1”命令（大小写不敏感）；要清除路由器 R1 所在的线路，可以使用“cr1”命令。这里是利用路由器的 banner motd 功能实现的，该功能使得用户 Telnet 到路由器后，就显示以上简易菜单。

```
Terminal-Server#copy  running-config  startup-config  //保存配置
```

4. 实验调试

（1）测试能否从访问服务器上控制路由器和交换机

在计算机上配置网卡的 IP 地址为 10.3.24.60/255.255.255.0 网段上的 IP 地址，打开 DOS 命令行窗口。首先测试计算机和路由器的 IP 连通性，再进行 Telnet 远程登录。测试如下：

```
C:\Documents and Settings\longkey>ping 10.3.24.31
Pinging 10.3.24.31 with 32 bytes of data:
Reply from 10.3.24.31: bytes=32 time<1ms TTL=255
Reply from 10.3.24.31: bytes=32 time<1ms TTL=255
Reply from 10.3.24.31: bytes=32 time=1ms TTL=255
Reply from 10.3.24.31: bytes=32 time=18ms TTL=25
Ping statistics for 10.3.24.31:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%)
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 18ms, Average = 4ms
//表明计算机能 ping 通访问服务器
C:\Documents and Settings\longkey>telnet 10.3.24.31
User Access Verification
Password:在此输入密码 CISCO
        **************************************
        R1-------R1      cr1------clear line 66
        R2-------R2      cr2------clear line 67
        R3-------R3      cr3------clear line 68
        R4-------R4      cr4------clear line 69
        S1-------s1      cs1------clear line 70
        S2-------s2      cs2------clear line 71
        S3-------s3      cs3------clear line 72
        **************************************
//Telnet 到 10.3.24.31 后，出现简易菜单
Terminal-Server>cr1
[confirm]
 [OK]
Terminal-Server>  //先用“cr1”命令清除线路 66，该线路上连接了路由器 R1
Terminal-Server>r1
Trying R1 (1.1.1.1, 2066)... Open
        **************************************
        R1-------R1      cr1------clear line 66
        R2-------R2      cr2------clear line 67
```

```
R3-------R3        cr3------clear line 68
R4-------R4        cr4------clear line 69
S1-------s1        cs1------clear line 70
S2-------s2        cs2------clear line 71
S3-------s3        cs3------clear line 72
************************************
R1>
```

输入“r1”命令，如果出现“R1>”或者“Router>”等字符，表明可以控制路由器 R1 了；如果出现以下情况：

```
Terminal-Server>r1
Trying R1 (1.1.1.1, 2066)...
% Connection refused by remote host
```

在执行几次“cr1”命令后，重新执行“r1”命令。

（2）测试能否从访问服务器上控制各路由器和交换机

重复步骤（1），可以打开不同路由器或者交换机的控制窗口，这样就可以在一台计算机上同时配置不同的路由器和交换机了，如图 1-5 所示。当然，一台路由器只能被一台计算机所控制。

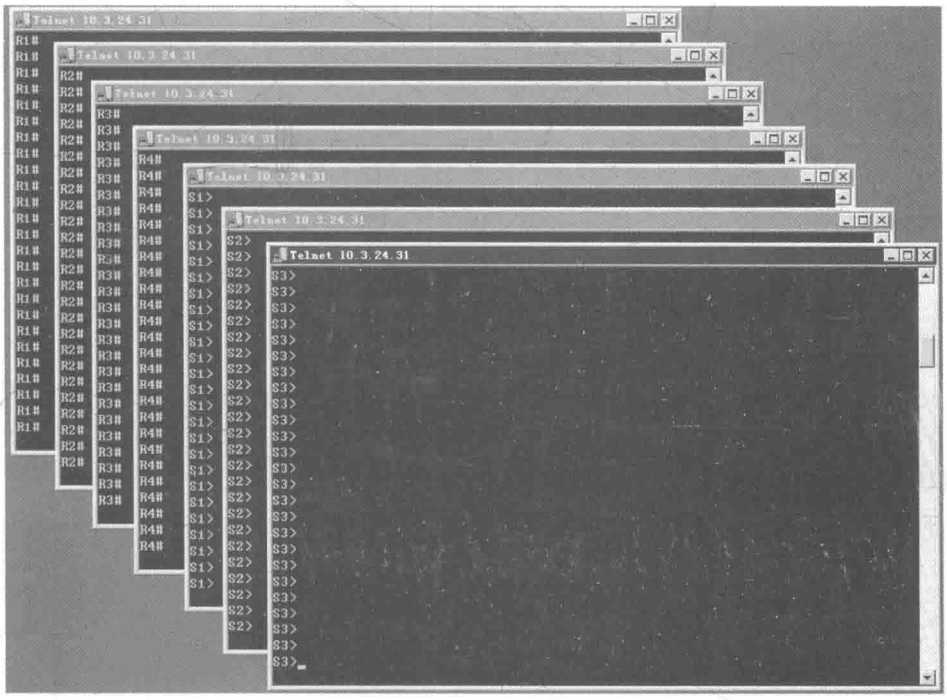


图 1-5　打开多个路由器或者交换机的控制窗口

提示

在实际应用中，如果须要配置多台设备，不建议使用 Windows 自带的 Telnet 程序，可以选用 SecureCRT 等专业终端软件，这些软件的功能完善，更方便使用。使用 SecureCRT 软件打开多个路由器或者交换机的控制窗口，如图 1-6 所示。

图 1-6　使用 SecureCRT 软件打开多个路由器或者交换机的控制窗口

1.3　实验 2：交换机的密码恢复

1. 实验目的

通过本实验可以掌握交换机的密码恢复步骤。

2. 实验拓扑

交换机的密码恢复和 IOS 恢复实验拓扑如图 1-7 所示。

图 1-7　交换机的密码恢复和 IOS 恢复实验拓扑

3. 实验步骤

Cisco 交换机的密码恢复步骤和路由器的密码恢复方法差别较大，并且不同型号的交换机恢复方法也有所差异。和路由器一样，在恢复交换机密码的过程中操作者也要在交换机的现场。以下是 Catalyst 3560 V2（Catalyst 2950 也类似）交换机的密码恢复步骤。

① 拔掉交换机电源，按住交换机前面板的 Mode 键不放，接上电源，此时，你会看到如下提示。

```
Base ethernet MAC Address: 00:23:ac:7d:6c:80
Xmodem file system is available.
The password-recovery mechanism is enabled.

The system has been interrupted prior to initializing the
flash filesystem.  The following commands will initialize
the flash filesystem, and finish loading the operating
system software:
    flash_init
```

```
boot
```

② 输入 **flash_init** 命令。

```
switch: flash_init
Initializing Flash...
flashfs[0]: 456 files, 6 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 32514048
flashfs[0]: Bytes used: 17016320
flashfs[0]: Bytes available: 15497728
flashfs[0]: flashfs fsck took 14 seconds.
...done Initializing Flash.
```

③ 修改配置文件名。

```
switch: dir flash:
Directory of flash:/
2      -rwx   1639        <date>                config.text
4      -rwx   7960810     <date>                c3560-advipservicesk9-mz.122-46.SE.bin
15497728 bytes available (17016320 bytes used)
//config.text 是交换机的启动配置文件，和路由器的 startup-config 类似

switch: rename flash:config.text flash:config.old
//修改启动配置文件名，这样交换机在启动时就读不到 config.text 了，交换机启动后将没有任何配置，从而没有了密码
```

④ 输入 **boot** 命令重启系统，这次就不要再按住 Mode 键了。启动需要等待几分钟时间。

⑤ 当出现如下提示时，输入 n。

```
Would you like to enter the initial configuration dialog? [yes/no]:n
```

⑥ 用 **enable** 命令进入 enable 状态，并将文件 config.old 改回 config.text。

```
Switch#rename flash:config.old flash:config.text
Destination filename [config.text]?回车
```

⑦ 将原配置装入内存。

```
Switch#copy   flash:config.text   running-config
Destination filename [running-config]?回车
```

⑧ 修改密码。

```
S1#configure terminal
S1(config)#enable secret cisco
S1(config)#exit
```

⑨ 将配置重新写入 nvram。

```
S1#copy running-config startup-config
Destination filename [startup-config]?回车
```

1.4 实验 3：交换机的 IOS 恢复

1. 实验目的

通过本实验可以掌握交换机的 IOS 恢复步骤。

2. 实验拓扑

交换机的 IOS 恢复实验拓扑如图 1-7 所示。为了节约时间，本实验使用了一个较小的 IOS c3560-advipservicesk9-mz.122-46.SE.bin 进行恢复。

3. 实验步骤

如果交换机已经正常开机，IOS 不小心被破坏，则 IOS 可以从 TFTP 服务器上恢复（使用 **copy tftp flash** 命令，本书不在此介绍该方法）。然而，如果交换机无法正常开机，交换机 IOS 不能从 TFTP 服务器恢复，而要使用 XModem 方式，该方式是通过 Console 口从计算机下载 IOS，因此速度很慢。步骤如下：

① 把计算机的串口和交换机的 Console 口连接好，用超级终端软件连接上交换机，默认时 Console 的通信速率是 9 600 bps。

② 交换机开机后（因为 IOS 有故障，所以无法正常开机），执行以下命令。

```
Interrupt within 5 seconds to abort boot process.
Boot process failed...

The system is unable to boot automatically.  The BOOT
environment variable needs to be set to a bootable
image.
switch: flash_init
```

由于默认时 Console 的波特率（通信速率）是 9 600 bps，如果用该速率来传送 IOS 会很费时，所以需要把 Console 的波特率改为 115 200 bps，如下：

```
switch: set BAUD 115200
```

这将造成超级终端软件和交换机的连接断开，请用新的速率 115 200 bps，重新把超级终端软件和交换机进行连接。

③ 输入拷贝指令。

```
switch:copy -b 4096 xmodem: flash:c3560-advipservicesk9-mz.122-46.SE.bin
```

该命令的含义是通过 Xmodem 方式拷贝文件，保存在 Flash 中，文件名为 **c3560-advipservicesk9-mz.122-46.SE.bin**，4096 是缓冲区的大小。出现如下提示：

```
Begin the Xmodem or Xmodem-1K transfer now...
CCCC
```

在超级终端窗口中，选择【发送】→【发送文件】菜单，打开图 1-8 窗口，选择 IOS 文件，协议为“Xmodem”。单击“发送”按钮开始发送文件。由于速度很慢，通常需要几个小时，请耐心等待，通信速率为 115 200 bps，如图 1-9 所示。