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

◎ 王隆杰　梁广民　编著
◎ 马　刚　李涤非　审校

以企业需求为**指导**

提升读者的实际操作技能

讲求**实用**

理论够用，**操作**为主

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

思科系列丛书

思科网络实验室 CCNP（交换技术）实验指南

王隆杰　梁广民　编著

马　刚　李涤非　审校

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。全书分为 8 章，主要内容包括：实验台拓扑，VLAN、Trunk、VTP 与链路聚集，STP，VLAN 间路由，高可用性，交换机的安全，QoS，组播。本书的重点是实验，希望通过实验能有效地帮助读者掌握技术原理及其使用场合。本书采用 Catalyst3560 作为硬件平台（IOS 版本为 12.2）。

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，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. —北京：电子工业出版社，2012.5
（思科系列丛书）

ISBN 978-7-121-16904-5

Ⅰ. ①思… Ⅱ. ①王… ②梁… Ⅲ. ①计算机网络—信息交换机—工程技术人员—资格考试—自学参考资料 Ⅳ. ①TN915.05

中国版本图书馆 CIP 数据核字（2012）第 084871 号

策划编辑：宋 梅
责任编辑：宋 梅
印 刷：北京丰源印刷厂
装 订：三河市鹏成印业有限公司
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：787×1 092 1/16 印张：24.25 字数：621 千字
印 次：2012 年 5 月第 1 次印刷
印 数：4 000 册 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。

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。

服务热线：（010）88258888。

序

仔细阅读了王隆杰和梁广民老师的这部新作，我对他们多年来能够潜心钻研网络技术并不断取得的成果表示敬佩。两位老师是中国区思科网络技术学院金牌教师，均通过两个领域的 CCIE 认证考试，具有扎实的网络基础和娴熟的网络技能，多年来一直工作在教学第一线，其教学风格和教学效果得到来自全国各地的教师和学生的高度认可。在他们的指导下，该校 150 多名学生通过 CCIE 认证考试，登上了网络领域的珠穆朗玛峰，同时他们指导的学生在网络大赛中成绩斐然，是中国至今囊括思科网络技术学院学生所有级别（中国大陆地区、大中华区、亚太区）比赛冠军的唯一院校。他们以企业实际需要来组织和编写本书，并把自己对网络技术的热情以及从事第一线教学工作的经验和专业知识倾注于此书，书中所阐述的网络原理深入浅出，案例充足、实用，实验结果和分析说明详尽，与从国外引进的原版翻译教材相比，更适合中国人的阅读思维和习惯，有助于读者快速理解和掌握知识，提高网络技能。

我相信本书对于加入思科网络技术学院的学生、计划参与思科认证考试的人员以及从事网络工程的技术人员都是非常有帮助的。

思科公司总裁约翰·钱伯斯先生曾说，“互联网和教育是推动社会公平发展的两个核心动力”。秉承这一理念，思科公司积极参与和推动中国教育事业的发展，在中国设立了近 400 所思科网络技术学院，在校学生超过 5 万名，累计参加学习的学生人数超过 15 万名。思科公司始终坚信，互联网必将改变人们的工作、学习、生活和娱乐方式，而这一理念的实现，是全体支持互联网发展的研究专家、系统厂商、技术与应用开发商、运营商、教育机构和消费者共同努力的结果。在此也感谢二位老师为此所付出的努力！

思科系统（中国）网络技术有限公司
中国思科网络技术学院总经理

2012 年 5 月 1 日

前　言

CCNP 涉及交换的内容不是很多，然而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和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。也许理论和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？那就让我们在实验室做做实验吧，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 642-813）所需的知识精心规划了 58 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设实验台的时间。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。鉴于现用 CCNP 教材对 QoS 和组播的介绍不是很深入，本书对 QoS 和组播的理论做了较多介绍，这和本书以实验为主的编写原则有些相悖。本书并未编写无线网络的内容，如果下一版没有篇幅的限制，应该会把这些内容加入其中。

全书分为 8 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、中继和带宽汇聚、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；第 7 章用很大的篇幅从理论上对 QoS 进行简明、系统性的介绍，包括 CLI 下的各种队列技术、MQC 的分类和标记技术、用于拥塞避免的 WRED，以及流量整形和流量监控，详细介绍了三层交换上的 QoS 技术——SRR；第 8 章着重介绍组播理论，包括管理组成员的 IGMP 协议、组播路由协议 PIM 的密集和稀疏模式、稀疏模式中 RP 的自动选举，以及在二层交换机上防止组播泛洪的 IGMP Snooping。

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，参加编写的还有张喜生、石淑华、杨旭、刘平、张立涓、石光华、邹润生、杨名川和齐治文。感谢北京邮电大学马刚和李涤非老师在百忙之中审校全书。感谢思科公司韩江总经理、刘亢经理和熊露颖经理对本书提出的建设性意见和建议，也感谢韩江总经理在百忙之中为本书作序。感谢沃尔夫网络实验室（www.wolf-lab.com）对本书的关键技术给予的指导和帮助。如果没有他们的帮助本书是不可能在很短的时间内高质量完成的，在此也向他们表示衷心的感谢！

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

2012 年 5 月于深圳

目　录

第 1 章　交换机基本配置

本章首先将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），本书所有的实验均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。

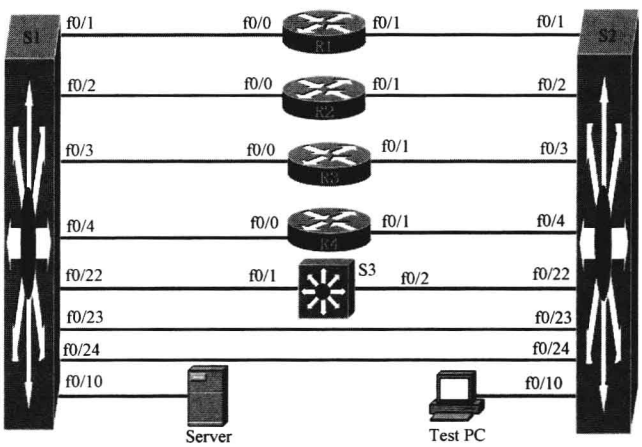

图 1-1　本书实验拓扑（以太网连接部分）

在图 1-1 拓扑中，4 台路由器均为 CISCO2811 路由器，也可以采用 CISCO2801 路由器（差别在于 CISCO2811 带有一个扩展插槽，而 CISCO2801 没有扩展插槽），IOS 采用 c2800nm-advipservicesk9-mz.124-24.T1.bin；3 台三层交换机为 Catalyst 3560，IOS 采用 c3560-advipservicesk9-mz.122-46.SE.bin 。所有路由器的 FastEthernet0/0 以太网接口和交换机 S1 进行连接；FastEthernet0/1 以太网接口则和交换机 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 接口连接到 S1

的 FastEthernet0/22 上，FastEthernet0/2 接口连接到 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。

如图 1-2 拓扑所示，4 台路由器之间通过串行链路进行连接。

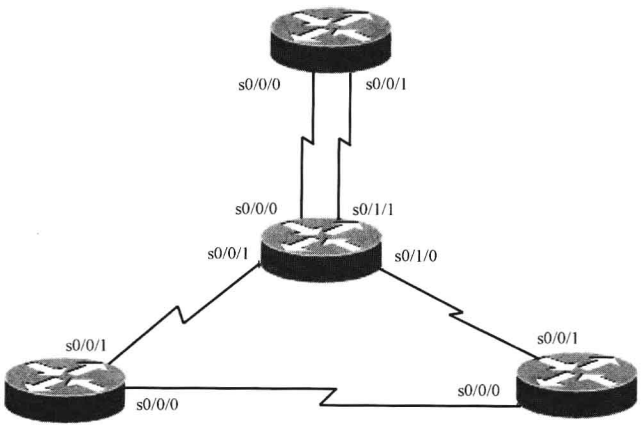

图 1-2　本书实验拓扑（广域网连接部分）

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性拔插 Console 线，非常不方便。访问服务器可以解决这个问题，连接方法如图 1-3 所示。访问服务器可以是一台有 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。

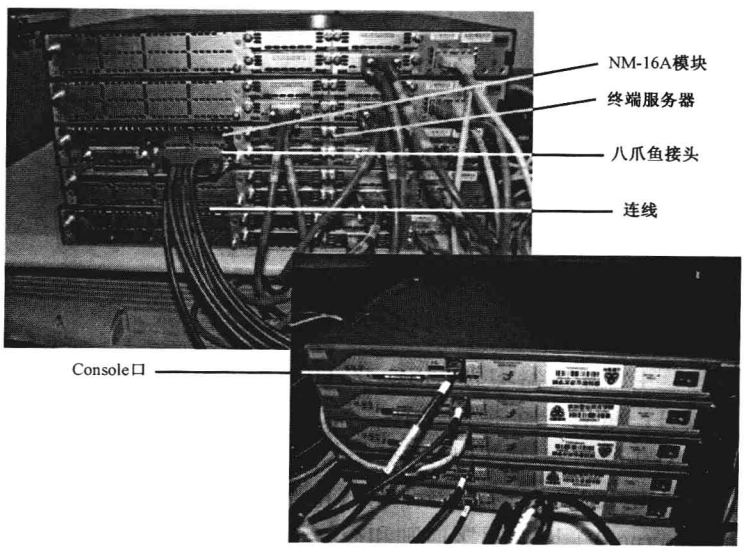

图 1-3　访问服务器和网络设备的连接方法

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-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。

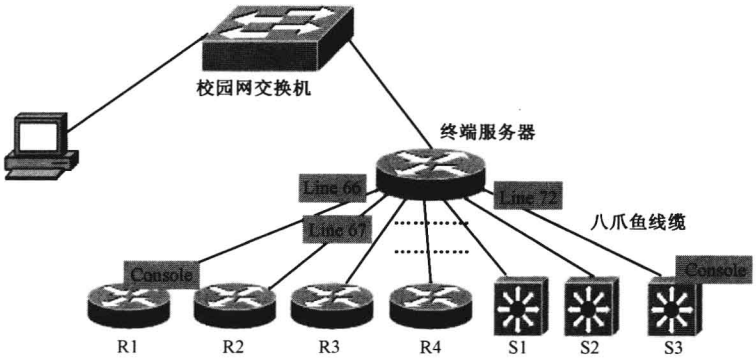

图 1-4　访问服务器与各路由器和交换机连接实验拓扑

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 ?
  <1-988>   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。路由器支持多少 vty 和路由器的 IOS 有关
Terminal-Server(config)#line vty 0 988
Terminal-Server(config-line)#no login
Terminal-Server(config-line)#logging synchronous
```

```
Terminal-Server(config-line)#exec-timeout 0 0
Terminal-Server(config-line)#exit
//以上允许任何人不需密码就可以 Telnet 该访问服务器，并且即使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 10.3.24.31 255.255.255.192
Terminal-Server(config-if)#no shutdown
Terminal-Server(config-if)#exit
//配置以太网接口的 IP 地址，并打开接口
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 10.3.24.62
//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 个接口，线路编号为 66～81，这里实际上只用了 66～72。记住线路的编号，后面需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
//在进入线路模式下，线路允许所有传入，实际上，只允许 Telnet 进入即可
Terminal-Server(config-line)#no exec
//不允许这个 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 接口的 IP 地址，loopback 接口是一个逻辑上的接口，路由器上可以任意创建几乎无穷多的 loopback 接口，该接口可以永远是 UP 的。loopback 接口经常用于测试等。

```
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，所以在以上使用“**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
//以上是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
//以上是使得人们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
        **************************************
@
```

以上是制作一个简单的菜单，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 10.3.24.60/255.255.255.192 网段上的 IP 地址，并打开 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
//以上表明计算机能 ping 通访问服务器
C:\Documents and Settings\longkey>telnet 10.3.24.31
          ************************************
          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。

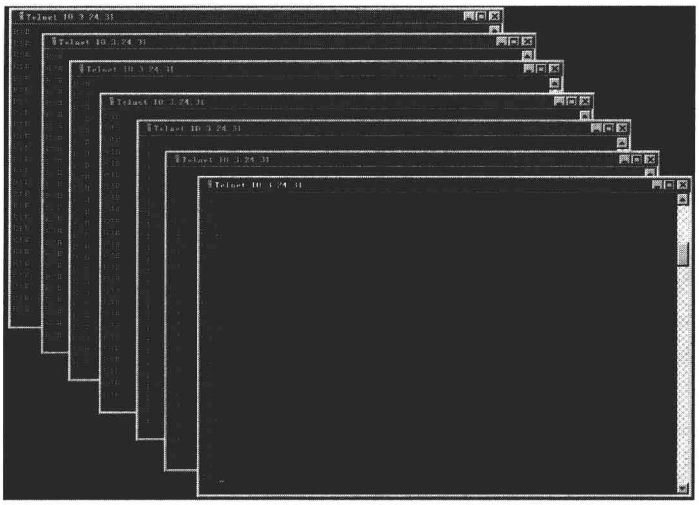

图 1-5　打开多个路由器或者交换机的控制窗口

提示

在实际应用中，如果需要配置多台设备，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。如图 1-6 所示。

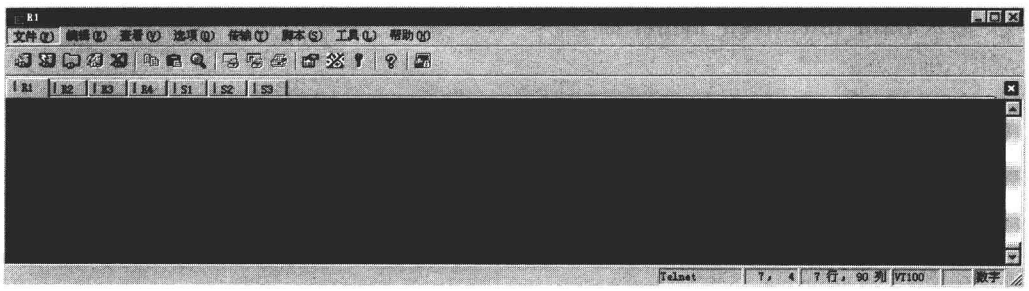

图 1-6　使用 SecureCRT 软件打开多个路由器或者交换机的控制窗口