第 3 章　网络设备基本配置

本章学习目标

- 掌握网络设备基本配置方法
- 熟悉利用 Console 口对网络设备进行配置的过程
- 精通网络设备几种常见的配置模式
- 精通网络设备基本配置命令
- 熟悉利用 Telnet 对网络设备进行配置的过程
- 了解利用 Web 对网络设备进行配置的过程
- 掌握 Show 命令
- 熟悉 CDP

本章先向读者介绍利用 Console 口对网络设备进行配置的过程，接着介绍常见的网络设备配置模式，详细介绍常见的网络设备基本配置命令。之后介绍利用 Telnet 以及 Web 对网络设备进行配置的过程。

本章最后介绍常见的 Show 命令，并介绍思科专有协议 CDP。

3.1　利用 Console 口对网络设备进行配置

网络设备是特殊用途的计算机，然而网络设备没有键盘和显示器等关键的外部设备，若不借助其他设备，就不可能对网络设备进行配置，因此，对网络设备进行配置需要借助计算机完成。对网络设备进行初始化配置，需要将计算机的串口和网络设备的 Console 口进行连接。对网络设备进行初始化配置后，就可以使用其他方式对网络设备进行配置了，如 Telnet、Web Browser、网络管理软件以及 AUX 等。

Console 口是网络设备的控制端口，Console 口使用专用连线直接连接至计算机的串口，然后利用终端仿真程序（如 Windows 下的“超级终端”）对路由器进行本地配置。路由器的 Console 口一般为 RJ-45 口。

Console 口是用来配置网络设备的，所以只有网管型网络设备才有 Console 口。并且还要注意，并不是所有网管型网络设备都有，因为网络设备的配置形式有多种，如通过 Telnet 命令行方式或 Web 方式等。

Console 线一般有 3 种类型，一种为两端均为 DB9 母头的配置线缆，如图 3.1 所示；另一种为一端为 DB9 公头，另一端为 DB9 母头的，如图 3.2 所示。两端可以分别插入计算机的串口和网络设备的 Console 口，现在的笔记本电脑基本已经不带串口，需要使用 USB 转串口的转接器；第三种为一端是 DB9 母头，另一端是 RJ-45 头

图 3.1　两端均为 DB9 母头的配置线缆

的配置线缆，如图 3.3 所示。

图 3.2　一端是 DB9 母头，另一端是 DB9 公头的配置线缆

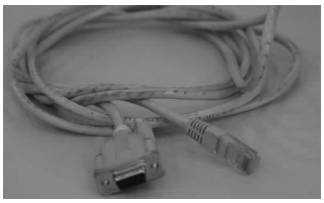

图 3.3　一端是 DB9 母头，另一端是 RJ-45 头的配置线缆

通过 Console 口连接并配置网络设备，是配置和管理企业级网络设备的必要步骤。因为其他配置方式往往需要借助网络设备的 IP 地址、域名或设备名称才可以实现，而新购买的网络设备显然不可能内置有这些参数，所以 Console 口是最常用、最基本的网络设备管理和配置端口。

不同类型的网络设备其 Console 口所处设备的位置不相同，有的位于前面板，有的位于后面板。通常，模块化网络设备大多位于前面板，而固定配置网络设备则大多位于后面板。在该端口的上方或侧方都会有类似 CONSOLE 或 Console 字样的标识。

除位置不同外，Console 口的类型也有所不同，绝大多数网络设备都采用 RJ-45 口，但也有少数采用 DB9 串口端口或 DB25 串口端口。

通过 Console 口访问网络设备的过程如下。

(1) 准备工作。

用配置线将计算机 COM1 口和网络设备的 Console 口连接起来，开启计算机和网络设备。

(2) 打开计算机操作系统的超级终端程序。

在 Windows 中依次选择“开始”→“程序”→“附件”→“通信”，单击通信菜单下的“超级终端”程序。在“连接描述”对话框中，为连接设置一个名称，如 switch；同时为连接选择一个图标。单击“确定”按钮，在“连接到”窗口中的“连接时使用”下拉菜单中选择计算机的 COM1 端口。单击“确定”按钮。使用笔记本电脑时，由于笔记本电脑通常没有 COM 口，所以需要使用 USB 转 COM 口的转接器，同时需要安装设备的驱动程序，否则不会出现串口。

(3) 设置通信参数。

在 COM1 属性窗口中，将对端口 COM1 属性进行设置，包括设置“每秒位数”“数据位”“奇偶校验”“停止位”“数据流控制”。由于网络设备出厂时 Console 口的通信波特率通常为 96000b/s，因此在 COM1 属性窗口中单击“还原默认值”按钮，默认值为：每秒位数为“96000”，数据位为“8”，奇偶校验为“无”，停止位为“1”，数据流控制为“无”。单击“确定”按钮，并且按回车键，此时在超级终端窗口中开始加载网络设备操作系统。

加载完操作系统后，可以对网络设备进行配置。如果确定连线没有问题，超级终端回车没有反应，这时很有可能是网络设备的 Console 口的通信波特率被修改了。此时需要修改 COM1 口属性对话框的波特率并逐一进行测试。

3.2 网络设备的基本配置

3.2.1 网络设备的常见配置模式

常见的网络设备配置模式有 6 种，分别为用户模式、特权模式、全局配置模式、线路配置模式、端口配置模式以及 VLAN 配置模式等。

1. 用户模式

```
Router>
```

用户模式网络设备开机直接进入的配置模式。在该模式下只能查询交换机的一些基本信息，如版本号(show version)等。

2. 特权模式

```
Router#
```

在普通用户模式下输入“enable”命令即可进入特权用户模式，在该模式下可以查看网络设备的配置信息和调试信息等，具体配置命令如下。

```
Router>enable
Router#
```

通过 exit 命令退回到用户模式。

3. 全局配置模式

在特权用户模式下输入“configure terminal”命令即可进入全局配置模式，在该模式下主要完成全局参数的配置，具体配置命令如下。

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

通过 exit 命令可以退回到特权模式。

```
Router(config)#exit
Router#
```

4. 线路配置模式

在全局配置模式下输入“line console console-list”或者“line vty vty-list”进入 Line 线路配置模式。该模式主要对控制台端口或虚拟终端 VTY 进行配置。其配置可以设置控制台和虚拟终端的用户级登录密码，以及其他与该配置模式有关的配置。进入控制台的具体配置如下。

```
Router(config)#line console 0
Router(config-line)#
```

进入编号为 0 的控制台端口。

```
Router(config-line)#exit
Router(config)#
```

通过 exit 命令退回到全局配置模式。

进入虚拟终端 VTY 的具体配置如下。

```
Router(config)#line vty 0 4
Router(config-line)#
```

进入虚拟终端配置模式，表示将对 VTY 的 0～4 号端口（即 0 号、1 号、2 号、3 号、4 号）进行配置。

```
Router(config-line)#exit
Router(config)#
```

通过 exit 命令退回到全局配置模式。

5. 端口配置模式

在全局配置模式下输入“interface interface-list”即可进入相应端口配置模式，在该模式下主要完成端口参数的配置。进入端口 fa0/0 的配置如下。

```
Router(config)#interface fastEthernet 0/0
Router(config-if)#
```

表示进入路由器 fastEthernet0/0 端口，即将对该端口进行配置。

```
Router(config-if)#exit
Router(config)#
```

通过 exit 命令退回到全局配置模式。

6. VLAN 配置模式

在全局配置模式下输入“vlan vlan-number”即可进入 vlan 配置模式，在该配置模式下可以完成 VLAN 的一些相关配置。进入 VLAN1 的具体配置如下。

```
Switch(config)#interface vlan 1
Switch(config-if)#
```

进入 vlan 端口模式。

```
Router(config-if)#exit
Router(config)#
```

通过 exit 命令退回到全局配置模式，VLAN 配置模式只能在网络设备交换机中配置。

3.2.2　网络设备的常见配置命令

1. 为设备配置主机名

利用命令 hostname 对网络设备进行命名。对路由器设备命名的配置如下。

```
Router(config)#hostname R1
R1(config)#
```

利用 no hostname 命令将设备名称恢复为配置前的名称。

```
R1(config)#no hostname
Router(config)#
```

对交换机设备命名，具体配置如下。

```
Switch(config)#hostname S1
S1(config)#
```

2. 显示配置命令

显示配置命令“show”用于帮助用户查看相关信息，根据“show”命令后面的参数决定显示信息的内容。该命令可以同时在用户模式和特权模式下运行，常见的参数如下。

```
Router#show running-config
```

用于查看当前的运行配置。

```
Router#show version
```

用于查看网络设备运行操作系统版本及相关引导信息。

```
Router#show startup-config
```

用于查看保存的配置信息。

```
Router#show ip route
```

用于查看路由信息。

3. 网络设备特权加密口令设置

网络设备不同配置模式下可执行的命令是不同的，用户模式可执行的命令明显少于特权模式下可执行的命令，特权模式的权限高于用户模式。通过 enable 命令可以将网络设备从用户模式直接切换成特权模式，这样的切换若不加以限制，会对网络设备的安全造成威胁。

（1）通过设置使能密码加强设备的安全性，具体配置过程如下。

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#enable password 123456
Router(config)#
```

通过以上命令将网络设备的使能密码设置为 123456。若通过 enable 命令从用户模式进入特权模式，此时需要输入密码。具体过程如下。

```
Router>enable
Router>enable
Password:
Router#
```

在将网络设备的工作模式由用户模式切换到特权模式时，需要输入密码“123456”，只有密码输入正确，才能顺利进入特权模式，才能对设备进行进一步的配置。

(2) 通过对使能口令进行加密加强口令的安全性。

使能密码的设置在一定程度上不是太安全，通过 show 命令查看配置信息时，可以看到加密的明文密码。下面是通过命令“Router # show running-config”查看到的配置信息，并且可以看到明文的使能密码为 123456，如图 3.4 所示。

通过执行命令“Router(config) # service password-encryption”，可以实现对使能口令进行加密。具体操作如下。

```
Router(config)#enable password 123456
Router(config)#service password-encryption
```

通过命令“Router # show running-config”，查看网络设备运行的配置信息。显示结果如图 3.5 所示。通过显示结果可以看出，原本的明文密码 123456 变成一串密文信息。

```
Router#show running-config
Building configuration...

Current configuration : 475 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
enable password 123456
!
!
!
!
  以下显示省略
```

图 3.4　可以直接查看到的明文密码信息

```
Router#show run
Building configuration...

Current configuration : 482 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Router
!
!
!
enable password 7 08701E1D5D4C53
!
!
!
!
'           以下显示省略
```

图 3.5　对使能密码进行加密

(3) 通过设置加密口令增强设备的安全性。

除了通过命令“Router(config) # service password-encryption”对使能口令进行加密以增强安全性外，还可以直接设置加密口令。具体设置如下。

```
Router(config)#enable secret 123
```

通过 show 命令查看配置命令结果如图 3.6 所示。

```
Router#show running-config
Building configuration...

Current configuration : 499 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
enable secret 5 $1$mERr$3HhIgMGBA/9qNmgzccuxv0
!
!
!
```

图 3.6　查看配置情况

可以看出，口令“123”在配置文件中以 MD5 加密的密文形式显示。

4. 帮助命令

在配置网络设备的过程中，如果有记不住的命令以及命令格式，可以通过在命令提示符下输入“?”请求帮助。

(1) 查看所在模式下可执行的命令。

```
Router>?
```

该命令可以查看用户模式下可执行的命令。

(2) 查看特权模式下可执行的命令。

```
Router#?
```

(3) 查看用户模式下以字母 e 开头的命令。

```
Router>e?
enable  exit
```

(4) 查看命令所带的格式参数。

```
Router>enable ?
  <0-15>Enable level
  view  Set into the existing view
```

5. 命令简写

在网络设备的具体配置过程中，有时候并不需要输入完整的命令格式。可以通过命令简写对设备进行配置。

```
Router>en
Router#
```

在通过命令 enable 将设备的工作模式由用户模式切换成特权模式时，只输入 en 即可。原因是，在用户模式下可执行的命令中，以 en 开头的命令只有 enable，也就是 en 能够唯一确定命令 enable 。如果仅输入命令 e，由于以 e 开头的命令有两个，分别为 enable 以及 exit，不能唯一确定，所以执行出错，如下所示。

```
Router>e
%Ambiguous command: "e"
```

6. 通过 Tab 键自动补齐

```
Router#en<tab>
Router#enable
```

在该模式下以 en 开头的命令只有 enable，因此在该情况下可以实现自动补齐。若此时以 en 开头的命令不止一个，则自动补齐失败。

7. 取消操作命令

在网络设备的配置过程中，有时需要清除已经配置的命令参数，此时可以采用取消命令 no 完成，以下是通过取消命令 no 对设置的特权口令进行取消的操作。

```
Router(config)#enable password 123      设置特权口令
Router(config)#no enable password       取消特权口令
```

经过取消后，又恢复成没有设置特权口令的状态。在网络设备配置过程中有时需要将关闭的端口打开，关闭端口状态一般为 shutdown，使用“no shutdown”命令可以对关闭端口 shutdown 进行相反操作，即打开端口。具体配置如下。

```
Router(config)#interface fastEthernet 0/1
Router(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
```

8. 历史记录

配置网络设备时，经常会遇到以下几种情况：①需要重复执行已经执行过的命令；②由于打错命令导致执行错误，需要对命令进行修改后再次执行；③需要掌握最近对设备所输入的配置命令情况。以上情况可以使用设备上的命令缓存，通过调入命令缓存中的历史记录解决。具体查看历史记录操作如下：①使用 Ctrl＋P 组合键，或者使用上箭头向上查找先前使用的命令；②使用 Ctrl＋N 组合键，或者使用下箭头向下查找先前使用的命令；③通过使用命令 show history 查看历史命令缓存。通过执行命令 show history 查看历史命令过程如下。

```
Router#show history
enable
configure terminal
show history
```

以上通过 show history 命令可以查看到已经配置过的保存在缓存中的命令。默认情况下，Cisco 设备缓存保存最近执行过的 10 条命令。关于历史缓存中可以保存历史命令的数目，可以通过以下命令进行修改。

```
Router(config)#line console 0
Router(config-line)#history size ?
<0-256>Size of history buffer
Router(config-line)#history size 3
```

以上命令将历史缓存数量设置为 3。在实际的工程项目中，为了设备的安全，防止别人了解设备执行过的命令情况，往往将历史缓存数值设置为 0，通过命令 show history 查看不到该设备已经执行过的命令情况。

9. 设置控制台口令，加强设备安全性

前面提到通过设置使能特权口令以及加密特权口令，可以防止非授权用户直接从用户模式进入特权模式，但不能限制非授权用户进入普通用户模式，非授权用户通过用户模式同样可以执行相关命令操作设备，从而对设备安全造成影响。通过设置控制台口令可以防止非授权用户直接进入用户模式，具体配置如下。

```
Router#config t
Router(config)#line console 0
Router(config-line)#password 123
```

```
Router(config-line)#login
```

再次进入设备时，显示结果如下。

```
User Access Verification
Password:
```

此时只有输入正确的口令，才能进入用户模式，加强设备的安全性。此时仅通过设置口令的方式限制用户进入普通用户模式不是最佳的选择，为了限制用户进入用户模式，可以同时设置用户名和口令的方式对身份进行验证，从而加强设备的安全性。具体配置如下。

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#username tdp password 123
Router(config)#line console 0
Router(config-line)#login local
```

配置完成后，通过 exit 命令退出系统，当再次进入系统时，需要同时输入用户名和口令，两者同时匹配才能进入系统的用户模式。具体如下。

```
User Access Verification
Username: tdp
Password:
Router>
```

10. 取消域名解析命令

在对网络设备进行配置过程中，有时容易输错命令，默认情况下，网络设备执行错误命令时往往将错误命令当成域名进行解析，从而导致整个过程耗时较长。为了避免较长的域名解析过程，通常需要关闭网络设备域名解析功能。

输入错误命令同时没有关闭域名解析功能，需要等待系统域名解析过程的情况如下：

```
Router>enble
Translating "enble"...domain server (255.255.255.255)
```

通过关闭网络设备域名解析功能，可以避免网络设备配置人员长时间等待。关闭网络设备域名解析过程的配置如下。

```
Router(config)#no ip domain-lookup
```

再次输入错误的命令，系统执行效果如下。

```
Router>enble
Translating "enble"
%Unknown command or computer name, or unable to find computer address
Router>
```

结果显示，输入错误命令时系统直接报错，而不再进行域名解析导致配置人员长时间等待了。

11. 开启日志同步

在对网络设备进行配置过程中，有时系统自动弹出日志信息，这些日志信息会阻隔网络

设备配置人员敲入的命令，从而影响命令的输入，通过开启日志同步命令之后，日志信息不会分隔敲到一半的命令行。

开启日志同步的具体命令如下。

```
Router(config)#line console 0
Router(config-line)#logging synchronous
```

12. 设置控制台会话超时时间

控制台 EXEC 会话超时时间默认为 10min。也就是说，当没有对系统进行任何操作的情况下，系统会在 10min 后自动退出。通过 exec-timeout 命令可以设置超时时间，通常情况下设置永不超时，也就是不让系统自动退出，配置方法如下。

```
Router(config-line)#exec-timeout 0 0
```

命令行中的“ 0 0”的含义如下：前面的“0”设置的是分钟，后面的“0”设置的是秒。设置参数值“0 0”表示系统永不超时，不会自动退出。

13. 标语命令配置

标语命令 banner 用于设置登录网络设备时显示的警示性信息，用来警示入侵者。具体配置过程如下。

```
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#banner motd $                    //表明以下警示语以$符号结束
Enter TEXT message. End with the character '$'.
Warning Don't configure my device, and if configured, you're going to be responsible
for the consequences!!! $
```

当退出系统再次进入时，系统将显示如下信息。

```
Press RETURN to get started.
Warning Don't configure my device, and if configured, you're going to be responsible
for the consequences!!!                         //对入侵者加以警示
Router>
```

14. 为网络设备配置地址信息

为路由器端口“fastEthernet 0/0”配置网络参数，将其 IP 地址配置为 192.168.1.1，子网掩码配置为 255.255.255.0，具体配置过程如下。

```
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
```

为交换机 VLAN1 配置网络参数，将其 IP 地址配置为 192.168.1.1，子网掩码配置为 255.255.255.0，具体配置过程如下。

```
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Switch(config-if)#no shu
```

```
%LINK-5-CHANGED: Interface Vlan1, changed state to up
```

15. 保存配置

首先介绍什么是 running-config 和 startup-config。

(1) running-config 指的是网络设备目前正在运行的、当前的配置。这个配置在设备的运行内存中。随着系统关机或重启,该配置会丢失。

(2) startup-config 指的是网络设备在启动时,系统初始化需要引导的配置。这个配置保存在网络设备的 nvram 可擦除存储器中。在系统关机或重启后,这个配置信息不会丢失。

在对网络设备进行配置时,命令及时生效,配置结果体现在 running-config 配置文件中,当网络设备关机或重启时,配置会丢失。所以,通常将配置文件保存到 nvram 可擦除存储器中,避免重启或关闭时配置信息丢失。具体操作如下。

```
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

该命令的效果是将设备正在运行的配置文件 running-config 保存到 nvram 可擦除存储器中。因此,每次在对网络设备路由器或者交换机作新配置时,如果不希望由于系统关机或重启而丢失,则需要使用命令 copy running-config startup-config 进行保存。

除了使用 copy running-config startup-config 保存配置信息,还可以直接通过命令 write 对设备的配置信息进行保存,具体操作如下。

```
Router#write
Building configuration...
[OK]
Router#
```

16. 对网络设备进行批量配置

在网络工程中对大量的网络设备进行配置,工作量相当大。对于统一购买的网络设备,往往需要对它们进行统一的初始化配置,如果对每台设备进行逐条命令输入,将消耗大量的精力。为了减轻工作量,此时可以进行一次性批量配置处理。通过在记事本中一次输入多条命令,将这些命令一次性粘贴到网络设备配置窗口中,可以对网络设备进行批量配置。

对网络设备进行批量配置,具体过程如下:首先将网络设备共同需要配置的命令写在记事本上,如图 3.7 所示。这里特别注意设备配置命令的前后连贯性,即执行命令的工作模式一定要吻合。

然后在所有需要初始化的设备的配置窗口中一次性粘贴这些命令,如图 3.8 和图 3.9 所示。

这样可以大大节约时间,并且能够保证所有设备都进行相同的初始化配置。

图 3.7　在记事本中输入批量命令

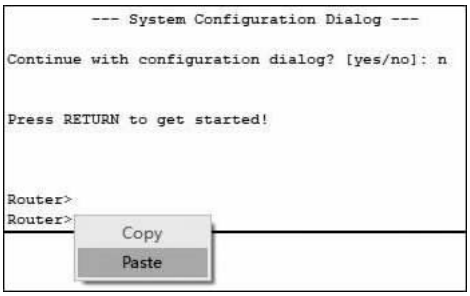

图 3.8　将记事本中的批量命令粘贴到设备的配置界面中

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#exit
Router(config)#enable password 123
Router(config)#username tdp password 123456
Router(config)#line console 0
Router(config-line)#password 321
Router(config-line)#login
```

图 3.9　网络设备执行批量命令结果

3.3　利用 Telnet 对网络设备进行配置

利用控制台 Console 口和计算机串口相连对网络设备进行配置，是对网络设备进行配置的基本方法，该配置方式的弊端是必须将计算机的串口利用全反线和网络设备的 Console 口相连，而全反线的长度是受限制的，这样计算机和被配置设备物理上要求靠近，这给远距离对网络设备进行配置造成一定的困难。Telnet 远程配置可以解决远距离对网络设备进行配置的问题。具体利用任意联网计算机，通过 Telnet 远程登录网络设备，并对其进行配置。

下面分别探讨交换机和路由器这两种设备利用 Telnet 进行配置的方法。

3.3.1　利用 Telnet 对路由器进行远程配置

利用 Telnet 对路由器进行配置结构图如图 3.10 所示，笔记本电脑利用路由器控制台 Console 口对其进行初始化配置。电脑 PC0、交换机及路由器连接成一个网络。通过该网络可以远程登录(Telnet)路由器，从而对路由器进行配置。

若要实现远程登录对路由器进行配置，需要互联互通的网络环境。图 3.10 所示网络环境的搭建需要进行基本的网络配置，具体如下。

首先在笔记本电脑上执行超级终端程序，利用路由器控制台对其进行基本配置。下面是对路由器端口 f0/0 配置其网络地址。

```
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
```

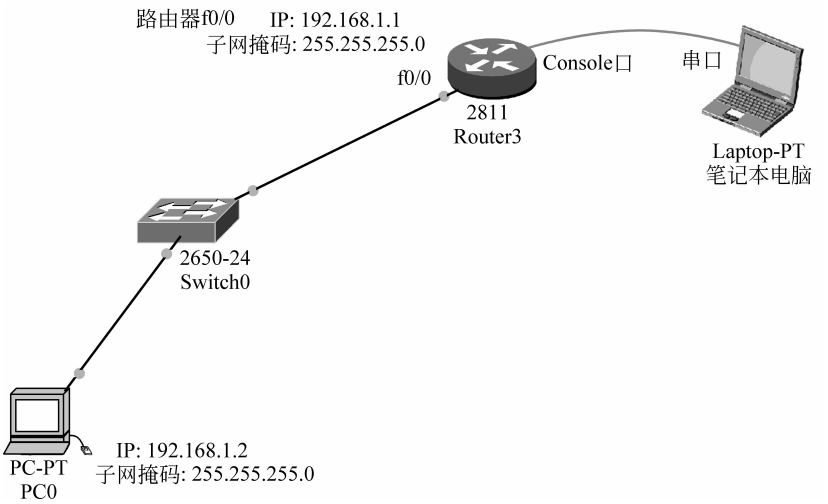

图 3.10　利用 Telnet 对路由器进行配置结构图

```
Router(config-if)# no shutdown
```

若通过 Telnet 对网络设备进行配置，需要配置设备的使能口令，命令如下。

```
Router(config)#enable password 321
```

另外需要配置远程登录线路口令，具体如下。

```
Router(config)#line vty 0 4
```

该命令表示配置远程登录线路，“0　4”是远程登录的线路编号，“vty”(virtual teletype terminal)表示虚拟终端，一种网络设备连接方式，表示下面是对 vty 的 0 到 4 号端口(即 0 号、1 号、2 号、3 号、4 号)进行配置。vty 线路指的是我们进行 Telnet 的时候使用的线路。“0　4”具体指的是对从第一个 Telnet 到第五个 Telnet 线路进行设置，即同时可以有 5 条线路进入虚拟终端。

```
Router(config-line)#password 123          //配置远程登录口令
Router(config-line)#login                 //要求口令验证
```

接下来如图 3.10 所示配置终端计算机 PC0 网络地址参数，通过计算机 PC0 远程登录对路由器进行配置。

```
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open
Warning Don't configure my device, and if configured, you're going to be responsible
for the consequences!!!
User Access Verification
Password:                                 //输入口令 321
Router>en
Router>enable
Password:                                 //输入口令 123
```

```
Router#
```

如果需要在 PC0 远程登录时既要输入用户名，又要输入口令进行验证，此时需要通过控制台对路由器做如下配置。

```
Router(config)#username tdp password 321
Router(config)#line vty 0 4
Router(config-line)#login local
```

再次验证通过 PC0 远程登录路由器对路由器进行配置的过程如下。

```
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open
Warning Don't configure my device, and if configured, you're going to be responsible
for the consequences!!!
    User Access Verification
    Username: tdp                          //输入用户名 tdp
    Password:                              //输入口令 321
    Router>en
    Password:                              //输入特权口令 123
    Router#
```

3.3.2　利用 Telnet 对交换机进行远程配置

利用 Telnet 对交换机进行配置结构图如图 3.11 所示。

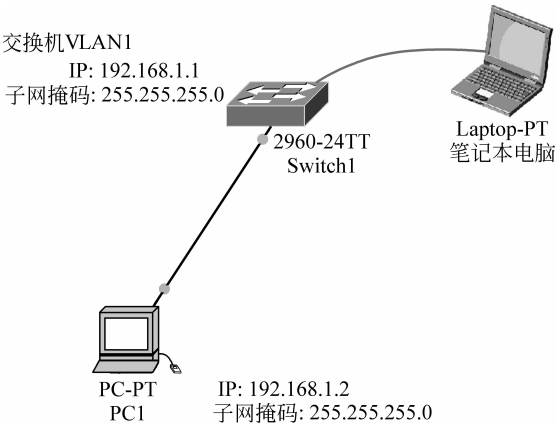

图 3.11　利用 Telnet 对交换机进行配置结构图

首先在笔记本电脑上利用交换机控制台 Console 口对交换机进行基本配置，包括配置交换机管理地址——VLAN1 地址。默认情况下，交换机的所有端口均属于 VLAN1，VLAN1 是交换机默认 VLAN，每个 VLAN 只有一个活动的管理地址，因此对交换机设置管理地址，首先选择 VLAN1 端口，俗称交换机虚拟端口(Switch Virtual Interface，SVI)。

配置交换机 VLAN1 网络地址参数，具体如下。

```
Switch#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Switch(config-if)#no shu
```

接下来为 Telnet 用户配置用户名和登录口令。

```
Switch(config)#line vty 0 4
Switch(config-line)#password 123          //设置远程登录访问密码
Switch(config-line)#login                 //要求口令验证,打开登录认证功能
Switch(config-line)#exit
Switch(config)#enable password 321        //设置使能口令
```

为 PC1 配置网络地址,如图 3.11 所示,IP 为 192.168.1.2,子网掩码为 255.255.255.0。通过计算机远程登录交换机过程如下。

```
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open
User Access Verification
Password:                                 //输入口令 123
Switch>enable
Password:                                 //输入使能口令 321
Switch#
```

如果同时需要利用用户名和密码进行登录验证,则需要进行如下配置。

```
Switch(config)#username tdp password 123    //设置登录用户名和口令
Switch(config)#line vty 0 4
Switch(config-line)#login local
```

通过计算机远程登录交换机过程如下。

```
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open
User Access Verification
Username: tdp
Password:                                 //输入口令 123
Switch>en
Password:                                 //输入使能口令 321
Switch#
```

3.4 利用 Web 对路由器进行配置

利用 Web 对路由器进行配置,需要完成如下基本操作。首先对路由器进行基本配置,具体配置过程如下。

(1) 在路由器配置模式下执行 ip http server 命令。

(2) 同在配置模式下,使用 ip http authentication 命令选择认证方式。

(3) 为路由器配置端口 IP 地址。

对计算机进行的相关操作如下。

(1) 在 IE 浏览器的地址栏中输入路由器端口 IP 并回车。

(2) 从 Web Console 里下载并安装 java plug-in 即可。另外,不是所有的路由器 iOS 都支持 Web 方式。

3.5　利用 Web 对交换机进行配置

利用 Web 对交换机进行配置,需要完成如下基本操作。首先对交换机进行基本配置,具体配置过程如下。

(1) 在交换机配置模式下执行 ip http server 命令。

(2) 同在配置模式下,使用 ip http authentication 命令选择认证方式。

(3) 为交换机配置管理 IP 地址。

对计算机进行相关操作如下。

(1) 在 IE 浏览器的地址栏中输入交换机管理 IP 并回车。

(2) 从 Web Console 里下载并安装 java plug-in 即可。另外,不是所有的交换机 iOS 都支持 Web 方式。

3.6　show 命令集

在网络设备配置过程中,经常需要查看相关配置信息、系统配置结果以及网络设备运行状态,利用 show 命令可以查看。下面是在网络设备配置过程中经常使用的 show 命令。

(1) show interfaces: 查看所有端口的详细信息。

(2) show interfaces fastEthernet 0/0: 查看端口 fastEthernet 0/0 的详细信息。

(3) show ip interface brief: 查看端口的简要信息。

(4) show version: 查看系统硬件的配置、软件版本号等。

(5) show running-config: 查看网络设备交换机或路由器当前正在运行的配置信息,包括设备名称、密码、端口配置情况等,位于网络设备的 RAM 中。

(6) show startup-config: 查看网络设备交换机或路由器保存在 NVRAM 中的配置信息,包括设备名称、密码、端口配置情况等。它在启动网络设备时载入 RAM,成为 running-config。

(7) show ip route: 查看路由表。

(8) show ip nat translations: 查看网络地址转换情况。

(9) show flash: 显示闪存的布局和内容信息。

(10) show cdp interface: 显示打开的 CDP 端口信息。

3.7　CDP

思科发现协议(Cisco Discovery Protocol,CDP)是由思科公司推出的一种私有的二层网络协议,它能够运行在大部分的思科设备上。通过运行 CDP,思科设备能够在与它们直

连的设备之间分享有关操作系统软件版本，以及 IP 地址、硬件平台等相关信息。

这个协议是用来发现邻居的，也是 Cisco 私有协议。它能发现邻居是因为包里面有 TTL 字段，在 CDP 包里这个字段为 1。当路由器或者交换机收到这个信息后，会把 TTL 值减 1。当 TTL 为零的时候，这个数据将不会再进行传递了，所以使用这个协议只能发现邻居。如图 3.12 所示，Switch1 只能发现 Router0，不能发现 Switch0 。具体命令“show cdp”后面的参数如下。

```
Router0#show cdp ?
entry         Information for specific neighbor entry
interface     CDP interface status and configuration
neighbors     CDP neighbor entries
<cr>
```

(1) show cdp neighbors：显示有关直连设备的信息，其中包括设备的主机名、接收数据包的端口、保持时间、邻居设备的性能、设备类型和连接的端口 ID。

(2) show cdp neighbors detail：显示邻居详细信息，包括直连设备的 IP 地址和 iOS 版本号。

(3) show cdp entry * 与 show cdp neighbors detail 相同。

(4) show cdp entry * protocols：显示直连邻居的 IP 地址。

(5) show cdp entry * version：显示直连邻居的 iOS 版本。

(6) show cdp traffic：显示设备发送和接收的 CDP 数据包。

(7) show cdp interface：显示每个端口使用的 CDP 信息，包括线路的封装类型、定时器和保持时间。

下面通过例子具体探讨 CDP 的作用。

CDP 要发挥作用，首先须保证网络连通性，图 3.12 所示网络，其连通性具体配置如下。

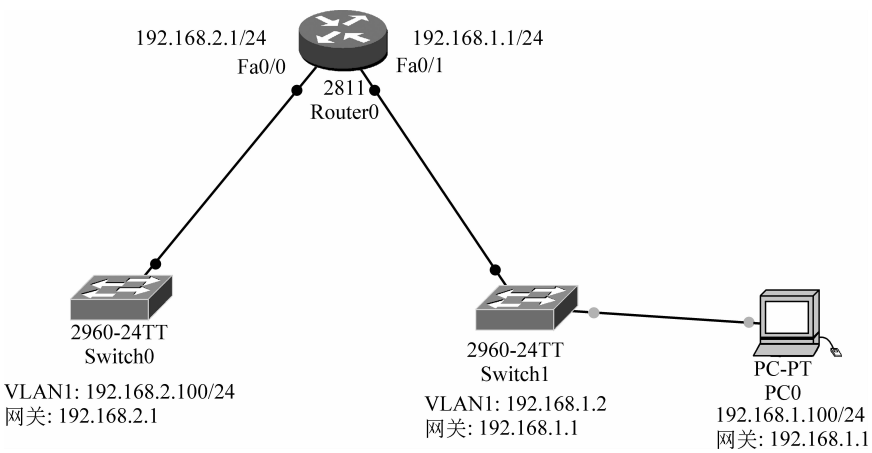

图 3.12　CDP 网络拓扑结构

首先对路由器 Router0 进行配置。

```
Router0(config)#interface fastEthernet 0/0                  //进入端口 fa0/0
Router0(config-if)#ip address 192.168.2.1 255.255.255.0     //配置 IP 地址
```

```
Router0(config-if)#no shu                                    //激活该端口
Router0(config-if)#exit                                      //退出
Router0(config)#interface fastEthernet 0/1                   //进入端口 fa0/1
Router0(config-if)#ip address 192.168.1.1 255.255.255.0      //配置 IP 地址
Router0(config-if)#no shu                                    //激活端口
```

其次对交换机 Switch0 进行配置。

```
Switch0(config)#interface vlan 1                            //进入交换机管理端口 vlan1
Switch0(config-if)#ip address 192.168.2.100 255.255.255.0 //配置 IP 地址
Switch0(config-if)#no shu                                    //激活
Switch0(config-if)#exit                                      //退出
Switch0(config)#ip default-gateway 192.168.2.1               //配置默认网关
```

最后对交换机 Switch1 进行配置。

```
Switch1(config)#interface vlan 1                             //进入管理端口 vlan1
Switch1(config-if)#ip address 192.168.1.2 255.255.255.0      //配置 IP 地址
Switch1(config-if)#no shu                                    //激活
Switch1(config-if)#exit                                      //退出
Switch1(config)#ip default-gateway 192.168.1.1               //配置默认网关
```

另外，将计算机 IP 地址配置为 192.168.1.100，子网掩码配置为 255.255.255.0，网关配置为 192.168.1.1，通过计算机 ping 交换机 Switch0 测试网络连通性，结果如下。

```
C:\>ping 192.168.2.100
Pinging 192.168.2.100 with 32 bytes of data:
Reply from 192.168.2.100: bytes=32 time<1ms TTL=254
Reply from 192.168.2.100: bytes=32 time<1ms TTL=254
Reply from 192.168.2.100: bytes=32 time<1ms TTL=254
Reply from 192.168.2.100: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.2.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C: \>
```

结果表明，计算机能够 ping 通交换机 Switch0，整个网络互联互通。接下来配置交换机和路由器，使它们能够远程登录。

首先配置交换机 Switch1，具体配置过程如下。

```
Switch1(config)#username t1 password 123                     //设置用户名和密码
Switch1(config)#enable password 321                          //配置使能密码
Switch1(config)#line vty 0 4
Switch1(config-line)#login local
Switch1(config-line)#exit
```

其次配置路由器 Router0，具体配置过程如下。

```
Router0(config)#username t2 password 1234                    //配置用户名密码
Router0(config)#line vty 0 4
Router0(config-line)#login local
Router0(config-line)#exit
Router0(config)#enable password 4321                         //配置使能口令
```

最后配置交换机 Switch0，具体配置过程如下。

```
Switch0(config)#username t3 password 12345                   //配置用户名密码
Switch0(config)#line vty 0 4
Switch0(config-line)#login local
Switch0(config-line)#exit
Switch0(config)#enable password 54321                        //配置使能口令
Switch0(config)#
```

利用 CDP 命令通过发现邻居，从而发现整个网络拓扑，具体操作过程如下。

首先在 PC0 上通过 Telnet 命令登录交换机 Switch1。

```
C:\>telnet 192.168.1.2
Trying 192.168.1.2 ...Open
User Access Verification
Username: t1
Password:
Switch1>en
Password:
Switch1#
```

通过在交换机 Switch1 上执行 cdp 命令，查看邻居设备情况，具体操作如下。

```
Switch1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID Local Intrface  Holdtme  Capability Platform  Port ID
Router0     Fas 0/1          139         R       C2800     Fas 0/1
Switch1#
```

结果显示，邻居设备 ID 号为 Router0，利用本地设备端口 fa0/1 与邻居设备 Router0 端口 fa0/1 相连，并且邻居设备型号为 C2800。

通过命令 show cdp entry 查看邻居设备详细信息，结果如下。

```
Switch1#show cdp entry *
Device ID: Router0
Entry address(es):
IP address : 192.168.1.1
Platform: cisco C2800, Capabilities: Router
Interface: FastEthernet0/1, Port ID (outgoing port): FastEthernet0/1
Holdtime: 156
Version:
```

```
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(15)T1,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team
advertisement version: 2
Duplex: full
Switch1#
```

可以发现邻居设备端口 fa0/1，其 IP 地址为 192.168.1.1。接着进一步通过 Telnet 登录到 Router0，利用 show cdp neighbors 发现设备 Router0 的邻居情况。

```
Switch1#telnet 192.168.1.1
Trying 192.168.1.1 ...Open
User Access Verification
Username: t2
Password:
Router0>en
Password:
Router0#
```

通过 show cdp neighbors 命令发现 Router0 的邻居情况，结果如下。

```
Router0#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID Local Intrface     Holdtime     Capability     Platform     Port ID
Switch0        Fas 0/0            138          S            2960       Fas 0/1
Switch1        Fas 0/1            129          S            2960       Fas 0/1
Router0#
```

通过 cdp 命令可以看到，路由器 Router0 的邻居设备有两个，分别为 Switch0 和 Switch1，其中交换机 Switch1 的情况刚才已经清楚了，Switch0 为路由器 Router0 连接的另一个设备，具体为：邻居设备的 ID 为 Switch0，其设备型号为 2960，本设备 Router0 的 fa0/0 与邻居设备的 fa0/1 相连。根据以上信息可以构建网络拓扑结构。

通过 show cdp entry 命令可以查看邻居设备的具体情况，结果如下。

```
Router0#show cdp entry *
Device ID: Switch0
Entry address(es):
IP address : 192.168.2.100
Platform: cisco 2960, Capabilities: Switch
Interface: FastEthernet0/0, Port ID (outgoing port): FastEthernet0/1
Holdtime: 151
Version :
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE
SOFTWARE (fc1)
```