中 北 大 学

网络设备与集成

实验指导书

内部资料

电子与计算机科学技术学院网络工程系 2009

目　录

第 3 章 交换机基础配置

3.1 交换机的基本配置

本节包括交换机基本配置、交换机远程配置和利用 TFTP 管理交换机的配置。至于交换机的工作原理、结构等内容在这里不复赘言。

3.1.1 交换机配置的基础知识

1．网管型交换机

交换机的类型有多种方法，如果按交换机是否支持网络管理功能，可以将交换机分为“网管型”和“非网管型”两大类。网管型交换机能够提供了基于终端控制口（Console）、基于 Web 页面以及支持 Telnet 远程登录网络等多种网络管理方式，因此网络管理人员可以对该交换机的工作状态、网络运行状况进行全局地性管理，使所有的网络资源处于良好的状态。图 3.1 为网管型交换机产品外观图。

图 3.1 网管型交换机外观图

网管型交换机支持简单网络管理协议 SNMP，SNMP 协议由一整套简单的网络通信规范组成，可以完成所有基本的网络管理任务，对网络资源的需求量少，具备一些安全机制。

而所谓非网管型交换机是指在使用中几乎不需任何配置，纯属“傻瓜”型，像集线器一样，接上电源插好网线就可以正常工作了。

2．网管型交换机的配置

网管型交换机的配置过程比较复杂，具体的配置方法会因不同应用、不同品牌、不同系列的交换机而有所不同。本节仅仅介绍交换机的基本配置方法。通常网管型交换机的配置主要用两种方法：一种是本地配置，另一种是远程网络配置，但后者只有在前一种配置成功后才可进行。

本地配置的任务主要包括两点：

其一是，在计算机上安装 windows xp 自带的“超级终端”（Hyper Terminal）组件， 建立一个新的超级终端连接，配置数据传输率并给以命名。那么“超级终端”的功能是什么呢？超级终端技术是利用服务器的运算能力，支持众多终端同时进行工作的一种计算模式。终端机无需进行任何运算，只需要通过 PC 机、Modem 和网络，将键盘、鼠标等的输入传送给服务器，同时接受服务器传回的显示信号，显示在屏幕上即可。在终端方式下，全部运算都集中在服务器上进行。其最大的优点就是时效性非常强，只受 Modem 速度影响而不受网络速度的控制，不受地域限制，不用交付网费。

其二是，为交换机配置管理 IP 地址，这主要是为以后通过 telnet 等方式进行远程配置而做准备的。下面介绍交换机基本配置的主要内容。

（1）基本配置的物理连接

由于笔记本电脑携带方便，所以经常用来配置交换机，当然也可以采用台式机。其连接如图 3.2 所示：利用一条反转线（一端是 EIA/TIA 568A 或 568B，而另一端是其的反序），将计算机的 COM 端口与交换机的 Console 端口连接。

图 3.2 本地配置的连接

Console 端口是专门用于对交换机进行配置和管理的端口，由于其他配置方式都需要借助于交换机的 IP 地址、域名或设备名称才可以实现，而新购买的交换机没有内置这些参数，所以，通过 Console 端口连接并配置交换机，是配置交换机第一步，也是网络管理员必须掌握的管理和配置方式。

Console 端口的位置，有的位于前面板，有的则位于后面板，但在其上方或侧方都会有“CONSOLE”字样作为标识，是容易找到的。如图 3.3 所示。

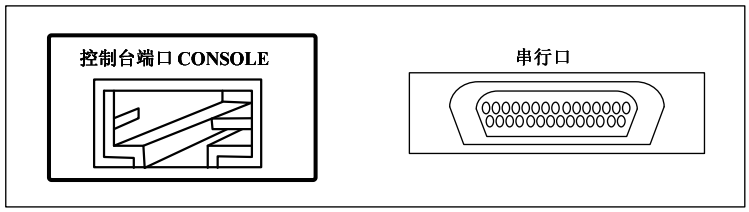


图 3.3 Console 端口的位置

绝大多数 Console 端口都采用 RJ－45 端口，但也有少数采用 DB－9 或 DB－25 端口，而且都需要通过专门的 Console 线连接至配置所用计算机的指定端口。

（2）配置 windows 自带的“超级终端”（Hyper Terminal）组件

首先打开计算机和交换机电源，检查计算机是否安装有“超级终端”组件。如果在“附件”中没有发现该组件，可通过“添加／删除程序”的方式添加该 Windows 组件。

“超级终端”安装好后就可以与交换机进行通信了，在使用超级终端建立与交换机的通信之前，必须先对超级终端进行必要的设置。现以 Windows xp 系统为例，配置步骤如下：

首先单击“开始”→“程序”→“附件”→“通信” →单击“超级终端”，弹出如图 3.4 所示的 Hyper Terminal 界面：

图 3.4 连接说明对话框

而后在“名称”文本框中键入一个自定的、便于识别的超级终端连接名称，如键入“red”，您还可以为这个连接项选择一个自己喜欢的图标，然后单击“确定”，弹出如图 3.5 所示的“连接到”对话框。

图 3.5 “连接到”对话框

图 3.6 COM1 对话框

在“连接时使用”下拉列表框中选择与交换机相连的计算机的串口。单击“确定”按钮，弹出如图 3.6 所示的 COM1 对话框。

在“每秒位数”下拉列表框中选择“9600”。数据流控制选择“无”其他选项全采用默认值。然后单击“确定”，如果通信正常，就会显示交换机的初始配置情况，并显示交换机的当前模式。

3．交换机所使用的 CLI

在交换机的首次使用时只能使用串口方式连接交换机，称为带外（outband）管理方式。在进行了相关配置后，可以通过 telnet 虚拟终端方式连接和管理交换机。

交换机所使用的软件系统称为网间操作系统（Inter-network Operating System,IOS）。通常称为“命令行界面”（Command－Line Interface，CLI），它是一个基于命令行的软件系统模式，在交换机、路由器、防火墙都有。这种模式实际上就是一系列相关命令，但是，CLI 与 DOS 命令不同，CLI 可以对命令和参数缩写，只要它包含的字符足以与其他当前所用的命令和参数能区别开来即可。

在软件配置方面思科、华为、锐捷等公司的产品所用的配置命令基本可以兼容。交换机的配置和管理可以通过多种方式实现，既可以使用命令行和菜单（Menu），也可以使用图形界面的 Web 浏览器或专门的网管软件。然而，命令行方式的功能更强大，虽然难度也较大，但仍然是最主要的配置模式。

（1）IOS 的命令模式

CLI 命令的模式将命令划分成若干独立的集合，例如：interface fastEthernet number 命令就只能在全局配置模式下执行。以下是支持的主要命令模式：

- User EXEC 模式（用户模式）；
- Privileged EXEC 模式（特权模式）；
- Global configuration 模式（全局配置模式）；
- Interface configuration 模式（接口配置模式）；
- Config-vlan 模式（VLAN 配置模式）；

当在不同的模式下，CLI 界面中会出现不同的提示符。表 3-1 列出了命令的模式、如何访问每个模式、模式的提示符、如何离开模式。

这里假定交换机的名字为缺省的“switch”。

表 3.1 命令模式概要

命令模式	访问方法	提示符	离开或访问下一模式
User EXEC 用户模式	访问交换机时首先进入该模式	Switch>	输入 exit 命令离开该模式； 要进入特权模式，输入 enable 命令。
Privileged EXEC 特权模式	在用户模式下，使用 enable 命令进入该模式	Switch#	返回到用户模式，输入 disable 命令； 进入全局配置模式，输入 configure 命令。
Global configuration 全局配置模式	在特权模式下，使用 configure 命令进入该模式	Switch(config)#	返回到特权模式，输入 exit 命令或 end 命令，或者键入 Ctrl+Z 组合键； 进入接口配置模式，输入 interface 命令； 要进入 VLAN 配置模式，输入 vlan vlan_id 命令。
Interface configuration 接口配置模式	在全局配置模式下，使用 interface 命令进入该模式	Switch(config-if)#	返回到特权模式，输入 end 命令，或键入 Ctrl+Z 组合键； 返回到全局配置模式，输入 exit 命令； 在 interface 命令中必须指明要进入哪一个接口配置子模式。
Config-vlan VLAN 配置模式	在全局配置模式下，使用 vlan vlan_id 命令进入该模式	Switch(config-vlan)#	返回到特权模式，输入 end 命令，或键入 Ctrl+Z 组合键； 返回到全局配置模式，输入 exit 命令。

（2）命令模式的应用和缩写

任何 IOS 命令只能在各自的命令模式下才能执行，因此，在执行某个命令之前，必须先进入相应的命令模式。例如“interface type_number”命令只能在全局模式下执行，而“duplex full-flow-control”命令只能在接口配置模式下执行。

但是，在交换机 CLI 命令中的帮助命令“？”，可以在任何命令模式下应用，只要键入“？”，即可显示该命令模式下所有可用的命令及其用途，也可以在一个命令和参数后面加“？”，以寻求相关的帮助。

帮助命令用途很多，例如：

在“＃”提示符下键入“？”并回车，即可显示在特权模式下有哪些可用的命令；

“show ？”并回车，可以查看“Show”命令的用法；

在特权模式下键入“c？”，系统将显示以“c”开头的所有命令。也就是说，“？”具有局部关键字查找功能。如果只记得某个命令的前几个字符，就可以使用“？”，让系统列出所有以该字符或字符串开头的命令。

IOS 命令均支持缩写，例如：

可将“show configure”缩写为“sh conf”；

把“interface type_number”缩写成“int ty-num”等等。

（3）使用历史命令

为方便操作，CLI 系统提供了用户输入的命令的记录。该特性在重新输入长而且复杂的命令时将十分有用。

从历史命令记录重新调用输入过的命令，可执行表 3.2 中的操作：

表 3.2 调用历史命令记录

操作	结果
Ctrl-P或上方向键	在历史命令表中浏览前一条命令。从最近的一条记录开始，重复使用该操作可以查询更早的记录。
Ctrl-N或下方向键	在使用了Ctrl-P或上方向键操作之后，使用该操作在历史命令表中回到更近的一条命令。重复使用该操作可以查询更近的记录。

（4）理解 CLI 的提示信息

用户在使用 CLI 时，设备会提供必要的提示信息，下面列出了用户在使用 CLI 管理交换机时可能遇到的一些常见的错误提示信息：

• 用户没有输入足够的字符，交换机无法识别唯一的命令：

% Ambiguous command: "show c"

遇到这种情况时，请重新输入命令，紧接着发生歧义的单词输入一个问号，可能的关键字将被显示出来。

• 用户没有输入该命令的必需的关键字或者变量参数：

% Incomplete command.

此时可以重新输入命令，输入空格再输入一个问号，可能输入的关键字或者变量参数将被显示出来。

• 用户输入命令错误：

% Invalid input detected at‘^’marker.

符号（^）指明产生错误的单词的位置，在所在地命令模式提示符下输入一个问号，该模式允许的命令的关键字将被显示出来。

（5）编辑快捷键

表 3.3 列出了 CLI 下的编辑快捷键：

表 3.3 CLI 编辑快捷键

功能	快捷键	说明
在编辑行内移动光标	左方向键或Ctrl+B	光标移到左边一个字符。
	右方向键或Ctrl+F	光标移到右边一个字符。
	Ctrl+A	光标移到命令行的首部。
	Ctrl+E	光标移到命令行的尾部。
删除输入的字符	Backspace键	删除光标左边的一个字符
	Delete 键	删除光标所在的字符
输出时屏幕滚动一行或一页	Return 键	在显示内容时用回车键将输出的内容向上滚动一行，显示下一行的内容，仅在输出内容未结束时使用。
	Space 键	在显示内容时用空格键将输出的内容向上滚动一页，显示下一页内容，仅在输出内容未结束时使用。

（6）命令行滑动窗口

用户可以使用编辑功能中的滑动窗口特性，来编辑超过单行宽度的命令，使命令行的长度得以延伸。当编辑的光标接近右边框时，整个命令行会整体向左移动 20 个字符，但是仍然可以使光标回到前面的字符或者回到命令行的首部。

如表 3.3 所示，编辑命令行时光标向左回退一个字符可以使用左方向键或 Ctrl+B，回到行首可以使用 Ctrl+A；编辑命令行时光标向右前进一个字符可以使用右方向键或 Ctrl+F，移动到行尾可以使用 Ctrl+E。

例如配置模式的命令 mac-address-table static 的输入可能超过一个屏幕的宽度（默认的终端行宽是 80 个字符）。当光标第一次接近行尾时，整个命令行整体向左移动 20 个字符。命令行前部被隐藏的部分被符号（$）代替。每次接近右边界时都会向左移动 20 个字符长度。

Switch(config)# mac-address-table static 00d0.f800.0c0c vlan 1 interface

Switch(config)# $tatic 00d0.f800.0c0c vlan 1 interface fastEthernet

Switch(config)# $tatic 00d0.f800.0c0c vlan 1 interface fastEthernet 0/1

可以使用 Ctrl-A 快捷键回到命令行的首部。这时命令行尾部被隐藏的部分将被符号（$）代替：

Switch(config)# mac-address-table static 00d0.f800.0c0c vlan 1 interface $

使用命令行滑动窗口结合历史命令的功能，可以重复调用复杂的命令。

3.1.2 交换机的基础配置实验

1．CLI 命令模式

前文已经介绍了交换机的 IOS，这里具体地了解一下 CLI 中这些模式的差别：

（1）用户模式

当用户访问交换机时，自动进入用户模式。在用户模式下的用户级别称为普通用户级，在特权级别下的用户级别称为特权用户级。普通用户级别能够使用的 Exec 命令（即可执行命令）只是特权用户级别 Exec 命令的一个子集。在这种情况下，用户通常只能进行一些简单的测试操作，或者查看系统的一些信息。

用户模式所能执行的 Exec 命令由设备提供的功能决定，要查看全部命令列表，在命令模式提示符下键入查询符号（?）：

Switch> ?

（2）特权模式

因为特权模式的命令管理着许多设备的运行参数，必须使用口令保护来防止非授权使用，所以从用户模式进入特权模式必须输入正确的口令。特权模式的命令集包含了用户模式的全部命令。如果系统管理员设置了特权级别的口令，则进入特权模式之前将提示需要输入口令，输入的口令在屏幕上不会显示。

特权模式的提示符为设备的名称后紧跟‘#’符号，如：Switch#

在用户模式下使用 enable 命令进入特权模式：

Switch> enable

Switch#

特权模式所能执行的 Exec 命令由设备提供的功能决定，要查看全部命令列表，在命令模式提示符下键入查询符号（?）：

Switch# ?

要返回到用户模式，输入 disable 命令。

（3）全局配置模式

全局配置模式提供了从整体上对交换机特性产生影响的配置命令，在特权模式下，使用 configure 命令进入该模式。下面是使用 configure 命令进入该模式的例子：

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

全局配置模式所能执行的配置命令由设备提供的管理功能决定，要查看全部命令列表，在命令模式提示符下键入查询符号（?）：

Switch(config)# ?

要返回到特权模式，输入 exit 命令或 end 命令，或者键入 Ctrl+Z 组合键。

（4）接口配置模式

接口配置模式只影响具体的接口，进入接口配置模式的命令必须指明接口的类型。 使用 interface type number 命令进入接口配置模式，命令的提示符改变为如下形式：

Switch(config-if)#

接口配置模式所能执行的配置命令由设备提供的接口管理功能决定，要查看全部命令列表，在命令模式提示符下键入查询符号（?）：

Switch(config-if)# ?

要返回到特权模式，输入 end 命令，或键入 Ctrl+Z 组合键；要返回到全局配置模式，输入 exit 命令。

（5）VLAN 配置模式

该模式用来配置具体 VLAN 相关的特性，用 VLAN 的 ID 来区分不同的 VLAN。

在全局配置模式下，使用 vlan vlan_id 命令进入该模式。

Switch(config)# vlan 2000

Switch(config-vlan)#

VLAN 配置模式所能执行的配置命令由设备提供的 VLAN 管理功能决定，要查看全部命令列表，在命令模式提示符下键入查询符号（?）：

Switch(config-vlan)# ?

要返回到特权模式，输入 end 命令或键入 Ctrl+Z 组合键；要返回到全局配置模式，输入 exit 命令。

2．交换机的远程配置

当交换机已经完成了基本配置，就可以利用交换机的普通端口，通过 IP 地址与交换机进行远程配置通信，不过要注意，只有是网管型的交换机才具有这种管理功能。另外，如果交换机配置了堆叠，由于它们是一个整体，只有一台具有网管能力，配置好这一台也就配置好堆叠型交换机了。

远程配置有 Telnet/SSH 或 Web 浏览器两种方式，下面先介绍常用的 Telnet 方式，SSH 将在本书第七章关于交换机安全管理的内容中说明。

Telnet 是一种远程访问协议，可用来登录到远程计算机、网络设备或专用 TCP／IP 网络。Windows 98 以上版本、UNIX／Linux 等系统中都内置有 Telnet 客户端程序，可以用它来实现与远程交换机的通信。

在使用 Telnet 连接至交换机前，应做好以下准备工作：

- 在用于配置和管理的计算机中安装有 TCP／IP 协议，并配置好了 IP 地址；
- 被管理的交换机已经配置好 IP 地址，否则，必须通过 Console 端口进行设置；
- 在被管理的交换机上建立了具有管理权限的用户帐户，即配置了 TELNET 登陆密码。

Telnet 命令的一般格式为：

telnet ［*Hostname* ［*port*］］

这里要注意的是“Hostname”包括了交换机的名称，但前提是存在相应的名字解析，因而我们一般使用为交换机管理所配置的 IP 地址。格式后面的“Port”一般是不需要输入的，它是用来设定 Telnet 通信所用的端口的，一般来说 Telnet 通信端口，在 TCP／IP 协议中规定为 23 号端口，最好不要更改。

当交换机的 Telnet 登陆配置完成后，在计算机上运行 Telnet 客户端程序，即可登录至远程交换机，进入配置界面的步骤为：单击“开始”→“运行”→在对话框中输入登录 telnet 172.16.0.1（交换机 IP），单击“确定”回车键，建立与远程交换机的连接。

图 3.7 所示为计算机通过 Telnet 与 S2126 交换机建立连接时显示的界面，输入正确的密码即可进入到该交换机的用户模式下。

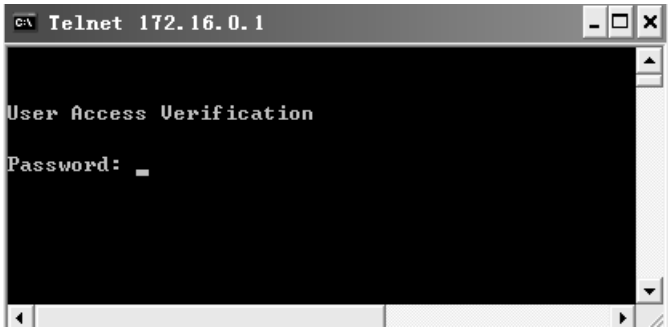


图 3.7 TELNET 连接界面

3．实验环境与说明

（1）实验目的

掌握交换机的本地配置方法和 CLI 的模式操作，配置交换机支持 Telnet，实现远程管理。

（2）实验设备和连接

实验设备和连接图如图 3.8 所示，一台锐捷 S2126G/S3550 交换机连接 1 台 PC 机，交换机命名为 Switch。

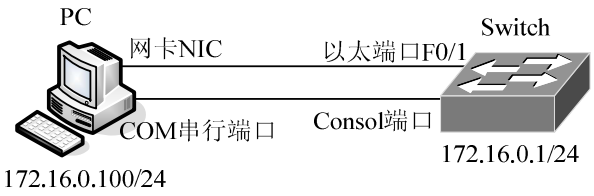


图 3.8 交换机基本配置实验

（3）实验分组

每四名同学为一组，一人一台交换机（S2126 或 S3550），每人各自独立完成实验。

4．实验步骤

步骤 1：按照如图 3.8 所示连接好设备，由于实验室 RACK 实验台设备的配置是通过 RCMS 实现管理的，因此学生不需要做 Console 连线，只需登陆 RCMS 即可。为验证 TELNET 配置，将配线架学生机 2＃网卡和所选择的交换机 F0/1 端口对应接口连接。

步骤 2：在交换机上配置 IP 地址。键入下述命令：

```
switch>enable                                    ！从用户模式进入特权模式
switch # configure terminal                      ！从特权模式进入全局配置模式
switch (config)# hostname SwitchA                ！设置交换机名称为为“SwitchA”
SwitchA (config)#
```

步骤 3：配置交换机远程登陆密码

```
SwitchA (config)# enable secret level 1 0 star     ！将交换机远程登陆密码配置为“star”
```

步骤 4：配置交换机特权模式口令

```
SwitchA (config)# enable secret level 15 0 star    ！将交换机特权模式口令配置为“star”
```

说明：在实验室中设置特权密码一律为 star，凡擅自更改将为实验室管理工作造成麻烦，引起的后果自负（诸如取消实验资格，实验成绩记零分），请同学们审慎对待。

步骤 5：为交换机分配管理 IP 地址

```
SwitchA (config)# interface vlan 1                 ！进入交换机管理接口配置模式
SwitchA (config-if)# ip address 172.16.0.1  255.255.255.0    ！配置交换机的 IP 地址
SwitchA (config-if)# no shutdown                   ！启用端口
```

说明：为 VLAN 1 的管理接口分配 IP 地址（表示通过 VLAN 1 来管理交换机），设置交换机的 IP 地址为 172.16.0.1，对应的子网掩码为 255.255.255.0

验证交换机的配置：

```
SwitchA # show ip interface        ！验证交换机 IP 地址已经配置，管理端口已经开启
Interface                  : VL1                    ！接口
Description                : Vlan 1                 ！描述
OperStatus                 : up                     ！操作状态已经开启
ManagementStatus           : Enable                 ！管理状态为可能
Primary Internet Address   :172.16.0.1/24           ！主 IP 地址
Broadcast address          : 255.255.255.255        ！广播地址
Physaddress                : 00d0.f8fe .1e48        ！物理地址
```

步骤 6：验证计算机可以经由 telnet 远程登录到交换机

将 PC 机的 2＃网卡配置为与交换机相同网段的 IP 地址，例如图 3.8 所示的 172.16.0.100。在命令行模式下（开始－运行－CMD）执行如下操作：

```
C:\> telnet 172.16.0.1
```

屏幕显示图 3.7 所示 TELNET 连接界面，输入登陆密码 star，进入特权模式，输入特权密码 star，操作如图 3.9 所示。

图 3.9 Telnet 操作界面示意

步骤 7：在超级终端或 Telnet 方式下，显示交换机 MAC 地址表的记录。

```
SwitchA #show mac-address-table
Vlan            MAC Address              Type        Interface
---------------------------------------- -------- -------------------------
1               00e0.4c10.71aa           DYNAMIC     Fa0/1
```

如果地址表为空，则在 PC 上开一命令行窗口，运行命令：c:\>ping 172.16.0.1，能 ping 通则在交换机上执行 show mac-address-table 可查看到 PC 的 MAC 地址。请记录你所看到的 MAC 地址，填写表 3.4。

表 3.4 交换机 MAC 地址表记录

VLAN	MAC Address	Type	Interface

对比 PC 机的 MAC 地址，PC 的 MAC 地址可以在命令行下输入：ipconfig /all 查看。结合你所学到的知识，说明交换机工作的基本原理（学习－过滤－转发）：

步骤 8：修改交换机 MAC 地址的老化时间

```
SwitchA (config)# mac-address-table aging-time 10
！将交换机 MAC 地址老化时间设置为 10 秒，默认为 300 秒。
```

注意：S3550/3760 设置 aging-time 范围 10－1000000，S2126/S2150G 的为 300－1000000。

```
SwitchA (config)# end                          ！从交换机全局配置模式返回至特权模式
SwitchA# show mac-address-table                ！显示交换机 MAC 地址表的记录
```

思考：在 aging-time 时间内和时间外分别执行 show mac-address-table，看到的结果有何不同？请分析 aging-time 的功能是什么？交换机 MAC 地址表为什么要设置 aging-time？

步骤 9：保存交换机配置

交换机的当前配置可以使用 show running-config 查看：

```
SwitchA# show running-config
```

验证结果显示：

```
System software version : 1.61(2) Build Aug 31 2005 Release
Building configuration...
Current configuration : 308 bytes
!
version 1.0
!
hostname SwitchA              ！交换机名称
vlan 1
!
enable secret level 1 5 $2,1u_;C3&-8U0<D4'.tj9=GQ+/7R:>H          ！远程登陆密码
enable secret level 15 5 $2H.Y*T73C,tZ[V/4D+S(\W&QG1X)sv'      ！特权模式密码
!
interface vlan 1
 no shutdown                  ！交换机处于启动状态，缺省状态为关闭 shutdown
 ip address 172.16.0.1 255.255.0.0          ！交换机的 IP 地址
!
end
```

交换机的当前配置在 RAM 当中，交换机启动时载入记录在 FLASH 中的 config.text 配置文件，因此，当交换机配置更改后应当保存配置。保存配置的命令如下：

```
SwitchA# copy running-config startup-config  或 SwitchA# write memory
```

执行过程如下：

```
SwitchA# copy running-config startup-config   ！如果特权密码设置不是 star，请不要保存
Building configuration...
[OK]
SwitchA#
```

步骤 10：在交换机特权模式下，分别执行下列检测命令：

```
show interface fastethernet 0/1              ！该命令查看接口设置和统计信息
show ip interface                            ！该命令显示三层 IP 接口的各个属性
show running-config                          ！该命令显示当前的全部配置信息
show mac-address-table                       ！该命令显示设备 MAC 地址表（交换表）
```

仔细阅读这些命令的结果，思考设备所显示的相关信息。

3.1.3 利用 TFTP 服务器备份和恢复交换机配置实验

网管型交换机除了提供基本的设备配置外，根据设备的支持和具体需要往往还要配置 VLAN、STP、堆叠、端口聚合、端口镜像和端口安全等，三层交换机则可能有更多配置。

前面我们已经知道了锐捷交换机的配置文件 config.text 记录在设备 FLASH 中，如果某台交换机的配置文件由于误操作或意外原因被破坏了，则可能给网络管理造成很大的麻烦。

在这种情况下，可以通过 TFTP 服务器中的备份文件进行恢复，这是网络管理员的职责，所以应当具备这个能力。

1．TFTP 服务器

简单文件传输协议（Trivial File Transfer Protocol，TFTP）是 TCP/IP 的应用层协议。它是一个很小且易于实现的文件传送协议。虽然 TFTP 也使用客户服务器方式，但是由于使用 UDP 数据报，因此 TFTP 需要有自己的差错改正措施。与 FTP 相比，TFTP 只支持文件传送而不支持交互，没有列目录的功能，也不能对用户进行身份鉴别。

实验中，我们使用锐捷提供的 Trivial FTP Server 来实现 TFTP 服务器，该软件可以在 http://www.ruijie.com.cn 下载。执行该软件的主界面如图 3.10 所示。

图 3.10 Trivial FTP Server 窗体界面

Trivial FTP Server 几乎不需要配置，启动该软件后，PC 机就成为一台 TFTP 服务器。唯一可以配置的是用户可以点击窗口中的按钮打开目录对话框，更改服务器主目录，如果不更改的话，Trivial FTP Server 的执行文件所在路径将成为服务器主目录。任何 TFTP 连接和文件操作都将显示在主窗体的状态界面中。

2．配置文件的复制命令

在交换机 IOS 中，从源向目的复制文件，在特权模式下使用 copy 命令。

copy 命令的格式如下：

copy *source-url destination-url*

其中，source-url 表示需要被复制的源文件的别名或 URL，destination-url 表示需要复制的目的文件的别名或 URL。表 3.5 列举了在锐捷交换机中可以使用的 URL 参数。

表 3.5 URL 参数

关键字	源或目的
running-config	表示正在运行的当前配置
xmodem	该前缀表示文件通过 xmodem 方式传输
tftp:	该前缀表示文件通过 tftp 方式传输
flash:	该前缀表示交换机文件系统
startup-config	表示当前正在运行的配置文件，是文件名为 config.text 文件的别名

3．实验环境与说明

（1）实验目的

掌握通过 TFTP 服务器备份和还原交换机配置的方法。

（2）实验设备和连接

实验设备和连接图与 3.1.2 交换机的基础配置实验相同，参见图 3.8。

（3）实验分组

每四名同学为一组，一人一台交换机（S2126 或 S3550），每人各自独立完成实验。

4．实验步骤

步骤 1：在交换机上完成 3.1.2 交换机的基础配置实验步骤 1 至步骤 5，保存配置；配置 PC 机 IP 地址为 172.16.0.100，运行 Trivial FTP Server。

步骤 2：验证交换机与 TFTP 服务器的连通性

SwitchA# ping 172.16.0.100　　！验证交换机与 TFTP 服务器的连通性

Sending 5,100 byte ICMP Echos to 172.16.0.10

Timeout is 2000 milliswconds　　！超时为 2000ms

!!!!!

Success rate is 100 percent (5/5)

Minimum=1ms, Maxmum=2ms, Average=1ms

注意 PC 机使用 Windows XP 系统时，应关闭系统防火墙。

步骤 3：备份交换机的配置：

SwitchA# copy startup-config tftp:　　！将交换机的配置备份到 TFTP 服务器

Address of remote host [ ] 172.16.0.100　　！指定 TFTP 服务器的 IP 地址

Destination filename [config-text]?　　！提示选择要保存的文件的名称

%Success: Transmission success, file length 302　　！传输成功，文件长 302 字节

下面验证已经保存的配置文件：

在 TFTP 服务器上打开配置文件，系统路径下的 config.text，显示配置文件内容。将其中 enable secret level 15 5 $2H.Y*T73C,tZ[V/4D+S(\W&QG1X)sv' 行删除并保存。

步骤 4：将 TFTP 服务器保存的配置加载到交换机：

SwitchA# copy tftp: startup-config　　！加载保存的配置到交换机的初始文件中

Source filename [ ]? config.text　　！提示键入源文件名

Address of remote host [] 172.16.0.10　　！这是 TFTP 服务器的 IP 地址

%Success :Transmission success, file length 244

下面验证交换机已经更新为新的配置：

SwitchA# show configure　　！显示交换机的配置文件，相当于 startup-config

对比 show running-config 的差别，二者有何区别？

步骤 5：重新启动交换机，使新配置生效

SwitchA# reload　　！重新启动交换机

System configuration has been modified.Save? [yes/no]

　　！系统已经更新，存储吗？选 no 即可

Proceed with reload? [confirm]

待交换机重启后，进入特权模式，与重启前相比，操作上有何区别？

3.2 虚拟局域网 VLAN

本节介绍虚拟局域网 VLAN 的基本配置方法、跨交换机 VLAN 的实现、基于三层交换的 VLAN 连通以及交换机端口聚合的有关配置。其中涉及到的有关协议和应用技术在本节中会结合实验要求作出具体说明。

3.2.1 VLAN 实现交换机端口隔离实验

交换机可以连接多台计算机，无论是在企业网或者园区网中，都可以将一些计算机按交

换机端口划分为不同的 VLAN，划归不同 VLAN 的计算机可以实现相互隔离。

1．虚拟局域网 VLAN 简介

虚拟局域网 VLAN 是通过将局域网内设备逻辑地而不是物理地划分成一个个网段的技术。这里所说的网段仅仅是逻辑网段的概念，而不是真正的物理网段。可以将 VLAN 理解为是在物理网络上通过设备配置逻辑地划分出来的逻辑网络，相当于 OSI 参考模型的第二层的广播域。由于实现了广播域分隔，VLAN 可以将广播风暴控制在一个 VLAN 内部，划分 VLAN 后，随着广播域的缩小，网络中广播包消耗的带宽所占的比例大大降低，网络性能得到显著提高。不同的 VLAN 间的数据传输是通过第三层（网络层）的路由来实现的，因此使用 VLAN 技术，结合数据链路层和网络层的交换设备可搭建安全可靠的网络。同时，由于 VLAN 是逻辑的而不是物理的，因此在规划网络时可以避免地理位置的限制。

如上所述，VLAN 具有控制网络广播、提高网络性能；分隔网段、确保网络安全；简化网络管理、提高组网灵活性的功能。

目前业界公认的 VLAN 划分方法有如下几种：

- 基于端口的 VLAN（Port-Based）
- 基于协议的 VLAN（Protocol-Based）
- 基于 MAC 层分组的 VLAN（MAC-Layer Grouping）
- 基于网络层分组的 VLAN（Network-Layer Grouping）
- 基于 IP 组播分组的 VLAN（IP Multicast Grouping）
- 基于策略的 VLAN（Policy-Based）

其中基于端口的静态 VLAN 是划分虚拟局域网最简单也是最有效的方法，它实际上是某些交换机端口的集合，网络管理员只需要管理和配置交换机端口，而不管交换机端口连接什么设备。这种划分 VLAN 的方法是根据以太网交换机的端口来划分的，是目前业界定义 VLAN 最广泛的方法，IEEE802.1Q 规定了这种划分 VLAN 的国际标准。

2．VLAN 的基本配置命令

基于端口的 VLAN 在实现上包括两个步骤，首先启用 VLAN（用 VLAN ID 标识），而后将交换机端口指定到相应 VLAN 下。配置命名如下：

（1）vlan 命令

语法格式为：vlan *vlan-id*

该命令执行于全局配置模式下，是进入 VLAN 配置模式的导航命令。使用该命令的 no 选项可以删除 VLAN：no vlan *vlan-id*

注意：缺省的 VLAN（VLAN 1）不允许删除。

例如启用 VLAN 10，执行如下：

```
Switch(config)#vlan 10
Switch(config-vlan)#
```

（2）switchport access 命令

语法格式为：

switchport access vlan *vlan-id*

no switchport access vlan

使用该命令将一个端口设置为 statics accessport，并将它指派为一个 VLAN 的成员端口。使用该命令的 no 选项将该端口指派到缺省的 VLAN 中。switch port 缺省模式为 access，缺省的 VLAN 为 VLAN 1。

如果输入的是一个新的 VLAN ID，则交换机会创建一个 VLAN，并将该端口设置为该 VLAN 的成员。如果输入的是已经存在的 VLAN ID，则增加 VLAN 的成员端口。

例如将交换机 F0/5 端口指定到 VLAN 10 的配置为：

Switch(config)# interface fastEthernet 0/5

Switch(config-if)# switchport access vlan 10

3．实验环境与说明

（1）实验目的

掌握交换机的静态 VLAN（基于交换机端口）的配置方法，了解 VLAN 的基本功能。

（2）实验设备和连接

实验设备和连接图如图 3.11 所示，一台锐捷 S2126G 交换机连接 2 台 PC 机。

图 3.11 交换机端口隔离实验

（3）实验分组

每四名同学为一组，其中每两人一小组，每小组各自独立完成实验。

4．实验步骤

步骤 1：按照如图 3.11 所示连接好设备，将配线架学生机 2＃网卡和所选择的交换机 F0/1、F0/2 端口对应接口连接。例如在配线架上连接 N1－S7F1、N2－S7F2（将第一和第二台学生机分别连接实验台七号设备 S2126 的 F0/1 和 F0/2 端口）。

进入交换机配置。

步骤 2：首先划分 VLAN 创建 VLAN10 和 VLAN20

```
S2126G# configure terminal                    ！进入交换机全局配置模式
S2126G(config)# vlan 10                       ！创建 vlan 10
S2126G(config-vlan)# name test10              ！将 Vlan 10 命名为 test10
S2126G(config-vlan)# exit                     ！返回交换机全局配置模式
S2126G(config)# vlan 20                       ！创建 vlan 20
S2126G(config-vlan)# name test20              ！将 Vlan 20 命名为 test20
```

步骤 3：将交换机端口划分至 VLAN

```
S2126G(config)# interface fastethernet 0/1    ！进入 F0/1 的接口配置模式
S2126G(config-if)# switch access vlan 10      ！将 F0/1 端口加入 vlan 10 中
S2126G(config-if)# interface fastethernet 0/2 ！进入 F0/2 的接口配置模式
S2126G(config-if)# switch access vlan 20      ！将 F0/2 端口加入 vlan 20 中
```

步骤 4：VLAN 配置验证

```
S2126# show vlan                    ！该命令显示 VLAN 的成员端口等信息
VLAN Name                              Status      Ports
---- -------------------------------- --------- -------------------------------
1    default                           active    Fa0/3 ,Fa0/4 ,Fa0/5
                                                 Fa0/6 ,Fa0/7 ,Fa0/8
                                                 Fa0/9 ,Fa0/10,Fa0/11
                                                 Fa0/12,Fa0/13,Fa0/14
                                                 Fa0/15,Fa0/16,Fa0/17
                                                 Fa0/18,Fa0/19,Fa0/20
                                                 Fa0/21,Fa0/22,Fa0/23
```

```
                                        Fa0/24
10    test10                            active    Fa0/1
20    test20                            active    Fa0/2
S2126#
```

显示状态说明 F0/1 已经划归 test10，F0/2 已经划归 test20。

步骤 5：测试结果

将 PC1 和 PC2 的 IP 地址设为 172.16.20.0/24 的 IP，验证 PC1 和 PC2 不能相互 ping 通。

下面可以将目前的配置清空，准备下一个实验，清空命令为：

```
Delete flash:config.text          ！清除配置文件
Delete flash:vlan.dat             ！删除 VLAN 配置文件
```

PC1 的 IP 地址设置为：_____；

PC2 的 IP 地址设置为：_____；

步骤 5 测试结果：PC1 和 PC2 能否相互 ping 通？ □ 能； □ 不能；

清除交换机配置后重启，PC1 和 PC2 能否相互 ping 通？ □ 能； □ 不能；

3.2.2 跨交换机的 VLAN 划分实验

1．IEEE802.1Q 标准

1996 年 3 月，IEEE802.1 Internet Working 委员会结束了对 VLAN 初期标准的修订工作，统一了 Frame-Tagging（帧标记）方式中不同厂商的标签格式，制定 IEEE802.1Q VLAN 标准，进一步完善了 VLAN 的体系结构。

802.1Q 定义了 VLAN 的桥接规则，能够正确识别 VLAN 的帧格式，更好地支持多媒体应用。它为以太网提供了更好服务质量（QOS）保证和安全的能力。

如图 3.12 所示，IEEE802.1Q 使用 4Byte 的标记头来定义 Tag（标记）。Tag 头中包括 2Byte 的 VPID（VLAN Protocol Identifier）和 2Byte 的 VCI（VLAN Control Information）。其中：VPID 为 0x8100，标识该数据帧承载 IEEE802.1Q 的 Tag 信息；VCI 包含组件：3 bits 用户优先级、1 bits CFT（Canonical Format Indicator），默认值为 0（表示以太网）和 12 bits 的 VID（VLAN Identifier，VLAN 标识符）。

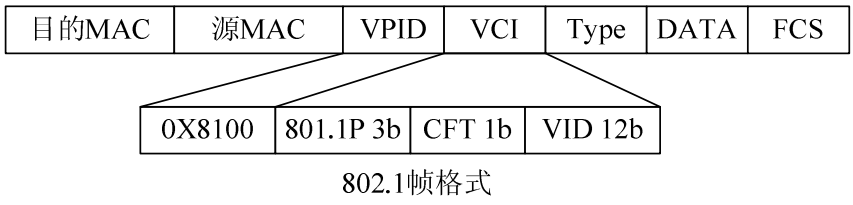


图 3.12 802.1Q 帧格式

基于 802.1Q Tag VLAN 用 VID 来划分不同 VLAN，当数据帧通过交换机的时候，交换机根据数据帧中 Tag 的 VID 信息来识别它们所在的 VLAN（若帧中无 Tag 头，则应用帧所通过端口的默认 VID 来识别它们所在的 VLAN）。这使得所有属于该 VLAN 的数据帧，不管是单播帧、组播帧还是广播帧，都将被限制在该逻辑 VLAN 中传输。

当使用多台交换机分别配置 VLAN 后，可以使用 Trunk（干道）方式实现跨交换机的 VLAN 内部连通，交换机的 Trunk 端口不隶属于某个 VLAN，而是可以承载所有 VLAN 的帧。跨交换机的 VLAN 实现使得网络管理的逻辑结构可以完全不受实际物理连接的限制，极大地提高了组网的灵活性。

互联的交换机能够通过识别数据帧的目的 MAC 地址和 VLAN 信息，将它发送到正确的 VLAN 和端口中。而在互联端口出现拥塞时，交换机都能够通过识别 802.1P 协议（它是

802.1Q 的补充，它定义了优先级的概念）字段的优先级信息，优先转发高优先级的数据包。这种方式受到多厂家设备的支持，已经在不同产品组成的二层网络中普遍使用。

2．Port VLAN 和 Tag VLAN

在 VLAN 配置中，我们使用 switchport mode 命令来指定一个二层接口（switch port）的模式，可以指定该接口为 access port 或者为 trunk port。使用该命令的 no 选项将该接口的模式恢复为缺省值（access）。其命令执行在接口模式下，语法格式如下：

switchport mode {access | trunk}

no switchport mode

如果一个 switch port 的模式是 access，则该接口只能为一个 VLAN 的成员。可以使用 switchport access vlan 命令指定该接口是哪一个 VLAN 的成员，这种接口又称为 Port VLAN；

如果一个 switch port 的模式是 trunk，则该接口可以是多个 VLAN 的成员，这种配置被称为 Tag VLAN。Trunk 接口默认可以传输本交换机支持的所有 VLAN（1～4094），但是也可以通过设置接口的许可 VLAN 列表来限制某些 VLAN 的流量不能通过这个 trunk 口。

在 Trunk 口 修改许可 VLAN 列表的命令如下（本节实验对此不作要求）。

switchport trunk allowed vlan { all | [add | remove | except] *vlan-list* }

其中：all 的含义是许可 VLAN 列表包含所有的 VLAN；add 表示将指定的 VLAN 加入许可列表；remove 表示将指定的 VLAN 从许可列表中删除；except 表示将除列出的 v lan-list 外的所有 VLAN 加入许可列表。

Trunk 口能够收发 TAG 或者 UNTAG 的 802.1Q 帧，其中 UNTAG 帧是用来传输 Native VLAN 的流量。默认的 Native VLAN 是 VLAN 1，如果一个帧带有 Native VLAN 的 VLAN ID，在通过这个 Trunk 口转发时，会自动被剥去 TAG。配置 Native VLAN 在 Trunk 口接口模式下，执行 switchport trunk native vlan *vlan-id*。

3．实验环境与说明

（1）实验目的

掌握跨交换机的 VLAN 配置方法，了解 IEEE802.1Q 的基本原理，理解 Port VLAN 和 Tag VLAN 的使用。

（2）实验设备和连接

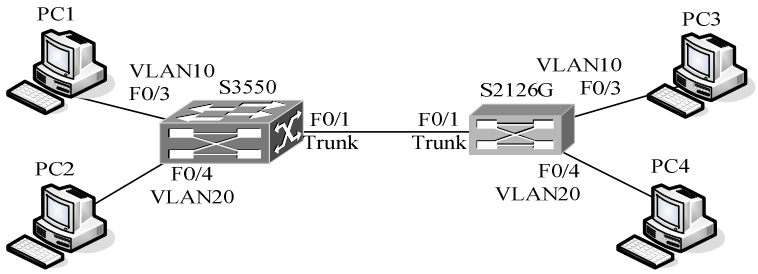


图 3.13 跨交换机划分 VLAN 实验

实验设备和连接图如图 3.13 所示，一台锐捷 S2126G 交换机连接一台 S3550 交换机，每台交换机各连接 2 台 PC 机。假设某企业的网络中，计算机 PC1 和 PC3 属于营销部门，PC2 和 PC4 属于技术部门，PC1 和 PC2 连接在 S3550 上，PC3 和 PC4 连接在 S2126 上，而两个部门要求互相隔离，本实验的目的是实现跨两台交换机将不同端口划归不同的 VLAN。

（3）实验分组

每四名同学为一组，其中每两人一小组，每小组各自独立完成实验。

4．实验步骤

步骤 1：按照网络拓扑在 RACK 机柜中选择一台 S3550 和一台 S2126，完成接线。例如，选择实验台 1－4＃PC 机，5＃交换机（S3550），7＃交换机（S2126）。可参考连接如下：S5F1－S7F1、N1－S5F3、N2－S5F4、N3－F7F3、N4－F7F4。

注意：随着大家对实验机柜配线架的熟悉，今后的实验将不再给出接线参考。

步骤 2：配置 S3550：

（1）设备标识

```
Switch# configure terminal
Switch(config)# hostname S3550
```

（2）在 S3550 上创建 VLAN10、VLAN20

```
S3550(config)# vlan 10                          ！创建 VLAN10
S3550(config-vlan)# name sales                  ！将 vlan 10 命名为营销 sales
S3550(config-vlan)# exit
S3550(config)# vlan 20                          ！创建 VLAN20
S3550(config-vlan)# name technical              ！将 vlan 20 命名为技术 technical
S3550(config-vlan)# end
S3550# show vlan                                ！验证配置
VLAN Name                                       Status      Ports
---- -------------------------------- --------- -------------------------------
1    default                                    active      Fa0/1 ,Fa0/2 ,Fa0/3 ,Fa0/4
                                                            Fa0/5 ,Fa0/6 ,Fa0/7 ,Fa0/8
                                                            Fa0/9 ,Fa0/10,Fa0/11,Fa0/12
                                                            Fa0/13,Fa0/14,Fa0/15,Fa0/16
                                                            Fa0/17,Fa0/18,Fa0/19,Fa0/20
                                                            Fa0/21,Fa0/22,Fa0/23,Fa0/24
10   sales                                      active
20   technical                                  active
```

可以看出，在 S3550 上 VLAN10 和 VLAN20 已经启用，但还没有指定端口。

（3）在 S3550 上把 F0/3 划归 VLAN10、F0/4 划归 VLAN20

```
S3550# configure terminal
S3550(config)# interface fastEthernet 0/3       ！进入 F0/3 接口配置模式
S3550(config-if)# switchport access vlan 10     ！将 F0/3 划归 vlan10
S3550(config-if)# end
```

使用 show vlan 命令验证 VLAN10 的配置，执行如下：

```
S3550# show vlan id 10                          ！验证配置
VLAN Name                                       Status      Ports
---- -------------------------------- --------- -------------------------------
10   sales                                      active      Fa0/3
```

可以看出 S3550 的接口 F0/3 已经被划归 VLAN10。

```
S3550# configure terminal
S3550(config)# interface fastEthernet 0/4       ！进入 F0/3 接口配置模式
S3550(config-if)# switchport access vlan 20     ！将 F0/4 划归 vlan20
S3550(config-if)# end
```

使用 show vlan 命令验证 VLAN20 的配置，执行如下：

```
S3550# show vlan id 20                          ！验证配置
```

```
VLAN Name                                Status    Ports
---- ------------------------------- --------- -------------------------------
20   technical                           active    Fa0/4
```

可以看出 S3550 的接口 F0/4 已经被划归 VLAN20。

步骤 3：S2126 的配置方法与步骤 2 完全相同，这里不再列出。注意应当完成以下任务：将设备名改为 S2126、创建 VLAN10 和 VLAN20、分别将 F0/3 和 F0/4 接口划分至 VLAN10 和 VLAN20。

步骤 4：配置 S3550 和 S2126 之间的 Trunk 连接：

以 S3550 为例，需要配置 F0/1 为 TAG 端口，配置命令如下：

```
S3550(config)# interface fastEthernet 0/1          ！进入 F0/1 接口配置模式
S3550(config-if)# switchport mode trunk            ！将 F0/1 设置为 Trunk 模式
```

验证 F0/1 已经设置为 tag vlan 模式的方法如下：

```
S3550# show interface fastEthernet 0/1 switchport
Interface      Switchport   Mode      Access   Native   Protected     VLAN lists
Fa0/1          Enable       Trunk     1        1        Disabled      All
```

注意 S2126 上也需要做同样配置：

```
S2126(config)# interface fastEthernet 0/1          ！进入 F0/1 接口配置模式
S2126(config-if)# switchport mode trunk            ！将 F0/1 设置为 Trunk 模式
```

步骤 5：配置计算机：

将 PC1 和 PC3 指定为 172.16.10.0/24 网段 IP， PC2 和 PC4 为 172.16.20.0/24 网段 IP。例如 PC1：172.16.10.10、PC2：172.16.20.20、PC3：172.16.10.30、PC4：172.16.20.40。

验证 PC1 与 PC3 能互相通信，但 PC2 与 PC3 不能互相通信。

```
C:\>ping 192.168.10.30      ！在 PC1 的命令行方式下验证能 Ping 通 PC3 。
Pinging 192.168.10.30 with 32 bytes of data:
Reply from 192.168.10.30: bytes=32 time<10ms TTL=128
Reply from 192.168.10.30: bytes=32 time<10ms TTL=128
Reply from 192.168.10.30: bytes=32 time<10ms TTL=128
Reply from 192.168.10.30: bytes=32 time<10ms TTL=128
Ping statistics for 192.168.10.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

```
C:\>ping 192.168.10.30      !在 PC2 的命令行方式下验证不能 Ping 通 PC3 。
Pinging 192.168.10.30 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.10.30:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
  Approximate round trip times in milli-seconds:
      Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

如果将 PC1、PC2、PC3 和 PC4 的 IP 地址设置在同一网段，例如 PC1：172.16.10.10、PC2：172.16.10.20、PC3：172.16.10.30、PC4：172.16.10.40。判断它们之间能否 ping 通，验证一下，将结果填入表 3.6。

表 3.6 VLAN 实验验证结果

验证机	所在 VLAN	验证机	所在 VLAN	能否连通
PC1		PC2		□ 能； □ 不能；
PC1		PC3		□ 能； □ 不能；
PC1		PC4		□ 能； □ 不能；
PC2		PC3		□ 能； □ 不能；
PC2		PC4		□ 能； □ 不能；
PC3		PC4		□ 能； □ 不能；

3.2.3 三层交换机实现 VLAN 间通讯及链路聚合应用实验

1．三层交换机简介

在一般的二层交换机组成的网络中，VLAN 实现了网络流量的分隔，不同的 VLAN 间是不能相互通信的。如果要实现 VLAN 间的通信必须借助路由来实现。一种方法是利用路由器，另一种则是借助具有三层功能的交换机。

三层交换机，从本质上讲就是带有路由功能（三层）的交换机。第三层交换机就是将第二层交换机和第三层路由器两者的优势有机而智能化地结合起来，可在各个层次提供线速功能。这种集成化的结构还引进了策略管理属性，不仅使第二层和第三层关联起来，而且还提供了流量优化处理、安全访问机制以及其他多种功能。

在一台三层交换机内，分别设置了交换模块和路由模块，内置的路由模块与交换模块类似，也使用了 ASIC 硬件处理路由。因此，与传统的路由器相比，可以实现高速路由。而且路由与交换模块是汇聚链接的，由于是内部连接，可以确保相当大的带宽。我们可以利用三层交换机的路由功能来实现 VLAN 间的通信。

下面我们使用一个简单的网络来概括三层交换机的工作过程：

使用 IP 的设备 A 通过三层交换机和设备 B 相连。

假如 A 要向 B 发送数据，已知目的 IP，那么 A 可以通过子网掩码取得网络地址，判断目的 IP 与自己是否在同一网段。如果在同一网段，但不知道转发数据所需要的 MAC 地址，A 就发送一个 ARP 请求广播，B 返回其 MAC 地址，A 用此 MAC 封装数据帧并发送给交换机，交换机启用二层交换模块，查找 MAC 地址表，将数据帧转发到相应的端口。

如果目的 IP 地址不在同一网段，那么 A 要实现和 B 的通信，在流缓存条目中没有对应 MAC 地址条目，就将第一个正常数据包发送向缺省网关（在操作系统 TCP/IP 配置中已经设好，对应于第三层路由设备），由此可以看出对于不是同一子网的数据，最先在 MAC 表中放的是缺省网关的 MAC 地址；然后就由三层模块接收此数据包，查询路由表以确定到达 B 的路由，同时将构造一个新的帧头，其中以缺省网关的 MAC 地址为源 MAC 地址，以主机 B 的 MAC 地址为目的 MAC 地址。通过一定的识别触发机制，确立主机 A 和主机 B 的 MAC 地址及转发端口的对应关系，并记录于流缓存条目表，以后的 A 到 B 的数据，就直接交由二层交换模块完成。

以上过程就是通常所说的一次路由多次转发。三层交换机不是简单的二层交换机和路由器的叠加，而是通过硬件结合实现数据的高速转发，特别适合于内网数据流量大、要求快速转发的园区网使用。

2．链路聚合技术

对于局域网交换机之间以及从交换机到高需求服务的许多网络连接来说，100M 甚至 1Gbps 的带宽是不够的。链路聚合技术（也称端口聚合）帮助用户减少了这种压力。

制定于 1999 年的 IEEE802.3ad（Link Aggregation Control Protocol，LACP）链路聚合控制协议，定义了如何将两个以上的以太网链路组合起来为高带宽网络连接实现负载共享、负载平衡以及提供更好的弹性。

端口聚合将交换机上的多个端口在物理上连接起来，在逻辑上捆绑在一起，形成一个拥有较大宽带的端口，形成一条干路，可以实现均衡负载，并提供冗余链路。Aggregate Port（以下简称 AP），符合 IEEE802.3ad 标准。它可以把多个端口的带宽叠加起来使用，比如全双工快速以太网端口形成的 AP 最大可以达到 800Mbps，或者千兆以太网接口形成的 AP 最大可以达到 8Gbps。

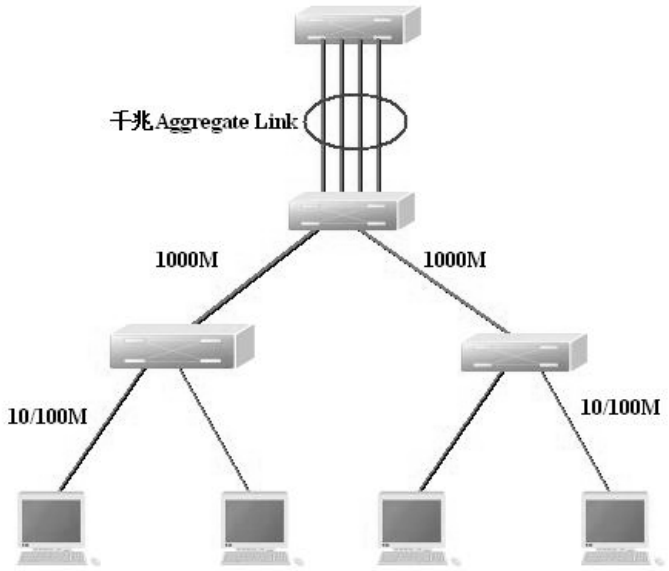


图 3.14 端口聚合

如图 3.14 所示，端口聚合可以帮助用户减少了来自主干网络带宽的压力，同时，链路聚合标准在点到点链路上提供了固有的、自动的冗余性，保证了网络的可靠性。

AP 根据报文的 MAC 地址或 IP 地址进行流量平衡，即把流量平均地分配到 AP 的成员链路中去。流量平衡的实现可以根据源 MAC 地址、目的 MAC 地址或源 IP 地址/目的 IP 地址对。在本节实验中，我们使用二层 AP。

配置二层 aggregate port 的基本命令如下：

Switch#configure terminal

Switch(config) # interface *interface-id*

Switch(config-if-range)#port-group *port-group-number*

说明：上述操作是将该接口加入一个 AP（如果这个 AP 不存在，则同时创建这个 AP）。

实验室的锐捷交换机最大支持 8 个端口聚合，在配置以太网链路聚合时应当注意：

- 组端口的速度必须一致；
- 组端口必须属于同一个 VLAN；
- 组端口使用的传输介质相同；
- 组端口必须属于同一层次，并与 AP 也要在同一层次。

3．实验环境与说明

（1）实验目的

掌握交换机链路聚合的配置方法，通过三层交换机 SVI 实现不同 VLAN 间的连通。

（2）实验设备和连接

实验设备和连接图如图 3.15 所示，大家可以看出本节实验的设备连接只是在上节 3.2.2 实验连接的基础上增加了一条链路，即 S3550 和 S2126G 之间的链路由 1 条（F0/1－F0/1）增加为 2 条（F0/1－F0/1、 F0/2－F0/2）。

注意：为防止实验过程中由于桥接环路所导致的广播风暴影响设备配置（交换机不断显示相关提示信息），可以在完成实验步骤 3 之后，再连接交换机的冗余链路。

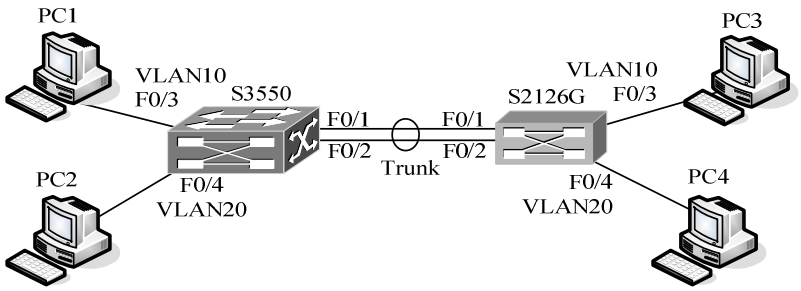


图 3.15 三层交换机实现 VLAN 间通讯及链路聚合应用实验

（3）实验分组

每四名同学为一组，其中每两人一小组，每小组各自独立完成实验。

4．实验步骤

步骤 1：按照网络拓扑在 RACK 机柜中选择一台 S3550 和一台 S2126，完成接线。

步骤 2：按照 3.2.2 实验步骤 2 和步骤 3 的方法配置 S3550 和 S2126，配置命令这里不再列出。注意应当完成以下任务：将设备名改为 S3550 和 S2126、分别创建 VLAN10 和 VLAN20、分别将 F0/3 和 F0/4 接口划分至 VLAN10 和 VLAN20。

步骤 3：在 S3550 和 S2126 上配置冗余链路聚合，以 S3550 为例，配置如下：

```
S3550# configure terminal
S3550(config)# interface range fastEthernet 0/1-2      ！使用该命令同时配置多个接口
S3550(config-if-range)#port-group 1                    ！配置 F0/1 和 F0/2 归属于 AG1
S3550(config-if-range)#exit
```

说明：用户可以使用 interface range 命令同时配置多个接口，配置的方法和配置单个接口完全相同。当进入 interface range 配置模式时，此时所能设置的属性应用于所选范围内的所有接口。

该命令的语法格式为：interface range *port-range*

其中 *port-range* 指定若干接口范围段，每个接口范围段包括一定范围的接口，接口范围段之间使用逗号（,）隔开。例如 interface range fastEthernet 0/1-5,0/7,1/1-2 选择了 3 个范围段共计 8 个接口。

不要忘记，S2126 上也要做相应配置。验证聚合端口配置可以使用 show aggregateport 命令，执行如下：

```
S3550# show aggregateport 1 summary                    ！显示聚合端口 AG1 摘要信息
Aggregateport    MaxPort    Switchport    Mode      Ports
AG1                 8          Enabled     Trunk     Fa0/1, Fa0/2
```

步骤 4：在 S3550 和 S2126 上配置聚合端口为干道（Trunk）方式，S3550 的配置如下：

```
S3550(config)# interface aggregatePort 1               ！进入 AG1 接口模式
S3550(config-if)# switchport mode trunk                ！将端口设为 tag vlan 模式
S3550(config-if)# end
```

S2126 的配置如下：

```
S2126(config)# interface aggregatePort 1                ！进入 AG1 接口模式
S2126(config-if)# switchport mode trunk                 ！将端口设为 tag vlan 模式
```

就这样便完成了将聚合端口配置为 TAG VLAN 的操作，为确定配置可以使用 show vlan 或 show interfaces 命令验证。

```
S3550# show vlan                                        ！查看 vlan 状态
VLAN Name                                    Status     Ports
---- ------------------------------- --------- -------------------------------
1    default                                 active     Fa0/1 ,Fa0/2 ,Fa0/5 ,Fa0/6
                                                        Fa0/7 ,Fa0/8,Fa0/9,Fa0/10
                                                        Fa0/11,Fa0/12,Fa0/13,Fa0/14
                                                        Fa0/15,Fa0/16,Fa0/17,Fa0/18
                                                        Fa0/19,Fa0/20,Fa0/21,Fa0/22
                                                        Fa0/23,Fa0/24
                                                        Ag1
10   VLAN0002                                active     Fa0/3
                                                        Ag1
20   VLAN0003                                active     Fa0/4
                                                        Ag1
S3550# show interfaces aggregatePort 1 switchport       ！查看 AP1 接口状态
Interface   Switchport   Mode      Access   Native     Protected   VLAN lists
---------- ---------- --------- ------- -------- --------- -------------------
Ag1         Enabled      Trunk       1          1          Disabled    All
```

步骤 5：配置 L3 交换机虚拟端口 SVI，默认情况下 L3 交换机并不能实现 VLAN 间的连通，我们可以通过配置 SVI，启动三层功能来实现 VLAN 间的连通，具体配置如下：

```
S3550# configure terminal
S3550(config)# interface vlan 10                        ！创建虚拟接口 vlan 10
S3550(config-if)# ip address 172.16.10.254 255.255.255.0
                                                        ！配置虚拟接口 vlan 10 的地址为 172.16.10.254
S3550(config-if)# no shutdown                           ！启用端口
S3550(config-if)# exit
S3550(config)# interface vlan 20                        ！创建虚拟接口 vlan 20
S3550(config-if)# ip address 172.16.20.254 255.255.255.0
                                                        ！配置虚拟接口 vlan 20 的地址为 172.16.20.254
S3550(config-if)# no shutdown                           ！启用端口
S3550(config-if)# end
S3550#
```

验证配置可以使用 show ip interface 命令，执行如下：

```
S3550#show ip interface
Interface                : VL10
Description              : Vlan 10
OperStatus               : up
ManagementStatus         : Enabled
Primary Internet address: 172.16.10.254/24
Broadcast address        : 255.255.255.255
```

PhysAddress : 00d0.f8b8.32a9

Interface : VL20
Description : Vlan 20
OperStatus : up
ManagementStatus : Enabled
Primary Internet address: 172.16.20.254/24
Broadcast address : 255.255.255.255
PhysAddress : 00d0.f8b8.32aa

L3 交换机启动路由功能的操作如下：

```
S3550(config)# ip routing                                    ！启动路由功能
```

说明：三层交换机启动路由功能后，可以进一步配置静态路由或动态路由选择协议，可与路由器结合解决网际互连（本节实验可以不需要执行该命令）。

```
S3550# show ip route                                         ！查看路由表
Type:   C - connected, S - static, R - RIP, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
Type Destination IP      Next hop        Interface     Distance    Metric    Status
---- ----------------- --------------- ---------- -------- -------- --------
C    172.16.10.0/24      0.0.0.0         VL10          0           0         active
C    172.16.20.0/24      0.0.0.0         VL20          0           0         active
S3550#
```

步骤 6：配置计算机：按照表 3.7 为 PC 机配置 TCP/IP 属性：

表 3.7 实验 PC 的 IP 设置

计算机	IP 地址	子网掩码	网关
PC1	172.16.10.10	255.255.255.0	172.16.10.254
PC2	172.16.20.20	255.255.255.0	172.16.20.254
PC3	172.16.10.30	255.255.255.0	172.16.10.254
PC4	172.16.20.40	255.255.255.0	172.16.20.254

配置完成后，执行以下验证操作：

（1）验证不同 VLAN 内的主机可以互相 ping 通。

（2）在 PC1 上执行 ping 172.16.10.30 –t ，在执行过程中断开交换机之间的一条链路，接上该链路后再断开另一条链路，我们会发现 PC1 与 PC3 仍然能够通信。理解 Aggregate Port 的作用。

说明：在命令 ping 172.16.10.30 –t 中，–t 的含义是在探测指定的计算机时，让用户主机不断向目标主机发送数据，也就是连续发送与接收回送请求和应答 ICMP 报文，直到手动停止，Ctr+C 停止 ping 命令。

3.3 生成树协议 STP

在局域网中，为了提高网络连接可靠性，经常提供冗余链路。所谓冗余链路就像公路、铁路一样，条条道路通北京，这条不通走那条。例如在大型企业网中，多半在核心层配置备份交换机（网桥），则与汇聚层交换机形成环路，这样做使得企业网具备了冗余链路的安全优势。但原先的交换机并不知道如何处理环路，而是将转发的数据帧在环路里循环转发，使

得网络中出现广播风暴，最终导致网络瘫痪。

为了解决冗余链路引起的问题，IEEE802 通过了 IEEE 802.1d 协议，即生成树协议（Spanning Tree Protocol，STP）。IEEE 802.1d 协议通过在交换机上运行一套复杂的算法，使冗余端口置于“阻塞状态”，从而使网络中的计算机通信时只有一条链路生效，而当这个链路出现故障时，STP 将会重新计算出网络的最优链路，将“阻塞状态”的端口重新打开，从而确保网络连接的稳定可靠。

生成树协议和其它协议一样，是随着网络的不断发展而不断更新换代的。在生成树协议发展的过程中，老的缺陷不断被克服，新的特性不断被开发出来。按照功能特点的改进情况，习惯上生成树协议的发展过程被分为三代：

第一代生成树协议：STP/RSTP

第二代生成树协议：PVST/PVST+

第三代生成树协议：MISTP/MSTP

本节将介绍这第一代生成树协议 STP 和 RSTP 协议。

3.3.1 生成树协议 STP 的应用实验

1．IEEE 801.1D 生成树协议简介

生成树协议（Spanning Tree Protocol，STP）最初是由美国数字设备公司（DEC）开发的，后经 IEEE 修改并最终制定了 IEEE 802.1d 标准。

STP 协议的主要思想是当网络中存在备份链路时，只允许主链路激活，如果主链路失效，备份链路才会被打开。大家知道，自然界中生长的树是不会出现环路的，如果网络也能够像树一样生长就不会出现环路。STP 协议的本质就是利用图论中的生成树算法，对网络的物理结构不加改变，而在逻辑上切断环路，封闭某个网桥，提取连通图，形成一个生成树，以解决环路所造成的严重后果。

为了理解生成树协议，必先了解以下概念：

（1）桥协议数据单元（Bridge Protocol Data Unit，BPDU）：交换机通过交换 BPDU 来获得建立最佳树型拓扑结构所需的信息。生成树协议运行时，交换机使用共同的组播地址“01-80-C2-00-00-00”来发送 BPDU；

（2）每个交换机有唯一的桥标识符（Brideg ID），由桥优先级和 MAC 地址组成；

（3）每个交换机的端口有唯一的端口标识符（Port ID），由端口优先级和端口号组成；

（4）对生成树的配置时，对每个交换机配置一个相对的优先级，对每个交换机的每个端口也配置一个相对的优先级，该值越小优先级越高；

（5）具有最高优先级的交换机被称为根桥（Root Bridge），如果所有设备都具有相同的优先级，则具有最低 MAC 地址的设备将成为根桥；

（6）网络中每个交换机端口都有一个根路径开销（Root Path Cost），根路径开销是某交换机到根桥所经过的路径开销（与链路带宽有关）的总和；

（7）根端口是各个交换机通往根桥的根路径开销最低的端口，若有多个端口具有相同的根路径开销，则端口标识符小的端口为根端口；

（8）在每个 LAN 中都有一个交换机被称为指定交换机（Designated Bridge），它是该 LAN 中与根桥连接而且根路径开销最低的交换机；

（9）指定交换机和 LAN 连接的端口被称为指定端口（Designated Port）。如果指定桥中有两个以上的端口连在这个 LAN 上，则具有最高优先级的端口被选为指定端口。根桥上的端口都可以成为指定端口，交换机上除根端口之外的端口都可以成为指定端口；

（10）根端口和指定端口进入转发（Forwarding）状态，其它的冗余端口则处于阻塞（Discarding）状态。

2．STP 配置的有关命令

（1）开启、关闭 STP 协议

锐捷交换机默认状态是关闭 STP 协议。

开启 STP 的命令为：Switch (config)# spanning-Tree

如果你要关闭 STP 协议，可以执行 no spanning-Tree 全局配置命令。

（2）配置交换机优先级

设置交换机的优先级关系着到底哪个交换机为整个网络的根交换机，同时也关系到整个网络的拓扑结构。建议管理员把核心交换机的优先级设置的高些（数值小），这样有利于整个网络的稳定。

交换机优先级的默认值为 32768，设置值 16 个，都为 4096 的倍数，包括：0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440；

配置交换机优先级使用如下命令：

Switch (config)# spanning-tree priority <0-61440>

如果要恢复默认值，执行 no spanning-tree priority 全局配置命令。

（3）配置端口优先级

和交换机优先级一样，端口优先级的设置值也是 16 个，都为 16 的倍数，分别为：0、16、32、48、64、80、96、112、128、144、160、176、192、208、224 和 240，默认值为 128。

配置交换机端口优先级使用如下命令：

Switch (config-if)# spanning-tree port-priority <0-240>

如果要恢复默认值，执行 no spanning-tree port-priority 接口配置命令。

（4）配置 BPDU 的时间选项

命令格式如下，使用 no 选项恢复默认设置：

spanning-tree {forward-time *seconds* | hello-time *seconds* | max-age *seconds* }

no spanning-tree [forward-time | hello-time | max-age]

语法描述可参见表 3.8，注意 forward-time、hello-time 和 max-age 三个值的范围是相关的，修改了其中一个会影响到其他两个的值范围。这三个值之间有一个制约关系：

2×(Hello Time +1.0)≤Max-Age Time ≤2×(Forward-Delay－1.0)

不符合这个条件的值不会设置成功。本节实验不要求更改 BPDU 的时间选项。

表 3.8 BPDU 的时间选项

forward-time *seconds*	端口状态改变的时间间隔，默认15秒，取值4－30
hello-time *seconds*	交换机定时发送BPDU报文的时间间隔，默认2秒，取值1－10
max-age *seconds*	BPDU报文消息生存的最长时间，默认20秒，取值6－40

（5）STP 信息显示和检测命令

本节实验中我们使用以下两个命令显示 STP 信息：

show spanning-tree ！显示交换机生成树状态

show spanning-tree interface ！显示交换机接口 STP 状态

3．实验环境与说明

（1）实验目的

掌握交换机 STP 的配置方法，理解 STP 协议的原理及其在冗余链路中的工作过程。

（2）实验设备和连接

实验设备和连接图如图 3.16 所示，选择两台 S2126G（或 S3550）交换机分别连接 1 台 PC，交换机间建立双链路连接。

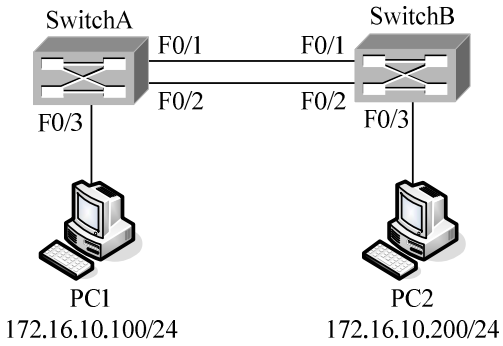


图 3.16 生成树 STP 的应用实验

（3）实验分组

每四名同学为一组，其中每两人一小组，每小组各自独立完成实验。

4．实验步骤

步骤 1：按照网络连接图完成设备连接，为防止实验过程中由于冗余链路可能导致的广播风暴的影响，可以在完成设备 STP 配置之后连接交换机的冗余链路；

步骤 2：在每台交换机上启动生成树协议，例如在 SwitchA 上进行配置：

```
SwitchA# configure terminal
SwitchA(config)# spanning-tree                    ！开启生成树协议
SwitchA(config)# spanning-tree mode stp           ！设置生成树为 STP（802.1D）
SwitchA(config)# end
```

实验室所采用的锐捷交换机在启动生成树协议后，默认使用 MSTP，因此需要改变模式为 STP。完成 SwitchA 的配置后，在 SwitchB 上也做相同设置；

步骤 3：配置 SwitchA 为根交换机：

当使用默认配置时，SwitchA 和 SwitchB 的交换机优先级为 32768，两者中 MAC 地址小的将成为根交换机。我们可以通过更改交换机优先级来指定其中的一台为根交换机。

```
SwitchA (config)# spanning-tree priority 4096     ！设置 SwitchA 的优先级为 4096
```

完成配置后可以使用 show spanning-tree 和 show spanning-tree interface 验证，请参考下面的例子按照要求执行操作并回答问题。

```
SwitchA# show spanning-tree     ！显示交换机的生成树模式及相关状态
stpVersion: STP                                   ！STP 的版本为 STP
SysStpStatus: Enabled                             ！STP 系统状态为启动（打开）
BaseNumPort: 24                                   ！基本端口数为 24
Maxage: 20                                        ！BPDU 生存的最长时间
HelloTime: 2                                      ！BPDU 报文的时间间隔
ForwardDelay: 15                                  ！端口状态改变的时间间隔
BridgeMaxAge: 20
BridgeHelloTime: 2
BridgeForwardDelay: 15
MaxHops: 20                                       ！最大中继跳数
TxHoldCount: 3
PathCostMethod: Long                              ！路径开销方式
BPDUGuaed: Disabled                               ！BPDU 保护未启动
```

BPDUFilter: Disabled ！BPDU 过滤未启动
BridgeAddr : **00d0.f8c0.2225** ！桥 MAC 地址
Priority: **4096** ！优先级为 4096
TimeSinceTopologyChange: 0d:0h:3m:9s ！拓扑改变的时间
TopologyChanges: 19
DesignateRoot: **100000D0F8C02225** ！指定根
RootCost: 0 ！根开销
RootPort: 0 ！根端口

（1）比较根交换机上 DesignateRoot 与 BridgeAddr、Priority，说明它们之间的关系。

SwitchB# show spanning-tree interface fastEthernet 0/1 ！显示 Fa0/1 接口 STP 状态
PortAdiminPortfast: Disabled
PortOperPortfast: Disabled
PortAdiminLinkType: auto
PortOperLinkType: point-to-point
PortBPDUGuaed: Disabled:
PortBPDUFilter: Disabled
PortState: **forwarding** ！Fa0/1 接口状态为转发
PortPriority: **128** ！端口优先级为 128
PortDesignateRoot: **100000D0F8C02225** ！端口指定根
PortDesignatedCost: 0
PortDesignatedBridge : 100000D0F8C02225 !
PortDesignatedPort: **8001** ！指定端口为 8001
PortForwardingTransitions: 2
PortAdiminPathCost: 0
PortOperPathCost: 200000
PortRole: **rootPort** ！端口角色为根端口

（2）在 SwitchA 和 SwitchB 上分别执行 show spanning-tree，分析显示结果，填写表 3.9。

表 3.9 SwitchA 和 SwitchB 的 STP 对比

参数	SwitchA	SwitchB
Priority		
BridgeAddr		
Brideg ID		
DesignateRoot		

（3）在 SwitchA 和 SwitchB 上分别执行 show spanning-tree interface 命令检查 F0/1 和 F0/2 接口，分析显示结果，填写表 3.10。

表 3.10 SwitchA 和 SwitchB 的接口 STP 对比

设备	SwitchA		SwitchB	
接口	F0/1	F0/2	F0/1	F0/2
PortRole				
PortState				

步骤 4：配置 PC1 和 PC2 的 IP 地址，验证网络拓扑发生变化时，ping 的丢失包的情况：用 ping 命令从 PC1 连续探测 PC2，命令如下：

C:\ping 172.16.10.200 –t　　！连续探测 PC2,显示结果如下：
Reply from 172.16.10. 200 bytes=32 times<10ms　TTL=64
Reply from 172.16.10. 200 bytes=32 times<10ms　TTL=64
Reply from 172.16.10. 200 bytes=32 times<10ms　TTL=64
Reply from 172.16.10. 200 bytes=32 times<10ms　TTL=64
Reply from 172.16.10. 200 bytes=32 times<10ms　TTL=64
……
可以正常 ping 通。

然后，断开交换机的 F0/1 与 F0/1 连接，观察 ping 的执行情况，可以发现会丢失若干个包，显示 Request timed out，一段时间后，系统自动恢复连通。理解 STP 协议的工作原理并回答下面问题：

（1）实验中，在拓扑改变过程中，出现了多少个丢包？以 ping 命令默认 2 秒超时计算，实验中交换机 F0/2 端口由 discarding（阻塞）状态转为 forwarding（转发）状态，存在多长时间的延迟？

（2）用 show spanning-tree interface 查看交换机 F0/2 端口，有什么变化？

3.3.2 快速生成树协议 RSTP 的应用实验

1．IEEE 801.1W 快速生成树协议

在介绍 RSTP 之前，我们首先说明一下在 STP 中存在的问题，这主要表现在收敛时间上。STP 协议解决了交换链路冗余问题，在拓扑发生改变时，新的 BPDU 要经过一定的时延才能传播到整个网络，这个时延称为 Forward Delay，协议默认为 15 秒。在所有交换机收到这个变化的消息之前，若旧拓扑结构中处于转发状态的端口还没有发现自己应当在新的拓扑中停止转发，则可能存在临时环路。为此，生成树使用了一种定时器策略，即在端口由阻塞状态到转发状态中间加上一个只学习 MAC 地址但不参与转发的中间状态，两次状态切换的时间都是 Forward Delay，这样就可以保证拓扑变化的时候不会产生临时环路。但是这个看似良好的解决方案却导致了至少两倍 Forward Delay 的收敛时间，造成了 STP 协议的最大缺陷。

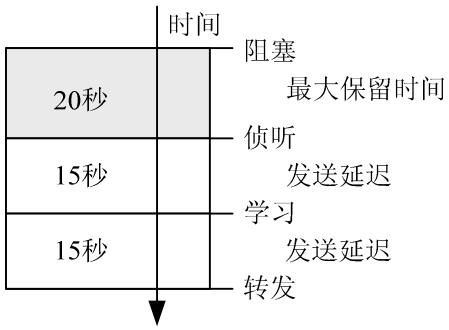


图 3.17 生成树性能的三个计时器

如图 3.17 所示，在默认状态下，BPDU 的报文周期为 2 秒，最大保留时间为 20 秒，端口状态改变（由侦听到学习，由学习到转发）的时间为 15 秒。当网络拓扑改变后，STP 要经过一定的时间（默认为 50 秒）才能够稳定，网络稳定是指所有端口或者进入转发状态或者进入阻塞状态。

50 秒的延迟对于早期网络或许不算什么，那时人们对网络的依赖性不强，但现在就不同了，早期的 STP 协议已经不能适应网络的发展需要。于是，作为 IEEE802.1d 标准的补充，IEEE802.1w 协议问世了。

IEEE802.1w 在 IEEE802.1d 的基础上做了三点重要改进，使得收敛速度快得多（最快 1 秒以内），因此 IEEE802.1w 又称为快速生成树协议（Rapid Spanning Tree Protocol ，RSTP）。RSTP 的主要改进为：

（1）为根端口和指定端口设置了快速切换用的替换端口（Alternate Port）和备份端口

（Backup Port）两种角色，当根端口/指定端口失效的情况下，替换端口/备份端口就会无时延的进入转发状态，而无须等待两倍 Forward Delay 的时间；

（2）在只连接了两个交换端口的点对点链路中，指定端口只需与下游交换机进行一次握手就可以无时延地进入转发状态；如果是连接了三台以上交换机的共享链路则需要等待两倍 Forward Delay 的时间；

（3）直接与终端计算机相连而不是连接其它交换机的端口可以被配置为边缘端口（Edge Port），边缘端口可以直接进入转发状态而不需要任何时延。

2．RSTP 配置的有关命令

（1）开启 RSTP 协议

锐捷交换机默认状态是关闭 STP 协议，开启 STP 后的默认模式是 MSTP。

本次实验中开启 RSTP 的配置为：

Switch (config)# spanning-Tree

Switch (config)# spanning-tree mode rstp

（2）配置路径开销

路径开销是以时间为单位的，在交换机生成树计算中，当根交换机确定后，其它交换机将各自选择“最粗壮”的链路（路径开销总和最低）作为到根交换机的路径。表 3.11 列出了设备默认的路径开销。

表 3.11 路径开销

带 宽	IEEE802.1d	IEEE802.1w
10Mbps	100	2000000
100Mbps	19	200000
1000Mbps	4	20000

当端口路径开销为默认值时，交换机会根据端口速率计算出该端口的 Path cost。从表 3.9 中我们可以看出 802.1d 标准的取值范围为短整型（short：1～65535），802.1w 的取值范围为长整型（long：1～200000000）。管理员一定要统一好整个网络中 Path cost 的标准。锐捷交换机默认模式采用长整型。

配置端口路径开销的计算方法，设置值为长整型（long）或短整型（short），配置命令为：Switch (config)# spanning-tree path-cost method long/short

如果要恢复默认设置，可用 no spanning-tree path-cost method 全局配置命令设置；

配置端口路径开销的命令为：Switch (config-if)# spanning-tree cost <1-200000000>，默认值为根据端口的链路速率自动计算，速率高的开销小，如果管理员没有特别需要可不必更改它，因为这样计算出的 Path cost 最科学。

RSTP 的交换机优先级、端口优先级、BPDU 的时间选项和检测命令与 STP 下的配置相同，由于上节实验已经做了介绍，这里不复赘言。

3．实验环境与说明

（1）实验目的

掌握交换机 RSTP 的配置方法，理解 RSTP 协议的特点和相关概念。

（2）实验设备和连接

实验设备和连接图如图 3.18 所示，S3550 交换机间建立双链路连接，两台 S2126G 交换机分别连接两台 S3550 交换机并各与 1 台 PC 相连。

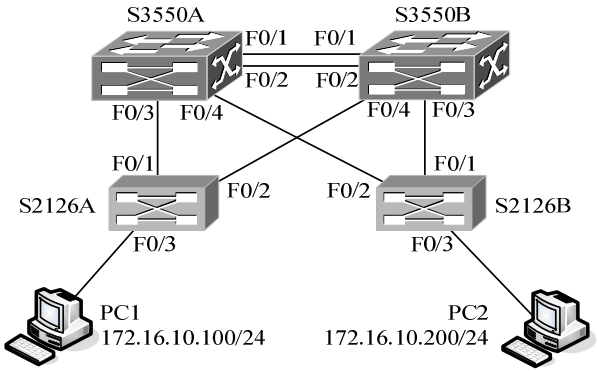


图 3.18 快速生成树 RSTP 的应用实验

（3）实验分组

每四名同学为一组，共同完成实验。

4．实验步骤

步骤 1：按照网络连接图完成设备连接，为防止实验过程中由于冗余链路可能导致的广播风暴的影响，可以在完成设备生成树协议配置之后再连接交换机间的冗余链路；

步骤 2：在每台交换机上启动生成树协议，例如在 S3550A 上进行配置：

```
S3550A# configure terminal
S3550A (config)# spanning-tree                    ！开启生成树协议
S3550A (config)# spanning-tree mode rstp          ！设置生成树为 RSTP（802.1W）
S3550A (config)# end
```

完成 SwitchA 的配置后，在 S3550B、S2126A 和 S2126B 上也做相同设置；

步骤 3：配置 S3550A 为根交换机：

```
S3550A (config)# spanning-tree priority 0         ！设置 SwitchA 的优先级为 0
```

步骤 4：配置 S3550A 和 S3550B 间的 F0/2 连接为主链路：

由于 S3550A 和 S3550B 间的 F0/1-F0/1、F0/2-F0/2 的路径开销相同，默认的端口优先级均为 128，因此 F0/1 链路将成为主链路（端口号较小）。如果要做出更改就必须更改端口优先级，可以在 S3550A 和 S3550B 上作出如下配置：

```
S3550A (config)# interface fastEthernet 0/2
S3550A (config-if)# spanning-tree port-priority 0     ！设置 F0/2 的端口优先级为 0
```

步骤 5：配置 S3550A 和 S2126A 间的端口速率为 10Mbps：

本次实验使用的交换机设备端口为快速以太口，指定 S3550A 为根交换机后，如果指定 S3550A 和 S2126A 间的端口速率为 10Mbps，S2126A 通过 F0/2 经 S3550B 的根路径开销将小于通过 F0/1 直连的路径开销，生成树的结构将因此而发生改变。我们这样做的目的也在于大家更好地理解生成树在网络中的建立过程。

在 Fastethernet 端口上设置速率的命令为：speed {10 | 100 | auto }，默认选项为 auto。

指定该链路速率为 10Mbps，可以在 S3550A 或 S2126A 上来做，以 S2126A 为例：

```
S2126A (config)# interface fastEthernet 0/1
S2126A (config-if)# speed 10
```

步骤 6：完成配置后分别在四台交换机上使用 show spanning-tree 和 show spanning-tree interface 验证配置，分析检测结果并回答下列问题。

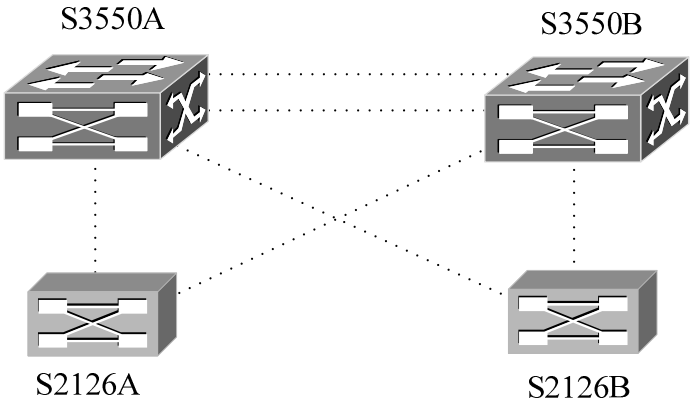
（1）写出 S3550A、S3550B、S2126A 和 S2126B 的桥标识符（Brideg ID），假若 S3550A 宕机，请判断哪一台设备将成为根交换机，为什么？

（2）根据检测结果填写表 3.12。

表 3.12 SwitchA 和 SwitchB 的接口 STP 对比

设备	S3550A				S2126A	
接口	F0/1	F0/2	F0/3	F0/4	F0/1	F0/2
PortRole						
PortState						
设备	S3550B				S2126B	
接口	F0/1	F0/2	F0/3	F0/4	F0/1	F0/2
PortRole						
PortState						

（3）根据表 3.12 的结果，在下图虚线上绘制生成树，并标出各个端口的类型（用 RP 表示根端口、DP 表示指定端口、AP 表示替换端口、BP 表示备份端口）。



（4）配置 PC1 和 PC2 的 IP 地址，验证网络拓扑发生变化时，ping 的丢失包的情况，对比上节实验有何差别？

第 4 章 路由器基础配置

4.1 路由器的基本配置

本节包括路由器基本配置、静态路由配置和利用 TFTP 管理路由器的配置。

4.1.1 路由器的基本配置实验

1．路由器简介

路由器是网络层设备，其工作模式与第二层交换相似，但路由器工作于 OSI 模型第三层，这个区别决定了路由和交换在转发数据时使用不同的控制信息，因为控制的 PDU 不同，实现功能的方式也不同。

路由器的本质功能在于：决定最优路由和转发数据包（网络层分组）。

路由器通过路由表来实现网络层路由功能，路由表中记录可以到达哪些网络以及数据分组去某个网络时下一步应该向哪里走。路由表的维护可以使用两种方法：静态路由和动态路由。作为专用的网际互连设备，路由器提供了强大的路由软件，可以适用于大规模的复杂网络结构；提供了丰富的接口类型，可以适用于各种 LAN/WAN 技术连接。同时由于可以处理更高层的 PDU，可以提供网络更高的安全管理手段。

在本书第一章中我们就已经了解到本书所基于的网络工程专业实验室的 RACK 单元中包括 4 台 RG-R1762 高性能安全模块化路由器，如图 4.1 所示。

图 4.1 RG-R1762 高性能安全模块化路由器

其主要性能如下：

- 连接接口：

包括 2 个 10M/100M 以太口，2 个高速同步口，1 个控制台口、1 个 AUX 口；

- 技术参数：

FLASH：8/72M；

SDRAM：64/320M；

包转发率：100kpps

2．路由器配置的相关知识

（1）RGNOS

在第 3 章实验中，我们已经了解了锐捷交换机的配置方法和相关概念。而本章，我们将了解路由器的有关配置。这里需要指出的是，锐捷系列路由器和交换机的网络操作系统平台被称为 RGNOS（Red-Giant Network Operating System）。

RGNOS 的系统文件（.bin）保存在设备 FLASH 中，在加电时加载到内存当中，RGNOS 在完成设备系统功能管理的同时，为用户提供统一的操作接口。由于以 IP 技术为核心，实现了组件化的软件体系结构，RGNOS 集成了众多先进核心技术特性，同时也兼容主流路由器和交换机产品的使用习惯。这也是目前众多大专院校的网络实验室锐捷产品的重要原因（当然，价格上的原因似乎更重要一些）。

在前面我们已经了解了基于交换机的 CLI 的有关内容和基本命令，本章将介绍关于路由器的内容。由于工作在网络层，牵扯到更多的管理项目，路由器配置所涉及的模式和命令远多于交换机，这些内容我们将逐渐了解。

关于设备的 Console 连接、CLI 命令模式、缩写和帮助功能，由于在第 3 章中已经做了介绍，这里不复赘言。

（2）路由器的存储体系

目前主流的路由器的存储体系包括 ROM、FLASH、DRAM 和 NVRAM，它们的主要功能如下：

ROM：相当于 PC 机的 BIOS

FLASH：相当于 PC 机硬盘，包含 IOS（锐捷路由器的管理软件称为 RGNOS）

DRAM：动态内存（当前配置，running-config）

NVRAM：配置文件（启动配置，startup-config）

注意：在锐捷交换机中没有 NVRAM 的概念，启动配置文件 config.text 和系统文件都记录在 FLASH 中。其实业界实现 NVRAM 的方式或者直接采用 FLASH 或者使用 RAM 加电的方法，这只是实现手段上的不同而已。

（3）模块化设备的接口表示

还记得第 3 章实验中，如何进入设备的接口模式吗？

Switch(config)# interface fastEthernet 0/1　　！进入快速以太口接口模式

路由器除提供局域网接口外，还提供了用于远程连接的广域网接口。RGNOS 目前支持的端口类型有 Ethernet、fastEthernet、Serial、Async、Loopback、Null、Tunnel、Group-Async、Dialer 等等，在非模块化设备上一般用 Type Number（接口类型 接口号）来标识端口。

模块化设备的接口标识为：

Type SlotNum/InterfaceNum（接口类型 插槽编号/端口编号）。

作为模块化设备，实验环境中的 R1762 的固定设备接口为两个 10/100M 以太接口：FastEthernet 1/0 和 FastEthernet 1/1；两个同步串口：Serial 1/2 和 Serial 1/3。其中 R1762-2 增加了扩展模块，提供两个同步串口：Serial 2/0 和 Serial 2/1。

（4）实验室 R1762 的串口连接

在实际使用中，路由器的 Serial 口可以连接同步 Modem，提供广域接入接入。（思考：物理层连接 DTE－DCE 模型）

在实验室中，使用 V.35 连接线连通设备同步串口。在实验中，为简化连线程序，学生实验采用实验台现有连接结构，如图 4.2 所示。

R1762-1 的 S1/2（DCE）连接 R1762-2 的 S1/2（DTE）；

R1762-3 的 S1/2（DCE）连接 R1762-2 的 S2/0（DTE）；

R1762-4 的 S1/2（DCE）连接 R1762-2 的 S2/1（DTE）；

注意：同步串口在使用 V.35 直连时连接线成对出现，DCE 端串口需要配置同步时钟。同学可以在 RACK 机柜底部看到 V.35 线对的连接。

如果实验室未提供所需连接，请注意在实验时应先连接好 Serial 口的 V.35 线对，再给设备加电，虽然厂商承诺 Serial 口是可以热插拔的，但建议还是最好不要这样做，以免接口损坏。

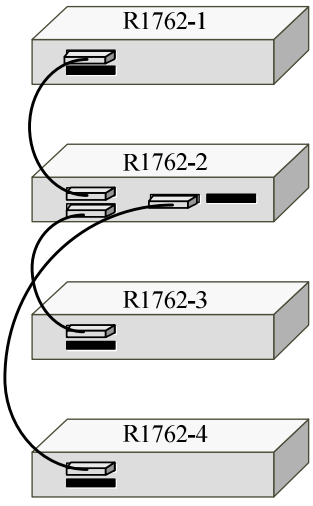


图 4.2 实验室 R1762 的连接

3．实验环境与说明

（1）实验目的

掌握路由器的基本配置，了解路由器的接口类型，掌握 CLI 的模式操作，配置路由器支持 Telnet，实现远程管理。

（2）实验设备和连接

实验设备和连接如图 4.3 所示，两台锐捷 R1762 路由器分别连接 1 台 PC，路由器之间串口相连。

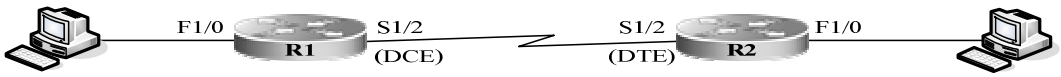


图 4.3 路由器基本配置实验

（3）实验分组

每四名同学为一组，一人一台路由器（R1762），协同完成实验。

4．实验步骤

步骤 1：连接配置

按照网络拓扑结构，在配线架上实现计算机和所选路由器 F1/0 接口的连线。由于不需要同学做串口连接，因此应当在实验开始前对设备作出合理的分组。实验室的 RACK 平台可以同时建立 3 组任务要求的网络结构，供 4 名同学同时实验。分组可参考如下：

表 4.1 路由实验分组参考

组号	PC1	PC2	R1-F1/0	R1-S1/2	R2-S1/2	R2-F1/0
1	N1	N2	R1762-1：F1/0	***R1762-1：S1/2***	***R1762-2：S1/2***	R1762-2：F1/0
2	N3	N2	R1762-3：F1/0	***R1762-3：S1/2***	***R1762-2：S2/0***	R1762-2：F1/0
3	N4	N2	R1762-4：F1/0	***R1762-4：S1/2***	***R1762-2：S2/1***	R1762-2：F1/0

注：斜体项为实验室预制连接，其它项同学可以自行定义。

按照上面的分组，配线架连线为 N1－R1F0、N2－R2F0、N3－R3F0、N4－R4F0。

由于三组连接实际上是互连在一起的，应当首先规划网络地址，避免冲突。可参考如下：

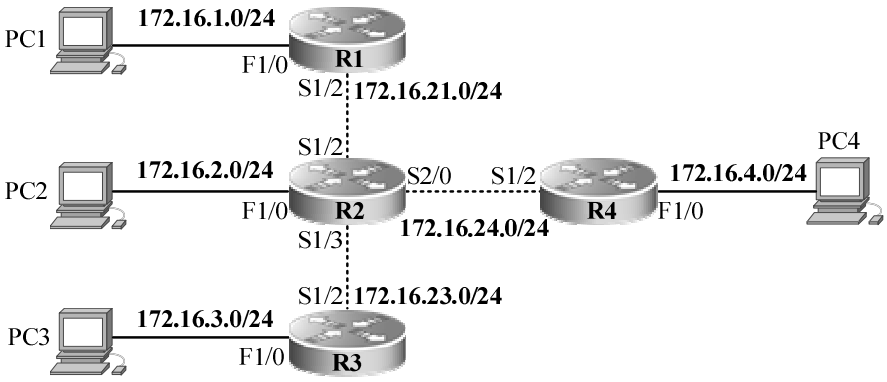


图 4.4 网络规划参考

如图 4.4 所示，1＃同学配置 PC1 和 R1762-1；2＃同学配置 PC2 和 R1762-2；3＃同学配置 PC3 和 R1762-3；4＃同学配置 PC4 和 R1762-4。在图 4.4 子网规划的基础上，确定各设备端口的 IP 地址，可参考下表：

表 4.2 实验设备接口 IP 参考

设备端口	IP 地址	设备端口	IP 地址
PC1	172.16.1.100	R1762-4：F1/0	172.16.4.1
PC2	172.16.2.100	R1762-1：S1/2	172.16.21.1
PC3	172.16.3.100	R1762-3：S1/2	172.16.23.1
PC4	172.16.4.100	R1762-4：S1/2	172.16.24.1
R1762-1：F1/0	172.16.1.1	R1762-2：S1/2	172.16.21.2
R1762-2：F1/0	172.16.2.1	R1762-2：S1/3	172.16.23.2
R1762-3：F1/0	172.16.3.1	R1762-2：S2/0	172.16.24.2

步骤 2：路由器配置

（1）配置路由器主机名

```
router> enable                          ！从用户模式进入特权模式
router# configure terminal              ！从特权模式进入全局配置模式
router (config)# hostname R1            !以 R1762-1 为例，将主机名配置为“R1”
R1(config)#
```

（2）配置路由器远程登陆密码

```
R1(config)# line vty 0 4                ！进入路由器虚拟终端线路 0 到 4
R1 (config-line)# login
R1 (config-line)# password star         ！将路由器远程登陆口令设置为“star”
```

（3）配置路由器特权模式口令

```
R1(config)# enable password 0 star      ！将路由器特权模式口令配置为“star”
或：R1(config)# enable secret 0 star    ！口令加密，优先级更高
```

（4）为路由器各接口分配 IP 地址

```
R1(config)# interface serial 1/2
R1(config-if)# ip address 172.16.21.1 255.255.255.0
    ！设置路由器 serial 1/2 的 IP 地址为 172.16.21.1，对应的子网掩码为 255.255.255.0
R1(config-if)# no shutdown              ！启用端口
R1 (config-if)# interface fastethernet 1/0
R1 (config-if)# ip address 172.16.1.1 255.255.255.0
    ！设置路由器 fastethernet 1/0 的 IP 地址为 172.16.1.1，对应的子网掩码为
255.255.255.0
R1(config-if)# no shutdown              ！启用端口
```

注意：设备端口默认为 shutdown，配置使用时记得要 no shutdown。

（5）配置接口时钟频率（DCE）

```
R1(config)# interface serial 1/2
R1(config-if) clock rate 64000          ！设置接口物理时钟频率为 64Kbps
```

注意：只在 V.35 DCE 连接端设置。

以上是 R1762-1 设备的基本配置，R1762-3 和 R1762-4 的配置与此相同，仅仅是设备名和端口 IP 参数的差别，这里不复赘言。

R1762-2 由于网络连接和设备接口的差别，应注意与前面配置的区别。可参考如下：

```
router> enable
router# configure terminal
router (config)# hostname R2            ！将主机名配置为“R2”
R2(config)#
R2(config)# enable secret star          ！将路由器特权模式口令配置为“star”
R2(config)# line vty 0 4                ！将路由器远程登陆口令设置为“star”
R2 (config-line)# login
R2 (config-line)# password star
R2 (config-line)# exit
R2(config)#
```

```
！设置路由器 fastethernet 1/0 的 IP 地址为 172.16.2.1，对应的子网掩码为 255.255.255.0
R2 (config)# interface fastethernet 1/0
R2 (config-if)# ip address 172.16.2.1 255.255.255.0
R2(config-if)# no shutdown
！设置路由器 serial 1/2 的 IP 地址为 172.16.21.2，对应的子网掩码为 255.255.255.0
R2(config)# interface serial 1/2
R2(config-if)# ip address 172.16.21.2 255.255.255.0
R2(config-if)# no shutdown
！设置路由器 serial 1/3 的 IP 地址为 172.16.23.2，对应的子网掩码为 255.255.255.0
R2(config)# interface serial 1/3
R2(config-if)# ip address 172.16.23.2 255.255.255.0
R2(config-if)# no shutdown
！设置路由器 serial 2/0 的 IP 地址为 172.16.24.2，对应的子网掩码为 255.255.255.0
R2(config)# interface serial 2/0
R2(config-if)# ip address 172.16.24.2 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# end
！保存配置（如果特权密码设置不是 star，不要保存）
R2# copy running-config startup-config
Building configuration...
[OK]
R2#
```

可以看出，R1762-2 为了与另外两组设备连通，多配置了两个串口；同时由于同步串口连接 V.35 DTE 端，不设接口时钟。

步骤 3：配置计算机

将计算机 2＃网卡配置为指定 IP，网关设置为对应路由器的 F1/0 的 IP。

步骤 4: 在路由器特权模式下执行 show running-config 查看当前配置，执行 show interface 命令查看端口状态统计信息。

以 show interface 为例，执行如下：

```
R1#show interface serial 1/2
serial 1/2 is UP , line protocol is UP  ①
Hardware is PQ2 SCC HDLC CONTROLLER serial
Interface address is: 172.16.21.1/24  ②
   MTU 1500 bytes, BW 2000 Kbit  ③
   Encapsulation protocol is HDLC, loopback not set  ④
   Keepalive interval is 10 sec , set
   Carrier delay is 2 sec
   RXload is 1 ,Txload is 1
   Queueing strategy: WFQ
   5 minutes input rate 17 bits/sec, 0 packets/sec
   5 minutes output rate 17 bits/sec, 0 packets/sec
      19 packets input, 418 bytes, 0 no buffer
      Received 19 broadcasts, 0 runts, 0 giants
      1 input errors, 0 CRC, 0 frame, 0 overrun, 1 abort
```

18 packets output, 396 bytes, 0 underruns
0 output errors, 0 collisions, 149 interface resets
1 carrier transitions
V35 DTE cable
DCD=up DSR=up DTR=up RTS=up CTS=up

其中①为端口状态，网络连通时为端口 up，协议 up；②为端口 IP 地址；③为带宽；④为端口封装类型。除此以外，该命令还有查看数据流量统计等其它功能。

验证路由器所配置的端口为 up, up

步骤 5：综合验证

（1）两台路由器互相 ping 对方的 Serial 口的地址，应该为通；

路由器上 ping 命令的格式为 ping *hostname|IP address*

其功能是从一台主机探测与另一台主机的连通性，以验证网络是否正常运行，是最常使用的故障诊断命令。命令发出后，探测方发出 5 个回应请求报文，如果网络正常运行将返回一组 ICMP 回应应答报文（echo）。ICMP 消息以 IP 数据包传输，因此接收到 ICMP 回应应答消息即可证明第三层以下的连接都工作正常。

简单的 IP ping 既可以在用户模式下执行，也可以在特权模式下执行。正常情况下，对方会返回 5 个回应请求，5 个惊叹号表明所有的请求都成功地接收到了，返回信息出中还包括最大、最小和平均往返时间等。

每一个“！”表明一个 echo 请求被成功的接受，如果不是“!”号，则表明 echo 请求未被接收到的原因有：. -请求超时，U-目的不可达，P-协议不可达，N-网络不可达，Q-源抑制，M-不能分段，？-不可知报文类型。例如：

R1# ping 172.16.21.2　　！从 R1762-1 上 ping R1762-2 的 S1/2 接口
Sending 5, 100-byte ICMP Echoes to 172.16.21.2, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

（2）两台主机分别 ping 与其直连的路由器的 Fastethernet 口，应为通；

（3）从与 R1 相连的主机可以 telnet 到 R1，与 R2 相连的主机可以 telnet 到 R2；

（4）4 台 PC 之间互相 ping，应该为不通。

4.1.2 路由器的静态路由配置实验

1．静态路由

上一节实验的配置并不能解决计算机之间的连通问题，端口配置后，路由器只能解决直连网络的连通。要想实现相隔网络之间的连通，就必须让路由器建立远程网络的路由记录。

路由器维护路由表的方式有两种：静态路由和动态路由。

- 静态路由是在路由器中设置的固定的路由表。除非网络管理员干预，否则静态路由不会发生变化。
- 动态路由是网络中的路由器之间相互通信，传递路由信息，利用收到的路由信息更新路由表的过程。它能实时地适应网络结构的变化。

静态路由是指由网络管理员手工配置的路由信息。静态路由除了具有简单、高效、可靠的优点外，它的另一个好处是网络安全保密性高。

静态路由的一般配置步骤为：

（1）为每条链路确定地址（包括子网地址和网络地址）；

（2）为每个路由器，标识非直连的链路地址；

（3）为每个路由器写出未直连的地址的路由语句（写出直连地址的语句是没必要的）。

配置静态路由使用命令 ip route，基本格式如下：

router(config)# ip route [网络编号] [子网掩码] [转发路由器的 IP 地址/本地接口]

2．实验环境与说明

（1）实验目的

在 4.1.1 实验完成的基础上，配置静态路由，实现网络连通。要求掌握静态路由的规划和相关配置。

（2）实验设备和连接

实验设备和连接与 4.1.1 实验相同，建议参考图 4.4。

（3）实验分组

每四名同学为一组，一人一台路由器（R1762），协同完成实验。

3．实验步骤

步骤 1：完成上次实验的设备配置，可参考 4.1.1 实验的步骤 1、步骤 2 和步骤 3。

要求完成路由器的基本配置（设备名、特权口令设置）、相关接口配置（IP 地址、启用、DCE 时钟）和验证计算机的 IP 配置。

步骤 2：路由规划：

图 4.4 网络规划中已经给出了网络拓扑中每个网段的子网地址，选择第一组连接设备如图 4.5 所示：

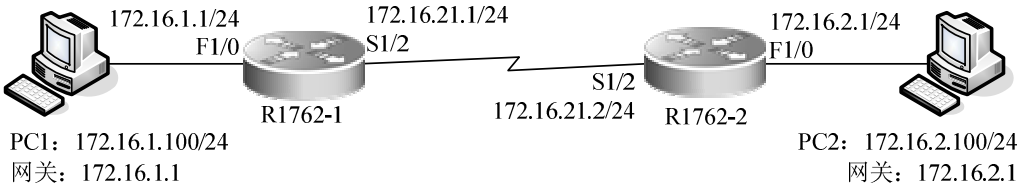


图 4.5 第一组拓扑参考

可以看出网络中共有 172.16.1.0/24，172.16.21.0/24，172.16.2.0/24 三个子网。其中 R1762-1 直连 172.16.1.0/24 和 172.16.21.0/24，R1762-2 直连 172.16.21.0/24 和 172.16.2.0/24。确定未直连的网络为：R1762-1 为 172.16.2.0/24，R1762-2 为 172.16.1.0/24。

以 R1762-1 为例，确定到达 172.16.2.0/24 网络的网关地址为 172.16.21.2；同样 R1762-2 到达 172.16.1.0/24 网络的网关地址为 172.16.21.1。思考并回答下面问题：

静态路由是怎样确定的？路由记录中网关地址是什么？

步骤 3：静态路由配置：

R1762-1 配置为：

```
R1(config)# ip route 172.16.2.0 255.255.255.0 172.16.21.2        ！配置静态路由
R1(config)# end
```

验证配置使用 show ip route 命令

```
R1# show ip route                                                  ！查看路由表
Codes:   C - connected, S - static,    R - RIP
         O - OSPF, IA - OSPF inter area
         N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
         E1 - OSPF external type 1, E2 - OSPF external type 2
         * - candidate default
Gateway of last resort is no set
```

C　　172.16.1.0/24 is directly connected, FastEthernet1/0

C　　172.16.21.0/24 is directly connected, serial 1/2

S　　172.16.2.0/24 [1/0] via 172.16.21.2　　！静态路由记录

R1762-2 配置为：

R2(config)# ip route 172.16.1.0 255.255.255.0 172.16.21.1　　！配置静态路由

注意：静态路由两端都要配置。上面仅给出了 R1762-2 和 R1762-1 的连接配置，R1762-2 和 R1762、R1762-4 的连接配置请根据网络规划自己确定。

步骤 4：实验验证：

PC1 和 PC2 之间可以相互 ping 通；

步骤 5：综合练习：

参考以上配置，结合图 4-6，实现全网连通。提示：R1762-2 需要配置 3 个未直连网络路由，而 R1762-1、R1762-3 和 R1762-4 则各需要配置 5 个未直连网络的静态路由。

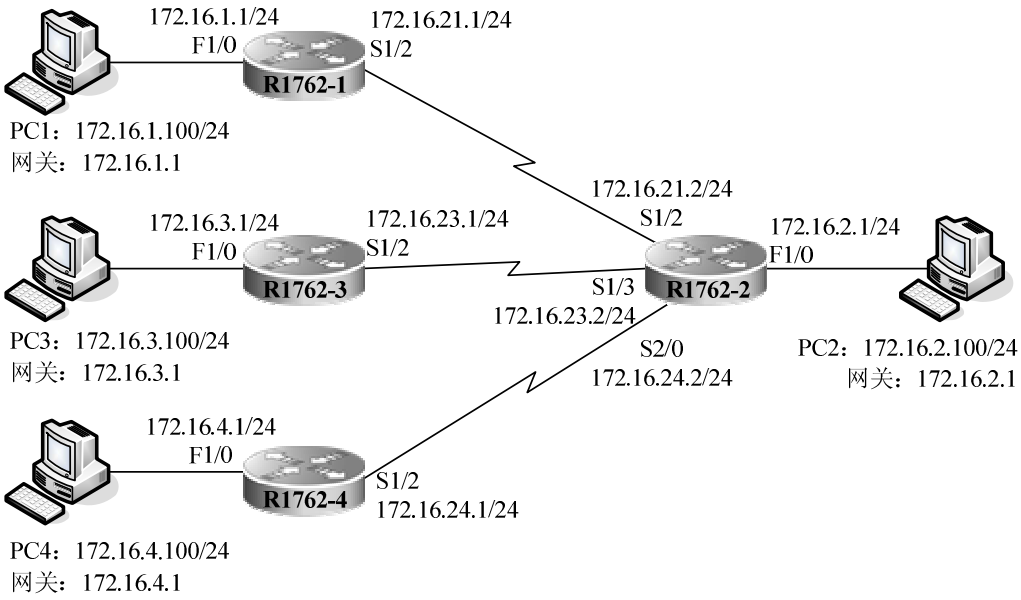


图 4.6 静态路由实验全网连接拓扑

根据图 4.6 确定要实现全网连通，路由器上要配置的全部静态路由，填写表 4.3。

表 4.3 实验需要配置的静态路由

设备	目的网络地址	目的网络掩码	下一跳地址
R1762-1			
R1762-2			
R1762-3			

R1762-4			
设备	目的网络地址	目的网络掩码	下一跳地址

在配置完成后，在路由器上执行 show ip route 可以看到全网路由记录，所有主机、路由器接口均可 ping 通。

步骤 6：配置缺省路由：

从图 4.6 中，我们可以发现 R1762-1、R1762-3 和 R1762-4 的对外出口只有一条链路，它们的静态路由指定的下一跳地址也是固定的，这种情况下，我们可以通过缺省路由来简化配置。缺省路由的配置命令为：ip route 0.0.0.0 0.0.0.0 [转发路由器的 IP 地址/本地接口]

在 R1762-1、R1762-3 和 R1762-4 上使用 no 选项删除已经建立的静态路由（no ip route *network-number network-mask* [*ip-address* | *interface-id* [*ip-address*]]），例如：

R1(config)# no ip route 172.16.2.0 255.255.255.0 172.16.21.2

在执行 show ip route 确认配置的静态路由已经删除的情况下，执行缺省路由的配置操作，以 R1762-1 为例：

R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.21.2　　！配置缺省路由

在完成在 R1762-1、R1762-3 和 R1762-4 的配置后，验证全网仍然连通。

4.1.3 路由器的动态路由－RIP 配置实验

1．动态路由

实验 4.1.2 中路由器的静态路由配置可以实现网络连通。静态路由在单一链路或简单网络结构中非常适用，但静态路由完全依赖于管理员的手动配置，当网络规模较大时、存在链路冗余或存在变动时，静态路由配置就成为一件费力不讨好的事情。在大型、复杂网络结构中，我们是通过动态路由来实现网络连通的。

动态路由是指路由器能够自动地建立自己的路由表，并且能够根据实际情况的变化适时地进行调整。动态路由协议被分为两类：

（1）外部网关协议（EGP）：

在自治系统之间交换路由选择信息的互联网络协议，如 BGP。

（2）内部网关协议（IGP）：

在自治系统内交换路由选择信息的路由协议，常用的因特网内部网关协议有 OSPF、RIP、IGRP、EIGRP。

其中，RIP 协议是应用较早、使用较普遍的内部网关协议（Interior Gateway Protocol,简称 IGP），适用于小型同类网络，是典型的距离矢量（distance-vector）协议。

2．RIP 协议简介

路由信息协议（Routing Information Protocols，RIP）是由施乐 Xerox 在 70 年代开发的，其前身是 Xerox 协议 GWINFO。国际上关于 IP RIP 在两个文档中有正式定义：RFC 1058 和 1723。RFC 1058（1988）描述了 RIP 的第一版实现，RFC 1723（1994）是它的更新，允许 RIP 分组携带更多的信息和安全特性。实验室设备 R1762 支持 RIPv2 配置，但我们本节实验只涉及 RIPv1 的基本配置。

（1）RIP 的工作原理

RIP 以规则的时间间隔及在网络拓扑改变时发送路由更新信息（基于 UDP 广播）。当路由器收到包含某表项的更新的路由更新信息时，就更新其路由表：该路径的 metric 值加上 1，发送者记为下一跳地址（网关地址）。

RIP 路由器只维护到目的的最佳路径（具有最小 metric 值的路径）。更新了自己的路由表后，路由器立刻发送路由更新把变化通知给其它路由器，这种更新（触发更新）是与周期性发送的更新信息无关的。

在 RIP 协议中，规定了最大跳级数为 15，如果从网络的一个终端到另一个终端的路由跳数超过 15 个，就被认为牵涉到了循环，因此当一个路径达到 16 跳，将被认为是达不到的，继而从路由表中删除。

默认配置下，RIP 协议每隔 30 秒定期向外发送一次更新报文。RIP 对每条路由有一个计时器，当收到新的有关这条路由的消息时，该计时器被重置；如果计时器超时（默认值为 180 秒）没有收到来自某一路由器的路由更新报文，则将所有来自此路由器的路由信息标志为不可达，若在其后 240 秒内仍未收到更新报文，就将这些路由从路由表中删除。

为了防止路由环路的出现（无穷计数问题），RIP 通过设置最大跳级数，实现水平分割、毒性反转，结合触发更新和抑制规则，保证了路由计算的有效收敛。

（2）RGNOS 中配置 RIP 协议的一般步骤为：

第一步：启用 RIP 进程

```
router(config)# router rip
router(config-router)#
```

第二步：配置 network 命令

```
router(config-router)# network <主类网络号>
```

其含义为：1）公布属于该主类的子网；

2）包含在该主类内的接口将发送和接收路由信息

第三步：配置均衡负载（代价相等）

```
router(config-router)# maximum-paths <1-6>                ！缺省为“4”
```

第四步：配置 RIP 发布初始度量值

```
router(config-router)#default-metric <1-4294967295>       ！缺省为 5，建议设置为 1
```

我们在本节实验中只涉及第一和第二步，maximum-paths 和 default-metric 使用默认配置。

（3）RGNOS 中 RIP 的调试可以采用以下命令：

```
router# show ip protocols                ！验证 RIP 的配置
router# show ip route                    ！显示路由表的信息
router# clear ip route                   ！清除 IP 路由表的信息
router# debug ip rip                     ！在控制台显示 RIP 的工作状态
```

3．实验环境与说明

（1）实验目的

在 4.1.1 实验完成的基础上，配置 RIP 协议，实现网络连通。

（2）实验设备和连接

实验设备和连接与 4.1.1 实验相同，建议参考图 4.4。

（3）实验分组

每四名同学为一组，一人一台路由器（R1762），协同完成实验。

4．实验步骤

步骤 1：完成 4.1.1 实验的设备配置，可参考 4.1.1 实验的步骤 1、步骤 2 和步骤 3。

要求完成路由器的基本配置（设备名、特权口令设置）、相关接口配置（IP 地址、启用、

DCE 时钟）和验证计算机的 IP 配置。

步骤 2：实验分析

分析图 4.4，我们可以知道：

R1762-1 直连 172.16.1.0/24 和 172.16.21.0/24；

R1762-2 直连 172.16.2.0/24、172.16.21.0/24、172.16.23.0/24 和 172.16.24.0/24；

R1762-3 直连 172.16.3.0/24 和 172.16.23.0/24；

R1762-4 直连 172.16.4.0/24 和 172.16.24.0/24。

这些直连网络就是路由器在启动 RIP 时需要公布的网络。

步骤 3：RIP 配置

S1762-1 为：

```
R1(config)# router rip                          ！启用 RIP 进程
R1(config-router)# network 172.16.1.0           ！公布直连网络
R1(config-router)# network 172.16.21.0          ！公布直连网络
R1(config-router)# end
```

S1762-2 为：

```
R2(config)# router rip                          ！启用 RIP 进程
R2(config-router)# network 172.16.2.0           ！公布直连网络
R2(config-router)# network 172.16.21.0          ！公布直连网络
R2(config-router)# network 172.16.23.0          ！公布直连网络
R2(config-router)# network 172.16.24.0          ！公布直连网络
R2(config-router)# end
```

S1762-3 为：

```
R1(config)# router rip                          ！启用 RIP 进程
R1(config-router)# network 172.16.3.0           ！公布直连网络
R1(config-router)# network 172.16.23.0          ！公布直连网络
R1(config-router)# end
```

S1762-4 为：

```
R1(config)# router rip                          ！启用 RIP 进程
R1(config-router)# network 172.16.4.0           ！公布直连网络
R1(config-router)# network 172.16.24.0          ！公布直连网络
R1(config-router)# end
```

步骤 4：综合验证

（1）验证接口

RIP 协议规定包含在公布网络内的接口将发送和接收路由信息，这些接口的状态应当是 UP 的，可以通过 show ip interface 命令查看接口，例如在 R1762-1 上执行如下命令：

```
R1# show ip interface brief                     ！显示接口的摘要信息
Interface                IP-Address(Pri)    OK?     Status
serial 1/2               172.16.21.1/24     YES     UP
serial 1/3               no address         YES     DOWN
FastEthernet 1/0         172.16.1.1/24      YES     UP
FastEthernet 1/1         no address         YES     DOWN
Null 0                   no address         YES     UP
R1#
```

在四台路由器上分别执行该命令，确定设备接口的状态。

（2）验证路由表

配置 RIP 协议的目的是建立动态路由，我们可以使用 show ip route 命令查看结果：

R1# show ip route　　！查看 R1762-1 的路由表

显示结果如下：

```
Codes:  C - connected, S - static,   R - RIP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        * - candidate default
Gateway of last resort is no set
C       172.16.1.0/24 is directly connected, FastEthernet 1/0
C       172.16.1.1/32 is local host.
R       172.16.2.0/24 [120/1] via 172.16.21.2, 00:00:27, serial 1/2
R       172.16.3.0/24 [120/2] via 172.16.21.2, 00:00:27, serial 1/2
R       172.16.4.0/24 [120/2] via 172.16.21.2, 00:00:27, serial 1/2
C       172.16.21.0/24 is directly connected, serial 1/2
C       172.16.21.1/32 is local host.
R       172.16.23.0/24 [120/1] via 172.16.21.2, 00:00:27, serial 1/2
R       172.16.24.0/24 [120/1] via 172.16.21.2, 00:00:27, serial 1/2
```

R2# show ip route　　！查看 R1762-2 的路由表

```
Codes:  C - connected, S - static,   R - RIP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        * - candidate default
Gateway of last resort is no set
R       172.16.1.0/24 [120/1] via 172.16.21.1, 00:00:27, serial 1/2
C       172.16.2.0/24 is directly connected, FastEthernet 1/0
C       172.16.2.1/32 is local host.
R       172.16.3.0/24 [120/1] via 172.16.23.1, 00:00:22, serial 1/3
R       172.16.4.0/24 [120/1] via 172.16.24.1, 00:00:29, serial 2/0
C       172.16.21.0/24 is directly connected, serial 1/2
C       172.16.21.2/32 is local host.
C       172.16.23.0/24 is directly connected, serial 1/3
C       172.16.23.2/32 is local host.
C       172.16.24.0/24 is directly connected, serial 2/0
C       172.16.24.2/32 is local host.
```

R1762-3 和 R1762-3 的执行结果与 R1762-1 相近，这里不在列出。路由表中标有 R 的项目就是设备通过 RIP 协议自动建立的路由记录。以 R1762-1 的第 1 条 R 记录为例：

172.16.1.0/24 [120/1] via 172.16.21.1, 00:00:27, serial 1/2

- 172.16.1.0/24 表明目的网络；
- [120/1]中 120 为管理代价（标识路由信息源的可信度，例如 RIP 为 120、直连网络为 0），1 为跳级数（RIP 协议的度量参数）

- 172.16.21.1 为转发路由器的 IP 地址；
- 00:00:27 是该记录已存活的时间（递增值）；
- serial 1/2 为本地接口。

（3）验证 RIP 的工作过程

在 RIP 配置中，可以使用 debug ip rip 来显示 RIP 的工作状态，用来调试分析。

在 R1762-1、R1762-2 和 R1762-3 上执行下面的命令：

```
R1# debug ip rip event                                    ！在控制台显示 RIP 事件
```

控制台将周期性的显示下面的信息（这是 R1762-1 上的观测结果，R1762-2 和 R1762-3 会有所区别）：

```
RIP: rip recveive packet. src: 172.16.21.2
peer exist
RIP: received response packet.
RIP: send response
RIP: send len: 24 ifin
RIP: send response
RIP: send len: 124 ifindex: 2
RIP: rip recveive packet. src: 172.16.21.2
peer exist
RIP: received response packet.
RIP: rip recveive packet. src: 172.16.21.2
peer exist
RIP: received response packet.
```

关于 RIP 的协议分析，在本书的后面会具体提到，这里暂不考虑。请观察几组 RIP 事件信息，测量一下间隔时间是多少？如果中间将 R1762-2 的 F1/0 口的连线断开（或接上），显示时间上会有什么变化吗？分析其中的差别和目的？

4.1.4 利用 TFTP 服务器备份和恢复路由器配置实验

我们在前面的 3.1.3 实验中已经了解了利用 TFTP 服务器备份和恢复交换机配置的有关操作，这里我们练习使用 TFTP 服务器备份和恢复路由器的配置。一般而言，路由器涉及到更多的配置，作为实现网络三层连接的重要设备，路由器承担着网络互连、甚至网络安全的重要任务，一旦配置文件损坏，其结果的严重性可想而知。

1．Copy 命令

我们在 3.1.3 中已经介绍过 RGNOS 中的 copy 命令，我们知道，该命令格式为：

copy *source-url destination-url*

copy 命令可以用于 IOS 及 CONFIG（配置文件）的备份和升级，在 R1762 路由器特权模式下执行命令帮助语句可以看到如下结果：

```
router# copy ?                                            ！查看 copy 命令 source-url 参数
  flash:           Copy from flash: file system
  running-config   Copy from current system configuration
  startup-config   Copy from startup configuration
  tftp:            Copy from tftp: file system
R1762# copy running-config ?                              ！查看 copy 命令 destination-url 参数
  flash:           Copy to flash: file system
```

running-config	Update (merge with) current system configuration
startup-config	Copy to startup configuration
tftp:	Copy to tftp: file system

我们可以看到，在 R1762 路由器上 copy 命令指定的源位置和目标位置可以是以下四个参数之一：

表 4.4 R1762 中支持的 copy 命令参数

flash:	FLASH（闪存），用于存放系统文件
running-config	DRAM（动态随机存储器），记录当前配置
startup-config	非易失性随机存储器（NVRAM），存放启动配置
tftp:	TFTP 服务器

注意：锐捷的 R1762 路由器没有设置单独的 NVRAM，启动配置文件记录在 FLASH 中，即 flash:config.text（别名为 startup-config），路由器在设备启动时加载启动配置文件。

Copy 命令的图解如下：

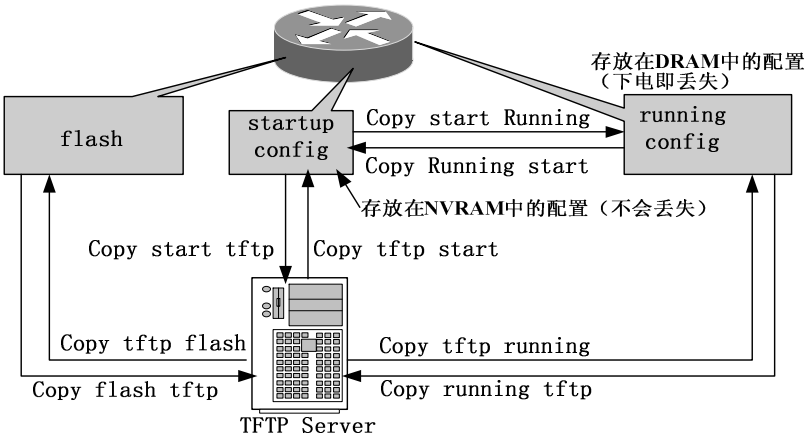


图 4.7 Copy 命令的图解示意

具体的配置命令如下：

（1）copy running-config startup-config	！将运行配置文件复制到 NVRAM 中去
（2）copy startup-config running-config	！用 NVRAM 中的配置覆盖 DRAM 中的配置
（3）copy startup-config tftp:	！将 NVRAM 中的配置复制到 tftp 服务器中
（4）copy running-config tftp:	！将 DRAM 中的配置复制到 tftp 服务器中
（5）copy tftp: running-config	！将 tftp 中的文件复制到路由器的 DRAM 中
（6）copy tftp: startup-config	！将 tftp 中的文件复制到路由器 NVRAM 中
（7）write / erase	！写入/删除 NVRAM 中的配置文件

在配置命令中参数 running-config 表示将配置存放在 DRAM 中。startup-config 表示将配置存放在 NVRAM 中。在设备配置过程中，任何命令只要键入后立即存入 DRAM 并运行，但掉电后会丢失。只有存放在 NVRAM 中的配置，在重新启动之后才会被复制到 DRAM 中运行，因此在确认配置正确无误后，应当使用命令 copy running-config startup-config 或 write memory 保存配置。

关于 TFTP 服务器，这里仍然使用锐捷提供的 Trivial FTP Server，3.1.3 实验说明中已经对此做过介绍，这里不复赘言。

2．实验环境与说明

（1）实验目的

掌握通过 TFTP 服务器备份和还原路由器配置的方法。

（2）实验设备和连接

实验设备和连接如图 4.8 所示，一台锐捷 R1762 路由器连接 1 台 PC 机，路由器命名为 R1762。

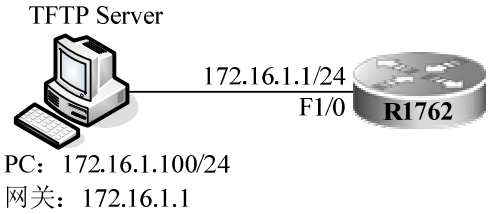


图 4.8 利用 TFTP 服务器备份和恢复路由器配置实验

（3）实验分组

每四名同学为一组，一人一台路由器（R1762），每人各自独立完成实验。

4．实验步骤

步骤 1：在路由器上完成如下配置：

```
router (config)# hostname R1 762                    ！将设备名配置为 R1762
R1762(config)# enable secret 0 star                 ！将特权模式口令配置为 star
R1762(config)# interface fastethernet 1/0           ！配置 fastethernet 1/0 接口
R1762(config-if)# ip address 172.16.1.1 255.255.255.0
R1762(config-if)# no shutdown
```

完成后，执行 copy running-config startup-config 或 write memory 保存配置，例如：

```
R1762# copy running-config startup-config
Building configuration...
[OK]
```

执行 show running-config 和 show startup-config 查看配置记录：

```
R1762# show running-config
Building configuration...
Current configuration : 713 bytes
!
version 8.32(building 53)
hostname R1762                                      ！设备名为 R1762
enable secret level 14 5 $1$df32$v546ADtx41856yvz
enable secret 5 $1$yLhr$4tvyAFDzpz4ywypr            ！特权模式口令配置为 star（密文）
!
interface serial 1/2
 clock rate 64000
!
interface serial 1/3
 clock rate 64000
!
interface FastEthernet 1/0                          ！fastethernet 1/0 接口配置
 ip address 172.16.1.1 255.255.255.0
 duplex auto
 speed auto
```

```
!
interface FastEthernet 1/1
 duplex auto
 speed auto
!
……<后面内容略去>
```

步骤 2：配置 PC 机 IP 地址为 172.16.1.100，运行 Trivial FTP Server，验证路由器与 TFTP 服务器的连通性。

我们在前面已经在路由器上执行过简单 ping 命令了，这里推荐大家使用扩展 ping 命令。与简单 ping 命令既可以在用户模式也可以在特权模式下执行不同，扩展 ping 命令只能在特权模式下执行。

扩展的 ping 命令适用于任何一种桌面协议。它包含更多的功能属性，因此可以获得更为详细的信息。通过这些信息我们可以分析网络性能下降的原因而不单单是服务丢失的原因。扩展的 ping 命令的执行方式也是敲入 ping。其使用方法如下所示：

```
R1# ping                                          ！执行扩展 ping
Protocol [ip]:                                    ！需要测试的协议，默认为 IP，直接回车
Target IP address: 172.16.1.100                   ！指定测试的目标地址
Repeat count [5]: 10                              ！指定 ping 的重复次数，默认为 5
Datagram size [100]: 2000
```

！指定报文大小，默认为 100B，如果怀疑报文由于延迟过长或者分片失败而丢失，可以提高报文的大小。例如，使用 2000B 报文来强制分片。

```
Timeout in seconds [2]:
```

！指定超时时间，默认 2 秒，如果怀疑超时是由于响应过慢而不是报文丢失，则可以提高该值，否则可以直接回车

```
Extended commands [n]: y
```

！回答 y 以获得扩展属性，默认为 n，跳过扩展属性项

```
Source address:172.16.1.1                         ！指定源地址，必须是路由器的启用接口
Sending 10, 2000-byte ICMP Echoes to 172.16.10.2, timeout is 2 seconds:
   < press Ctrl+C to break >
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 519/519/520 ms
```

步骤 3：备份路由器的配置：

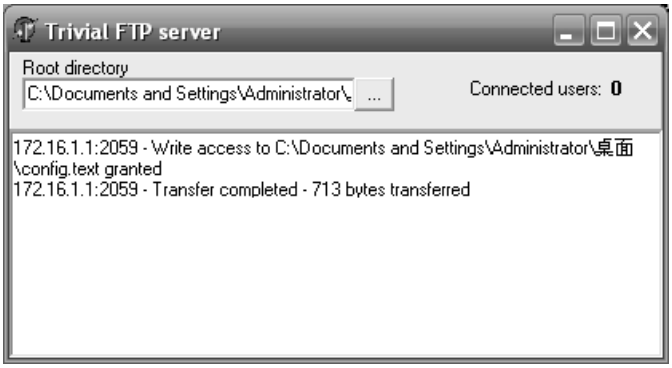


图 4.9 Trivial TFTP 界面

```
R1762# copy startup-config tftp:                  ！备份路由器的启动配置到 TFTP 服务器
Address or name of remote host []?172.16.1.100    ！指定 TFTP 服务器的 IP 地址
```

Destination filename [config.text]? ！提示选择要保存的文件的名称
Accessing tftp://172.16.1.100/config.text...
Success : Transmission success,file length 713 ！传输成功，文件长 713 字节

与此同时，可以在 TFTP 服务器端窗口看到状态提示信息，如图 4.9 所示：

在 TFTP 服务器系统目录下找到 config.text 文件，用记事本打开，对比刚才路由器上查看配置记录的结果，会发现这就是路由器的配置文件。

步骤 4：删除路由器的启动配置：

执行 erase 命令或 delete 删除路由器的启动配置，命令如下：

R1762# erase startup-config

或 R1762# delete flash:config.text

注意：不要用 delete 命令去删除 FLASH 中的其它文件，尤其是 rgnos.bin（IOS 系统文件），否则将造成设备无法启动，擅自操作将为实验室管理工作造成麻烦，引起的后果自负。

之后，重启路由器，执行如下：

R1762# reload ！重启设备
Proceed with reload? [confirm] ！提示是否重启，输入 y 回车

等待路由器重启结束后，由于删除了 config.text 启动配置文件，设备将还原为出厂状态：

Red-Giant> ！锐捷路由器的默认设备名
Red-Giant> enable ！特权口令为空
Red-Giant#

步骤 5：将 TFTP 服务器保存的配置加载到路由器：

重新配置 F1/0 接口，执行如下：

Red-Giant# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Red-Giant(config)# interface fastEthernet 1/0
Red-Giant(config-if)# ip address 172.16.1.1 255.255.255.0
Red-Giant(config-if)# no shutdown

完成之后，回到特权模式下，执行将 TFTP 服务器保存的配置加载到路由器的操作：

Red-Giant# copy tftp: startup-config ！拷贝 TFTP 服务器到路由器的启动配置
Address or name of remote host []?172.16.1.100 ！指定 TFTP 服务器的 IP 地址
Source filename []?config.text ！指定要读取的文件的名称
Accessing tftp://172.16.1.100/config.text...
Write file to flash: !
Write file to flash successfully!
Success : Transmission success,file length 713 ！文件复制成功

执行 show startup-config 可以看到启动配置已经被复原。

如果执行 copy tftp: running-config 则会看到：

Red-Giant# copy tftp running-config ！拷贝 TFTP 服务器到路由器的当前配置
Address or name of remote host []?172.16.1.100 ！指定 TFTP 服务器的 IP 地址
Source filename []?config.text ！指定要读取的文件的名称
Accessing tftp://172.16.1.100/config.text...
Success : Transmission success,file length 713 ！复制成功
R1762# ！提示符已经更改，配置复原

执行 show running-config 可以看到当前配置已经被复原。在执行了上面的操作后，可以

看到 Trivial TFTP 界面会显示如下的提示信息：

172.16.1.1:2057 - Read access to C:\Documents and Settings\Administrator\桌面\config.text granted

172.16.1.1:2057 - Transfer completed - 713 bytes transferred

172.16.1.1:2059 - Read access to C:\Documents and Settings\Administrator\桌面\config.text granted

172.16.1.1:2059 - Transfer completed - 713 bytes transferred

思考题：

1）为什么将 TFTP 服务器保存的配置加载到路由器时，在执行 copy 命令之前要重新配置 F1/0 接口？

2）如果只执行 copy tftp: startup-config，怎样让还原的配置生效？

4.2 点到点协议 PPP 配置

本节内容为路由器同步串口的点到点协议 PPP 及其认证配置，包括 PAP 认证、CHAP 单向认证和 CHAP 双向认证的配置实验。

4.2.1 配置 PPP 协议的 PAP 认证实验

1．PPP 协议介绍

路由器作为网络层设备，除了提供本地网络的三层连通外，更主要的功能是提供了用户网络的 WAN 接入。以实验室所使用的锐捷 R1762 高性能安全模块化路由器为例：该设备除了提供 2 个用于本地 LAN 连接的快速以太接口外，还提供了两个用于 WAN 接入的同步串口（Serial）。Serial 接口支持 HDLC、PPP 和 Frame Relay 的广域网封装协议，其中，目前使用最广泛的是 PPP 协议。

PPP（Point-to-Point Protocol，点到点协议）是 HDLC 的扩展，1994 年正式成为因特网的标准协议。PPP 协议的应用范围非常广泛，包括：拨号 PC 接入因特网访问服务器、通过 WAN 访问内部 LAN、在 VPN 中也利用 PPP 实现二层隧道协议 L2TP。也就是说，PPP 不仅适用于拨号用户，而且适用于租用的路由器对路由器线路。

（1）PPP 的协议体系

PPP 协议可以被看作是 HDLC 的扩展，其层次结构如图 4.10 所示：

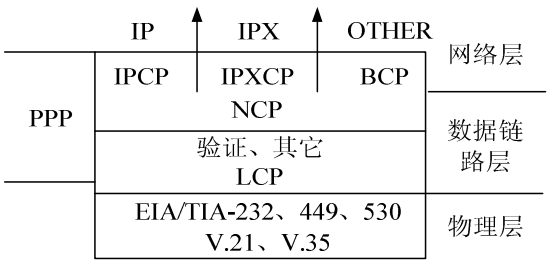


图 4.10 PPP 的层次结构

PPP 的主要实现功能如下：

- 采用高级数据链路控制协议 HDLC 作为点到点的串行链路上封装数据报的基本方法；
- 采用链路控制协议 LCP（Link Control Protocol）用于启动线路、测试、任选功能的协商及关闭连接；
- 采用网络控制协议 NCP（Network Control Protocol）用来建立和配置不同的网络层协议，PPP 允许同时采用多种网络层协议，如 IP、IPX 和 DECnet，PPP 使用 NCP 对多种协议进行封装。

（2）PPP 会话建立的过程

PPP 提供了建立、配置、维护和终止点到点连接的方法。从开始发起呼叫到最终通信完成后释放链路，PPP 的工作过程分为以下 4 个阶段：

• 链路的建立和配置协调

通信的发起方发送 LCP 帧来配置和检测数据链路，主要用于协商选择将要采用的 PPP 参数，包括身份验证、压缩、回叫、多链路等；

• 链路质量检测

在链路建立、协调之后，这一阶段是可选的；

• 网络层协议配置协调

通信的发起方发送 NCP 帧以选择并配置网络层协议，配置完成后，通信双方可以发送各自的网络层协议数据报；

• 关闭链路

通信链路将一直保持到 LCP 或 NCP 关闭链路，或者是发生一些外部事件（例如空闲时间超长或用户干预）

关于 PPP 协议规范详见 RFC1661。

2．PAP 介绍

为保证安全管理，PPP 提供了两种可选的身份认证方法：口令验证协议（PAP，Password Authentication Protocol）和挑战握手协议（CHAP，Challenge Handshake Authentication Protocol）。这里，我们首先介绍口令验证协议 PAP。

PAP 是一个简单实用的身份验证协议，PAP 认证进程只在双方的通信链路建立初始阶段进行。如果认证成功，在通信过程中不再进行认证；如果认证失败，则直接释放链路。

当通信双方都配置 PPP 协议并且选择 PAP 身份验证，同时它们之间的链路在物理层激活之后，认证客户端（被验证方）会不断发出身份认证请求，直到认证通过。当认证客户端路由器发送了用户名和口令之后，授权方（验证方）路由器会将收到的用户名和口令与本地数据库中的信息进行比较，如果正确则认证通过，否则认证失败。PAP 认证的基本过程如图 4.11 所示。

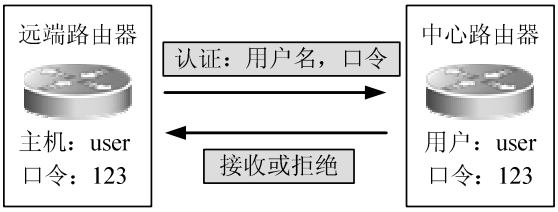


图 4.11 PAP 认证过程

从图 4.11 中可以看出，PAP 认证过程经过两个阶段，习惯上被称为两次握手：

第一阶段为被验证方（远端路由器）发送用户名和口令到验证方；

第二阶段为验证方（中心路由器）对接收的用户名和口令进行验证，并根据结果接收或拒绝链路连接的认证请求。

PAP 认证可以在一方进行，即由一方认证另一方的身份，也可以进行双向身份认证。这时将要求通信的双方都要通过对方的认证，否则，无法建立二者之间的链路。

3．配置 PPP 协议 PAP 认证的相关命令

（1）配置接口封装协议

路由器的 Serial 接口默认采用 HDLC 封装协议，因此，在通信双方选择 PPP 协议实现链路连接时，应当在双方接口上配置 PPP 协议，配置接口封装 PPP 协议的命令为：

Router(config-if)# **encapsulation ppp**

（2）配置 PPP 的 PAP 被验证方

被验证方发起 PPP 认证连接，发送用户名和口令，配置命令格式为：

Router(config-if)# **ppp pap sent-username** *username* **password** {0|7}*password*

其中 0 表示口令为明文，7 表示密文，口令类型（0 或 7）可省略，缺省时表示明文（0）。如果取消被验证方的 PAP 设置，可以执行：

Router(config-if)# **no ppp pap sent-username**

（3）配置 PPP 的 PAP 验证方

PPP 的 PAP 验证方需要执行两步操作：

第一步：设置 PPP 的 PAP 验证方

Router(config-if)# **ppp authentication pap**

第二步：创建用户数据库记录

Router(config)# **username** *username* **password** {0|7} *password*

注意：这里的 *username* 和 *password* 必须与被验证方的 pap sent-username 命令中的 *username* 和 *password* 保持一致，同样，{0|7}口令类型项也可以省略。

（4）调试和检测命令

- show interface serial　　！查看接口配置参数
- debug ppp　　！打开 PPP 协商调试开关

show interface 命令在前面的内容中已经做过介绍，通过该命令可以查看接口的配置状态，当查看的是封装了 PPP 的 serial 接口时可以查看 PPP 协商参数；

debug ppp 命令的格式为：

debug ppp [authentication | error | negotiation | packet]

其中：authentication 调试 PPP 认证，error 调试 PPP 协商错误，negotiation 调试 PPP 协商过程，packet 调试 PPP 协商报文。如果没有指定特定调试选项，则默认打开 PPP 认证协商调试选项。

4．实验环境与说明

（1）实验目的

掌握在路由器 serial 接口上 PPP 封装以及实现 PAP 验证的配置方法，理解 PAP 验证的一般过程。

（2）实验设备和连接

实验设备和连接如图 4.12 所示，通过 V.35 连接线把两台锐捷 R1762 路由器的 Serial 接口连接起来，路由器分别命名为 R1、R2。

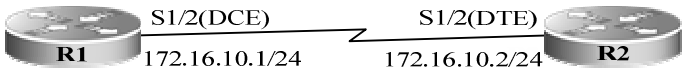


图 4.12 PPP 的 PAP 认证实验

（3）实验分组

每四名同学为一组，其中每两人一小组，每小组各自独立完成实验。

5．实验步骤

步骤 1：路由器基本配置：包括配置设备名、接口地址、启用接口；

R1 的配置如下：

Router> enable

Password:

```
Router# config terminal
Router (config)# hostname R1                          ！设备名为 R1
R1(config)# interface serial 1/2                      ！进入 S1/2 接口模式
R1(config-if)# ip address 172.16.10.1 255.255.255.0   ！配置 S1/2 接口 IP 地址
R1(config-if)# no shutdown                            ！启用 S1/2 接口
R1(config-if)# clock rate 64000                       ！设置时钟（DCE）
```

R2 的配置如下：

```
Router> enable
Password:
Router# config terminal
Router (config)# hostname R2                          ！设备名为 R2
R2(config)# interface serial 1/2                      ！进入 S1/2 接口模式
R2(config-if)# ip address 172.16.10.2 255.255.255.0   ！配置 S1/2 接口 IP 地址
R2(config-if)# no shutdown                            ！启用 S1/2 接口
```

配置完成后，使用 ping 命令做连通验证（R1 上执行 ping 172.16.10.2，第一次 ping）。

此时，在 R1 或 R2 上执行 show interface 命令查看接口状态，以 R2 为例：

```
R2# show interface serial 1/2
serial 1/2 is UP    , line protocol is UP
Hardware is PQ2 SCC HDLC CONTROLLER serial
Interface address is: 172.16.10.2/24
   MTU 1500 bytes, BW 2000 Kbit
   Encapsulation protocol is HDLC, loopback not
   Keepalive interval is 10 sec , set
   Carrier delay is 2 sec
   RXload is 1 ,Txload is 1
   Queueing strategy: WFQ
   5 minutes input rate 59 bits/sec, 0 packets/sec
   5 minutes output rate 20 bits/sec, 0 packets/sec
      373 packets input, 10828 bytes, 0 no buffer
      Received 298 broadcasts, 0 runts, 0 giants
      1 input errors, 0 CRC, 1 frame, 0 overrun, 0 abort
      324 packets output, 14592 bytes, 0 underruns
      0 output errors, 0 collisions, 15 interface resets
      1 carrier transitions
      V35 DTE cable
      DCD=up   DSR=up   DTR=up   RTS=up   CTS=up
```

可以看出，Serial 接口的默认封装协议是 HDLC。

步骤 2：配置接口封装为 PPP

在 R1 上配置接口封装：

```
R1(config)# interface serial 1/2
R1(config-if)# encapsulation ppp                      ！配置接口封装为 PPP
```

可以看到系统会有如下提示：

```
%LINE PROTOCOL CHANGE: Interface serial 1/2, changed state to DOWN
```

此时在 R1 上执行 ping 172.16.10.2，结果如何？（第二次 ping）
再在 R2 上配置接口封装：
R2(config)# interface serial 1/2
R2(config-if)# encapsulation ppp　　！配置接口封装为 PPP
可以看到系统会有如下提示：
%LINE PROTOCOL CHANGE: Interface serial 1/2, changed state to UP
仍然在 R1 上执行 ping 172.16.10.2，结果如何？（第三次 ping）
步骤 3：配置 R1 为 PAP 验证方
PAP 验证方的配置需要两步，执行如下：
R1(config)# username r2 password 0 star
　　！设置用户数据库，用户名：r2；加密类型：明文；口令：star
R1(config)# interface serial 1/2
R1(config-if)# ppp authentication pap　　！配置 R1 为 PAP 验证方
可以看到系统会有如下提示：
%LINE PROTOCOL CHANGE: Interface serial 1/2, changed state to DOWN
此时在 R1 上执行 ping 172.16.10.2，结果如何？（第四次 ping）
步骤 4：配置 R2 为 PAP 被验证方
PAP 被验证方的配置如下：
R2(config)# interface serial 1/2
R2(config-if)# ppp pap sent-username r2 password 0 star
　　！PAP 被验证方配置，发送用户名：r2；加密类型：明文；口令：star
可以看到系统会有如下提示：
%LINE PROTOCOL CHANGE: Interface serial 1/2, changed state to UP
仍然在 R1 上执行 ping 172.16.10.2，结果如何？（第五次 ping）
思考：在刚才执行的 5 次连通性检测中，哪次没有 ping 通，解释分别不通的原因？
步骤 5：综合验证与调试
在 R1 或 R2 上执行 show interface 命令查看接口状态，仍然以 R2 为例：
R2# show interface serial 1/2
serial 1/2 is UP　, line protocol is UP
Hardware is PQ2 SCC HDLC CONTROLLER serial
Interface address is: 172.16.10.2/24
　MTU 1500 bytes, BW 2000 Kbit
　Encapsulation protocol is PPP, loopback not set
　Keepalive interval is 10 sec , set
　Carrier delay is 2 sec
　RXload is 1 ,Txload is 1
　LCP Open
　Open: ipcp
　Queueing strategy: WFQ
　5 minutes input rate 174 bits/sec, 0 packets/sec
　5 minutes output rate 112 bits/sec, 0 packets/sec
　　565 packets input, 14043 by
　　Received 316 broadcasts, 0 runts, 0 giants
　　3 input errors, 0 CRC, 3 frame, 0 overrun, 0 abort

502 packets output, 16878 bytes, 0 underruns
0 output errors, 0 collisions, 22 interface resets
1 carrier transitions
V35 DTE cable
DCD=up DSR=up DTR=up RTS=up CTS=up

附注：BW：带宽，DLY：时延，HDLC：高级数据链路控制协议，DCD：数据载波寄存器，DSR：数据段寄存器，DTR：数据传送寄存器，RTS：请求发送，CTS：清除发送

可以看出，Serial 接口已经采用了 PPP 封装协议，LCP 链路协商已经完成。

实验的最后，我们使用 debug ppp 命令来观察 PAP 认证的过程：

在 R1 和 R2 上分别执行 debug ppp authentication 命令：

```
R1# debug ppp authentication                    ！打开 R1 调试 PPP 认证开关
R2# debug ppp authentication                    ！打开 R2 调试 PPP 认证开关
```

如果要看到 PAP 认证的过程，需要再执行下面的操作：

任选两台路由器之一，以 R2 为例：

```
R2(config)# interface serial 1/2
R2(config-if)# shutdown                         ！关闭 R2 的 S1/2 接口
R2(config-if)# no shutdown                      ！重新启用 R2 的 S1/2 接口
```

随后，在 R2 上就可以看到 PAP 认证的过程的调试信息，内容如下：

```
PPP: serial 1/2 PAP ACK received
PPP: serial 1/2 Passed PAP authentication with remote
PPP: serial 1/2 lcp authentication OK!
```

在 R1 上也会有相应的调试信息。

思考：为什么在关闭后又重新启用接口时才会看到 PAP 验证过程的调试信息？之前为什么看不到任何 PAP 验证过程的信息？如果之前做了双向 PAP 验证配置又会如何？

4.2.2 配置 PPP 协议的 CHAP 单向认证实验

在 4.2.1 实验中我们了解了路由器同步串口的 PPP 封装以及配置 PAP 验证的过程。由于 PAP 的认证只在链路建立初期进行，可以节省链路的开销，但它的缺点也是非常明显的。首先，PAP 的用户名和用户口令是以明文发送的，有可能被协议分析软件捕获而导致安全问题；其次，PAP 的验证是由被验证方发起，只进行所谓的两次握手，存在非授权用户反复尝试非法接入的可能。因此，在使用路由器建立 PPP 链路时，就安全而言，优先考虑的认证方法不是 PAP，而是 CHAP。

1．CHAP 介绍

CHAP（Challenge Handshake Authentication Protocol，挑战握手协议）比 PAP 认证要安全得多，因为 CHAP 不在线路上发送明文密码，而是发送经过散列算法加密后的摘要信息，其中包括由验证方产生的随机序列，也被称为“挑战字符串”；同时，CHAP 的身份认证可以随时进行，包括在双方正常通信的过程中。因此，非法用户即使截获并成功破译了一次密码，此密码也将在一段时间内失效。

CHAP 对系统要求很高，因为需要多次进行身份质询、响应，这需要耗费较多的处理器资源，因此 CHAP 多用于对安全要求很高的场合。

图 4.13 描述了 CHAP 的认证过程，可以看出 CHAP 认证包含三个阶段，通常称为三次握手：

阶段 1：当被验证方（远端路由器）向验证方（中心路由器）发送用户名做请求连接后，

验证方向被验证方发送一串随机字符（“挑战”阶段）；

阶段 2：被验证方利用 MD5 算法对口令和接收到的随机字符串进行加密产生密文，并将密文发送给验证方（“回应”阶段）；

阶段 3：验证方利用同样的方式对随机字符串和用户数据库中的记录进行加密，并将产生的密文与接收的密文进行比较，然后根据比较结果接受或拒绝连接请求。

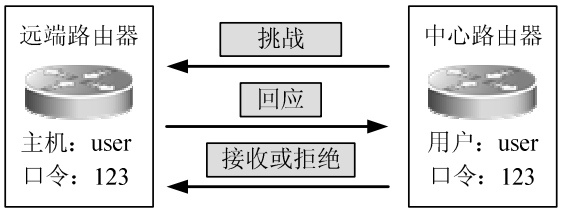


图 4.13 CHAP 认证过程

2．配置 PPP 协议 CHAP 认证的相关命令

（1）配置接口封装协议

上一节已经介绍了路由器的 Serial 接口默认采用 HDLC 封装协议，因此，在通信双方选择 PPP 协议实现链路连接时，应当在双方接口上配置 PPP 协议，命令为：

Router(config-if)# **encapsulation ppp**

（2）配置 PPP 的 CHAP 被验证方

配置 PPP 的 CHAP 被验证方的命令有两条：ppp chap hostname 用于指定 CHAP 认证时使用的主机名，ppp chap password 用于指定 CHAP 认证的公共口令。

- ppp chap hostname 命令的格式为：

Router(config-if)# **ppp chap hostname** *hostname*

Router(config-if)# **no ppp chap hostname**

其中，*hostname* 是在 CHAP 认证中发送的主机名称，该命令的 no 形式用于恢复缺省使用的主机名。缺省情况时，在任何 CHAP 认证中，均使用路由器的名称。

- ppp chap password 命令的格式为：

Router(config-if)# **ppp chap password** *encryption-type secret*

其中 *encryption-type* 表示密码报文的加密类型，*secret* 为 CHAP 认证的公共口令，该命令的 no 形式用于取消 CHAP 认证的公共口令。

随着网络规模的扩大，为了进行 CHAP 认证，必须为每台参与认证的路由器配置用户名/密码对，配置修改量会很大，如果使用 ppp chap hostname 和 ppp chap password 定义 CHAP 认证的公共主机别名和口令，则验证路由器只需要配置一个公共用户名/密码对即可，从而避免繁琐的验证数据库配置。

（3）配置 PPP 的 CHAP 验证方

- 设置 PPP 的 CHAP 验证方

Router(config-if)# **ppp authentication chap**

- 创建用户数据库记录

Router(config)# **username** *username* **password** *password*

使用的命令与 PPP 的 PAP 验证方相同，这里不复赘言。

（4）调试和检测命令

- show interface serial　　！查看接口配置参数
- debug ppp　　！打开 PPP 协商调试开关

3．实验环境与说明

（1）实验目的

使用 CHAP 认证方式对路由器 serial 接口上 PPP 进行验证，保证链路建立和网络安全性。理解 CHAP 验证的一般过程。

（2）实验设备和连接

实验设备和连接与 4.2.1 节实验相同，请参考图 4.12。

（3）实验分组

每四名同学为一组，其中每两人一小组，每小组各自独立完成实验。

4．实验步骤

步骤 1：路由器基本配置和串口 PPP 封装参见 4.2.1 实验步骤 1 和步骤 2，这里不再具体说明。

R1 配置如下：

```
Router# config terminal
Router (config)# hostname R1
R1(config)# interface serial 1/2
R1(config-if)# ip address 172.16.10.1 255.255.255.0
R1(config-if)# encapsulation ppp
R1(config-if)# no shutdown
R1(config-if)# clock rate 64000
```

R2 配置如下：

```
Router# config terminal
Router (config)# hostname R2
R2(config)# interface serial 1/2
R2(config-if)# ip address 172.16.10.2 255.255.255.0
R2(config-if)# encapsulation ppp
R2(config-if)# no shutdown
```

完成后，验证路由器 Serial 接口的连通性和 PPP 封装；

步骤 2：配置 R1 为 CHAP 验证方

```
R1(config)# username r2 password star
                ！设置用户数据库，用户名：r2；加密类型：缺省（明文）；口令：star
R1(config)# interface serial 1/2
R1(config-if)# ppp authentication chap          ！配置 R1 为 CHAP 验证方
```

可以看到系统会有如下提示：

```
%LINE PROTOCOL CHANGE: Interface serial 1/2, changed state to DOWN
```

步骤 3：配置 R2 为 CHAP 被验证方

```
R2(config)# interface serial 1/2
R2(config-if)# ppp chap hostname r2             ！CHAP 被验证方，发送主机名：r2；
R2(config-if)# ppp chap password star           ！CHAP 被验证方，发送口令：star；
```

可以看到系统会有如下提示：

```
%LINE PROTOCOL CHANGE: Interface serial 1/2, changed state to UP
```

注意：被验证方的发送主机名与口令要和验证方用户数据库的用户名与口令一致。

步骤 4：综合验证与调试

首先使用 ping 命令验证连通；

而后在 R1 或 R2 上执行 show interface 命令查看接口状态，确定 PPP 封装，链路协商已

经完成（接口 up，up）

最后使用 debug ppp 命令来观察 CHAP 认证的过程：

在 R1 和 R2 上分别执行 debug ppp authentication 命令：

R1# debug ppp authentication　　！打开 R1 调试 PPP 认证开关

R2# debug ppp authentication　　！打开 R2 调试 PPP 认证开关

同 4.2.1 实验中一样，在关闭后又重新启用接口时会看到 CHAP 验证过程的调试信息，内容如下：

验证方 R1（链路协商信息被略去，只保留 CHAP 的验证过程）

PPP: serial 1/2 Send CHAP challenge id=54 to remote host

PPP: serial 1/2 CHAP response id=54, received from r2

PPP: serial 1/2 Send CHAP success id=54 to remote

PPP: serial 1/2 remote router passed CHAP authentication.

PPP: serial 1/2 lcp authentication OK!

被验证方 R2（链路协商信息被略去，只保留 CHAP 的验证过程）

PPP: serial 1/2 Using CHAP hostname r2.

PPP: serial 1/2 recv CHAP challenge from R1

PPP: serial 1/2 username R1 not found in local router.

PPP: serial 1/2 Using default CHAP password.

PPP: serial 1/2 Passed CHAP authentication with remote.

PPP: serial 1/2 lcp authentication OK!

分析你所看到的 CHAP 验证过程，回答下面的问题：

1）R2 向 R1 发起连接呼叫，R1 接口已经配置 PPP CHAP 验证，LCP 协商使用 CHAP 和 MD5，在这次呼叫中，R1 要向呼叫者 R2 发出 CHAP 挑战消息，其中该挑战消息的序列号 ID 是多少？质询方的认证名（验证方的发送设备名）是什么？

2）R2 接收 R1 发送的挑战消息后，在本地用户数据库查找哪个用户没有找到？而后才使用默认的 CHAP password 出响应，这个口令是由那条命令建立的？

3）R1 接收的响应消息包括序列号 ID、发送设备名、R2 处理挑战消息中的 ID 和随机数与发送密码一起产生的散列编码，这里的序列号 ID 是多少？发送设备名是什么？散列编码中的发送密码是什么？

4）R1 根据接收的响应消息中的设备名查询本地用户数据库，找到对应的口令，并与之前发送挑战时保存的 ID 和随机数进行散列处理，将结果与响应消息中的哈希数比较，由于结果一致，发送验证成功的消息。在这里，验证成功的消息的 ID 是什么？本地用户数据库中找到的记录中用户名和口令分别是什么？这条记录是如何建立的？

4.2.3 配置 PPP 协议的 CHAP 双向认证实验

1．PPP 的身份验证过程

在 4.2.1 和 4.2.2 实验中，我们已经实现了 PPP 封装以及 PAP 和 CHAP 的验证配置，这里我对配置 PPP 身份验证的过程做一个总结：当配置 PPP 身份验证时，我们可以选择 PAP 或 CHAP 中的一种验证方式。在执行 encapsulation ppp 命令后，系统会根据配置选择验证方式，如果没有配置，PPP 进程会立即启动，否则 PPP 就会协商并确定进而执行身份验证。

图 4.14 显示了身份验证的过程，当确定验证方法后，身份验证进程检索本地数据库或安全服务器（通过使用命令 username password 建立），以检查用户所使用的用户名和密码是否匹配 CHAP 或 PAP 验证方式中指定的信息。

身份验证进程检查本地数据库或安全服务器返回的验证查询响应如果为肯定答复，PPP

进程就启动，如果是否定答复，用户将被立即拒绝。

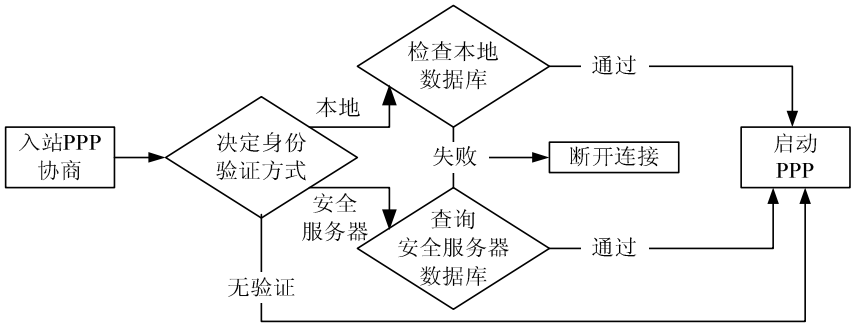


图 4.14 身份验证过程

如果选择 PAP 验证方式，在 PPP 链路建立阶段完成后，远程节点重复向路由器发送用户名和密码信息，直到验证通过或者链路终止；

如果选择 CHAP 验证发式，在 PPP 链路建立完成之后，本地路由器将发送一个挑战消息到远程节点。远程节点使用一个数值来回应挑战，这个数值是由散列算法（单向加密，典型为 MD5）基于密码和挑战消息计算产生的。本地路由器依靠由它自己计算出的期望值来检查回应。如果数值匹配，身份验证将被通过，否则连接将立即终止。

2．CHAP 身份验证过程

我们已经了解了 CHAP 的身份验证是由验证方发起，完成挑战、回应、确认三次握手，下面介绍一下这三个阶段的具体执行过程：

（1）挑战：由验证方向被验证方发出质询，具体过程如图 4.15 所示：

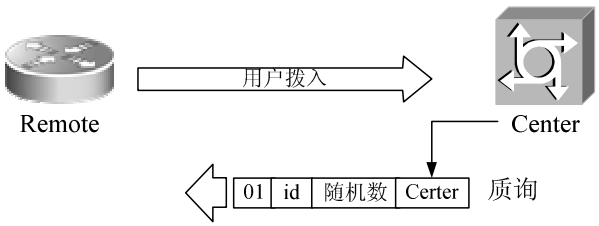


图 4.15 CHAP 身份验证过程 1：挑战阶段

- 远端设备 Remote 向 Certer 发起连接呼叫，呼叫进入接口已经配置了 CHAP 验证；
- LCP 协商使用 CHAP 和 MD5；
- Certer 需要向呼叫者发出一个 CHAP 挑战消息，该分组由以下内容组成：
  - 01：质询分组类型标识符
  - id：标识该挑战分组的序列号
  - Random：随机数
  - Certer：质询方的认证名（可用 ppp chap hostname 命令指定，缺省为设备名）
- 其中的 id 号和随机数由 Center 保存，被叫路由器会维护一个已发出的挑战消息的列表。

（2）回应：由被验证方向验证方发出的质询作出响应，具体过程如图 4.16 所示：

- 远端设备 Remote 接收挑战消息后执行如下处理：将序列号 id、随机数放入 MD5 哈希生成器，根据质询者的认证名查询密码，将匹配 Center 的 Password 一并放入 MD5 哈希生成器产生 MD5 数值。注意：如果没有质询者认证名的匹配记录，将使用缺省的认证口令（由 ppp chap password 命令指定）；
- Remote 根据处理结果向质询方 Center 发出回应，回应分组由以下部分组成：
  - 02：CHAP 回应分组的类型标识符

- id：序列号，复制自挑战分组
- hash：由 id、随机数和认证口令经 MD5 处理的密文结果
- Remote：本设备的认证名，认证方用来查找验证时所需的记录

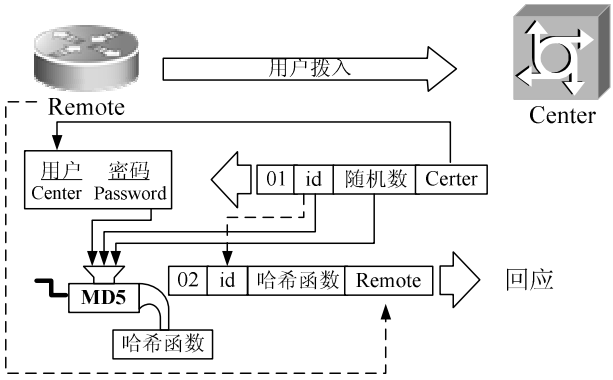


图 4.16 CHAP 身份验证过程 2：回应阶段

（3）确认：验证方接收被验证方回应后，比对用户数据库，根据结果决定接受或拒绝连接，具体过程如图 4.17 所示：

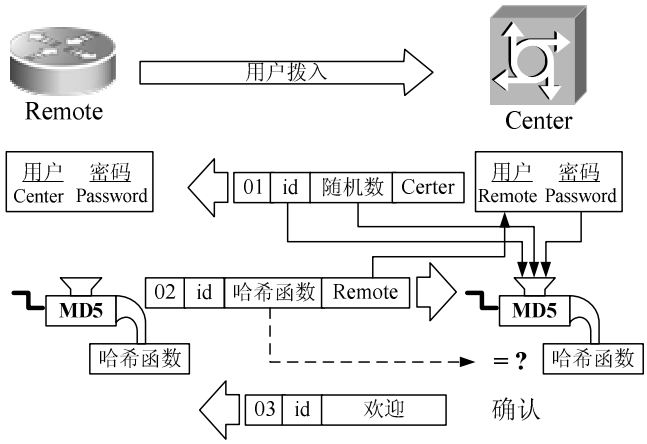


图 4.17 CHAP 身份验证过程 3：确认阶段

- 验证方 Center 接收回应消息后执行如下操作：用序列号 id 找出之前的挑战记录，把 id 和随机数放入 MD5 哈希生成器，根据回应消息的认证名查找口令（记录来自本地用户数据库或安全服务数据库，安全服务数据库可以是远程验证拨入用户服务 RADIUS 或终端访问控制器访问控制系统 TACACS 服务器）并将匹配的口令一并放入 MD5 哈希生成器产生 MD5 数值；
- 将 MD5 处理后的密文与回应消息中的值进行比对，如果一致即验证成功。
- 如果验证成功，验证方向被验证方发送成功消息，CHAP 验证成功消息组成如下：
  - 03：CHAP 验证成功的类型标识符
  - id：序列号，复制自回应分组
  - “Welcome in”：某种简单的文本消息，为了让用户可读
- 如果验证失败，验证方向被验证方发送失败消息，CHAP 验证失败消息组成如下：
  - 04：CHAP 验证失败的类型标识符
  - id：序列号，复制自回应分组
  - “Authentication Failure”：或其它类似的文本消息，为了让用户可读

3．CHAP 双向验证

上面的例子描述了 CHAP 单向验证的过程。在双向验证中，由于双方即作验证方又作

被验证方，以上的整个过程将重复进行，只是最初的“挑战”是由呼叫路由器发起的。

在配置 CHAP 双向验证时，由于缺省情况下，被验证方发送自己的设备名作为 PPP 用户认证名，因此可以不使用 ppp chap hostname 命令，于是双方的在配置本地用户数据库时（username password 命令）username 必须指定为对方的设备名（hostname）；当本地数据库存在匹配挑战消息中的质询者认证名时，将使用记录中的口令而不是缺省的认证口令（由 ppp chap password 命令指定）进行回复，因此双方也不需要指定缺省的认证口令；在双方确认时，由于是将对方的用户数据库记录的口令和本地数据库记录的口令进行比对，因此双方的口令必须一致。

在不使用 ppp chap hostname 定义 CHAP 认证的公共主机别名的情况下，CHAP 双向认证的配置步骤可以参考如下：

（1）双方使用 hostname 全局配置命令指定路由器设备名；

（2）双方使用 encapsulation ppp 接口配置命令启用 PPP 协议；

（3）双方使用 ppp authentication chap 接口配置命令启用 CHAP 验证；

（4）双方使用 username password 全局配置命令配置本地用户数据库，注意 username 指定为对方的 hostname，password 要一致。

4．实验环境与说明

（1）实验目的

配置 CHAP 双向验证，掌握 CHAP 验证的完整过程。

（2）实验设备和连接

实验设备和连接与 4.2.1 节和 4.2.2 节实验相同，请参考图 4.12。

（3）实验分组

每四名同学为一组，其中每两人一小组，每小组各自独立完成实验。

5．实验步骤

步骤 1：路由器基本配置和串口 PPP 封装参见 4.2.1 实验步骤 1 和步骤 2，这里不复赘言，配置要求如下：

配置路由器设备名为 R1 和 R2；配置 R1 的 serial 1/2 地址为 172.16.10.1/24，PPP 封装，clock rate 为 64000，启用接口；配置 R2 的 serial 1/2 地址为 172.16.10.2/24，PPP 封装，启用接口。

完成后验证连通；

步骤 2：双方启用 CHAP 验证

R1 配置如下：

```
R1(config)# interface serial 1/2
R1(config-if)# ppp authentication chap          ！配置 R1 为 CHAP 验证方
```

R2 配置如下：

```
R2(config)# interface serial 1/2
R2(config-if)# ppp authentication chap          ！配置 R2 为 CHAP 验证方
```

步骤 3：双方配置用户数据库

双方的用户名指定为对方的设备名，口令要一致。

R1 配置如下：

```
R1(config)# username R2 password star
```

R2 配置如下：

```
R2(config)# username R1 password star
```

注意：在 CHAP 认证中，会区分字母的大小写。

步骤 4：综合验证与调试

当看到系统有如下提示时，CHAP 的双向认证就已经通过。

%LINE PROTOCOL CHANGE: Interface serial 1/2, changed state to UP

最后使用 debug ppp 命令来观察 CHAP 双向认证的过程：

在 R1 和 R2 上分别执行 debug ppp authentication 命令：

R1# debug ppp authentication　　！打开 R1 调试 PPP 认证开关

R2# debug ppp authentication　　！打开 R2 调试 PPP 认证开关

同前面的实验一样，在关闭后又重新启用接口时会看到 CHAP 验证过程的调试信息，下面是在重新启用接口的 R1 上观察到的完整的 CHAP 验证调试信息：

PPP: serial 1/2 Send CHAP challenge id=42 to remote host

PPP: serial 1/2 authentication event enqueue, message type= [RECV_CHAP_CHALLENGE]

PPP: serial 1/2 authentication event enqueue, message type= [RECV_CHAP_RESPONSE]

PPP: dispose authentication message [RECV_CHAP_CHALLENGE]

PPP: serial 1/2 recv CHAP challenge from R2

PPP: dispose authentication message [RECV_CHAP_RESPONSE]

PPP: serial 1/2 CHAP response id=42, received from R2

PPP: serial 1/2 Send CHAP success id=42 to remote

PPP: serial 1/2 remote router passed CHAP authentication.

PPP: serial 1/2 Passed CHAP authentication with remote.

PPP: serial 1/2 lcp authentication OK!

PPP: ppp_clear_author (), protocol = TYPE_IPCP

对比你所看到的 R1 和 R2 上的 CHAP 验证过程的调试信息，分析并描述 CHAP 双向认证的完整过程：

思考题：

1）在 PPP 验证方如何取消 CHAP 验证？如何删除本地用户数据库的记录？以上面的 R1 为例，写出相关的配置命令：（要求写出 CLI 的提示符和完整的模式操作命令）

R1(config)#

2）如果双方设备名不变，要使用 Red-Giant 作为公共认证名，pass12345 作为公共认证口令，配置 CHAP 双向认证。与上面的配置相比，R1 和 R2 上应该增加的配置命令是什么？二者的用户数据库记录该如何建立？写出这两条命令：

R1(config-if)# _____

R1(config)# _____

3）在 R1 和 R2 上删除原有的用户数据库记录，以 Red-Giant 为公共认证名，pass12345 为认证口令，完成 CHAP 双向认证的配置。体会使用公共认证名和口令会带来哪些好处？

4.3 IP 访问控制列表的配置

作为网络层设备，路由器担负着实现网络互连的任务。一般情况下，路由器提供了内外

网连接以及不同的物理或逻辑子网（安全分组）的连接。既然路由器可以处理网络层分组，同时又位于不同的网络之间，因此，人们期望路由器可以起到网络安全的功能。

路由器的访问控制列表就提供了这种功能，它采用包过滤机制，允许用户使用访问列表来制定网络的安全策略，管理通过路由器的不同接口去往不同方向的信息流。对于许多网管员来说，配置路由器的访问控制列表是一件经常性的工作，可以说，访问控制列表是网络安全保障的第一道关卡。通过 IP 访问控制列表可以基于主机地址、目的地址和服务类型来允许或禁止为特定的用户提供资源。在未采用访问控制列表 ACL 的情况下，任何的网络流量都将不加限制的通过路由器传输。

4.3.1 标准 IP 访问控制列表的配置实验

1．访问控制列表的种类划分

访问控制列表 ACL 使用包过滤技术，在路由器上读取第三层及第四层包头中的信息如源地址、目的地址、源端口、目的端口等，根据预先定义好的规则对包进行过滤，从而达到访问控制的目的。实际上 ACL 是一些控制命令的集合，具有对指定的端口上的数据包实现允许或拒绝通过的功能。

最常用的 IP 基本 ACL 的类别有以下几种：

（1）标准 IP 访问控制列表：标准 IP 访问控制列表 ACL 编号范围为 1～99，其作用为根据数据包的源地址对数据进行过滤，采取拒绝或允许两种操作；

（2）扩展 IP 访问控制列表：扩展 IP 访问控制列表 ACL 编号范围是为 100～199，可以处理更多的匹配项，包括协议类型、源地址、目的地址、源端口、目的端口等，根据这些匹配项对数据包进行过滤，采取拒绝或允许两种操作；

（3）命名的 IP 访问控制列表：命名的 IP 访问控制列表 ACL 是以列表名代替列表编号来定义 IP ACL，同样包括标准和扩展两种列表，定义过滤的语句与编号方式中相似，可以方便地定义和引用列表；

2．访问控制列表的工作机制

访问控制列表 ACL 是一组命令语句，主要的应用方法是在分组出现下列行为：

- 入站（in）：进入入站路由器接口；
- 出站（out）：流出路由器接口；

图 4.18 描述了访问控制列表的工作机制：

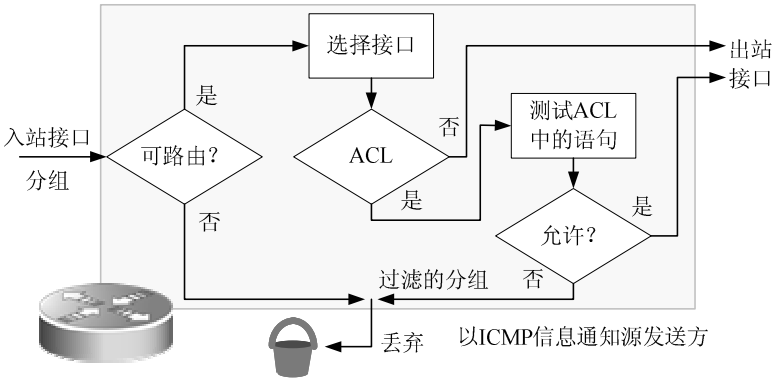


图 4.18 ACL 的工作机制

如图所示，当一个分组进入路由器某个接口时，路由器首先检查该分组是否可以路由，然后检查是否在入站接口上应用了 ACL；如果有 ACL，就将该分组与列表中的条件进行比较，如果分组被允许通过，就应用匹配的路由表条目决定转发的目的接口；而后路由器检查目的接口是否应用了 ACL，如果没有应用，分组被直接送到目的接口。

当路由器没有匹配目标网络的路由以及接收接口或转发接口所应用的 ACL 拒绝时，分组都将被丢弃。注意：ACL 不过滤路由器本身发出的分组，只过滤别的来源的分组。

IP ACL 是由多条允许或拒绝的命令语句构成的，在判定分组是否允许转发时，遵循以下的基本准则：

- 一切未被允许的就是禁止的；
- 按规则链来进行匹配：使用源地址、目的地址、源端口、目的端口、协议、时间段进行匹配（标准 IP ACL 仅检测源地址）；
- 从头到尾，至顶向下的匹配方式；
- 匹配成功马上停止，立刻使用该规则的允许或拒绝；

3．标准 IP 访问控制列表简介

标准 IP 访问控制列表能够对 IP 分组的源地址进行过滤，是一种简单、直接的数据控制手段，可以为特定主机或网络制定管理策略，通常允许（或拒绝）的是完整的协议。

（1）创建标准 IP ACL

Access-list 全局配置命令用于创建标准 IP ACL 规则，过滤数据分组，该命令在标准 IP ACL 中的格式为：

access-list [*list number*][permit|deny][*sourceaddress*][*wildcard-mask*]

使用 no access-list number 命令删除完整的访问列表，其中：

- list number：表号范围，标准 IP ACL 为 1～99；
- permit/deny：允许或拒绝，表示满足访问表项的分组是允许通过接口，还是要过滤掉；
- source address：源地址，源地址是主机或网络地址的点分十进制表示；
- wi1dcardmask：通配符掩码，用于匹配源地址，检测条件；缺省时表示 0.0.0.0，指定特定主机。

就配置而言，通配符掩码与子网掩码的方式是刚好相反的，其中，二进制的 0 表示一个“检测”条件，二进制的 1 表示一个“忽略”条件。

假设检测一个 C 类网络 198.78.46.0，若不使用子网，则当配置网络中的每一个工作站时，使用子网掩码 255.255.255.0。在子网掩码中，1 表示一个“检测”，而 0 表示一个“忽略”的条件。因此：网络地址要求匹配：24 位 1；主机地址忽略：8 位 0。

而通配符掩码的检测条件与子网掩码是相反的，网络地址要求匹配：24 位 0；主机地址忽略：8 位 1。所以匹配源地址 198.78.46.0 中的所有分组的通配符掩码为：0.0.0.255。

此外，在指定特定主机时，由于要匹配全部 32 位地址，所以通配符掩码为 0.0.0.0，这种情况下可以使用 host sourceaddress 来表示，也就是说，host 是通配符掩码 0.0.0.0 的简写。例如，假定我们希望允许从 198.78.46.8 来的报文，则使用标准的访问控制列表语句如下：

access-list 1 permit 198.78.46.8 0.0.0.0

如果采用关键字 host，可以用下面的语句来代替：

access-list 1 permit　host 198.78.46.8

与此相对照，any 是地址 0.0.0.0 255.255.255.255 的简写，用来指定所有主机。假定我们要拒绝从源地址 198.78.46.8 来的报文，并且要允许从其他源地址来的报文，标准的 IP 访问表可以使用下面的语句达到这个目的：

access-list 1 deny host 198.78.46.8

access-list 1 permit any

注意，这两条语句的顺序。访问列表语句的处理顺序是由上到下的，如果我们将两个语句顺序颠倒，将 permit 语句放在 deny 语句的前面，则我们将不能过滤来自主机地址 198.78.46.8 的报文，因为 permit 语句将允许所有的报文通过。可见访问列表中的语句顺序是很重要的，不合理的语句顺序将会在网络中产生安全漏洞，至少用户不能很好地利实现期

望的安全策略。

（2）在接口上应用标准 IP ACL

将 IP ACL 应用于路由器接口使用 ip access-group 接口配置命令，格式为：

ip access-group [*list number*] { in | out }

其中：list number 为已经创建的 ACL 表号；in 或 out 指明是进方向还是出方向，缺省时为出方向（out），使用 no ip access-group [list-number]命令将取消访问列表与接口的关联。

（3）IP ACL 配置说明

访问列表的编号指明了使用何种协议的访问列表，每个端口、每个方向、每条协议只能对应于一条访问列表。由于访问列表的内容决定了数据流的控制结果，因此限制语句的位置至关重要，应当注意：

- 具有严格限制条件的语句应放在访问列表所有语句的最上面；
- 在访问列表的最后有一条隐含声明：deny any；
- 正确的访问列表都至少应该有一条允许语句；
- 先创建访问列表，然后应用到端口上；
- 访问列表不能过滤由路由器自己产生的数据；

4．实验环境与说明

（1）实验目的

配置标准 IP ACL，理解 ACL 的原理、功能和相关注意事项；掌握对指定主机和指定网络规划安全策略的方法；掌握标准 IP ACL 配置的相关命令。

（2）实验设备和连接

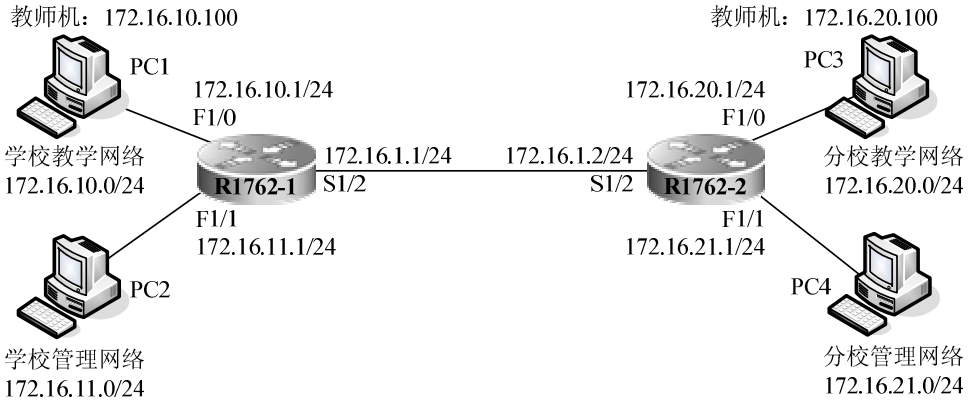


图 4.19 标准 IP ACL 的配置实验

实验设备和连接如图 4.19 所示：两台 R1762 路由器的两个 FastEthernet 接口各连接一个 PC，路由器之间串口相连。

配置标准 IP ACL 的要求如下：

- 学校管理网络和分校管理网络可以访问全部网络资源；
- 学校教学网络和分校教学网络只能相互访问，不能访问管理网络；
- 学校教学网络的指定教师机可以访问学校管理网络；
- 分校教学网络的指定教师机可以访问分校管理网络；

（3）实验分组

每四名同学为一组，其中每两人一小组，每人配置一台路由器，小组各自独立完成实验。

5．实验步骤

步骤 1：完成设备连接和路由器基本配置：

R1762-1 的配置为：

```
router (config)# hostname R1 762-1                    ！ 配置设备名
R1762-1 (config)# interface fastEthernet 1/0          ！ 配置 fastethernet 1/0 接口
R1762-1 (config-if)# ip address 172.16.10.1 255.255.255.0
R1762-1 (config-if)# no shutdown
R1762-1 (config-if)# interface fastEthernet 1/1       ！ 配置 fastethernet 1/1 接口
R1762-1 (config-if)# ip address 172.16.11.1 255.255.255.0
R1762-1 (config-if)# no shutdown
R1762-1 (config-if)# interface serial 1/2             ！ 配置 Serial 1/2 接口
R1762-1 (config-if)# ip address 172.16.1.1 255.255.255.0
R1762-1 (config-if)# no shutdown
```

R1762-2 的配置为：

```
router (config)# hostname R1 762-2                    ！ 配置设备名
R1762-2 (config)# interface fastEthernet 1/0          ！ 配置 fastethernet 1/0 接口
R1762-2 (config-if)# ip address 172.16.20.1 255.255.255.0
R1762-2 (config-if)# no shutdown
R1762-2 (config-if)# interface fastEthernet 1/1       ！ 配置 fastethernet 1/1 接口
R1762-2 (config-if)# ip address 172.16.21.1 255.255.255.0
R1762-2 (config-if)# no shutdown
R1762-2 (config-if)# interface serial 1/2             ！ 配置 Serial 1/2 接口
R1762-2 (config-if)# ip address 172.16.1.2 255.255.255.0
R1762-2 (config-if)# no shutdown
```

配置完成后，可以使用 show ip interface 命令检查设备的接口配置，以 R1762-1 为例：

```
R1762-1# show ip interface brief                      ！ 显示所有接口的 IP 状态简要
```

Interface	IP-Address(Pri)	OK?	Status
serial 1/2	172.16.1.1/24	YES	UP
serial 1/3	no address	YES	DOWN
FastEthernet 1/0	172.16.10.1/24	YES	UP
FastEthernet 1/1	172.16.11.1/24	YES	UP
Null 0	no address	YES	UP

确定设备的接口配置完成，F1/0、F1/1 和 S1/2 的状态为 UP。

步骤 2：路由器的路由配置：

可以通过前面实验中已经掌握的静态路由或动态路由 RIP 实现网络连通，这里就本实验而言，可以配置缺省路由：

```
R1762-1(config)# ip route 0.0.0.0 0.0.0.0 172.16.1.2
R1762-2(config)# ip route 0.0.0.0 0.0.0.0 172.16.1.1
```

注意：两端都要配置

完成后验证全网的连通性。

步骤 3：创建标准 IP ACL：

首先，就实验要求进行分析。

由于标准访问列表仅检测源地址，因此习惯上与靠近目的网络的接口建立关联。就配置要求而言，学校教学网络和分校教学网络没有设置过滤限制，任何站点都可以对它们进行访问；而学校管理网络和分校管理网络则要求对分组进行过滤：学校管理网络仅接收分校管理网络和学校教学网络中指定教师机的访问，分校管理网络则仅接收学校管理网络和分校教学

网络中指定教师机的访问。因此访问列表应当在两台 R1762 的 F1/1 接口上建立。

以 R1762-1 为例，F1/1 接口只转发来自网络 172.16.21.0/24 和主机 172.16.10.100 的分组；同样，R1762-2 的 F1/1 接口只转发来自网络 172.16.11.0/24 和主机 172.16.20.100 的分组。

在 R1762-1 上创建标准 IP 访问控制列表的配置为：

```
R1762-1(config)# access-list 10 permit 172.16.21.0 0.0.0.255
R1762-1(config)# access-list 10 permit host 172.16.10.100
R1762-1(config)# access-list 10 deny any
```

由于访问列表最后隐含“拒绝所有”的语句，因此 access-list 10 deny any 可以不设。

在 R1762-2 上创建标准 IP 访问控制列表的配置为：

```
R1762-2(config)# access-list 10 permit 172.16.11.0 0.0.0.255
R1762-2(config)# access-list 10 permit host 172.16.20.100
```

步骤 4：在设备接口上应用 ACL：

上一步骤对实验要求的分析已经说明：由于标准 ACL 只检测源地址，因而在应用时应当尽量靠近需要对源地址进行包过滤的目的网络。

在 R1762-1 上应用 ACL 的接口为 fastEthernet 1/1，出站方式，具体配置为：

```
R1762-1(config)# interface fastEthernet 1/1
R1762-1(config-if)# ip access-group 10 out          ！在接口出站方向上应用 ACL
```

R1762-2 的配置与之相同。

步骤 5：基本检测

可以使用 show access-lists 或 show ip access-lists 命令查看访问列表，以 R1762-1 为例：

```
R1762-1# show access-lists                          ！显示所有的 ACL
Standard IP access list 10 includes 3 items:
    permit 172.16.21.0, wildcard bits 0.0.0.255
    permit host 172.16.10.100
    deny   any
R1762-1# show ip access-lists                       ！显示 IP ACL
Standard IP access list 10 includes 3 items:
    permit 172.16.21.0, wildcard bits 0.0.0.255
    permit host 172.16.10.100
    deny   any
```

由于 R1762 仅配置了一个 IP 访问控制列表，表号为 10，因此上面两个命令的执行结果没有区别。此外，可以使用 show ip interface 命令查看设备接口的 ACL 绑定情况，以查看 R1762-1 的 fastEthernet 1/1 为例：

```
R1762-1#show ip interface fastEthernet 1/1          ！显示 F1/1 接口的 IP 状态
FastEthernet 1/1
  IP interface state is: UP
  IP interface type is: BROADCAST
  IP interface MTU is: 1500
  IP address is:
    172.16.10.1/24 (primary)
  IP address negotiate is: OFF
  Forward direct-boardcast is: ON
  ICMP mask reply is: ON
  Send ICMP redirect is: ON
```

Send ICMP unreachabled is: ON
DHCP relay is: OFF
Fast switch is: ON
Route horizontal-split is: ON
Help address is: 0.0.0.0
Proxy ARP is: ON
Outgoing access list is 10. ！接口出站应用 ACL：10
Inbound access list is not set. ！接口入站未应用 ACL

步骤 6：综合验证

按照表 4.5 完成对实验 PC 机的 IP 配置：

表 4.5 标准 IP ACL 实验 PC 机的 IP 配置

实验机	PC1	PC2	PC3	PC4
IP 地址	172.16.10.100	172.16.11.100	172.16.20.100	172.16.21.100
网关	172.16.10.1	172.16.11.1	172.16.20.1	172.16.21.1

根据刚才实验配置，自己判断 4 台 PC 之间的连通关系；然后实际 ping 一下，看你的判断是否正确？之后，将 PC1 的 IP 地址改为 172.16.10.10，PC2 的 IP 地址改为 172.16.20.10，再判断一下 PC 间的连通关系。如果两次都验证正确，则证明你已经理解了 IP 标准访问控制列表的基本概念。

4.3.2 扩展 IP 访问控制列表的配置实验

1．扩展 IP 访问控制列表简介

顾名思义，扩展的 IP 访问控制列表用于扩展设备的包过滤能力。一个扩展的 IP 访问控制列表允许用户根据如下内容过滤 IP 分组：源和目的地址、协议以及源和目的端口。因此，扩展访问控制列表可以提供更大的弹性和控制范围，使用的更加广泛。

（1）扩展 IP 访问控制列表的配置命令

扩展 IP 访问控制列表定义的主要项目为：源地址、目标地址和上层协议，一般语法格式为：

access-list <*list-number*> **{permit | deny}** <*protocol*> <*source-IP-address*> <*source-wildcard-mask*> <*destination-IP-address*> <*destination-wildcard-mask*> **[additional options]**

其中：list-number 表号范围为 100～199；protocol 指明需要检查的协议；根据不同的协议可以附加相应的其它条件。

在接口上应用扩展 IP ACL 与标准 IP ACL 相同，使用 ip access-group 接口配置命令，该命令在 4.3.1 节已经做过介绍，这里不复赘言。

（2）输入控制语句的顺序

与标准访问控制列表一样，扩展的 IP 访问控制列表可以使用多条独立的控制语句来定义多种控制准则，这些语句引用同一列表编号，以便绑定到同一个 ACL。

在配置 ACL 时，每条新配置的控制语句都将被追加到访问列表的最后，语句被创建后，就无法单独删除它，而只能删除整个列表。在上一节，我们已经了解了 ACL 的执行过程：路由器在转发还是阻断分组时，是按照 ACL 控制语句的创建次序来对分组进行比较的，一旦找到匹配的语句后就不再检查其它语句，所以访问列表语句的次序是非常重要的。

扩展访问控制列表的协议项定义了需要控制的协议，由于在 TCP/IP 协议栈中的各种协议之间有很密切的关系，因此应该注意将相对重要的过滤项放在靠前的位置。例如，管理员

针对某个源地址到目的地址通信流量的设置命令中，允许 IP 地址的语句放在拒绝 TCP 地址的语句前面，则后一个语句根本不起作用。但是如果将这两条语句换一下位置，则在允许该地址上的其他协议的同时，拒绝了 TCP 协议。

（3）基于 TCP/UDP 协议的访问控制

下面的命令是使用 CLI 帮助的方法，查看扩展访问列表的协议选项：

```
R1762-1(config)# access-list 101 permit ?
  <0-255>   An IP protocol number
  icmp      Internet Control Message Protocol
  ip        Any Internet Protocol
  tcp       Transmission Control Protocol
  udp       User Datagram Protocol
```

可以看出扩展 ACL 能够对整个 IP 或 IP 中具体的某项上层协议（服务）进行过滤。在指定 TCP 或 UDP 时可以进一步通过指定端口号来控制具体的高层协议类型。表 4.6 列举了一些常用的 TCP/UDP 端口号：

表 4.6 一些保留的 TCP/UDP 端口号

端口号	关键字	描述
20	FTP-DATA	文件传输协议（数据）
21	FTP	文件传输协议（控制）
23	TELNET	终端连接
25	SMTP	简单邮件传输协议
53	DOMAIN	域名服务（DNS）
69	TFTP	简单文件传输协议
80	HTTP	超文本传输协议
161	SNMP	简单网络管理协议

在使用 TCP 或 UDP 作为扩展 ACL 的协议选项时，可以使用 operator port 附加条件来过滤指定端口的 TCP 或 UDP 报文。其中 operator 操作符包括：lt（小于），gt（大于），eq（等于），neq（不等于）和 range（指定两个端口间的范围）；port 则指明操作的端口号，可以使用十进制数字或端口名称。

operator port 附加条件如果位于源地址和源通配符之后，那么它将匹配源端口；如果位于目的地址和目的通配符之后，那么它将匹配目的端口；如果缺省则代表 TCP 或 UDP 报文的全部端口都在列表语句的检测条件中。

例如，限定 192.168.1.0/24 网络主机不能访问 192.168.10.100 主机 WWW 服务的控制语句可以配置如下：

```
access-list 101 deny tcp 192.168.1.0 0.0.0.255 host 192.168.10.100 eq 80
```

2．配置扩展 IP 访问控制列表的相关命令

（1）定义扩展的 IP ACL

Router(config)# access-list <100-199> { permit /deny } 协议 源地址 源通配符 [源端口] 目的地址 目的通配符 [目的端口]

（2）应用扩展的 IP ACL 到接口

Router(config-if)# ip access-group <100-199> { in | out }

上节实验中，我们已经知道：标准访问控制列表不检查目的地址，为方便管理，一般尽可能放置在距离目标近的地方。而扩展的访问控制列表要检查源地址，目标地址和上层协议，为减少不必要的网络流量，应当尽可能的把扩展 ACL 放置在距离要被拒绝的通信流量近的

地方。可以这样总结 ACL 的放置准则：标准靠近目的，扩展靠近源。

注意：ACL 是通过过滤分组和拒绝不需要的通信流量来实现流量控制和安全策略的，放置 ACL 需要考虑的是网络中什么地方应该放置访问列表。正确的放置 ACL，不仅可以过滤通信流量，还可以使整个网络更有效的运行，为此，ACL 应放置在对网络增长影响最大的地方。此外，应当了解由于路由器不得不读取转发分组的更多信息和进行比对，ACL 的应用将会降低路由器的路由性能。

（3）访问列表的验证

- 显示所有（或指定表号）的 ACL：show access-lists <list-number>
- 显示所有（或指定表号）的 IP ACL：show ip access-lists <list-number>
- 显示所有（或指定）接口的访问列表应用：show ip interface <inter-type inter-num>

3．实验环境与说明

（1）实验目的

配置扩展 IP ACL，理解 TCP/IP 协议体系，全面掌握对网络流量实现控制和安全策略规划的方法；掌握扩展 IP ACL 配置的相关命令。

（2）实验设备和连接

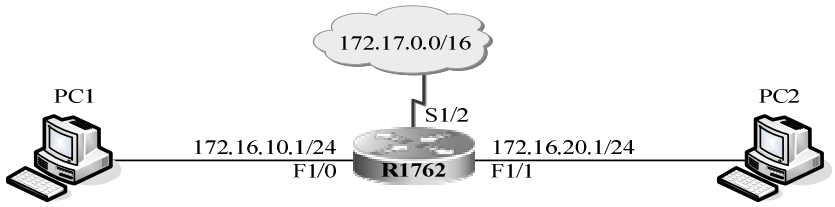


图 4.20 扩展 IP ACL 的配置实验

实验设备和连接如图 4.20 所示：一台 R1762 路由器的两个 FastEthernet 接口分别连接 172.16.10.0/24 和 172.16.20.0/24 网络（实验中用 PC 直连），Serial 接口连接 172.17.0.0/16 网络（实验中与另一台路由器连通即可）。

（3）实验分组

每四名同学为一组，每人配置一台路由器，各自独立完成实验。

4．实验步骤

步骤 1：完成设备连接和路由器基本配置：

```
router (config)# hostname R1 762                    ！配置设备名
R1762 (config)# interface fastEthernet 1/0          ！配置 fastethernet 1/0 接口
R1762 (config-if)# ip address 172.16.10.1 255.255.255.0
R1762 (config-if)# no shutdown
R1762 (config-if)# interface fastEthernet 1/1       ！配置 fastethernet 1/1 接口
R1762 (config-if)# ip address 172.16.20.1 255.255.255.0
R1762 (config-if)# no shutdown
```

配置完成后，使用 show ip interface brief 命令检查设备的接口配置，确定 F1/0 和 F1/1 的状态为 UP。

步骤 2：创建扩展 IP ACL：

```
R1762 (config)# access-list 110 deny tcp 172.16.2.0 0.0.0.255 172.16.1.0 0.0.0.255 eq 21
R1762 (config)# access-list 110 permit tcp 172.16.2.0 0.0.0.255 172.16.1.0 0.0.0.255 eq 80
R1762 (config)# access-list 110 deny ip any any
```

步骤 3：在设备接口上应用 ACL：

R1762(config)# interface fastEthernet 1/1

R1762-1(config-if)# ip access-group 110 in　　！在接口入站方向上应用 ACL

步骤 4：综合验证：

使用 show access-lists、show ip access-lists 和 show ip interface 命令查看访问列表及其与接口的关联，确定上面的配置均已完成。

思考：110 列表中有 3 条控制语句：第一条拒绝 172.16.2.0 对 172.16.1.0 进行 FTP 下载；第二条允许 172.16.2.0 对 172.16.1.0 进行 WWW 访问；第三条拒绝所有 IP 流量。根据你对扩展访问列表的理解，回答下列问题：

1)在完成上面的实验配置后，假如 172.17.0.0 网络已经连通，且除了 110 没有其它 ACL，判断表 4.7 中列举的网络通信是否可以。

表 4.7 扩展 IP ACL 实验分析一

网络通信	结果
172.16.2.0 对 172.16.1.0 的 FTP 服务器访问	□ 可以　□ 不可以
172.16.2.0 对 172.16.1.0 主机 TELNET	□ 可以　□ 不可以
172.16.2.0 对 172.16.1.0 的 WWW 服务器访问	□ 可以　□ 不可以
172.16.2.0 对 172.17.0.0 的 FTP 服务器访问	□ 可以　□ 不可以
172.16.2.0 对 172.17.0.0 的 WWW 服务器访问	□ 可以　□ 不可以
172.16.1.0 对 172.16.2.0 的 WWW 服务器访问	□ 可以　□ 不可以
172.16.1.0 对 172.17.0.0 的 WWW 服务器访问	□ 可以　□ 不可以

2）如果步骤 3 在设备接口上应用 ACL 的配置为：

R1762(config)# interface fastEthernet 1/0

R1762-1(config-if)# ip access-group 110 out

判断表 4.8 中列举的网络通信是否可以：

表 4.8 扩展 IP ACL 实验分析二

网络通信	结果
172.16.2.0 对 172.16.1.0 的 FTP 服务器访问	□ 可以　□ 不可以
172.16.2.0 对 172.16.1.0 主机 TELNET	□ 可以　□ 不可以
172.16.2.0 对 172.16.1.0 的 WWW 服务器访问	□ 可以　□ 不可以
172.16.2.0 对 172.17.0.0 的 FTP 服务器访问	□ 可以　□ 不可以
172.16.2.0 对 172.17.0.0 的 WWW 服务器访问	□ 可以　□ 不可以
172.16.1.0 对 172.16.2.0 的 WWW 服务器访问	□ 可以　□ 不可以
172.16.1.0 对 172.17.0.0 的 WWW 服务器访问	□ 可以　□ 不可以

3）如果步骤 3 在设备接口上应用 ACL 的配置为：

R1762(config)# interface serial 1/2

R1762-1(config-if)# ip access-group 110 out

判断表 4.9 中列举的网络通信是否可以：

表 4.9 扩展 IP ACL 实验分析二

网络通信	结果
172.16.2.0 对 172.16.1.0 的 WWW 服务器访问	□ 可以　□ 不可以
172.16.2.0 对 172.17.0.0 的 WWW 服务器访问	□ 可以　□ 不可以
172.16.1.0 对 172.16.2.0 的 WWW 服务器访问	□ 可以　□ 不可以
172.16.1.0 对 172.17.0.0 的 WWW 服务器访问	□ 可以　□ 不可以

4.3.3 命名的 IP 访问控制列表的配置实验

1．命名的 IP 访问控制列表

我们已经了解了 IP 的标准和扩展访问控制列表的相关知识和应用技术，在前面的实验中，访问控制列表的使用是基于编号（表号）的。在本教程所基于的锐捷全系列路由器除了可以使用编号方式外，还可以使用命名方式的 IP 访问控制列表。

相比较而言，命名的 IP 访问控制列表的配置更加符合管理员的习惯，某些厂商的网络设备甚至只提供了命名方式的访问控制列表的配置方法。

（1）命名的 IP 标准访问控制列表的配置

• 定义命名的标准访问列表

switch(config)# **ip access-list standard** *name*

switch(config-std-nacl)# **permit|deny** *sourceaddress wildcard-mask*

• 应用 ACL 到接口

switch(config-if)# **ip access-group** *name* { **in | out** }

（2）命名的 IP 扩展访问控制列表的配置

• 定义命名的标准访问列表

switch(config)# **ip access-list extended** *name*

switch(config-ext-nacl)# **permit|deny** *protocol source-address wildcard-mask destination-address wildcard-mask*

• 应用 ACL 到接口

switch(config-if)# **ip access-group** *name* { **in | out** }

可以看出所命名的 IP 访问控制列表使用管理员自己定义的名称而不是列表编号来进行标识，在定义时使用 ip access-list 命令，并通过 standard 或者 extended 来区分标准还是扩展的类型，而后在相应的列表配置模式下直接使用 permit（deny）语句。在应用到接口上时，命名和编号方式是一样的，只是执行 ip access-group 命令时用所命名的 name 取代了原先的编号。

这里需要指出的是，随着网络安全越来越受到关注，访问控制列表在园区网中得到了广泛的应用。目前主流的接入交换机除了支持 IP 访问控制列表外，还提供了更多类型的访问控制技术，如下所述：

MAC ACL：基于硬件地址的访问控制列表；

专家级 ACL：基于协议、IP 和 MAC 地址的访问控制列表；

ACL80：基于 IP 数据报的特征字符（例如 BT）的访问控制列表。

这些访问控制技术的配置和工作原理与命名的 IP 标准和扩展访问控制列表类似，本书不再专门讨论，有兴趣的读者可以参考相关的设备说明。

锐捷全系列交换机可针对物理接口和 SVI 接口应用 ACL（命名方式），但在应用时要注意：针对交换接口，只能配置入栈应用（In）；针对 SVI（三层）接口，则可以配置入栈（In）和出栈（Out）应用。

2．实验环境与说明

（1）实验目的

掌握命名的 IP 访问控制列表的配置以及相关调试和检测命令。

（2）实验设备和连接

实验设备和连接如图 4.21 所示：三层交换机 S3550 和二层交换机 S2126 通过 F0/1 相连。S2126 上连接三个 VLAN，通过 S3550 的 SVI 实现相互连接，IP 地址和 VLAN 接口规划如图示。要求通过 IP 访问控制列表实现对 VLAN10 的访问限制（只允许 VLAN30 和指定的

VLAN20 中的特定主机访问），并在 S2126 上控制网络病毒的传播。

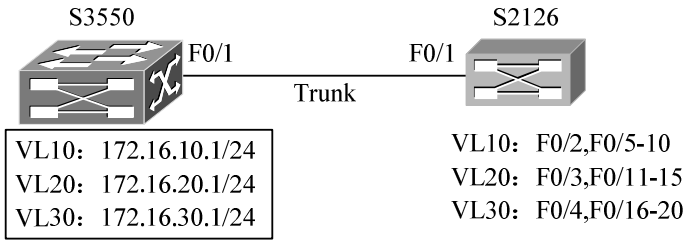


图 4.21 命名的 IP ACL 配置实验

（3）实验分组

每四名同学为一组，其中每两人一小组，每小组各自独立完成实验。

5．实验步骤

步骤 1：完成设备连接和设备名配置：

步骤 2：S2126 的基本配置：

按照要求完成 S2126 上 VLAN 规划，参考配置如下：

```
S2126(config)# vlan 10
S2126(config-vlan)# exit
S2126(config)# vlan 20
S2126(config-vlan)# exit
S2126(config)# vlan 30
S2126(config-vlan)# exit
S2126(config)# interface fastEthernet 0/1
2S2126(config-if)# switchport mode trunk
S2126(config-if)# exit
S2126(config)# interface range fastEthernet 0/2,0/5-10
S2126(config-if-range)# switchport access vlan 10
S2126(config-if-range)# exit
S2126(config)# interface range fastEthernet 0/3,0/11-15
S2126(config-if-range)# switchport access vlan 20
S2126(config-if-range)# exit
S2126(config)# interface range fastEthernet 0/4,0/16-20
S2126(config-if-range)# switchport access vlan 30
S2126(config-if-range)# end
```

完成配置后，使用 show vlan 验证配置信息，参考如下：

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------------------
1    default                           active    Fa0/1 ,Fa0/21,Fa0/22
                                                 Fa0/23,Fa0/24
10   VLAN0010                          active    Fa0/1 ,Fa0/2 ,Fa0/5
                                                 Fa0/6 ,Fa0/7 ,Fa0/8
                                                 Fa0/9 ,Fa0/10
20   VLAN0020                          active    Fa0/1 ,Fa0/3 ,Fa0/11
                                                 Fa0/12,Fa0/13,Fa0/14
                                                 Fa0/15
```

30	VLAN0030	active	Fa0/1 ,Fa0/4 ,Fa0/16 Fa0/17,Fa0/18,Fa0/19 Fa0/20

步骤 3：S3550 的基本配置：

按照要求完成 S3550 上 SVI 和 Trunk 接口配置，参考配置如下：

```
S3550(config)# vlan 10
S3550(config-vlan)# exit
S3550(config)# vlan 20
S3550(config-vlan)# exit
S3550(config)# vlan 30
S3550(config-vlan)# exit
S3550(config)# interface fastEthernet 0/1
S3550(config-if)# switchport mode trunk
S3550(config-if)# exit
S3550(config)# interface vlan 10
S3550(config-if)# ip address 172.16.10.1 255.255.255.0
S3550(config-if)# exit
S3550(config)# interface vlan 20
S3550(config-if)# ip address 172.16.20.1 255.255.255.0
S3550(config-if)# exit
S3550(config)# interface vlan 30
S3550(config-if)# ip address 172.16.30.1 255.255.255.0
S3550(config-if)# end
```

完成配置后使用 show ip interface 验证 SVI 接口的状态，参考如下：

```
Interface                   : VL10
Description                 : Vlan 10
OperStatus                  : up
ManagementStatus            : Enabled
Primary Internet address    : 172.16.10.1/24
Broadcast address           : 255.255.255.255
PhysAddress                 : 00d0.f8b8.8d06

Interface                   : VL20
Description                 : Vlan 20
OperStatus                  : up
ManagementStatus            : Enabled
Primary Internet address    : 172.16.20.1/24
Broadcast address           : 255.255.255.255
PhysAddress                 : 00d0.f8b8.8d07

Interface                   : VL30
Description                 : Vlan 30
OperStatus                  : up
ManagementStatus            : Enabled
```

Primary Internet address : 172.16.30.1/24
Broadcast address : 255.255.255.255
PhysAddress : 00d0.f8b8.8d08

步骤 4：配置命名的 IP 标准访问控制列表：

在 S3550 上通过 IP ACL 实现对 VLAN 10 的访问控制，要求只允许 VLAN 20 中的指定地址 172.16.20.100 和 VLAN 30 中的主机可以访问 VLAN 10：

```
S3550(config)# ip access-list standard my_acl                ！配置命名的标准 ACL
S3550(config-std-nacl)# permit host 172.16.20.100            ！允许特定主机地址
S3550(config-std-nacl)# permit 172.16.30.0 0.0.0.255         ！允许指定网段地址
S3550(config-std-nacl)# exit
S3550(config)# interface vlan 10
S3550(config-if)# ip access-group my_acl out                 ！在 VLAN10 上启用 ACL
S3550(config-if)# end
```

完成后执行 show ip access-lists 命令查看已经配置的访问控制列表，显示信息如下：

```
Standard IP access list: my_acl
    permit host 172.16.20.100
    permit 172.16.30.0 0.0.0.255
```

交换机上使用 show ip access-group 命令查看访问控制列表的接口上应用，如下所示：

```
S3550#show ip access-group
Interface       inbound access-list              outbound access-list
--------- ------------------------------ ------------------------------
VL10                                             my_acl
```

步骤 5：配置命名的 IP 扩展访问控制列表：

在 S2126 上通过 IP ACL 实现对网络病毒的传播限制，这里需要指出的是诸如冲击波一类的网络病毒的传播是针对 Windows 操作系统的特定端口的，只要限制针对这些端口的访问就可以限制这类网络病毒在网络中的扩散。

```
S2126(config)# ip access-list extended firewall              ！配置命名的扩展 ACL
S2126(config-ext-nacl)# deny udp any any eq 69               ！拒绝访问 UDP69 端口
S2126(config-ext-nacl)# deny tcp any any eq 135              ！拒绝访问 TCP135 端口
S2126(config-ext-nacl)# deny udp any any eq 135              ！拒绝访问 UDP135 端口
S2126(config-ext-nacl)# deny udp any any eq 137              ！拒绝访问 TCP137 端口
S2126(config-ext-nacl)# deny udp any any eq 138              ！拒绝访问 TCP138 端口
S2126(config-ext-nacl)# deny tcp any any eq 139              ！拒绝访问 TCP139 端口
S2126(config-ext-nacl)# deny udp any any eq 139              ！拒绝访问 UDP139 端口
S2126(config-ext-nacl)# deny tcp any any eq 445              ！拒绝访问 TCP445 端口
S2126(config-ext-nacl)# deny tcp any any eq 593              ！拒绝访问 TCP593 端口
S2126(config-ext-nacl)# deny tcp any any eq 4444             ！拒绝访问 TCP4444 端口
S2126(config-ext-nacl)# permit ip any any                    ！允许其他 IP 流量
S2126(config-ext-nacl)# exit
S2126(config)# interface range fastEthernet 0/2-20
S2126(config-if-range)# ip access-group firewall in          ！在 VLAN10 上启用 ACL
S2126(config-if-range)# end
```

完成后同样执行 show ip access-lists 和 show ip access-group 命令查看访问控制列表及其接口应用，具体显示信息这里不再给出。

思考题：

（1）步骤 4 中的标准 ACL 是在 VLAN10 的 SVI 接口上出栈应用的，能否替换为在 VLAN20 和 VLAN30 上以入栈方式应用？比较两种配置所带来的差别。

（2）步骤 5 中的扩展 ACL 是在 S2126 的二层接口上以入栈方式应用的，能否配置为出栈方式应用？理解交换机接口上应用 ACL 的要求。

4.4 其它应用配置

4.4.1 NAT/NAPT 配置实验

众所周知，第四版 IP 协议的一个很重要的局限性就是 IP 地址空间濒临耗尽所引起的地址危机，使用 128 比特地址的 IPv6 可以彻底解决地址空间问题。作为多年计划和研究的新一代 Internet 协议，IPv6 却并没有被急于投入，自然是由于 IPv6 的很多功能需待完善和实施，而更重要的原因则是对 IPv4 的短期扩展和利用直到目前来说还是很有效的。

这些用于缓解 IP 地址危机的解决方法包括无类别域间路由（CIDR）、可变长子网掩码（VLSM）、路由聚合和超网。本节所涉及的 NAT/NAPT 技术就是网络项目集成中用于扩展地址空间，提高地址利用率的重要手段。

1．NAT 概述

NAT 就是将网络地址从一个地址空间转换到另外一个地址空间的一个行为。这种特性，使得内部局域网呈现给外部网络的 IP 地址，可以与正在使用的 IP 地址空间完全不同。这样一个组织就可以将本来非全局可路由地址通过 NAT 之后，变为全局可路由地址，实现了原有网络与互联网的连接，而不需要重新给每台主机分配 IP 地址。

按照转换方式上的差别，NAT 包括两种类型：

（1）NAT（Network Address Translation，网络地址转换）

转换后，一个本地 IP 地址对应一个全局 IP 地址

（2）NAPT （Network Address Port Translation，网络地址端口转换）

转换后，多个本地地址对应一个全局 IP 地址

在 SOHO 网络中，NAT 可以通过代理服务器实现；而对于一定规模的局域网，管理员一般在接入路由器或者核心设备上来完成 NAT 服务。本节主要介绍在接入路由器上基于内部源地址的 NAT/NAPT 的配置。首先，我们了解一下 NAT 中的常见术语：

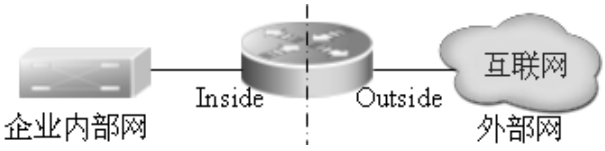


图 4.22 NAT 应用示意

如同 4.22 所示，NAT 设备位于内部网络和外部网络之间，其中：

Inside：表示内部网络，这些网络的地址需要被转换。在内部网络，每台主机都分配一个内部 IP 地址，但与外部网络通讯时，又表现为另外一个地址。每台主机的前一个地址又称为本地地址，后一个地址又称为全局地址。

Outside：指内部网络需要连接的网络，一般指互联网，也可以是另外一个机构的网络。外部的地址也可以被转换，即外部主机也可能同时具有内部地址和外部地址。

根据这种关系，NAT 做了以下定义：

- 内部本地地址（Inside Local Address）

分配给内部网络主机的 IP 地址，可能是非法的未向相关机构注册的 IP 地址，也可能是合法的私有网络地址。

• 内部全局地址（Inside Global Address）

合法的全局可路由地址，在外部网络代表着一个或多个内部本地地址。

• 外部本地地址（Outside Local Address）

外部网络的主机在内部网络中表现的 IP 地址，该地址是内部可路由地址。

• 外部全局地址（Outside Global Address）

外部网络分配给外部主机的 IP 地址。

2．基于内部源地址的 NAT 的配置

当内部网络需要与外部网络通讯时，需要配置 NAT 将内部私有 IP 地址转换成全局唯一 IP 地址。你可以配置静态或动态的 NAT 来实现互联互通的目的，或者需要同时配置静态和动态的 NAT。

其中，静态 NAT 用于需要内部主机向外部网络提供信息服务时配置，建立永久的一对一 IP 地址映射关系；而如果内部网络只访问外网服务，并不提供信息服务的主机，则使用动态 NAT 来建立临时的一对一 IP 地址映射关系。

（1）配置基于源地址的静态 NAT

• 建立静态的映射关系

Router (config)# **ip nat inside source static** *local-address global-address*

• 定义内网接口和外网接口

Router(config)# **interface** *interface-type interface-number*

Router(config-if)# **ip nat inside**

Router(config)# **interface** *interface-type interface-number*

Router(config-if)# **ip nat outside**

（2）配置基于源地址的动态 NAT

• 定义内网接口和外网接口

Router(config-if)# **ip nat outside**

Router(config-if)# **ip nat inside**

• 定义内部本地地址范围，只有匹配该列表才转换

Router(config)# **access-list** *access-list-number* **permit** *ip-address wildcard*

• 定义内部全局地址池

Router(config)# **ip nat pool** *address-pool start-address end-address* {**netmask** *mask* | **prefix-length** *prefix-length*}

• 建立映射关系

Router(config)# **ip nat inside source list** *access-list-number* **pool** *address-pool*

3．基于内部源地址的 NAPT 的配置

传统的 NAT 一般是指一对一的地址映射，不能同时满足所有的内部网络主机与外部网络通讯的需要。使用 NAPT，可以将多个内部本地地址映射到一个内部全局地址，路由器用“内部全局地址 ＋TCP/UDP 端口号”来对应“一个内部主机地址 ＋TCP/UDP 端口号”。

内部源地址 NAPT 配置也有两种情况：静态 NAPT 和动态 NAPT。

当你的内部主机需要对外部网络提供服务，而又缺乏全局地址，或者就没有申请全局地址，就可以考虑配置静态 NAPT；而如果只是让内部所有主机可以访问外部网络的话，则使用动态 NAPT。NAPT 的内部全局地址可以是路由器外部（Outside）接口的 IP 地址，也可以是向 ISP 申请来的注册地址。

（1）配置基于源地址的静态 NAPT

• 定义全局 IP 地址池

Router(config)# **ip nat inside source static {UDP | TCP}** *local-address port global-address port*

• 定义内网接口和外网接口

Router(config)# **interface** *interface-type interface-number*

Router(config-if)# **ip nat inside**

Router(config)# **interface** *interface-type interface-number*

Router(config-if)# **ip nat outside**

（2）配置基于源地址的动态 NAPT

• 定义内网接口和外网接口

Router(config-if)# **ip nat outside**

Router(config-if)# **ip nat inside**

• 定义内部本地地址范围，只有匹配该列表才转换

Router(config)# **access-list** *access-list-number* **permit** *ip-address wildcard*

• 定义内部全局地址池

Router(config)# **ip nat pool** *address-pool start-address end-address* {**netmask** *mask* | **prefix-length** *prefix-length*}

• 建立映射关系

Router(config)# **ip nat inside source list** *access-list-number* **pool** *address-pool* **overload**

可以看出配置基于源地址的动态 NAPT 和动态 NAT 的命令相同，只是在建立地址映射命令中加了 overload 参数选项。

4．实验环境与说明

（1）实验目的

了解 NAT/NAPT 的基本概念;掌握 RGNOS 中基于内部源地址的静态和动态 NAT/NAPT 配置以及相关调试和检测命令。

（2）实验设备和连接

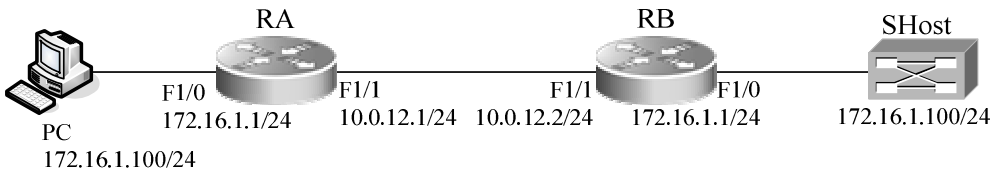


图 4.23 NAT/NAPT 的配置实验

实验设备和连接如图 4.23 所示：一台测试 PC 和一台 S2126 交换机分别连接的两台 R1762 路由器使用 F1/1 接口彼此相连。分别连接的内部网络地址重叠，在 RA 上配置动态 NAT/NAPT，实现内部 PC 的对外连接；在 RB 上配置静态 NAT/NAPT，实现外部网络对交换机 SHost 的访问。

（3）实验分组

每四名同学为一组，其中每两人一小组，每小组各自独立完成实验。

5．实验步骤

步骤 1：完成设备连接和设备名配置：

两台 R1762 配置设备名为 RA、RB，S2126 配置设备名为 SHost;

步骤 2：设备接口配置：

路由器的配置比较简单，只要设置 F1/0 和 F1/1 接口即可。

其中 RA 的配置为：

RA(config)# interface fastEthernet 1/0
RA(config-if)# ip address 172.16.1.1 255.255.255.0
RA(config-if)# no shutdown
RA(config-if)# exit
RA(config)# interface fastEthernet 1/1
RA(config-if)# ip address 10.0.12.1 255.255.255.0
RA(config-if)# no shutdown
RA(config-if)#exit
RB 的配置为：
RB(config)# interface fastEthernet 1/0
RB(config-if)# ip address 172.16.1.1 255.255.255.0
RB(config-if)# no shutdown
RB(config-if)# exit
RB(config)# interface fastEthernet 1/1
RB(config-if)# ip address 10.0.12.2 255.255.255.0
RB(config-if)# exit

交换机除了管理 IP 外，为了能够实现远程访问，还需要配置管理口令和缺省网关，具体配置如下：

SHost(config)# enable secret level 1 0 star　　！配置远程登录口令
SHost(config)# enable secret level 15 0 star　　！配置特权口令
SHost(config)# interface vlan 1　　！配置管理 IP
SHost(config-if)# ip address 172.16.1.100 255.255.255.0
SHost(config-if)# no shutdown
SHost(config-if)# exit
SHost(config)# ip default-gateway 172.16.1.1　　！配置缺省网关
SHost(config)#exit

配置 PC 的 IP 地址为 172.16.1.100/24，缺省网关为 172.16.1.1，并使用 ipconfig/all 验证。

步骤 3：NAT 地址映射规划和路由配置：

由于 RA 和 RB 连接的内部网络地址重叠，现规划地址转换关系如下：

RA 连接的 172.16.1.0/24 网络转换为 10.0.1.0/24；RB 连接的 172.16.1.0/24 网络转换为 10.0.2.0/24。根据转换的全局可路由地址，完成路由器的路由配置：

RA 的配置为：
RA(config)# ip route 10.0.2.0 255.255.255.0 10.0.12.2
RB 的配置为：
RB(config)# ip route 10.0.1.0 255.255.255.0 10.0.12.1

步骤 4：静态 NAT 配置：

在 RB 上配置基于源地址的静态 NAT，建立本地地址 172.16.1.100 与全局地址 10.0.2.100 的映射关系，配置命令为：

RB(config)# interface fastEthernet 1/0
RB(config-if)# ip nat inside　　！配置内部接口
RB(config-if)#exit
RB(config)# interface fastEthernet 1/1
RB(config-if)# ip nat outside　　！配置外部接口
RB(config-if)# exit

RB(config)# ip nat inside source static 172.16.1.100 10.0.2.100 ！静态 NAT 地址映射

步骤 4：动态 NAT 配置：

在 RA 上配置基于源地址的动态 NAT，建立全局地址池 10.0.1.1～10.0.1.2，实现本地地址 172.16.1.0/24 的对外访问。配置命令为：

RA(config)# interface fastEthernet 1/0

RA(config-if)# ip nat inside ！配置内部接口

RA(config-if)# exit

RA(config)# interface fastEthernet 1/1

RA(config-if)# ip nat outside ！配置外部接口

RA(config-if)# exit

RA(config)# access-list 1 permit 172.16.1.0 0.0.0.255 ！定义内部本地地址范围

RA(config)# ip nat pool my_pool 10.0.1.1 10.0.1.2 netmask 255.255.255.0

！定义内部全局地址池

RA(config)# ip nat inside source list 1 pool my_pool ！建立映射关系

步骤 5：NAT 配置检测：

在 PC 机上执行：telnet 10.0.2.100，实现远程登录交换机后，分别在 RA 和 RB 上使用 show ip nat translations 命令查看 NAT 地址转换记录：

RA 的显示信息参考如下：

RA# show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
tcp	10.0.1.1:1056	172.16.1.100:1056	10.0.2.100:23	10.0.2.100:23

RB 的显示信息参考如下：

RB# show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
tcp	10.0.2.100:23	172.16.1.100:23	10.0.1.9:1056	10.0.1.9:1056

在 PC 机上继续执行 telnet 10.0.2.100，并在路由器上执行 show ip nat translations 命令查看 NAT 地址转换记录，回答下面的问题：

（1）PC 机可以建立几条 Telnet 会话？

（2）记录 RA 观察到的地址转换：

Inside global：_____

Inside local：_____

步骤 6：NAPT 配置：

在 RA 和 RB 上执行如下：

RA# clear ip nat translation * ！清除地址转换记录

RA# show ip nat translations

确认转换记录已被清空。

由于 NAPT 的配置和 NAT 的配置相近，所以我们可以在前面实验的基础上来实现基于源地址的静态和动态 NAPT 配置。RA 的 RB 的执行如下：

RA(config)# no ip nat inside source list 1 pool my_pool ！取消 NAT 地址映射

RA(config)# ip nat inside source list 1 pool my_pool overload ！建立 NAPT 地址映射

RB(config)# no ip nat inside source static 172.16.1.100 10.0.2.100

！取消 NAT 地址静态映射

RB(config)# p nat inside source static tcp 172.16.1.100 23 10.0.2.100 2003

！建立 NAPT 地址静态映射

步骤 7：NAPT 配置检测：

在 PC 机上执行 telnet 10.0.2.100 2003，实现远程登录交换机，反复执行多次，分别在 RA 和 RB 上使用 show ip nat translations 命令查看 NAT 地址转换记录：

RA 的显示信息参考如下：

RA#show ip nat translations

Pro Inside global	Inside local	Outside local	Outside global
tcp 10.0.1.1:1060	172.16.1.100:1060	10.0.2.100:2003	10.0.2.100:2003
tcp 10.0.1.1:1062	172.16.1.100:1062	10.0.2.100:2003	10.0.2.100:2003
tcp 10.0.1.2:1061	172.16.1.100:1061	10.0.2.100:2003	10.0.2.100:2003
tcp 10.0.1.2:1063	172.16.1.100:1063	10.0.2.100:2003	10.0.2.100:2003

RB 的显示信息参考如下：

RB# show ip nat translations

Pro Inside global	Inside local	Outside local	Outside global
tcp 10.0.2.100:2003	172.16.1.100:23	10.0.1.1:1060	10.0.1.1:1060
tcp 10.0.2.100:2003	172.16.1.100:23	10.0.1.2:1061	10.0.1.2:1061
tcp 10.0.2.100:2003	172.16.1.100:23	10.0.1.1:1062	10.0.1.1:1062
tcp 10.0.2.100:2003	172.16.1.100:23	10.0.1.2:1063	10.0.1.2:1063

对比步骤 5 观察的记录，回答下面的问题：

（1）在执行多次远程登录的情况上是否一致？

（2）对比并说明静态 NAT、动态 NAT、静态 NAPT 和动态 NAPT 的各自特点和适合的应用环境。

4.4.2 DHCP 配置实验

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）基于 Client/Server 工作模式，网络中配置 DHCP 服务的目的是为需要动态配置的主机分配 IP 地址和提供各种主机配置参数。使用 DHCP 服务可以简化管理员对网络内部用户的管理，用户只需要通过 DHCP 来自动获取地址，而不用去了解诸如子网掩码、缺省网关、DNS 和 WINS 服务器地址的具体细节。

1．DHCP 概述

由于扩展方便、容易管理，通常管理员喜欢使用 Windows/Linux 服务器来提供 DHCP 服务。虽然如此，网络设备厂商所提供的网络设备一般也提供了可选的、具有全部特性的 DHCP 服务配置。

RGNOS 软件的 DHCP 服务器完全根据 RFC 2131 实现，主要功能就是为主机分配和管理 IP 地址。DHCP 工作的基本流程如图 4.24 所示：

图 4.24 DHCP 基本工作流程

DHCP 请求 IP 地址的过程可以概括如下：

（1）主机发送 DHCPDISCOVER 广播包在网络上寻找 DHCP 服务器；

（2）DHCP 服务器向主机发送 DHCPOFFER 单播数据包，包含 IP 地址、MAC 地址、域名信息以及地址租期；

（3）主机发送 DHCPREQUEST 广播包，正式向服务器请求分配已提供的 IP 地址；

（4）DHCP 服务器向主机发送 DHCPACK 单播包，确认主机的请求。

DHCP 客户端可以接收到多个 DHCP 服务器的 DHCPOFFER 数据包，然后可能接受任何一个 DHCPOFFER 数据包，但客户端通常只接受收到的第一个 DHCPOFFER 数据包。另外，DHCP 服务器 DHCPOFFER 中指定的地址不一定为最终分配的地址，通常情况下，DHCP 服务器会保留该地址直到客户端发出正式请求。

正式请求 DHCP 服务器分配地址 DHCPREQUEST 采用广播包，是为了让其它所有发送 DHCPOFFER 数据包的 DHCP 服务器也能够接收到该数据包，然后释放已经 OFFER（预分配）给客户端的 IP 地址。

在网络建设中，应用 DHCP 服务器，可以带来以下好处：

- 简化配置任务，降低网络建设成本

采用动态地址分配，大大简化了设备配置，对于没有专业技术人员的地方部署设备，更是降低了部署成本。

- 集中化管理

当对几个子网进行配置管理，有任何配置参数变动，只需要修改和更新 DHCP 服务器的配置。

2．DHCP 服务器配置

（1）启用 DHCP 服务器

要启用 DHCP 服务器或中继代理，全局配置模式中执行以下命令：

Red-Giant(config)#**service dhcp**

说明：在 RGNOS 早期版本（6.10 以前）中，缺省情况下，DHCP 服务器是启用的，DHCP 中继代理是关闭的，而且两者不能并存。使用 no service dhcp 可以启用 DHCP 中继代理特性，关闭 DHCP 服务器。在新版本中同时支持 DHCP 中继代理和 DHCP 服务器。

（2）DHCP 地址池配置

和 NAT 一样，DHCP 服务器需要管理员定义地址池，可以分配的地址以及给客户端传送的相关各项地址参数，都需要在 DHCP 地址池中进行定义。你可以给 DHCP 地址池起个有意义、易记忆的名字，地址池的名字由字符和数字组成。RGNOS 软件可以定义多个地址池，并根据 DHCP 请求包中的中继代理 IP 地址来决定分配哪个地址池的地址。如果 DHCP 请求包中没有中继代理的 IP 地址，就分配与接收 DHCP 请求包接口的 IP 地址同一子网的地址给客户端，如果不存在中继代理或者接口地址所在网段的地址池，则地址分配失败。

DHCP 地址池配置的必要配置命令如下：

- 配置地址池名并进入其配置模式

Red-Giant(config)# **ip dhcp pool *dhcp-pool***

- 配置地址池子网和掩码

Red-Giant(dhcp-config)# **network *network-number* [*mask*]**

地址池为 DHCP 服务器提供了一个可分配给客户端的地址空间。除非有地址排斥配置，否则所有地址池中的地址都有可能分配给客户端。DHCP 在分配地址池中的地址，是按顺序进行的，如果该地址已经在 DHCP 绑定表中或者检测到该地址已经在该网段中存在，就检查下一个地址，直到分配一个有效的地址。

DHCP 地址池配置的其它可选特性配置如下：

• 配置客户端缺省网关

Red-Giant(dhcp-config)# **default-router *address***

• 配置地址租期

Red-Giant(dhcp-config)# **lease {*days [hours] [minutes]* | infinite}**

缺省情况下租期为 1 天

• 配置客户端的域名

Red-Giant(dhcp-config)# **domain-name *domain***

• 配置域名服务器

Red-Giant(dhcp-config)# **dns-server *address***

• 配置 NetBIOS WINS 服务器

Red-Giant(dhcp-config)# **netbios-name-server *address***

（3）DHCP 排斥地址配置

如果没有特别配置，DHCP 服务器会试图将在地址池中定义的所有子网地址分配给 DHCP 客户端。因此，如果你想保留一些地址不想分配，比如已经分配给服务器或者路由器了，你必须明确定义这些地址是不允许分配给客户端的。

要配置哪些地址不能分配给客户端，在全局配置模式中执行以下命令：

Red-Giant(config)# **ip dhcp excluded-address** *low-ip-address* [*high-ip-address*]

该命令所定义范围的 IP 地址 DHCP 不会分配给客户端。取消配置地址排斥使用该命令的 no 选项：

Red-Giant(config)# **no ip dhcp excluded-address** *low-ip-address* [*high-ip-address*]

3．DHCP 中继代理及配置

DHCP 中继代理，就是在 DHCP 服务器和客户端之间转发 DHCP 数据包。当 DHCP 客户端与服务器不在同一个物理网络上，就必须有 DHCP 中继代理来转发 DHCP 请求和应答消息。DHCP 中继代理的数据转发，与通常路由转发是不同的，通常的路由转发相对来说是透明传输的，路由器一般不会修改 IP 包内容。而 DHCP 中继代理接收到 DHCP 消息后，重新生成一个 DHCP 消息，然后转发出去。

在 DHCP 客户端看来，DHCP 中继代理就象 DHCP 服务器；在 DHCP 服务器看来，DHCP 中继代理就像 DHCP 客户端。

通常情况下，使用接入层交换机来做 DHCP 中继代理，其配置如下：

Switch(config)# **ip helper-address *address***

由于 DHCP 中继代理设备通过 helper-address 指定了 DHCP 服务器的地址，因此在转发 DHCP 请求时使用单播方式，这样可以限制广播流量，同时也有效防止了网络内部潜在的“伪装 DHCP 服务器”所导致的网络攻击。

4．实验环境与说明

（1）实验目的

了解 DHCP 协议的工作过程；掌握 RGNOS 中 DHCP 服务器和中继代理的配置。

（2）实验设备和连接

实验设备和连接如图 4.25 所示：

一台 S3550 三层交换机连接两台测试计算机，并通过开启三层接口 F0/1 连接 R1762 路由器。在路由器上配置服务器，通过交换机的中继代理为 VLAN10 和 VLAN20 中的计算机提供 DHCP 服务。

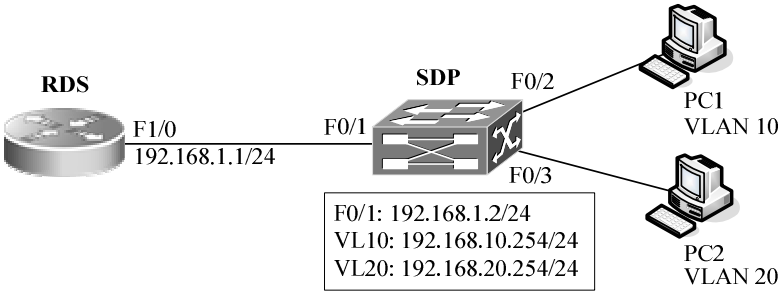


图 4.25 DHCP 的配置实验

（3）实验分组

每四名同学为一组，其中每两人一小组，每小组各自独立完成实验。

5．实验步骤

步骤 1：完成设备连接和设备名配置：

R1762 配置设备名为 RDS，S3550 配置设备名为 SDP；

步骤 2：设备接口配置：

路由器的配置比较简单，只要设置 F1/0 接口即可：

```
RDS(config)#interface fastEthernet 1/0
RDS(config-if)#ip address 192.168.1.1 255.255.255.0        ！接口地址配置
RDS(config-if)#no shutdown
RDS(config-if)#exit
```

三层交换机则需要完成 F0/2 和 F0/3 接口的 VLAN 配置以及三层接口 F0/1 和 SVI 接口的配置，其中 VLAN 配置参考如下：

```
SDP(config)#vlan 10                                        ！开启 VLAN10
SDP(config-vlan)#exit
SDP(config)#vlan 20                                        ！开启 VLAN20
SDP(config-vlan)#exit
SDP(config)#interface fastEthernet 0/2
SDP(config-if)#switchport access vlan 10                   ！接口指派 VLAN
SDP(config-if)#exit
SDP(config)#interface fastEthernet 0/3
SDP(config-if)#switchport access vlan 20                   ！接口指派 VLAN
SDP(config-if)#end
```

三层接口 F0/1 参考配置如下：

```
SDP(config)#interface fastEthernet 0/1
SDP(config-if)#no switchport                               ！开启三层接口
SDP(config-if)#ip address 192.168.1.2 255.255.255.0        ！地址配置
SDP(config-if)#no shutdown
SDP(config-if)#exit
```

VLAN10 和 VLAN20 的 SVI 接口配置如下：

```
SDP(config)#interface vlan 10                              ！VL10 的 SVI 接口配置
SDP(config-if)#ip address 192.168.10.254 255.255.255.0
SDP(config-if)#exit
SDP(config)#interface vlan 20                              ！VL20 的 SVI 接口配置
SDP(config-if)#ip address 192.168.20.254 255.255.255.0
```

SDP(config-if)#end

完成配置后，可以使用 show vlan 和 show ip interface 检查配置信息。

步骤 3：设备连通配置：

使用静态路由完成实验设备的网络连通。

三层交换机的配置如下：

SDP(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1

路由器的配置如下：

RDS(config)#ip route 192.168.10.0 255.255.255.0 192.168.1.2

RDS(config)#ip route 192.168.20.0 255.255.255.0 192.168.1.2

完成配置后使用 show ip route 验证路由配置信息，并使用 ping 命令验证设备连通。

RDS#ping 192.168.1.2

Sending 5, 100-byte ICMP Echoes to 192.168.1.2, timeout is 2 seconds:

< press Ctrl+C to break >

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

步骤 4：DHCP 服务器配置：

在路由器上配置 DHCP 服务器，为 VLAN10 和 VLAN20 指定地址池，子网掩码和缺省网关。

```
RDS(config)#service dhcp                                  ！开启 DHCP 服务
RDS(config)#ip dhcp pool DHCP_POOL_VL10                   ！创建 DHCP 地址池
RDS(dhcp-config)#network 192.168.10.0 255.255.255.0       ！指定地址池网段（VL10）
RDS(dhcp-config)#default-router 192.168.10.254            ！指定缺省网关
RDS(dhcp-config)#exit
RDS(config)#ip dhcp pool DHCP_POOL_VL20                   ！创建 DHCP 地址池
RDS(dhcp-config)#network 192.168.20.0 255.255.255.0       ！指定地址池网段（VL20）
RDS(dhcp-config)#default-router 192.168.20.254            ！指定缺省网关
RDS(dhcp-config)#end
```

步骤 5：DHCP 中继代理配置：

在三层交换机上配置 DHCP 中继代理，执行如下：

```
SDP(config)#service dhcp                                  ！开启 DHCP 服务
SDP(config)#ip helper-address 192.168.1.1                 ！指定代理的服务器
```

步骤 6：验证与测试：

按照实验拓扑，设置 PC1 的 IP 地址为自动获取，完成连接后开启测试网卡。

成功派发地址后，可以使用 show ip dhcp server statistics 命令查看 DHCP 服务器信息：

```
RDS#show ip dhcp server statistics
Lease counter                1
Address pools                2
Automatic bindings           1
Manual bindings              0
Expired bindings             0
Malformed messages           0

Message                      Received
BOOTREQUEST                     4
```

DHCPDISCOVER	1
DHCPREQUEST	1
DHCPDECLINE	0
DHCPRELEASE	0
DHCPINFORM	2

Message	Sent
BOOTREPLY	4
DHCPOFFER	1
DHCPACK	3
DHCPNAK	0

思考：在上面的提示信息中，DHCP 服务的租期是多少？配置了几个地址池？已经派发出的地址有几个？

已派发地址的绑定信息可以使用 show ip dhcp binding 查看，例如：

RDS#show ip dhcp binding

IP address	Hardware address	Lease expiration	Type
192.168.10.1	001e.907c.658d	1 days 23 hours 58 mins	Automatic

步骤 7：DHCP 排斥地址配置与测试：

在路由器上配置 VLAN20 的排斥地址，执行如下：

RDS(config)#ip dhcp excluded-address 192.168.20.1 192.168.20.100

RDS(config)#ip dhcp excluded-address 192.168.20.201 192.168.20.254

而后设置 PC2 的 IP 地址为自动获取，完成连接后开启测试网卡。如图 4.26 所示，通过 DHCP 指派成功获得了地址参数。

图 4.26 网络适配器状态

思考并回答下面的问题：

（1）在当前的 DHCP 服务配置中，VLAN10 对应的地址池的有效地址范围是多少？VLAN20 的又是多少？

（2）配置 DHCP 排斥地址的目的是什么？

（3）如果网络中某主机静态配置了地址池中的 IP 地址，新的客户申请地址时是否会出现地址冲突？

步骤 8：DHCP 调试命令与验证

成功完成步骤 1～7 后，使用 show ip dhcp binding 查看指派地址绑定信息，并完成下表：

表 4.10 地址绑定信息

IP 地址	MAC 地址	租期	类型

要进行 DHCP 服务器的调试，应该在命令执行模式中执行以下命令：

Red-Giant# **debug ip dhcp server** {**events**| **packet**}

我们可以通过调试信息进一步了解 DHCP 服务的执行过程。

首先，禁用测试 PC 的网卡，而后清除 DHCP 地址的绑定信息，执行如下：

RDS#clear ip dhcp binding *

而后打开 DHCP 服务调试，执行如下：

RDS#debug ip dhcp server

最后，再次开启网卡，重新获取地址，可以看到如下的提示信息：

recv dhcp packet from interface 2, 192.168.1.2, len=300

dhcpd.c, 893 Server id =0.0.0.0

dhcpd.c, 880 Server id =0.0.0.0

dhcpd listen on udp port 67

dhcpd.c, 809 Server id =0.0.0.0

Packet type : DHCP Discover

op = 1　htype = 1　hlen = 6　hops = 1

xid = 6ea1c212　secs = 0　flags = 0

ciaddr = 0.0.0.0

yiaddr = 0.0.0.0

siaddr = 0.0.0.0

giaddr = 192.168.20.254

chaddr = 00:1e:90:7c:65:8d

……

限于篇幅，这里只给出了最前面的提示信息，DHCP Discover、DHCP Offer、DHCP Request 和 DHCP Ack 报文的具体提示请查看自己的调试结果。认真阅读并回答下面的问题：

（1）DHCP 基于 TCP 还是 UDP 协议？

（2）DHCP 使用的传输层端口号是多少？

（3）根据调试信息，描述实验中 DHCP 完整的工作过程。

4.4.3 单臂路由配置实验

众所周知 VLAN 间的互通可以使用三层交换机来实现，但是大多数情况企业网络搭建初期购买的仅仅是二层可管理型交换机，如果要购买三层交换机实现 VLAN 互通功能的话，以前的二层设备将可能被丢弃。这样就造成了极大的浪费。那么有没有什么办法在仍然使用二层设备的基础上，实现三层交换机的功能呢?

单臂路由就提供了这样的一种方法。

1．单臂路由

单臂路由的功能原理如图 4.27 所示：

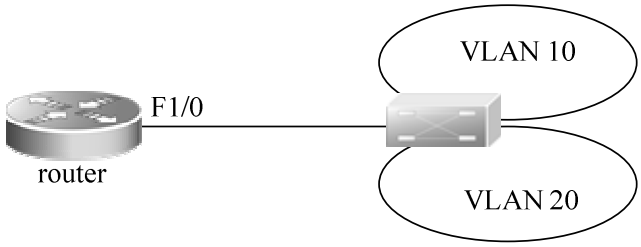


图 4.27 单臂路由示例

可以看出在 router 路由器与交换机之间是通过外部线路连接的，这个外部线路只有一

条，但是它在逻辑上是分开的，需要路由的数据包会通过这个线路到达路由器，经过路由后再通过此线路返回交换机进行转发。所以大家给这种拓扑方式起了一个形象的名字——单臂路由。说白了，单臂路由就是数据包从哪个口进去，又从哪个口出来，而不象传统网络拓扑中数据包从某个接口进入路由器又从另一个接口离开路由器。

那么什么时候要用到单臂路由呢？在企业内部网络中划分了 VLAN，当 VLAN 之间有主机需要通信，但交换机不支持三层交换，这时候就可以采用一台支持 802.1Q 的路由器实现 VLAN 的互通。

单臂路由的实现需要在以太接口上建立子接口，并分配 IP 地址作为该 VLAN 的网关，同时启动 802.1Q 协议。基本配置过程如下：

（1）进入或创建一个封装 802.1Q 的子接口

Red-Giant(config)# **interface FastEthernet *Sub_interface_number***

（2）封装 802.1Q 并指定 VLAN ID 号

Red-Giant((config-subif))# **encapsulation dot1Q *VlanID***

注意：VLAN ID 必须与交换机上的对应 VLAN ID 一致

（3）指定接口 IP 地址

Red-Giant((config-subif))# **ip address *ip-address mask***

完成封装 VLAN 标识任务以后，必须为封装 VLAN 标识的以太网子接口指定 IP 地址。显而易见，封装 802.1Q 的以太网子接口的 IP 地址一般是该 VLAN 内主机连接其他 VLAN 的网关。

2．实验环境与说明

（1）实验目的

了解单臂路由的应用环境；掌握单臂路由的配置方法。

（2）实验设备和连接

实验如图设备的连接和 IP 规划 4.28 所示：S2126 上划分 VLAN10 和 VLAN20，在路由器 R1762-B 上配置单臂路由，实现 VLAN 连通；在 R1762-B 配置缺省路由，实现本地 VLAN 的对外连接；在 R1762-A 配置静态路由，连通远端的 VLAN10 和 VLAN20。

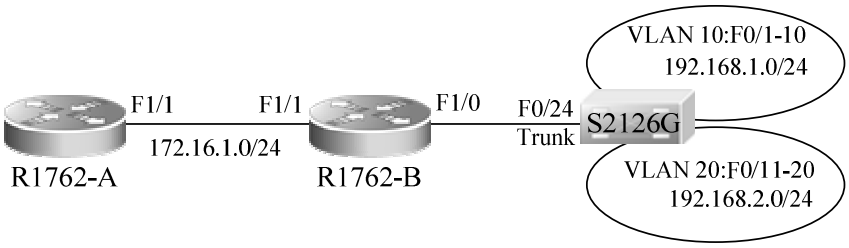


图 4.28 单臂路由的配置实验

（3）实验分组

每四名同学为一组，其中每两人一小组，每小组各自独立完成实验。

3．实验步骤

步骤 1：完成设备连接和设备名配置：

步骤 2：S2126G 的 VLAN 配置和验证：

首先，启用 VLAN10 和 VLAN20：

S2126G(config)# vlan 10

S2126G(config-vlan)# exit

S2126G(config)# vlan 20

S2126G(config-vlan)# exit

而后按照要求把 F0/1-10 接口指派给 VLAN10，F0/11-20 接口指派给 VLAN20：

```
S2126G(config)# interface range fastEthernet 0/1-10
S2126G(config-if-range)# switchport access vlan 10
S2126G(config-if-range)# exit
S2126G(config)# interface range fastEthernet 0/11-20
S2126G(config-if-range)# switchport access vlan 20
S2126G(config-if-range)# exit
```

最后，配置 F0/24 接口为 Trunk：

```
S2126G(config)# interface fastEthernet 0/24
S2126G(config-if)# switchport mode trunk
S2126G(config-if)#end
```

完成配置后可以使用 show vlan 命令查看 VLAN 的配置结果，如下所示：

```
S2126G# show vlan
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/21,Fa0/22,Fa0/23
                                                 Fa0/24
10   VLAN0010                          active    Fa0/1 ,Fa0/2 ,Fa0/3
                                                 Fa0/4 ,Fa0/5 ,Fa0/6
                                                 Fa0/7 ,Fa0/8 ,Fa0/9
                                                 Fa0/10,Fa0/24
20   VLAN0020                          active    Fa0/11,Fa0/12,Fa0/13
                                                 Fa0/14,Fa0/15,Fa0/16
                                                 Fa0/17,Fa0/18,Fa0/19
                                                 Fa0/20,Fa0/24
```

步骤 3：R1762-B 的接口配置和单臂路由配置：

F1/1 的接口配置为：

```
R1762-B(config)# nterface fastEthernet 1/1
R1762-B(config-if)# ip address 172.16.1.2 255.255.255.0
R1762-B(config-if)# no shutdown
R1762-B(config-if)# exit
```

单臂路由的子接口配置为：

```
R1762-B(config)# interface fastEthernet 1/0
R1762-B(config-if)# no ip address
R1762-B(config-if)# exit
R1762-B(config)# interface fastEthernet 1/0.1
R1762-B(config-subif)# encapsulation dot1Q 10
R1762-B(config-subif)# ip address 192.168.1.1 255.255.255.0
R1762-B(config-subif)# no shutdown
%LINE PROTOCOL CHANGE: Interface FastEthernet 1/0.1, changed state to UP
R1762-B(config-subif)# exit
R1762-B(config)# interface fastEthernet 1/0.2
R1762-B(config-subif)# encapsulation dot1Q 20
R1762-B(config-subif)# ip address 192.168.2.1 255.255.255.0
```

R1762-B(config-subif)# no shutdown
%LINE PROTOCOL CHANGE: Interface FastEthernet 1/0.2, changed state to UP
R1762-B(config-subif)# exit
使用 show ip route 验证上面的配置，参考如下：
R1762-B(config)#show ip route
Codes: C - connected, S - static, R - RIP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
* - candidate default
Gateway of last resort is no set
C 172.16.1.0/24 is directly connected, FastEthernet 1/1
C 172.16.1.2/32 is local host.
C 192.168.1.0/24 is directly connected, FastEthernet 1/0.1
C 192.168.1.1/32 is local host.
C 192.168.2.0/24 is directly connected, FastEthernet 1/0.2
C 192.168.2.1/32 is local host.
可以看到路由器已经建立了直连路由。
步骤 4：R1762-A 的接口配置和静态路由配置：
F1/1 接口配置为：
R1762-A(config)# interface fastEthernet 1/1
R1762-A(config-if)# ip address 172.16.1.1 255.255.255.0
R1762-A(config-if)# no shutdown
R1762-A(config-if)# exit
对于 R1762-A 而言，需要为非直连的 VLAN10 和 VLAN20 网络配置静态路由：
R1762-A(config)# ip route 192.168.1.0 255.255.255.0 172.16.1.2
R1762-A(config)# ip route 192.168.2.0 255.255.255.0 172.16.1.2
R1762-A(config)# end
使用 show ip route 验证配置，显示参考如下：
C 172.16.1.0/24 is directly connected, FastEthernet 1/1
C 172.16.1.1/32 is local host.
S 192.168.1.0/24 [1/0] via 172.16.1.2
S 192.168.2.0/24 [1/0] via 172.16.1.2
步骤 5：R1762-B 的缺省路由配置：
由于 R1762-B 只有一条来自 R1762-A 的连接路径，因此可以配置缺省路由：
R1762-B(config)# ip route 0.0.0.0 0.0.0.0 172.16.1.1
R1762-B(config)# end
查看路由表，可以看到标有 S*的缺省路由记录，如下所示：
S* 0.0.0.0/0 [1/0] via 172.16.1.1
C 172.16.1.0/24 is directly connected, FastEthernet 1/1
C 172.16.1.2/32 is local host.
C 192.168.1.0/24 is directly connected, FastEthernet 1/0.1
C 192.168.1.1/32 is local host.
C 192.168.2.0/24 is directly connected, FastEthernet 1/0.2

C　　192.168.2.1/32 is local host.

步骤 6：综合验证：

用两台 PC 机，分别连接 S2126G 的 VLAN10 和 VLAN20 接口，按照地址规划指定 IP 地址，使用 ping 命令验证全网连通。

思考：

（1）实现不同 VLAN 间连通可以使用那些方法？

（2）单臂路由提供了一种经济的小型网络组建方式，以本实验为例，如果 R1762-B 为本地接入路由器，只有连接 R1762-A 的接口地址是唯一的全局可路由地址，如何实现内部 VLAN10 和 VLAN20 的对外访问。在刚才实验的基础上，完成所需的动态 NAPT 配置。