1 计算机网络课程设计

本章课程设计采用实验室实际操作为主，课后练习、研讨和设计为辅，结合工程实践，为一个中小型企业局域网进行拓扑设计和网络设备选型，结合模拟软件全面地分析和调试各种网络设备，完成路由、交换等实验内容，在实际操作中理解网络技术，逐步巩固和深化理论知识，从而掌握网络工程中的常用技术和实际操作技能。

1.1 网络设备与网络模拟软件

1.1.1网络设备初始配置

常用的网络设备主要有中继器、集线器、二层交换机、三层交换机和路由器等。网络设备生产厂商有很多家，主流厂家简介如表1-1所示。

表1-1 网络设备厂商简介

网络设备生产商	公司总部	产品优势
思科（CISCO）	美国（1984.12）	思科公司的经营范围几乎覆盖了网络建设的每个部分。思科制造的路由器、交换机和其他设备承载了全球80%的互联网通信。
瞻博网络（JuniperNetworks）	美国（1996.2）	Juniper的主要产品线包括广域网络加速、VF系列、E系列、J系列、M系列、T系列路由器产品家族，SRX系列防火墙，EX系列网络交换机及SDX服务部署系统等。
华为（Huawei）	深圳（1987）	华为的产品主要涉及通信网络中的交换网络、传输网络、无线及有线固定接入网络和数据通信网络及无线终端产品，为世界各地通信运营商及专业网络拥有者提供硬件设备、软件、服务和解决方案。
中兴（ZTE）	深圳（1985）	研发生产通讯设备和终端的公司，为全球160多个国家和地区的电信运营商提供创新技术与产品解决方案，通过全系列的无线、有线、业务、终端产品和专业通信服务，满足全球不同运营商的差异化需求。
锐捷网络(Ruijie)	福建福州（2001.1）	锐捷网络坚持走自主研发的道路，是中国网络解决方案领导品牌。锐捷网络已连续7年稳居企业网市场国内厂商占有率排名首位。
华三（H3C）	杭州（2003.1）	主要提供IT基础架构产品及方案的研究、开发、生产、销售及服务。截至2013年底，华三通信累计申请专利超过4700件，其中发明专利比例超过85%。2013年，华三通信有效发明专利拥有量国内排名第六。
深圳普联（TP-Link）	深圳（1996）	专门从事网络与通信终端设备研发、制造和行销的业内主流厂商，产品线覆盖网络安全、路由器、交换机、XDSL、集线器、光纤收发器、MODEM、网卡等全系列网络产品。
友讯集团（D-LINK）	台湾（1986成立）	台湾第一家上市的网络公司，以自创D-Link品牌行销全球，产品遍及100多个国家。

神州数码 (Digital China)	联想分拆的公司 (2001上市)	由原联想集团分拆而来，经营包括笔记本电脑、显示设备、移动办公设备、计算机外围设备、PC、服务器、 数码相机、手持设备、计算机配件等千余种IT产品。

在常见的网络互联设备中，中继器、集线器等都是非网管的设备，只能实现简单的网络连接，不具有可管理性。而路由器和绝大多数交换机都具有很高的智能性，能对所连接的网络实施管理，提高网络的工作效率。在网络建设中，一般不直接使用这些设备的出厂默认配置，必须对各种设备进行配置。

1、 配置网络管理设备的方式

借助计算机对网络设备进行配置和管理，一般配置访问有4种方式：

①通过PC与网络设备直接相连。

②通过Telnet对网络设备进行远程管理。

③通过Web对网络设备进行远程管理。

④通过SNMP管理工作站对网络设备进行管理。

后面三种方式均要通过网络传输，只有第一种方式通过Console口直连。大多数网络设备都有一个Console口，网络管理员利用这个端口连接用户计算机，实现对网络设备的配置管理。网络设备第一次使用的时候，必须采用通过Console口方式配置。下面介绍通过Console口访问路由器(以Cisco 2821为例），带有Console口的交换机也可用此方法，具体配置步骤如下：

（1）连接计算机COM1口和路由器的Console口，设备开机。用反转线（Rollover）连接计算机的串口和路由器的Console口，反转线的一端接在路由器的Console口上，另一端接到一个DB9-RJ45的转接头上，DB9则接到计算机的串口上，如图1-1所示。所谓的反转线就是线两端的RJ45接着上的是反的，如图1-2所示。计算机和路由器连接好后，就可以使用各种各样的终端软件配置路由器了。

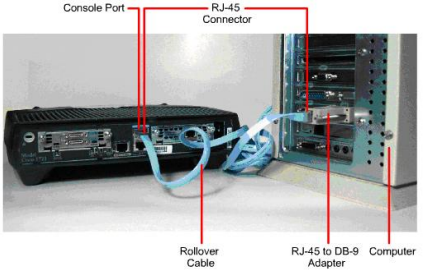


图1-1 计算机和路由器通过Console口连接

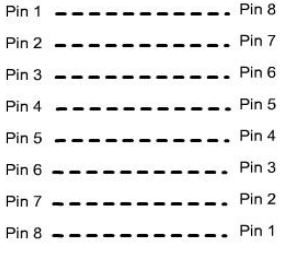


图1-2 反转线的线序

（2）打开超级终端。在Windows中的【开始】→【程序】→【附件】→【通信】菜单下打开“超级终端”程序，出现图1-3窗口。在“名称”对话框中输入名称，例如“Router”，按【确定】按钮。出现图1-4窗口时，在“连接时使用”下拉菜单中选择计算机的COM1口，按【确定】按钮。

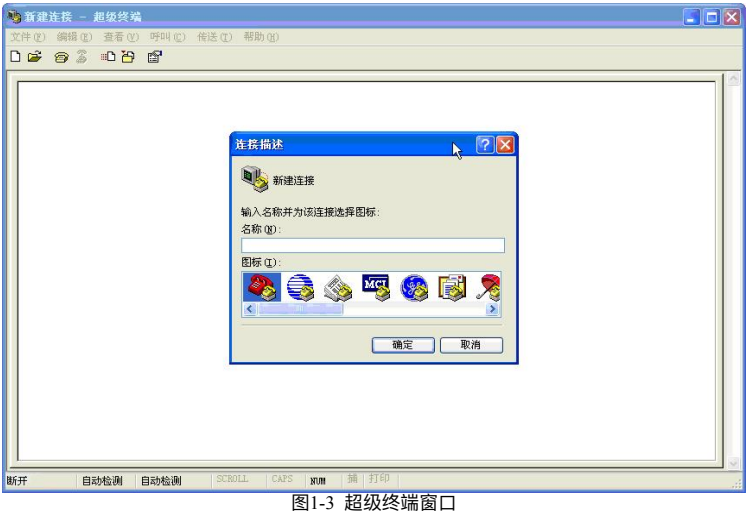


图1-3 超级终端窗口

图1-4 选择COM口

（3）设置通信参数。通常路由器出厂时，波特率为9600bps，因此在图1-5窗口中，单击【还原为默认值】按钮设置超级终端的通信参数，再单击【确定】按钮。按【回车】键，看看超级终端窗口上是否出现路由器提示符或其他字符，如果出现提示符或者其他字符，则说明计算机已经连接到路由器，我们可以开始配置路由器了。

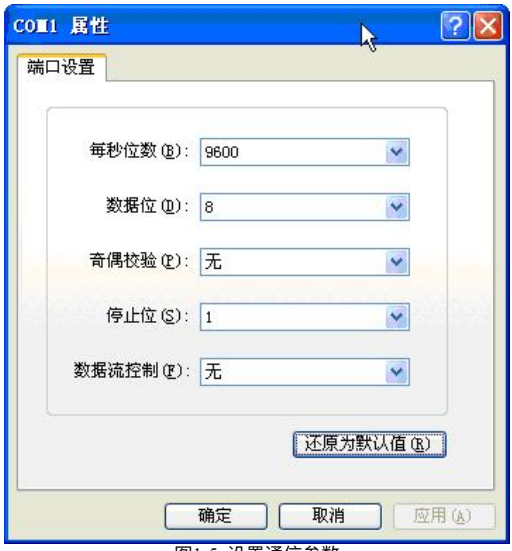


图1-5 设置通信参数

（4）关闭路由器电源，稍后重新打开电源，路由器的开机过程如下：

System Bootstrap，Version 12.4(1r)[hqluong 1r]，RELEASE SOFTWARE(fc1)
//以上显示BOOT ROM的版本
Copyright(c)2005by Cisco Systems，Inc.
Initializing memory for ECC
C2821 processor with 262144 Kbytes of main memory
Main memory is configured to 64 bit mode with ECC enabled
//以上显示路由器的内存大小
Readonly ROMMON initialized
Program load compleate，entry point :0x8000f000，size:0x274bf4c
Self decompressing the image:
##

##[OK]
//以上是IOS解压过程
Smart Init is enabled
Smart init is sizing iomem
ID MEMORY_REQ TYPE

0x003DA000 C2821 Mainboard

0x00264050 Onboard VPN

0x000021B8 Onboard USB

0x002C29F0 public buffer pools

0x0021000 public particle pools
TOTAL: 0x00B13BF8

.....(省略)
A summary of U.S.laws governing Cisco cryptographic products may be found at:
http://www.Cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to

export@Cisco.com
Installed image archive
Cisco 2821（revision49.46）with249856K/12288Kbytes of memory. //内存大小
Processor board ID FHK 1039F21Q
2 Gigabit Ethernet interfaces //两个千兆位以太网接口
2 Low-speed serial(sync/async)interfaces //两个低速串行口（同步/异步）
1 Virtual Provate Network(VPN)Module //一个VPN网络模块
DRAM configuration is 64 bits wide with parity enabled
239Kbyest of non- volatile configuration memory. //NVRAM的大小
62720Kbytes of ATA conmpactFlash(Read/Write) //FLASH卡的大小
---System Configration Dialog---
Continue with configuration dialog? [yes/no]
//以上提示是否进入配置对话模式？一般回答“no”结束该模式

当网络设备已配置好IP地址后，还可以用相应线缆连接网络设备以太口，通过Telnet等方式连接配置设备。

2、交换机基本配置

交换机配置操作是衡量网管人员水平高低的一个重要标志。交换机管理界面分为用户模式、特权模式和配置模式，用户当前所处的命令模式决定了可以使用的命令。使用交换机附带的串口电缆连接交换机的Console口和计算机的串口（RJ-45口）。在计算机中，选择【开始】→【程序】→【附件】→【通信】菜单下打开”超级终端”程序，“开始”“程序”“附件”“通信”“超级终端”命令，按照前面介绍的操作步骤进入交换机的用户状态。

Switch>

注意：交换机不需配置(采用默认配置直)可直接工作，如果在启动过程中出现很多提示信息，按Ctrl+C组合键可以跳过Setup配置，直接进入用户模式工作状态。

当用户和交换机管理界面建立一个新的会话连接时，用户首先处于用户模式，可以使用用户模式的命令。在命令提示符下输入问号可以列出每个命令模式可以使用的命令。Catalyst 2950交换机的基本配置步骤如下：

（1）配置主机名

Switch>enable
//进入交换机的特权模式
Switch#conf terminal
Enter configuration commands，one per line. End with CNTL/Z
//进入交换机的配置模式
Switch(config)#hostname S1
//将交换机命名为S1

（2） 配置密码

S1(config)#enable secret cisco
S1(config)#line vty 0 15
//以上是进入交换机的VTY虚拟终端，“vty0 15”表示vty0到vty15，共16个虚拟终端
S1(config-line)#passwrod cisco
S1(config-line)#login
//配置vty的密码，即Telnet密码，使用Telnet，必须先设置密码

（3）接口基本配置

交换机的以太网接口默认是开启的，对于交换机的以太网口可以配置其双工模式和速率等。

S1(config)#interface f0/1
switch(config-if)#duples{full|half|auto}
//duplex来用配置接口的双工模式：full——全双工；half——半双工；auto——自动检测双工的模式
switch(config-if)#speed{10|100|1000|auto}
//speed命令用来配置交换机的接口速度，10——10Mbps；100——100 Mbps；1000——1000 Mbps；auto——自动检测接口速度

（4）配置管理地址

交换机也允许被Telnet，这时需要在交换机上配置一个IP地址，这个地址是在VLAN接口上配置的。如下：

S1(config)#int vlan 1
S1(config-if)#ip address 172.16.0.1 255.255.0.0
S1(config-if)#no shutdown

S1(config)#ip default-gateway 172.16.0.254

//以上在VLAN1接口上配置了管理地址，接在VLAN1上的计算机可以直接Telnet该地址。为了其他网段的计算机也可以Telnet交换机，我们在交换机上配置了默认网关。

（5）保存配置

S1#copy running-config startup-config

Destination filename[startup-config]?

Building configuration...

［OK］

3、路由器基本配置

路由器实际上是一台特殊用途的计算机，和常见的PC一样，路由器有CPU、内存和BOOT ROM。和计算机相比，路由器没有键盘、硬盘和显示器，但多了NVRAM、FLASH及各种各样的接口。

路由器能根据IP包头的信息来选择一条最佳的路径，将数据包发送实现不同网段主机之间的互相访问。路由器是按路由表进行选路和转发的，路由表由逐条的路由信息构成，可以通过以下三种方式产生：

①直接路由：只要给路由器端口分配IP地址，路由器会自动产生本端口IP所在的IP段的路由信息。

②静态路由：在简单的网络拓扑中，可以通过手动的方式配置路由器的未知网段的路由信息，实现网络的互连。

③动态路由：在复杂的网络拓扑中，可以通过在路由器上运行路由协议，由路由器之间互相自动学习产生路由信息。

路由器拥有自己的操作系统，通常称为IOS（Internetwork Operating System）。和计算机上的Windows一样，IOS是路由器的灵魂，所有配置是通过IOS完成的。Cisco的IOS是命令行界面（Command Line Interface，CLI），CLI有如下两种基本工作模式：

①用户模式（User Mode）：通常用来查看路由器的状态。在此状态下，无法对路由器进行配置，可以查看的路由器信息也是有限的。

②特权模式（Privilege Mode）：可以更改路由器的配置，当然也可以查看路由器的所有信息。

在CLI下，可以使用“show”命令查看存放在路由中不同部件中的信息，也在路由器的各种模式间进行切换来对路由器进行配置。

与交换机设备不一样的是，路由器不仅硬件结构复杂，还集成了丰富的协议系统。因此，路由器的配置要复杂得多，而且必须经过配置后才能正常工作。各种不同品牌的操作系同.配置方法也有所区别，但过程和原理基本相似。下面以 Cisco 2821为例，简单介绍路由器的基本配置。

Router>enable

Router#

//以上是进入路由器的特权模式

Router#configure terminal

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

Router(config)#

//以上是进入路由器的配置模式

Router(config)#interface g0/0

Router(config-if)#

//以上是进入路由器的以太网口g0/0接口， g0/0接口中g表示GigabitEthernet，0/0表示是第0个插槽中的第0个接口。S0/0/0则表示为第0个插槽中的第0个模块上的第0个串行接口

Router(config-if)#ip address 172.16.0.1 255.255.0.0

//以上是配置接口的IP地址

Router(config-if)#no shutdown

//以上是打开接口，默认路由器的所有接口都是关闭的，这一点和交换机有很大差别

Router(config-if)#end

//退出配置模式

Router#conf terminal

Router#(config)line vty 0 4

//以上是进入路由器的VTY虚拟终端下”vty 0 4”表示vty 0 到vty 4，共5个虚拟终端

Router(config-line)#password CISCO

Router(config-line)#login

//以上是配置vty的密码，即Telnet密码

Router(config-line)#exit

```
Router(config)#enable password CISCO
//以上是配置进入到路由器特权模式的密码
Router(config)#hostname R1
//将交换机命名为R1
R1(config)#end
```

1.1.2 模拟软件的使用

路由器和交换机价格昂贵，配置路由器和交换机除了使用真实设备以外，初学者学习一般使用模拟软件。常见的Cisco 网络模拟软件有Boson netsim、Dynamips、GNS3和Packet Tracer等很多种，读者可以自行选择一款使用,本章实验内容选用Packet Tracer模拟器完成。Packet Tracer是Cisco公司开发的网络入门的经典模拟器，具有真实的操作界面，比其他任何第三方软件（如Boson）更加人性化，对初学者有很大的帮助。

下载并安装Cisco Packet Tracer 6.0正式版，运行Packet Tracer，打开Packet Tracer主界面如图1-6所示。

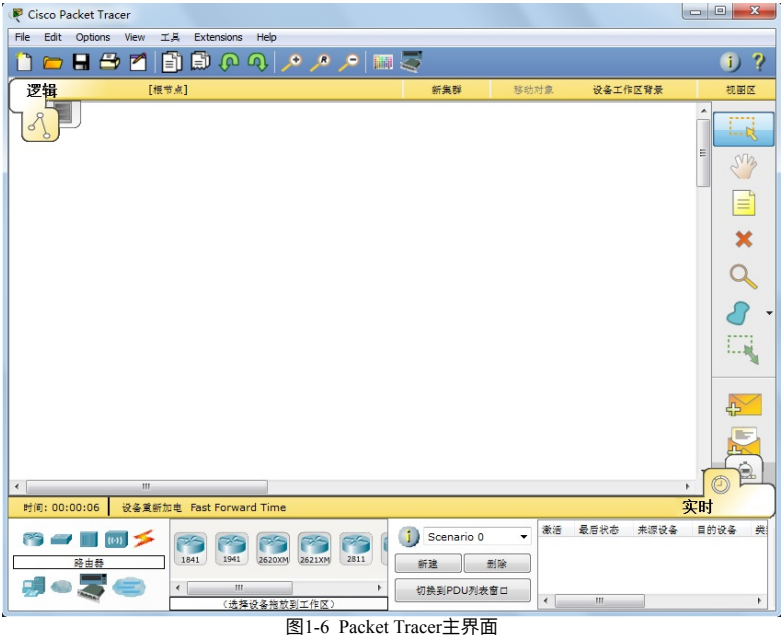


图1-6 Packet Tracer主界面

主界面提供很多选项，读者可根据实验要求选择包括路由器、交换机、集线器、无线设备、电缆、计算机、网云、用户自定义设备等各种类型的设备，添加模块，再选择合适的连接线缆，创建网络拓扑图，再对网络设备进行配置管理。在Packet Tracer中创建一个如图1-7所示的逻辑拓扑图，步骤如下：

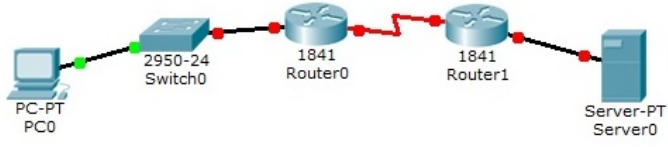


图1-7 逻辑拓扑图

（1） 添加设备

在设备选择区域，选择一台思科1841路由器，按住鼠标左键不放，将其拖入中间空白区

域。照此方法依次添加其他设备，如图1-8所示。

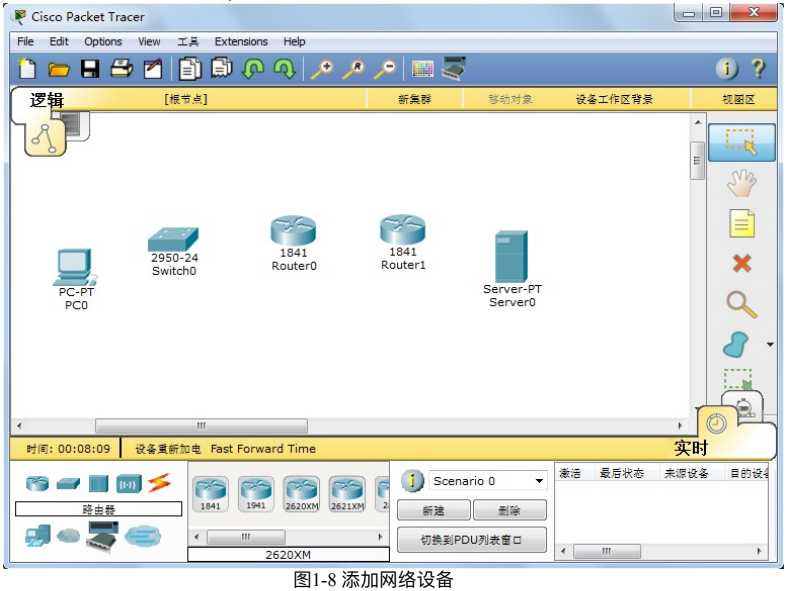


图1-8 添加网络设备

（2） 添加模块

思科1841路由器默认配置有两个快速以太网接口，但没有串行接口，如图1-9所示，因此需要加选配件。

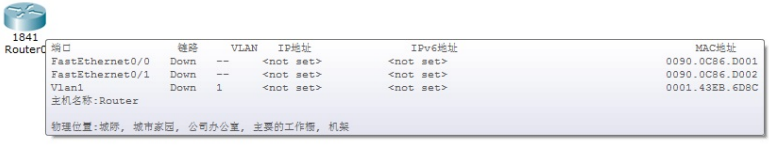


图1-9 路由器接口及状态显示

单击路由器Router0，打开如图1-10所示的窗口，可看到思科1841路由器可以支持的模块类型、具体模块的说明、模块的外观和路由器的空插槽以及电源开关等信息。先单击电源按钮，关闭路由器的电源，然后在左侧拖住WIC-2T模块放在路由器的空槽上。WIC-2T模块是有两个串行接口的小口模块。添加完模块后，再单击电源按钮，给路由器加电。使用同样的方法给其他设备添加相应模块。

图1-10 添加模块窗口

（3）添加连线

添加完网络设备和相应模块后，接下来添加它们之间的联线。Packet Tracer提供如图1-11所示的连接线缆。

图1-11 线缆类型

上图中的第一种线缆是自动线缆（根据场合自动选择线缆类型，不建议读者使用）。第二种是配置线，是连接计算机COM口和路由器或交换机Console口的线缆。第三种是直通双绞线，适合在交换机和主机、路由器和主机之间，也就是不同的设备之间互连采用。第四种是交叉双绞线，用在相同的设备间互连，如计算机和计算机、交换机和交换机之间等，但现在很多设备都具有智能性，也接受了直通线，具体要看设备说明。第五种是光纤。第六种是电话线。第七种是同轴电缆。第八种和第九种分别是DCE串口线和DTE串口线，通常用于连接思科路由器串行接口，一根串行线连接两台设备，线缆的一端为起始端DCE，配置时间钟来保持同步，另一端为终止段DTE。第十种是Octal线缆，俗称“八爪线”，多用于终端服务器连接多台其他设备。

依次选择合适的线缆连接每台设备的相应端口，如图1-12所示，完成网络拓扑图的创建，保存拓扑图。

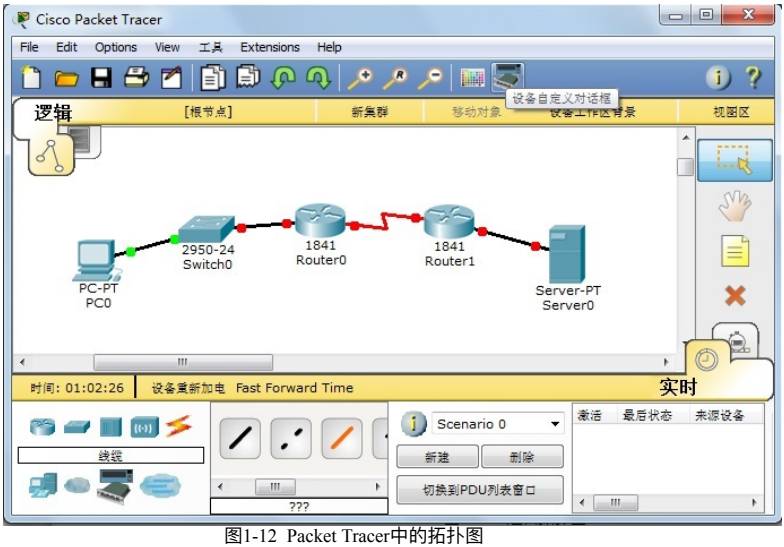


图1-12 Packet Tracer中的拓扑图

1.1.3 实验1 组建简单的以太网

以太网（Ethernet）是目前最具影响力的局域网，广泛应用于办公自动化等各个领域。通过组装以太网，可以熟悉局域网所使用的基本设备和器件，学习双绞线的制作方法，了解网卡的配置方法，掌握以太网的连通性测试方法。

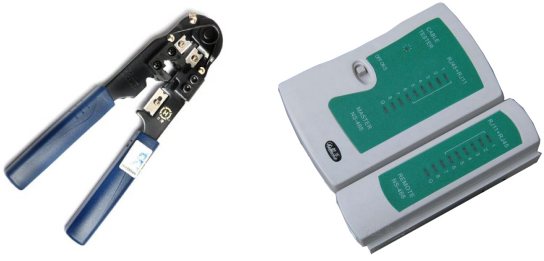
1、 所需设备、器件及工具

在动手组装以太网之前，需要准备计算机、网卡、集线器和其他网络器件。组装成100M以太网所需的设备和配件如表1-2所示。

表1-2 组建以太网所需的设备和器件

设备和器件名称	数量
PC计算机	2台以上
带RJ-45端口的100M以太网网卡	2块以上
100M以太网集线器	1台
RJ-45水晶头	4个以上
5类以上非屏蔽双绞线	若干米

除了以上设备和器件外，还需准备必要的工具，如制作网线使用的网线钳1把，以及测量电缆连通性的电缆测试仪1台，如图1-13所示。



（a）网线钳 （b）电缆测试仪

图1-13 网线钳和电缆测试仪

2、 制作双绞线

双绞线需要通过RJ-45水晶头与网卡、集线器或交换机等设备相连，双绞线与水晶头的连接须符合EIA/TIA规范，包括T568A和T568B两种标准，其规定的线序标准如表1-3所示。

表1-3 线序标准

引针号	1	2	3	4	5	6	7	8
T568A	白/绿	绿	白/橙	蓝	白/蓝	橙	白/棕	棕
T568B	白/橙	橙	白/绿	蓝	白/蓝	绿	白/棕	棕

在同一网络中，如用集线器到网卡的连接线，双绞线两端用同一标准T568B，如图1-14所示，这就是直通双绞线，也叫正线；当双绞线连接网卡到网卡时，线的一端使用T568A，另一端使用T568B，如图1-15所示，这就是交叉双绞线，也叫反线。用于集线器或交换机之间级联的双绞线，其接线标准要看具体的集线器和交换机，有些要求使用直通电缆，有些要求使用交叉电缆。

图1-14 常规双绞线接法

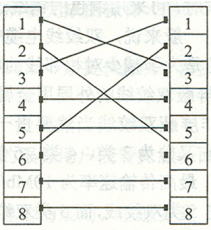


图1-15 交叉双绞线接法

直通双绞线的制作方法如下：

1) 剪断：利用网线钳的剪线刀口剪取适当长度的网线。

2) 剥线：用网线钳的剪线刀口将线头剪齐，再将线头放入剥线刀口，让线头触及前挡板，然后适度握紧压线钳同时慢慢旋转双绞线，让刀口划开双绞线的保护胶皮，拔下胶皮。

3) 理线：剥去外包皮后即可见到双绞线的4对8根线，并且可以看到每对的颜色都不同，按照表1-3所示的线序标准，拆开、理顺、捋直，然后将线序排列整齐。

4) 剪齐：把线尽量拉直(不要缠绕) 、压平(不要重叠) 、挤紧理顺(朝一个方向紧靠), 然后用压线钳把线头剪平齐。这样，在双绞线插入水晶头后，每条线都能良好接触水晶头中的 插针，避免接触不良。如果以前剥的皮过长，可以在这里将过长的细线剪短，保留的去掉外层绝缘皮的部分约为14mm, 这个长度正好能将各细导线插入到各自的线槽。如果该段留得过长，一方面由于线对不再互绞而增加串扰，另一方面由于水晶头不能压住护套而可能导致电缆从水晶头中脱出，造成线路的接触不良甚至中断。

5) 插入：用拇指和中指捏住水晶头，使有塑料弹片的一侧向下，针脚一方朝向远离自己的方向，并用食指抵住；另一手捏住双绞线外面的胶皮，缓缓力用将8条导线同时沿RJ-45头内的8个线槽插入，一直插到线槽的顶端。

6) 压线：确认所有导线都到位，并检查水晶头的线序无误后，就可以用压线钳压制RJ-45头了。将RJ-45头从无牙的一侧推入压线钳夹槽后，用力握紧线钳，将突出在外面的针脚全部压入水晶头内。

在把水晶头的两端都做好后即可用网线测试仪进行测试，如果测试仪上8个指示灯都依次为绿色闪过，证明网线制作成功。如果出现任何一个灯为红灯或黄灯，就证明存在断路或接触不良现象，此时最好先对两端水晶头再用网线钳压一次，再测，如果故障依然存在，再检查一下两端芯线的排列顺序是否正确，将不正确的那端剪掉重新制作水晶头。如果芯线顺序正确，但测试仪在重测后仍显示红色灯或黄色灯，则表明其中存在芯线接触不好。此时只穿先剪掉一端重做一个水晶头，再测，如果故障消失，则不必重做另一端水晶头，否则还得把另一端水晶头也剪掉重做。直到测试全为绿色指示灯闪过为止。制作的方法不同测试仪上的指示灯亮的顺序也不同，如果制作的是直通线，则测试仪上的灯应该是依次顺序的亮；如果制作的是交叉双绞线，则测试仪的另一端闪亮顺序应该是3、6、1、4、5、2、7、8 。

3、组建简单的以太网

将网卡安装在计算机上，在计算机使用的操作系统中正确配置IP地址、网关和DNS等信息。利用制作好的双绞线将计算机和集线器连接起来，就组成了一个如图1-16所示的简单以太网了。

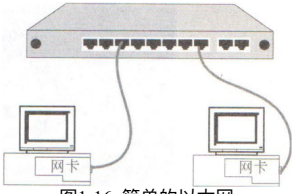


图1-16 简单的以太网

4、 网络连通性测试

在完成计算机与集线器连接之后，需要测试网络的连通性，以保证网络的畅通。大部分集线器和部分网卡都可以通过观察其状态指示灯的变化情况来了解网络的连通情况。我们通常使用网络测试命令来检查网络的连通性。

在计算机的Windows中的【开始】→【程序】→【附件】→【命令提示符】菜单下打开“命令提示符”界面（在运行栏中输入“cmd”命令也可打开该界面），输入“ipconfig /all”命令，察看当前的TCP/IP、MAC地址、DNS和WINS服务器配置的设置值，如图1-17所示。

图1-17 ipconfig /all显示的结果

使用“ping”命令ping另一台主机的IP地址，测试网络连通性。“ping”命令是测试网络连通性最常用的命令之一。它通过发送数据包到对方主机，再由对方主机将该数据包返回来测试网络的连通性。如果测试成功，命令将给出测试包发出到收回所用的时间，在以太网中，这个时间通常小于10ms。“ping”命令的测试成功不仅表示网络的是有效的，而且也表示操作系统中网络通信模块的运行是正确的。如果网络不通，“ping”命令将给出超时提示。这时，需要重新检查网络的硬件和软件，直到ping通为止。

1.2 路由实验

路由器最主要的功能就是转发数据包。互联网实际上就是由具有路由选择功能的路由器将多个网络连接所组成的。路由器在转发数据包时，要先在路由表（Routing Table）中查找相应的路由。

本节主要介绍静态路由与默认路由、RIP协议的基本配置，以及利用路由器实现DHCP和NAT等功能。

1.2.1 实验2 静态路由

路由器由直连网络、静态路由和动态路由等途径建立路由表。静态路由简单、路由负载小、可控性强，在小型网络中经常被使用。通过该实验，读者可以理解路由表的概念，掌握ip route命令的使用，能根据需求正确配置静态路由和默认路由。

1、 实验拓扑

实验拓扑图如图1-18所示。

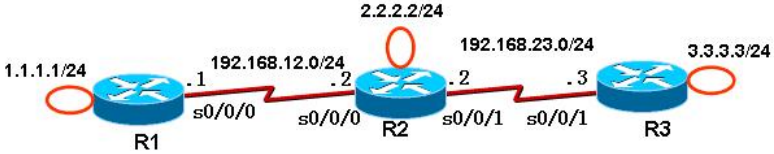


图1-18 静态路由和默认路由实验拓扑图

2、实验步骤

要使1.1.1.0/24，2.2.2.0/24和3.3.3.0/24网络能够互相通信，可按如下所述配置静态路由。

（1） 在各路由器上配置IP地址，保证直连链路的连通性

```
R1(config)#int loopback0
R1(config-if)#ip address 1.1.1.1 255.255.255.0
//以上配置Loopback 0接口的IP地址，Loopback接口是一个逻辑上的接口，路由器上可以任意创建无穷多个Loopback接口，该接口可以永远是UP的。Loopback接口经常用于测试等
R1(config)#int s0/0/0
R1(config-if)#ip address 192.168.12.1 255.255.255.0
R1(config-if)#no shutdown
//以上配置路由器的串口s0/0/0接口，s0/0/0表示为第0个插槽中的第0个模块上的第0个串行接口，并激活端口
R2(config)#int loopback0
R2(config-if)#ip address 2.2.2.2 255.255.255.0
R2(config)#int s0/0/0
R2(config-if)#clock rate 128000
R2(config-if)#ip address 192.168.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config)#int s0/0/1
R2(config-if)#clock rate 128000
//R2这一端是DCE，需要配置时钟
R2(config-if)#ip address 192.168.23.2 255.255.255.0
R2(config-if)#no shutdown
R3(config)#int loopback0
R3(config-if)#ip address 3.3.3.3 255.255.255.0
R3(config)#int s0/0/1
R3(config-if)#clock rate 128000
R3(config-if)#ip address 192.168.23.1 255.255.255.0
R3(config-if)#no shutdown
```

（2） 在R1上配置静态路由

```
R1(config)#ip route 2.2.2.0 255.255.255.0 s0/0/0
//下一跳为接口形式，s0/0/0是点对点的链路，注意：应该是R1上的s0/0/0
R1(config)#ip route 3.3.3.0 255.255.255.0 192.168.12.2
//下一跳为IP地址形式，192.168.12.2是R2上的IP地址
```

注意：以上两种方式都可配置静态路由，我们一般选用第二种IP地址形式

（3） 在R2上配置静态路由

```
R2(config)#ip route 1.1.1.0 255.255.255.0 s0/0/0
R2(config)#ip route 3.3.3.0 255.255.255.0 s0/0/1
R2(config)#ip route 1.1.1.0 255.255.255.0 192.168.1.1
R2(config)#no ip route 1.1.1.0 255.255.255.0 192.168.1.1
//配置路由，输错了路由出口地址192.168.12.1，可以在该命令前加no，删除该条路由。
R2(config)#ip route 1.1.1.0 255.255.255.0 192.168.12.1
```

（4） 在R3上配置静态路由

```
R3(config)#ip route 1.1.1.0 255.255.255.0 s0/0/1
R3(config)#ip route 2.2.2.0 255.255.255.0 s0/0/1
```

3、实验调试

（1）在R1，R2，R3上查看路由表

```
R1#show ip route
Codes: C - connected， S - static， I - IGRP， R - RIP， M - mobile， B - BGP
       D - EIGRP， EX - EIGRP external， 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， E - EGP
       i - IS-IS， L1 - IS-IS level-1， L2 - IS-IS level-2， ia - IS-IS inter area

        * - candidate default， U - per-user static route， o – ODR

        P - periodic downloaded static route
Gateway of last resort is not set
    C    192.168.12.0/24 is directly connected， Serial0/0/0
     1.0.0.0/24 is subnetted， 1 subnets
    C          1.1.1.0 is directly connected， Loopback0

             2.0.0.0/24 is subnetted， 1 subnets
    S          2.2.2.0 is directly connected， Loopback0
        3.0.0.0/24 is subnetted， 1 subnets
    S          3.3.3.0［1/0］via 192.168.12.2
    R2#show ip route
    Codes: C - connected， S - static， I - IGRP， R - RIP， M - mobile， B - BGP
        D - EIGRP， EX - EIGRP external， 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， E - EGP
        i - IS-IS， L1 - IS-IS level-1， L2 - IS-IS level-2， ia - IS-IS inter area
        * - candidate default， U - per-user static route， o - ODR
        P - periodic downloaded static route
    Gateway of last resort is not set
    C    192.168.12.0/24 is directly connected， Serial0/0/0
        1.0.0.0/24 is subnetted， 1 subnets
    S          1.1.1.0 is directly connected， Serial0/0/0
         2.0.0.0/24 is subnetted， 1 subnets
    C          2.2.2.0 is directly connected， Loopback0
         3.0.0.0/24 is subnetted， 1 subnets
    S          3.3.3.0 is directly connecte，Serial0/0/1
    C    192.168.12.0/24 is directly connected， Serial0/0/1
    R3#show ip route
    Codes: C - connected， S - static， I - IGRP， R - RIP， M - mobile， B - BGP
        D - EIGRP， EX - EIGRP external， 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， E - EGP
        i - IS-IS， L1 - IS-IS level-1， L2 - IS-IS level-2， ia - IS-IS inter area
        * - candidate default， U - per-user static route， o - ODR
        P - periodic downloaded static route
    Gateway of last resort is not set
        1.0.0.0/24 is subnetted， 1 subnets
    S          1.1.1.0 is directly connected， Serial0/0/1
         2.0.0.0/24 is subnetted， 1 subnets
    S          2.2.2.0 is directly connected， Serial0/0/1
         3.0.0.0/24 is subnetted， 1 subnets
    C          3.3.3.0 is directly connecte，Loopback0
    C    192.168.23.0/24 is directly connected， Serial0/0/1
```

（2）从各路由器的环回口ping其他路由器的环回口

```
R1#ping 2.2.2.2 source loopback 0
Type escape sequence to abort.
Sending 5， 100-byte ICMP Echos to 2.2.2.2， timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
```

！！！！！
Success rate is 100 percent (5/5)，round-trip min/avg/max = 12/14/16 ms
//从R1的loopback 0应该可以ping通R2的loopback 0接口

*** 模拟器不支持这种方式ping。可用以下模式ping：

```
R1#ping
Protocol [ip]:
Target IP address: 2.2.2.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 1.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/15 ms
```

R2#ping 1.1.1.1 source loopback 0
R2#ping 3.3.3.3 source loopback 0
//从R2的loopback 0应该可以ping通R1和R3的loopback 0接口
R3#ping 1.1.1.1 source loopback 0
R3#ping 2.2.2.2 source loopback 0
//从R3的loopback 0也应该可以ping通R1和R2的loopback 0接口
【提示】虽然从R1的loopback0可以ping通R3的loopback 0，数据需要以过192.168.23.0/24网络，但是在R1上，我们并没有添加192.168.23.0/24的路由。路由器转发数据包完全是根据路由表进行的，并且数据是一跳一跳地被转发的，就像接力赛似的。当从R1的loopbak 0口ping R3的loopback 0口时，IP数据包的源IP为1.1.1.1，目的IP 为 3.3.3.3 。R1路由器首先查路由表，数据包被发到了R2；R2路由器也查路由表（3.3.3.0/24路由），数据包被发到了R3；R3知道这是直连路由。R3响应R1的数据包进行类似的过程。
（3）从R1上ping 2.2.2.2，从R1上ping 3.3.3.3
R1#ping 2.2.2.2
Type escape sequence to abort.
Sending 5， 100-byte ICMP Echos to 2.2.2.2， timeout is 2 seconds:
！！！！！
Success rate is 100 percent (5/5)，round-trip min/avg/max = 12/14/16 ms
//可以ping 通
R1#ping 3.3.3.3
Type escape sequence to abort.
Sending 5， 100-byte ICMP Echos to 3.3.3.3， timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
//以上无法ping 通，原因在于使用ping命令时，如果不指明源接口，则R1路由器使用s0/0/0接口的IP地址（192.168.12.1）作为IP数据包的源IP地址。当R3上响应R1的数据包时，数据包是发向192.168.12.1的。然而，由于R3没有192.168.12.0/24的路由，数据包无法发送。即：数据包从R1到了R3后，无法返回R1。
4、配置默认路由
从R1上ping 3.3.3.3不通，是因为数据包从R1到了R3后，无法返回R1。因此，应给每个路由器配置一条默认路由，当路由器转发数据包时，在路由表中找不到相应的路由时，将自动选

择默认路由转发该数据包。

R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.12.2

R2(config)#ip route 0.0.0.0 0.0.0.0 192.168.12.1

//R2实际上由两个路由出口：R1上的192.168.12.1和R3上的192.168.23.3端口，可随便选择其中一个。

R3(config)#ip route 0.0.0.0 0.0.0.0 192.168.23.2

再次从各路由器的环回口ping其他路由器的环回口。比较两次ping的结果，仔细分析原因。

5、命令汇总

表1-4列出了本实验涉及到的主要命令。

表1-4 静态路由命令汇总

命令	作用
ip route	配置静态路由
no ip route1.1.1.0 255.255.255.0 192.168.1.1	删除指定路由
show ip route	查看路由表
ping 2.2.2.2 source loopback 0	指定源端口进行ping 测试
show running-config	显示正在使用的配置参数

1.2.2 实验3 RIP基本配置

动态路由协议包括距离向量路由协议和链路状态路由协议。RIP（Routing Information Protocol，路由信息协议）是使用最广泛的距离向量协议。

RIP是由Xerox在２０世纪７０年代开发的，最初定义在RFC1058，分为版本1和版本2。RIP用两种数据包传输更新：更新和请求，每个有RIP功能的路由器在默认情况下，每隔30 s利用UDP520端口向与它直连的网络邻居广播(RIPv1)或组播(RIPv2)路由更新。现在一般使用RIPv2版本。

1、拓扑结构

实验拓扑图如图1-19所示。

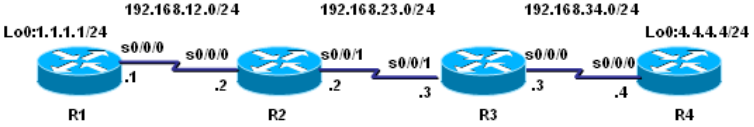


图1-19 RIP基本配置

2、实验步骤

（1）步骤1：配置路由器R1

R1(config)#router rip　　//启动RIP进程

R1(config-router)#version 2　　//配置RIP版本2

R1(config-router)#no auto-summary　　//关闭自动汇总

R1(config-router)#network 1.0.0.0　　//通告网络

R1(config-router)#network 192.168.12.0

（2）步骤2：配置路由器R2

R2(config)#router rip

R2(config-router)#version 2

R3(config-router)#no auto-summary

R2(config-router)#network 192.168.12.0

R2(config-router)#network 192.168.23.0

（3）步骤3：配置路由器R3

R3(config)#router rip

R3(config-router)#version 2

R3(config-router)#no auto-summary

R3(config-router)#network 192.168.23.0

R3(config-router)#network 192.168.34.0

（4）步骤4：配置路由器R4

R4(config)#router rip

R4(config-router)#version 2

R4(config-router)#no auto-summary
R4(config-router)#network 192.168.34.0
R4(config-router)#network 4.0.0.0
3、实验调试
（1）show ip route
该命令用来查看路由表
R1#show ip route
Codes: C - connected， S - static， R - RIP， M - mobile， B - BGP
D - EIGRP， EX - EIGRP external， 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
i - IS-IS， su - IS-IS summary， L1 - IS-IS level-1， L2 - IS-IS level-2
ia - IS-IS inter area， * - candidate default， U - per-user static route
o - ODR， P - periodic downloaded static route
Gateway of last resort is not set
C 192.168.12.0/24 is directly connected， Serial0/0/0
1.0.0.0/24 is subnetted， 1 subnets
C 1.1.1.0 is directly connected， Loopback0
4.0.0.0/8 is variably subnetted，2 subnets， 2 mask
R 4.4.4.0/24 [120/3] via 192.168.12.2， 00:00:22， Serial0/0/0
R 192.168.23.0/24 [120/1] via 192.168.12.2， 00:00:22， Serial0/0/0
R 192.168.34.0/24 [120/2] via 192.168.12.2， 00:00:22， Serial0/0/0
以上输出表明路由器R1学到了3条RIP路由，其中路由条目“R 4.4.4.0/24 [120/3] via 192.168.12.2， 00:00:03， Serial0/0/0”的含义如下。
①R：路由条目是通过RIP路由协议学习来的；
②4.4.4.0/24：目的网络；
③120：RIP路由协议的默认管理距离；
④3：度量值，从路由器R1到达网络4.4.4.0/24的度量值为3跳；
⑤192.168.12.2：下一跳地址；
⑥00:00:22：距离下一次更新还有8（30-22）s；
⑦Serial0/0/0：接收该路由条目的本路由器的接口。
从上面输出的路由条目“4.4.4.0/24”可以看到，RIPv2路由更新是携带子网信息的，而RIPv1是不传递子网信息的。
（2）show ip protocols
R1#show ip protocols
Routing Protocol is “rip”
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Sending updates every 30 seconds， next due in 19 seconds
Invalid after 180 seconds， hold down 180， flushed after 240
Redistributing: rip
Default version control: send version 2， receive version 2
Interface Send Recv Triggered RIP Key-chain
Serial0/0 2 2
Loopback0 2 2
//RIPv2在默认情况下只接收和发送版本2的路由更新
【提示】
可以通过命令”ip rip send version”和”ip rip receive version”来控制在路由器接口上接收和发送的版本。例如，在s0/0/0接口上接收版本1和版本2的路由更新，但是只发送版本2的路由更新，配置如下
R1(config-if)#ip rip send version 2
R1(config-if)#ip rip receive version 1 2
【注意】
接口特性是优于进程特性的，对于本实验，虽然在RIP进程中配置了”version 2”，但是，如果在接口上配置了”ip rip receive version 1 2”，则该接口可以接收版本1和版本2的路由更新。
4、命令汇总
表1-5列出了本实验涉及到的主要命令。
表1-5 RIP命令汇总

命令	作用
show ip route	查看路由表
show ip protocols	查看IP路由协议配置和统计信息
debug ip rip	动态查看RIP的更新过程
clear ip route *	清除路由表
route rip	启动RIP进程
networ	通告网
version	定义RIP的版本
ip rip send version	配置RIP发送的版本
ip rip receive version	配置RIP接收的版本

1.2.3 实验4 DHCP

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）采用客户/服务器（Client/Server）模式。在动态分配IP地址的方案中，每台计算机并不设定固定的IP地址，而是在计算机开机时才被分配一个IP地址，这台计算机被称为DHCP客户端，负责给DHCP客户端分配IP地址的计算机称为DHCP服务器。DHCP服务器能够从预告设置的IP地址池里自动给主机分配 IP地址，它不仅能够保证IP地址不重复分配，也能及时回收IP地址以提高IP地址的利用率。

1、拓扑结构

实验拓扑图如图1-20所示。

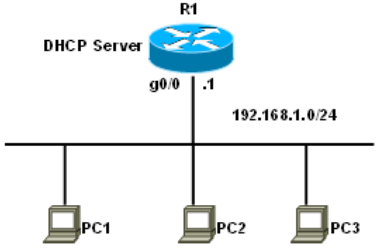


图1-20 DHCP基本配置

2、实验步骤

（1）配置路由器R1提供DHCP服务

```
R1(config)#interface g0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config)#service dhcp                    //DHCP服务
R1(config)#no ip dhcp conflict logging     //关闭DHCP冲突日志
R1(config)#ip dhcp pool ccie               //定义地址池，命名为ccie
R1(dhcp-config)#network 192.168.1.0 /24   //DHCP服务器要分配的网络和掩码
R1(dhcp-config)#domain-name cisco.com     //域名
R1(dhcp-config)#default-router 192.168.1.1
//默认网关，这个地址要和相应网络所连接的路由器的以太口地址相同
R1(dhcp-config)#netbios-name-server 192.168.1.2    //WINS服务器
R1(dhcp-config)#dns-server 192.168.1.4             //DNS服务器
R1(dhcp-config)#lease infinite                     //定义租期
R1(dhcp-config)#ip dhcp excluded-address 192.168.1.1 192.168.1.5    //排除的地址段
```

（2）设置Windows客户端

首先在Windows下把TCP/IP地址设置为自动获得（如图1-21），如果DHCP服务器还提供DNS和WINS等，也把它们设置为自动获得。

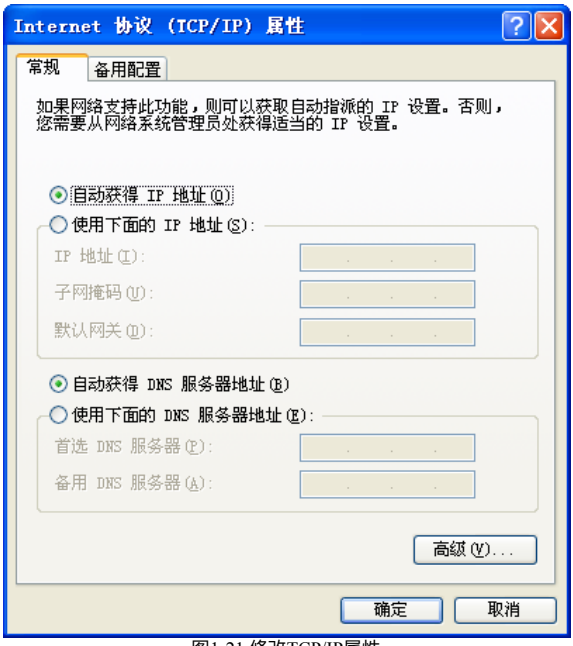


图1-21 修改TCP/IP属性

3、实验调试

（1）在客户端测试

在“命令提示符”下，执行“ipconfig /renew”命令可以更新IP地址；执行“ipconfig /all”命令可以看到IP地址、WINS、DNS和域名是否正确；要释放地址用“ipconfig /release”命令。

C：\>ipconfig /renew
Windows IP Configuration
Ethernet adapter 本地连接:
Connection-sepecific DNS Suffix .:cisco.com
IP Address.....: 192.168.1.7
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1

C:\>ipconfig/all
Windows IP Configuration
Ethernet adapter 本地连接:
Connection-sepecific DNS Suffix .:cisco.com
Description.....:Realtek RTL8139/810x Family Fast Ethernet NIC
Physical Address.....:00-60-67-00-DD-5B
Dhcp Enabled.....:YES
Autoconfiguration Enabled.....:YES
IP Address.....:192.168.1.7
Subnet Mask.....:255.255.255.0
Default Gateway.....:192.168.1.1
DHCP Server.....:192.168.1.1
DNS Servers.....:192.168.1.4
Primary WINS Server.....:192.168.1.2

Lease Obtained.....:20014年1月25日 13:01:01
Lease Expires.....:2038年1月19日 1:14:07

（2）show ip dhcp pool

该命令用来查看DHCP地址池的信息。

```
R1#show ip dhcp pool
Pool ccie:
Utilization mark(high/low)    :100/0
Subnet size(first/next)       :0/0
Total addresses               :254      //地址池中共计254个地址
Leased addresses              :2        // 已经分配出去2个地址
Pending event                 :none
1 subnet is currently in the pool:
Current index        IP address range                  Leased addresses
192.168.1.8          192.168.1.1   -192.168.1.254      2
```

//下一个将要分配的地址、地址池的范围以及分配出去的地址的个数

（3）show ip dhcp binding

该命令用来查看DHCP的地址绑定情况。

```
R1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address       Client-ID/                Lease expiration                Type
                 Hardware address/
                 Username

192.168.1.6              0063.6973.636f.2d       Infinite                Automatic
192.168.1.7              0100.6067.00dd.5b       Infinite                Automatic
```

以上输出表明DHCP服务器自动分配给客户端的IP地址以及所对应的客户端的硬件地址。

4、命令汇总

表1-6列出了本实验涉及到的主要命令。

表1-6 DHCP命令汇总

命令	作用
show ip dhcp pool	查看DHCP地址池的信息
show ip dhcp binding	查看DHCP的地址绑定情况
show ip dhcp database	查看DHCP数据库
show ip interface	查看接口信息
debug ip dhcp server events	动态查看DHCP服务器的事件
service dhcp	开启DHCP服务
no ip dhcp conflict logging	关闭DHCP冲突日志
ip dhcp pool	配置DHCP分配的地址池
network	DHCP服务器要分配的网络的掩码
default-router	默认网关
domain-name	域名
netbios-name-server	域名服务器
lease	配置租期
ip dhcp excluded-address	排除地址段

1.2.3 实验5 NAT

NAT（Network Address Translation，网络地址翻译）一个IETF标准，允许一个机构以一个地址出现在Internet上，是解决IP地址短缺的重要手段。NAT技术使一个私有网络可以通过Internet注册IP连接到外部世界，位于Inside网络和Outside网络中的NAT路由器在发送数据包之前，负责把内部IP地址翻译成外部合法的IP地址。NAT将每个局域网节点的IP地址转换成一个合法的IP地址，反之亦然。它也可以应用到防火墙技术中，把个别IP地址隐藏起来不被外界发现，对内部网络设备起到保护的作用，同时，它还可以帮助网络超越地址的限制，合理地安排网络中的公有Internet地址和私有IP地址的使用。

NAT有3 种类型：静态NAT、动态NAT和端口地址转换（PAT）。

（1） 静态NAT

在静态NAT中，内部网络中的每个主机都被永久映射成外部网络中的某个合法的地址。静态地址转换将内部本地地址与内部合法地址进行一对一的转换，且需要指定和哪个合法地址进行转换。如果内部网络有E-mail服务器或FTP服务器等可以为外部用户提供的服务，这些服务器的IP地址必须采用静态地址转换，以便外部用户可以使用这些服务。

（2）动态NAT：

动态NAT首先要定义合法地址池，然后采用动态分配的方法映射到内部网络。动态NAT是动态一对一的映射。

（3）PAT

PAT则是把内部地址映射到外部网络的IP地址的不同端口上，从而可以实现多对一的映射。PAT对于节省IP地址是最为有效的。

1、拓扑结构

实验拓扑图如图1-22所示。

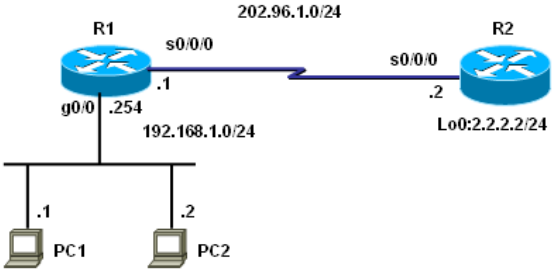


图1-22 NAT配置

2、 静态NAT配置和调试

（1）配置路由器R1提供NAT服务

```
R1(config)#ip nat inside source static 192.168.1.1 202.96.1.3
//配置静态NAT映射
R1(config)#ip nat inside source static 192.168.1.2 202.96.1.4
R1(config)#interface g0/0
R1(config-if)#ip nat inside
//配置NAT内部接口
R1(config)#interface s0/0/0
R1(config-if)#ip nat outside
//配置NAT外部接口
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#no auto-summary
R1(config-router)#network 202.96.1.0
```

（2）配置路由器R2

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#no auto-summary
R2(config-router)#network 202.96.1.0
R2(config-router)#network 2.0.0.0
```

（3）实验调试

使用debug ip nat命令查看地址翻译的过程。

在PC1和PC2上ping 2.2.2.2（路由器R2 的环回接口），此时应该是通的，路由器R1的输出信息如下：

```
R1#debug ip nat
*Mar  4 02:02:12.779:NAT*:s=192.168.1.1->202.96.1.3， d=2.2.2.2[20240]
*Mar  4 02:02:12.779:NAT*:s=2.2.2.2， d= 202.96.1.3-> 192.168.1.1 [14435]
.....
*Mar  4 02:02:12.779:NAT*:s=192.168.1.2->202.96.1.4， d=2.2.2.2[25]
*Mar  4 02:02:12.779:NAT*:s=2.2.2.2， d= 202.96.1.4-> 192.168.1.2 [25]
```

以上输出表明了NAT的转换过程。首先把私有地址”192.168.1.1”和”192.168.1.2”分别转换成

公网地址”202.96.1.3”和”202.96.1.4”访问地址”2.2.2.2”，然后回来的时候把网地址”202.96.1.3”和”202.96.1.4”分别转换成私有地址”192.168.1.1”和”192.168.1.2”。

使用show ip nat translations命令查看NAT表。在静态映射时，NAT表一直存在。

```
R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
---202.96.1.3          192.168.1.1        ---                ---
---202.96.1.4          192.168.1.2        ---                ---
```

以上输出表明了内部全局地址和内部局部地址的对应关系。

【提示】

① 内部局部（Inside Local）地址：在内部网络使用的地址，往往是RFC1918地址；

② 内部全部（Inside Global）地址：用来代替一个或多个本地IP地址的、地外的、向NIC注册过的地址；

③ 外部局部（Outside Local）地址：一个外部主机相对于内部网络所用的IP地址，不一定是合法的地址；

④ 外部局部（Outside Global）地址：外部网络主机的合法IP地址。

3、 动态NAT配置和调试

（1）配置路由器R1提供NAT服务

```
R1(config)#ip nat pool NAT 202.96.1.3 202.96.1.100 netmask 255.255.255.0
//配置动态NAT转换的地址池
R1(config)ip nat inside source list 1 pool NAT
//配置动态NAT映射
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
//允许动态NAT转换的内部地址范围
R1(config)#interface g0/0
R1(config-if)#ip nat inside
R1(config-if)#interface s0/0/0
R1(config-if)#ip nat outside
```

（2） 实验调试

在PC1访问2.2.2.2（路由器R2的环回接口）的WWW服务，在PC2上分别Telnet和ping 2.2.2.2（路由器R2的环回接口），调试结果如下：

```
R1#debug ip nat
IP NAT debugging is on
R1#clear ip nat translation *//清除动态NAT表
*Mar  4 01:34:23.075:NAT*:s=192.168.1.1->202.96.1.4， d=2.2.2.2[19833]
*Mar  4 01:34:23.087:NAT*:s=2.2.2.2， d= 202.96.1.4-> 192.168.1.1 [62333]
.....
*Mar  4 01:28:49.867:NAT*:s=192.168.1.2->202.96.1.3， d=2.2.2.2[62864]
*Mar  4 01:28:49.875:NAT*:s=2.2.2.2， d= 202.96.1.3-> 192.168.1.2 [54062]
.....
```

【提示】

如果动态NAT地址池中没有足够的地址进行动态映射，则会出现类似下面的信息，提示NAT转换失败，并丢弃数据包。

```
*Feb 22 09:02:59.075:NAT:translation failed(A)，dropping packet s=192.168.1.2 d=2.2.2.2
```

使用show ip nat translations命令查看NAT表。

```
R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 202.96.1.4:1721    192.168.1.1:1721   2.2.2.2:80         2.2.2.2:80
---202.96.1.4          192.168.1.1        ---                ---
icmp 202.96.1.3:3      192.168.1.2:3      2.2.2.2:3          2.2.2.2:3
tcp 202.96.1.3:14347   192.168.1.2:14347  2.2.2.2:23         2.2.2.2:23
---202.96.1.3          192.168.1.2        ---                ---
```

以上信息表明当PC1和PC2第一次访问“2.2.2.2”地址时，NAT路由器R1为主机PC1和PC2动态分配两个全局地址“202.96.1.4”和“202.96.1.3”，在NAT表中生成两条动态映射的记录，同时会在NAT表中生成和应用相对应的协议和端口号的记录（过期时间为60 s）。在动态没有过期（过期时间为86400 s）之前，再有应用从相同主机发起时，NAT路由器直接查NAT表，然后为

应用分配相应的端口号。

使用show ip nat statistics命令查看NAT转换的统计信息。

```
R1#show ip nat statistics
Total active translations:5(0 static， 5 dynamic；3 extended)
//有5 个转换是动态转化
Outside interfaces:
Serial0/0/0
//NAT外部接口
Inside interfaces:
GigabitEthernet0/0
//NAT内部接口
Hits:54  Misses:6
CEF Translated packets:60，CEF Punted packets:5
Expired translations:12   //NAT表中过期的转换
Dynamic mappings:    //动态映射
--Inside Source
[Id: 1] access-list 1 pool NAT refcount 2
pool NAT:netmask 255.255.255.0   //地址池名字和掩码
start 202.96.1.3 end 202.96.1.100   //地址池范围
type generic，total addresses 98，allocated 2 (2%)，misses 0
//共98个地址，分出去2 个
Queued Packets:0
```

4、 动态PAT配置和调试

（1）配置路由器R1提供NAT服务

```
R1(config)#ip nat pool NAT 202.96.1.3 202.96.1.100 netmask 255.255.255.0
R1(config)#ip nat side source list 1 pool NAT overload   //配置PAT
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)#interface g0/0
R1(config-if)#ip nat inside
R1(config-if)#interface s0/0/0
R1(config-if)#ip nat outside
```

（2）实验调试

在PC1访问2.2.2.2（路由器R2的环回接口）的WWW服务，在PC2上分别Telnet和ping 2.2.2.2（路由器R2的环回接口），调试结果如下：

```
R1#debug ip nat
*Mar  4 01:53:47.983:NAT*:s=192.168.1.1->202.96.1.3， d=2.2.2.2[20056]
*Mar  4 01:53:47.995:NAT*:s=2.2.2.2， d= 202.96.1.3-> 192.168.1.1 [46201]
*Mar  4 01:54:03.015:NAT*:s=192.168.1.2->202.96.1.4， d=2.2.2.2[20787]
*Mar  4 01:54:03.219:NAT*:s=2.2.2.2， d= 202.96.1.4-> 192.168.1.2 [12049]
.....
R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 202.96.1.3:1732     192.168.1.1:1732   2.2.2.2:80         2.2.2.2:80
icmp 202.96.1.3:4       192.168.1.2:4      2.2.2.2:4          2.2.2.2:4
tcp 202.96.1.3:12320    192.168.1.2:12320  2.2.2.2:23         2.2.2.2:23
```

以上输出表明进行PAT转换使用的是同一个IP地址的不同端口号。

```
R1#show ip nat statistics
Total active translations:3(0 static，3 dynamic；3 extended)
Outside interfaces:
Serial0/0/0
Inside interfaces:
GigabitEthernet0/0
CEF Translated packets:760，CEF Punted packets:47
Expired translations:19
Dynamic mappings:
--Inside Source
[Id； 1] access-list 1 pool NAT refcount 3
pool NAT:netmask 255.255.255.0
```

start 202.96.1.3 end 202.96.1.100
type generic，total addresses 98，allocated 1 (1%)，misses 0
Queued Packets:0

【提示】

动态NAT的过期时间是86 400 s，PAT的过期时间是60 s，通过”show ip nat translations verbose”命令可看。也可以通过下面的命令来修改超时时间：

R1(config)#ip nat translation timeout ？ //?为修改后的具体超时时间

参数timeout的范围是0~2 147 483 。

如果主机的数量不是很多，可以直接使用outside接口地址配置PAT，不必定义地址池，命令如下：

R1(config0#ip nat inside source list 1 interface s0/0/0 overload

5、命令汇总

表1-7列出了本实验涉及到的主要命令。

表1-7 NAT命令汇总

命令	作用
clear ip nat translation *	清除动态NAT表
show ip nat translation	查看NAT表
show iop nat statistics	查看NAT转换的统计信息
debug ip nat	动态查看NAT转换过程
ip nat inside source static	配置静态NAT
ip nat inside	配置NAT内部接口
ip nat outside	配置NAT外部接口
ip nat pool	配置动态NAT地址池
ip nat inside source list access-list-number pool name	配置动态NAT
ip nat inside source list access-list-number pool name overload	配置PAT

1.3 交换实验

交换机是局域网中的最重要的设备，和路由器一样，本质上也是一台特殊的计算机，也有CPU和RAM等部件，也采用IOS。交换机不仅仅具有2层交换功能，它还具有VLAN等功能。VLAN技术让我们可以很容易的控制广播域的大小。本节主要介绍在单个交换机上划分VLAN，以及使用Trunk、VTP等技术实现多个交换机间的VLAN配置和VLAN间的通信。

1.3.1 实验6 单个交换机上划分VLAN

1、实验拓扑

实验拓扑图如图1-23所示。

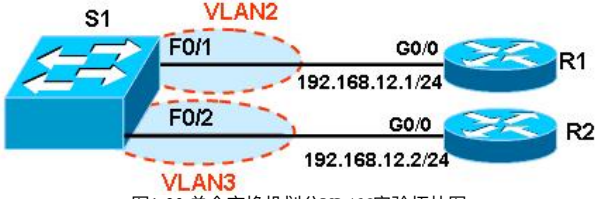


图1-23 单个交换机划分VLAN实验拓扑图

2、实验步骤

要配置VLAN，首先要创建VLAN，然后才能把交换机的端口划分到特定的端口上。

（1）在划分VLAN前，需先配置路由器R1和R2的g0/0接口，从R1 ping 192.168.12.2进行测试。默认时，交换机的全部接口都在VLAN 1上，R1和R2应该能够通信。

（2）在S1上创建VLAN。

S1#vlan database
//进入到VLAN配置模式
S1(vlan)#vlan 2 name VLAN2
VLAN 2 added:
Name: VLAN2
//以上创建VLAN，2就是VLAN的编号，VLAN号的范围为1~1 001，VLAN2是该VLAN的名字
S1(vlan)#vlan 3 name VLAN3
VLAN 3 added:
Name: VLAN3
S1(vlan)#exit
APPLY completed.
Exiting....
//退出VLAN模式，创建的VLAN立即生效
交换机中的VLAN信息存放在单独的文件中flash:vlan.dat，因此如果要完全清除交换机的配置，除了使用”erase starting-config”命令外，还可使用”delete flash:vlan.dat”命令把VLAN数据删除
新的IOS版本中，可以在全局配置模式中创建VLAN，如下所述。
S1(config)#vlan 2
S1(config-vlan)#name VLAN 2
S1(config-vlan)#exit
S1(config)#vlan 3
S1(config-vlan)#name VLAN 3
（3）把端口划分在VLAN中
S1(config)#interface f0/1
S1(config-if)#switch mode access
//以上把交换机端口的模式改为access模式，说明该端口是用于连接计算机的，而不是用于Trunk
S1(config-if)#switch access vlan 2
//然后把该端口f0/1划分到VLAN2中
S1(config)#interface f0/2
S1(config-if)#switch mode access
S1(config-if)#switch access vlan 3
默认时，所有交换机接口都在VLAN 1上，VLAN 1是不能删除的。如果有多个接口需要划分到同一VLAN下，也可以采用如下快捷方式，注意”-”前的空格。
S1(config)#interface range f0/2 - 3
S1(config-if-range)#switch mode access
S1(config-if-range)#switch access vlan 2
如果要删除VLAN，使用“no vlan 2”命令即可。删除某一VLAN后，要记得把该VLAN上的端口重新划分到别的VLAN上，否则将导致端口的“消失”。
3、实验调试
（1）查看VLAN
使用“show vlan”或者“show vlan brief”命令查看VLAN信息，以及每个VLAN上有什么端口。要注意这里只能看到的是本交换机上哪个端口在VLAN上，而不能看到其他交换机的端口在什么VLAN上。如下：
S1#show vlan
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，Fa0/24，Gi0/1，Gi0/2
2 VLAN2 active
3 VLAN3 active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
.....（省略）
//在交换机，VLAN1是默认VLAN，不能删除，也不能改名。此外，还有1002和1003等

VLAN存在。

（2）VLAN间的通信

由于f0/1和f0/2属于不同VLAN，从R1 ping 192.168.12.2应该不能成功了。

1.3.2 实验7 多个交换机间的VLAN配置

当一个VLAN跨过不同的交换机时，在同一VLAN上但是却在不同的交换机上的计算机进行通信时需要使用Trunk。Trunk技术使得一条物理线路可以传送多个VLAN的数据。交换机从属于某一VLAN（例如VLAN 3）的端口接收到数据，在Trunk链路上进行传输前，会加上一个标记，表明该数据是VLAN 3的；到了对方交换机，交换机会把该标记去掉，只发送到属于VLAN 3的端口上。

有两种常见的帧标记技术：ISL和802.1Q。ISL技术在原有的帧上重新加了一个帧头，并重新生成了帧检验序列（FCS），ISL是Cisco特有的技术，因此不能在Cisco交换机和非Cisco交换机之间使用。而802.1Q技术在原有帧的源MAC地址字段后插入标记字段，同时用新的FCS字段替代了原有的FCS字段，该技术是国际标准，得到所有厂家的支持。Cisco交换机之间的链路是否形成Trunk是可以自动协商的，这个协议称为DTP（Dynamic Trunk Protocol），DTP还可以协商Trunk链路的封装类型。

VTP（VLAN Trunk Protocol）提供了一种用于在交换机上管理VLAN的方法，该协议使得我们可以在一个或者几个中央点（Server）上创建、修改和删除VLAN，VLAN信息通过Trunk链路自动扩散到其他交换机，任何参与VTP的交换都可以接受这些修改，所有交换机保持相同的VLAN信息。

VTP被组织成管理域（VTP Domain），相同域中的交换机能共享VLAN信息。根据交换机在VTP域中的作用不同，VTP可以分为以下3种模式。

①服务器模式（Server）：在VTP服务器上能创建、修改和删除VLAN，同时这些信息会通告给域中的其他的交换机。在默认情况下，交换机是服务器模式。每个VTP域必须至少有一台服务器，域中的VTP服务器可以有多台。

②客户机模式（Client）：VTP客户机上不允许创建、修改和删除VLAN，但它会监听来自其他交换机的VTP通告并更改自己的VLAN信息。接收到的VTP信息也会在Trunk链路上向其他交换机转发，因此这种交换机还能充当VTP中继。

③透明模式（Transparent）：这种模式的交换机不参与VTP。可以在这种模式的交换机上创建、修改和删除VLAN，但是这些VLAN信息并不会通告给其他交换机，它也不接受其他交换机的VTP通告而更新自己的VLAN信息。然而需要注意的是，它会通过Trunk链路转发接收到的VTP通告，从而充当 了VTP中继的角色，因此完全可以把该交换机看成是透明的。

VTP通告是以组播帧的方式发送的，VTP通告中有一个字段称为修订号（Revision），初始值为0.只要在VTP Server上创建、修改和删除VLAN，通告的Revision就增加1，通告中还包含了VLAN的变化信息。需要注意的是：高Revision的通告会覆盖低Revision的通告，而不管发送者是Server还是Client。交换机只打官腔比本地在哪保存的Resivison号更高的通告；如果交换机收到比自己的Resivison号更低的通告，会用自己的VLAN信息反向覆盖。

1、 实验拓扑

实验拓扑图如图1-24所示。

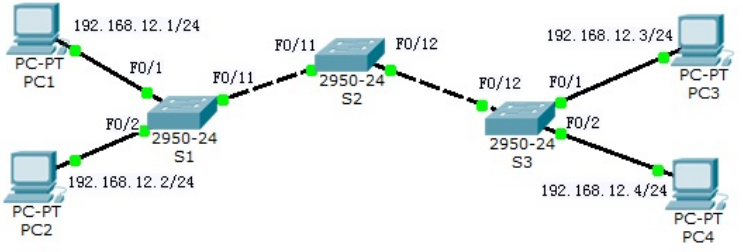


图1-24 VLAN、Trunk和VTP实验拓扑图

2、 配置步骤

（1）按照拓扑图正确配置各个PC机的IP地址等，然后在S1上创建VLAN2，并把接口F0/2划分到VLAN2。

S1(config)#vlan 2

S1(config-vlan)#name VLAN 2
S1(config-vlan)#exit
S1(config)#interface f0/2
S1(config-if)#switch mode access
S1(config-if)#switch access vlan 2
将S3上接口F0/2划分到VLAN2，但不创建新的VLAN。
S3(config)#interface f0/2
S3(config-if)#switch mode access
S3(config-if)#switch access vlan 2
（2）分别在S1、S2和S3相应端口上配置Trunk链路。
S1(config)#int f0/1
S1(config-if)#switchport trunk encanpsulation dot1q
//以上是配置Trunk链路的封装类型，同一链路的两端封装要相同。有的交换机，例如2950只能封装dot1q，因此无须执行该命令
S1(config-if)#switch mode trunk
//以上是把接口配置为Trunk
S2(config)#int f0/11
S2(config-if)#switchport trunk encanpsulation dot1q
S2(config-if)#switch mode trunk
S2(config)#int f0/12
S2(config-if)#switchport trunk encanpsulation dot1q
S2(config-if)#switch mode trunk
S3(config)#int f0/12
S3(config-if)#switchport trunk encanpsulation dot1q
S3(config-if)#switch mode trunk
需要在链路的两端都进行检查，才能确认Trunk的形成，可使用”show interface f0/11 switchport”命令查看交换机端口的trunk状态。
S1#show int f0/11 switchport
Name: Fa0/11
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
.....（省略）
【提示】和DTP配置有关的命令如下所述，这些命令不能任意组合。
“switchport trunk encapsulation{negotiate|isl|dot1q}”：配置Trunk链路上的封装类型，可以是双方协商确定，也可以是指定的isl或者dot1q。
“switchport nonegotiate”：Trunk链路上不发送协商包，默认是发送的。
“switch mode {trunk|dynamic desirable|dynamic auto}”：
Turnk——该设置将端口置为永久trunk模式，封装类型由”switchport trunk encapsulation”命令决定；
Dynamic desirable——端口主动变为trunk，如果另一端为negotiate，dynamic desirable和dynamic auto，将成功协商；
Dynamic auto——被动协商，如果另一端为negotiate和dynamic desirable，将成功协商。
默认时，catalyst2950和3550的配置是desirable模式；而catalyst 3560是auto模式，所以，两台3560交换机之间不会自动形成Trunk，3560交换机和2950交换机之间却可以形成Trunk。
如果想把接口配置为Trunk，使用：
S1(config-if)#switchport trunk encapsulation {isl|dot1q}
S1(config-if)#switchport mode trunk
S1(config-if)#no switchport negotiate
如果想把接口配置为nonegotiate，使用：
S1(config-if)#switchport trunk encapsulation {isl|dot1q}
S1(config-if)#switchport mode trunk
S1(config-if)#no switchport nonegotiate

如果想把接口配置为desirable，使用：
S1(config-if)#switchport mode dynamic desirable
S1(config-if)#switch trunk encapsulation{negotiate|isl|dot1q}
如果想把接口配置为auto，使用：
S1(config-if)#switchport mode dynamic auto
S1(config-if)#switch trunk encapsulation{negotiate|isl|dot1q}
（3）配置Native VLAN：
S1(config)#int f0/11
S1(config-if)#switchport trunk native vlan 2
//以上是在Trunk链路上配置Native VLAN，我们把它改为VLAN 2了，默认是VLAN 1
S2(config)#int f0/11
S2(config-if)#switchport trunk native vlan 2
S2(config)#int f0/12
S2(config-if)#switchport trunk native vlan 2
S3(config)#int f0/12
S3(config-if)#switchport trunk native vlan 2
（4）配置VTP
①配置S1为VTP server
S1(config)#vtp mode server
Device mode already VTP SERVER.
//以上配置S1为VTP server，实际上这时默认值
S1(config)#vtp domain VTP-TEST
Changing VTP domain name from NULL to VTP-TEST
//以上配置VTP域名
S1(config)#vtp password cisco
Setting device VLAN database password to cicso
//以上配置VTP的密码，目的是为了安全，防止不明身份的交换机加入到域中，不配置也能使用
②配置S2为VTP transparent
S2#vlan database
S2(vlan)#vtp transparent
Setting device VTP TRANSPARENT mode.
S2(vlan)#vtp domain VTP-TEST
Domain name already set to VTP-TSET
S2(config)#vtp password cisco
Setting device VLAN database password to cicso
【提示】
有的IOS版本只支持在VLAN Database下配置VLAN。
③配置S3为VTP client
S3>en
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#vtp mode client
Setting device to VTP CLIENT mode.
S3(config)#vtp domain VTP-TEST
Changing VTP domain name from NULL to VTP-TEST
S3(config)#vtp password cisco
Setting device VLAN database password to cisco
3、 实验调试
（1）分别在S1、S2和S3上查看VLAN信息，会看到S3上有了VLAN2，但S2上没有，因为S2是透明模式。
S3#show vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18

Fa0/19, Fa0/20, Fa0/21, Fa0/22
Fa0/23, Fa0/24
2 VlAN2 active Fa0/2
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup
//可以看到S3已经学习到了在S1上创建的VLAN2
（2）查看VTP信息
S1#show vtp status
VTP Version : 2 //该VTP支持版本2
Configuration Revision : 1 //修订号为1，该数值非常重要
Maximum VLANs supported locally : 1005
Number of existing VLANs : 7 //VLAN数量
VTP Operating Mode : Server //VTP模式
VTP Domain Name : VTP-TEST //VTP域名
VTP Pruning Mode : Disabled //VTP修剪没有启用
VTP V2 Mode : Disabled //VTP版本2没有启用，现在是版本1
VTP Traps Generation : Disabled
MD5 digest : 0xD4 0x30 0xE7 0xB7 0xDC 0xDF 0x1B 0xD8
Configuration last modified by 0.0.0.0 at 3-1-93 00:22:16
Local updater ID is 0.0.0.0(no valid interface found)
在S1上，修改、创建或者删除VLAN，在S2和S3上使用“Show vtp status”命令观察revision数值是否增加1 。
（3）配置修建版本2
S1(config)#vtp pruning
S1(config)#vtp version 2
S1#show vtp status
VTP Version : 2
Configuration Revision : 2
Maximum VLANs supported locally : 1005
Number of existing VLANs : 7
VTP Operating Mode : Server
VTP Domain Name : VTP-TEST
VTP Pruning Mode : Enabled //VTP修剪启用了
VTP V2 Mode : Enabled //VTP版本为2了
VTP Traps Generation : Disabled
MD5 digest : 0xA6 0x56 0x25 0xDE 0xE2 0x39 0x6A 0x10
Configuration last modified by 0.0.0.0 at 3-1-93 00:32:28
Local updater ID is 0.0.0.0(no valid interface found)
VTP修剪和VTP版本只需要在一个VTP server上进行即可，其他server 或者client会自动跟着更改。VTP修剪是为了防止不必要必要的流量从Trunk链路上通过，通常需要启用。

1.3.3 实验8 VLAN间路由

在交换机上划分VLAN后，VLAN间的计算机就无法通信了。VLAN间的通信需要借助第3层设备，可以使用路由器来实现这个功能，如果使用路由器，通常会采用单臂路由模式。实践上，VLAN间的路由大多是通过3层交换机实现的，3层交换机可以看成是路由器加交换机，然而因为采用了特殊的技术，其数据处理能力比路由器要大得多。
1、实验拓扑
实验拓扑图如图1-25所示。

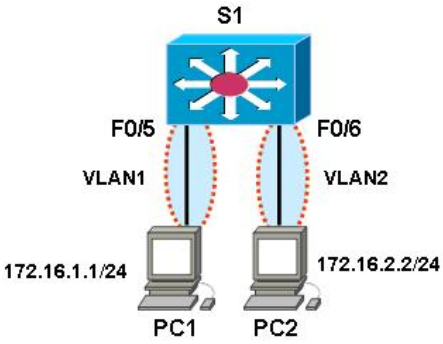


图1-25 VLAN间路由实验拓扑图

交换机S1可选择有3层功能的Catalyst 3560交换机，Catalyst 2950系列交换机不行，它属于二层交换机，没有路由功能。

2、实验步骤

用S1来实现分别处于VLAN1和VLAN2的PC1和PC2间的通信。

（1）在S1上划分VLAN

```
S1(config)#vlan 2
S1(config-vlan)#exit
S1(config)#int f0/5
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 1
S1(config-if)#in f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 2
```

（2）配置3层交换

```
S1(config)#ip routing
//以上S1的路由功能，这时S1就启用了3层功能
S1(config)#int vlan 1
S1(config-if)#no shutdown
S1(config-if)#ip address 172.16.1.254 255.255.255.0
S1(config)#int vlan 2
S1(config-if)#no shutdown
S1(config-if)#ip address 172.16.2.254 255.255.255.0
```

//在VLAN接口上配置IP地址即可，VLAN 1接口上的地址就是PC1的网关，VLAN 2接口上的地址就是PC2的网关

【提示】

要在3层交换机上启用路由功能，还需要启用CEF（命令为：ip cef），不过这是默认值。和路由器一样，3层交换机上同样可以运行路由协议 。

4.实验调试

（1）检查S1上的路由表

```
S1#show ip route
（此处省略）
172.16.0.0/24 is subnetted，2 subnets
C     172.16.1.0 is directly connected，Vlan1
C     172.16.2.0 is directly connected，Vlan2
```

//和路由器一样，3层交换上也有路由表

（2）测试PC1和PC2间的通信

在PC1和PC2上配置IP地址和网关，PC1的网关指向：172.16.1.254， PC2的网关指向：172.16.2.254。测试PC1和PC2的通信。

1.3.4 交换实验命令汇总

表1-8列出了交换实验涉及到的主要命令。

表1-8 交换实验命令汇总

命令	作用
vlan database	进入到VLAN Database配置模
vlan 2 name VLAN 2	创建VLAN 2
switch access vlan 2	把端口划分到VLAN 2中
interface range f0/2 -3	批量配置接口的属性
show vlan	查看VLAN的信
switchport trunk encanpsulation	配置Trunk链路的封装类型
switch mode accsess	把接口配置为访问模式
switch mode trunk	把接口配置为Trunk
show interface f0/13 switchport	查看交换机端口的状态
switchport nonegotiat	Trunk链路上不发送Trunk协商包
vtp mode serve	配置交换机为VTP server
vtp domain VTP-TEST	配置VTP域名为 VTP-TEST
vtp password cisco	配置VTP的密码
vtp mode client	配置交换机为VTP client
vtp transparent	配置交换机为VTP transparen
show vtp status	显示VTP的状态
vtp pruning	启用VTP修剪
vtp version 2	VTP版本为 2
ip routing	打开路由功能
ip cef	开启CEF功能

1.4 网络设计和局域网综合配置

任何规模的网络建设，前期良好的规划、周密的论证、谨慎的决策、明晰而有层次的设计和施工，对网络今后的建设和管理都将起到事半功倍的效果。一个好的局域网离不开良好的设计。

1.4.1 网络设计

网络设计和规划是一个复杂的系统工程，不仅涉及很多的网络设备，更涉及很多不同的工作部门和不同的工作人员。网络设计要求设计人员熟悉用户的需求、每种设备的功能和工作原理，且要对各种局域网技术、广域网技术有深入的理解，只有这样才能够设计出高质量的计算机网络系统。

根据用户对计算机网络的功能需求和目标，网络设计大体上可以分成以下几个方面：

1、用户需求分析

用户的应用需求是网络建设的核心，好的网络规划需求分析可大大提高网络未来应用和管理的效率，降低网络工程资金，使未来的网络扩展减少弯路。

网络需求分析的内容是在用户需求调查的基础上，分析用户的网络应用要求和网络建设所要达到的目标。了解用户网络的业务内容，网络应用的环境，网络的安全保障措施以及网络未来的扩充，从而为整个网络系统建设确定其功能上、性能上和安全上的应用要求。

2、网络设计目标

在应用需求分析的基础上，确定不同网络服务类型，进而确定系统建设的具体目标，包括网络设施、站点设置、开发应用和管理等方面的目标。

3、网络分层设计

使用分层式网络设计模型建立一个局域网来满足中小型企业需求，已经成为一种潮流。和其他网络设计相比，分等级的网络更容易管理和扩展，排除故障也迅速。

分层网络设计把一个复杂的网络问题分解为多个小的、更容易解决的问题，每一层负责解决特定的问题。典型的分层设计模型把网络设计分为三层：接入层（Access）、汇聚层

（Distribution）和核心层（Core）。分层网络的设计功能及网络拓扑如图1-26所示。

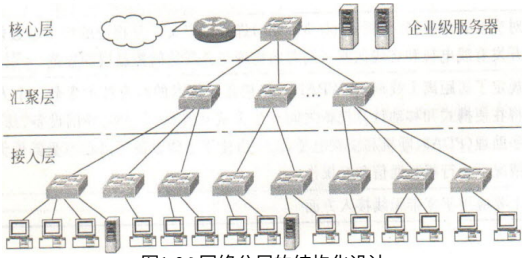


图1-26 网络分层的结构化设计

（1） 接入层

接入层是桌面设备的汇集点，它为网络提供通信并实现网络入口控制，最终用户通过接入层访问网络。接入层的终端设备有计算机、打印机、IP电话等，也可以包括路由器、交换机、网桥、无线AP等设备。一般在接入层实施冲突域的隔离、VLAN的划分和交换机的端口安全。

（2） 汇聚层

汇聚层主要负责连接接入层结点和核心层中心，汇集分散的接入点，扩大核心层设备的端口密度和种类，汇集各区域的数据流量，把核心层同网络的其他部分区分开来。该层的目的是实现VLAN 间的通信和广播域的划分，并定义了网络的策略，包括路由更新、路由汇总、VLAN间通信、地址聚合、访问控制和路由的重分布等。

（3）核心层

核心层是网络的高速交换主干，主要实现骨干网络之间的优化传输，负责整个网络的网内数据交换。通常情况下，核心层用来提供Internet的接入和楼宇之间的连接，核心层连接的设备主要包括汇聚层设备和企业级服务器。

使用分层网络设计有很多优点。分级网络很容易扩展，能在汇聚层和核心层提供冗余路径。可以把接入层上连至汇聚、汇聚层上连至核心层的多条链路进行汇聚，以提供更高速的带宽。在接入层实施端口安全，在汇聚层实施策略，将不安全因素限制在更小的范围内，不至于影响核心层，使网络更加安全。总之，分层网络设计结构清晰，便于管理，易于维护。

4、组网技术和设备选型

快速以太网（Fast Ethernet）技术以其良好的传输质量和交换能力兼容网络中的所有设备，较少网络建设的重新投资，建立在其应用上的方便、可管理性和扩展性良好等众多技术优势，已经成为现今网络的主流，在所有技术中有更大的竞争力和发展前景。从网络费用、维护、安全和扩展方面而言，下一代Gigabit Ethernet技术已成为大型Fast Ethernet的升级目标。

选择计算机网络系统的设备主要考虑因素有：用户对网络主干带宽和交换能力的需求；设备的整体性能、可靠性和兼容性等；设备的性价比、维护及售后服务等。典型的如，接入层交换机选择Catalyst 2950、Catalyst 2960等二层交换机，汇聚层交换机Catalyst 3550-EMI、Catalyst 3560、Catalyst 3570等三层交换机，核心层选择Catalyst 4500、Catalyst 4900、Catalyst 6500等三层交换机，当然各层也可以选择等次更高的交换机。

5、网络设计文档

网络设计的最后一步是为网络的逻辑设计和物理实现建立文档，包括详细的网络物理拓扑图和逻辑拓扑图、各配线间的详细信息表格、设备列表等。主要内容包括以下方面：

①统计信息点。根据用户需求及设计图纸确定布线系统内的信息点。

②根据施工现场情况及用户需求确定工作区使用的模块和插座面板。

③计算水平线缆的需求数量，确定线缆的布线方式和线缆走向。

④计算垂直线缆的需求数量，确定线缆的布线方式。

⑤确定各配线间机柜的安装位置及配线架的数量。

⑤确定接入方式以及接入媒体和设备。

1.4.2 局域网综合配置

某中央高校有学生处、人事处、财务处、学生社团中心、信息中心、后勤集团和各学院办公行政部门等多个教学和管理职能部门，这些部门分布在两个校区50余栋建筑楼宇内。该大学校园网络逻辑拓扑图如图1-27所示。

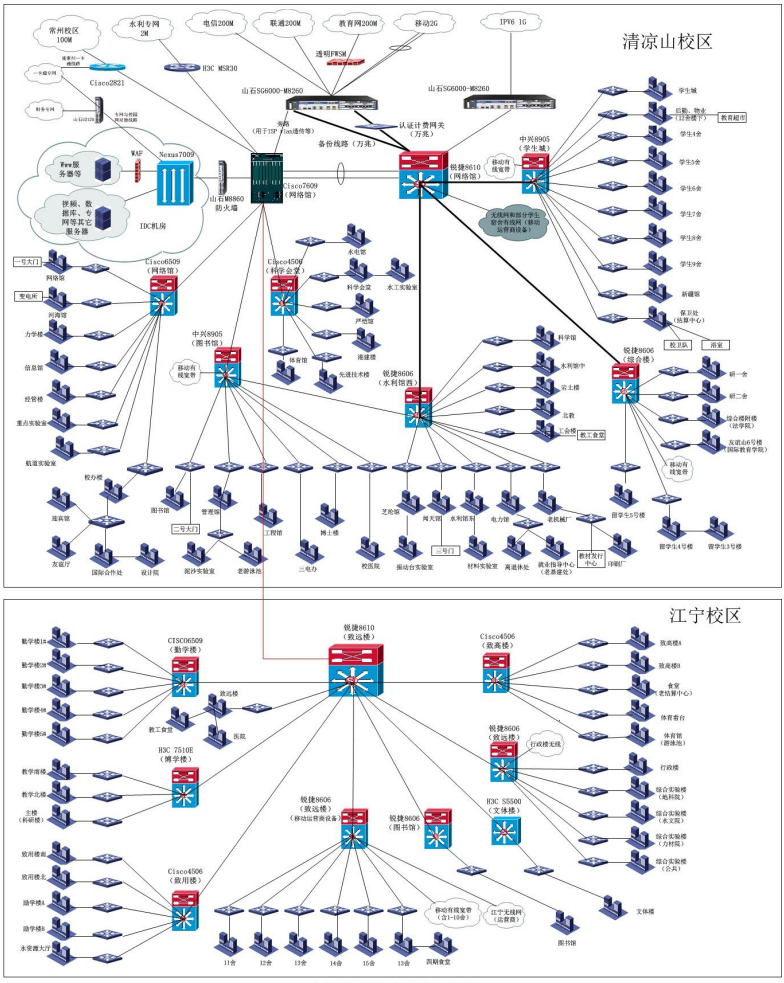


图1-27 某高校网络逻辑拓扑图

该学校网是典型的层次化结构局域网，主干网络由两个主干网中央节点和15个分节点及各个接入点的局域网组成。所有的网络设备配置的都是以太网板块和接口，主要包括10万兆/万兆/千兆/百兆 SFP以太网光口板卡（此时还需要插入单模/多模SFP模块使用）和千兆/百兆以太网电口板卡（采用双绞线进行连接）。低速的广域网连接大多采用串口，如上图中与水利专网连接用的H3C MSR30-20路由器，就配置了Serial串口。

主干网中央节点分别设在清凉山校区网络馆和江宁校区致远楼，选取锐捷8610三层交换机作为核心层网络交换机，其中网络馆节点也是全校的主干中心。

核心层一般是一个网状拓扑结构，要求能保证本局域网的高速可靠的数据转发。上图江宁校区网络是一个典型的树形网络，用一台锐捷8610作为该校区的核心设备，底下各个汇聚到接入都必须通过该设备进行数据传输，重要性不言而喻。从整体来看，江宁校区的锐捷8606、清凉山校区的锐捷8610和思科7609又构成了整个校园网的核心层。同时，核心层还负责与出口互联网的连接，从某种意义上来讲，出口设备也可以算作核心层，因为出口设备也必须判断多个

出口的状态等情况，从而选择最佳的线路连接互联网。

核心层设备对硬件参数要求是最高的。核心设备一般都是模块化设计，根据需求配置引擎板和业务板。以思科7609为例，7600代表设备档次，09代表设备插槽总数是9个，在该网络中配置了2块Supervisor Engine 720引擎板卡、一块WS-X6724-SFP千兆光口以太网业务板卡、一块WS-X6148-GE-TX 48口千兆以太网电口板卡和一块WS-SVC-FWM-1防火墙板卡，背板带宽720Gbps、包转发速率30Mpps。最初以此思科7609设备为单核心，随着网络需求的增加，此硬件配置已不能满足校园网需求的，后来将核心更改为背板带宽9.6Tbps,包转发率1920Mpps的锐捷8610。

从完美的网络设计角度来看，此校园网存在不少单点故障，就核心层来说，每个校区应配备双核心或多台设备组成的逻辑单核心，底下汇聚层设备都至少需要两条链路上联到核心层。

汇聚交换机的定义较为模糊，从物理连接上来看，只要下面连接有多台交换机，其本身就可以成为汇聚交换机。上图中，每栋楼宇都至少配置一台性能较高的三层/二层交换机作为汇聚交换机，负责本楼宇的网络连接。从逻辑意义上来讲，只有启用了三层路由协议且作为该区域网络的默认网关的交换机才能称为汇聚交换机。如江宁校区勤学楼的思科6509，下联有勤学楼的1-5号楼及实验室，所有勤学楼的默认网关都是此设备，勤学楼的思科6509再与江宁核心8610交换机做三层路由数据转发。

汇聚交换机与核心交换机的主要区别就是负责的区域大小不一样，所以汇聚交换机的设备性能参数要求就没有核心交换机那么高了，具体选用什么型号视流量情况等而定。当汇聚交换机性能不足造成网络延迟等异常情况时，就需要考虑更换高档一点的交换机了。

关于校园网VLAN的规划，一般的需要考虑三种VLAN：设备VLAN、用户VLAN及特殊需求VLAN。设备VLAN包括设备管理VLAN和设备互连VLAN，可采用VLAN号范围限定在1-99。用户VLAN因为不需要透传，终结在汇聚交换机网关设备上，使用的VLAN号范围可以很随便，但为了规范，使用范围限定在100-2000。以该校园网为例，大概2-4层楼就可以划一个VLAN，一个汇聚交换机负责的区域一般不会超过100个，所以VLAN号末两位表示VLAN号，前面1位或2位为该汇聚交换机在校园网主干节点的编号。如VLAN号1910，就表示主干节点编号是19的汇聚交换机下的VLAN10； 特殊需求的VLAN，主要是指跨整个校区建立的逻辑专网，如学校的一卡通专网，终端设备遍及各个食堂、图书馆等。这些VLAN需要做全校范围内的透传，一般可采用较大的VLAN号，如4000等。当VLAN需要做透传时，一定要注意做好裁剪，将不必要的VLAN从trunk口中剔除。

总体来说，该校园网虽是典型的层次化结构，但在某些方面特别是避免单点故障方面还有改善的空间。校园网也是动态变化的，比如新建一栋楼宇、改变楼宇功能等，对于这种典型的层次化网络，网络管理也将会变得越来越复杂，对网络管理员的要求也会越来越高。正因为如此，部分学校对校园网进行了扁平化，去掉汇聚层，只剩下一个核心层，底下都是接入层，用户的所有网络流量都经过核心控制和转发，大大降低了网络的复杂性。

请参考图1-27高校逻辑网络结构图，选择某栋楼宇，如江宁校区勤学楼，调查并整理用户需求，选择合适的网络设备，规划设计网络逻辑拓扑。从IP地址分配、VLAN划分、二层交换机VLAN设置、三层交换机VLAN和路由设置，以及交换机之间的VTP设置等方面，利用模拟软件Packet Tracer逐步完成网络拓扑图中网络设备的综合配置和调试。