计算机网络实验指导书　CISCO 版（2015）

实验一　双绞线水晶头制作

一、实验内容

学习 EIA/TIA568 标准，学习 RJ45 接口类型，学习双绞线水晶头制作方法。EIA/TIA-568 标准规定了两种 RJ45 接头网线的连接标准，即 EIA/TIA-568A 和 EIA/TIA-568B。

EIA/TIA-568A 的线序是：1=白/绿,2=绿,3=白/橙,4=蓝,5=白/蓝,6=橙,7=白/棕,8=棕 ；

EIA/TIA-568B 的线序是：1=白/橙,2=橙,3=白/绿,4=蓝,5=白/蓝,6=绿,7=白/棕,8=棕。

二、实验目的

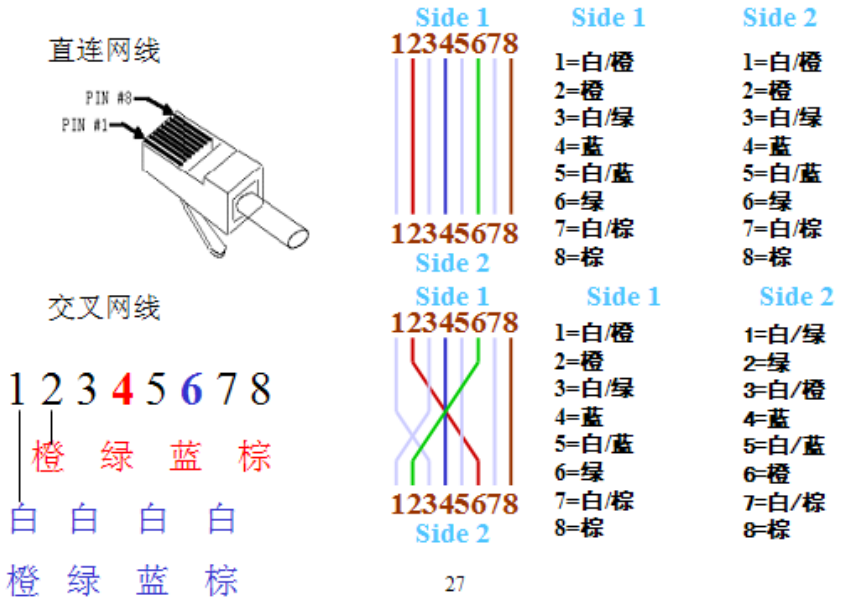
掌握 EIA568A、EIA568B 标准，根据需要制作各种网络设备之间的互连双绞线，学习使用测试工具，掌握双绞线测试方法。

使用双绞线工具制作 EIA568A、EIA568B 标准的直连网线和交叉网线，用于网络设备之间互连。

三、实验工具

双绞线 RJ 45 夹线钳若干、双绞线测试工具若干、双绞线若干、RJ45 水晶接线头若干。

四、相关预备知识：



27

双绞线有两种类型：直连网线和交叉网线。直连网线又称平行线，主要用在集线器（或交换机）间的级联、服务器与集线器（交换机）的连接、计算机与集线器（或交换机）的连接。交叉线主要用在计算机与计算机、交换机与交换机、集线器与集线器之间的连接、计算机与路由器、路由器与路由器之间的连接。如下表：

表 1 设备连接方式表

	计算机 MDI	路由器 MDI	交换机 MDIX	交换机 MDI	集线器
计算机 MDI	交叉	交叉	直连	N/A	直连
路由器 MDI	交叉	交叉	直接	N/A	直连
交换机 MDIX	直连	直连	交叉	直连	交叉
交换机 MDI	N/A	N/A	直连	交叉	直连
集线器	直连	直连	交叉	直连	交叉

表 2**RJ-45 MDI** 接口引脚分配表

引脚号	10Base-T/100Base-TX		1000Base-T	
	信号	功能	信号	功能
1	**Tx+**	**发送**数据	BIDA+	双向数据线 A+
2	**Tx-**	**发送**数据	BIDA-	双向数据线 A-
3	**Rx+**	**接收**数据	BIDB+	双向数据线 B+
4	保留	-	BIDC+	双向数据线 C+
5	保留	-	BIDC-	双向数据线 C-
6	**Rx-**	**接收**数据	BIDB-	双向数据线 B-
7	保留	-	BIDD+	双向数据线 D+
8	保留	-	BIDD-	双向数据线 D-

表 3 RJ-45 MDI-X 接口引脚分配

引脚号	10Base-T/100Base-TX		1000Base-T	
	信号	功能	信号	功能
1	**Rx+**	**接收**数据	BIDB+	双向数据线 B+
2	**Rx-**	**接收**数据	BIDB-	双向数据线 B-
3	**Tx+**	**发送**数据	BIDA+	双向数据线 A+
4	保留	-	BIDD+	双向数据线 D+
5	保留	-	BIDD-	双向数据线 D-
6	**Tx-**	**发送**数据	BIDA-	双向数据线 A-
7	保留	-	BIDC+	双向数据线 C+
8	保留	-	BIDC-	双向数据线 C-

提示：对比表 2 和表 3 可以看出 100 兆以太网端口只用到了 1236 四根线，而 EIA568B 标准中，1、2 为一对互绕在一起的线，3、4 为一对互绕在一起的线，这样电流同向的线绕在一起可以有效减少电磁干扰达到比较高的传输速度。

EIA568A 和 EIA568B 的线序恰好是 1、2 和 3、6 反绕，因此两端都按 EIA568B 标准排列线序则是直连网线；一端按 EIA568A 标准，另一端按 EIA568B 标准排列线序则刚好是交叉网线。千兆以太网端口则使用全部 8 条线以提高带宽，目前 5 类和超 5 类双绞线可以支持千兆速度。

五、网线制作步骤

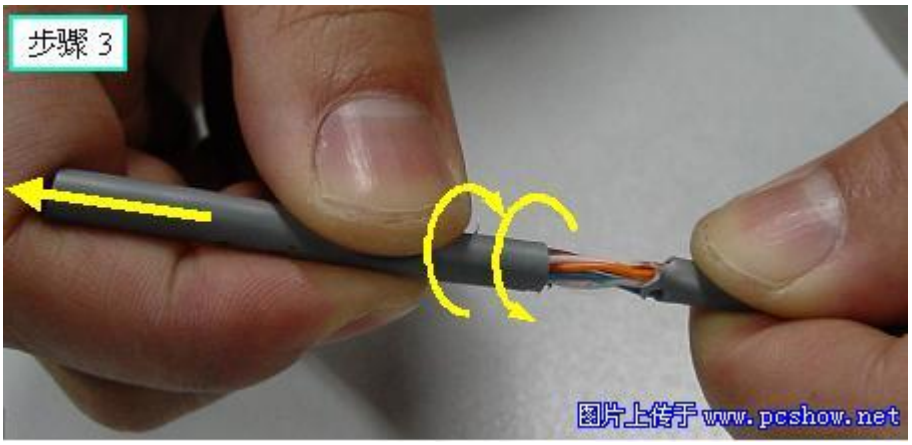
- **制作直连网线：两端都按 EIA568B 标准排列线序。**
- **制作交叉网线：一端按 EIA568A 标准排列，另一端按 EIA568B 标准排列。**

制作步骤：

1）准备

2）转被剥线（剥去外皮 3cm，不宜太长或太短）

3）抽出外套层

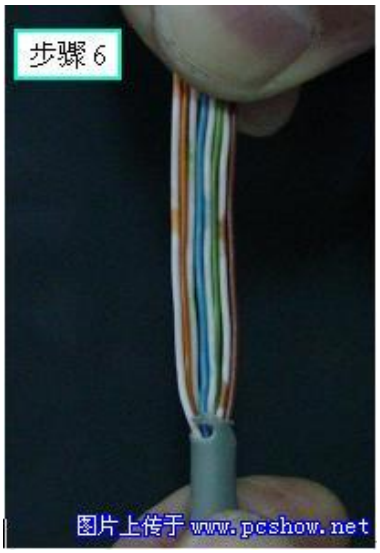


4）露出 4 对电缆

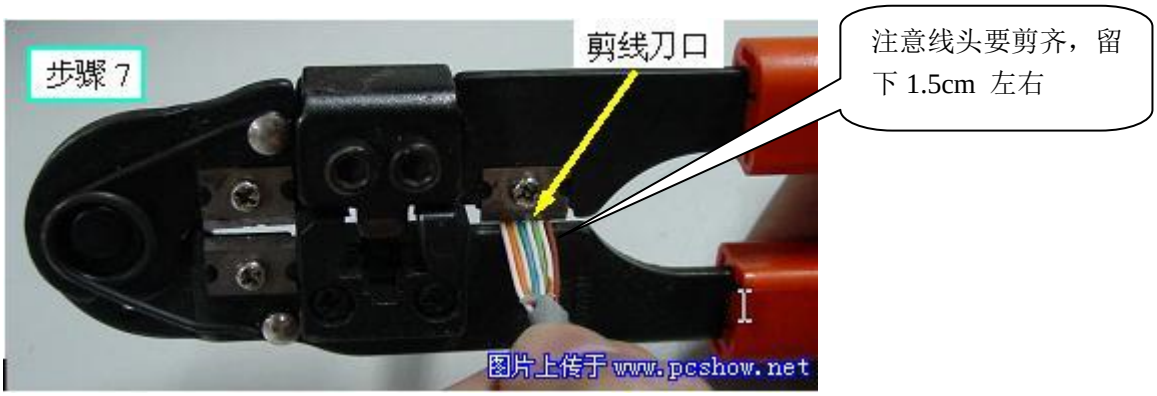
5）按序号排好

图中线序为 568B

6）排列整齐

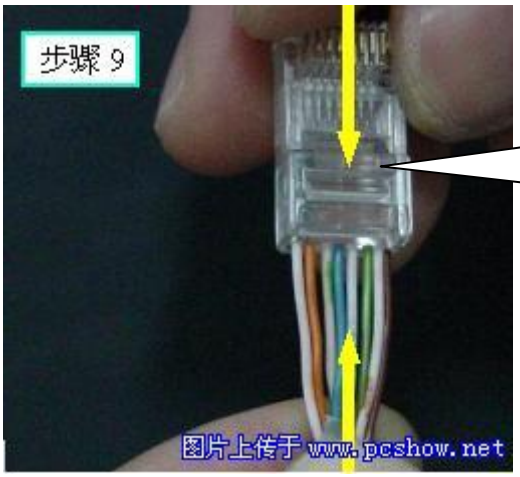


7）剪断

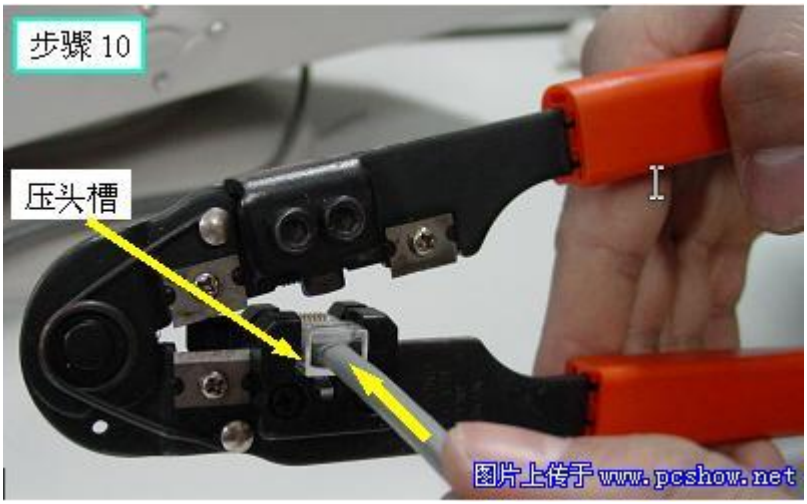


8）剪断后

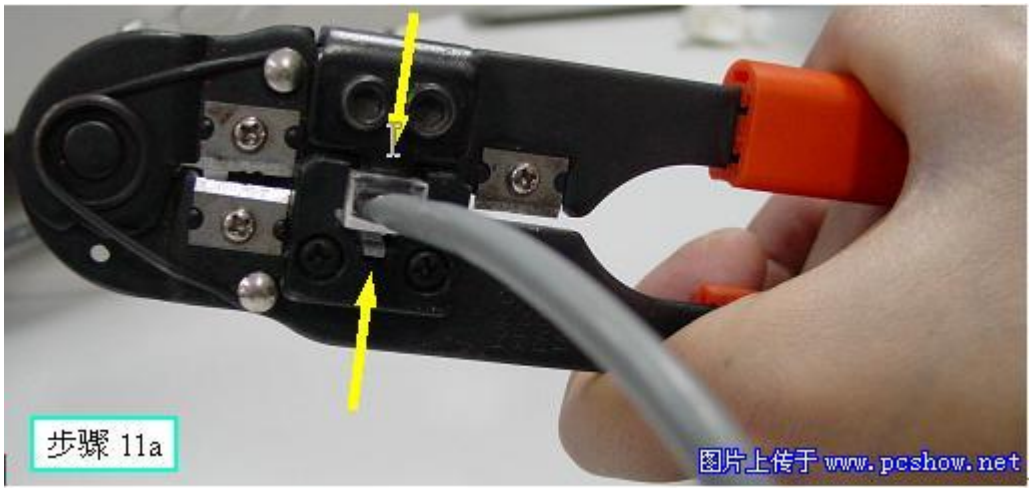
9）放入插头



10）准备压实



11A）压紧



11B）压紧

12）完成并测试

六、水晶头制作实验评价指标

（1）剥去外皮时没有切伤内部铜线外皮

（2）线序正确

（2）双绞线插入水晶头尽头

（3）外皮被水晶头线卡卡紧

（4）通过线缆测试仪通断测试

实验二　网络流量捕获与网络设备模拟器实验

一、实验目的

1、掌握网络流量捕获软件 Wireshark 的基本使用方法

2、掌握使用 Wireshark 捕获网络数据、分析协议数据封装格式

3、掌握 CISCO 网络模拟器 Packet tracer 的基本使用方法。

二、实验属性

验证性实验

三、实验仪器设备及器材

具备 Windows 操作系统的 PC 机、安装 Wireshark 和 Packet tracer 软件。

四、实验要求

1、预习报告中需解决以下问题：windows 环境下常用的网络命令。

2、使用网络命令或使用相应应用软件产生被捕获数据并分析协议数据内容。

3、按规定要求写出实验报告。

五、实验预备知识

(一) windows 环境下常用的网络命令介绍

（1）IP 地址与以太网卡硬件地址查看命令：　**ipconfig**

（2）网络连接测试命令：**ping**

（3）地址解析命令：**ARP**

（4）文件传输命令:**FTP**

（5）显示协议及其端口信息和当前的 TCP/IP 网络连接：**Netstat**

（6）路由跟踪命令：　**Tracert**

（7）远程登录命令：**Telnet**

（1）ipconfig 命令

Ipconfig 命令应该是最最基础的命令了，主要功能就是显示用户所在主机内部的 IP 协议的配置信息等资料。

它的主要参数有：

1、all：显示与 TCP/IP 协议相关的所有细节信息，其中包括测试的主机名、IP 地址、子网掩码、节点类型、是否启用 IP 路由、网卡的物理地址、默认网关等。

2、renew all：更新全部适配器的通信配置情况，所有测试重新开始。

3、release all：释放全部适配器的通信配置情况。

4、renew n：更新第 n 号适配器的通信配置情况，所有测试重新开始。

例如：　C:\>ipconfig ，显示如下

Windows IP Configuration

Ethernet adapter 本地连接:

Connection-specific DNS Suffix . :

IP Address. . . . . : 192.168.0.14
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1

（2）ping 命令

PING 命令是一个在网络中非常重要的并且常用的命令，主要是用来测试网络是否连通。该命令通过发送一个 ICMP（网络控制消息协议）包的回应来看是否和对方连通，一般我们用来测试目标主机是否可以连接，或者可以通过 TTL 值来判断对方的操作系统的版本。

常用参数说明：-a -t -r

使用举例：

Ping 计算机名 ping wangluo21 //获取计算机 IP

Ping IP 地址 ping -a 172.16.22.36 //获取计算机名

Ping 域名 ping www.ecjtu.jx.cn

比如你想测试你和 IP 地址为 192.168.0.1 的机器是否连通，那么就可以使用这个命令：ping 192.168.0.1，那么如果连通就会有如下返回：

C:\>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
。。。。。
Ping statistics for 192.168.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
如果不连通的话，就会返回超时：
Pinging 192.168.0.1 with 32 bytes of data:
Request timed out.
。。。。。。 .
Ping statistics for 192.168.0.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

那么就证明你和该计算机的网络不通，也许是对方没有上网，或者装了防火墙。

在局域网中，如果是同一个工作组的机器，你可以通过 **ping 对方的机器名称获得对方的 IP 地址**，

参数：

-t 可以不间断的向一个机器发送包

-l 包大小参数还能设定发送包的最大值，这样差不多句有了 DoS 的功能了，也就是在黑客技术中的洪水攻击，最大值为 65500。如：

C:\>ping 192.168.0.1 -t -l 65500

因为加了-t 参数，ping 命令本身是不会停止的，于是我们就可以使用 Ctrl + C 来终止该命令。ping 命令还有一些别的参数，请自己参考帮助。

（3）Arp 命令

显示和修改“地址解析协议”(ARP) 所使用的到以太网的 IP 或令牌环物理地址翻译表。该命令只有在安装了 TCP/IP 协议之后才可用。

arp -a [inet_addr] [-N [if_addr]]

arp -d inet_addr [if_addr]

arp -s inet_addr ether_addr [if_addr]

参数：

-a（或 g）：通过询问 TCP/IP 显示当前 ARP 项。如果指定了 inet_addr，则只显示指定计算机的 IP 和物理地址。

inet_addr：以加点的十进制标记指定 IP 地址。

-N：显示由 if_addr 指定的网络界面 ARP 项。

if_addr：指定需要修改其地址转换表接口的 IP 地址（如果有的话）。如果不存在，将使用第一个可适用的接口。

-d：删除由 inet_addr 指定的项。

-s：在 ARP 缓存中添加项，将 IP 地址 inet_addr 和物理地址 ether_addr 关联。物理地址由以连字符分隔的 6 个十六进制字节给定。使用带点的十进制标记指定 IP 地址。项是永久性的，即在超时到期后项自动从缓存删除。

ether_addr：指定物理地址。

（4）FTP 命令

FTP 命令是一个文件传输的命令，该命令可以在两台互联的机器之间传送文件，这跟我们常用的 FTP 软件是一样的，但是我们的软件一般都是 GUI(可视)界面的，但它是命令类型的。 格式如下：

ftp [-v] [-n] [-i] [-d] [-g] [-s:filename] [-a] [-w:windowsize] [computer]

参数解释

-v：禁止显示远程服务器响应。

-n：禁止自动登录到初始连接。

-i：多个文件传送时关闭交互提示。

-d：启用调试、显示在客户端和服务器之间传递的所有 ftp 命令。

-g：禁用文件名组，它允许在本地文件和路径名中使用通配符字符（* 和 ?）。-s: filename：指定包含 ftp 命令的文本文件；当 ftp 启动后，这些命令将自动运行。该参数中不允许有空格。使用该开关而不是重定向 (>)。

-a：在捆绑数据连接时使用任何本地接口。

-w:windowsize：替代默认大小为 4096 的传送缓冲区。

Computer：指定要连接到远程计算机的计算机名或 IP 地址。如果指定，计算机必须是行的最后一个参数。

FTP 命令主要是在网上进行文件的传输，它的子命令非常多，我们挑一些主要的来讲。 一般在命令提示符下输入 FTP 后，就打开如下界面：

C:\>ftp

ftp>

那么我们输入的命令都是在"ftp>"后面的，也就是说我们输入 ftp 命令后，那么我们就进入了 FTP 的平台，所有的操作都是基于 FTP 上的。假如我们要打开一台网络上已经开了 FTP 服务的服务器，那么我们就可以登陆到该服务器,然后上传/下载文件,有时候我们的权限是只能下载,那么我们就不能上传,这具体要看你有的权限。

假如我们要打开一个 FTP 服务器,那么我们就可以在 FTP 平台下输入：

open 主机 IP 端口

例如：ftp>open 192.168.0.39 21，那么就会显示下面的效果：

C:\>ftp

ftp> open 192.168.0.39

Connected to 192.168.0.39.

220 Serv-U FTP Server v4.2 for WinSock ready...

User (192.168.0.39none)):

到这里就需要我们输入用户名，如果是对方的服务器是支持匿名的，那么我们就可以输入像 ftp 之类的用户，如：

User (192.168.0.39none)): ftp

331 User name okay, please send complete E-mail address as password.

Password:

密码也是输入 ftp，那么就会显示登陆成功，如下：

Password: ***

230-(欢迎你来到 FTP192.168.0.39 服务器!）

230 User logged in, proceed.

ftp>

显示 230 就代表代表登陆成功，如果显示别的，比如 530，那么就是用户名

或密码错误，登陆失败。

登陆后就可以使用一些命令，包括上传/下载，执行外部命令等。要获得FTP 的所有命令，可以键入 help 命令，它所有命令列表如下：ftp> help

我们把常用的命令解释一下：

1．!：执行一个非 FTP 平台下的外部命令，如：!cls，那么将清除屏幕。

2．delete：删除一个文件，比如在你的当前 FTP 根目录下有一个 dir1.txt 的文件，你需要删除它，就输入 delete dir1.txt。

3．ls：列出现在有的文件列表，该命令是 Unix/Linux 下的一个命令，主要是列出该目录下的文件，而不管文件夹

4．put：从本地计算机上传一个文件到 FTP 服务器上，

例如：put　cmd.exe，那么就会把当前目录下有的 cmd.exe 传的 FTP 服务器

5．上的当前目录,该命令是最常用的。

6．ascii：该命令可以使上传的文件是按照 ASCII 码来传输的。

7．get：该命令也比较常用，也是把对方 FTP 服务器上的文件下载到自己的当前目录。如：get cmd.exe，就会把 FTP 服务器上的

8．cmd.exe 文件下载到当前目录。

9．mdelete/rmdir：删除一个目录/文件夹,比如：mdelete a ，那么该文件夹将被删除。

10．pwd：显示当前所处在 FTP 的那个目录下，相当于显示当前路径。例如：

ftp> pwd

257 "/SOFTWARE/safe_tools" is current directory.

11．quit/bye：结束当前的 FTP 连接，并且退出 FTP。

12．type：设定文件传输类型，类型有： [ascii | binary | image | tenex],如果你是传文本文件之类的就使用 ascii 码，如果是应用程序的话，就使用 binary，如果是图片就使用 image。FTP 默认的是 ascii 码，如果你要传应用程序，就要使用 binary。例如我们要上传一个 lk.exe 的文件，那么我们先设置传输模式为 binary，然后再上传,如：

ftp> type binary （ 200 Type set to I. ）

ftp> put lk.exe （200 PORT Command successful. ）

13．mget：同时下载多个文件。

14．mput：同时上传多个文件。

15．user：向远程主机器表示自己的身份，如：

ftp> user

Username: ftp

331 User name okay, please send complete E-mail address as password.

Password: ***

230 User logged in, proceed.

16．cd：切换目录，进入一个目录使用 cd 目录,退到上一个层目录使用 cd ..（注意中间有一个空格)，该命令比较常用。

17．help/?：显示帮助，主要是显示在 FTP 下可以用的命令。

18．rename：重命名，给文件重新命名。

19．close：关闭当前的 FTP 连接，但是不退出 FTP，和 quit/bye 命令不一样。如：

ftp> clos

221 Goodbye!

20．open 打开一个 FTP 连接。如：

ftp> open 192.168.0.39

Connected to 192.168.0.39.

220 Serv-U FTP Server v4.2 for WinSock ready...

User (192.168.0.39none)):

FTP 中比较常用的命令就这些，当然还设计一些别的命令，而且也要因不同的 FTP 服务器支持的命令不一样而定，所以如果碰到实际应用中不同，请参考相关的资料。

（5）Netstat

显示协议统计和当前的 TCP/IP 网络连接。该命令只有在安装了 TCP/IP 协议后才可以使用。

netstat [-a] [-e] [-n] [-s] [-p protocol] [-r] [interval]

参数说明：

-a：显示所有连接和侦听端口。服务器连接通常不显示。

-e：显示以太网统计。该参数可以与 -s 选项结合使用。

-n：以数字格式显示地址和端口号（而不是尝试查找名称)。

-s：显示每个协议的统计。默认情况下，显示 TCP、UDP、ICMP 和 IP 的统计。

-p ：选项可以用来指定默认的子集。

-p protocol：显示由 protocol 指定的协议的连接；protocol 可以是 tcp 或 udp。如果与 -s 选项一同使用显示每个协议的统计，protocol 可以是 tcp、udp、icmp 或 ip。

-r：显示路由表的内容。

Interval：重新显示所选的统计，在每次显示之间暂停 interval 秒。按 CTRL+B 停止重新显示统计。如果省略该参数，netstat 将打印一次当前的配置信息。

（6）Tracert 命令

tracert 命令主要用来显示数据包到达目的主机所经过的路径，显示数据包经过的中继节点清单和到达时间。该命令的使用格式：

tracert 主机 IP 地址或主机名

该诊断实用程序将包含不同生存时间 (TTL) 值的 Internet 控制消息协议 (ICMP) 回显数据包发送到目标，以决定到达目标采用的路由。要在转发数据包上的 TTL 之前至少递减 1，必需路径上的每个路由器，所以 TTL 是有效的跃点计数。数据包上的 TTL 到达 0 时，路由器应该将“ICMP 已超时”的消息发送回源系统。Tracert 先发送 TTL 为 1 的回显数据包,并在随后的每次发送过程将 TTL 递增 1，直到目标响应或 TTL 达到最大值，从而确定路由。路由通过检查中级路由器发送回的“ICMP 已超时”的消息来确定路由。不过，有些路由器悄悄地下传包含过期 TTL 值的数据包，而 tracert 看不到。

tracert [-d] [-h maximum_hops] [-j computer-list] [-w timeout] target_name

/d：指定不将地址解析为计算机名。

-h maximum_hops：指定搜索目标的最大跃点数。

-j computer-list：指定沿 computer-list 的稀疏源路由。

-w timeout：每次应答等待 timeout 指定的微秒数。

target_name：目标计算机的名称。

执行结果返回数据包到达目的主机前所历的中断站清单，并显示到达每个继站的时间。该功能同 ping 命令类似，但它所看到的信息要比 ping 命令详细得多，它把你送出的到某一站点的请求包，所走的全部路由均告诉你，并且告诉你通过该路由的 IP 是多少，通过该 IP 的时延是多少。 该命令参数有：

-d：不解析目标主机的名称

-h： maximum_hops 指定搜索到目标地址的最大跳跃数

-j：host_list 按照主机列表中的地址释放源路由

-w：timeout 指定超时时间间隔，程序默认的时间单位是毫秒

使用 tracert 命令可以很好的连接和目标主机的连接通道，一般为下一不的入侵或者测试获得详细的网络信息打好基础，例如中途经过多少次信息中转，每次经过一个中转站时花费了多长时间。通过这些时间，我们可以很方便地查出用户主机与目标网站之间的线路到底是在什么地方出了故障等情况。如果我们在 tracert 命令后面加上一些参数，还可以检测到其他更详细的信息。例如使用参数－d，可以指定程序在跟踪主机的路径信息时，同时也解析目标主机的域名。

我们简单的使用该命令来测试到达 www.baidu.com 的时间和经过的 IP 地址：

C:\>tracert www.baidu.com

Tracing route to www.baidu.com [202.108.250.228]

over a maximum of 30 hops:

1 <1 ms <1 ms <1 ms 192.168.0.1

2 1 ms <1 ms 1 ms 211.152.23.6

3 * 5 ms 3 ms 211.152.47.253

4 3 ms 3 ms 3 ms 210.78.156.66

5 3 ms 9 ms 4 ms 211.99.57.113

6 6 ms 5 ms 7 ms 202.108.250.228

Trace complete.

看信息我们知道我们通过了 6 个 IP 节点和使用的时间。第一个一般是我们的机器是从该 IP 出去的，第二个开始就是经过的路由，最后一个当然就是我们的目的地了。在入侵中，如果你肯对这些地址层曾追查的话，一定会有大收获啦。

（7）Telnet 命令

Telnet 命令是一个远程登陆的命令，就可以通过这个命令来远程登陆网络上已经开发了远程终端功能的服务器，来达到像本地计算机管理远程计算机。 该

命令格式：**telnet 远程主机 IP 端口**

例如:telnet 192.168.0.1 23

如果我们不输入端口,则默认为 23 端口。一般登陆后，对方远程终端服务就会要求你输入用户名和密码，正确就让你登陆。

一般出现如下消息：

Welcome to Microsoft Telnet Service

login: root

password: ******

如果登陆成功后将出现如下信息：

*===

Welcome to Microsoft Telnet Server.

*===

C:\Documents and Settings\root>

这就表示已经 telnet 到了对方的系统，就可以做在你用户权限内的所有操作。

(二) Wireshark 软件介绍与应用案例

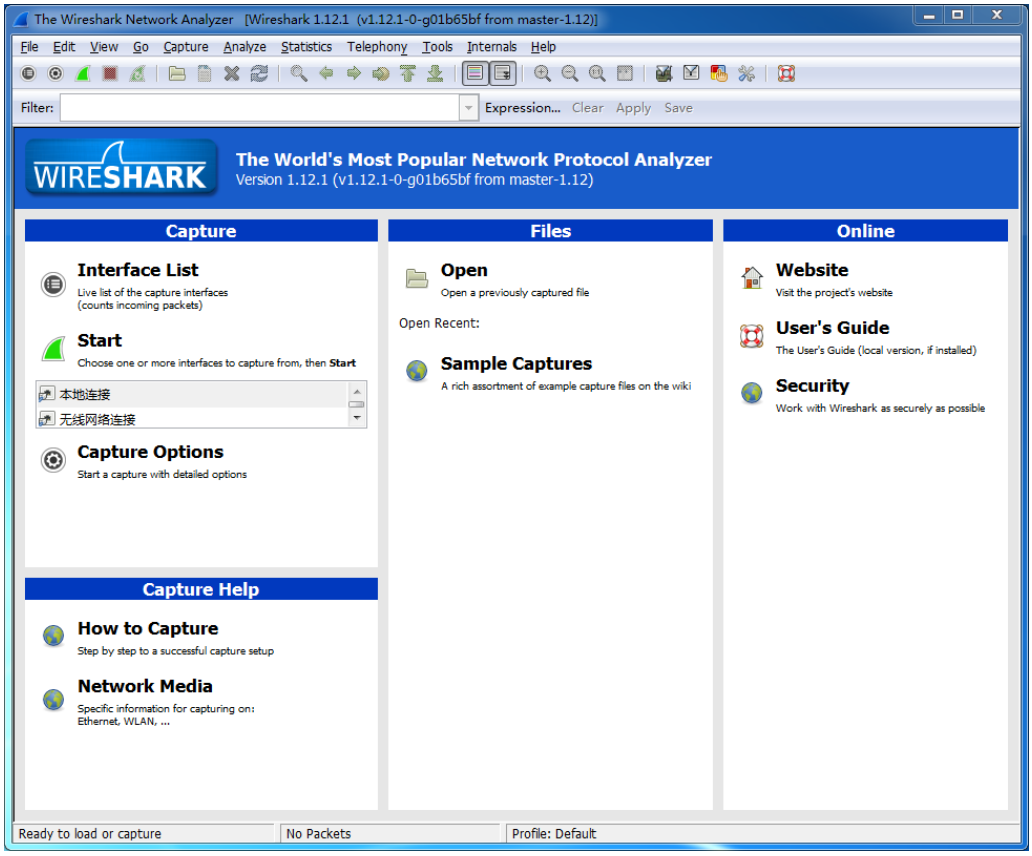
下载、安装 Wireshark

设用户计算机的网卡（以太网适配器）本地连接配置如下:

物理地址. . . . . : 74-D4-35-79-68-65

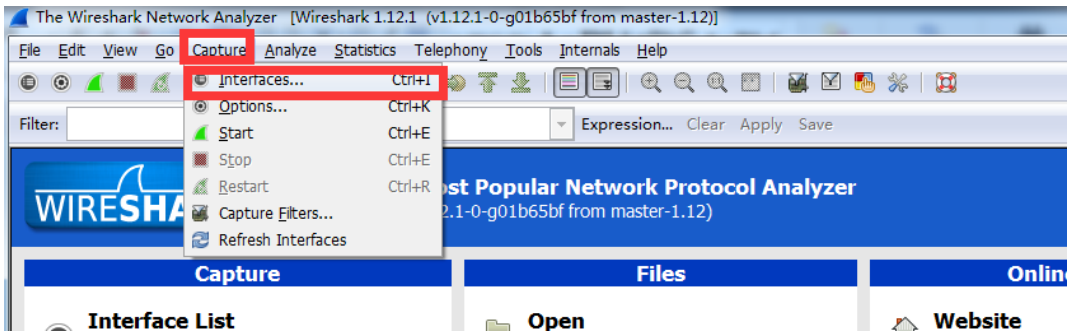
DHCP 已启用 . . . . . : 是
自动配置已启用. . . . . : 是
本地链接 IPv6 地址. . . . . : fe80::d843:50ba:8a23:5524%11(首选)
IPv4 地址 . . . . . : 10.3.9.8(首选)
子网掩码 . . . . . : 255.255.255.0
获得租约的时间 . . . . . : 2014 年 12 月 3 日 14:50:51
租约过期的时间 . . . . . : 2014 年 12 月 3 日 22:50:51
默认网关. . . . . : 10.3.9.254
DHCP 服务器 . . . . . : 211.64.120.175
DHCPv6 IAID . . . . . : 242537525
DHCPv6 客户端 DUID . . . . . : 00-01-00-01-1B-CF-E0-67-74-D4-35-79-68-65
DNS 服务器 . . . . . : 211.137.191.26
218.201.96.130
TCPIP 上的 NetBIOS . . . . . : 已启用

Wireshark启动后，如图所示：

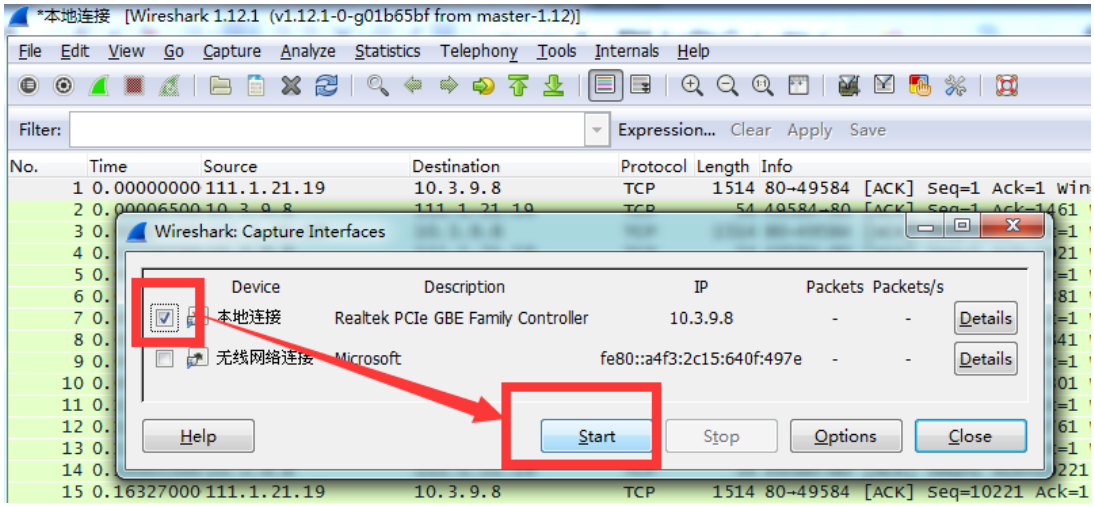


抓包步骤：

1）点击Capture菜单，选Interfaces...项。

2） 

3）打开如下图所示窗口。

4） 

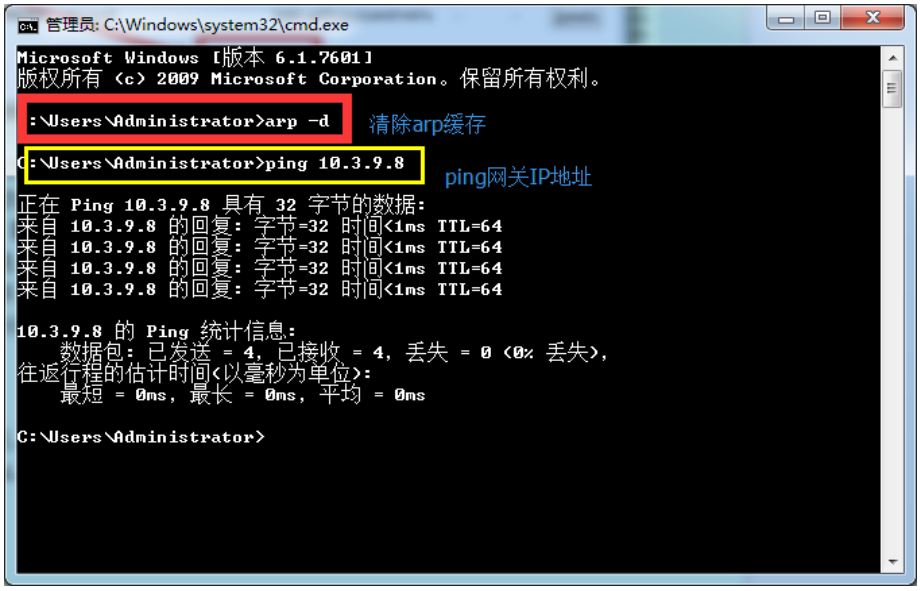
5）

6）选择要抓包的接口右边的Start按钮，本例选择了抓取IP地址为10.3.9.8的接口。

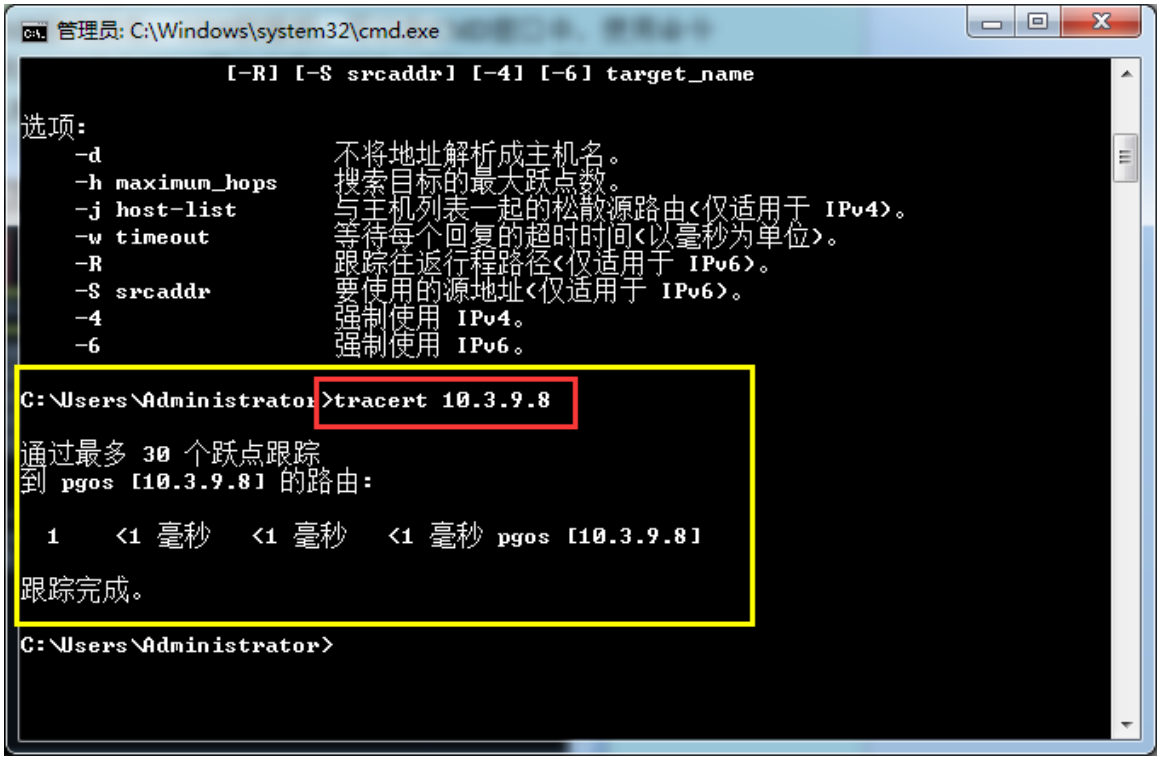
点击Start按钮后将启动抓包过程。

注意：为配合抓包，需要进行网络通信。

1）要抓ARP分组的包、ICMP报文的包、UDP数据报，可以在CMD窗口中，使用命令ARP -D删除当前ARP缓存，使用PING命令PING某台主机IP地址。

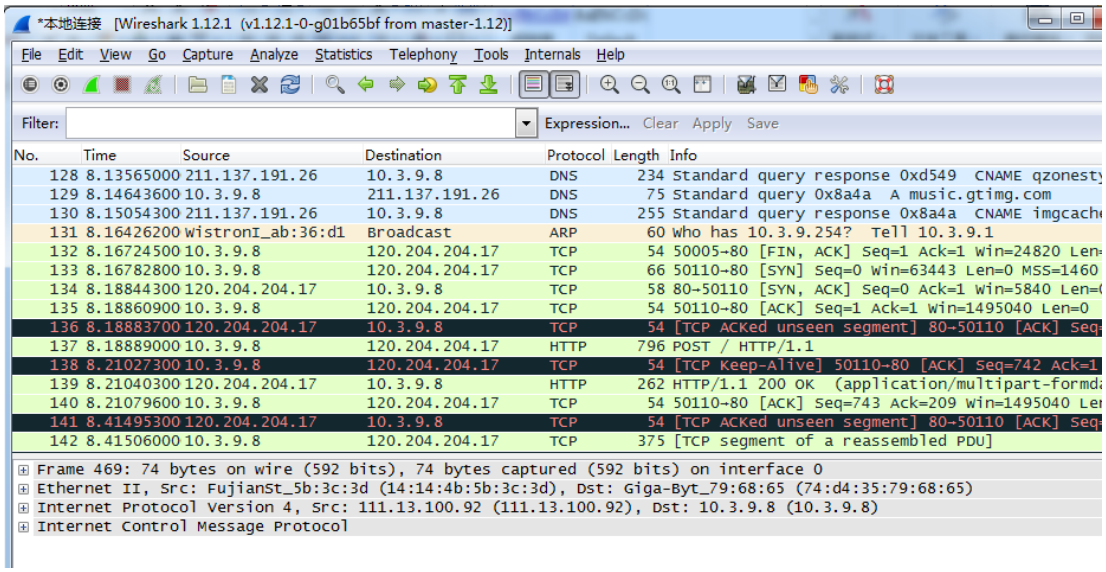


使用TRACERT命令跟踪分组从源点到终点的路径（如下图）。



2）要抓取TCP报文段，需打开IE浏览器，访问一个WWW网站（例如www.baidu.com）。

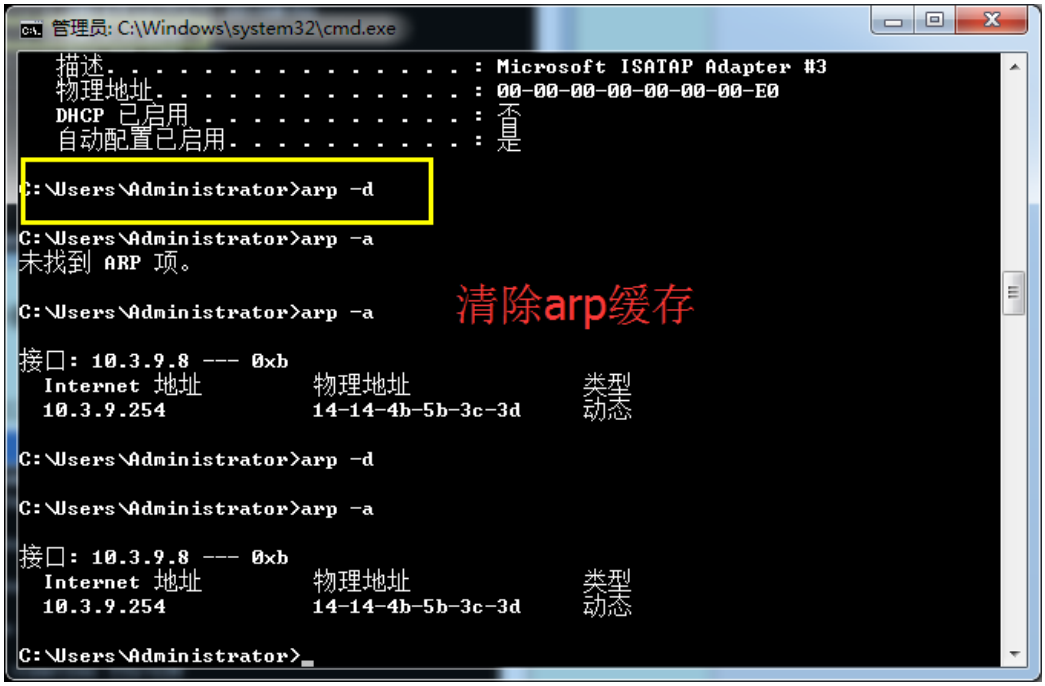
将窗口切换到Wireshark，可以看到抓到了TCP、UDP、ICMP、ARP的包，如下图所示。



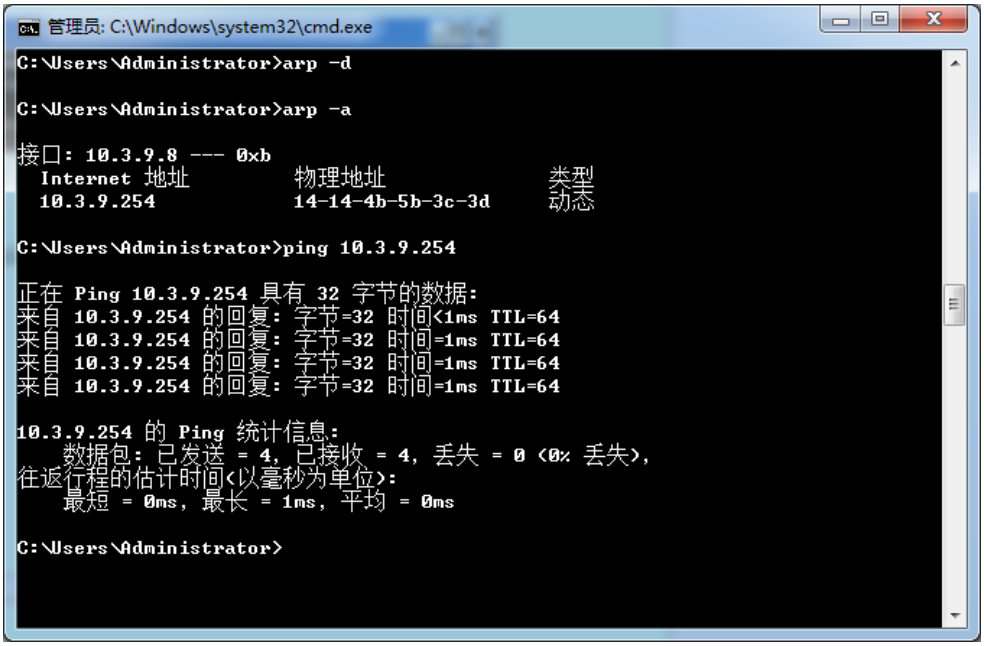
下面分析所用到的包，其抓包的环境是：

1）实验计算机所安装操作系统为Windows 7

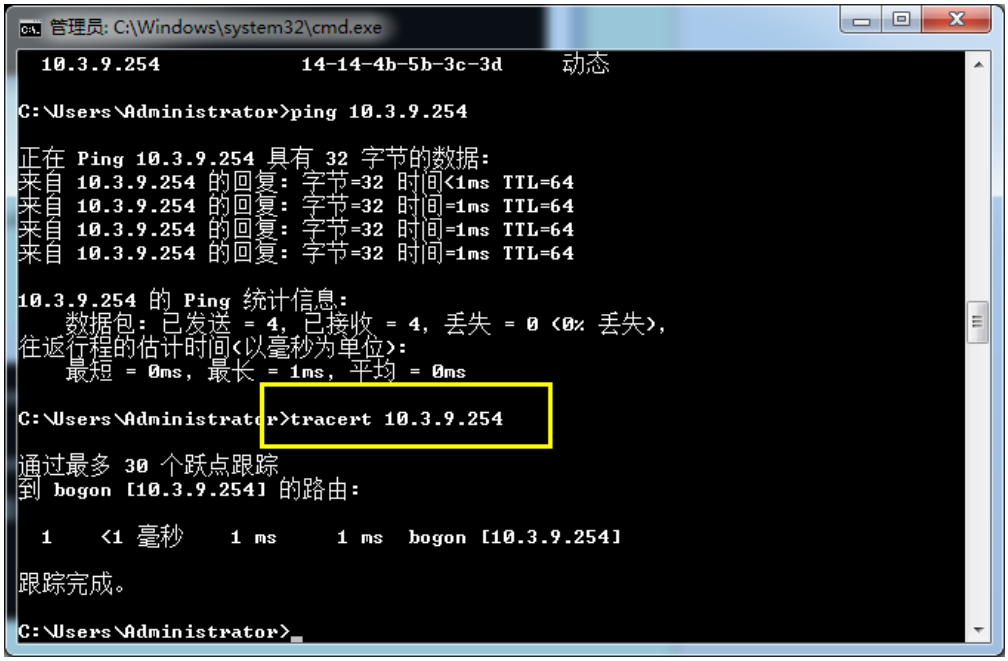
(2)在CMD窗口运行“ARP –D”命令删除ARP缓存，用以抓取ARP分组;



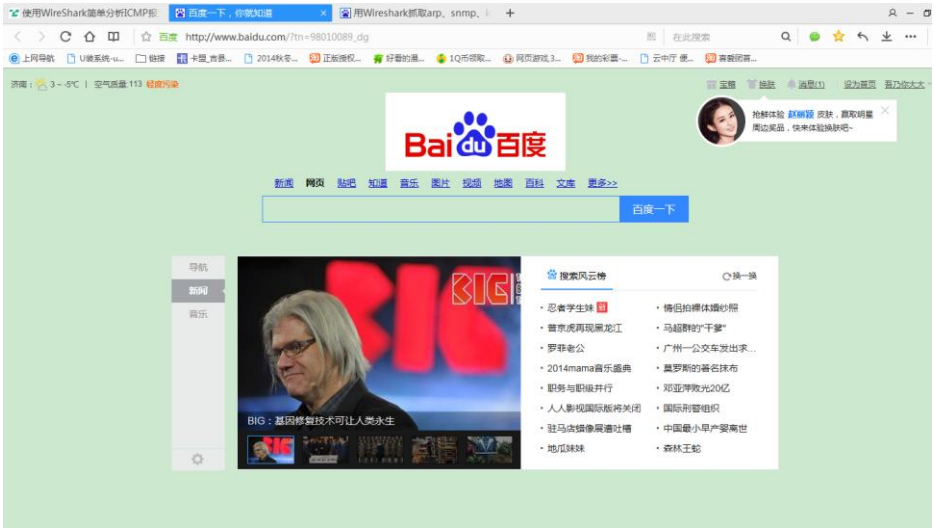
(3)在CMD窗口运行“PING 10.3.9.254”，用以抓取ICMP报文;



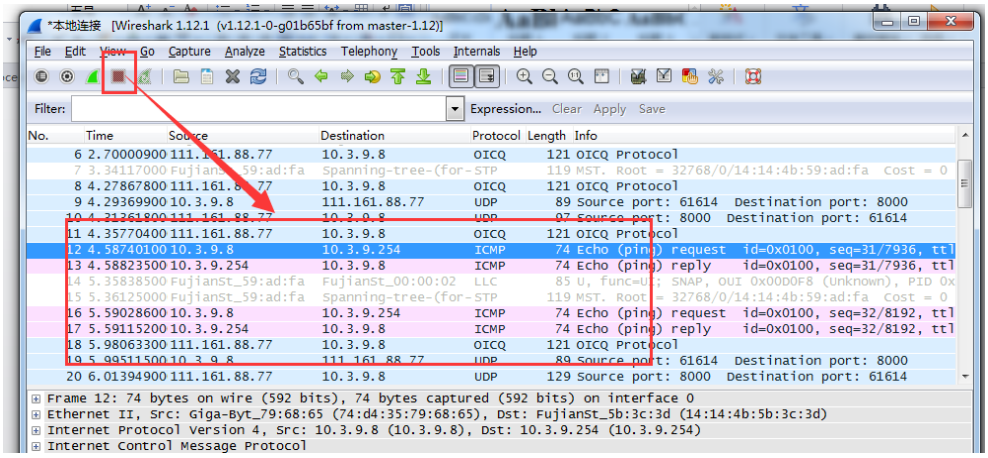
(4)在CMD窗口运行“TRACERT 10.3.9.254”，用以抓取UDP数据报和ICMP报文；



(5)在浏览器窗口打开HTTP://WWW.BAIDU.COM网站，用以抓取TCP报文段。



点击Stop按钮完成抓包。如下图所示。

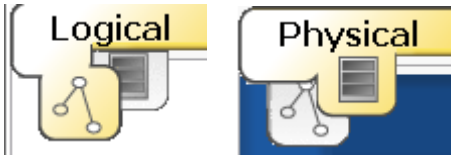


(三) Packet Tracer 软件使用介绍

Packet Tracer 是与新版 CCNA Discovery 和 CCNA Exploration 并行发布的一个网络模拟器。PT 提供可视化、可交互的用户图形界面，来模拟各种网络设备及其网络处理过程，使得实验更直观、更灵活、更方便。

PT 提供两个工作区：逻辑工作区（Logical）与物理工作区（Physical）。

- 逻辑工作区：主要工作区，在该区域里面完成网络设备的逻辑连接及配置。
- 物理工作区：该区域提供了办公地点（城市、办公室、工作间等）和设备的直观图，可以对它们进行相应配置。

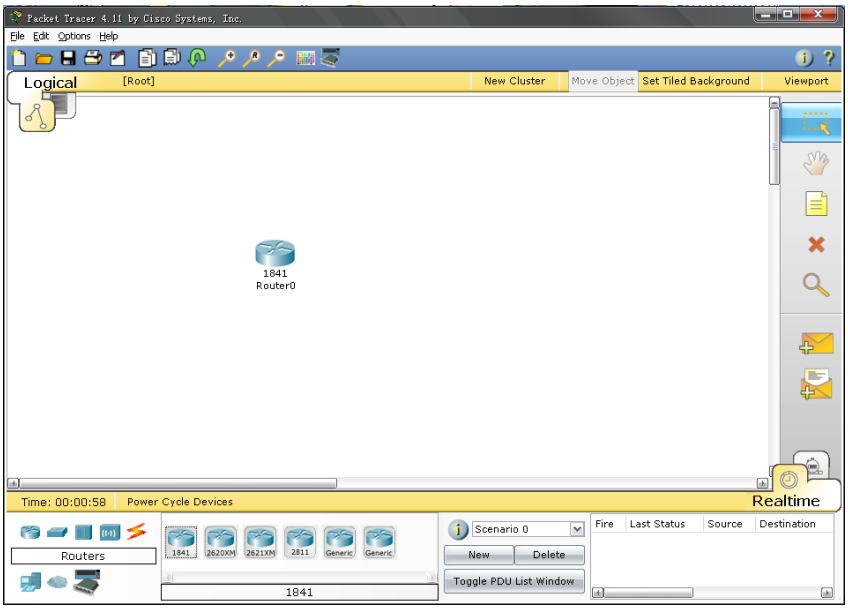
左上角可以切换这两个工作区域。 

PT 提供两种工作模式：实时模式（Real-time）与模拟模式（simulation）。

- 实时模式：默认模式。提供实时的设备配置和 Cisco IOS CLI（Command Line Interface）模拟。
- 模拟模式：Simulation 模式用于模拟数据包的产生、传递和接收过程，可逐步查看。

右下角可以切换这两种模式。 

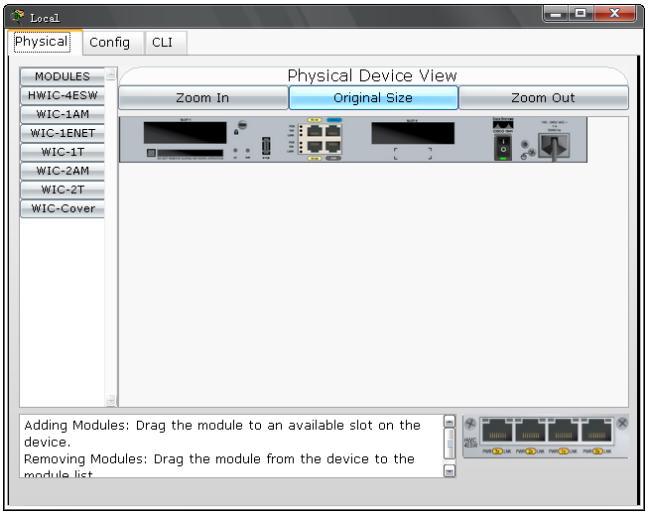
Packet Tracer 界面操作如下：



- 逻辑工作区（Logical Workplace）（中间最大块的地方）：显示当前的拓扑结构和各个设备的状态。
- 图例导航区（Symbol Navigation）（左下角）：切换不同的设备图例。如单击路由器图标，右边出现所有可选的路由器型号。

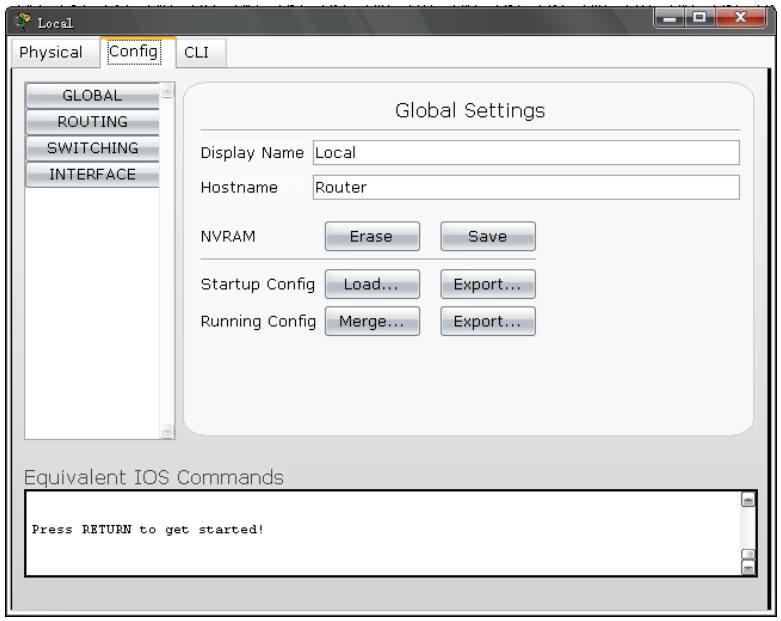
从导航区可以拖动某个设备图标到工作区。单击工作区中的设备，可以调出该设备的设置界面：

1. 在 Physical 标签下可以进行设备模块的配置。默认情况下，设备没有安装任何模块。我们可以从左边的 MODULES 列表拖动需要的模块到设备的空插槽中（左下角有相应的模块说明）。注意拖放前要关闭设备的电源（在图片中点击电源即可）。



2. 在 Config 标签下可以进行图形界面交互配置（GUI），下面文本框会显示等价的命令

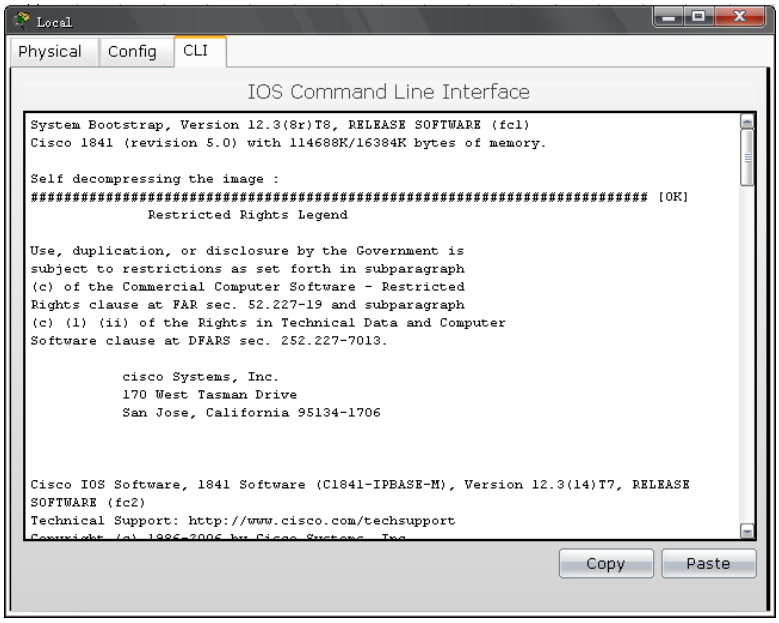
行语句。



配置包括 GLOBAL、ROUTING、SWITCHING、INTERFACE 四个大项。点击每项可以出现具体的子项列表（随设备不同而略有不同）：

- GLOBAL：Settings
- ROUTING：Static；RIP
- SWITCHING：VLAN Database
- INTERFACE：包括设备上的所有物理接口，如 FastEthernet0/1 等。

3. 在 CLI 标签下可以进行命令行的配置，它与在交互界面下进行的配置是等效的：



六、实验内容

1、安装相应数据捕获软件 Wire shark 和 网络模拟软件 Packet tracer

2、使用 Ipconfig/all 命令查看计算机网卡属性，获取 IP 地址、默认网关地址、网卡硬件地址

3、启动 Wire shark，分别捕获 ping 网关、Tracert www.baidu.com 等命令的数据

4、使用网络模拟软件 Packet tracer 组成简单网络并正确连接设备

5、将相关命令或操作结果用截图的方法保存在实验报告中

实验三　交换机 VLAN 配置

一、实验目的

1、掌握交换机基本配置命令

2、掌握交换机 Telnet 配置

2、理解 VLAN 的概念、原理及划分 VLAN 的方法。

2、掌握基于交换机端口的 VLAN 划分方法。

3、掌握 Cisco2950 交换机的单交换机和跨交换机 VLAN 配置方法，了解各配置命令的作用。

二、实验属性

验证性试验。

三、实验仪器设备及器材

Cisco 2950 交换机、具备 Windows 操作系统的 PC 机、直通双绞线、交叉双绞线、Cisco 配置线缆。

四、实验要求

1、预习报告中需解决以下问题：熟练掌握 Cisco2950 交换机 VLAN 相关配置命令以及各命令的作用。

2、试验中正确使用仪器设备，独立操作。

3、试验后按规定要求写出实验报告。

五、实验预备知识

（一）交换机基本配置模式

Cisco 交换机提供了几种配置模式（或称之为配置视图），各配置模式下所能使用的配置命令各不相同，这几种配置模式如下：

普通用户模式：开机直接进入普通用户模式，在该模式下我们只能查询交换机的一些基础信息，如版本号（show version）。提示信息：**switch>**

特权用户模式：在普通用户模式下输入 enable 命令即可进入特权用户模式，在该模式下我们可以查看交换机的配置信息和调试信息等等。提示信息：**switch#**

全局配置模式：在特权用户模式下输入 configure terminal 命令即可进入全局配置模式，在该模式下主要完成全局参数的配置。提示信息：**switch(config)#**

接口配置模式：在全局配置模式下输入 interface *fa0/1* 即可进入接口配置模式，在该模式下主要完成接口参数的配置。提示信息：**switch(config-if)#**

VLAN 配置模式：在全局配置模式下输入 vlan database 即可进入 VLAN 配置模式下该配置模式下可以完成 VLAN 的一些相关配置。**switch(vlan)#**

注意：在使用命令行进行配置的时候，不可能完全记住所有的命令格式和参数，思科交换机提供了强有力的帮助功能，在任何模式下均可以使用“？”来查看命令的格式或参数，具体用法如下。

1. 在任何模式下直接键入“？”　　查询任何模式下可以使用的所有命令
2. 在前缀字符后键入“？”　　可以查看该视图下以该前缀开头的所有命令
   如键入“s？”可以查询所有以字符 s 开头的所有命令
3. 命令单词后跟一个空格和一个“？” 如“show ？”用来查看 show 命令的参数

交换机工作模式切换

（1）登陆交换机，进入用户模式。连接交换机并且登陆。请注意现在交换机上的显示符号。显示如下：Switch>

（2）使用 help 命令，使用 help 命令（？）查看在用户模式下路有器所支持的命令。

（3）进入特权模式，输入（enable）命令，进入特权模式。如果交换机有密码保护那么此时需要输入确认密码。注意现在所显示符号和用户模式时的差别。显示如下：Switch#

（4）使用 help 命令，使用 help 命令（？）查看在特权模式下路有器所支持的命令。注意和用户模式下的区别。

（5）进入全局配置模式，输入命令（configure terminal or config t）进入全局配置模式。注意现在所显示符号以及命令提示。显示如下：Switch(config) #

（6）使用 help 命令，使用 help 命令（？）查看在全局配置模式下路有器所支持的配置命令。

（7）退出全局配置模式，使用快捷键（Ctrl+Z）退出全局配置模式，进入特权模式。也可以使用命令（exit）退出全局配置模式。

（8）退出特权模式，使用命令（disable）从特权模式会到用户模式。

（9）退出交换机，使用命令（exit）退出交换机。这个命令可以用来从特权模式中退出交换机。

（二）交换机名称、口令设置命令格式

（1）交换机改名：通过超级终端进入交换机，并进入全局模式，键入命令：

Switch(config)#hostname switch2950

Switch2950 (config)#

你会发现交换机的命令提示行的名称由 Switch 更改为 Switch2950。

（2）全局模式下，设定明文口令 cisco,此口令可以限制对特权模式的访问。在配置文件中可以看见口令。注意：口令一般不应以较为简单或有明显特征的单词，不过在实验的过程中可以采用象 cisco 这样的单词。口令区分大小写。

Switch2950 (config)#enalbe password cisco

（3）全局模式下，设定加密口令 Cisco,此口令可以限制对特权模式的访问。

Switch2950 (config)#enalbe secret cisco

注意加密口令与明文口令同时设置时，只有加密口令有效。

（4）接口模式下，设定控制台终端的登陆口令,cisco。

Switch2950 (config)#line console 0　　进入接口模式

Switch2950 (config-line)#login

Switch2950 (config-line)#password cisco

（5）接口模式下，设定远程登陆口令,cisco

Switch2950 (config)#line vty 0 4

Switch2950 (config)#login

Switch2950 (config)#password cisco

注：vty 0 4 是 5 个不同的虚拟终端连接。

（6）以上口令设置中，除了 enable secret 设置加密口令外，其余均可通过 show run 命令在配置文件中查看。可以通过全局命令将明文口令加密。

Switch2950 (config)#service password-encryption

（7）交换机命令历史，Cisco 交换机会保存输入过的命令，并可以对保存的命令的个数进行设置，同时可以再次通过快捷方式进行使用，这在再次输入很长或很复杂的命令时很有用。缺省情况下，系统会保存 10 条命令，最大可以设置 256 条命令。

设置命令行数为 100

Switch2950#terminal history size 100

（8）任何时候可以使用 show running-config 命令查看命令配置，可以在特权模式下使用 copy running-config startup-config 命令保存配置。

（三）交换机端口配置命令示例

（1）由用户模式进入特权模式

开始进入交换机提示符配置界面的模式模式即为用户模式，提示符为 Switch>

键入命令 enable 即进入特权模式，提示符为 Switch#

继续键入 config terminal 命令，则由特权模式进入全局配置模式，提示符为 Switch(config)#

配置模式转换示例：

```
Switch>
Switch> enable
Switch#
Switch# config terminal
Switch(config)#
```

（2）接口配置模式下配置端口速度和工作模式

在全局配置模式下，执行 interface 命令，即进入接口配置模式。在该模式下，可对选定的接口（端口）进行配置，并且只能执行配置交换机端口的命令。接口配置模式的命令行提示符为：student1(config-if)#

例如，若要设置 Cisco Catalyst 2950 交换机的 0 号模块上的第 1 个快速以太网端口的端口通讯速度设置为 100M，全双工方式，则配置命令为：

```
Switch (config)#interface fastethernet 0/1
Switch (config-if)#speed 100
Switch (config-if)#duplex full
Switch (config-if)#end
```

（3）查看交换机配置文件

在特权模式下使用命令 show running-config 可以查看交换机的当前配置情况：

```
Switch#show running-config
Building configuration...
Current configuration : 1107 bytes
!
version 12.1
no service password-encryption
!
hostname Switch
!
interface FastEthernet0/1
 duplex full
 speed 100
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
```

!

.....

!

end

（四）交换机命令的撤销

格式：no　原来的命令行

如：no speed 100　　# 取消速度设置为 100 的命令

no duplex full　# 取消设置为全双工的命令

（五）使用 telnet 方式配置交换机实验示例

（1）通过 Console 口搭建本地配置环境

在交换机第一次使用的时候，必须采用通过 Console 口方式对交换机进行配置，具体的操作步骤如下：

第一步：如下图所示，将一字符终端或者计算机的串口通过标准的 RS232 电缆和交换机的 Console 口（也叫配置口）连接。

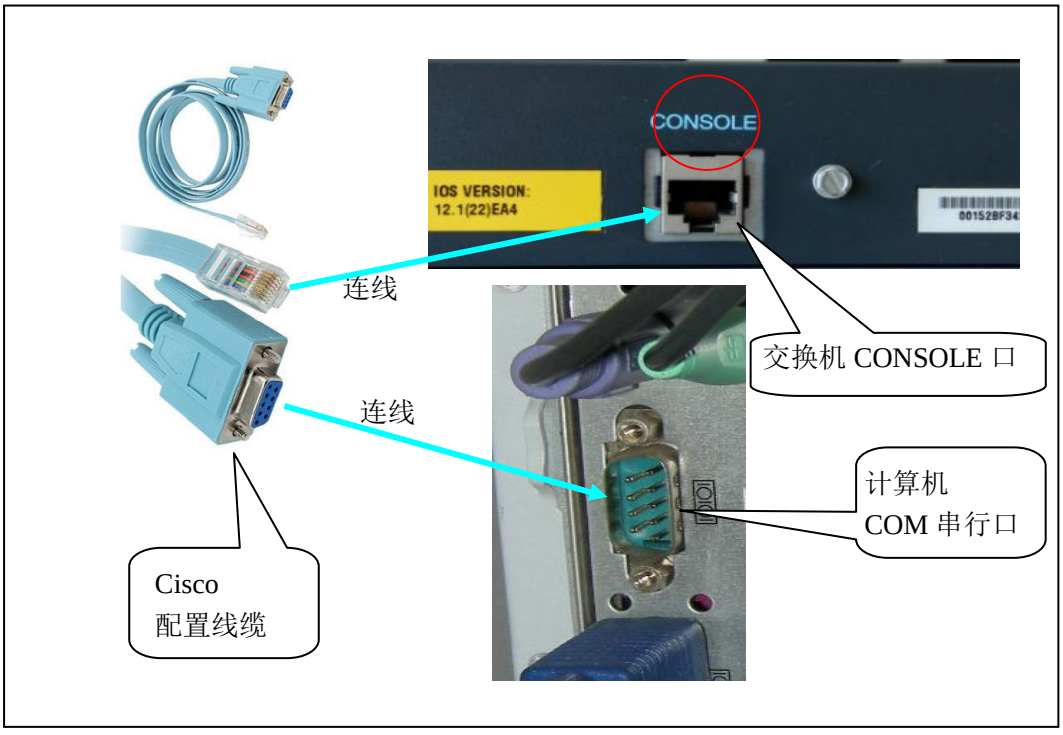


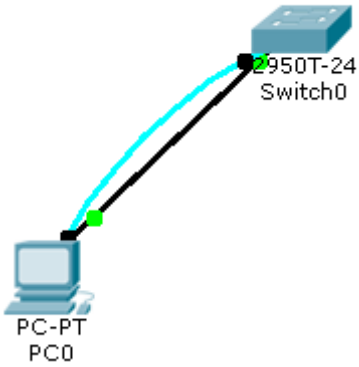
图 1：通过 Console 口搭建本地配置环境

第二步：配置终端的通讯设置参数，如果采用计算机，则需要运行终端仿真程序，如 Windows 操作系统提供的 Hyperterm(超级终端)等，以下以超级终端为例，说明具体的操作过程。运行超级终端软件，建立新连接，选择和交换机的 Console 连接的串口，设置通讯参数：9600 波特率、8 位数据位、1 位停止位、无校验、无流控，并且选择终端仿真类型位 VT100，与实验三交换机基本配置实验一样操作步骤一样打开 Windows 的超级终端的设置

界面。

第三步：交换机上电，启动交换机，这时将在终端屏幕，或者计算机的超级终端窗口内显示自检信息，自检结束后提示用户键入回车，直到出现命令行提示符“Switch>”。

第四步：这时便可以在终端上或者超级终端中对交换机进行配置，查看交换机的运行状态，如果需要帮助，可以随时键入“？”，交换机便可以随时提供详细的在线帮助了。

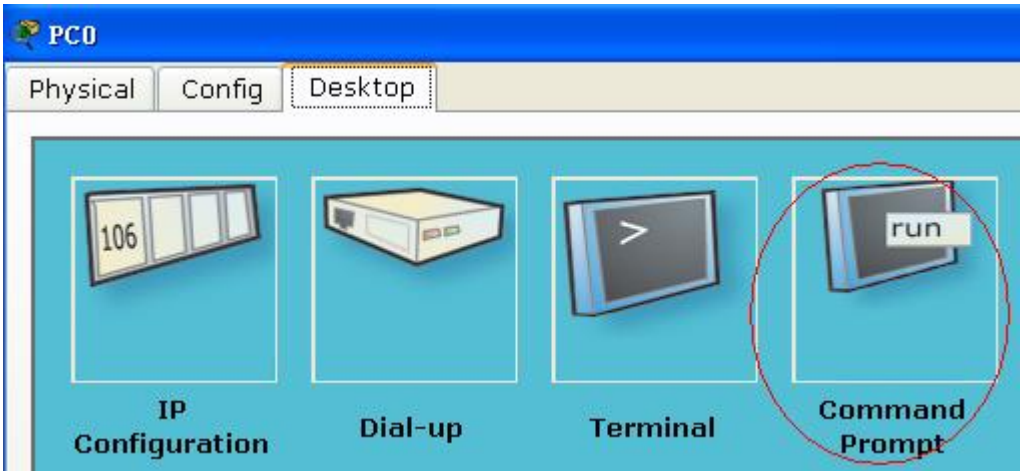


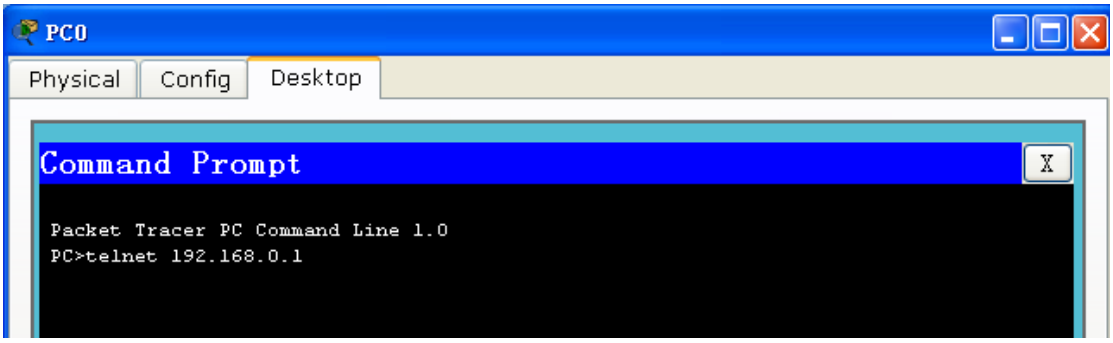
（2）使用双绞线连接计算机网卡和交换机任意一个网络接口，将计算机的 IP 地址设置为 192.168.0.2（计算机 IP 地址可以选择 192.168.0.0 网段内任意一个地址，但不能和下面的交换机管理 IP 地址相同，以免发生冲突），子网掩码设置为 255.255.255.0。

（3）使用超级终端配置交换机，命令如下：

```
Switch>enable                    #进入特权模式
Switch#configure terminal      #进入全局配置模式
Enter configuration commands, one per line.   End with CNTL/Z.
Switch(config)#interface vlan 1      #进入 VLAN 配置模式
Switch(config-if)#ip address 192.168.0.1 255.255.255.0   #配置交换机管理 IP 地址
#此步骤若 IP 地址或掩码弄错了，则可以用命令 no ip address 来删除前面设置的错误参数，重新输入正确的命令行。
Switch(config-if)#no shutdown          #激活（开启）交换机端口
                                       #以下为端口开启后（up）的显示信息
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
Switch(config-if)#exit       #返回上级配置模式（视图）
Switch(config)#enable password 111111     #设置进入特权模式的密码
Switch(config)#line vty 0 4                #  进入线路配置模式
                                           #配置管理虚拟终端用户 0~4，共 5 个用户
Switch(config-line)#password 222222       #设置 telent 的密码
Switch(config-line)#login                  #密码设置为登录（login）交换机时有效
Switch(config-line)#end                    #等价于 Ctrl+Z 快捷键，返回特权模式提示符
Switch #
```

（4）在模拟器的计算机命令符模式下进入登录交换机的命令





输入 telent 的密码（222222），登录后切换到特权模式和全局配置模式管理交换机。

（六）VLAN 基本概念和原理

- (1)VLAN 的概念
  - 虚拟局域网是以局域网交换机为基础，通过交换机软件实现根据功能、部门、应用等因素将设备或用户组成虚拟工作组或逻辑网段的技术。
  - 特点是在组成逻辑网时无须考虑用户或设备在网络中的物理位置。VLAN 可以在一个交换机或者跨交换机实现。
- (2)VLAN 的实现原理
  - 1986 年 3 月，IEEE 802 委员会发布了 IEEE 802.1q VLAN 标准。
  - 1988 年，IEEE 批准了 802.3ac 标准，这个标准定义了虚拟局域网的以太网帧格式，在传统的以太网的帧格式中插入一个 4 字节的标识符，称为 VLAN 标记，用来指明发送该帧的工作站属于哪一个虚拟局域网，如图 1 所示。如果还使用传统的以太网帧格式，那么就无法划分虚拟局域网。
  - VLAN 标记字段的长度是 4 字节，插在以太网 MAC 帧的源地址字段和长度／类型字段之间。VLAN 标记的前两个字节和原来的长度／类型字段的作用一样，总是设置为 0x8100，称为 802.1q 标记类型。
  - 虚拟局域网是由一些局域网网段构成的与物理位置无关的逻辑组，而这些网段具有某些共同的需求。每一个 VLAN 的帧都有一个明确的标识符，指明发送这个帧的工作站是属于哪一个 VLAN。
  - 利用以太网交换机可以很方便地实现虚拟局域网（VLAN）。虚拟局域网其

实只是局域网给用户提供的一种服务，而并不是一种新型局域网。

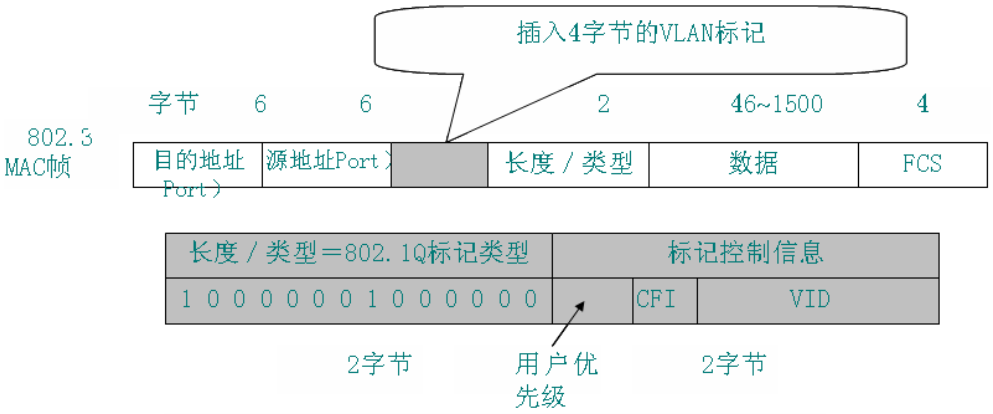


图1　虚拟局域网以太网帧格式

- (3)VLAN 的实现方式
  - 基于交换端口的 VLAN
  - 基于 MAC 地址的 VLAN
  - 基于路由协议的 VLAN
  - 基于策略的 VLAN
    - 按 MAC 地址划分；
    - 按 IP 地址划分；
    - 按以太网协议类型划分；
    - 按网络的应用划分
- （4）VLAN 的优越性

任何新技术要得到广泛支持和应用，肯定存在一些关键优势，VLAN 技术也一样，它的优势主要体现在以下几个方面：

（a）增加了网络连接的灵活性

借助 VLAN 技术，能将不同地点、不同网络、不同用户组合在一起，形成一个虚拟的网络环境 ，就像使用本地 LAN 一样方便、灵活、有效。VLAN 可以降低移动或变更工作站地理位置的管理费用，特别是一些业务情况有经常性变动的公司使用了 VLAN 后，这部分管理费用大大降低。

（b）控制网络上的广播

VLAN 可以提供建立防火墙的机制，防止交换网络的过量广播。使用 VLAN，可以将某个交换端口或用户赋于某一个特定的 VLAN 组，该 VLAN 组可以在一个交换网中或跨接多个交换机， 在一个 VLAN 中的广播不会送到 VLAN 之外。同样，相邻的端口不会收到其他 VLAN 产生的广 播。这样可以减少广播流量，释放带宽给用户应用，减少广播的产生。

（c）增加网络的安全性

因为一个 VLAN 就是一个单独的广播域，VLAN 之间相互隔离，这大大提高了网络的利用率，确保了网络的安全保密性。人们在 LAN 上经常传送一些保密的、关键性的数据。保密的数据应 提供访问控制等安全手段。一个有效和容易实现的方法是将网络分段成几个不同的广播组， 网络管理员限制了 VLAN 中用户的数量，禁止未经允许而访问 VLAN 中的应用。交换端口可以基 于应用类型和访问特权来进行分组，被限制的应用程序和资源一般置于安全性 VLAN 中

六、实验内容

1、单交换机 VLAN 实验示例

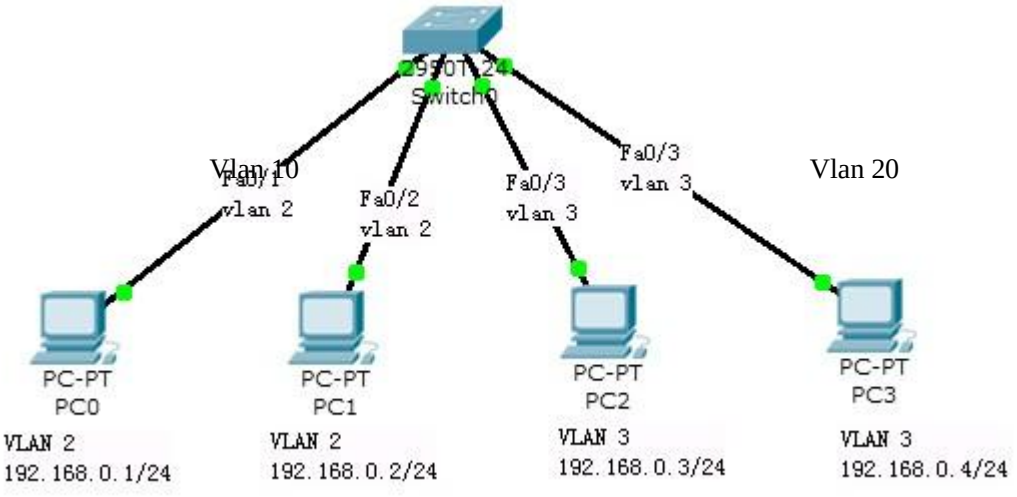


图 1 单交换机 VLAN 实验拓扑图

【实验步骤】

第一步 使用超级终端或 Tenlet 方式登录到交换机

使用改名命令将交换机名改成 SwitchA

第二步：建立 2 个 VLAN。

SwitchA(config)#vlan 2 #创建 VLAN 10

SwitchA(config-vlan)#exit #退出 VLAN 配置模式

SwitchA(config)#vlan 3 #创建 VLAN 20

SwitchA(config-vlan)#end #退出 VLAN 配置模式,返回到特权模式

SwitchA#show vlan #显示 VLAN 配置信息

#删除 VLAN 可以用命令 SwitchA(config)#no vlan 10

第三步：把端口 F0/1、F0/2 放入 VLAN 2 中

SwitchA(config)#interface fastethernet 0/1 #进入 fastethernet0/1 端口配置

SwitchA(config-if)#switch access vlan 2 #将 fastethernet0/1 端口加入到 VLAN 2

SwitchA(config-if)#exit //返回上级视图

SwitchA(config)#interface fastethernet 0/2 #进入 fastethernet0/2 端口配置

SwitchA(config-if)#switch access vlan 2 #将 fastethernet0/2 端口加入到 VLAN 2

第四步：把端口 F0/3、F0/4 放入 VLAN 3 中

SwitchA (config)#interface fastethernet 0/3 #进入 fastethernet0/3 端口配置

SwitchA (config-if)#switch access vlan 3 #将 fastethernet0/3 端口加入到 VLAN 3

SwitchA (config)#interface fastethernet 0/4 #进入 fastethernet0/4 端口配置

SwitchA (config-if)#switch access vlan 3 #将 fastethernet0/4 端口加入到 VLAN 3

SwitchA(config-if)#end # 退出到特权模式

第五步：显示 VLAN 配置

SwitchA#show vlan # 显示 VLAN 配置信息

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    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
                                                Gig1/1, Gig1/2
2    VLAN0002                         active    Fa0/1, Fa0/2
3    VLAN0003                         active    Fa0/3, Fa0/4
```

第六步：检测实验结果

通过命令 ping 测试 VLAN 配置正确性。相同 VLAN 的两台计算机之间能 ping 通，若两台计算机之间不能 ping 通，则说明 PC 是属于不同的 VLAN，即不同的 VLAN 之间不能直接通信。

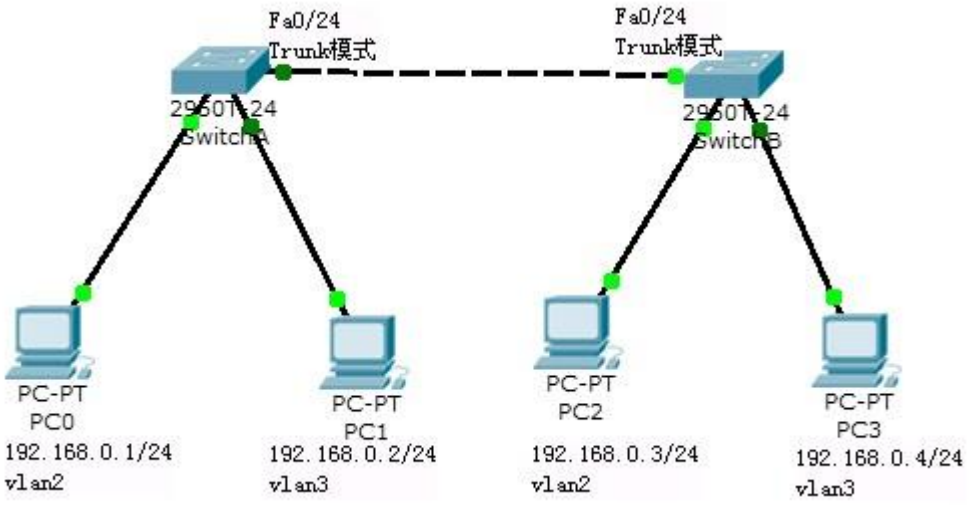
实验注意事项：

1) 默认情况下，交换机的所有端口都属于 VLAN1。该 VLAN 不能被删除。建议在划分 VLAN 前，将 PC 机接入交换机的任意端口，并测试其连通性。
2) 交换机的所有端口在默认情况下都属于 access 模式，可以直接将端口加入到某一 VLAN。具有 access 模式的端口只能属于一个 VLAN.。可以通过 switch mode access/trunk 命令更改端口的模式。
3) 可以通过 switch(config)#no vlan 2 删除 VLAN 10。删除 VLAN 前先将 VLAN 中的端口移出。命令为：

   switch(config)#interface fastethernet 0/5

   Switch(config-if)# no switchport
4) 实验报告中注意描述 VLAN 的配置过程，记录 VLAN 间连通性的测试结果，并分析总结。要说明主机的配置信息。它们是否属于同一个网段。

2、跨交换机 VLAN 实验示例



实验拓扑图

【实验步骤】

第一步 登录到第一个交换机

Switch(config)#hostname SwitchA　#将交换机名字改为 SwitchA

第二步：在交换机 A（SwitchA）上建立 2 个 VLAN 2 ， VLAN 3。

SwitchA(config)#vlan 2　　#创建 VLAN 2
SwitchA(config-vlan)#exit　　#返回到全局模式
SwitchA(config)#vlan 3　　#创建 VLAN 3
SwitchA(config-vlan)#end　　!返回到特权模式
SwitchA#show vlan　　!显示 VLAN 的配置

第三步：将端口 F0/1、F0/2 分别放入 VLAN2 和 VLAN3。

SwitchA(config)#interface fastethernet 0/1　#进入接口 F0/1 配置模式
SwitchA(config-if)#switchport access vlan 2　　#将 F0/1 分配给 VLAN 2
SwitchA(config-if)#exit
SwitchA(config)#interface fastethernet 0/2 #进入接口 F0/2 配置模式
SwitchA(config-if)#switchport access vlan 3　　#将 F0/2 分配给 VLAN 3
SwitchA(config-if)#exit

第四步：把交换机 SwitchA 与 SwitchB 连接的 0/24 接口做成 trunk 模式。(Tag VLAN)

SwitchA(config)#interface fastethernet 0/24 #进入接口 0/24 配置
SwitchA(config-if)#switchport mode trunk　　#配置 Trunk 模式
#默认情况下，接口均为 access 模式，即接入模式，将接口设置为接入模式可以用命令 switchport mode access。
SwitchA(config-if)#end　# 退出到特权模式

第五步：显示 VLAN 配置和 trunk 配置。

SwitchA #show vlan　　# 显示 VLAN 配置信息
SwitchA #show interface fastethernet 0/24 switchport
或
SwitchA #show interface fastethernet 0/24 trunk

第六步：登录到交换机 B

Switch(config)#hostname SwitchB #将交换机改名为 SwitchB。

第七步：在交换机 Switch B 上建立 VLAN 2、VLAN 3

SwitchB(config)#vlan 2　　#创建 VLAN 2
SwitchB(config-vlan)#exit　　#返回到特权模式
SwitchB (config)#vlan 3　　#创建 VLAN 3
SwitchB (config-vlan)#end　　#返回到特权模式
SwitchB#show vlan　　#显示 VLAN 的配置

第八步：将端口 F0/1、F0/2 分别放入 VLAN2 和 VLAN3。

SwitchB (config)#interface fastethernet 0/1　#进入接口 F0/1 配置模式
SwitchB (config-if)#switchport access vlan 2　　#将 F0/1 分配给 VLAN 2
SwitchB (config-if)#exit
SwitchB (config)#interface fastethernet 0/2 #进入接口 F0/2 配置模式

SwitchB (config-if)#switchport access vlan 3　　#将 F0/2 分配给 VLAN 3
SwitchB (config-if)#exit

第九步：把交换机 SwitchB 与 SwitchA 连接的 0/24 接口做成 trunk 模式。

SwitchB(config)#interface fastethernet 0/24
SwitchB(config-if)#switchport mode trunk　　#配置 Trunk
SwitchB(config-if)#end　# 退出到特权模式

第十步：显示 VLAN 配置和 trunk 配置

SwitchB #show vlan　　# 显示 VLAN 配置信息
SwitchB #show interface fastethernet 0/24 switchport
或 SwitchB #show interface fastethernet 0/24 trunk

第十一步：检测与实验结果分析

通过 ping 测试配置结果。PC1 和 PC3、PC2 和 PC4 属于同一个 VLAN，可以直接通信。PC1 和 PC2、PC3 和 PC4 属于不同 VLAN 不能直接通信。

注意事项：

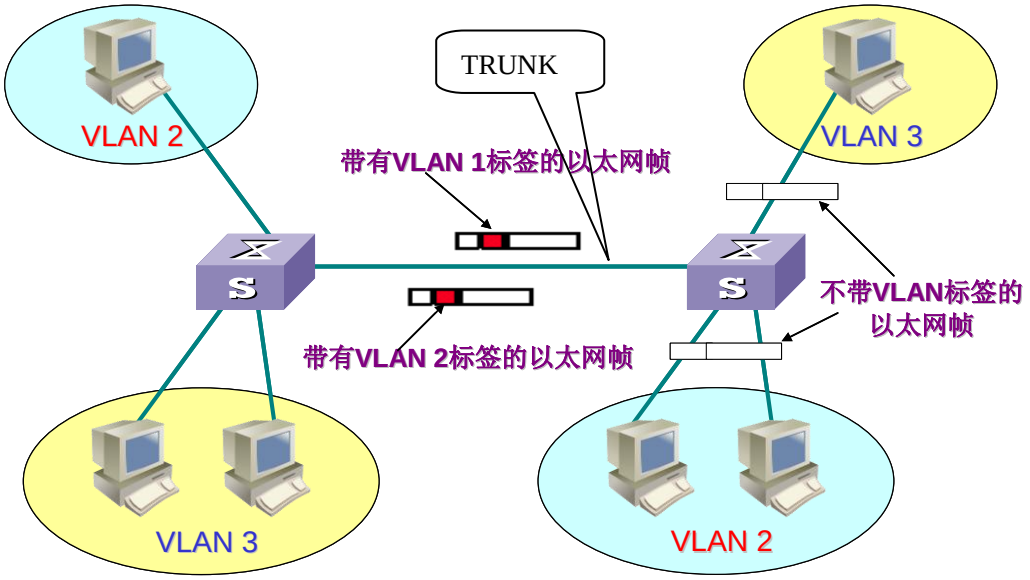
1、 在建立设置 trunk 模式前、后，分别测试跨交换机的相同 VLAN 通信。
2、 Trunk 端口在默认模式下支持所有 VLAN 的传输。即 trunk 模式的端口可以属于多个 VLAN。
3、 实验报告注意描述配置过程，记录测试结果并分析总结。

附 1：交换机实验命令小结

表 1-1 交换机实验命令小结

命令	作用
enable	从用户模式进入特权模式
configure terminal	进入配置模式
interface f0/1	进入以太网接口 f0/1 配置模式
ip address 172.16.0.1 255.255.255.0	配置接口的 IP 地址
no shutdown	打开接口
line vty 0 4	进入虚拟终端 vty 0~vty 4
password CISCO	配置密码
login	用户要进入交换机，需要先进行登录
exit	退回到上一级模式
enable password CISCO	配置进入特权模式的密码，密码不加密
end	直接回到特权模式
show int f0/1	显示 f0/1 接口信息
hostname SwitchA	配置交换机的名字
switchport mode access	将端口设置为 access 模式
switchport mode trunk	将端口设置为 trunk 模式
Show vlan	查看 vlan 配置情况
Show running-config	查看交换机当前运行的配置情况

附 2：带有 VLAN 标签的数据帧在通信中的变化图



实验四　交换机端口链路聚合实验

一、实验目的

1、掌握基于交换机端口的配置命令。

2、理解端口聚合基本原理

3、掌握端口链路聚合配置方法。

二、实验属性

验证性试验。

三、实验仪器设备及器材

Cisco 2950 交换机、具备 Windows 操作系统的 PC 机、直通双绞线、交叉双绞线、Cisco 配置线缆。

四、实验要求

1、预习报告中需解决以下问题：熟练掌握 Cisco2950 交换机 VLAN 相关配置命令以及各命令的作用。

2、试验中正确使用仪器设备，独立操作。

3、试验后按规定要求写出实验报告。

五、实验预备知识

端口聚合（又称为链路聚合)，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，可以实现负载分担，并提供冗余链路。

技术原理

- 端口聚合使用的是 EtherChannel 特性，在交换机到交换机之间提供冗余的高速的连接方式。将两个设备之间多条 FastEthernet 或 GigabitEthernet 物理链路捆在一起组成一条设备间逻辑链路，从而增强带宽，提供冗余。
- 两台交换机到计算机的速率都是 100M，SW1 和 SW2 之间虽有两条 100M 的物理通道相连，可由于生成树的原因，只有 100M 可用，交换机之间的链路很容易形成瓶颈，使用端口聚合技术，把两个 100M 链路聚合成一个 200M 的逻辑链路，当一条链路出现故障，另一条链路会继续工作。
- 一台 S2000 系列以太网交换机只能有 1 个汇聚组，1 个汇聚组最多可以有 4 个端口。**组内的端口号必须连续，但对起始端口无特殊要求。**
- 在一个端口汇聚组中，端口号最小的作为主端口，其他的作为成员端口。同一个汇聚组中成员端口的链路类型与主端口的链路类型保持一致，即如果主端口为 Trunk 端口，则成员端口也为 Trunk 端口；如主端口的链路类型改为 Access 端口，则成员端口的链路类型也变为 Access 端口。
- 所有参加聚合的端口都必须工作在全双工模式下，且工作速率相同才能进行聚合。并且聚合功能需要在链路两端同时配置方能生效。
- 端口聚合主要应用的场合：
    - **交换机与交换机之间的连接**：汇聚层交换机到核心层交换机或核心层交换机之间。
    - **交换机与服务器之间的连接**：集群服务器采用多网卡与交换机连接提供集中访问。
    - **交换机与路由器之间的连接**：交换机和路由器采用端口聚合解决广域网和局域网连接瓶颈。
    - **服务器和路由器之间的连接**：集群服务器采用多网卡与路由器连接提供集中

访问

- 视图：全局配置模式下
- 命令：

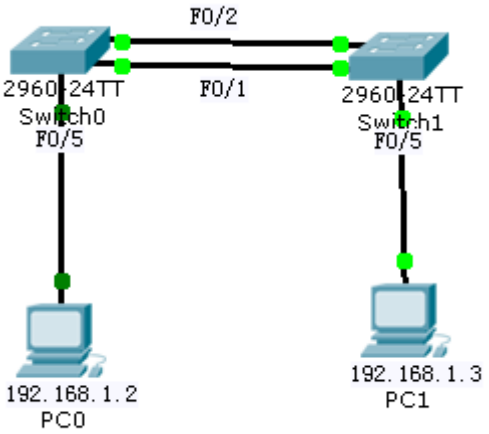
  interface range interface_name1 **to** interface_name2

  Switchport mode trunk

  channel-group 1 mode on 加入链路组 1 并开启
- 参数：
  - ➔ interface_name1：聚合起始端口
  - ➔ interface_name2：聚合结束端口。
  - ➔ trunk 表示端口可以转发所有 Vlan 包
  - ➔ 将 2 个或多个物理端口组合在一起成为一条逻辑的路径 ，即链路 channel-group，同时也形成了一个逻辑端口 port-channel（一个整体）
- switchport mode access 是直接接主机的，所属 VLAN 中的接口，都是 access
- switchport mode trunk trunk mode 的接口可以同时传输多个 VLAN 信息的。
- trunk mode 常用在两个 SWITCH and ROUTER， switch and switch
- 特权模式下
- Switch#show etherchannel summary：显示相关汇聚端口组的信息；

六、实验内容

按下图连接和配置设备：Switch_2960 2 台；PC 4 台；直连线



Switch0:具体操作

Switch>

Switch#config t

Switch(config)#interface range f0/1-2

Switch(config-if-range)#Switchport mode trunk //设置端口模式为 trunk

Switch(config-if-range)#channel-group 1 mode on //加入链路组 1 并开启

Switch(config-if-range)#exit

Switch(config)#port-channel load-balance dst-ip //按照目标主机 IP 地址数据分发来实现负载平衡

Switch(config)#exit

Switch#show etherchannel summary

Switch1:具体操作

Switch>

Switch#config t

Switch(config)#interface range f0/1-2

Switch(config-if-range)#Switchport mode trunk //设置端口模式为 trunk

Switch(config-if-range)#channel-group 1 mode on //加入链路组 1 并开启

Switch(config-if-range)#exit

Switch(config)#port-channel load-balance dst-ip //按照目标主机 IP 地址数据分发来实现以太网通道组负载平衡

Switch(config)#exit

Switch#show etherchannel summary //显示以太网通道组的情况

PC0 设置

192.168.1.2

255.255.255.0

PC1 设置

192.168.1.3

255.255.255.0

PC0 ping PC1 Reply

PC1 ping PC0 Reply

实验五　路由器基本配置

一、实验目的

1．了解路由器的基本功能、工作状态判断等基础知识。

2．了解路由器的基本配置方式。

3．熟悉路由器的命令行配置。

二、实验属性

验证性试验。

三、实验仪器设备及器材

路由器、配置网卡的计算机、网线、Console 控制线缆。

四、实验要求

1、预习报告中需解决以下问题：熟练掌握 Cisco2621 路由器基本配置命令以及各命令的作用。

2、试验中正确使用仪器设备，独立操作。

3、试验后按规定要求写出实验报告。

五、实验内容

1．熟悉路由器各部分的功能，识别路由器的各种接口。

2．用超级终端通过 Console 口完成路由器的基本配置。

六、路由器相关接口配置命令格式

（1）进入指定的接口配置模式

配置每个接口，首先必须进入这个接口的配置模式模式,首先进入全局配置模式，然后输入进入指定接口配置模式，命令格式如下 ：

命令	作用
Router(config)#interface interface-type interface-number	创建一个接口，并进入指定接口配置模式

例如：进入快速以太网口的 0 号模块上的第 0 个端口，步骤是：

Router#config terminal

Router(config)#interface FastEthernet 0/0

（2）配置IP地址

除了 NULL 接口，每个接口都有其 IP 地址，IP 地址的配置是使用接口必须考虑的，命令如下：

命令	作用
Router(config-if)#ip address ip-address ip-mask	配置该接口的网络地址
Router(config-if)#no ip address	删除该接口的网络地址

（3）配置最大传输单元MTU

最大传输单元 MTU 是 IP 报文的特性，它的取值范围是 64－65535 字节，设定命令如下所示：

命令	作用
Router(config-if)#mtu bytes	配置MTU大小
Router(config-if)#no mtu	恢复MTU的缺省值

（4）关闭和重启接口

在需要的时候，接口必须被关闭，比如在接口上更换电缆，然后再重新启动接口。用 shutdown 命令来关闭端口，用 no shutdown 命令来重新启动该接口，如：

Router(config)#interface fa0/0　#进入接口配置模式

Router(config-if)#shutdown　　#关闭接口

Router(config-if)# no　shutdown　#重启接口

七、实验步骤

1、通过Console口搭建本地配置环境

在路由器第一次使用的时候，必须采用通过 Console 口方式对路由器进行配置，具体的操作步骤如下：

第一步：如下图所示，将一字符终端或者计算机的串口通过标准的 RS232 电缆和路由器的 Console 口（也叫配置口）连接。

第二步：配置终端的通讯设置参数，如果采用计算机，则需要运行终端仿真程序，如 Windows 操作系统提供的 Hyperterm(超级终端)等，以下以超级终端为例，说明具体的操作过程。运行超级终端软件，建立新连接，选择和路由器的 Console 连接的串口，设置通讯参数：9600 波特率、8 位数据位、1 位停止位、无校验、无流控，并且选择终端仿真类型位 VT100，与实验三交换机基本

配置实验一样操作步骤一样打开 Windows 的超级终端的设置界面。

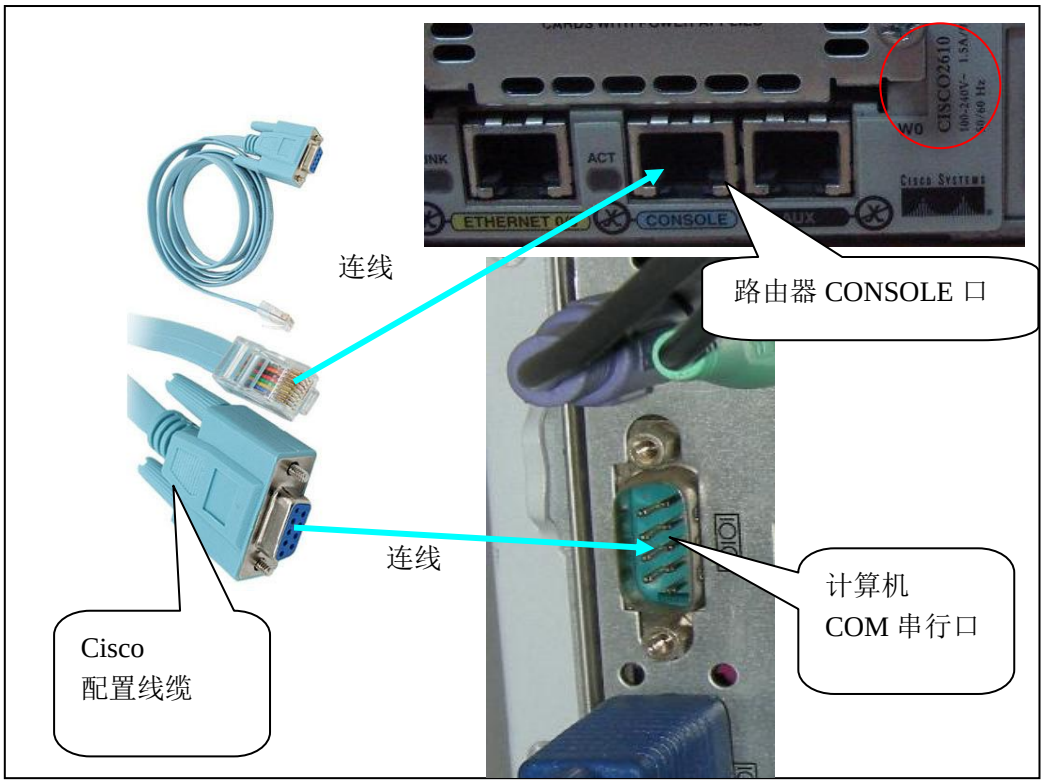


图 1：通过 Console 口搭建本地配置环境

第三步：路由器上电，启动路由器，这时将在终端屏幕，或者计算机的超级终端窗口内显示自检信息，自检结束后提示用户键入回车，直到出现命令行提示符“Router>”。

第四步：这时便可以在终端上或者超级终端中对路由器进行配置，查看路由器的运行状态，如果需要帮助，可以随时键入“？”,路由器便可以随时提供详细的在线帮助了。

2、在管理计算机上使用Telnet配置管理路由器

如果用户对路由器已经配置好各接口的 IP 地址，同时可以正常的进行网络通讯了，则可以通过局域网或者广域网，使用 Telnet 客户端登陆到路由器上，对路由器进行本地或者远程的配置。下面详细介绍具体的配置步骤。

□ 说明：

通过Telnet方式对路由器进行配置，首要条件是路由器接口配置了IP地址等参数，远程管理路由器的计算机IP地址必须和路由器接口IP在同一个地址段，路由器和计算机才能连通，否则不能通过Telnet方式对路由器进行配置，另外必须在line vty 中配置密码，才可以登陆，

同时在全局配置层中必须配置控制密码，否则无法进入特权层对路由器进行配置。

第一步：如果建立本地 Telnet 配置环境，则只需要将计算机上的网卡接口通过局域网与路由器的以太网口连接；如果需要建立远程 Telnet 配置环境，则需要将计算机和路由器的广域网口连接。

第二步：在 Windows 的 DOS 命令提示符下，直接输入 Telnet a.b.c.d，这里的 a.b.c.d 为路由器的以太口的 IP 地址（如果在远程 Telnet 配置模式下，为路由器的广域网口的 IP 地址），与路由器建立连接，提示输入登陆密码，如果没有配置密码，会出现“Password required, but none set”的提示，正确输入密码后，出现“Router>”。

第三步：这时便可以利用计算机的 Telnet 客户端对路由器进行配置，查看路由器的运行状态，如果需要帮助，可以随时键入“？”,路由器便可以随时提供详细的在线帮助了

说明：

通过Telnet方式对路由器配置过程中，不要修改路由器的接口的IP地址，否则Telnet连接会断开连接。如果确实有必要修改，可以在修改接口IP地址后，重新用新的IP地址进行Telnet登陆，利用Telnet方式对路由器进行配置，一般缺省情况下，可以同时运行5个Telnet连接。

八、使用Telnet方式对路由器进行配置实验示例

（1）实验拓扑图

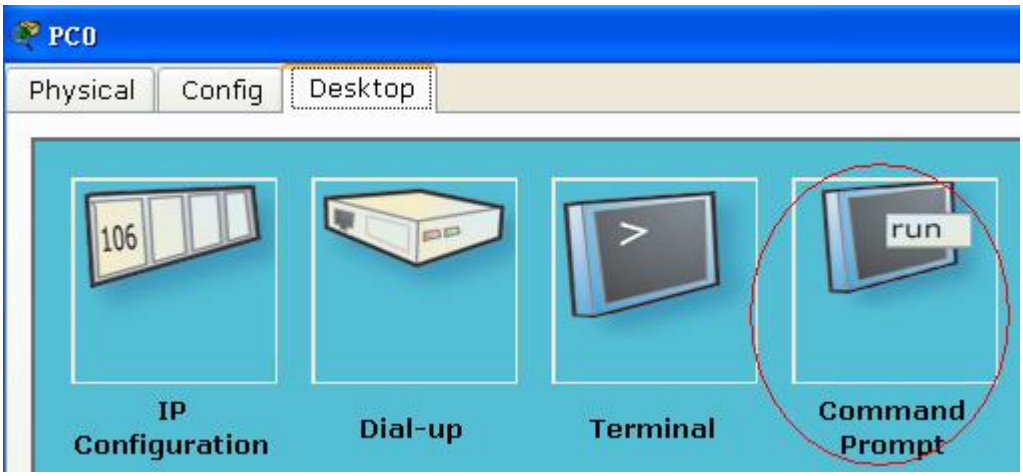
（2）计算机配置

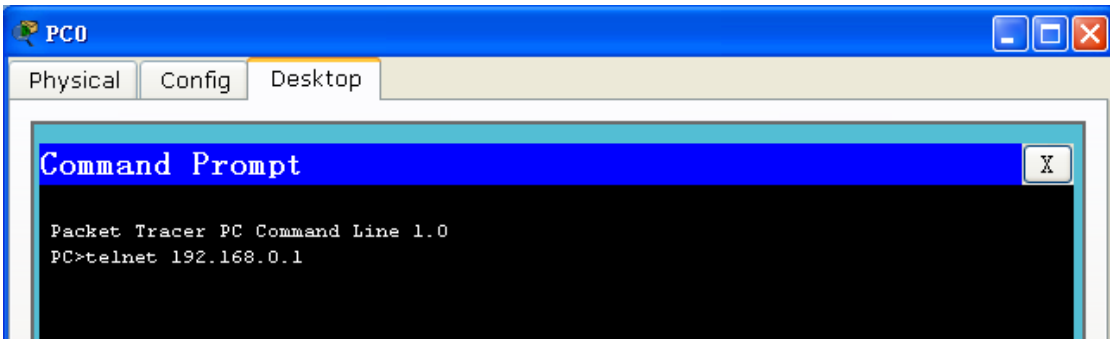
计算机配置 IP 地址为 192.168.0.2/24

（3）路由器配置命令

```
Router>enable                    #进入特权模式
Router#configure terminal     #进入全局配置模式
Enter configuration commands, one per line.   End with CNTL/Z.
Router(config)#enable password 111111          #设置路由器进入特权模式密码
Router(config)#interface fastEthernet 0/0       #进入路由器接口 f0/0 配置模式
Router(config-if)#ip address 192.168.0.1 255.255.255.0 #配置路由器接口地址
Router(config-if)#no shut                                  #开启路由器接口
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#exit
Router(config)#line vty 0 4                  #设置虚拟终端用户
Router(config-line)#login                    #密码在 login 时有效
Router(config-line)#password 222222                #设置 Telnet 密码
```

（4）在模拟器的计算机命令符模式下进入登录交换机的命令





输入 telent 的密码（222222），登录后切换到特权模式和全局配置模式管理交换机。输入 telnet 的密码（222222）和特权密码（111111）后切换到特权模式和全局配置模式管理路由器。

实验六　配置静态路由

一、实验目的

1、理解静态路由的概念、原理。

2、掌握静态路由策略配置方法。

3、掌握 Cisco 路由器的静态路由配置命令。

二、实验属性

验证性试验。

三、实验仪器设备及器材

Cisco 2621、Cisco 2811 路由器，具备 Windows 操作系统的 PC 机，直通双绞线，交叉双绞线，串行线缆，Cisco 配置线缆。

四、实验要求

1、预习报告中需解决以下问题：熟练掌握 Cisco 路由器静态路由相关配置命令以及各命令的作用。

2、试验中正确使用仪器设备，独立操作。

3、试验后按规定要求写出实验报告。

五、实验原理

- 路由器属于网络层设备，能够根据 IP 包头的信息，选择一条最佳路径，将数据包转发出去。实现不同网段的主机之间的互相访问。路由器是根据路由表进行选路和转发的。而路由表里就是由一条条路由信息组成。
- 生成路由表主要有两种方法：手工配置和动态配置，即静态路由协议配置和动态路由协议配置。
- 静态路由是指有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。
- 缺省路由可以看做是静态路由的一种特殊情况。当数据在查找路由表时，没有找到和目标相匹配的路由表项时，为数据指定路由。

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。由于静态路由不能对网络的改变作出反映，一般用于网络规模不大、拓扑结构固定的网络中。静态路由的优点是简单、高效、可靠。

通过配置静态路由，用户可以人为地指定对某一网络访问时所要经过的路径，在网络结构比较简单，且一般到达某一网络所经过的路径唯一的情况下采用静态路由是一种比较好的网络解决方案。

当 IP 子网中的一台主机发送 IP 分组给同一 IP 子网的另一台主机时，它将直接把 IP 分组送到网络上，对方就能收到。而要送给不同 IP 子网上的主机时，它要选择一个能到达目的子网上的路由器，把 IP 分组送给该路由器，由路由器负责把 IP 分组送到目的地。

如果没有找到这样的路由器，主机就把 IP 分组送给一个称为“**缺省网关**（default gateway）”的路由器上。“缺省网关”是每台主机上的一个配置参数，它是接在同一个网络上的某个路由器端口的 IP 地址。

路由器转发 IP 分组时，只根据 IP 分组目的 IP 地址的网络号部分，选择合适的端口，把 IP 分组送出去。同主机一样，路由器也要判定端口所接的是否是目的子网，如果是，就直接把分组通过端口送到网络上，否则，也要选择下一个路由器来传送分组。路由器也有它的缺省网关，用来传送不知道往哪儿送的 IP 分组。这样，通过路由器把知道如何传送的 IP 分组正确转发出去，不知道的 IP 分组送给“缺省网关”路由器，这样一级级地传送，IP 分

组最终将送到目的地，送不到目的地的 IP 分组则被网络丢弃了。

六、静态路由配置命令格式

（1）为路由器设置静态路由的语法如下：

Router(config)# ip route *network* [*mask*] {*address* | *interface*}[*distance*]

其中：

network：所要到达的目的网络号或子网号

mask：目的网络的子网掩码

address：到达目的网络所经由的下一跳路由器接口的 IP 地址

【下一跳 IP 地址：相邻路由器近端接口 IP 地址】

Interface：接口名称（用于到达目标网络的本机网络接口）

Distance：主该路由指定的管理距离（可选）

（2）对路由器进行默认路由的设置，语法如下：

Router(config)# ip route *0.0.0.0 0.0.0.0* {*address* | *interface*}[*distance*]

其中，0.0.0.0 0.0.0.0 代表任意地址和任意掩码；另外三个参数与配置静态路由中使用的含义相同。例如，在路由器 Router 上设置一条默认路由的语句如下：

Router(config)# ip route 0.0.0.0 0.0.0.0 222.1.1.1

（3）查看路由表的命令如下：

Router# show ip route

（4）查看路由表端口的详细信息命令如下：

Router# show ip interface

如显示接口 f0/0 信息命令：show ip interface f0/0

（5）给路由器的某一个端口设置 IP 地址的语法如下：

Router(config)# ip address {IP 地址} {子网掩码}

七、配置实例

1、简单静态路由配置实验示例

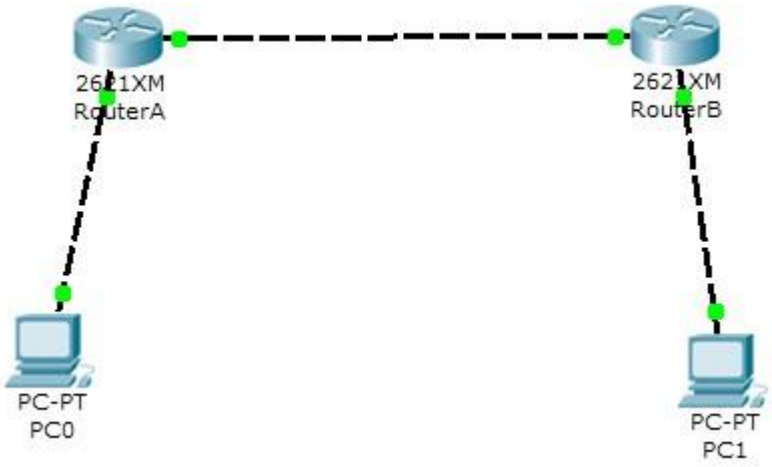


图 1 简单静态路由配置实验拓扑图

（1）路由器 A 配置命令

Router>enable

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RouterA(config)#hostname RouterA #给路由器命名
RouterA(config)#interface FastEthernet0/0 #进入路由器接口配置模式
RouterA(config-if)#ip address 172.16.30.1 255.255.255.252 #配置路由器接口 IP 和掩码
RouterA(config-if)#no shutdown #开启路由器接口

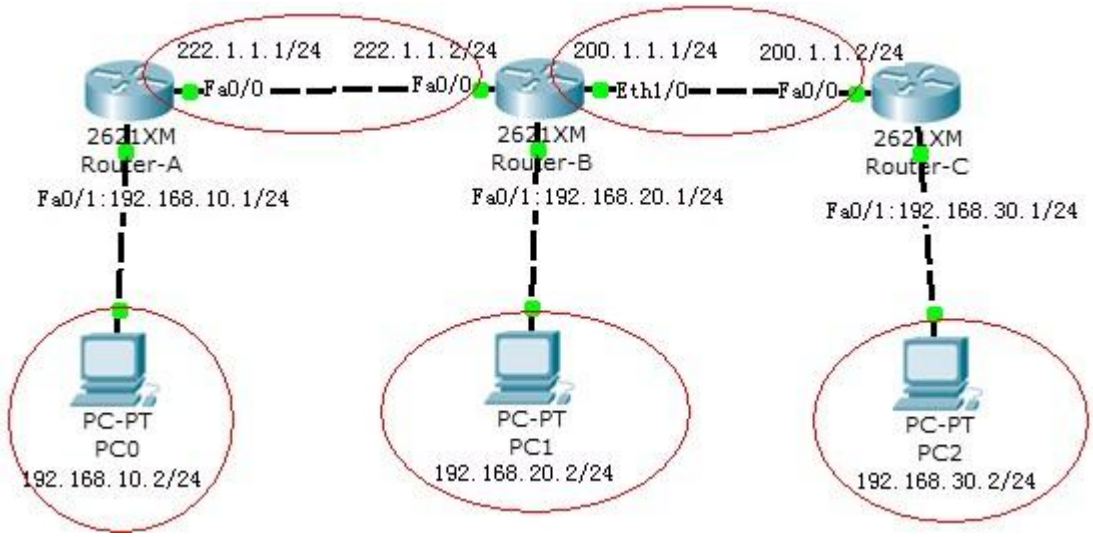
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
RouterA(config-if)#exit
RouterA(config)#interface FastEthernet0/1
RouterA(config-if)#ip address 192.168.0.1 255.255.255.0 #配置路由器接口 IP 和掩码
RouterA(config-if)#no shutdown #开启路由器接口
RouterA(config-if)#exit
RouterA(config)#ip route 192.168.100.0 255.255.255.0 172.16.30.2 #设置静态路由

（2）路由器 B 配置命令
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router (config)#hostname RouterB
RouterB(config)#interface FastEthernet0/0
RouterB(config-if)#ip address 172.16.30.2 255.255.255.252
RouterB(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
RouterB(config-if)#
RouterB(config-if)#exit
RouterB(config)#interface FastEthernet0/1
RouterB(config-if)#ip address 192.168.100.1 255.255.255.0
RouterB(config-if)#no shutdown
RouterB(config-if)#exit
RouterB(config)#ip route 192.168.0.0 255.255.255.0 172.16.30.1 #设置静态路由

（3）计算机配置 IP 地址
PC0 配置地址 192.168.0.2/24，默认网关 192.168.0.1（即相连的路由器接口 IP）
PC1 配置地址 192.168.100.2/24，默认网关 192.168.100.1 （同上）

（4）在 PC0 上 pingPC1，验证实验正确性
Ping 192.168.100.2

2、复杂静态路由配置实验示例



实验拓扑图

【实验命令】

路由器 A:

RouterA>enable
RouterA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RouterA(config)#interface FastEthernet0/0
RouterA(config-if)#ip address 222.1.1.1 255.255.255.0
RouterA(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
RouterA(config-if)#
RouterA(config-if)#exit
RouterA(config)#interface FastEthernet0/1
RouterA(config-if)#ip address 192.168.10.1 255.255.255.0
RouterA(config-if)#no shutdown
RouterA(config-if)#exit
RouterA(config)#ip route 192.168.20.0 255.255.255.0 222.1.1.2 **#设置静态路由**
RouterA(config)#ip route 200.1.1.0 255.255.255.0 222.1.1.2 **#设置静态路由**
RouterA(config)#ip route 192.168.30.0 255.255.255.0 222.1.1.2 **#设置静态路由**

使用命令查看路由器 A 路由表：

RouterA(config)#exit
RouterA#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 192.168.10.0/24 is directly connected, FastEthernet0/1
S 192.168.20.0/24 [1/0] via 222.1.1.2 #静态路由
S 192.168.30.0/24 [1/0] via 222.1.1.2 #静态路由
S 200.1.1.0/24 [1/0] via 222.1.1.2 #静态路由
C 222.1.1.0/24 is directly connected, FastEthernet0/0

路由器 B:

RouterB>enable
RouterB#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RouterB(config)#interface FastEthernet0/0
RouterB(config-if)#ip address 222.1.1.2 255.255.255.0
RouterB(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
RouterB(config-if)#
RouterB(config-if)#exit
RouterB(config)#interface FastEthernet0/1
RouterB(config-if)#ip address 192.168.20.1 255.255.255.0
RouterB(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
RouterB(config-if)#
RouterB(config-if)#exit
RouterB(config)#interface Ethernet1/0
RouterB(config-if)#ip address 200.1.1.1 255.255.255.0
RouterB(config-if)#no shutdown
RouterB(config-if)#exit
RouterB(config)#ip route 192.168.10.0 255.255.255.0 222.1.1.1 **#设置静态路由**
RouterB(config)#ip route 192.168.30.0 255.255.255.0 200.1.1.2

路由器 C:

RouterC>enable
RouterC#configure terminal
Enter configuration commands, one per line. End with CNTL/Z. **#设置静态路由**
RouterC(config)#interface FastEthernet0/0
RouterC(config-if)#ip address 200.1.1.2 255.255.255.0
RouterC(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
RouterC(config-if)#
RouterC(config-if)#exit
RouterC(config)#interface FastEthernet0/1
RouterC(config-if)#ip address 192.168.30.1 255.255.255.0
RouterC(config-if)#no shutdown
RouterC(config)#ip route 0.0.0.0 0.0.0.0 200.1.1.1　#设置缺省路由

特别提示：路由器 C 使用上面一条缺省路由来代替下面三条静态路由
RouterC(config)#ip route 192.168.10.0　255.255.255.0 200.1.1.1
RouterC(config)#ip route 192.168.20.0　255.255.255.0 200.1.1.1
RouterC(config)#ip route 222.1.1.0　255.255.255.0 200.1.1.1

使用 ping 命令测试三台 PC 之间的联通性。

实验七　动态路由 RIP 配置

一、实验目的

掌握在路由器上配置 RIP 的方法，本实验属于验证性实验。

二、实验设备

R2621 路由器（两台）、V35 线缆、双绞线若干。

三、实验项目

1、查看 IP 路由表

2、创建 RIP 路由进程

3、定义 RIP 版本

4、关闭路由自动汇聚

5、RIP 认证配置

6、RIP 时钟调整

四、实验内容

1、查看IP路由表

路由器的最基本功能就是路由，对一个具体的路由器来说，路由就是将从一个接口接收到的数据包，转发到另外一个接口的过程，该过程类似交换机的交换功能，只不过在链路层我们称之为交换，而在IP层称之为路由；而对于一个网络来说，路由就是将包从一个端点（主机）传输到另外一个端点（主机）的过程。

路由的完成离不开两个最基本步骤：第一个步骤为选径，路由器根据到达数据包的目标地址和路由表的内容，进行路径选择；第二个步骤为包转发，根据选择的路径，将包从某个接口转发出去。

路由表是路由器进行路径抉择的基础，路由表的内容（路由表项，通常也称为路由）来源有两个：静态配置和路由协议动态学习。路由表内容如下：

-

router#show ip route

Codes: C - connected, S - static, R - RIP, D - EIGRP,

EX - EIGRP external, O- OSPF, IA - OSPF inter area

E1 - OSPF external type 1, E2 - OSPF external type 2,

* - candidate default

Gateway of last resort is 10.5.5.5 to network 0.0.0.0

C 172.16.11.0 is directly connected, serial1/2

O E2 172.22.0.0/16 [110/20] via 10.3.3.3, 01:03:01, Serial1/2

S* 0.0.0.0/0 [1/0] via 10.5

2、创建RIP路由进程

路由器要运行 RIP 路由协议，首先需要创建 RIP 路由进程，并定义与 RIP 路由进程关联的网络。

要创建 RIP 路由进程，在全局配置模式中执行以下命令：

步骤	命令	作用
第一步	Router(config)#**router rip**	创建RIP路由进程
第二步	Router(config-router)#**network** *network-number*	定义关联网络

说明：

Network命令定义的关联网络有两层意思：1）RIP只对外通告关联网络的路由信息；2）RIP只向关联网络所属接口通告路由信息。

3、定义RIP版本

RGNOS 软件支持 RIP 版本 1 和版本 2，RIPv2 可以支持认证、密钥管理、路由汇聚、CIDR 和 VLSMs。

缺省情况下，RGNOS 可以接收 RIPv1 和 RIPv2 的数据包，但是只发送 RIPv1 的数据包。你可以通过配置，只接收和发送 RIPv1 的数据包，也可以只接收和发送 RIPv2 的数据包。

要配置软件只接收和发送指定版本的数据包，在路由进程配置模式中执行以下命令：

命令	作用
Router(config-router)#**version** {1 | 2}	定义RIP版本

以上命令使软件缺省情况下只接收和发送指定版本的数据包，如果需要可以更改每个接口的缺省行为。

4、关闭路由自动汇聚

RIP 路由自动汇聚，就是当子网路由穿越有类网络边界时，将自动汇聚成有类网络路由。**RIPv2** 缺省情况下将进行路由自动汇聚，**RIPv1** 不支持该功能。**RIPv2** 路由自动汇聚的功能，提高了网络的伸缩性和有效性。如果有汇聚路由存在，在路由表中将看不到包含在汇聚路由内的子路由，这样可以大大缩小路由表的规模。

通告汇聚路由会比通告单独的每条路由将更有效率，主要有以下因素：

★ 当查找**RIP**数据库时，汇聚路由会得到优先处理；

★ 当查找**RIP**数据库时，任何子路由将被忽略，较少了处理时间。

有时可能希望学到具体的子网路由，而不愿意只看到汇聚后的网络路由，这时需要关闭路由自动汇总功能。

要配置路由自动汇聚，在 **RIP** 路由进程模式中执行以下命令：

命令	作用
Router(config-router)#**no auto-summary**	关闭路由自动汇总
Router(config-router)#**auto-summary**	打开路由自动汇总

5、 RIP认证配置

RIPv1不支持认证，如果路由器配置RIPv2路由协议，可以在相应的接口配置认证。

密钥串定义了该接口可使用的密钥集合，如果密钥串没有配置，即使接口应用了密钥串，也不会有认证行为发生。

RGNOS支持两种RIP认证方式：明文认证和MD5认证。缺省的认证方式为明文认证。

要配置RIP认证，在接口配置模式中执行以下命令：

步骤	命令	作用
第一步	Router(config-if)#**ip rip authentication key-chain** *key-chain-name*	应用密钥串，启用RIP认证
第二步	Router(config-if)#**ip rip authentication mode** {**text** | **md5**}	配置接口RIP认证模式：明文或MD5

6、RIP时钟调整

RIP提供了时钟调整的功能，你可以根据网络的具体情况进行时钟调整，使RIP路由协议能够运行的更好。可以对以下时钟进行调整：

路由更新时间：以秒计，定义了路由器发送路由更新报文的周期；

路由无效时间：以秒计，定义了路由表中路由因没有更新而变为无效的时间；

路由清除时间：以秒计，该时间过后，该路由将被清除出路由表；

通过调整以上时钟，可能会加快路由协议的收敛时间以及故障恢复时间。要调整RIP时钟，在RIP路由进程配置模式中执行以下命令：

命令	作用
Router(config-router)#**timers basci** *update invalid flush*	调整RIP时钟

缺省情况下，更新时间为 30 秒，无效时间为 180 秒，清除时间为 240 秒。

RIP(Routing Information Protocol)是一种内部网关协议，它适应于小型网络。它是距离矢量协议中最简单的一种。运行 RIP 协议的设备使用 UDP 报文去交换路由信息。

使用 RIP 时，交换机每 30 秒(缺省值)发送路由信息的更新报文(即为“通告”)。如果交换机 A 在 180 秒(缺省值)或用户设定的时间内没有收到交换机 B 的更新报文，则该交换机 A 会将由交换机 B 提供的路由置为不可用。如果在 120 秒(缺省值)或用户设定的时间后仍然没有更新报文，则该交换机 A 会删除所有由交换机 B 提供的路由。

五、实验命令列表

RIP 使用跳数(metric)来评估不同的路由。跳数一般是表示在路由中所经过的路由器的数量。在发送更新报文时将访问本地网络的花费(即默认跳数)作为本地直连路由得跳数，缺省为 1；跳数值为 16 的路由表示目的地址不可达。由于 RIP 的有效跳数被限制在 0～15 之间，这使得 RIP 协议不适用于大型的网络。

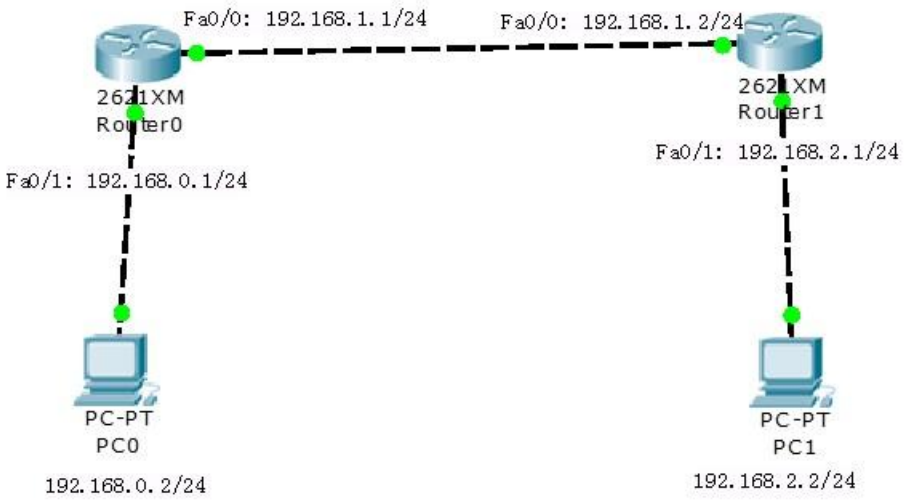
在特权模式下，用户可以按照下表启用 RIP 并进行配置。

命令		含义
步骤 **1**	**configure terminal**	进入全局配置模式。
步骤 **2**	**router rip**	打开 RIP，进入配置模式
步骤 **3**	**network** *network-number*	设置 Rip 路由的网络范围，Rip 发送和接收路由更新只在网络范围内的接口进行。对于用户设定的任意网络范围，我们都将自动为您进行有类地址的转化，其中 0.0.0.0 表示包含全部网络范围，即包含全部网络接口。
步骤 **4**	**default-metric** *number*(1～15)	(可选)设置默认跳数，缺省的情况下为 1。
步骤 **5**	**neighbor** *ip-address*	(可选)定义一个与自己交换路由信息的邻居，这允许 RIP 和非广播网络中的路由器交换路由信息。
步骤 **6**	**offset-list** *access-list-name* **{in | out}** *offset* [*interface-id*]	(可选) 用户可以通过 acl 列表或者接口来限制偏移表的跳数。

步骤 **7**	**timers basic** *update invalid holddown*	(可选)调整路由协议的计时器。update：发送更新报文的时间间隔，缺省为 30 秒。有效范围为 0 到 2147483647 秒。invalid：宣布路由无效的时间间隔。缺省为 180 秒。有效范围为 1 到 2147483647 秒。holddown：在一条 RIP 路由表被删除之前应该保持的时间。缺省的时间为 120 秒。有效范围为 0 到 2147483647 秒。
步骤 **8**	**version** {**1**|**2**}	(可选)配置交换机只接收和发送 RIP1 和 RIP2 或者接收 RIP1 和 RIP2 发送 RIP1。缺省情况下为第三种。同样也可以通过接口配置命令 **ip rip** {*send*|*receive*} **version** {1|2|1 2}来控制网络接口的接收和发送版本。
步骤 **9**	**no validate-update-source**	(可选)禁止源地址验证。缺省情况下，交换机会对源地址进行验证并且将源地址无效的更新报文丢弃。在通常情况下，不建议关闭该选项。如果需要接收一台不在网络中的设备发送的更新报文，则可以使用该命令。
步骤 **10**	**default-information originate [route-map** *route-map-name* **]**	(可选) 允许 RIP 对存在缺省路由进行分发.包括用户静态设置的或者通过路由协议动态学习到的。
步骤 **11**	**End**	退回到特权模式。
步骤 **12**	**show ip protocols rip [routing-network| redistribute-info | | routing-information-source**] **show ip rip[interface | neighbor | offset-list]**	查看设置。
步骤 **13**	**copy running-config startup-config**	保存配置。

六、RIP 实验示例

（1）实验拓扑图



RIP 实验拓扑图

（2）计算机配置

PC0 配置 IP 地址为 192.168.0.2/24　默认网关：192.168.0.1

PC1 配置 IP 地址为 192.168.2.2/24　默认网关：192.168.2.1

（3）路由器配置命令

◆ **第一个路由器配置命令：**

Router>enable　　#进入特权模式

Router#configure terminal　　#进入全局配置模式

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

Router(config)#int f0/0　　#进入路由器接口 f0/0 配置模式

Router(config-if)#ip address 192.168.1.1 255.255.255.0　　#配置路由器接口 IP 地址

Router(config-if)#no shut　　#开启路由器接口

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

Router(config-if)#int f0/1　　#进入路由器接口 f0/1 配置模式

Router(config-if)#ip address 192.168.0.1 255.255.255.0　　#配置路由器接口 IP 地址

Router(config-if)#no shut　　#开启路由器接口

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Router(config-if)#exit

Router(config)#router rip

Router(config-router)#?

auto-summary	Enter Address Family command mode
default-information	Control distribution of default information
distance	Define an administrative distance
exit	Exit from routing protocol configuration mode
network	Enable routing on an IP network
no	Negate a command or set its defaults
passive-interface	Suppress routing updates on an interface
redistribute	Redistribute information from another routing protocol

```
  timers                Adjust routing timers
  version               Set routing protocol version
Router(config-router)#network 192.168.0.0   #定义路由器关联网络（声明路由器直接相连的网络号）
Router(config-router)#network 192.168.1.0   #定义路由器关联网络（声明路由器直接相连的网络号）
Router(config-router)#version 2        #制定 RIP 运行的版本号
Router(config-router)#end
```

◆ **第二个路由器配置命令：**

```
Router>enable                  #进入特权模式
Router#configure terminal      #进入全局配置模式
Enter configuration commands, one per line.   End with CNTL/Z.
Router(config)#int f0/0                  #进入路由器接口 f0/0 配置模式
Router(config-if)#ip address 192.168.1.2 255.255.255.0      #配置路由器接口 IP 地址
Router(config-if)#no shut                                    #开启路由器接口
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
Router(config-if)#int f0/1               #进入路由器接口 f0/1 配置模式
Router(config-if)#ip address 192.168.2.1 255.255.255.0      #配置路由器接口 IP 地址
Router(config-if)#no shut                #开启路由器接口
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#?
  auto-summary          Enter Address Family command mode
  default-information   Control distribution of default information
  distance              Define an administrative distance
  exit                  Exit from routing protocol configuration mode
  network               Enable routing on an IP network
  no                    Negate a command or set its defaults
  passive-interface     Suppress routing updates on an interface
  redistribute          Redistribute information from another routing protocol
  timers                Adjust routing timers
  version               Set routing protocol version
Router(config-router)#network 192.168.2.0   #定义路由器关联网络（声明路由器直接相连的网络号）
Router(config-router)#network 192.168.1.0   #定义路由器关联网络（声明路由器直接相连的网络号）
Router(config-router)#version 2        #制定 RIP 运行的版本号
Router(config-router)#end
Router#debug ip rip                    #打开 RIP 调试开关
RIP protocol debugging is on
Router#RIP: received v2 update from 192.168.1.1 on FastEthernet0/0
     192.168.0.0/24 via 0.0.0.0 in 1 hops
     #该显示信息表示路由器 B 的接口 Fa0/0 收到了来自 192.168.1.1 的路由信息：192.168.1.1
所在的路由器与网络 192.168.0.0/24 之间的距离为 1
Router#no debug ip rip          #关闭 RIP 调试开关
```

Router#show ip route　　#查看路由表
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　　192.168.1.0/24 is directly connected, FastEthernet0/1
C　　192.168.2.0/24 is directly connected, FastEthernet0/0
R　　192.168.0.0/24 [120/1] via 192.168.1.1, 00:00:05, FastEthernet0/0　　#RIP 获得的路由信息

请分析下列 rip 协议调试信息的含义并将分析结果写入实验报告册中：
RIP: sending　v2 update to 224.0.0.9 via FastEthernet0/1 (192.168.2.1)
RIP: build update entries
192.168.0.0/24 via 0.0.0.0, metric 2, tag 0
192.168.1.0/24 via 0.0.0.0, metric 1, tag 0
RIP: sending　v2 update to 224.0.0.9 via FastEthernet0/0 (192.168.1.2)
RIP: build update entries
192.168.2.0/24 via 0.0.0.0, metric 1, tag 0
RIP: received v2 update from 192.168.1.1 on FastEthernet0/0
192.168.0.0/24 via 0.0.0.0 in 1 hops
RIP: received v2 update from 192.168.1.1 on FastEthernet0/0
192.168.0.0/24 via 0.0.0.0 in 1 hops

实验八　动态路由 OSPF 协议配置

一、实验目的

- 掌握 OSPF 协议的配置方法；
- 掌握查看通过动态路由协议 OSPF 学习产生的路由；
- 熟悉广域网线缆的链接方式；

二、实验设备

PC 2 台；三层交换机 3560　1 台；路由器 2621　2 台；直连线；交叉线；DCE 串口线

三、实验背景

假设校园网通过一台三层交换机连到校园网出口路由器上，路由器再和校园外的另一台路由器连接。现要做适当配置，实现校园网内部主机与校园网外部主机之间的相互通信。为了简化网管的管理维护工作，学校决定采用 OSPF 协议实现互通。

四、技术原理

OSPF 开放式最短路径优先协议，是目前网路中应用最广泛的路由协议之一。属于内部网管路由协议，能够适应各种规模的网络环境，是典型的链路状态协议。OSPF 路由协议通过向全网扩散本设备的链路状态信息，使网络中每台设备最终同步一个具有全网链路状态的数据库，然后路由器采用 SPF 算法，以自己为根，计算到达其他网络的最短路径，最终形成全网路由信息。

五、实验相关命令格式

（1）启用一个 OSPF 路由

命令格式：　router　ospf　process-id　　#(也理解为进入路由器配置模式)

Router(config)#router　ospf　?

<1~65535> process ID

process-id　　#指定 OSPF 进程号，只在本地有效。

【举例】

routerA(config)#router ospf 10　　#指定 OSPF 进程号为 10

（2）将一个区域中几个网段定义成一个网络范围，。

[no] network　network_id [wild mask] area area_id [advertise | notadvertise]

【参数说明】

network_id 和 wild mask 为网络号 ID 和反掩码，点分十进制格式。

area_id 为区域号。

advertise 和 notadvertise 指定是否将到这一网络范围路由的摘要信息广播出去。

no network 命令取消网络范围

【缺省情况】

系统缺省没有配置网络范围。

【命令模式】

OSPF 协议配置模式

【使用指南】
一旦将某一网络的范围加入到区域中，到区域中所有落在这一范围内的 IP 地址的内部路由都不再被独立地广播到别的区域，而只是广播整个网络范围路由的摘要信息。引入网络范围和对该范围的限定，可以减少区域间路由信息的交流量。
【举例】
定义网络范围 10.0.0.0 255.0.0.0 加入到区域 2 中。
Router(config-if-Router)#network 10.0.0.0 **0.0.0.255** area 2

（3）启动或停止 OSPF 协议的运行
格式：router ospf enable
【缺省情况】
系统缺省不运行 OSPF 协议。
【命令模式】
全局配置模式
【使用指南】
使用此命令运行或终止 OSPF 协议。
【举例】
启动 OSPF 协议的运行。
Router(config)#router ospf enable

（4）显示 OSPF 连接状态数据库信息
格式：show ip ospf database
【命令模式】
特权用户模式
【使用指南】
根据该命令的输出信息，可以查看 OSPF 连接状态数据库信息，有助于用户进行故障诊断。
【举例】
Router(config)#show ip ospf database

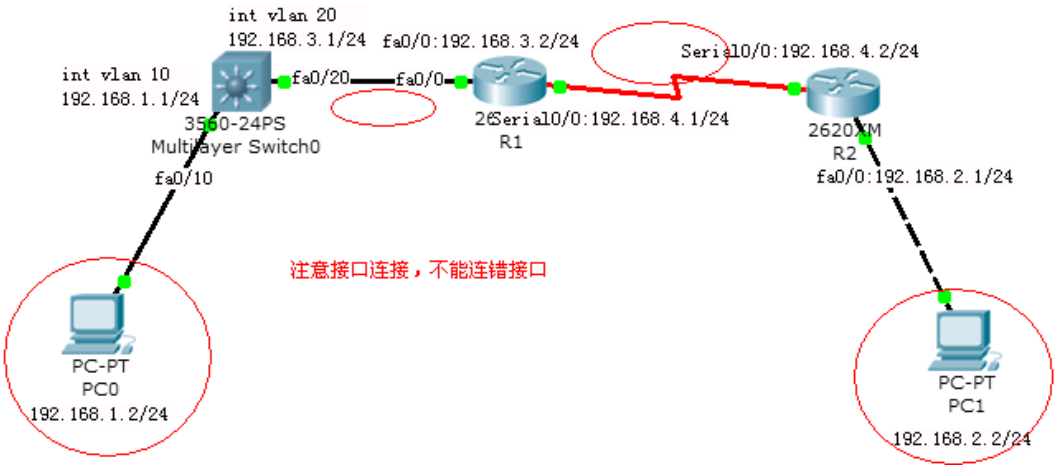
（5）显示 OSPF 接口信息。
格式：show ip ospf interface interface-type interface-number
【参数说明】
interface-type 为接口类型。
interface-number 为接口编号。
【命令模式】
特权用户模式
【使用指南】
根据该命令输出信息，查看接口上 OSPF 的配置和运行情况，用户可以确认配置是否正确和进行 OSPF 故障诊断。
【举例】
Router(config)#show ip ospf interface serial 1

（6）显示 OSPF 路由表信息。
命令格式：show ip ospf routing

【命令模式】
特权用户模式
【使用指南】
该命令输出信息有助于用户进行 OSPF 故障诊断。
【举例】
Router(config)#show ip ospf routing

六、点到点链路上的单区域 OSPF 配置实验示例

1、实验拓扑图



OSPF 实验拓扑图

2、操作步骤：

（1）在本实验中的三层交换机上划分 VLAN10 和 VLAN20，其中 VLAN10 用于连接校园网主机，VLAN20 用于连接 R1。

（2)路由器之间通过 V35 电缆通过串口连接，DCE 端连接在 R1 上，配置其时钟频率 64000。

（3）主机和交换机通过直连线，主机与路由器通过交叉线连接。

（4）在 S3560 上配置 OSPF 路由协议。

（5）在路由器 R1、R2 上配置 OSPF 路由协议。

（6）将 PC1、PC2 主机默认网关设置为与直连网路设备接口 IP 地址。

（7）验证 PC1、PC2 主机之间可以互相同信；

3、各实验设备主要命令及注释

PC1

IP: 192.168.1.2
Submask: 255.255.255.0
Gateway: 192.168.1.1

PC2

IP: 192.168.2.2
Submask: 255.255.255.0
Gateway: 192.168.2.1

S3560 交换机命令

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.   End with CNTL/Z.
Switch(config)#int fa0/10
Switch(config-if)#switchport access vlan 10
% Access VLAN does not exist. Creating vlan 10
Switch(config-if)#int fa0/20
Switch(config-if)#switchport access vlan 20
% Access VLAN does not exist. Creating vlan 20
Switch(config-if)#exit
Switch(config)#int vlan 10
%LINK-5-CHANGED: Interface Vlan10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#int vlan 20

%LINK-5-CHANGED: Interface Vlan20, changed state to up

Switch(config-if)#
Switch(config-if)#ip address 192.168.3.1 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#end

Switch#conf t
Enter configuration commands, one per line.   End with CNTL/Z.
Switch(config)#ip routing    #启动 IP 路由
Switch(config)#router ospf 1                  #启动 OSPF 进程 tin
Switch(config-router)#network 192.168.1.0 0.0.0.255 area 0     #在区域 0 声明网络
Switch(config-router)#network 192.168.3.0 0.0.0.255 area 0     #在区域 0 声明网络
Switch(config-router)#end
```

路由器 R1 命令：

```
Router>en
Router#conf t
Enter configuration commands, one per line.   End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int fa0/0
```

R1(config-if)#ip address 192.168.3.2 255.255.255.0
R1(config-if)#no shut

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config-if)#
R1(config-if)#exit
R1(config)#int serial 0/0 #进入串行口配置模式
R1(config-if)#clock rate 64000 #配置串口时钟频率
#仅在串行线一端配置时钟，另一边的串口不用配置时钟。
R1(config-if)#ip address 192.168.4.1 255.255.255.0
R1(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0, changed state to down
R1(config-if)#
R1(config-if)#exit
R1(config)#router ospf 2
R1(config-router)#network 192.168.3.0 0.0.0.255 area 0
R1(config-router)#network 192.168.4.0 0.0.0.255 area 0
R1(config-router)#end

路由器 R2

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
R2(config)#int fa0/0
R2(config-if)#ip address 192.168.2.1 255.255.255.0
R2(config-if)#no shut

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R2(config-if)#exit
R2(config)#int serial 0/0
R2(config-if)#ip address 192.168.4.2 255.255.255.0
R2(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0, changed state to up
R2(config-if)#exit
R2(config)#router ospf 3
R2(config-router)#network 192.168.2.0 0.0.0.255 area 0
R2(config-router)#network 192.168.4.0 0.0.0.255 area 0
R2(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console

```
R2#show ip route          #查看路由表

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

O    192.168.1.0/24 [110/783] via 192.168.4.1, 00:00:51, Serial0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
O    192.168.3.0/24 [110/782] via 192.168.4.1, 00:00:51, Serial0/0
C    192.168.4.0/24 is directly connected, Serial0/0
R2#
R2#show ip ospf database     #显示 OSPF  连接状态数据库信息
            OSPF Router with ID (192.168.4.2) (Process ID 3)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
192.168.3.1     192.168.3.1     283         0x80000003 0x0050d1 2
192.168.4.2     192.168.4.2     108         0x80000003 0x004935 3
192.168.4.1     192.168.4.1     108         0x80000004 0x00ca45 3

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.3.1     192.168.3.1     283         0x80000001 0x00fd2d
R2#
R2#
R2#show ip ospf ?
  <1-65535>          Process ID number
  border-routers     Border and Boundary Router Information
  database           Database summary
  interface          Interface information
  neighbor           Neighbor list
  <cr>
R2#show ip ospf int s0/0 ?
  <cr>
R2#show ip ospf int s0/0
Serial0/0 is up, line protocol is up
```

Internet address is 192.168.4.2/24, Area 0
Process ID 3, Router ID 192.168.4.2, Network Type POINT-TO-POINT, Cost: 781
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:08
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
Adjacent with neighbor 192.168.4.1
Suppress hello for 0 neighbor(s)

更多 OSPF 资料，请参考网址：
http://cisco.chinaitlab.com/List_147.html

附 A：OSPF 原理介绍

OSPF 是一种典型的链路状态路由协议。采用 OSPF 的路由器彼此交换并保存整个网络的链路信息，从而掌握全网的拓扑结构，独立计算路由。因为 RIP 路由协议不能服务于大型网络，所以，IETF 的 IGP 工作组特别开发出链路状态协议——OSPF。目前广为使用的是 OSPF 第二版，最新标准为 RFC2328。

OSPF 作为一种内部网关协议（Interior Gateway Protocol，IGP），用于在同一个自治域（AS）中的路由器之间发布路由信息。区别于距离矢量协议(RIP)，OSPF 具有支持大型网络、路由收敛快、占用网络资源少等优点，在目前应用的路由协议中占有相当重要的地位。

基本概念和术语

1. 链路状态

OSPF 路由器收集其所在网络区域上各路由器的连接状态信息，即链路状态信息（Link-State），生成链路状态数据库(Link-State Database)。路由器掌握了该区域上所有路由器的链路状态信息，也就等于了解了整个网络的拓扑状况。OSPF 路由器利用“最短路径优先算法(Shortest Path First, SPF)”，独立地计算出到达任意目的地的路由。

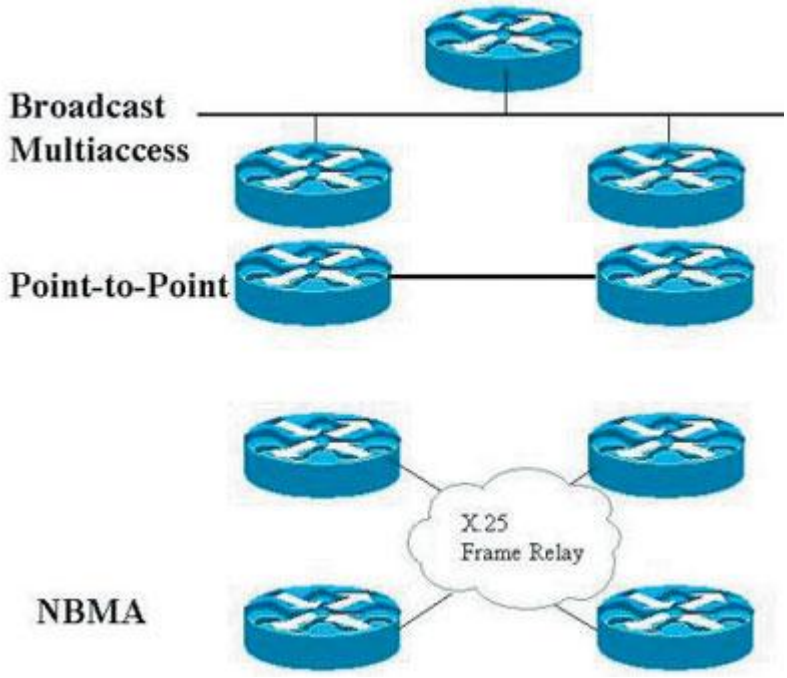
2. 区域

OSPF 协议引入“分层路由”的概念，将网络分割成一个“主干”连接的一组相互独立的部分，这些相互独立的部分被称为“区域” (Area)，“主干”的部分称为“主干区域”。每个区域就如同一个独立的网络，该区域的 OSPF 路由器只保存该区域的链路状态。每个路由器的链路状态数据库都可以保持合理的大小，路由计算的时间、报文数量都不会过大。

3. OSPF 网络类型

根据路由器所连接的物理网络不同，OSPF 将网络划分为四种类型：广播多路访问型（Broadcast MultiAccess）、非广播多路访问型（None Broadcast MultiAccess，NBMA）、点到点型（Point-to-Point）、点到多点型（Point-to-MultiPoint）。

广播多路访问型网络如：Ethernet、Token Ring、FDDI。NBMA 型网络如：Frame Relay、X.25、SMDS。Point-to-Point 型网络如：PPP、HDLC。具体结构如后图所示。



4. 指派路由器（DR）和备份指派路由器（BDR）

在多路访问网络上可能存在多个路由器，为了避免路由器之间建立完全相邻关系而引起的大量开销，OSPF 要求在区域中选举一个 DR。每个路由器都与之建立完全相邻关系。DR 负责收集所有的链路状态信息，并发布给其他路由器。选举 DR 的同时也选举出一个 BDR，在 DR 失效的时候，BDR 担负起 DR 的职责。

点对点型网络不需要 DR，因为只存在两个节点，彼此间完全相邻。 协议组成 OSPF 协议由 Hello 协议、交换协议、扩散协议组成。本文仅介绍 Hello 协议，其他两个协议可参考 RFC2328 中的具体描述。

当路由器开启一个端口的 OSPF 路由时，将会从这个端口发出一个 Hello 报文，以后它也将以一定的间隔周期性地发送 Hello 报文。OSPF 路由器用 Hello 报文来初始化新的相邻关系以及确认相邻的路由器邻居之间的通信状态。

对广播型网络和非广播型多路访问网络，路由器使用 Hello 协议选举出一个 DR。在广播型网络里，Hello 报文使用多播地址 224.0.0.5 周期性广播，并通过这个过程自动发现路由器邻居。在 NBMA 网络中，DR 负责向其他路由器逐一发送 Hello 报文。

协议操作

第一步：建立路由器的邻接关系

所谓“邻接关系”（Adjacency）是指 OSPF 路由器以交换路由信息为目的，在所选择的相邻路由器之间建立的一种关系。 路由器首先发送拥有自身 ID 信息（Loopback 端口或最大的 IP 地址）的 Hello 报文。与之相邻的路由器如果收到这个 Hello 报文，就将这个报文内的 ID 信息加入到自己的 Hello 报文内。

如果路由器的某端口收到从其他路由器发送的含有自身 ID 信息的 Hello 报文，则它根据该端口所在网络类型确定是否可以建立邻接关系。

在点对点网络中，路由器将直接和对端路由器建立起邻接关系，并且该路由器将直接进入到第三步操作：发现其他路由器。若为 MultiAccess 网络，该路由器将进入选举步骤。

第二步：选举 DR/BDR

不同类型的网络选举 DR 和 BDR 的方式不同。

MultiAccess 网络支持多个路由器，在这种状况下，OSPF 需要建立起作为链路状态和 LSA 更新的中心节点。选举利用 Hello 报文内的 ID 和优先权(Priority)字段值来确定。优先权字段值大小从 0 到 255，优先权值最高的路由器成为 DR。如果优先权值大小一样，则 ID 值最高的路由器选举为 DR， 优先权值次高的路由器选举为 BDR。优先权值和 ID 值都可以直接设置。

第三步：发现路由器

在这个步骤中，路由器与路由器之间首先利用 Hello 报文的 ID 信息确认主从关系，然后主从路由器相互交换部分链路状态信息。每个路由器对信息进行分析比较，如果收到的信息有新的内容，路由器将要求对方发送完整的链路状态信息。这个状态完成后，路由器之间建立完全相邻（Full Adjacency）关系，同时邻接路由器拥有自己独立的、完整的链路状态数据库。

在 MultiAccess 网络内，DR 与 BDR 互换信息，并同时与本子网内其他路由器交换链路状态信息。

在 Point-to-Point 或 Point-to-MultiPoint 网络中，相邻路由器之间互换链路状态信息。

第四步: 选择适当的路由器

当一个路由器拥有完整独立的链路状态数据库后，它将采用 SPF 算法计算并创建路由表。OSPF 路由器依据链路状态数据库的内容，独立地用 SPF 算法计算出到每一个目的网络的路径，并将路径存入路由表中。

OSPF 利用量度（Cost）计算目的路径，Cost 最小者即为最短路径。在配置 OSPF 路由器时可根据实际情况，如链路带宽、时延或经济上的费用设置链路 Cost 大小。Cost 越小，则该链路被选为路由的可能性越大。

第五步：维护路由信息

当链路状态发生变化时，OSPF 通过 Flooding 过程通告网络上其他路由器。OSPF 路由器接收到包含有新信息的链路状态更新报文，将更新自己的链路状态数据库，然后用 SPF 算法重新计算路由表。在重新计算过程中，路由器继续使用旧路由表，直到 SPF 完成新的路由表计算。新的链路状态信息将发送给其他路由器。值得注意的是，即使链路状态没有发生改变，OSPF 路由信息也会自动更新，默认时间为 30 分钟。

实验九 访问控制列表 ACL 实验

一、实验目的

理解标准 IP 访问控制列表和扩展 IP 访问控制列表的原理及功能；

掌握编号的 IP 访问控制列表的配置方法；

二、实验设备

计算机、CISCO R2621 路由器、交换机、V35 线缆、双绞线若干。

三、实验相关原理

ACL 的全称为接入控制列表（Access Control Lists），也称访问控制列表（Access Lists），俗称防火墙，在有的文档中还称包过滤。ACLs 通过定义一些规则对网络设备接口上的数据包文进行控制；允许通过或丢弃，从而提高网络可管理型和安全性；

IP ACL 分为两种：标准 IP 访问列表和扩展 IP 访问列表，编号范围为 1～99、1300～1999、100～199、2000～2699；

（1）标准 IP 访问控制列表可以根据数据包的源 IP 地址定义规则，进行数据包的过滤；

扩展 IP 访问列表可以根据数据包的原 IP、目的 IP、源端口、目的端口、协议来定义规则，进行数据包的过滤；

IP ACL 基于接口进行规则的应用，分为：入栈应用(in)和出栈应用(out)；

访问列表中定义的典型规则主要有以下：源地址、目标地址、上层协议、时间区域；

（2）扩展 IP 访问列表（编号 100-199、2000、2699）使用以上四种组合来进行转发或阻断分组；可以根据数据包的源 IP、目的 IP、源端口、目的端口、协议来定义规则，进行数据包的过滤。

扩展 IP 访问列表的配置包括以下两部：

- 定义扩展 IP 访问列表
- 将扩展 IP 访问列表应用于特定接口上

三、实验项目

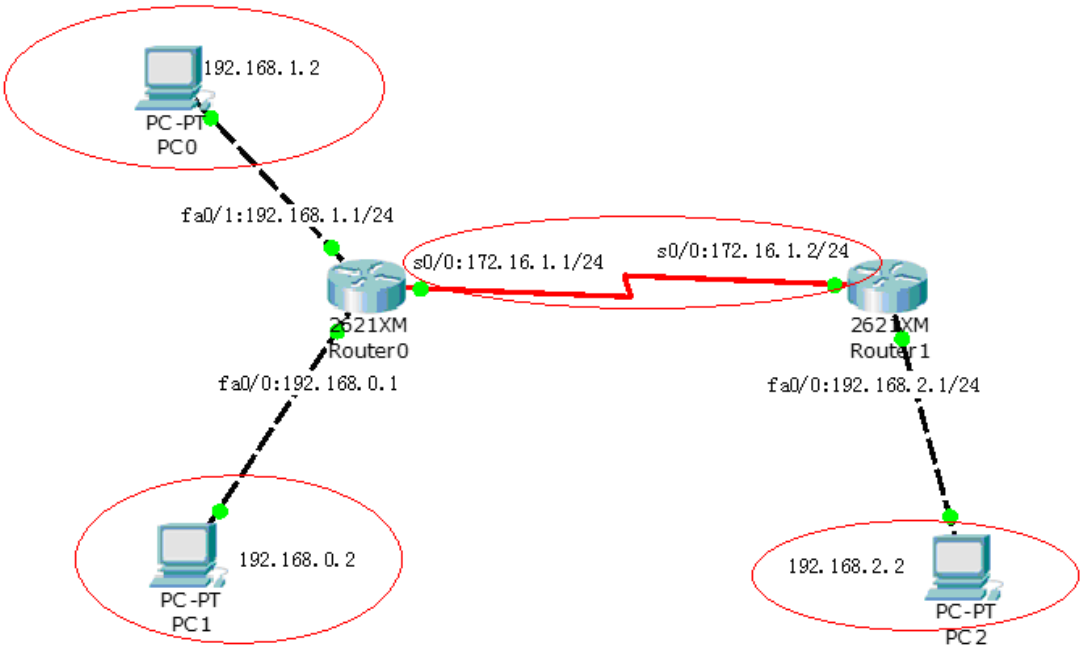
1、标准 IP 访问控制列表实验

实验要求：

假设你是公司的网络管理员，公司的经理部、财务部们和销售部门分属于不同的 3 个网段，三部门之间用路由器进行信息传递，为了安全起见，公司领导要求销售部门不能对财务部进行访问，但经理部可以对财务部进行访问。

用 PC0 代表经理部的主机、PC1 代表销售部的主机、PC2 代表财务部的主机。要求使用标准 ACL 实现 PC0 可以访问 PC2，但 PC1 不能访问 PC2。

实验拓扑图如下：



实验操作步骤：

（1)路由器之间通过 V.35 电缆通过串口连接，DCE 端连接在 R1 上，配置其时钟频率 64000；主机与路由器通过交叉线连接。

（2）配置路由器接口 IP 地址。

（3）在路由器上配置静态路由协议，让三台 PC 能够相互 Ping 通，因为只有在互通的前提下才涉及到方控制列表。

（4）在 R1 上编号的 IP 标准访问控制

（5）将标准 IP 访问控制应用到接口上。

（6）验证主机之间的互通性。

各设备具体参数配置和命令如下：

PC0

IP: 192.168.1.2

Submask: 255.255.255.0

Gageway: 192.168.1.1

PC1

IP: 192.168.0.2

Submask: 255.255.255.0

Gageway: 192.168.0.1

PC2

IP: 192.168.2.2

Submask: 255.255.255.0

Gageway: 192.168.2.1

Router0 命令如下：

Continue with configuration dialog? [yes/no]: no

Press RETURN to get started!

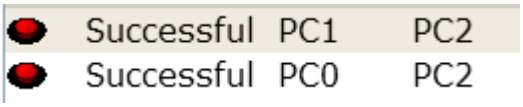
```
Router>en
Router#conf    t
Enter configuration commands, one per line.    End with CNTL/Z.
Router(config)#int fa0/1
Router(config-if)#ip add 192.168.1.1 255.255.255.0      #配置以太口 IP 地址
Router(config-if)#no shut
Router(config-if)#int fa0/0
Router(config-if)#ip add 192.168.0.1 255.255.255.0      #配置以太口 IP 地址
Router(config-if)#no shut
Router(config-if)#int s0/0
Router(config-if)#ip add 172.16.1.1 255.255.255.0      #配置串口 IP 地址
Router(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0, changed state to up
Router(config-if)#clock rate 64000                  #设置串口时钟频率（只需在一端设置）
Router(config-if)#exit
Router(config)#router rip                           #启动并配置 RIP 协议
Router(config-router)#network 192.168.0.0       #声明直接相连的网络
Router(config-router)#network 192.168.1.0
Router(config-router)#network 172.16.1.0
Router(config-router)#version 2          #  制定 vip 版本
Router(config-router)#end
Router#show ip route                #显示路由表
显示路由表如下：
Router#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
           172.16.0.0/24 is subnetted, 1 subnets
     C       172.16.1.0 is directly connected, Serial0/0
     C       192.168.0.0/24 is directly connected, FastEthernet0/0
     C       192.168.1.0/24 is directly connected, FastEthernet0/1
     R       192.168.2.0/24 [120/1] via 172.16.1.2, 00:00:26, Serial0/0
```

Router1 命令如下：

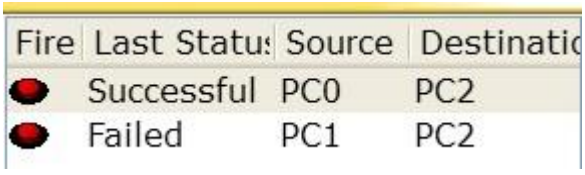
```
Router>en
Router#conf t
Enter configuration commands, one per line.    End with CNTL/Z.
Router(config)#int fa0/0
```

Router(config-if)#ip add 192.168.2.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int s0/0
Router(config-if)#ip add 172.16.1.2 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.168.2.0
Router(config-router)#network 172.16.1.0
Router(config-router)#version 2
Router(config-router)#end

测试 PC0、PC2、PC3 之间的连通性，正常结果如下图：

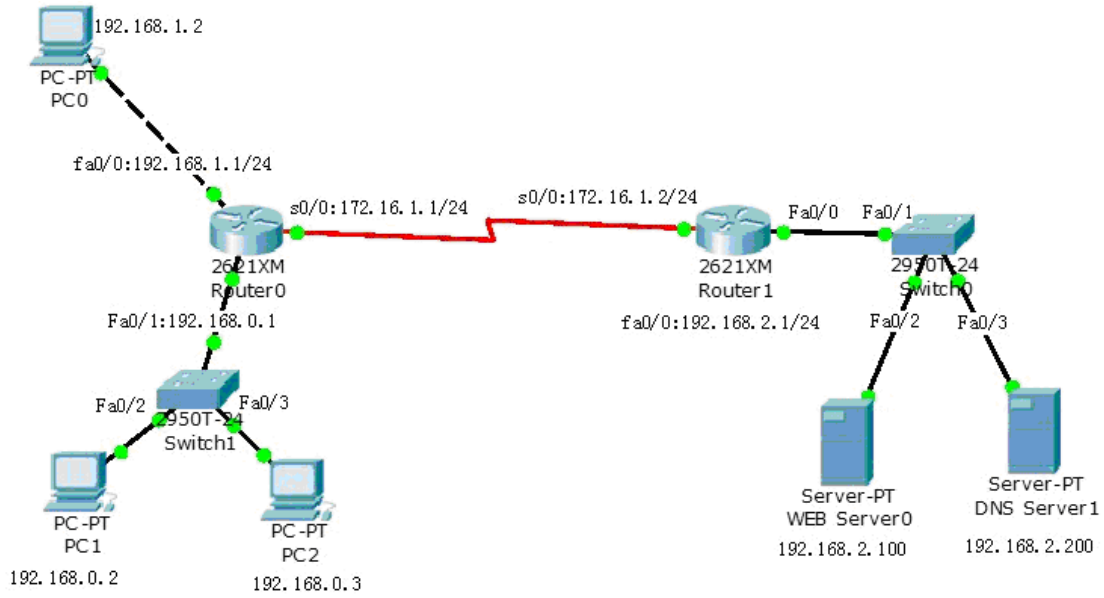


配置标准 ACL，允许 PC0 所在网段访问 PC2 所在网段
拒绝 PC1 所在网段访问 PC2 所在网段
在 Router0 上配置如下命令：
Router#conf t
Router(config)#access-list 10 permit 192.168.1.0 0.0.0.255
#允许 PC0 所在网段访问 PC2 所在网段
Router(config)#access-list 10 deny 192.168.0.0 0.0.0.255
#拒绝 PC1 所在网段访问 PC2 所在网段
#删除 ACL 命令是 Router(config)#no access-list 10
Router(config)#int s0/0
Router(config-if)#ip access-group 10 out #将 ACL 策略应用在接口 S0/0 上
Router#show access-lists 10 #查看 ACL 策略情况
Standard IP access list 10
permit 192.168.1.0 0.0.0.255 (1 match(es))
deny 192.168.0.0 0.0.0.255 (1 match(es))
测试 PC0、PC1、 PC2 之间的连通性：



2、扩展 IP 访问控制列表实验

实验拓扑图如下：



实验要求：

按拓扑图连接所有设备并配置 IP 等参数

合理配置扩展 ACL 策略，使得：

- PC0 所在网段 IP 地址在 192.168.1.2~192.168.1.126 的计算机能访问 WEB Server0，地址在 192.168.1.129~192.168.1.254 的计算机不能访问 WEB Server0

- PC1 能所在网段除了 PC2 之外，其他计算机都可以访问 WEB Server0 的网站。

Fire	Last Status	Source	Destination	Type	Color
	Failed	PC2	WEB Server0	ICMP	
	Successful	PC2	DNS Server1	ICMP	

- PC1 虽然能访问 WEB Server0 的网站，但无法 Ping 通 WEB Server0，但 WEB Server0 能 ping 通 PC1。如下图所示：

Fire	Last Status	Source	Destination	Type
	Successful	PC1	DNS Server1	ICMP
	Failed	PC1	WEB Server0	ICMP
	Successful	WEB Server0	PC1	ICMP

计算机与路由器 IP 等参数配置（略）

在路由器 Router0 上创建 ACL 101，并应用到接口 S0/0 的 out 方向上：

Router#conf t

Router(config)#access-list 101 permit ip 192.168.1.0 0.0.0.127 any

#允许网段 IP 地址在 192.168.1.2~192.168.1.126 的计算机能访问外网

Router(config)#access-list 101 deny ip 192.168.1.128 0.0.0.127 any

#拒绝网段 IP 地址在 192.168.1.129~192.168.1.254 的计算机访问外网

Router(config)#access-list 101 deny ip host 192.168.0.3 192.168.2.100 0.0.0.0

#拒绝 PC2（192.168.0.3） 访问外网

Router(config)#access-list 101 deny icmp 192.168.0.2 0.0.0.0 192.168.2.100 0.0.0.0 echo

#使 PC1 能访问 WEB Server0 的网站，但无法 Ping 通 WEB Server0，但 WEB Server0 能 ping 通 PC1

Router(config)#access-list 101 permit ip 192.168.0.0 0.0.0.255 any

#允许地址段 192.168.0.0 其他的计算机访问外网，注意此条必须放在最后，ACL 是按顺序最小匹配原则。

Router(config)#int s0/0

Router(config-if)#ip access-group 101 out #将 ACL 101 列表应用在 S0/0 接口的 out 方向上

Router(config)#end

使用命令查看 ACL 101 :

Router#show access-lists 101

Extended IP access list 101

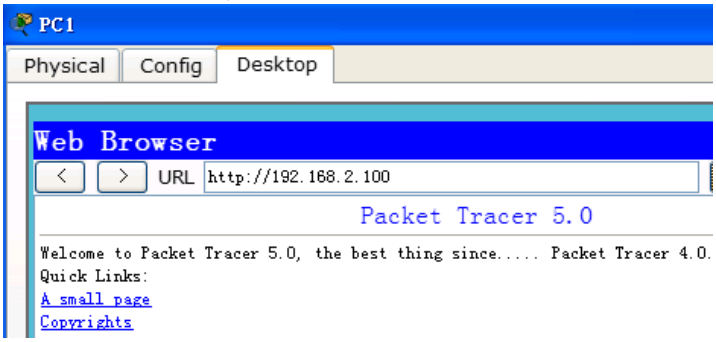
deny icmp host 192.168.0.2 host 192.168.2.100 echo (3 match(es))

permit ip 192.168.1.0 0.0.0.127 any (2 match(es))

deny ip 192.168.1.128 0.0.0.127 any (1 match(es))

deny ip host 192.168.0.3 host 192.168.2.100 (2 match(es))

permit ip 192.168.0.0 0.0.0.255 any (6 match(es))



上图为 PC1 访问 WEB server 0 网站示意图。

实验十 网络地址转换 NAT 实验

一、实验目的

理解 NAT 网络地址转换的原理及功能；

掌握静态 NAT 的配置，实现局域网访问互联网；

二、实验设备

计算机、CISCO R2621 路由器、交换机、V35 线缆、双绞线若干。

三、实验相关原理

私有网络 IP 地址，即互联网路由器均不对这些地址进行路由转发，只能应用于私有内部网络，主要用来解决 IP 地址不足问题，私有网络地址可以在不同单位内部自由使用，且可以重复使用。私有网络 IP 地址段如下：

A 类私有 IP 地址段： 10.0.0.0 ~ 10.255.255.255

B 类私有 IP 地址段： 172.16.0.0 ~ 172.31.255.255

C 类私有 IP 地址段： 192.168.0.0 ~ 192.168.255.255

网络地址转换 NAT（Network Address Translation），被广泛应用于各种类型 Internet 接入方式和各种类型的网络中。原因很简单，NAT 不仅完美地解决了 IP 地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。

默认情况下，内部 IP 地址是无法被路由到外网的，内部主机 10.1.1.1 要与外部 Internet 通信，IP 包到达 NAT 路由器时，IP 包头的源地址 10.1.1.1 被替换成一个合法的外网 IP，并在 NAT 转发表中保存这条记录。当外部主机发送一个应答到内网时，NAT 路由器受到后，查看当前 NAT 转换表，用 10.1.1.1 替换掉这个外网地址。

NAT 将网络划分为内部网络和外部网络两部分，局域网主机利用 NAT 访问网络时，是将局域网内部的本地地址转换为全局地址（互联网合法的 IP 地址）后转发数据包；

NAT 有 3 种类型：静态 NAT、动态 NAT 和端口地址转换（PAT）。

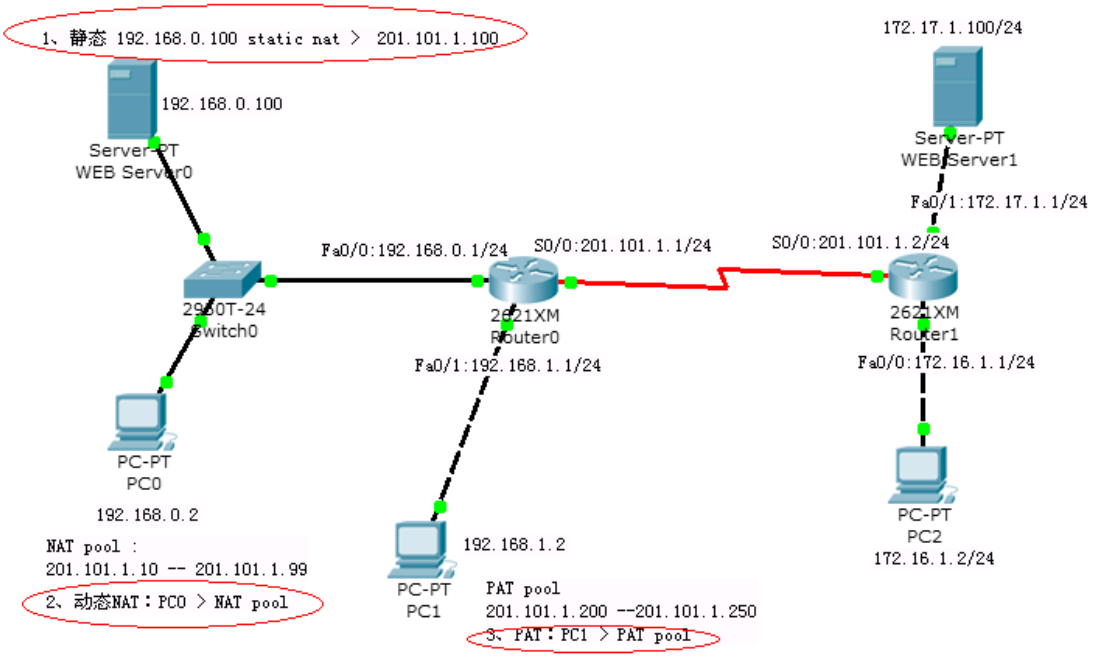
（1）静态 NAT：在静态 NAT 中，内部网络中的每个主机都被永久映射成外部网络中的某个合法的地址。静态地址转换将内部本地地址与内部合法地址进行一对一的转换，且需要指定和哪个合法地址进行转换。如果内部网络有 E-mail 服务器或 FTP 服务器等可以为外部用户提供的服务，这些服务器的 IP 地址必须采用静态地址转换，以便外部用户可以使用这些服务。**<内 IP > → <外 IP> （1:1）**

（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。**<内 IP > → <外 IP> （动态 1:1）**

（3）NAPT：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。**<内 IP，内端口 > → <外 IP，外端口> （n:1）**

三、实验内容

1、拓扑图



2、按拓扑图连接相关设备，并且配置设备 IP 地址，设置默认路由策略。

(1)计算机参数配置：

WEB Server0 ：

IP 192.168.0.100/24　　网关：192.168.0.1

WEB Server1 ：

IP 172.17.1.100/24　　网关：172.17.1.1

PC0:

IP 192.168.0.2/24　　网关：192.168.0.1

PC1:

IP 192.168.1.2/24　　网关：192.168.1.1

PC2:

IP 172.16.1.2/24　　网关：172.16.1.1

(2) 路由器配置 IP 和默认路由

Router0 配置：

```
Router>en
Router#conf t
Router(config)#int fa0/0
Router(config-if)#ip add 192.168.0.1 255.255.255.0
Router(config-if)#no shut
```

Router(config-if)#int fa0/1
Router(config-if)#ip add 192.168.1.1 255.255.255.0
Router(config-if)#no shut

Router(config-if)#int s0/0
Router(config-if)#ip add 201.101.1.1 255.255.255.0
Router(config-if)#clock rate 64000
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#ip route 0.0.0.0 0.0.0.0 201.101.1.2　　#设置默认路由

Router1 配置：
Router>en
Router#conf t
Router(config)#int fa0/0
Router(config-if)#ip add 172.16.1.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int s0/0
Router(config-if)#ip add 201.101.1.2 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#int fa0/1
Router(config-if)#ip add 172.17.1.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
~~Router(config)#ip route 0.0.0.0 0.0.0.0 201.101.1.1　#设置默认路由~~

(3) 静态 NAT 配置
　将 SERVER0 192.168.0.100　静态映射成　201.101.1.100

在 Router0 上配置静态 NAT 命令：
Router#conf t
Router(config)#int fa0/0
Router(config-if)#ip nat inside　　#指定 NAT 内接口
Router(config-if)#int s0/0
Router(config-if)#ip nat outside　　#指定 NAT 外接口
Router(config-if)#exit
Router(config)#ip nat inside source static 192.168.0.100 201.101.1.100　#设置静态 NAT

在 Router0 上查看静态 NAT 策略：
Router#show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
---	201.101.1.100	192.168.0.100	---	

验证静态 NAT：

在 PC2 上使用 Ping 命令测试与 201.101.1.100 的连通性，结果如下：

PC>ping 201.101.1.100

Pinging 201.101.1.100 with 32 bytes of data:

Reply from 201.101.1.100: bytes=32 time=125ms TTL=126

Reply from 201.101.1.100: bytes=32 time=109ms TTL=126

Reply from 201.101.1.100: bytes=32 time=109ms TTL=126

Reply from 201.101.1.100: bytes=32 time=125ms TTL=126

Ping statistics for 201.101.1.100:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 109ms, Maximum = 125ms, Average = 117ms

在 PC2 上使用 Ping 命令测试与 **192.168.0.100** 的连通性，结果如下：

PC>ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

应该是不可达，下面红字部分有误

Reply from 201.101.1.100: bytes=32 time=95ms TTL=126

Reply from 201.101.1.100: bytes=32 time=125ms TTL=126

Reply from 201.101.1.100: bytes=32 time=125ms TTL=126

Reply from 201.101.1.100: bytes=32 time=125ms TTL=126

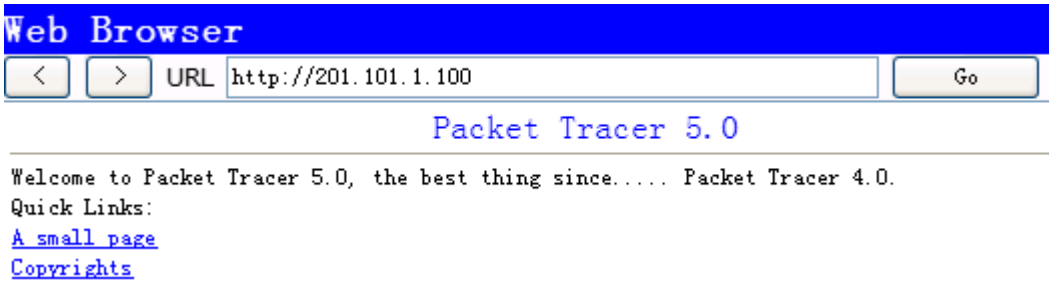
Ping statistics for 192.168.0.100:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 95ms, Maximum = 125ms, Average = 117ms

在 PC2 上浏览 WEB Server0 的网站，结果如下图：



(4) 动态 NAT 配置

实现 PC0：192.168.0.2 –>（ 201.101.1.10 ~ 201.101.1.99），PC0 可以随机选择一个外部 IP，实现对外网访问。

动态 NAT 必须和 ACL 列表配合使用，步骤如下：

1) 创建 ACL 策略并应用到相应端口上

2) 建立地址池 pool

3) 使用 ip nat 命令建立动态 NAT
4) 使用 ip nat outside 命令指定 NAT 外接口、使用 ip nat inside 命令指定 NAT 内接口

a）在 Router0 上创建 ACL 策略并应用到相应端口上
Router(config)#access-list 10 permit 192.168.0.0 0.0.0.255
#创建标准列表 10，允许 192.168.0.0/24 访问外网
Router(config)#access-list 10 deny any #阻止其他的访问请求
Router(config)#int fa0/0
Router(config-if)#ip access-group 10 in #将 ACL 应用到接口 fa0/0 上
b）在 Router0 上创建动态地址池（201.101.1.10 ~ 201.101.1.99）
Router(config)#ip nat pool dynat-pool_1 201.101.1.10 201.101.1.99 netmask 255.255.255.0
#建立动态 NAT 地址池
c）使用 ip nat 命令建立动态 NAT
Router(config)#ip nat inside source list 10 pool dynat-pool_1

d）使用 ip nat outside 命令指定 NAT 外接口、使用 ip nat inside 命令指定 NAT 内接口
Router#conf t
Router(config)#int fa0/0
Router(config-if)#ip nat inside #指定 NAT 内接口
Router(config-if)#int s0/0
Router(config-if)#ip nat outside #指定 NAT 外接口
Router(config-if)#exit

注意：这个步骤在前面静态 NAT 时已经做过，可以不需再重复做。

测试动态 NAT：
使用命令查看 NAT 转换情况：
Router#show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
---	201.101.1.100	192.168.0.100	---	---
---	202.101.1.10	192.168.0.2	---	---

(5) PAT 配置
实现 PC0：**（192.168.1.2 ，内端口）–>（ 202.101.1.200 ~ 202.101.1.250，外端口）**，PC1 可以随机选择一个外部 IP，且外端口可随机使用空闲端口，实现对外网访问。
PAT 也必须和 ACL 列表配合使用，步骤如下：
1) 创建 ACL 策略并应用到相应端口上
2) 建立地址池 pool
3) 使用 ip nat 命令建立动态 PAT
4) 使用 ip nat outside 命令指定 NAT 外接口、使用 ip nat inside 命令指定 NAT 内接口

a）在 Router0 上创建 ACL 策略并应用到相应端口上

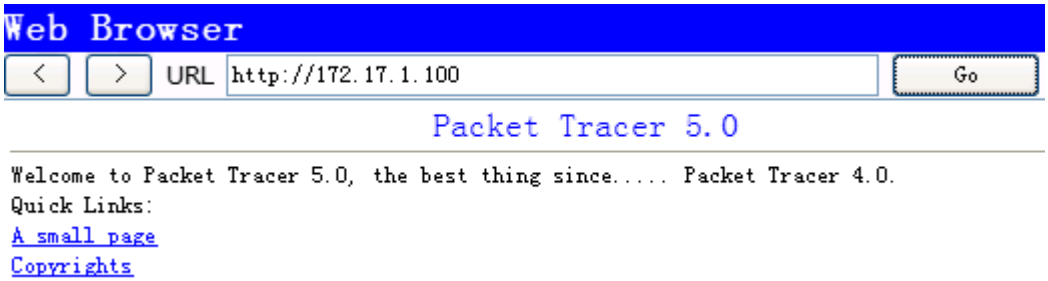
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 any
#创建扩展列表 101，允许 192.168.1.0/24 访问外网
Router(config)#access-list 101 deny ip any any
#阻止其他的访问请求
Router(config)#int fa0/1
Router(config-if)#ip access-group 101 in #将 ACL101 应用到接口 fa0/1 上
b）在 Router0 上创建动态地址池（201.101.1.200 ~ 201.101.1.250）
Router(config)#ip nat pool pat-pool_2 201.101.1.200 201.101.1.250 netmask 255.255.255.0

c）使用 ip nat 命令建立动态 NAT
Router(config)#ip nat inside source list 101 pool pat-pool_2 overload

d）使用 ip nat outside 命令指定 NAT 外接口、使用 ip nat inside 命令指定 NAT 内接口
Router#conf t
Router(config)#int fa0/1
Router(config-if)#ip nat inside
Router(config-if)#int s0/0
Router(config-if)#ip nat outside
Router(config-if)#exit

注意：这个步骤在前面静态 NAT 时已经做过，可以不需再重复做。

测试 PAT：
在 PC1 上 ping WEB Server1
Ping 172.17.1.100
在 PC1 上访问 WEB Server1 网站



使用命令查看 PAT 转换情况：
Router#show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
---	201.101.1.100	192.168.0.100	---	---
---	202.101.1.10	192.168.0.2	---	---

tcp 201.101.1.200:1026 192.168.1.2:1026 172.17.1.100:80
注意：上面蓝色的字体的条目即为 PAT 映射
表示 192.168.1.2:1026 → 201.101.1.200:1026