

江南大学

实验指导书

课程名称： 计算机网络

专业名称： 计算机科学与技术

编制学院： 物联网工程学院

编制人员： 王晓锋

二〇一六年六月

实 验 目 录

实验 1：网线的制作

实验 2：网络设备的基本操作

实验 3：基础网络构建与诊断

实验 4：VLAN 配置

实验 5：生成树配置

实验 6：链路聚合配置

实验 7：ARP 配置

实验 8：DHCP 配置

实验 9：静态路由配置

实验 10：RIP 协议配置

实验 11：OSPF 协议配置

实验 12：网络报文捕获与分析

实验一 网线的制作

1.1 实验目的

- (1) 了解标准 568A 与 568B 网线的线序；
- (2) 了解交叉线和直通线的不同应用场合；
- (3) 掌握网线的制作和测试方法。

1.2 实验内容

- (1) 制作一条直连网线。

1.3 实验原理

1.3.1 双绞线

非屏蔽双绞线（Unshielded Twisted Pair, UTP）是在塑料绝缘外皮里面包裹着 8 根信号线，它们每 2 根为一对相互缠绕，总共形成 4 对，双绞线也因此得名，如图 1-1 所示。双绞线这样互相缠绕的目的，就是利用铜线中电流产生的电磁场互相作用抵消邻近线路的干扰，并减少来自外界的干扰。每对线在每英寸长度上相互缠绕的次数决定其抗干扰的能力和通信的质量，缠绕得越紧密其通信质量越高，就可以支持更高的网络数据传输速率，当然它的成本也就越高。

国际电工委员会和国际电信委员会 EIA/TIA（Electronic Industry Association/Telecommunication Industry Association）已经制定了 UTP 网线的国际标准，并根据使用的领域不同分为几个类别（Category 或者简称 Cat），每种类别的网线生产厂家都会在其绝缘外皮上标注其种类，例如 Cat-5 或者 Category-5。具体内容见表 1-1。

表 1-1 EIA/TIA 为 UTP 电缆规定的类别

类别	频率	应用范围
1	远少于 1MHz	语音级电话；POTS；报警系统
2	最高为 1MHz	语音级电话；IBM 小型计算机和大型机终端；ARCnet；LocalTalk
3	最高为 16MHz	语音级电话；10Base-T 以太网；4Mb/s 令牌环网；100VG-AnyLAN
4	最高为 20MHz	16 Mb/s 令牌环网
5	最高为 100MHz	100Base-TX；OC-3（ATM）；SONet
5e	最高为 100MHz	1000Base-T（千兆位以太网）

在日常的局域网当中，一般的双绞线、集线器和交换机均使用 RJ-45 连接器进行连接。基于 RJ-45 的网络连接线分为直连线和交叉线两种。

1.3.2 RJ-45 连接器

制作网线所需要的 RJ-45 连接器（俗称水晶头）前端有 8 个凹槽，简称 8P（Position，

位置)。凹槽内的金属接点共有 8 个, 简称 8C (Contact, 触点), 所以 RJ-45 也被叫做 8P8C, 如图 1-1 所示。特别需要注意的是 RJ-45 水晶头引脚序号, 当金属片面对我们时从左至右引脚序号是 1~8, 序号对于网络连线非常重要, 不能颠倒。

EIA/TIA 的布线标准中规定了两种双绞线的线序 568A 与 568B。对 RJ-45 连线方式规定如下:

(1) 1、2 用于发送, 3、6 用于接收, 4、5, 7、8 是双向线。

(2) 1、2 线必须是双绞, 3、6 双绞, 4、5 双绞, 7、8 双绞。

这样可以最大限度地抑制干扰信号, 提高传输质量。

标准 568A: 白绿-1, 绿-2, 白橙-3, 蓝-4, 白蓝-5, 橙-6, 白棕-7, 棕-8, 如图 1-2 所示。

标准 568B: 白橙-1, 橙-2, 白绿-3, 蓝-4, 白蓝-5, 绿-6, 白棕-7, 棕-8, 如图 1-2 所示。

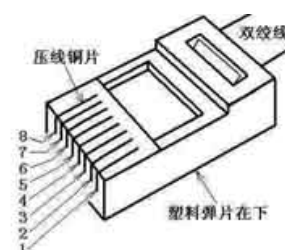


图 1-1 RJ-45 连接器

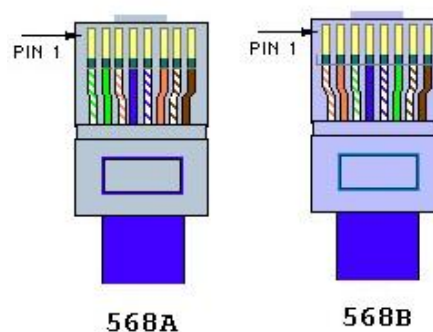


图 1-2 标准 568A 和标准 568B

1.3.3 直连线介绍

大多数情况下, 双绞线电缆的线路是直通连接的。计算机使用分开的线路来发送和接收数据, 计算机及其他设备相互通信时一般通过各自的发送和接收端口进行, 设备 A 通过发送端口发送数据到设备 B 的接收端口, 同时设备 A 也通过接收端口接收设备 B 发送端口发出的数据, 就是说, 在发送和接收线路对之间必须出现信号交叉。通常集线器会负责进行信号的交叉。当计算机通过集线器与其他计算机相连时, 集线器内部可以完成发送端口与接收端口之间的匹配。目前很多交换机也可以自动识别直连线和交叉线, 决定是否进行信号转换。

综上所述, 所谓的直连线就是双绞线两端的发送端口与发送端口直接相连, 接收端口与接收端口直接相连。

由于直连线一端的每个引线与另一端的对应引线相连, 所以只要方向正确, 线路是什么颜色并不重要。也就是说, 两种连接方式没有本质的区别, 但是必须做出明确的决定, 究竟使用哪一种标准, 避免因混淆造成无效连接。本实验统一采用 568B 标准。

1.3.4 交叉线介绍

如果要把两台计算机直接连接起来形成一个简单的两节点以太网, 或者将集线器与集线器通过普通的端口进行级连, 就必须使用交叉线。

所谓的交叉线即指双绞线两端的发送端口与接收端口交叉相连。要求双绞线的两头连线要 1-3、2-6 进行交叉, 即如果在一端, 白橙线对应到水晶头的第一个引脚, 则在另一端的水晶头, 白橙线要对应到其第三个引脚。

在进行设备连接时, 需要正确地选择线缆。将设备的 RJ-45 接口分为 MDI (Media Dependent Interface) 和 MDIX 两类。当两种类型的接口通过双绞线互连时 (两个接口都是 MDI 或都是 MDIX), 使用交叉网线; 当不同类型的接口 (一个接口是 MDI, 一个接口是 MDIX) 通过双绞线互连时, 使用直连网线。通常主机和路由器的接口属于 MDI, 交换机和集线器的接口属于 MDIX。例如路由器与主机相连, 采用交叉网线; 交换机与主机相连则采用直连网线。表 1-2 示意了如何选择双绞线连接设备, 表中 N/A 表示不可连接。

表 1-2 设备间连线

	主机	路由器	交换机 MDIX	交换机 MDI	集线器
主机	交叉	交叉	直连	N/A	直连
路由器	交叉	交叉	直连	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

需要指出的是,随着技术的发展,目前一些新的网络设备可以自动识别连接的网线类型,用户不管采用直连网线或者交叉网线均可以正确连接设备。如华为 3Com 公司的 QuidwayS3026、QuidwayS3526 以太网交换机的 10/100M 以太网接口就具备智能 MDI/MDIX 识别技术。

1.3.5 卡线钳

卡线钳可以完成剪线、剥线和压线三个步骤,是制作网线的首选工具。卡线钳种类很多,具体使用时应参考使用说明,本实验采用市场上比较常见的品种,如图 1-3 所示。

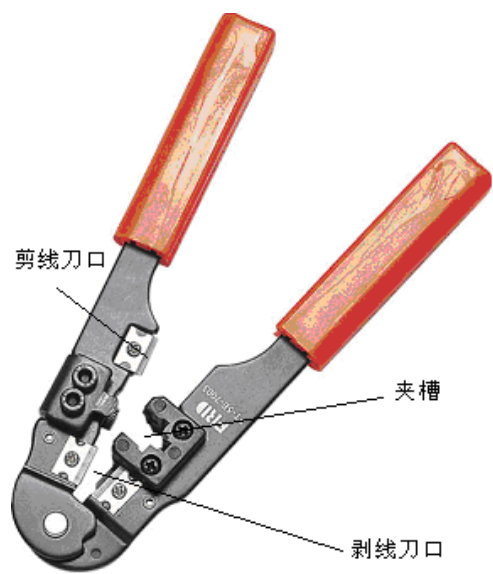


图 1-3 卡线钳

1.3.6 电缆测试仪

电缆测试仪分为信号发射器和信号接收器两部分,各有 8 盏信号灯。测试时将网线两端分别插入电缆测试仪的信号发射器和信号接收器,打开电源。如果网线制作成功,则发射器和接收器上同一条线对应的指示灯会亮起来,依次从 1 号到 8 号(针对直连线的情况)。如图 1-4 所示。



图 1-4 电缆测试仪

如果网线制作有问题，灯亮的顺序就不可预测。比如：若发射器的第 1 个灯亮时，接收器第 7 个灯亮，则表示线做错了（不论是直连线还是交叉线，都不可能有 1 对 7 的情况）；若发射器的第一个灯亮时，接收器却没有任何灯亮起，那么这只引脚与另一端的任一只引脚都没有连通，可能是导线中间断了，或是两端至少一个金属片未接触该条芯线。一定要经过测试，否则断路会导致无法通信，短路有可能损坏网卡或交换机。

1.4 实验环境与分组

- (1) 双绞线 2 段，卡线钳 2 个，水晶头若干，电缆测试仪 2 台；
- (2) 每组 4 名同学，两两合作进行实验。

1.5 实验步骤

第一步：剥线

用卡线钳剪线刀口将双绞线端头剪齐，再将双绞线端头伸入剥线刀口，使线头触及前挡板，然后适度握紧卡线钳同时慢慢旋转双绞线，让刀口划开双绞线的保护胶皮，取出端头从而剥下保护胶皮。剥线的长度为 13mm~15mm，不宜太长或太短。剥好的线头如图 1-5 所示。



图 1-5 剥好的线头

第二步：理线

双绞线由 8 根有色导线两两绞合而成，按照标准 568B 的线序排列，整理完毕后用剪线刀口将前端修齐。

第三步：插线

一只手捏住水晶头，将水晶头有弹片的一侧向下，另一只手捏平双绞线，稍稍用力将排好的线平行插入水晶头内的线槽中，8 条导线顶端应插入线槽顶端，如图 1-6 所示。

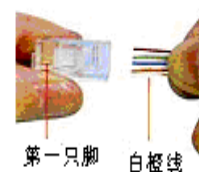


图 1-6 插线

注意：将并拢的双绞线插入 RJ-45 接头时，白橙线要对着 RJ-45 的第 1 只引脚。

第四步：压线

确认所有导线都到位后，将水晶头放入压线钳夹槽中，用力捏几下压线钳，压紧线头即

可。

按照以上 4 步制作双绞线的另一端，即可完成制作。

第五步：检测

将制作好的网线两端分别插入电缆测试仪的信号发射器和信号接收器，打开电源。检测网线是否制作成功。如果检测不成功，找出失败原因并更正，直到成功为止。

1.6 实验总结

通过本次实验，应该了解网线制作和测试的方法，熟悉不同标准 RJ-45 连接器的线序。虽然本次实验只要求做直连网线，但也应该掌握交叉网线的制作方法，理解交叉线和直连线的不同应用范围及其原理。

实验2 网络设备的基本操作

1.1 实验内容与目标

- 使用 SecureCRT 软件登录设备
- 掌握基本系统操作命令的使用
- 掌握基本文件操作命令的使用
- 使用 FTP 上传下载文件

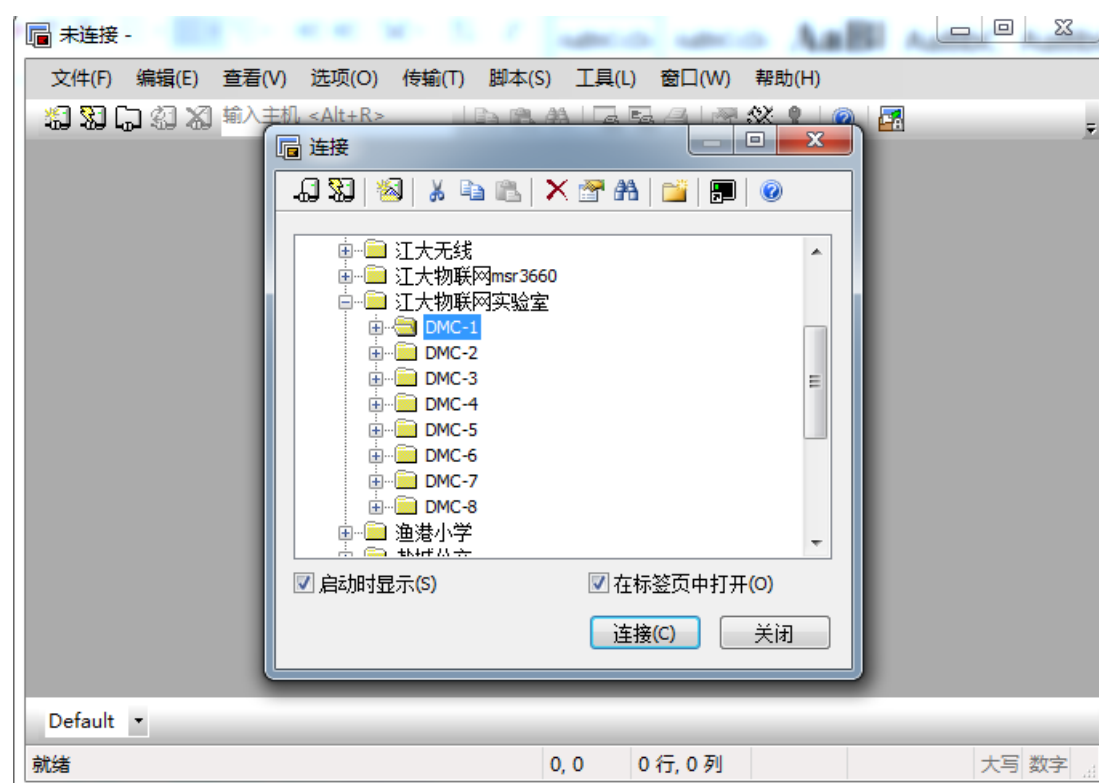
1.2 实验过程(以下均以第一组为例)

实验任务一：通过 SecureCRT 登录

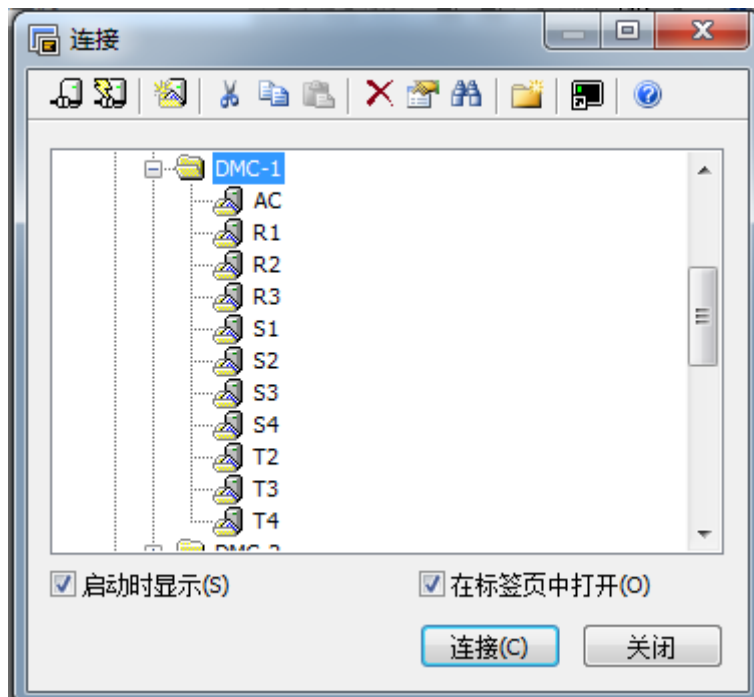
本实验的主要任务是熟悉并掌握通过 SecureCRT 连接进行设备配置的方法。

步骤一：启动 PC，运行 SecureCRT

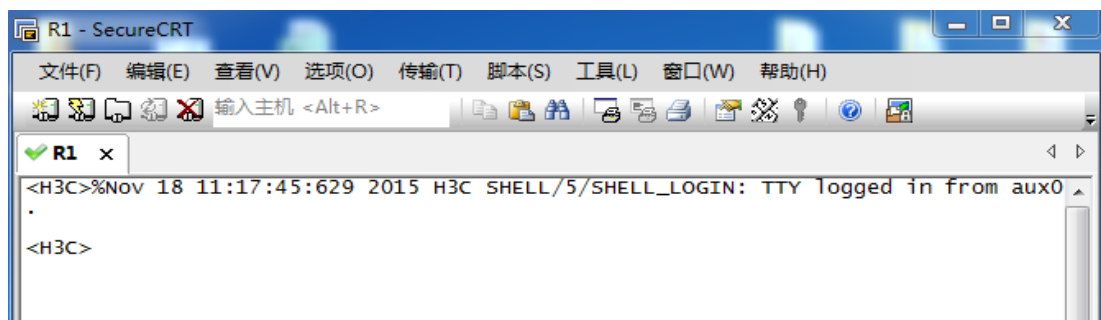
在 PC 桌面打开 SecureCRT



选择自己所在组，可以看到自己所在组中的设备（第一组：DMC-1/第二组：DMC-2/第三组：DMC-3/第四组：DMC-4/第五组：DMC-5/第六组：DMC-6/第七组：DMC-7/第八组：DMC-8）。



双击设备名称，按下回车键，进入设备配置界面。



实验任务二：使用系统操作及文件操作的基本命令

步骤一：进入系统视图

完成实验任务一时，配置界面处于用户视图下，此时执行 `system-view` 命令进入系统视图。

```
<H3C>system-view
```

System View: return to User View with Ctrl+Z.

```
[H3C]
```

此时提示符变为[***]形式，说明用户已经处于系统视图。

在系统视图下，执行 `quit` 命令可以从系统视图切换到用户视图。

```
[H3C]quit
```

```
<H3C>
```

步骤二：学习使用帮助特性和补全键

H3C Comware 平台支持对命令行的输入帮助和智能补全功能。

输入帮助特性：在输入命令时，如果忘记某一个命令的名称，可以在配置视图下仅输入该命令的前几个字符，然后键入 `<?>`，系统则会自动列车以刚才输入的前几个字符开头的所

有命令。当输入完一个命令时，也可以用<?>来查看紧随该命令的下一个命令参数。

```
[H3C]sys
```

```
[H3C]sysname
```

```
[H3C]sysname ?
```

```
TEXT Host name (1 to 64 characters)
```

智能补全功能：在输入命令时，不需要输入一条命令的全部字符，仅输入前几个字符，再键入 Tab 键，系统会自动补全该命令。如果有多个命令都具有相同的前缀字符的时候，连续键入 Tab，系统会在这几个命令之间切换。

步骤三：更改系统名称

使用 sysname 命令更改系统名称。

```
[H3C]sysname 1-R1
```

```
[1-R1]
```

步骤四：显示系统运行配置

使用 display current-configuration 命令显示系统当前运行的配置，由于使用的设备及模块不同，操作时显示的具体内容也会有所不同。在如下配置信息中，请注意查看刚刚配置的 sysname AHPTC 命令，同时请查阅接口信息，并与设备的实际接口和模块进行比对。

```
[1-R1]display cu
```

```
#
```

```
version 7.1.049, Release 0106P21
```

```
#
```

```
sysname 1-R1
```

```
#
```

```
password-recovery enable
```

```
#
```

```
vlan 1
```

```
#
```

```
controller Cellular0/0
```

```
#
```

```
controller Cellular0/1
```

```
#
```

```
interface Aux0
```

```
#
```

```
interface Serial1/0
```

```
#
```

```
interface Serial2/0
```

```
#
```

```
interface NULL0
```

```
#
```

```
interface GigabitEthernet0/0
```

```
port link-mode route
```

```
---- More ----
```

用空格键可以继续翻页显示，回车键进行翻行显示，或使用 Ctrl+C 结束显示。

步骤五：保存配置

使用 save 命令保存配置。

```
<1-R1>sa
```

The current configuration will be written to the device. Are you sure? [Y/N]:y

选择 Y，确定将当前运行配置写进设备存储介质中。

Please input the file name(*.cfg)[cfa0:/startup.cfg]

(To leave the existing filename unchanged, press the enter key):config.cfg

系统提示请输入保存配置文件的文件名，注意文件名的格式为*.cfg。该实验中系统默认将配置文件保存在 CF 卡中，保存后文件名为 config.cfg，如果不更改系统默认保存的文件名，请按回车键。

Validating file. Please wait...

Configuration is saved to device successfully.

这是第一次保存配置文件的过程。如果以后再次以 config.cfg 保存配置文件，则显示如下：

```
<1-R1>sa
```

The current configuration will be written to the device. Are you sure? [Y/N]:y

Please input the file name(*.cfg)[cfa0:/config.cfg]

(To leave the existing filename unchanged, press the enter key):config.cfg

cfa0:/config.cfg exists, overwrite? [Y/N]:y

Validating file. Please wait...

Configuration is saved to device successfully.

显示保存的配置：

```
<1-R1>display saved-configuration
```

```
#
```

```
version 7.1.049, Release 0106P21
```

```
#
```

```
sysname 1-R1
```

```
#
```

```
password-recovery enable
```

```
#
```

```
vlan 1
```

```
#
```

```
controller Cellular0/0
```

```
#
```

```
controller Cellular0/1
```

```
#
```

```
interface Aux0
```

```
#
```

```
interface Serial1/0
```

```
#
```

```
interface Serial2/0
```

```
#
```

```
interface NULL0
```

```
#
```

```
interface GigabitEthernet0/0
```

```

port link-mode route
combo enable copper
#
interface GigabitEthernet0/1
port link-mode route
#
interface GigabitEthernet0/2
port link-mode route
#
scheduler logfile size 16
#
line class aux
user-role network-admin
#
line class tty
user-role network-operator
#
line class vty
user-role network-operator
#
line aux 0
user-role network-admin
#
line vty 0 63
user-role network-operator
#
domain system
#
aaa session-limit ftp 32
aaa session-limit telnet 32
aaa session-limit http 32
aaa session-limit ssh 32
aaa session-limit https 32
domain default enable system
#
role name level-0
description Predefined level-0 role
#
role name level-1
description Predefined level-1 role
#
role name level-2
description Predefined level-2 role
#

```

```
role name level-3
  description Predefined level-3 role
#
role name level-4
  description Predefined level-4 role
#
role name level-5
  description Predefined level-5 role
#
role name level-6
  description Predefined level-6 role
#
role name level-7
  description Predefined level-7 role
#
role name level-8
  description Predefined level-8 role
#
role name level-9
  description Predefined level-9 role
#
role name level-10
  description Predefined level-10 role
#
role name level-11
  description Predefined level-11 role
#
role name level-12
  description Predefined level-12 role
#
role name level-13
  description Predefined level-13 role
#
role name level-14
  description Predefined level-14 role
#
user-group system
#
return
<1-R1>
```

由于执行了 save 命令，保存配置与运行配置一致。

抓取设备配置

打开 SecureCRT,文件—会话日志



选择文件保存目录---写入文件名---文件格式—保存



在 **SecureCRT** 中输入 display current-configuration 查看设备配置

```
[1-S1]display current-configuration
```

```
#
```

```
version 5.20, Release 2108P01
```

```
#
```

```
sysname 1-S1
```

```
#
```

```
super password level 3 cipher $c$3$uA83CZDXBuThiOojlrhpUujpAYq33g==
```

```
#
```

```
ftp server enable
```

```
#
```

```
irf mac-address persistent timer
```

```
irf auto-update enable
```

```
undo irf link-delay
```

```
#
```

```
domain default enable system
```

```
#
```

```
telnet server enable
```

```
#
```

```
dot1x
```

```
.....
```

再次打开 **SecureCRT**,文件—勾选取消会话日志



步骤六：删除和清空配置

当需要删除某条命令时，可以使用 `undo` 命令进行逐条删除。例如删除 `sysname` 命令后，系统名称恢复成 `H3C`。

```
[1-R1]undo sysname
```

```
[H3C]
```

当需要恢复到出厂默认配置时，首先在用户视图下执行 `reset saved-configuration` 命令用于清空保存配置（只是清除保存配置，当前配置还是存在的），

```
[1-R1]quit
```

```
<1-R1>reset saved-configuration
```

```
The saved configuration file will be erased. Are you sure? [Y/N]:y
```

```
Configuration file in cfa0: is being cleared.
```

```
Please wait ...
```

```
Configuration file is cleared.
```

执行 `reboot` 重启设备后，选择不保存已经正在运行的配置，即可恢复到出厂默认配置。

```
<1-R1> reboot
```

```
Start to check configuration with next startup configuration file, please wait.....DONE!
```

```
Current configuration may be lost after the reboot, save current configuration? [Y/N]:n
```

```
This command will reboot the device. Continue? [Y/N]:y
```

```
Now rebooting, please wait...
```

```
%Nov 18 12:38:07:017 2015 r2 DEV/5/SYSTEM_REBOOT: System is rebooting now.
```

```
System is starting...
```

步骤七：显示文件目录

使用 `dir` 命令显示 CF 卡上所有文件列表。

```
<1-S1>dir
```

```
Directory of flash:/
```

0	-rw-	287	Jan 01 2010 02:33:41	system.xml
1	-rw-	14384	Jan 01 2010 02:33:41	config.cwmp
2	-rw-	2503	Jan 01 2010 01:25:15	config.cfg
3	-rw-	352785	Jan 01 2010 01:29:46	logfile.log
4	-rw-	24876032	Aug 08 2008 20:00:00	s3600v2_e-cmw520-r2108p01.bin
5	drw-	-	Jan 01 2010 00:00:22	seclog

```
126592 KB total (100634 KB free)
```

使用 `more` 命令显示文本内容

```
<1-S1>more logfile/logfile.log
```

```
%@0%Jan 1 00:00:11 2010 H3C %%10IC/6/SYS_RESTART: System restarted --
```

```
H3C Comware Software.
```

```
%@1%Jan 1 00:01:01:705 2010 H3C IFNET/3/LINK_UPDOWN: Aux0/0/0 link status is UP.
```

```
%@2#Jan 1 00:01:10:840 2010 8-S1 DEVM/4/SYSTEM COLD START:
```


Trap 1.3.6.1.4.1.25506.6.8.4<hh3cSysColdStartTrap>: system cold start.

% @3#Jan 1 00:01:11:093 2010 8-S1 SHELL/4/LOGIN:

Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1<hh3cLogIn>: login from Console

% @4#Jan 1 00:01:11:194 2010 8-S1 SHELL/5/SHELL_LOGIN: Console logged in from aux0.

% @5#Jan 1 00:01:30:019 2010 8-S1 SHELL/6/SHELL_CMD: -Task=au0-IPAddr=**-User=**;
Command is display version

% @6#Jan 1 00:01:30:629 2010 8-S1 SHELL/6/SHELL_CMD: -Task=au0-IPAddr=**-User=**;
Command is q

% @7#Jan 1 00:01:31:209 2010 8-S1 SHELL/4/LOGOUT:

Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.2<hh3cLogOut>: logout from Console

% @8#Jan 1 00:01:31:210 2010 8-S1 SHELL/5/SHELL_LOGOUT: Console logged out from
aux0.

% @9#Jan 1 04:12:15:828 2010 8-S1 SHELL/4/LOGIN:

Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1<hh3cLogIn>: login from Console

实验任务三：通过 Telnet 登录交换机

交换机 Telnet (V5 版本)

PC----- (vlan-interface 1) 交换机

步骤一：配置交换机 Telnet 用户

<1-S1>sys

System View: return to User View with Ctrl+Z.

[1-S1]local-user test

New local user added..

为该用户创建登入时的认证密码，密码为 test。这里可以 password 命令指定密码显示方式。密码有两种显示方式，simple 指定以明文方式显示密码，cipher 则指定以密文方式显示密码。

[1-S1-luser-test]password simple test

设置该用户使用 telnet 服务类型，该用户的优先级 level 为 0（0 为访问级、1 为监控级、2 为系统级、3 为管理级，数值越小，用户的优先级越低）。

[1-S1-luser-test]service-type telnet

[[1-S1-luser-test] authorization-attribute level 3

查看该视图下配置的用户信息：

[1-S1-luser-test]dis this

#

local-user test

password cipher \$c\$3\$105BcQsK9kIYP6uuVJRWF3HbwRo0CO4=

authorization-attribute level 3

service-type telnet

#

return

[1-S1-luser-test]quit

[1-S1]

步骤二：配置 super 口令

Super 命令用来将用户从当前级别切换到指定级别。设置用户切换到 level 3 的密码为 H3C，密码明文显示。

```
[1-S1]super password level 3 simple H3C
```

步骤三：配置对 telnet 用户使用缺省的本地认证

进入 VTY 0~15 用户界面，系统支持 16 个 VTY 用户同时访问。VTY 口属于逻辑终端线，用于设备进行 telnet 或 SSH 访问。

```
[1-S1]user-interface vty 0 15
```

路由器可以采用本地或第三方服务器来对用户进行认证，这里使用本地认证授权方式（认证模式为 scheme）。

```
[1-S1-ui-vty0-15]authentication-mode scheme
```

```
[1-S1-ui-vty0-15]dis this
```

```
user-interface aux 0
```

```
user-interface vty 0 15
```

```
authentication-mode scheme
```

```
#
```

```
return
```

```
[1-S1-line-vty0-15]quit
```

```
[1-S1]
```

步骤四：打开 telnet 服务

```
[1-S1]telnet server enable
```

步骤五：进入接口视图，配置以太口和 PC 网卡地址

使用 interface 命令进入以太接口视图，使用 ip address 配置路由器以太口地址。

```
[1-S1]interface vlan-interface 1
```

```
[1-S1-Vlan-interface1]ip address 192.168.0.1 255.255.255.0
```

```
[1-S1-Vlan-interface1]dis ip interface brief
```

```
*down: administratively down
```

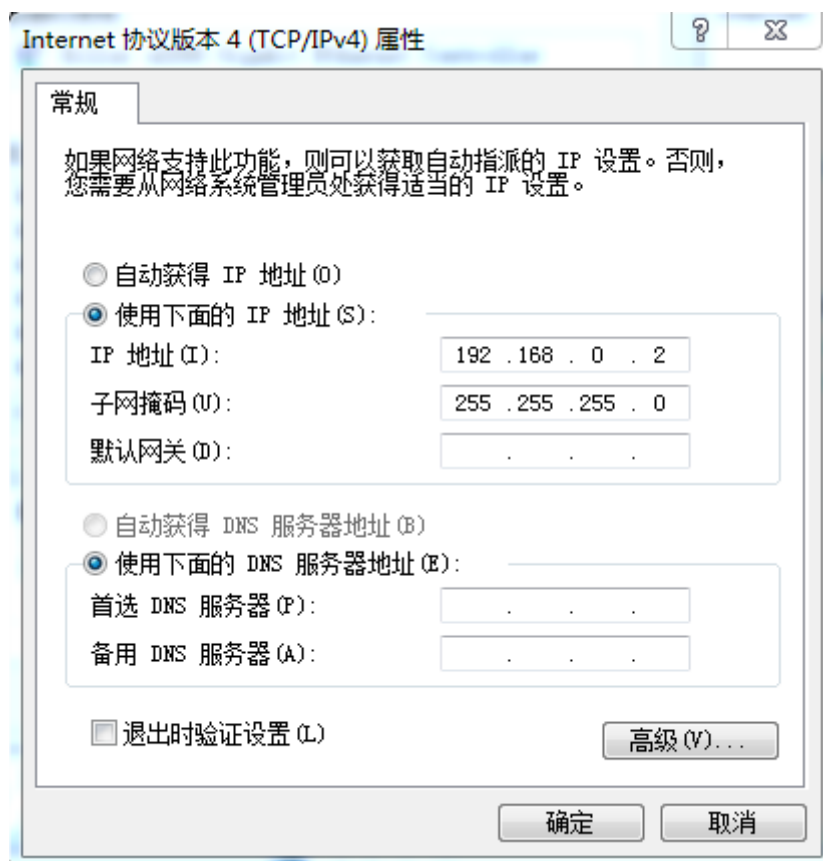
```
(s): spoofing
```

Interface	Physical	Protocol	IP Address	Description
Vlan1	up	up	192.168.0.1	Vlan-inte...

```
[1-S1-Vlan-interface1]quit
```

```
[1-S1]
```

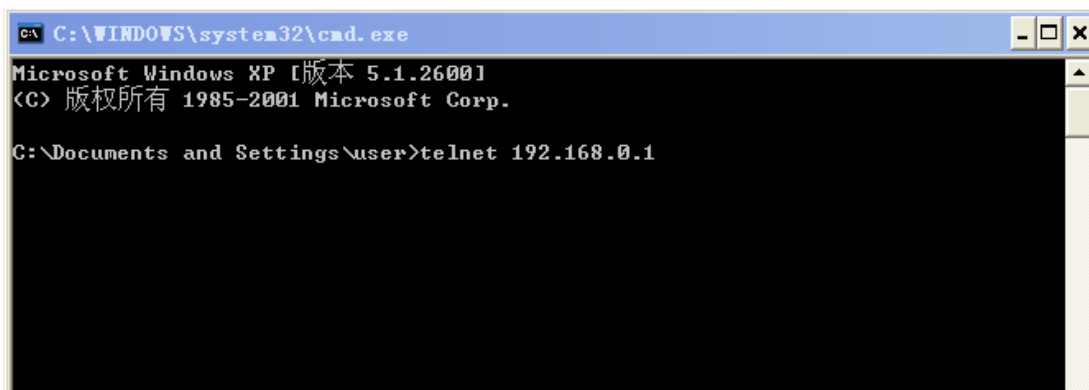
同时为 PC 配置一个与路由器接口相同网段的 IP 地址。



配置完成后，在 CRT 上能看到交换机接口 interface Vlan-interface1 自动 UP 的信息。

步骤六：使用 telnet 登录

使用网线连接 PC 和交换机相连，在 PC 命令窗口中，telnet 路由器的以太网 IP 地址，并回车。



输入 telnet 用户名（test）及口令（test），进入配置界面，使用?查看此时该用户权限下可使用的命令。此时登录用户级别处于管理级，可以看到并使用所有的命令。

```
C:\ Telnet 192.168.0.1
*****
Login authentication

Username:test
Password:
<1-S1>?
User view commands:
  archive      Specify archive settings
  backup       Backup next startup-configuration file to TFTP server
  boot-loader  Set boot loader
  bootrom      Update/read/backup/restore bootrom
  cd           Change current directory
  cfd          Connectivity fault detection (IEEE 802.1ag)
  clock        Specify the system clock
  cluster      Run cluster command
  copy         Copy from one file to another
```

步骤七：使用 super 命令切换管理权限

使用 super 命令查看权限

<1-S1> super 2

<1-S1> super 3

```
C:\ Telnet 192.168.0.1
*****
* Copyright (c) 2004-2013 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent,                               *
* no decompiling or reverse-engineering shall be allowed.                  *
*****

Login authentication

Username:test
Password:
<1-S1>su
<1-S1>super 2
User privilege level is 2, and only those commands can be used
whose level is equal or less than this.
Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
<1-S1>su
<1-S1>super 3
Please input the password to change the privilege level. Press CTRL_C to abort.
Password:
User privilege level is 3, and only those commands can be used
whose level is equal or less than this.
Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
<1-S1>
```

步骤八：清空配置，重新启动

先使用 reset saved-configuration 清空配置，再使用 reboot 命令重新启动系统。

实验任务四：通过 Telnet 登录路由器

路由器 Telnet (V7 版本)

PC----- (g0/1) 路由器

步骤一：配置路由器 Telnet 用户

```
<1-R1>sys
```

System View: return to User View with Ctrl+Z.

```
[1-R1]local-user test
```

New local user added.

为该用户创建登入时的认证密码，密码为 test。这里可以 password 命令指定密码显示方式。密码有两种显示方式，simple 指定以明文方式显示密码，cipher 则指定以密文方式显示密码。

```
[1-R1-luser-manage-test]password simple test
```

设置该用户使用 telnet 服务类型，该用户的优先级 level 为 0（0 为访问级、1 为监控级、2 为系统级、3 为管理级，数值越小，用户的优先级越低）。

```
[1-R1-luser-manage-test]service-type telnet
```

```
[1-R1-luser-manage-test]authorization-attribute user-role ?
```

```
[1-R1-luser-manage-test]authorization-attribute user-role network-admin
```

```
[1-R1-luser-manage-test]dis this
```

```
#
```

```
local-user test
```

```
password
```

hash

```
$h$6$SjHrmuf8qBUv8gwy$x5zBoBxY0Y9ELflgTR0Xnhg+9owIo+xr3q4gpkWAg91kisETTMwzdp/c1o1ah0RfiS8rE+LRakxLcf6EqsOFew==
```

```
authorization-attribute user-role network-admin
```

```
#
```

```
[1-R1-luser-manage-test]quit
```

```
[1-R1]
```

步骤二：配置 super 口令

Super 命令用来将用户从当前级别切换到指定级别。设置用户切换到 level 3 的密码为 H3C，密码明文显示。

```
[1-R1]super password role network-admin simple H3C
```

```
[1-R1]super password role level-10 simple H3C10
```

步骤三：配置对 telnet 用户使用缺省的本地认证

进入 VTY 0~15 用户界面，系统支持 16 个 VTY 用户同时访问。VTY 口属于逻辑终端线，用于设备进行 telnet 或 SSH 访问。

```
[1-R1] line vty 0 63
```

路由器可以采用本地或第三方服务器来对用户进行认证，这里使用本地认证授权方式（认证模式为 scheme）。

```
[1-R1-line-vty0-63]authentication-mode scheme
```

```
[1-R1-line-vty0-63]dis this
```

```
#
line aux 0
  user-role network-admin
#
line vty 0 63
  authentication-mode scheme
  user-role network-operator
#
return
[1-R1-line-vty0-63]quit
[1-R1]
```

步骤四：打开 telnet 服务

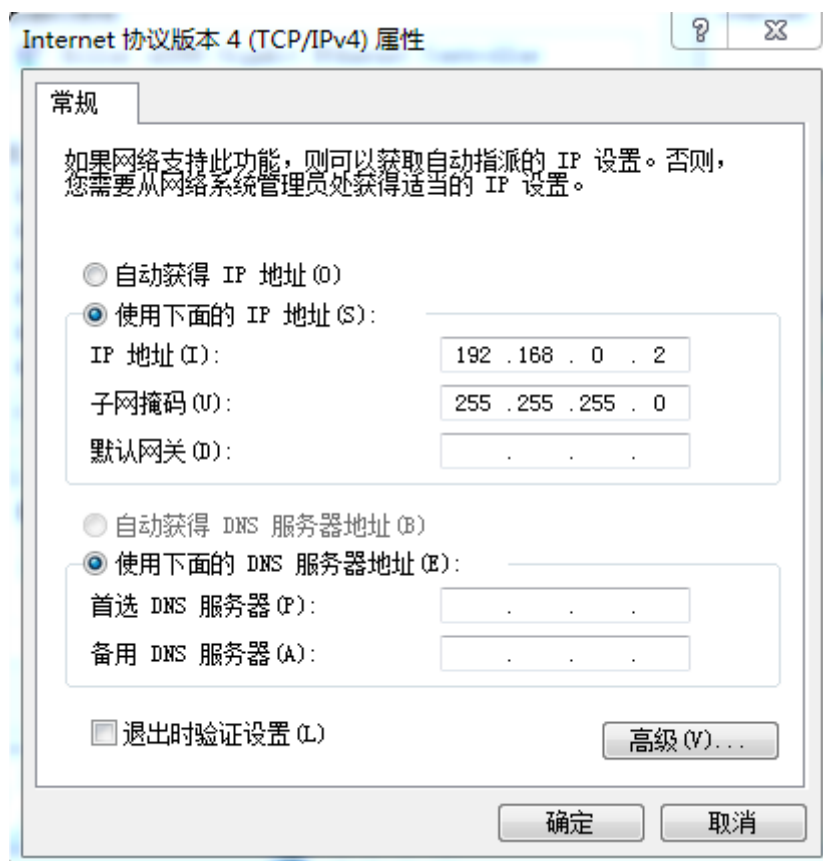
```
[1-R1]telnet server enable
% Start Telnet server
```

步骤五：进入接口视图，配置以太网口和 PC 网卡地址

使用 interface 命令进入以太网接口视图，使用 ip address 配置路由器以太网口地址。

```
[1-R1]interface GigabitEthernet 0/1
[1-R1-GigabitEthernet0/1]ip address 192.168.0.1 255.255.255.0
[1-R1-GigabitEthernet0/1]dis this
#
interface GigabitEthernet0/1
  port link-mode route
  ip address 192.168.0.1 255.255.255.0
#
return
[1-R1-GigabitEthernet0/1]quit
[1-R1]
```

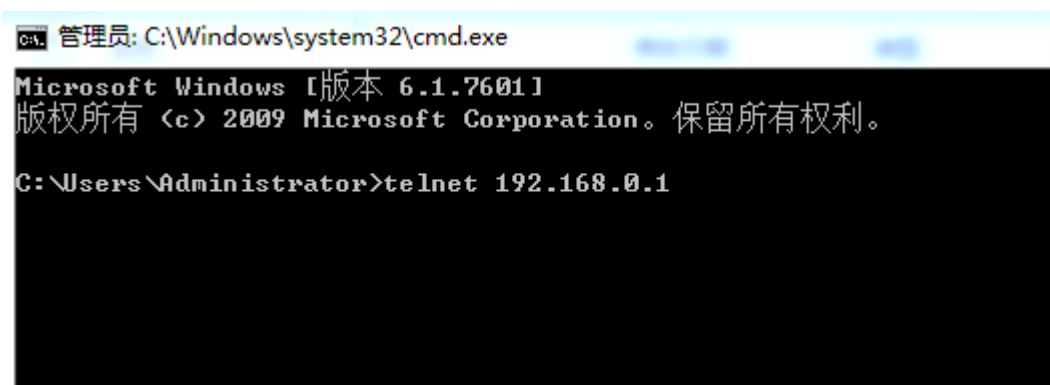
同时为 PC 配置一个与路由器接口相同网段的 IP 地址。



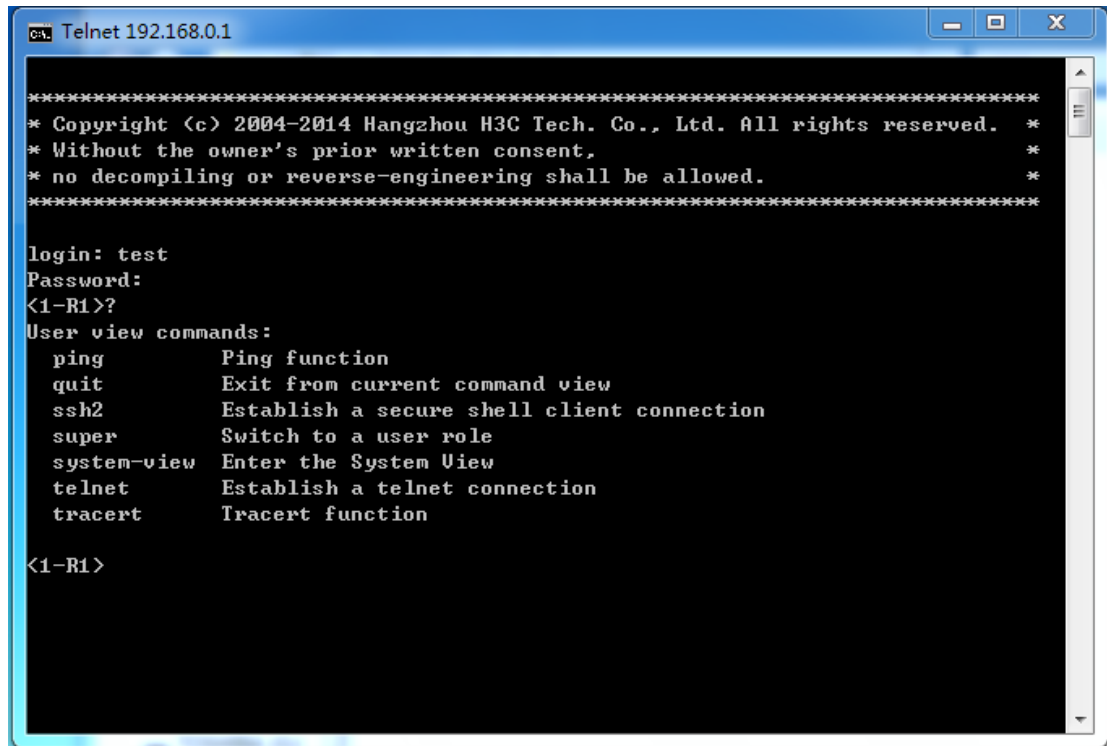
配置完成后，在 CRT 上能看到路由器接口 GigabitEthernet 0/1 自动 UP 的信息。

步骤六：使用 telnet 登录

使用交叉网线连接 PC 和路由器的以太网口 GigabitEthernet 0/1，在 PC 命令窗口中，telnet 路由器的以太网口 IP 地址，并回车。



输入 telnet 用户名及口令，进入配置界面，使用?查看此时该用户权限下可使用的命令。由于此时登录用户级别处于访问级，所以只能看到并使用有限的几个命令。



```
C:\> Telnet 192.168.0.1

*****
* Copyright (c) 2004-2014 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent,                               *
* no decompiling or reverse-engineering shall be allowed.                 *
*****

login: test
Password:
<1-R1>?
User view commands:
  ping      Ping function
  quit      Exit from current command view
  ssh2      Establish a secure shell client connection
  super      Switch to a user role
  system-view Enter the System View
  telnet    Establish a telnet connection
  tracert   Tracert function

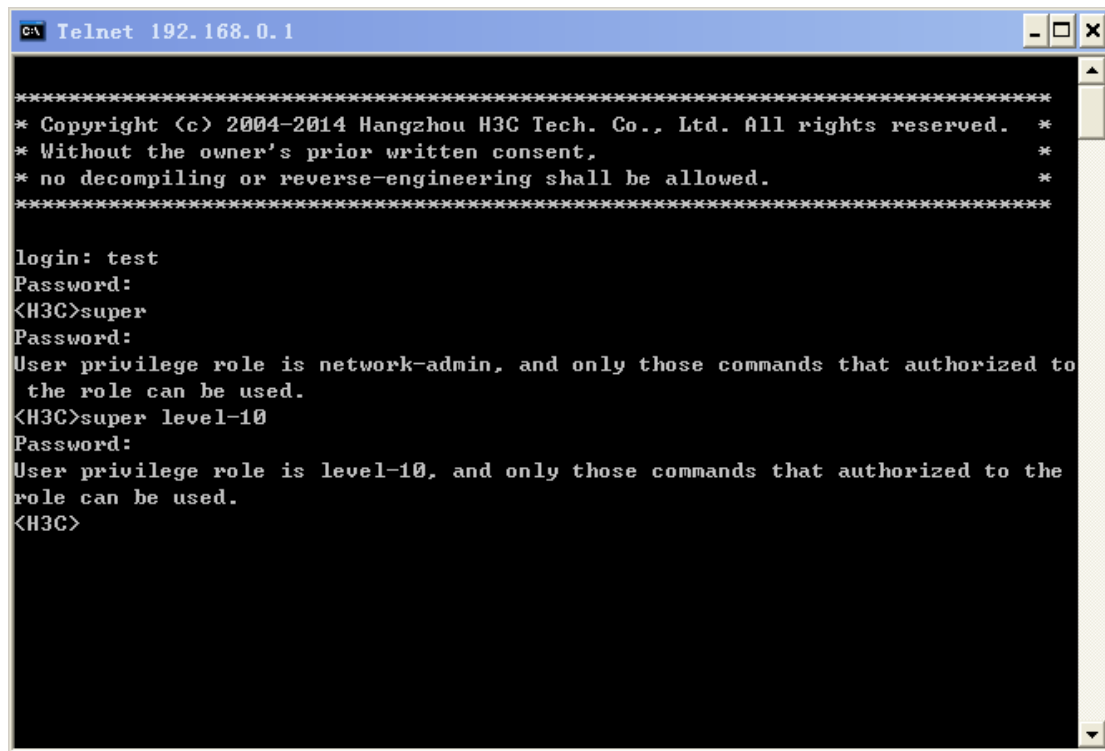
<1-R1>
```

步骤七：使用 super 命令切换管理权限

使用 super 命令查看权限

<1-R1> super

<1-R1> super level-10



```
C:\> Telnet 192.168.0.1

*****
* Copyright (c) 2004-2014 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent,                               *
* no decompiling or reverse-engineering shall be allowed.                 *
*****

login: test
Password:
<H3C>super
Password:
User privilege role is network-admin, and only those commands that authorized to
the role can be used.
<H3C>super level-10
Password:
User privilege role is level-10, and only those commands that authorized to the
role can be used.
<H3C>
```

步骤八：清空配置，重新启动

先使用 `reset saved-configuration` 清空配置，再使用 `reboot` 命令重新启动系统。

实验任务五：配置交换机 FTP 服务

步骤一：通过 console 口配置 FTP 用户

```
[1-S1]local-user ftp
[1-S1-luser-ftp]password simple ftp
[1-S1-luser-ftp]service-type ftp
设置该用户使用 FTP 服务类型，并设置该用户的优先级 level 为管理员
[1-S1-luser-ftp] authorization-attribute level 3
[1-S1-luser-ftp]dis local-user user-name ftp
The contents of local user ftp:
State: Active
ServiceType: ftp
Access-limit: Disabled Current AccessNum: 0
User-group: system
Bind attributes:
Authorization attributes:
security audit is configured
Total 1 local user(s) matched.
[1-S1-luser-ftp]
[1-S1-luser-ftp]quit
[1-S1]
```

步骤二：打开 FTP 服务

```
[1-S1]ftp server enable
```

步骤三：进入接口视图，配置以太口和 PC 网卡地址

使用 `interface` 命令进入以太接口视图，使用 `ip address` 配置路由器以太口地址。

```
[1-S1]interface vlan-interface 1
[1-S1-Vlan-interface1]ip address 192.168.0.1 255.255.255.0
[1-S1]dis ip interface brief
*down: administratively down
(s): spoofing


| Interface | Physical | Protocol | IP Address  | Description  |
|-----------|----------|----------|-------------|--------------|
| Vlan1     | up       | up       | 192.168.0.1 | Vlan-inte... |


[1-S1-Vlan-interface1]quit
[1-S1]
```

同时为 PC 配置一个与路由器接口相同网段的 IP 地址。

步骤四：使用 FTP 登录

使用网线连接 PC 和交换机，在 PC 命令行窗口中，FTP 路由器的以太口 IP 地址，并回车。

输入 FTP 用户名及口令:

```
C:\WINDOWS\system32\cmd.exe - ftp 192.168.0.1
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\user>ftp 192.168.0.1
Connected to 192.168.0.1.
220 FTP service ready.
User <192.168.0.1:(none)>: ftp
331 Password required for ftp.
Password:
230 User logged in.
ftp>
```

步骤五：使用 FTP 下载文件

get logfile.log

使用 FTP 中的 get 命令下载配置文件到本地目录 “C:\Documents and Settings\user”

```
C:\WINDOWS\system32\cmd.exe - ftp 192.168.0.1
Connected to 192.168.0.1.
220 FTP service ready.
User <192.168.0.1:(none)>: ftp
331 Password required for ftp.
Password:
230 User logged in.
ftp> dir
200 Port command okay.
150 Opening ASCII mode data connection for /*.
-rwxrwxrwx 1 noone nogroup 0 Jan 01 03:07 test.txt
-rwxrwxrwx 1 noone nogroup 2016 Jan 01 00:04 config.cfg
-rwxrwxrwx 1 noone nogroup 287 Jan 01 00:03 system.xml
-rwxrwxrwx 1 noone nogroup 6461 Jan 01 00:03 config.cwmp
-rwxrwxrwx 1 noone nogroup 37530 Jan 01 07:52 logfile.log
-rwxrwxrwx 1 noone nogroup 24876032 Aug 08 2008 s3600v2_e-cmw520-r2108p01
.bin
drwxrwxrwx 1 noone nogroup 0 Jan 01 00:00 seclog
226 Transfer complete.
ftp: 收到 484 字节, 用时 0.03Seconds 15.61Kbytes/sec.
ftp> get logfile.log
200 Port command okay.
150 Opening ASCII mode data connection for /logfile.log.
226 Transfer complete.
ftp: 收到 37530 字节, 用时 0.09Seconds 399.26Kbytes/sec.
ftp>
```

步骤六：清空配置，重新启动

实验任务六：配置路由器 FTP 服务

步骤一：通过 console 口配置 FTP 用户

[1-R1]local-user ftp

[1-R1-luser-manage-ftp]password simple ftp

```
[1-R1-luser-manage-ftp]service-type ftp
设置该用户使用 FTP 服务类型，并设置该用户的优先级 level 为管理员
[1-R1-luser-manage-ftp]authorization-attribute user-role network-admin
[1-R1]dis local-user
Total 1 local users matched.

Device management user ftp:
State: Active
Service type: None
User group: system
Bind attributes:
Authorization attributes:
Work directory: cfa0:
User role list: network-admin, network-operator [1-S1-luser-ftp]
[1-R1-luser-ftp]quit
[1-R1]
```

步骤二：打开 FTP 服务

```
[1-R1]ftp server enable
```

步骤三：进入接口视图，配置以太口和 PC 网卡地址

使用 interface 命令进入以太接口视图，使用 ip address 配置路由器以太口地址。

```
[1-R1]interface GigabitEthernet 0/1
[1-R1-GigabitEthernet0/1]ip address 192.168.0.1 255.255.255.0
[1-R1-GigabitEthernet0/1]dis this
#
interface GigabitEthernet0/1
port link-mode route
ip address 192.168.0.1 255.255.255.0
#
return
```

```
[1-R1-GigabitEthernet0/1]dis ip interface brief
```

*down: administratively down

(s): spoofing (l): loopback

Interface	Physical	Protocol	IP Address	Description
Aux0	up	down	--	--
GE0/0	down	down	--	--
GE0/1	up	up	192.168.0.1	--
GE0/2	down	down	--	--
S1/0	up	up	--	--
S2/0	down	down	--	--

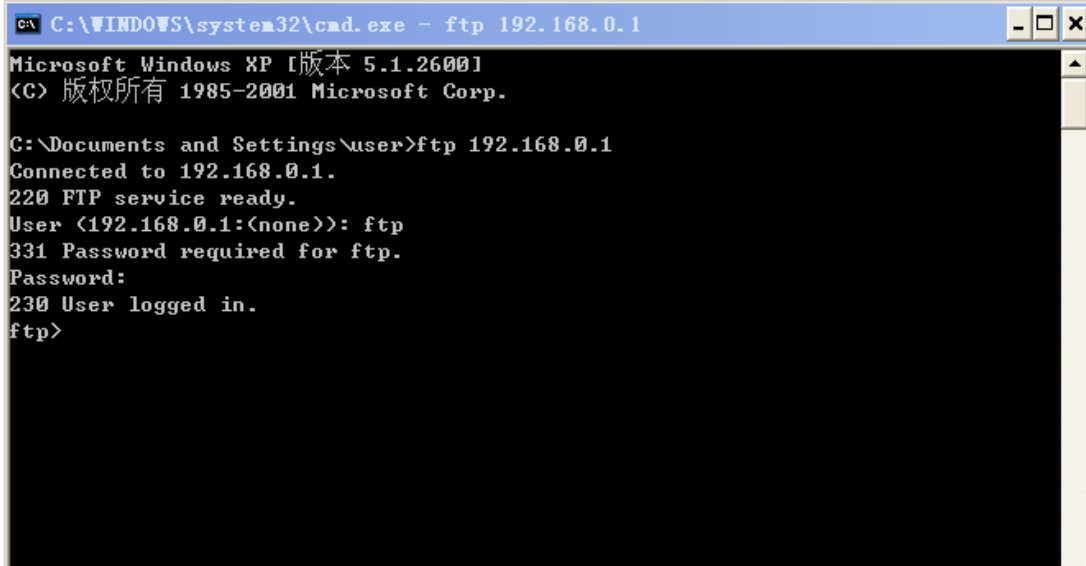
```
[1-R1-GigabitEthernet0/1]quit
```

[1-R1]同时为 PC 配置一个与路由器接口相同网段的 IP 地址。

步骤四：使用 FTP 登录

使用交叉网线连接 PC 和路由器的以太网口，在 PC 命令行窗口中，FTP 路由器的以太网口 IP 地址，并回车。

输入 FTP 用户名及口令：



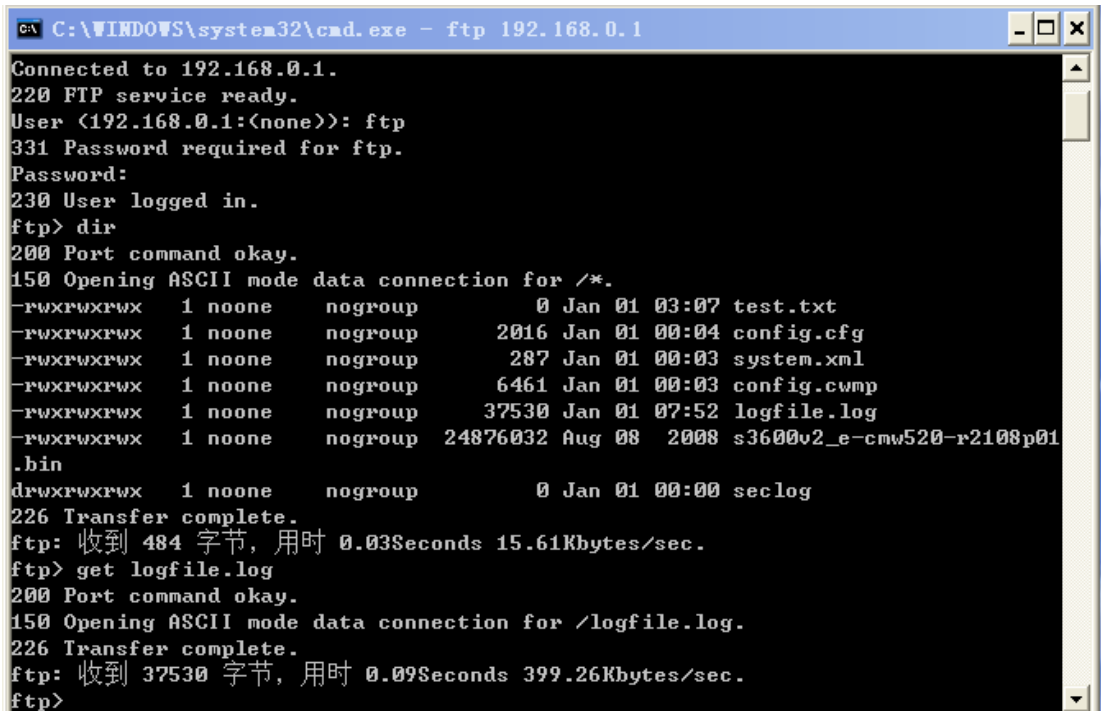
```
C:\WINDOWS\system32\cmd.exe - ftp 192.168.0.1
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\user>ftp 192.168.0.1
Connected to 192.168.0.1.
220 FTP service ready.
User (192.168.0.1:(none)): ftp
331 Password required for ftp.
Password:
230 User logged in.
ftp>
```

步骤五：使用 FTP 下载文件

get logfile.log 用于下载文件

使用 FTP 中的 get 命令下载配置文件到本地目录 “C:\Documents and Settings\user”



```
C:\WINDOWS\system32\cmd.exe - ftp 192.168.0.1
Connected to 192.168.0.1.
220 FTP service ready.
User (192.168.0.1:(none)): ftp
331 Password required for ftp.
Password:
230 User logged in.
ftp> dir
200 Port command okay.
150 Opening ASCII mode data connection for /*.
-rwxrwxrwx 1 noone nogroup 0 Jan 01 03:07 test.txt
-rwxrwxrwx 1 noone nogroup 2016 Jan 01 00:04 config.cfg
-rwxrwxrwx 1 noone nogroup 287 Jan 01 00:03 system.xml
-rwxrwxrwx 1 noone nogroup 6461 Jan 01 00:03 config.cwmp
-rwxrwxrwx 1 noone nogroup 37530 Jan 01 07:52 logfile.log
-rwxrwxrwx 1 noone nogroup 24876032 Aug 08 2008 s3600v2_e-cmw520-r2108p01
.bin
drwxrwxrwx 1 noone nogroup 0 Jan 01 00:00 seclog
226 Transfer complete.
ftp: 收到 484 字节, 用时 0.03Seconds 15.61Kbytes/sec.
ftp> get logfile.log
200 Port command okay.
150 Opening ASCII mode data connection for /logfile.log.
226 Transfer complete.
ftp: 收到 37530 字节, 用时 0.09Seconds 399.26Kbytes/sec.
ftp>
```

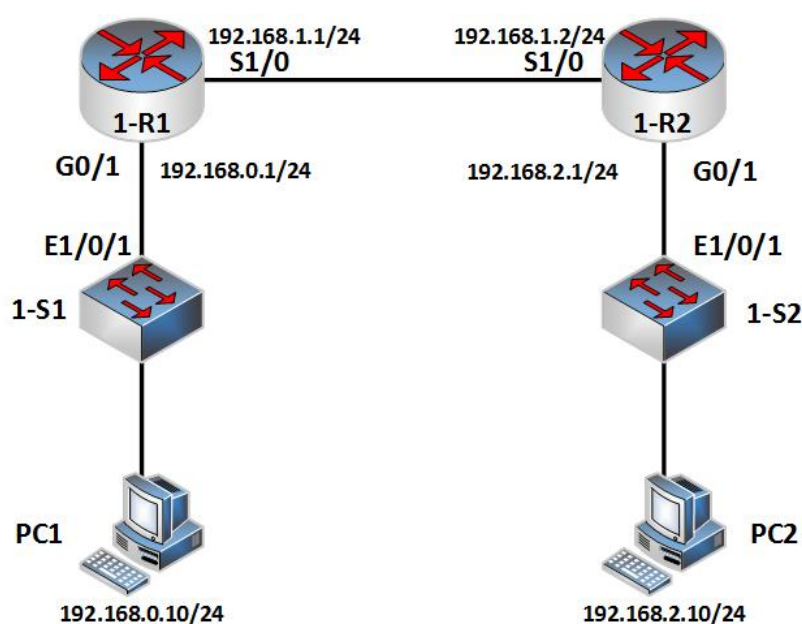
步骤六：清空配置，重新启动

实验3 基础网络构建与诊断

2.1 实验内容与目标

- 掌握路由器通过串口相连的基本方法
- 掌握 ping、tracert 系统连通检测的使用方法
- 掌握 debug 命令的使用方法

2.2 实验组图



2.3 实验过程

实验任务一：搭建基本连接环境

本实验任务供学员熟悉并掌握路由器、交换机、PC 的基本网络连接配置。

步骤一：完成 PC、交换机、路由器互连

在教师指导下，完成 2 台路由器通过串口电缆背靠背相连；路由器以太网口分别下接一台交换机；PC 通过网线连接到交换机端口上。

步骤二：配置 IP 地址

将所有设备的配置清空重启开始下面的配置。

使用 ip address 命令配置路由器的串口和以太网 IP 地址。

1-R1 的配置如下

```
[H3C]sysname 1-R1
```

```
[1-R1]interface GigabitEthernet 0/1
[1-R1-GigabitEthernet0/1]ip add 192.168.0.1 24
[1-R1-GigabitEthernet0/1]quit
[1-R1]interface Serial 1/0
[1-R1-Serial1/0]ip ad 192.168.1.1 24
[1-R1-Serial1/0]dis ip interface brief
*down: administratively down
(s): spoofing (l): loopback
```

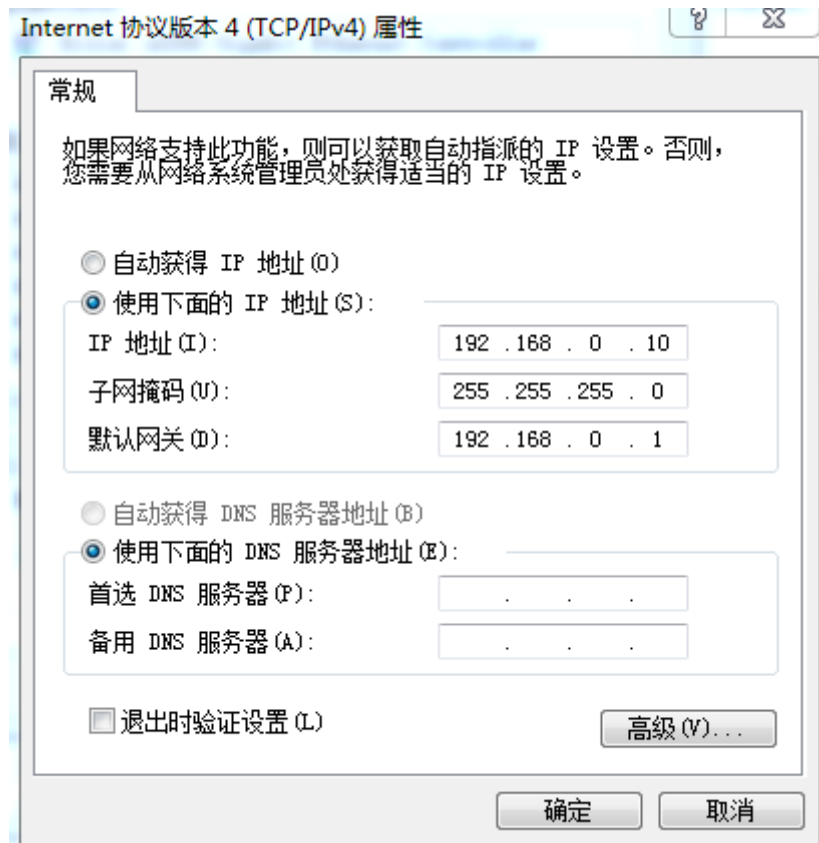
Interface	Physical	Protocol	IP Address	Description
Aux0	up	down	--	--
GE0/0	down	down	--	--
GE0/1	up	up	192.168.0.1	--
GE0/2	down	down	--	--
S1/0	up	up	192.168.1.1	--
S2/0	up	up	--	--

1-R2 的配置如下

```
[H3C]sysname 1-R2
[1-R2]interface GigabitEthernet 0/1
[1-R2-GigabitEthernet0/1]ip add 192.168.2.1 24
[1-R2-GigabitEthernet0/1]quit
[1-R2]interface Serial 1/0
[1-R2-Serial1/0]ip ad 192.168.1.2 24
[1-R2-Serial1/0]dis ip interface brief
*down: administratively down
(s): spoofing (l): loopback
```

Interface	Physical	Protocol	IP Address	Description
Aux0	up	down	--	--
GE0/0	down	down	--	--
GE0/1	up	up	192.168.2.1	--
GE0/2	down	down	--	--
S1/0	up	up	192.168.1.2	--
S2/0	up	up	--	--

PC1 的网络 IP 地址设置如下：



PC1 通过二层交换机连接到路由器接口 G0/1，那么 PC1 的网关地址应该设置为路由器的接口 G0/1 的 IP 地址。

PC2 的网络 IP 地址设置如下：

IP 地址：192.168.2.10

子网掩码：255.255.255.0

默认网关：192.168.2.1

实验任务二：使用 ping 命令检查连通性

步骤一：1-R1 ping 1-R2

通过 CRT 登入到 1-R1 后，ping 1-R2 的串口 S1/0，检查路由器之间串口的连通性。

```
[1-R1]ping 192.168.1.2
```

```
Ping 192.168.1.2 (192.168.1.2): 56 data bytes, press CTRL_C to break
```

```
56 bytes from 192.168.1.2: icmp_seq=0 ttl=255 time=24.353 ms
```

```
56 bytes from 192.168.1.2: icmp_seq=1 ttl=255 time=24.191 ms
```

```
56 bytes from 192.168.1.2: icmp_seq=2 ttl=255 time=24.072 ms
```

```
56 bytes from 192.168.1.2: icmp_seq=3 ttl=255 time=24.080 ms
```

```
56 bytes from 192.168.1.2: icmp_seq=4 ttl=255 time=24.239 ms
```

```
--- Ping statistics for 192.168.1.2 ---
```

```
5 packets transmitted, 5 packets received, 0.0% packet loss
```

round-trip min/avg/max/std-dev = 24.072/24.187/24.353/0.105 ms

[1-R1]%Nov 26 11:23:55:174 2015 1-R1 PING/6/PING_STATISTICS: Ping statistics for 192.168.1.2: 5 packets transmitted, 5 packets received, 0.0% packet loss, round-trip min/avg/max/std-dev = 24.072/24.187/24.353/0.105 ms.

结果显示，1-R1 收到 ICMP 的 echo reply 报文，1-R2 可以 ping 通 1-R2。反之亦然。

查看路由器 ping 命令携带的参数：

<1-R1>ping ?

-a	Specify the source IP address
-c	Specify the number of echo requests
-f	Specify packets not to be fragmented
-h	Specify the TTL value
-i	Specify an outgoing interface
-m	Specify the interval for sending echo requests
-n	Numeric output only. No attempt will be made to lookup host addresses for symbolic names
-p	No more than 8 "pad" hexadecimal characters to fill out the sent packet. For example, -p f2 will fill the sent packet with 000000f2 repeatedly
-q	Display only summary
-r	Record route. Include the RECORD_ROUTE option in the ECHO_REQUEST packets and display the route
-s	Specify the payload length
-t	Specify the wait time for each reply
-topology	Specify a topology
-tos	Specify the TOS value
-v	Display the received ICMP packets other than ECHO-RESPONSE packets
-vpn-instance	Specify a VPN instance
STRING<1-253>	IP address or hostname of remote system
ip	IP information
ipv6	IPv6 information

例如，可以使用参数-c 来设定发送 50 个 ping 报文：

<1-R1>ping -c 50 192.168.1.2

Ping 192.168.1.2 (192.168.1.2): 56 data bytes, press CTRL_C to break

56 bytes from 192.168.1.2: icmp_seq=0 ttl=255 time=24.366 ms

56 bytes from 192.168.1.2: icmp_seq=1 ttl=255 time=24.253 ms

.....

56 bytes from 192.168.1.2: icmp_seq=48 ttl=255 time=23.972 ms

56 bytes from 192.168.1.2: icmp_seq=49 ttl=255 time=24.114 ms

--- Ping statistics for 192.168.1.2 ---

50 packets transmitted, 50 packets received, 0.0% packet loss


```
round-trip min/avg/max/std-dev = 23.969/24.125/24.366/0.083 ms
<1-R1>%Nov 26 14:20:51:900 2015 1-R1 PING/6/PING_STATISTICS: Ping statistics for
192.168.1.2: 50 packets transmitted, 50 packets received, 0.0% packet loss, round-trip
min/avg/max/std-dev = 23.969/24.125/24.366/0.083 ms.
```

可以使用-s 参数来设定发送 ping 报文的字节为 512bytes:

```
<1-R1>ping -s 512 192.168.1.2
Ping 192.168.1.2 (192.168.1.2): 512 data bytes, press CTRL_C to break
512 bytes from 192.168.1.2: icmp_seq=0 ttl=255 time=140.351 ms
512 bytes from 192.168.1.2: icmp_seq=1 ttl=255 time=140.005 ms
512 bytes from 192.168.1.2: icmp_seq=2 ttl=255 time=140.175 ms
512 bytes from 192.168.1.2: icmp_seq=3 ttl=255 time=140.231 ms
512 bytes from 192.168.1.2: icmp_seq=4 ttl=255 time=140.237 ms

--- Ping statistics for 192.168.1.2 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 140.005/140.200/140.351/0.113 ms
<1-R1>%Nov 26 14:23:12:805 2015 1-R1 PING/6/PING_STATISTICS: Ping statistics for
192.168.1.2: 5 packets transmitted, 5 packets received, 0.0% packet loss, round-trip
min/avg/max/std-dev = 140.005/140.200/140.351/0.113 ms.
```

也可以使用参数-a 来设定 ping 报文的源地址，在网络调试中常常使用加源地址 ping 来检查网络的连通性。这里使用 1-R1 接口 S1/0 地址为源地址，ping 1-R2 S1/0:

```
<1-R1>ping -a 192.168.1.1 192.168.1.2
Ping 192.168.1.2 (192.168.1.2) from 192.168.1.1: 56 data bytes, press CTRL_C to break
56 bytes from 192.168.1.2: icmp_seq=0 ttl=255 time=24.279 ms
56 bytes from 192.168.1.2: icmp_seq=1 ttl=255 time=23.975 ms
56 bytes from 192.168.1.2: icmp_seq=2 ttl=255 time=24.217 ms
56 bytes from 192.168.1.2: icmp_seq=3 ttl=255 time=24.113 ms
56 bytes from 192.168.1.2: icmp_seq=4 ttl=255 time=24.264 ms

--- Ping statistics for 192.168.1.2 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 23.975/24.170/24.279/0.113 ms
<1-R1>%Nov 26 14:24:07:687 2015 1-R1 PING/6/PING_STATISTICS: Ping statistics for
192.168.1.2: 5 packets transmitted, 5 packets received, 0.0% packet loss, round-trip
min/avg/max/std-dev = 23.975/24.170/24.279/0.113 ms.
加源地址 ping 时，只能使用设备自身的本地接口地址。
```

步骤二：PC1 ping 1-R1

进入 PC1 命令行窗口，ping 1-R1 的 G0/1 口和 S1/0 口地址。

```
管理员: C:\Windows\system32\cmd.exe

Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\user>ping 192.168.0.1

正在 Ping 192.168.0.1 具有 32 字节的数据:
来自 192.168.0.1 的回复: 字节=32 时间<1ms TTL=255
来自 192.168.0.1 的回复: 字节=32 时间<1ms TTL=255
来自 192.168.0.1 的回复: 字节=32 时间<1ms TTL=255
来自 192.168.0.1 的回复: 字节=32 时间<1ms TTL=255

192.168.0.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\user>ping 192.168.1.1

正在 Ping 192.168.1.1 具有 32 字节的数据:
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=255

192.168.1.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\user>
```

步骤三: PC1 ping PC2

进入 PC1 命令行窗口, ping PC2 的 IP 地址。

```
C:\Windows\system32\cmd.exe

C:\Users\user>ping 192.168.2.10

正在 Ping 192.168.2.10 具有 32 字节的数据:
来自 192.168.0.10 的回复: 无法访问目标主机。
来自 192.168.0.10 的回复: 无法访问目标主机。
来自 192.168.0.10 的回复: 无法访问目标主机。
来自 192.168.0.10 的回复: 无法访问目标主机。

192.168.2.10 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),

C:\Users\user>
```

结果显示, PC1 无法 ping 通 PC2 的 IP 地址。这是为什么呢?

让我们一步一步来排查为什么 ping 不通

首先，PC1 ping 1-R1 的 G0/1 和 S1/0 口，结果显示可以 ping 通。

其次，PC1 ping 1-R2 的 S1/0 口，结果显示无法 ping 通。

最后，PC1 ping PC2，结果显示无法 ping 通。结果证明，由于 PC1 发送给 1-R2 和 PC2 的 ICMP 请求报文（echo request），没有收到回应报文（echo reply）。

在 1-R1 上使用 display ip routing-table 命令查看一下 1-R1 的路由表：

[1-R1]display ip routing-table

Destinations : 17

Routes : 17

Destination/Mask	Proto	Pre Cost		NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.0/24	Direct	0	0	192.168.0.1	GE0/1
192.168.0.0/32	Direct	0	0	192.168.0.1	GE0/1
192.168.0.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.255/32	Direct	0	0	192.168.0.1	GE0/1
192.168.1.0/24	Direct	0	0	192.168.1.1	S1/0
192.168.1.0/32	Direct	0	0	192.168.1.1	S1/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	S1/0
192.168.1.255/32	Direct	0	0	192.168.1.1	S1/0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

在路由表 destination 项中，没有看到 192.168.2.0 表项，所以 1-R1 当收到 PC1 发送给 PC2 的 ping 报文后，不知道如何转发，会丢弃该报文。结果就是 PC1 无法 ping 通 PC2。

但是在路由表中，有具体路由表项 192.168.1.2，为什么 PC1 无法 ping 通 1-R2 的串口呢？因为 1-R2 的路由表项中没有 192.168.0.0 表项，所以虽然 1-R1 将 PC1 ping 请求报文发送给 1-R2，但是 1-R2 不知道如何转发 ping 的回应报文给 PC1。所以，PC1 也无法 ping 通 1-R2 的串口。

步骤四：配置静态路由

使用 ip route-static 命令分别在路由器 1-R1 和 1-R2 上配置静态路由，目的网段为对端路由器与 PC 的互连网段，并将路由下一跳指向对端路由器的接口地址：

1-R1 上配置：

```
[1-R1]ip route-static 192.168.2.0 255.255.255.0 192.168.1.2
```

1-R2 上配置：

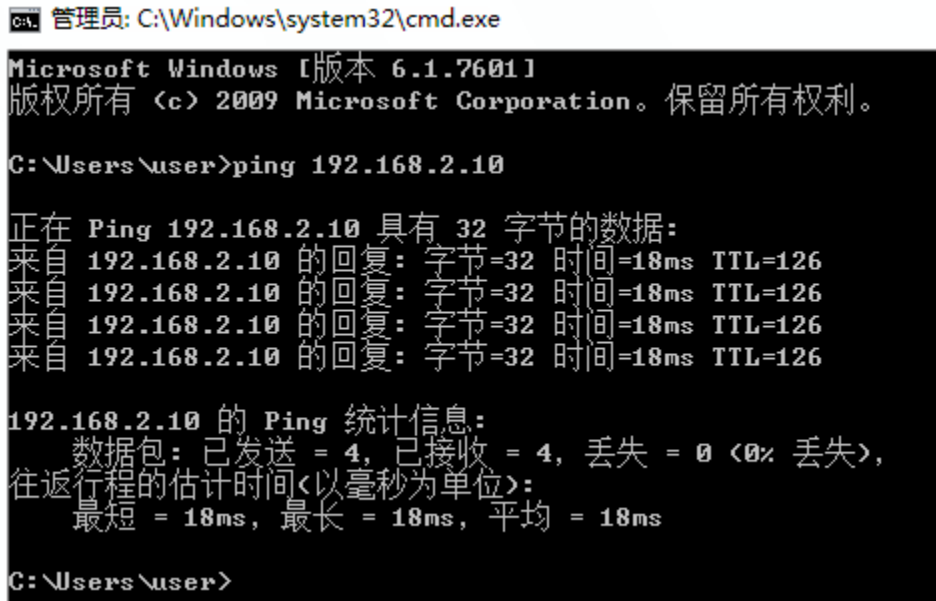
```
[1-R2]ip route-static 192.168.0.0 255.255.255.0 192.168.1.1
```

查看配置的静态路由：

```
[1-R2]dis ip routing-table protocol static
```

步骤五：PC1 ping PC2

可见，在 1-R1 和 1-R2 上配置完静态路由后，PC1 可以 ping 通 PC2。



```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\user>ping 192.168.2.10

正在 Ping 192.168.2.10 具有 32 字节的数据:
来自 192.168.2.10 的回复: 字节=32 时间=18ms TTL=126
来自 192.168.2.10 的回复: 字节=32 时间=18ms TTL=126
来自 192.168.2.10 的回复: 字节=32 时间=18ms TTL=126
来自 192.168.2.10 的回复: 字节=32 时间=18ms TTL=126

192.168.2.10 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 18ms, 最长 = 18ms, 平均 = 18ms

C:\Users\user>
```

实验任务三：使用 tracert 命令检查连通性

通过使用 tracert 命令，用户可以查看报文从源设备传送到目的设备所经过的路由节点。当网络出现故障时，用户可以使用该命令分析出现故障的网络节点。

步骤一：启动 unreachable 与 ttl-expires

在 2 个路由器上系统视图上启动 unreachable 与 ttl-expires，参考命令如下：

```
[1-R1]ip ttl-expires enable
[1-R1]ip unreachable enable
[1-R2]ip ttl-expires enable
[1-R2]ip unreachable enable
```

步骤二：在 1-R1 上 tracert PC2

```
[1-R1]tracert 192.168.2.10
```

traceroute to 192.168.2.10 (192.168.2.10), 30 hops at most, 52 bytes each packet, press CTRL_C to break

```
 1  192.168.1.2 (192.168.1.2)  16.848 ms  16.607 ms  16.580 ms
 2  192.168.2.10 (192.168.2.10)  19.777 ms  19.762 ms  19.695 ms
```

结果显示第一跳为 1-R2，第二跳为 PC2。

注意关闭 PC2 的防火墙。

查看路由器 tracert 命令携带的参数：

```
[1-R1]tracert ?
```

```
-a          Specify the source IP address used by TRACERT
-f          Specify the TTL value for the first packet
```

-m	Specify the maximum TTL value
-p	Specify the destination UDP port number
-q	Specify the number of probe packets sent each time
-t	Set the Type of Service (ToS) value
-topology	Specify a topology
-vpn-instance	Specify a VPN instance
-w	Set the timeout to wait for each reply
STRING<1-253>	IP address or hostname of the destination device
ipv6	IPv6 information

实验任务四：使用 debug 命令查看调试信息

步骤一：开启 1-R1 终端对信息的监视和显示功能

在 1-R1 上执行 terminal monitor 用于开启终端对系统信息的监视功能, 执行命令 terminal debugging 用于开启终端对调试信息的显示功能。

```
<1-R1>terminal monitor
```

The current terminal is enabled to display logs.

```
<1-R1>terminal debugging
```

The current terminal is enabled to display debugging logs.

步骤二：在 1-R1 上执行命令 debug ip icmp 用于开启系统 ICMP 模块的调试功能。

```
<1-R1>debugging ip icmp
```

步骤三：在 1-R1 上 ping 1-R2，观察调试信息输出

在 1-R1 上 ping 1-R2 的串口地址，连续发送 10 个 ping 报文。

```
<1-R1>ping -c 10 192.168.1.2
```

步骤四：关闭调试开关

调试结束后，使用 undo debugging all 命令，关闭所有模块的调试开关。

实验4 VLAN 配置

4.1 实验内容与目标

- 掌握 VLAN 的基本工作原理
- 掌握 access 链路端口和 trunk 链路端口的基本配置

4.2 实验组网图

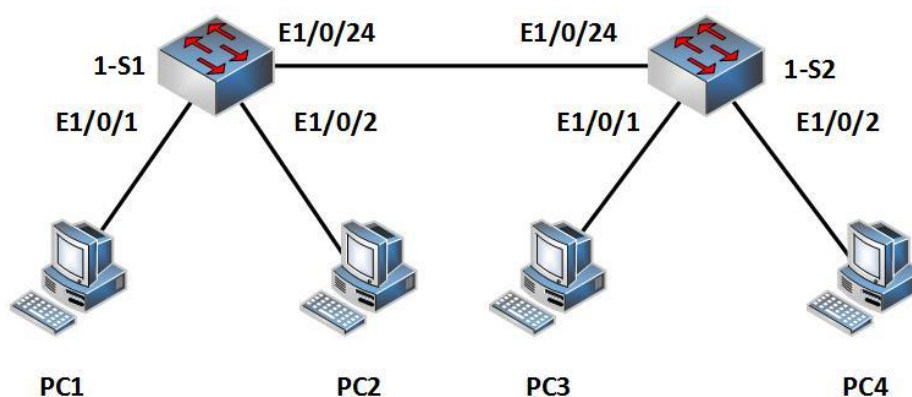


图 3-1 VLAN 实验环境图

4.3 实验过程

实验任务一：配置 access 链路端口

本实验任务通过在交换机上配置 access 链路端口而使 PC 间处于不同 VLAN，隔离 PC 间的访问，从而使学生加深对 access 链路端口的理解。

步骤一：建立物理连接

按照图 3-1 进行连接，并检查设备的软件版本及配置信息，确保各设备软件版本符合要求，所有配置为初始状态。如果配置不符合要求，请在用户模式下擦除设备中的配置文件，然后重启设备以使系统采用缺省的配置参数进行初始化。

以上步骤会用到以下命令：

```
<1-S1>display version  
<1-S1>>reset saved-configuration  
<1-S1>>reboot
```

步骤二：配置 PC 机的 IP 地址

PC 机的配置参数如下：

设备名称	IP 地址	网关
PC1	172.16.0.1/24	--
PC2	172.16.0.2/24	--
PC3	172.16.0.3/24	--
PC4	172.16.0.4/24	--

步骤三：PC 机间的连通性测试

使用 Ping 命令测试 4 个 PC 机的连通性，都能相互 ping 通。

步骤四：观察缺省 VLAN

在交换机上查看 VLAN，如下所示：

```
[1-S1]display vlan
Total 1 static VLAN exist(s).
The following static VLANs exist:
1(default),
[1-S1]dis vlan 1
VLAN ID: 1
VLAN Type: static
Route Interface: configured
Description: VLAN 0001
Name: VLAN 0001
Tagged   Ports: none
Untagged Ports:
    Ethernet1/0/1      Ethernet1/0/2      Ethernet1/0/3
    Ethernet1/0/4      Ethernet1/0/5      Ethernet1/0/6
    Ethernet1/0/7      Ethernet1/0/8      Ethernet1/0/9
    Ethernet1/0/10     Ethernet1/0/11     Ethernet1/0/12
    Ethernet1/0/13     Ethernet1/0/14     Ethernet1/0/15
    Ethernet1/0/16     Ethernet1/0/17     Ethernet1/0/18
    Ethernet1/0/19     Ethernet1/0/20     Ethernet1/0/21
    Ethernet1/0/22     Ethernet1/0/23     Ethernet1/0/24
    GigabitEthernet1/0/25  GigabitEthernet1/0/26  GigabitEthernet1/0/27
    GigabitEthernet1/0/28
```

.....

从以上输出可知，交换机上的缺省 VLAN 是 vlan 1，所有的端口处于 vlan 1 中；端口的 pvid 是 1，且是 access 链路端口类型。

1-S2 交换机上的 VLAN 查看方法与 1-S1 交换机一致。

配置 1-S1：

```
[1-S1]vlan 2
[1-S1-vlan2]port ethernet 1/0/1
```

配置 1-S2：

```
[1-S2]vlan 2
[1-S2-vlan2]port ethernet 1/0/1
```

在交换机上查看有关 vlan 2 的信息，如下所示：

```
[1-S1]display vlan
Total 2 VLAN exist(s).
The following VLANs exist:
  1(default), 2,
[1-S1]display vlan 2
VLAN ID: 2
VLAN Type: static
Route Interface: not configured
Description: VLAN 0002
Name: VLAN 0002
Tagged    Ports: none
Untagged Ports:
  Ethernet1/0/1
```

步骤五：测试 VLAN 间的隔离

通过 ping 命令来测试处于不同 VLAN 间的 PC 能否互通。

用 ping 命令来测试到 PC 的互通性。其结果应该是 PC1 与 PC2 不能互通，PC3 和 PC4 不能互通；PC1 与 PC3 不能互通；PC2 与 PC4 能互通。证明不同 VLAN 之间不能互通，连接在同一交换机上的 PC 被隔离了。

实验任务二：配置 trunk 链路端口

本任务是在交换机间配置 trunk 链路端口，来使同一 VLAN 中的 PC 能够跨交换机访问。通过本实验，学生应该能够掌握 trunk 链路端口的配置及作用。

步骤一：跨交换机 VLAN 互通测试

在上个实验中，PC1 和 PC3 都属于 vlan 2。在 PC1 上使用 ping 命令来测试于 PC3 能否互通。其结果应该不能，如下所示：

```
C:\Documents and Settings\Administrator>ping 172.168.0.3
```

```
Pinging 172.168.0.3 with 32 bytes of data:
```

```
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
```

```
Ping statistics for 172.168.0.3:
```

```
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

PC1 与 PC3 之间不能互通。因为交换机之间的端口 Ethernet 1/0/24，是 access 链路端口，且属于 vlan 1，不允许 vlan 2 的数据帧通过。

要想让 vlan 2 数据帧通过 Ethernet 1/0/24，需要设置端口为 trunk 链路端口。

步骤二：配置 trunk 链路端口

在 1-S1 和 1-S2 上配置端口 Ethernet 1/0/24 为 trunk 链路端口。


```
[1-S1]interface Ethernet 1/0/24
[1-S1-Ethernet1/0/24]port link-type trunk
[1-S1-Ethernet1/0/24]port trunk permit vlan all
```

```
[1-S2]interface Ethernet 1/0/24
[1-S2-Ethernet1/0/24]port link-type trunk
[1-S2-Ethernet1/0/24]port trunk permit vlan all
```

查看配置好的端口信息：

```
[1-S1-Ethernet1/0/24]dis this
```

```
#
interface Ethernet1/0/24
  port link-mode bridge
  port link-type trunk
  port trunk permit vlan all
#
return
```

配置完成后，查看 vlan 2 信息：

```
[1-S1]dis vlan 2
VLAN ID: 2
VLAN Type: static
Route Interface: not configured
Description: VLAN 0002
Name: VLAN 0002
Tagged   Ports:
    Ethernet1/0/24
Untagged Ports:
    Ethernet1/0/1
```

可以看到，vlan 2 中包含了端口 Ethernet 1/0/24，且数据帧是以带有标签的形式通过端口的。

配置完成后，查看交换机接口信息：

```
[1-S1]display interface Ethernet 1/0/24
```

```
....
Allow jumbo frame to pass
PVID: 1
Mdi type: auto
Port link-type: trunk
VLAN passing   : 1(default vlan), 2
VLAN permitted: 1(default vlan), 2-4094
Trunk port encapsulation: IEEE 802.1q
....
```

从以上信息可知，端口的 pvid 值是 1，端口类型是 trunk，允许所有的 vlan（1~4096）

通过，但实际上时 vlan 1 和 vlan 2 能够通过此端口。1-S2 上 vlan 和端口 Ethernet 1/0/24 的信息与此类似

步骤三：跨交换机 VLAN 互通测试

在 PC1 上用 ping 命令来测试于 PC3 能否互通。其结果应该是能够互通，如下所示：

```
C:\Documents and Settings\Administrator>ping 172.16.0.3
```

```
Pinging 172.16.0.3 with 32 bytes of data:
```

```
Reply from 172.16.0.3: bytes=32 time<1ms TTL=128
```

```
Reply from 172.16.0.3: bytes=32 time<1ms TTL=128
```

```
Reply from 172.16.0.3: bytes=32 time<1ms TTL=128
```

```
Reply from 172.16.0.3: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 172.16.0.3:
```

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

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

实验5 生成树配置

5.1 实验内容与目标

- 了解 STP 的基本工作原理
- 掌握 STP 的基本配置方法

5.2 实验组网图

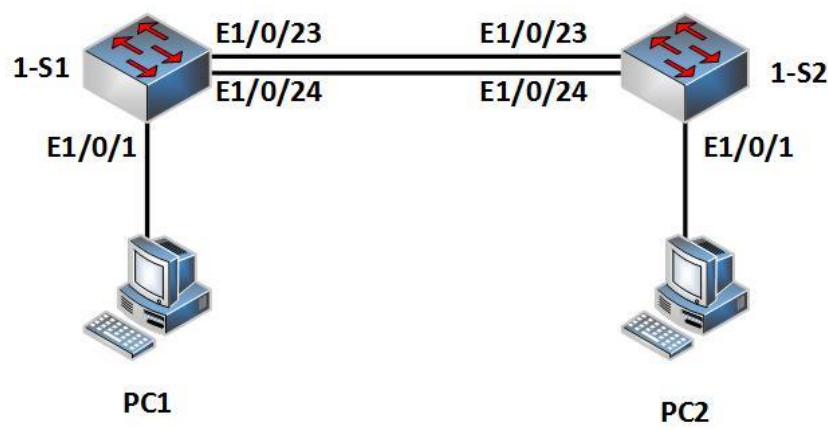


图 4-1 STP 实验组网图

5.3 实验过程

实验任务一：STP 基本配置

本实验通过在交换机上配置 STP 根桥及边缘端口，来使读者掌握 STP 根桥及边缘端口的配置命令和查看方法。然后通过观察端口状态迁移，来加深了解 MSTP 协议的快速收敛特性。

步骤一：建立物理连接

按照图 4-1 进行连接，并检查设备的软件版本及配置信息，确保各设备软件版本符合要求，所有配置为初始状态。如果配置不符合要求，请在用户模式下擦除设备中的配置文件，然后重启设备以使系统采用缺省的配置参数进行初始化。

步骤二：配置 PC 的 IP 地址

PC 机的配置参数如下：

设备名称	IP 地址	网关
PC1	172.16.0.1/24	--
PC2	172.16.0.2/24	--

步骤三：配置 STP

本实验任务是配置 STP 根桥及边缘端口。在系统视图下启用 STP，并设置 1-S1 的优先级为 0，以使 1-S1 为根桥；并且配置连接 PC 的端口为边缘端口。

```
[1-S1]stp enable
[1-S1]stp priority 0
[1-S1]interface Ethernet 1/0/1
[1-S1-Ethernet1/0/1]stp edged-port enable
```

```
[1-S2]stp enable
[1-S2]stp priority 4096
[1-S2]interface Ethernet 1/0/1
[1-S2-Ethernet1/0/1]stp edged-port enable
```

步骤四：查看 STP 信息

分别在 1-S1 和 1-S2 上查看 STP 信息。正确信息应如下所示：

```
[1-S1]dis stp
-----[CIST Global Info][Mode MSTP]-----
CIST Bridge           :0.741f-4aec-99a1
Bridge Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC        :0.741f-4aec-99a1 / 0
CIST RegRoot/IRPC     :0.741f-4aec-99a1 / 0
CIST RootPortId       :0.0
```

```
[1-S1]dis stp brief
```

MSTID	Port	Role	STP State	Protection
0	Ethernet1/0/1	DESI	FORWARDING	NONE
0	Ethernet1/0/23	DESI	FORWARDING	NONE
0	Ethernet1/0/24	DESI	FORWARDING	NONE

以上信息表明，1-S1 是根桥，其上所有端口是指定端口（DESI），处于转发状态。

```
<1-S2>display stp
-----[CIST Global Info][Mode MSTP]-----
CIST Bridge           :4096.741f-4aec-9689
Bridge Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC        :0.741f-4aec-99a1 / 200
CIST RegRoot/IRPC     :4096.741f-4aec-9689 / 0
```

```
<1-S2>dis stp brief
```

MSTID	Port	Role	STP State	Protection
0	Ethernet1/0/1	DESI	FORWARDING	NONE
0	Ethernet1/0/23	ROOT	FORWARDING	NONE
0	Ethernet1/0/24	ALTE	DISCARDING	NONE

以上信息表明，1-S2 是非根桥，端口 Ethernet1/0/23 是根端口，处于转发状态，负责在交换机之间转发数据；端口 Ethernet1/0/24 是备份根端口，处于阻塞状态；连接 PC 的端口 Ethernet1/0/1 是指定端口。

步骤五：STP 冗余特性验证

STP 不但能够阻塞冗余链路，并且能够在活动链路断开时，通过激活被阻塞链路的冗余链路而恢复网络的连通。

在 PC1 上执行命令 “ping 172.16.0.2 -t”，以使 PC1 向 PC2 不间断发送 ICMP 报文。

在 1-S2 上查看 STP 端口状态，确定交换机间哪个端口处于转发状态。

[H3C]dis stp brief

MSTID	Port	Role	STP State	Protection
0	Ethernet1/0/1	DESI	FORWARDING	NONE
0	Ethernet1/0/23	ROOT	FORWARDING	NONE
0	Ethernet1/0/24	ALTE	DISCARDING	NONE

将交换机之间处于 STP 转发状态的端口上的电缆断开（Ethernet1/0/23），观察 PC1 上发送的 ICMP 报文有无丢失。正常情况下，应该没有报文丢失或仅有一个报文丢失。

再次在 1-S2 上查看 STP 端口状态，看端口状态是否有变化。如下所示：

[1-S2]dis stp brief

MSTID	Port	Role	STP State	Protection
0	Ethernet1/0/1	DESI	FORWARDING	NONE
0	Ethernet1/0/24	ROOT	FORWARDING	NONE

可以看出，原来处于阻塞状态的端口 Ethernet1/0/24 迁移到了转发状态。

无报文丢失说明目前 STP 的收敛速度很快。其实，这就是 RSTP/MSTP 相对于 STP 德改进之一。缺省情况下，交换机运行 MSTP，1-S2 上的两个端口中一个是根端口，另一个是备份根端口。当原端口断开时，备份根端口快速切换到转发状态。

注意：如果在 PC1 上 ping 172.16.0.2 -t 是出现了 “request timed out”，表明 PC2 无回应，需要检查 PC2 是否开启了防火墙或交换机配置是否有问题。

步骤六：端口状态迁移查看

将步骤五中交换机之间处于 STP 转发状态的端口上的电缆重新连接（Ethernet1/0/23）。

在交换机 1-S1 上断开端口 Ethernet1/0/1 的电缆，再重新连接，并且在 1-S1 上查看交换机输出信息。如下：

#Jan 1 03:36:47:949 2010 1-S1 MSTP/1/PFWD:

Trap 1.3.6.1.4.1.25506.8.35.14.0.1<hh3cPortMstiStateForwarding>: Instance 0's Port 0.9371648 has been set to forwarding state!

%Jan 1 03:36:48:160 2010 1-S1 IFNET/3/LINK_UPDOWN: Ethernet1/0/1 link status is UP.

%Jan 1 03:36:48:260 2010 1-S1 MSTP/6/MSTP_FORWARDING: Instance 0's port Ethernet1/0/1 has been set to forwarding state.

可以看到，端口在连接电缆后马上成为转发状态。这是因为端口被配置成边缘端口，无须延迟而进入转发状态。

在前面实验中，端口状态迁移速度很快。为了清晰观察端口状态，我们在连接 PC 的端口 Ethernet1/0/1 上取消边缘端口配置，如下：

[1-S1]interface Ethernet 1/0/1

[1-S1-Ethernet1/0/1]undo stp edged-port

配置完成后，断开端口 Ethernet 1/0/1 的电缆，再重新连接，并且在 1-S1 上查看端口 Ethernet 1/0/1 的状态。注意每隔几秒执行命令查看一次，以能准确看到端口状态的迁移过程。例如：

[1-S1]dis stp br

MSTID	Port	Role	STP State	Protection
0	Ethernet1/0/1	DESI	DISCARDING	NONE
0	Ethernet1/0/23	DESI	FORWARDING	NONE
0	Ethernet1/0/24	DESI	FORWARDING	NONE

[1-S1]dis stp br

MSTID	Port	Role	STP State	Protection
0	Ethernet1/0/1	DESI	LEARNING	NONE
0	Ethernet1/0/23	DESI	FORWARDING	NONE
0	Ethernet1/0/24	DESI	FORWARDING	NONE

[1-S1]

#Jan 1 03:46:39:319 2010 1-S1 MSTP/1/PFWD:

Trap 1.3.6.1.4.1.25506.8.35.14.0.1<hh3cPortMstiStateForwarding>: Instance 0's Port 0.9371648 has been set to forwarding state!

%Jan 1 03:46:39:530 2010 1-S1 MSTP/6/MSTP_FORWARDING: Instance 0's port Ethernet1/0/1 has been set to forwarding state.

%Jan 1 03:46:39:680 2010 1-S1 MSTP/6/MSTP_DETECTED_TC: Instance 0's port Ethernet1/0/1 detected a topology change.

可知，端口从 discarding 状态先迁移到 learning 状态，最后到 forwarding 状态。从以上实验可知，取消边缘端口配置后，STP 收敛速度变慢了。

实验6 链路聚合配置

6.1 实验内容与目标

- 了解以太网交换机链路聚合的基本工作原理
- 掌握以太网交换机静态链路聚合的基本配置方法

6.2 实验组网图

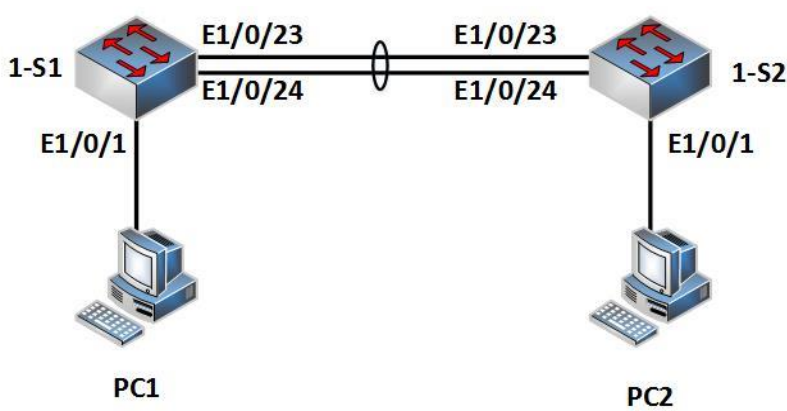


图 6-1 链路聚合实验组网图

6.3 实验过程

实验任务一：交换机静态链路聚合配置

本实验通过在交换机上配置静态链路聚合，使读者掌握静态链路聚合的配置命令和查看方法。然后通过断开聚合组中的某条链路并观察网络连接是否中断，来加深了解链路聚合所实现的可靠性。

步骤一：建立物理连接

按照图 6-1 进行连接(先不连接 E1/0/23 间的网线)，并检查设备的软件版本及配置信息，确保各设备软件版本符合要求，所有配置为初始状态。如果配置不符合要求，请在用户模式下擦除设备中的配置文件，然后重启设备以使系统采用缺省的配置参数进行初始化。

步骤二：配置 PC 的 IP 地址并测试连通性

PC 机的配置参数如下：

设备名称	IP 地址	网关
PC1	172.16.0.1/24	--
PC2	172.16.0.2/24	--

使用 ping 命令测试 PC1 与 PC2 的连通性，此时应该连通的。

将两个交换机的 E1/0/23 端口互连，如图 6-1。进一步使用 ping 命令测试 PC1 与 PC2 的连通性，此时反而不连通（交换机间形成环路引起，若没有此效果，则在 PC1 与 PC2 上清空 ARP 表，参考命令 “arp -d”）。

步骤三：配置静态聚合

链路聚合可以分为静态聚合和动态聚合，本实验任务是验证静态聚合。首先在系统视图下创建聚合端口，然后把物理端口加入聚合组中。

```
[1-S1]interface Bridge-Aggregation 1
[1-S1-Bridge-Aggregation1]qu
[1-S1]interface Ethernet 1/0/23
[1-S1-Ethernet1/0/23]port link-aggregation group 1
[1-S1-Ethernet1/0/23]qu
[1-S1]interface Ethernet 1/0/24
[1-S1-Ethernet1/0/24]port link-aggregation group 1
```

```
[1-S2]interface Bridge-Aggregation 1
[1-S2-Bridge-Aggregation1]qu
[1-S2]interface Ethernet 1/0/23
[1-S2-Ethernet1/0/23]port link-aggregation group 1
[1-S2-Ethernet1/0/23]qu
[1-S2]interface Ethernet 1/0/24
[1-S2-Ethernet1/0/24]port link-aggregation group 1
```

步骤三：查看聚合组信息

分别在 1-S1 和 1-S2 上查看所配置的聚合组信息。正确信息应如下所示：

```
[1-S1]display link-aggregation summary
```

Aggregation Interface Type:

BAGG -- Bridge-Aggregation, RAGG -- Route-Aggregation

Aggregation Mode: S -- Static, D -- Dynamic

Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing

Actor System ID: 0x8000, 741f-4aec-99a1

AGG Interface	AGG Mode	Partner ID	Select Ports	Unselect Ports	Share Type
BAGG1	S	none	2	0	Shar

```
[1-S1]display link-aggregation verbose
```

Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing

Port Status: S -- Selected, U -- Unselected

Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,

D -- Synchronization, E -- Collecting, F -- Distributing,

G -- Defaulted, H -- Expired

Aggregation Interface: Bridge-Aggregation1

Aggregation Mode: Static

Loadsharing Type: Shar

Port	Status	Priority	Oper-Key

Eth1/0/23	S	32768	1
Eth1/0/24	S	32768	1

[1-S2]display link-aggregation summary

Aggregation Interface Type:

BAGG -- Bridge-Aggregation, RAGG -- Route-Aggregation

Aggregation Mode: S -- Static, D -- Dynamic

Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing

Actor System ID: 0x8000, 741f-4aec-9689

AGG Interface	AGG Mode	Partner ID	Select Ports	Unselect Ports	Share Type

BAGG1	S	none	2	0	Shar

[1-S2]display link-aggregation verbose

Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing

Port Status: S -- Selected, U -- Unselected

Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
D -- Synchronization, E -- Collecting, F -- Distributing,
G -- Defaulted, H -- Expired

Aggregation Interface: Bridge-Aggregation1

Aggregation Mode: Static

Loadsharing Type: Shar

Port	Status	Priority	Oper-Key

Eth1/0/23	S	32768	1
Eth1/0/24	S	32768	1

以上信息表明，交换机上有一个链路聚合端口，其 ID 是 1，组中包含了 2 个 selected 状态端口，并工作在负载分担模式下。

步骤四：链路聚合组验证

在 PC1 上执行 ping 命令，以使 PC1 向 PC2 不间断发送 ICMP 报文，如下所示：

```
C:\Documents and Settings\Administrator>ping 172.16.0.2 -t
```

Pinging 172.16.0.2 with 32 bytes of data:

Reply from 172.16.0.2: bytes=32 time<1ms TTL=128

Reply from 172.16.0.2: bytes=32 time<1ms TTL=128

.....

注意观察交换机面板上的端口 LED 显示灯，闪烁表明有数据流通过。将聚合组中 LED 显示灯闪烁的端口上电缆断开，观察 PC1 上发送的 ICMP 报文有无丢失。

正常情况下，应该没有报文丢失。

无报文丢失说明聚合组中的两个端口是互相备份的。当一个端口不能转发数据流时，系统将数据流从另一个端口发送出去。

实验7 ARP 配置

7.1 实验内容与目标

- 掌握 ARP 的工作机制
- 掌握 ARP 代理的工作原理及配置方法

7.2 实验组网图

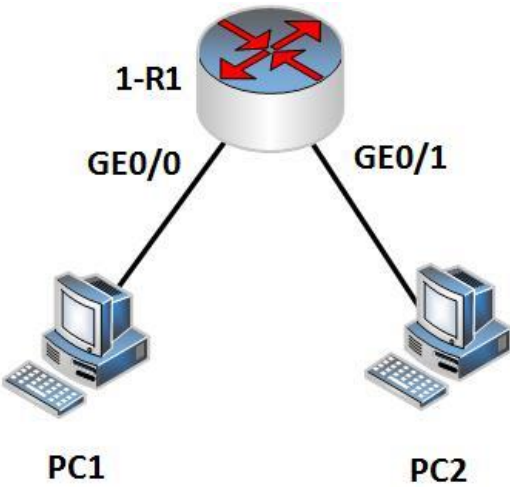


图 7-1 ARP 实验组网图

7.3 实验过程

实验任务一：ARP 表项观察

本实验通过观察设备上的 ARP 表项建立过程，是学生能够了解 ARP 协议的基本工作原理。

步骤一：建立物理连接

按照图 7-1 进行连接，并检查设备的软件版本及配置信息，确保各设备软件版本符合要求，所有配置为初始状态。如果配置不符合要求，请在用户模式下擦除设备中的配置文件，然后重启设备以使系统采用缺省的配置参数进行初始化。

步骤二：配置 PC 及路由器的 IP 地址

表 7-1 IP 地址列表

设备名称	接口	IP 地址	默认网关
PC1	--	172.16.0.1/24	172.16.0.254
PC2	--	172.16.1.1/24	172.16.1.254

1-R1	G0/0	172.16.0.254/24
1-R1	G0/1	172.16.1.254/24

根据上表所示在 PC 上配置 IP 地址和网关。配置完成后，在 PC 的“命令提示符”窗口下，键入命令 ipConfig 来验证 PC 的 IP 地址是否配置正确。PC1 的结果应该如下所示：

```
[1-R1]interface GigabitEthernet 0/0
[1-R1-GigabitEthernet0/0]ip address 172.16.0.254 24
```

```
[1-R1]interface GigabitEthernet 0/1
[1-R1-GigabitEthernet0/1]ip address 172.16.1.254 24
```

步骤三：查看 ARP 信息

首先，我们在 1-R1 及 PC1、PC2 上用命令来查看他们的 ip 地址和 MAC 地址。1-R1 的接口 MAC 地址与 IP 地址如下：

```
[1-R1]display interface GigabitEthernet 0/0
GigabitEthernet0/0
Current state: UP
Line protocol state: UP
Description: GigabitEthernet0/0 Interface
Bandwidth: 1000000kbps
Maximum Transmit Unit: 1500
Internet Address is 172.16.0.254/24 Primary
IP Packet Frame Type:PKTFMT_ETHNT_2, Hardware Address: 741f-4a4d-0d4d
IPv6 Packet Frame Type:PKTFMT_ETHNT_2, Hardware Address: 741f-4a4d-0d4d
....
```

```
[1-R1]display interface GigabitEthernet 0/1
GigabitEthernet0/1
Current state: UP
Line protocol state: UP
Description: GigabitEthernet0/1 Interface
Bandwidth: 1000000kbps
Maximum Transmit Unit: 1500
Internet Address is 172.16.1.254/24 Primary
IP Packet Frame Type:PKTFMT_ETHNT_2, Hardware Address: 741f-4a4d-0d4e
IPv6 Packet Frame Type:PKTFMT_ETHNT_2, Hardware Address: 741f-4a4d-0d4e
....
```

在 PC1 上通过命令：ipconfig /all 查看 MAC 地址及 IP 地址：
以太网适配器 本地连接：

```
连接特定的 DNS 后缀 . . . . . :
描述. . . . . : Realtek PCIe GBE Family Controller
物理地址. . . . . : 44-8A-5B-00-24-0F
DHCP 已启用 . . . . . : 否
自动配置已启用. . . . . : 是
本地链接 IPv6 地址. . . . . : fe80::505d:7b20:75a7:2932%11(首选)
```

IPv4 地址: **172.16.0.1**(首选)
子网掩码: 255.255.255.0
默认网关.....:

PC2 的接口 MAC 地址与 IP 地址如下:
以太网适配器 本地连接:

连接特定的 DNS 后缀:
描述.....: Realtek PCIe GBE Family Controller
物理地址.....: **44-8A-5B-00-21-E8**
DHCP 已启用: 否
自动配置已启用.....: 是
本地链接 IPv6 地址.....: fe80::9128:7553:4a83:490e%11(首选)
IPv4 地址: **172.16.1.1**(首选)
子网掩码: 255.255.255.0
默认网关.....:

根据以上信息，我们做一张表，表的内容是 PC 及 1-R1 的 IP 地址与 MAC 地址对应关系，如下所示：

表 7-2 IP 地址与 MAC 地址对应关系表

设备名称	接口	IP 地址	MAC 地址
PC1	--	172.16.0.1/24	44-8A-5B-00-24-0F
PC2	--	172.16.1.1/24	44-8A-5B-00-21-E8
1-R1	G0/0	172.16.0.254/24	741f-4a4d-0d4d
1-R1	G0/1	172.16.1.254/24	741f-4a4d-0d4e

然后，分别在 PC1 和 PC2 的“命令提示符”窗口下用 ping 命令来测试 pc 到 1-R1 的可达性，然后查看 pc 及 1-R1 建立 ARP 表项。

测试完成后，分别在 PC1、PC2 和 1-R1 上查看 ARP 表项信息。

PC1 的信息如下所示：

```
C:\Users\user>arp -a
接口: 172.16.0.1 --- 0xb
Internet 地址      物理地址      类型
172.16.0.254      74-1f-4a-4d-0d-4d      动态
```

PC2 的正确信息应如下所示：

```
C:\Users\user>arp -a
接口: 172.16.1.1 --- 0xb
Internet 地址      物理地址      类型
172.16.1.254      74-1f-4a-4d-0 d-4e      动态
```

1-R1 的正确信息应如下所示：

```
<1-R1>dis arp
Type: S-Static    D-Dynamic    O-Openflow    M-Multiport    I-Invalid
IP address        MAC address    VLAN          Interface      Aging Type
```

172.16.1.1	448a-5b00-21e8 N/A	GE0/1	19	D
172.16.0.1	448a-5b00-240f N/A	GE0/0	17	D

把我们所做的表 7-2 和 pc 及 1-R1 上的 ARP 表项对比一下。可知，pc 及 1-R1 都建立了正确的 ARP 表项，表项中包含了 IP 地址和对应的 MAC 地址。

实验任务二：ARP 代理配置

本实验通过在设备上配置 ARP 代理，是设备能够对不同子网间的 ARP 报文进行转发，是学生能够了解 ARP 代理的基本工作原理，掌握 ARP 代理的配置方法。

步骤一：修改 pc 的 IP 地址

基于实验任务一的网络拓扑，修改 PC1、PC2 的 IP 地址：

表 7-3 IP 地址列表

设备名称	接口	IP 地址	默认网关
PC1	--	172.16.0.1/ 16	172.16.0.254
PC2	--	172.16.1.1/ 16	172.16.1.254
1-R1	G0/0	172.16.0.254/24	
1-R1	G0/1	172.16.1.254/24	

步骤三：ARP 代理配置

此时，PC1 和 PC2 之间是不可达的。如果在 PC1 上测试到 PC2 之间的可达性，结果应该如下所示：

```
C:\Users\user>ping 172.16.1.1
```

正在 Ping 172.16.1.1 具有 32 字节的数据:

请求超时。

请求超时。

请求超时。

请求超时。

172.16.1.1 的 Ping 统计信息:

数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失)

为什么呢？但是 1-R1 上两个接口的子网是不同的（分别为 172.16.0.0/24 和 172.16.1.0/24），所以它不会再两个不同子网之间转发 ARP 报文。但如果配置了 ARP 代理，路由器可以像二层交换机一样转发 ARP 报文。

在 1-R1 上配置 ARP 代理：

```
[1-R1]interface GigabitEthernet 0/0
```

```
[1-R1-GigabitEthernet0/0]proxy-arp enable
```

```
[1-R1]interface GigabitEthernet 0/1
```

```
[1-R1-GigabitEthernet0/1]proxy-arp enable
```

配置完成后，在 PC1 上用 ping 命令测试 PC2 的可达性，此时应该是可达的，如下：

```
C:\Users\user>ping 172.16.1.1
```

正在 Ping 172.16.1.1 具有 32 字节的数据:
 来自 172.16.1.1 的回复: 字节=32 时间<1ms TTL=127
 来自 172.16.1.1 的回复: 字节=32 时间<1ms TTL=127
 来自 172.16.1.1 的回复: 字节=32 时间<1ms TTL=127
 来自 172.16.1.1 的回复: 字节=32 时间<1ms TTL=127

172.16.1.1 的 Ping 统计信息:
 数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
 往返行程的估计时间(以毫秒为单位):
 最短 = 0ms, 最长 = 0ms, 平均 = 0ms

另外, 通过 PC1 使用 ping 命令测试到 172.16.1.254 的连通性。

步骤四：查看 ARP 信息

在 PC1 上查看 ARP 表项, 如下所示:

C:\Users\user>arp -a

接口: 172.16.0.1 --- 0xb

Internet 地址	物理地址	类型
172.16.0.254	74-1f-4a-4d-0d-4d	动态
172.16.1.1	74-1f-4a-4d-0d-4d	动态
172.16.1.254	74-1f-4a-4d-0d-4d	动态

ARP 表项中 172.16.1.1 对应的 MAC 地址与 1-R1 接口 G0/0 的 MAC 地址相同。也就是说, 在 PC1 看来, 1-R1 接口 G0/0 就是 PC2。实际上, 是 1-R1 的接口 G0/0 执行了 ARP 代理功能, 为 PC1 发出的 ARP 请求提供了代理应答。

同理, PC2 也会认为 1-R1 的接口 G0/1 就是 PC1。在 1-R1 上查看 ARP 表项, 如下所示:

C:\Users\user>arp -a

接口: 172.16.0.1 --- 0xb

Internet 地址	物理地址	类型
172.16.1.254	74-1f-4a-4d-0d-4e	动态
172.16.0.1	74-1f-4a-4d-0d-4e	动态
172.16.0.254	74-1f-4a-4d-0d-4e	动态

在 1-R1 上的 ARP 表项如下:

[1-R1]dis arp

Type: S-Static	D-Dynamic	O-Openflow	M-Multiport	I-Invalid
IP address	MAC address	VLAN	Interface	Aging Type
172.16.0.1	448a-5b00-240f	N/A	GE0/0	16 D
172.16.1.1	448a-5b00-21e8	N/A	GE0/1	17 D

实验8 DHCP 配置

8.1 实验内容与目标

- 完成本实验，您应该能够：
- 了解 DHCP 协议工作原理
 - 掌握设备作为 DHCP 服务器的常用配置命令
 - 掌握设备作为 DHCP 中继的常用配置

8.2 实验组网图

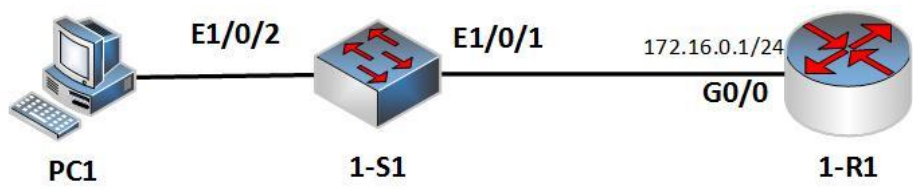


图 8-1 DHCP 实验组网图

8.3 实验过程

实验任务一：PC1 直接通过 1-R1 获得 IP 地址

本实验通过配置 DHCP 客户机从处于同一个子网中的 DHCP 服务器获得 IP 地址，网关等信息，是学生能够找到路由器上 DHCP 服务器的配置。

步骤一：建立物理连接

按照图 7-1 进行连接，并检查设备的软件版本及配置信息，确保各设备软件版本符合要求，所有配置为初始状态。如果配置不符合要求，请在用户模式下擦除设备中的配置文件，然后重启设备以使系统采用缺省的配置参数进行初始化。

步骤二：在路由器接口配置 IP 地址

表 8-1 IP 地址列表

设备名称	接口	IP 地址	网关
1-R1	G0/0	172.16.0.1/24	--

配置 1-R1：

```
[1-R1]interface GigabitEthernet 0/0
[1-R1-GigabitEthernet0/0]ip add 172.16.0.1 24
```

步骤三：配置 1-R1 作为 DHCP 服务器

配置 1-R1：

```
[1-R1]dhcp enable
```

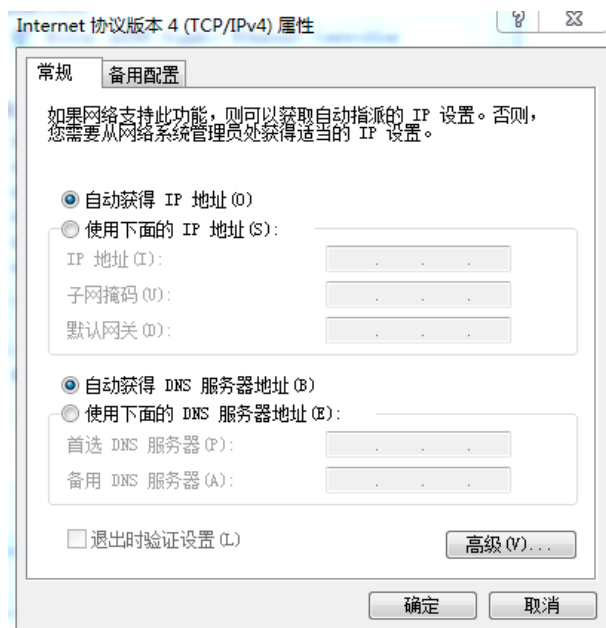


```

[1-R1]dhcp server forbidden-ip 172.16.0.1
[1-R1]dhcp server ip-pool pool1
[1-R1-dhcp-pool-pool1]network 172.16.0.0 mask 255.255.255.0
[1-R1-dhcp-pool-pool1]gateway-list 172.16.0.1
配置完成后，可以用以下命令来查看 1-R1 上 DHCP 相关配置：
[1-R1]dis cu
#
version 7.1.049, Release 0106P21
#
sysname 1-R1
#
dhcp enable
dhcp server forbidden-ip 172.16.0.1
#
password-recovery enable
#
vlan 1
#
dhcp server ip-pool pool1
network 172.16.0.0 mask 255.255.255.0
gateway-list 172.16.0.1
.....
interface GigabitEthernet0/0
port link-mode route
combo enable copper
ip address 172.16.0.254 255.255.255.0
#

```

步骤四：PC1 通过 DHCP 服务器获得 IP 地址



如图所示，选中“自动获得 IP 地址”和“自动获得 DNS 服务器地址”并确定，以确保 PC1 配置为 DHCP 客户端。

在 PC1 的“命令提示符”窗口下，键入命令 `ipconfig /all` 来验证 PC1 能否获得 IP 地址和网关等信息。正确的结果应该如下所示：

以太网适配器 本地连接:

```
连接特定的 DNS 后缀 . . . . .:
描述. . . . .: Realtek PCIe GBE Family Controller
物理地址. . . . .: 44-8A-5B-00-24-0F
DHCP 已启用 . . . . .: 是
自动配置已启用. . . . .: 是
本地链接 IPv6 地址. . . . .: fe80::505d:7b20:75a7:2932%11(首选)
IPv4 地址 . . . . .: 172.16.0.2(首选)
子网掩码 . . . . .: 255.255.255.0
获得租约的时间 . . . . .: 2015 年 12 月 1 日 14:24:50
租约过期的时间 . . . . .: 2015 年 12 月 2 日 14:24:50
默认网关. . . . .: 172.16.0.1
DHCP 服务器 . . . . .: 172.16.0.1
```

步骤五：查看 DHCP 服务器相关信息

在 1-R1 上用命令 `dis dhcp server statistics` 查看 DHCP 服务器的统计信息：

[1-R1]display dhcp server statistics

```
Pool number: 1
Pool utilization: 0.39%
Bindings:
  Automatic: 1
  Manual: 0
  Expired: 0
Conflict: 0
Messages received: 4
  DHCPDISCOVER: 1
  DHCPREQUEST: 1
  DHCPDECLINE: 0
  DHCPRELEASE: 0
  DHCPINFORM: 2
  BOOTPREQUEST: 0
Messages sent: 4
  DHCPOFFER: 1
  DHCPACK: 3
  DHCPNAK: 0
  BOOTPREPLY: 0
Bad Messages: 0
```

从以上输出可以得知，目前路由器上有一个地址池，有一个 IP 被自动分配给了客户端。

用 `display dhcp server free-ip` 来查看 DHCP 服务器可供分配的 IP 地址资源：

[1-R1]display dhcp server free-ip

Pool name: pool

Network: 172.16.0.0 mask 255.255.255.0

IP ranges from 172.16.0.3 to 172.16.0.255

用 display dhcp server ip-in-use 来查看 DHCP 服务器已经分配的 IP 地址：

[1-R1]display dhcp server ip-in-use

IP address	Client identifier/ Hardware address	Lease expiration	Type
172.16.0.2	0144-8a5b-0024-0f	Dec 2 14:23:42 2015	Auto(C)

可知，IP 地址 172.16.0.2、172.16.0.1 不是可分配的 IP 地址资源。因为 172.16.0.1 被禁止分配，所以 172.16.0.2 被分配给了 PC1。

实验任务二：PC1 通过 DHCP 中继方式获得 IP 地址

本实验通过配置 DHCP 客户机从处于不同子网的 DHCP 服务器获得 IP 地址、网关等信息，是学生能够掌握 DHCP 的配置。

步骤一：建立物理连接

按照图 7-1 进行连接，并检查设备的软件版本及配置信息，确保各设备软件版本符合要求，所有配置为初始状态。如果配置不符合要求，请在用户模式下擦除设备中的配置文件，然后重启设备以使系统采用缺省的配置参数进行初始化。

步骤二：在设备上配置 IP 地址及路由

表 8-2 设备 IP 地址列表

设备名称	物理接口	IP 地址	VLAN 虚接口
1-S1	E1/0/1	172.16.0.2/24	Vlan-interface1
	E1/0/2	172.16.1.1/24	Vlan-interface2
1-R1	G0/0	172.16.0.1/24	--

在 1-S1 上配置 VLAN 虚接口及 IP：

[1-S1]vlan 2

[1-S1-vlan2]int e1/0/2

[1-S1-Ethernet1/0/2]port access vlan 2

[1-S1]interface Vlan-interface 1

[1-S1-Vlan-interface1]ip add 172.16.0.2 24

[1-S1]interface Vlan-interface 2

[1-S1-Vlan-interface2]ip add 172.16.1.1 24

[1-R1]interface GigabitEthernet 0/0

[1-R1-GigabitEthernet0/0]ip add 172.16.0.1 24

步骤三：在 1-R1 上配置 DHCP 服务器及在 1-S1 上配置 DHCP 中继

[1-R1]dhcp enable

[1-R1]dhcp server forbidden-ip 172.16.1.1

[1-R1]dhcp server ip-pool pool2

[1-R1-dhcp-pool-pool2]network 172.16.1.0 mask 255.255.255.0

[1-R1-dhcp-pool-pool2]gateway-list 172.16.1.1

[1-S1]dhcp enable

```
[1-S1]dhcp relay server-group 1 ip 172.16.0.1
[1-S1]int vlan 2
[1-S1-Vlan-interface2]dhcp select relay
[1-S1-Vlan-interface2]dhcp relay server-select 1
```

步骤四：配置静态路由

```
[1-R1] ip route-static 172.16.1.0 24 172.16.0.2
```

步骤五：PC1 通过 DHCP 中继获得 IP 地址

断开 PC1 与 1-S1 之间的连接线缆，再接上，以使 PC1 重新发起 DHCP 请求。

完成重新获取地址后，在 PC1 的“命令提示符”窗口下，键入命令 ipconfig 来验证 PC1 能否获得 IP 地址和网关信息。正确结果应该如下所示：

以太网适配器 本地连接:

```
连接特定的 DNS 后缀 . . . . .:
描述. . . . .: Realtek PCIe GBE Family Controller
物理地址. . . . .: 44-8A-5B-00-24-0F
DHCP 已启用 . . . . .: 是
自动配置已启用. . . . .: 是
本地链接 IPv6 地址. . . . .: fe80::505d:7b20:75a7:2932%11(首选)
IPv4 地址 . . . . .: 172.16.1.2(首选)
子网掩码 . . . . .: 255.255.255.0
获得租约的时间 . . . . .: 2015 年 12 月 2 日 15:06:21
租约过期的时间 . . . . .: 2015 年 12 月 3 日 15:06:21
默认网关. . . . .: 172.16.1.1
DHCP 服务器 . . . . .: 172.16.0.1
```

步骤六：查看 DHCP 中继信息

查看地址池:

```
[1-R1]dis dhcp server pool
Pool name: 2
Network: 172.16.1.0 mask 255.255.255.0
expired 1 0 0 0
gateway-list 172.16.1.1
```

在 1-S1 上查看 DHCP 中继服务器组的信息:

```
[1-S1]display dhcp relay server-group 1
No.          Group IP
1            172.16.0.1
```

再查看接口对应的 DHCP 中继服务器组信息:

```
[1-S1]dis dhcp relay interface vlan 2
Interface name          Server-group
Vlan-interface2        1
```

再查看 DHCP 中继的相关统计信息:

```
[1-S1]display dhcp relay statistics server-group 1
DHCP relay server-group      #1
```

Packet type	Packet number
Client -> Server:	
DHCPDISCOVER	1
DHCPREQUEST	1
DHCPINFORM	0
DHCPRELEASE	0
DHCPDECLINE	0
BOOTPREREQUEST	0
Server -> Client:	
DHCPOFFER	1
DHCPACK	1
DHCPNAK	0
BOOTPREPLY	0

实验9 静态路由配置

9.1 实验内容与目标

- 掌握路由转发的基本原理
- 掌握静态路由、缺省路由的配置方法
- 掌握查看路由表的基本命令

9.2 实验组网图

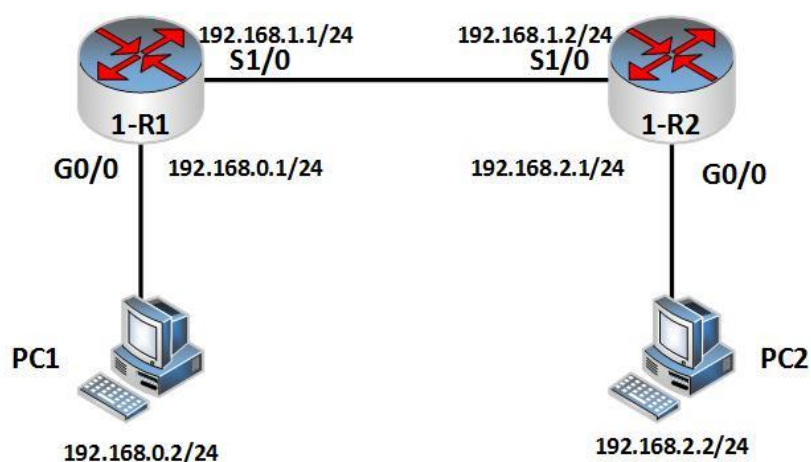


图 9-1 静态路由配置实验

9.3 实验过程

实验任务一：查看路由表

本实验主要是通过通过在路由器上通过查看路由表，观察路由表中路由项。通过本次实验，学生能够掌握如何使用命令来查看路由表，及了解路由项中要素的含义。

步骤一：建立物理连接

按照图 9-1 进行连接，并检查设备的软件版本及配置信息，确保各设备软件版本符合要求，所有配置为初始状态。如果配置不符合要求，请在用户模式下擦除设备中的配置文件，然后重启设备以使系统采用缺省的配置参数进行初始化。

步骤二：在路由器上查看路由表

首先，在路由器上查看路由表，如下所示：

```
[1-R1]dis ip routing-table
```

Destinations : 8

Routes : 8

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

由以上输出可知，目前路由器只有目的地址是 127.0.0.0 的路由，这是路由器的环回地址直连路由。

步骤三：配置 IP 地址

如表所示，配置 PC 机的 IP 地址以及路由器的 IP 地址。

表 9-1 IP 地址列表

设备名称	接口	IP 地址	网关
1-R1	S1/0	192.168.1.1/24	--
	G0/0	192.168.0.1/24	
1-R2	S1/0	192.168.1.2/24	
	G0/0	192.168.2.1/24	
PC1		192.168.0.2/24	192.168.0.1/24
PC2		192.168.2.2/24	192.168.2.1/24

配置 1-R1:

```
[1-R1]int S1/0
[1-R1-Serial1/0]ip ad 192.168.1.1 24
[1-R1-Serial1/0]int g 0/0
[1-R1-GigabitEthernet0/0]ip ad 192.168.0.1 24
```

配置 1-R2:

```
[1-R2]int s1/0
[1-R2-Serial1/0]ip ad 192.168.1.2 24
[1-R2-Serial1/0]int g 0/0
[1-R2-GigabitEthernet0/0]ip ad 192.168.2.1 24
```

配置完成后，再次查看路由表。例如，在 1-R1 上查看路由表，如下：

```
[1-R1]display ip routing-table
```

Destinations : 17 Routes : 17

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.0/24	Direct	0	0	192.168.0.1	GE0/0
192.168.0.0/32	Direct	0	0	192.168.0.1	GE0/0
192.168.0.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.255/32	Direct	0	0	192.168.0.1	GE0/0
192.168.1.0/24	Direct	0	0	192.168.1.1	S1/0
192.168.1.0/32	Direct	0	0	192.168.1.1	S1/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	S1/0
192.168.1.255/32	Direct	0	0	192.168.1.1	S1/0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

由上输出可知，配置了 IP 地址 192.168.0.1 和 192.168.1.1 后，路由表中有了直连路由。
在 1-R1 上关闭接口，如下：

```
[1-R1-Serial1/0]int g 0/0
[1-R1-GigabitEthernet0/0]shutdown
查看路由表，如下：
[1-R1]dis ip routing-table
```

Destinations : 13 Routes : 13

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.0/24	Direct	0	0	192.168.1.1	S1/0
192.168.1.0/32	Direct	0	0	192.168.1.1	S1/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	S1/0
192.168.1.255/32	Direct	0	0	192.168.1.1	S1/0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

可知，在接口 shutdown 后，所运行的链路层协议关闭，直连路由也就自然消失了。
再开启接口，如下：

```
[1-R1-Serial1/0]int g 0/0
[1-R1-GigabitEthernet0/0]undo shutdown
```

等到链路层协议 UP 后，再次查看路由表，可以发现接口 GigabitEthernet0/0 的直连路由又出现了。

实验任务二：静态路由配置

本实验主要是通过通过在路由器上配置静态路由，从而达到 pc 间能够互相访问的目的。通过本实验，学生能够掌握静态路由的配置，加深对路由环路产生原因的理解。

步骤一：在 pc 配置 IP 地址

按表 9-1 所示在 pc 上配置 IP 地址和网关。并在 windows 下用 ipconfig 命令查看所配置的 IP 地址和网关是否正确。

在 pc1 上用 ping 来测试到网关的可达性。

```
C:\Users\user>ping 192.168.0.1
```

正在 Ping 192.168.0.1 具有 32 字节的数据:

来自 192.168.0.1 的回复: 字节=32 时间<1ms TTL=255

来自 192.168.0.1 的回复: 字节=32 时间<1ms TTL=255

来自 192.168.0.1 的回复: 字节=32 时间<1ms TTL=255

来自 192.168.0.1 的回复: 字节=32 时间<1ms TTL=255

192.168.0.1 的 Ping 统计信息:

数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),

往返行程的估计时间(以毫秒为单位):

最短 = 0ms, 最长 = 0ms, 平均 = 0ms

再测试 pc 间的可达性。

```
C:\Users\user>ping 192.168.2.2
```

正在 Ping 192.168.2.2 具有 32 字节的数据:

请求超时。

请求超时。

请求超时。

请求超时。

192.168.2.2 的 Ping 统计信息:

数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),

以上输出信息显示 1-R1 返回了目的网络不可达的信息给 PC1, 说明 1-R1 没有到达 PC2 的路由。

查看路由表, 是因为 1-R1 路由表上没有到达 PC2 所在网段的路由。PC1 发出的报文到达 1-R1 后, 1-R1 就会丢失并返回不可达信息给 PC1。我们可以通过配置静态路由而使网络可达。

步骤二：静态路由配置规划

请学生考虑, 在 1-R1 和 1-R2 上应该配置到何目的网络的静态路由, 其下一跳应该指向哪个 IP 地址。

步骤三：配置静态路由

```
[1-R1]ip route-static 192.168.2.0 24 192.168.1.2
```

```
[1-R2]ip route-static 192.168.0.0 24 192.168.1.1
```

配置完成后，在 1-R1 上查看路由表，如下：

[1-R1]dis ip routing-table

Destinations : 18

Routes : 18

Destination/Mask	Proto	Pre Cost		NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.0/24	Direct	0	0	192.168.0.1	GE0/0
192.168.0.0/32	Direct	0	0	192.168.0.1	GE0/0
192.168.0.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.255/32	Direct	0	0	192.168.0.1	GE0/0
192.168.1.0/24	Direct	0	0	192.168.1.1	S1/0
192.168.1.0/32	Direct	0	0	192.168.1.1	S1/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	S1/0
192.168.1.255/32	Direct	0	0	192.168.1.1	S1/0
192.168.2.0/24	Static	60	0	192.168.1.2	S1/0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

测试 pc 间的可达性。如下：

C:\Users\user>ping 192.168.2.2

正在 Ping 192.168.2.2 具有 32 字节的数据:

来自 192.168.2.2 的回复: 字节=32 时间=18ms TTL=126

来自 192.168.2.2 的回复: 字节=32 时间=18ms TTL=126

来自 192.168.2.2 的回复: 字节=32 时间=18ms TTL=126

来自 192.168.2.2 的回复: 字节=32 时间=18ms TTL=126

192.168.2.2 的 Ping 统计信息:

数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),

往返行程的估计时间(以毫秒为单位):

最短 = 18ms, 最长 = 18ms, 平均 = 18ms

步骤四：路由环路观察

为了人为造成环路，首先删除所有的静态路由，然后在 1-R1 和 1-R2 上分别配置一条缺

省路由，下一跳互相指向对方。

```
[1-R1]undo ip route-static 192.168.2.0 24 192.168.1.2
[1-R2]undo ip route-static 192.168.0.0 24 192.168.1.1
[1-R1]ip route-static 0.0.0.0 0 s1/0
[1-R2]ip route-static 0.0.0.0 0 s1/0
```

配置完成后，在 1-R1 上查看路由表，显示结果如下：

```
[1-R1]dis ip routing-table
```

Destinations : 18

Routes : 18

Destination/Mask	Proto	Pre Cost		NextHop	Interface
0.0.0.0/0	Static	60	0	0.0.0.0	S1/0
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.0/24	Direct	0	0	192.168.0.1	GE0/0
192.168.0.0/32	Direct	0	0	192.168.0.1	GE0/0
192.168.0.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.255/32	Direct	0	0	192.168.0.1	GE0/0
192.168.1.0/24	Direct	0	0	192.168.1.1	S1/0
192.168.1.0/32	Direct	0	0	192.168.1.1	S1/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	S1/0
192.168.1.255/32	Direct	0	0	192.168.1.1	S1/0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

在 2 个路由器上系统视图上启动 unreachableables 与 ttl-expires，参考命令如下：

```
[1-R1]ip ttl-expires enable
[1-R1]ip unreachableables enable
[1-R2]ip ttl-expires enable
[1-R2]ip unreachableables enable
```

然后在 pc1 上用 tracert 命令来观察环路情况。

```
C:\Users\user>tracert 3.3.3.3
```

通过最多 30 个跃点跟踪到 3.3.3.3 的路由

```
1    <1 毫秒    <1 毫秒    <1 毫秒  192.168.0.1
2    21 ms     21 ms     21 ms   192.168.1.2
```

3	26 ms	26 ms	26 ms	192.168.1.1
4	47 ms	47 ms	47 ms	192.168.1.2
5	52 ms	52 ms	52 ms	192.168.1.1
6	73 ms	73 ms	73 ms	192.168.1.2
7	78 ms	78 ms	77 ms	192.168.1.1
8	102 ms	99 ms	99 ms	192.168.1.2
9	105 ms	103 ms	109 ms	192.168.1.1
10	142 ms	139 ms	125 ms	192.168.1.2
11	135 ms	130 ms	130 ms	192.168.1.1
12	153 ms	151 ms	151 ms	192.168.1.2
13	156 ms	155 ms	155 ms	192.168.1.1
14	177 ms	177 ms	177 ms	192.168.1.2
15	182 ms	181 ms	182 ms	192.168.1.1
16	203 ms	203 ms	203 ms	192.168.1.2
17	208 ms	207 ms	208 ms	192.168.1.1
18	229 ms	229 ms	229 ms	192.168.1.2
19	233 ms	233 ms	233 ms	192.168.1.1
20	255 ms	255 ms	255 ms	192.168.1.2
21	259 ms	259 ms	259 ms	192.168.1.1
22	281 ms	281 ms	281 ms	192.168.1.2
23	285 ms	285 ms	285 ms	192.168.1.1
24	306 ms	307 ms	306 ms	192.168.1.2
25	311 ms	311 ms	311 ms	192.168.1.1
26	333 ms	333 ms	332 ms	192.168.1.2
27	373 ms	372 ms	373 ms	192.168.1.1
28	359 ms	359 ms	359 ms	192.168.1.2
29	404 ms	379 ms	364 ms	192.168.1.1
30	384 ms	385 ms	384 ms	192.168.1.2

跟踪完成。

C:\Users\user>

由以上输出可以看到，到目的地址 3.3.3.3 的报文匹配了缺省路由，报文被转发到了 1-R1，而 1-R2 又根据它的缺省路由，把报文转发回了 1-R1。这样就形成了转发环路，报文在两台路由器之间被循环转发，直到 TTL 值到 0 后被丢弃。

所有在不同路由器上配置到相同网段的静态路由时，不要配置路由的下一跳互相指向对方，否则就形成环路。

实验10 RIP 协议配置

10.1 实验内容与目标

- 加深 RIP 协议原理的理解
- 了解 RIP 实现运行机制
- 熟悉 RIP 路由配置
- 熟悉 RIP 路由维护

10.2 实验组网图

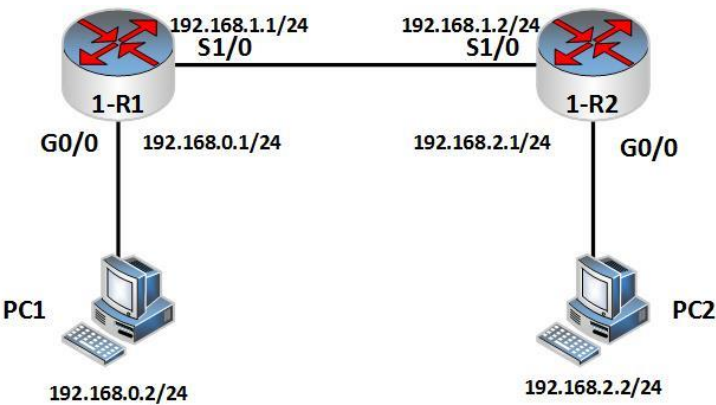


图 10-1 RIP 实验组网图

10.3 实验过程

实验任务一：配置 RIPv1

本实验主要通过配置在路由器上配置 RIPv1 协议，达到 pc 之间能够互访的目的。通过本次实验，学生应能够掌握 RIPv1 协议的基本配置。

按照图 10-1 进行连接，并检查设备的软件版本及配置信息，确保各设备软件版本符合要求，所有配置为初始状态。如果配置不符合要求，请在用户模式下擦除设备中的配置文件，然后重启设备以使系统采用缺省的配置参数进行初始化。

步骤一：在 pc 和路由器配置 IP 地址

表 10-1 IP 地址列表

设备名称	接口	IP 地址	网关
1-R1	S1/0	192.168.1.1/24	--
	G0/0	192.168.0.1/24	--

1-R2	S1/0	192.168.1.2/24	--
	G0/0	192.168.2.1/24	--
PC1		192.168.0.2/24	192.168.0.1/24
PC2		192.168.2.2/24	192.168.2.1/24

配置 1-R1:

```
[1-R1]int S1/0
[1-R1-Serial1/0]ip ad 192.168.1.1 24
[1-R1-Serial1/0]int g 0/0
[1-R1-GigabitEthernet0/0]ip ad 192.168.0.1 24
```

配置 1-R2:

```
[1-R2]int s1/0
[1-R2-Serial1/0]ip ad 192.168.1.2 24
[1-R2-Serial1/0]int g 0/0
[1-R2-GigabitEthernet0/0]ip ad 192.168.2.1 24
```

按表 10-1 所示配置 IP 地址和网关。配置完成后，在 windows 下用命令查看，如下所示:

```
C:\Users\user>ping 192.168.0.1
```

正在 Ping 192.168.0.1 具有 32 字节的数据:

来自 192.168.0.1 的回复: 字节=32 时间<1ms TTL=255

来自 192.168.0.1 的回复: 字节=32 时间<1ms TTL=255

来自 192.168.0.1 的回复: 字节=32 时间<1ms TTL=255

来自 192.168.0.1 的回复: 字节=32 时间<1ms TTL=255

192.168.0.1 的 Ping 统计信息:

数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):

最短 = 0ms, 最长 = 0ms, 平均 = 0ms

```
C:\Users\user>ping 192.168.2.2
```

正在 Ping 192.168.2.2 具有 32 字节的数据:

请求超时。

请求超时。

请求超时。

请求超时。

192.168.2.2 的 Ping 统计信息:

数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),

PC 的网关返回了目的网络不可达的信息。这说明路由器没用到达目的。在路由器上查看路由表。例如，在 1-R1 上查看路由表，如下:

```
[1-R1]dis ip routing-table
```

Destinations : 17

Routes : 17

Destination/Mask	Proto	Pre Cost	NextHop	Interface
0.0.0.0/32	Direct	0 0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0 0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0 0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0 0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0 0	127.0.0.1	InLoop0
192.168.0.0/24	Direct	0 0	192.168.0.1	GE0/0
192.168.0.0/32	Direct	0 0	192.168.0.1	GE0/0
192.168.0.1/32	Direct	0 0	127.0.0.1	InLoop0
192.168.0.255/32	Direct	0 0	192.168.0.1	GE0/0
192.168.1.0/24	Direct	0 0	192.168.1.1	S1/0
192.168.1.0/32	Direct	0 0	192.168.1.1	S1/0
192.168.1.1/32	Direct	0 0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0 0	192.168.1.2	S1/0
192.168.1.255/32	Direct	0 0	192.168.1.1	S1/0
224.0.0.0/4	Direct	0 0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0 0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0 0	127.0.0.1	InLoop0

可以看到，1-R1 路由表中没有到 PC2 所在网段 192.168.2.0 的路由。所以当 pc 发出到报文到 1-R1 后，1-R1 就丢弃并返回不可达信息给 PC1。我们可以在路由器上配置 RIP 协议来解决这个问题。

步骤三：启用 RIP 协议

```
[1-R1]rip
[1-R1-rip-1]network 192.168.0.0
[1-R1-rip-1]network 192.168.1.0
```

```
[1-R2]rip
[1-R2-rip-1]network 192.168.1.0
[1-R2-rip-1]network 192.168.2.0
```

配置完成后，在 1-R1 路由器上查看路由表。如下：

```
[1-R1]dis ip routing-table
```

Destinations : 18 Routes : 18

Destination/Mask	Proto	Pre Cost	NextHop	Interface
0.0.0.0/32	Direct	0 0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0 0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0 0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0 0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0 0	127.0.0.1	InLoop0
192.168.0.0/24	Direct	0 0	192.168.0.1	GE0/0
192.168.0.0/32	Direct	0 0	192.168.0.1	GE0/0
192.168.0.1/32	Direct	0 0	127.0.0.1	InLoop0

192.168.0.255/32	Direct	0	0	192.168.0.1	GE0/0
192.168.1.0/24	Direct	0	0	192.168.1.1	S1/0
192.168.1.0/32	Direct	0	0	192.168.1.1	S1/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	S1/0
192.168.1.255/32	Direct	0	0	192.168.1.1	S1/0
192.168.2.0/24	RIP	100	1	192.168.1.2	S1/0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

可以看到路由表中有到目的网络 192.168.2.0/24 的路由, 这个路由是通过 RIP 学习到的。

然后再测试 pc 间的可达性。如下:

C:\Users\user>ping 192.168.2.2

正在 Ping 192.168.2.2 具有 32 字节的数据:

来自 192.168.2.2 的回复: 字节=32 时间=18ms TTL=126

来自 192.168.2.2 的回复: 字节=32 时间=18ms TTL=126

来自 192.168.2.2 的回复: 字节=32 时间=18ms TTL=126

来自 192.168.2.2 的回复: 字节=32 时间=18ms TTL=126

192.168.2.2 的 Ping 统计信息:

数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),

往返行程的估计时间(以毫秒为单位):

最短 = 18ms, 最长 = 18ms, 平均 = 18ms

步骤四: 查看 RIP 的运行状态

[1-R1]dis rip

Public VPN-instance name:

RIP process: 1

RIP version: 1

Preference: 100

Checkzero: Enabled

Default cost: 0

Summary: Enabled

Host routes: Enabled

Maximum number of load balanced routes: 32

Update time : 30 secs Timeout time : 180 secs

Suppress time : 120 secs Garbage-collect time : 120 secs

Update output delay: 20(ms) Output count: 3

Silent interfaces: None

Default routes: Disabled

Verify-source: Enabled

Networks:


```
192.168.0.0          192.168.1.0
Configured peers: None
Triggered updates sent: 2
Number of routes changes: 3
Number of replies to queries: 1
```

从以上输出信息可知，目前路由器运行的是 RIP v1，自动聚合功能是打开；路由更新周期（update time）是 30 秒，network 命令所指定的网段是 192.168.1.0，192.168.0.0。

打开 RIP 的 debugging，观察 RIP 收发协议报文的情况。

```
<1-R1>terminal debugging
```

The current terminal is enabled to display debugging logs.

```
<1-R1>debugging rip 1 packet
```

```
<1-R1>*Dec  7 09:58:59:565 2015 1-R1 RIP/7/RIPDEBUG: RIP 1 : Sending response on
interface GigabitEthernet0/0 from 192.168.0.1 to 255.255.255.255
```

```
*Dec  7 09:58:59:565 2015 1-R1 RIP/7/RIPDEBUG:   Packet: version 1, cmd response,
length 44
```

```
*Dec  7 09:58:59:565 2015 1-R1 RIP/7/RIPDEBUG:       AFI 2, destination 192.168.1.0,
cost 1
```

```
*Dec  7 09:58:59:566 2015 1-R1 RIP/7/RIPDEBUG:       AFI 2, destination 192.168.2.0,
cost 2
```

```
*Dec  7 09:58:59:566 2015 1-R1 RIP/7/RIPDEBUG: RIP 1 : Sending response on interface
Serial1/0 from 192.168.1.1 to 255.255.255.255
```

```
*Dec  7 09:58:59:566 2015 1-R1 RIP/7/RIPDEBUG:   Packet: version 1, cmd response,
length 24
```

```
*Dec  7 09:58:59:566 2015 1-R1 RIP/7/RIPDEBUG:       AFI 2, destination 192.168.0.0,
cost 1
```

```
*Dec  7 09:59:00:005 2015 1-R1 RIP/7/RIPDEBUG: RIP 1 : Receiving response from
192.168.1.2 on Serial1/0
```

```
*Dec  7 09:59:00:006 2015 1-R1 RIP/7/RIPDEBUG:   Packet: version 1, cmd response,
length 24
```

```
*Dec  7 09:59:00:006 2015 1-R1 RIP/7/RIPDEBUG:       AFI 2, destination 192.168.2.0,
cost 1
```

结束实验后关闭 debugging 信息。

```
<1-R1>undo terminal debugging
```

实验11 OSPF 协议配置

11.1 实验内容与目标

- 掌握单区域 OSPF 配置方法
- 掌握 OSPF 路由选择的方法

11.2 实验组网图

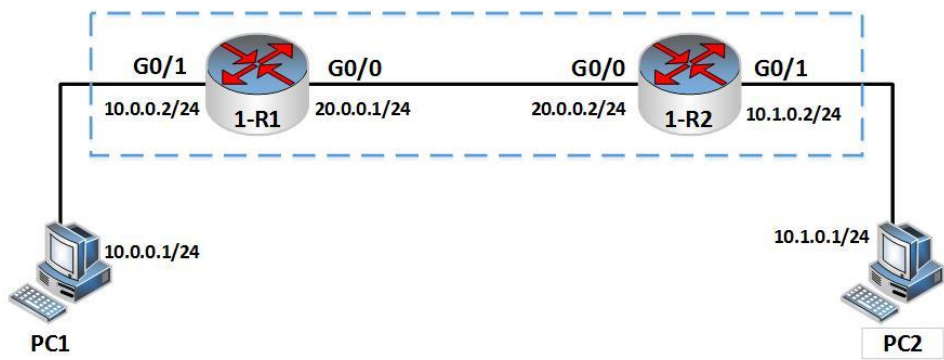


图 11-1 实验任务一环境图

11.3 实验过程

实验任务一：单区域 OSPF 基本配置

步骤一：搭建实验环境

按照图 11-1 进行连接，并检查设备的软件版本及配置信息，确保各设备软件版本符合要求，所有配置为初始状态。如果配置不符合要求，请在用户模式下擦除设备中的配置文件，然后重启设备以使系统采用缺省的配置参数进行初始化。

步骤二：在 pc 和路由器配置 IP 地址

表 11-1 IP 地址列表

设备名称	接口	IP 地址	网关
1-R1	G0/0	20.0.0.1/24	--
	G0/1	10.0.0.2/24	--
1-R2	G0/0	20.0.0.2/24	--
	G0/1	10.1.0.2/24	--
PC1		10.0.0.1/24	10.0.0.2
PC2		10.1.0.1/24	10.1.0.2

```
[1-R1]int GigabitEthernet 0/0
[1-R1-GigabitEthernet0/0]ip add 20.0.0.1 24
[1-R1-GigabitEthernet0/0]int g0/1
[1-R1-GigabitEthernet0/1]ip add 10.0.0.2 24
[1-R1-GigabitEthernet0/1]int loopback 0
[1-R1-LoopBack0]ip add 1.1.1.1 32
```

```
[1-R2]int GigabitEthernet 0/0
[1-R2-GigabitEthernet0/0]ip add 20.0.0.2 24
[1-R2-GigabitEthernet0/0]int g0/1
[1-R2-GigabitEthernet0/1]ip add 10.1.0.2 24
[1-R2-GigabitEthernet0/1]int loopback 0
[1-R2-LoopBack0]ip add 2.2.2.2 32
```

步骤三：检查网络连通性和路由器路由表

在 PC1 上 ping PC2，显示如下：

```
C:\Users\user>ping 10.1.0.1
```

正在 Ping 10.1.0.1 具有 32 字节的数据：

请求超时。

请求超时。

请求超时。

请求超时。

10.1.0.1 的 Ping 统计信息：

数据包：已发送 = 4，已接收 = 0，丢失 = 4 (100% 丢失)，

结果显示，无法 ping 通。这是因为在 1-R1 上没有到 10.1.0.1 的路由。

在 1-R1 上使用 `dis ip routing-table` 命令查看路由表，显示如下：

```
[1-R1]dis ip routing-table
```

Destinations : 17

Routes : 17

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
1.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.0.0.0/24	Direct	0	0	10.0.0.2	GE0/1
10.0.0.0/32	Direct	0	0	10.0.0.2	GE0/1
10.0.0.2/32	Direct	0	0	127.0.0.1	InLoop0
10.0.0.255/32	Direct	0	0	10.0.0.2	GE0/1
20.0.0.0/24	Direct	0	0	20.0.0.1	GE0/0
20.0.0.0/32	Direct	0	0	20.0.0.1	GE0/0
20.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
20.0.0.255/32	Direct	0	0	20.0.0.1	GE0/0

127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

1-R1 上只有直连路由，没有到达 PC2 的路由表项。

步骤四：配置 OSPF

```
[1-R1]router id 1.1.1.1
[1-R1]ospf 1
[1-R1-ospf-1]area 0
[1-R1-ospf-1-area-0.0.0.0]network 1.1.1.1 0.0.0.0
[1-R1-ospf-1-area-0.0.0.0]network 10.0.0.0 0.0.0.255
[1-R1-ospf-1-area-0.0.0.0]network 20.0.0.0 0.0.0.255
```

```
[1-R2]router id 2.2.2.2
[1-R2]ospf 1
[1-R2-ospf-1]area 0
[1-R2-ospf-1-area-0.0.0.0]network 2.2.2.2 0.0.0.0
[1-R2-ospf-1-area-0.0.0.0]network 10.1.0.0 0.0.0.255
[1-R2-ospf-1-area-0.0.0.0]network 20.0.0.0 0.0.0.255
```

步骤五：检查路由器 OSPF 邻居状态及路由表

在 1-R1 上使用 display ospf peer 命令查看 OSPF 邻居状态，显示如下：

```
[1-R1]dis ospf peer
```

OSPF Process 1 with Router ID 1.1.1.1

Neighbor Brief Information

Area: 0.0.0.0

Router ID	Address	Pri	Dead-Time	State	Interface
2.2.2.2	20.0.0.2	1	38	Full/BDR	GE0/0

1-R1 与 router id 为 2.2.2.2 的路由器上配置 IP 地址 20.0.0.2 的接口互为邻居，1-R2 的配置 IP 地址 20.0.0.2 的接口为该网段的 DR 路由器。此时，邻居状态达到 full，说明 1-R1 和 1-R2 之间的链路状态数据库已经同步，1-R1 具备到达 1-R2 的路由信息。

在 1-R1 上使用 display ospf routing 命令查看路由器的 OSPF 的 OSPF 路由表，显示如下：

```
[1-R1]dis ospf routing
```

OSPF Process 1 with Router ID 1.1.1.1

Routing Table

Routing for network

Destination	Cost	Type	NextHop	AdvRouter	Area
-------------	------	------	---------	-----------	------

20.0.0.0/24	1	Transit	0.0.0.0	1.1.1.1	0.0.0.0
10.0.0.0/24	1	Stub	0.0.0.0	1.1.1.1	0.0.0.0
2.2.2.2/32	1	Stub	20.0.0.2	2.2.2.2	0.0.0.0
10.1.0.0/24	2	Stub	20.0.0.2	2.2.2.2	0.0.0.0
1.1.1.1/32	0	Stub	0.0.0.0	1.1.1.1	0.0.0.0

Total nets: 5

Intra area: 5 Inter area: 0 ASE: 0 NSSA: 0

[1-R1]dis ip routing-table

Destinations : 19 Routes : 19

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
1.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
2.2.2.2/32	O_INTRA	10	1	20.0.0.2	GE0/0
10.0.0.0/24	Direct	0	0	10.0.0.2	GE0/1
10.0.0.0/32	Direct	0	0	10.0.0.2	GE0/1
10.0.0.2/32	Direct	0	0	127.0.0.1	InLoop0
10.0.0.255/32	Direct	0	0	10.0.0.2	GE0/1
10.1.0.0/24	O_INTRA	10	2	20.0.0.2	GE0/0
20.0.0.0/24	Direct	0	0	20.0.0.1	GE0/0
20.0.0.0/32	Direct	0	0	20.0.0.1	GE0/0
20.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
20.0.0.255/32	Direct	0	0	20.0.0.1	GE0/0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

(注: O_INTRA: OSPF intra area)

此时，全网络是连通的。

在 PC1 上 ping PC2:

C:\Users\user>ping 10.1.0.1

可以 ping 通。

实验 12 网络报文捕获与分析

● 实验任务

1. 了解和掌握以太网帧、IP 报文、ICMP 报文、TCP 报文格式；
2. 了解数据报各字段的功能。
3. 了解应用层协议报文解析。

● 实验环境

1. WindowsXP IE 浏览器
2. TCP/IP 协议
3. 江南大学校园网环境

● 实验内容

1. 安装报文捕获工具 iris
2. iris 的基本运行
 - a) Iris 运行界面

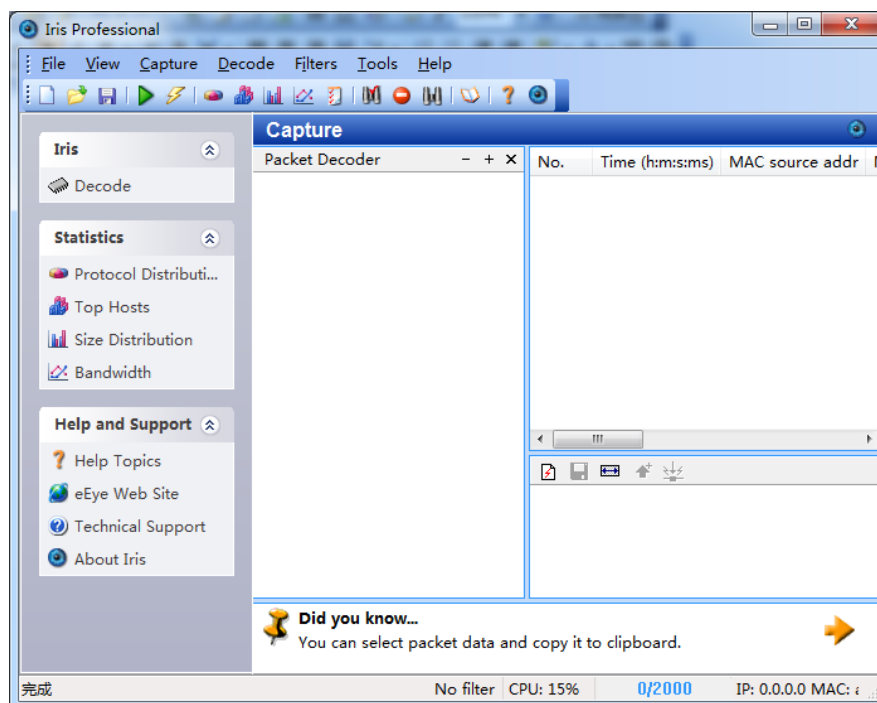


图 1 iris 运行界面

b) Iris 过滤规则设置

通过点击 Filters->Edit Filter, 进行过滤规则设置。如图 2, 通过点击 Layer 2, 3, 只选择捕获 ICMP 报文。其他类型过滤规则, 如 Ports (端口) 等, 可以尝试设置。

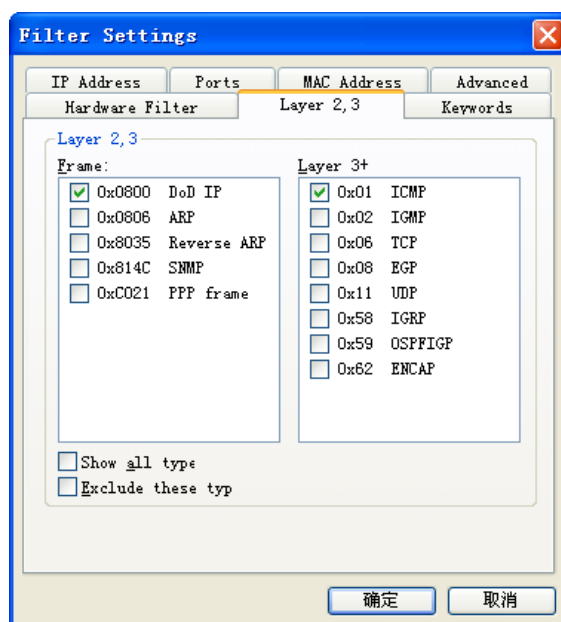


图 2 Iris 过滤规则设置

c) Iris 报文捕获开始与终止

点击 “start/stop capture”, 进行报文捕获开始与终止。

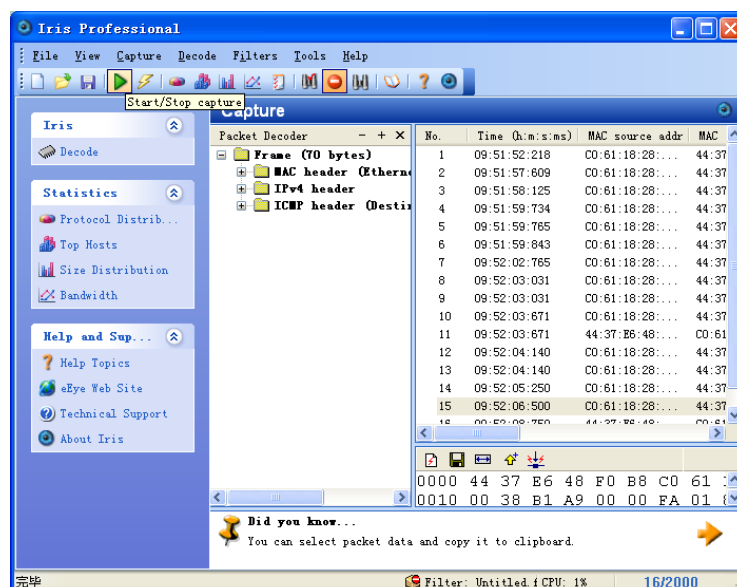


图 3 Iris 报文捕获开始/终止

d) Iris 捕获报文分析实例

如图 4，右侧每行对应一个捕获的报文，点击任意报文，右侧下方显示该报文的 16 进制内容。通过点开“packet Decoder”，可以获得该报文的每一个域的详细信息。

参照《计算机网络》教科书的“以太网 MAC 帧格式”；“IP 数据报的格式”；“ICMP 协议报文的格式”；“UDP 报文段的格式”；“TCP 报文段的格式”等，看看所捕获的报文是否与这些格式对应。

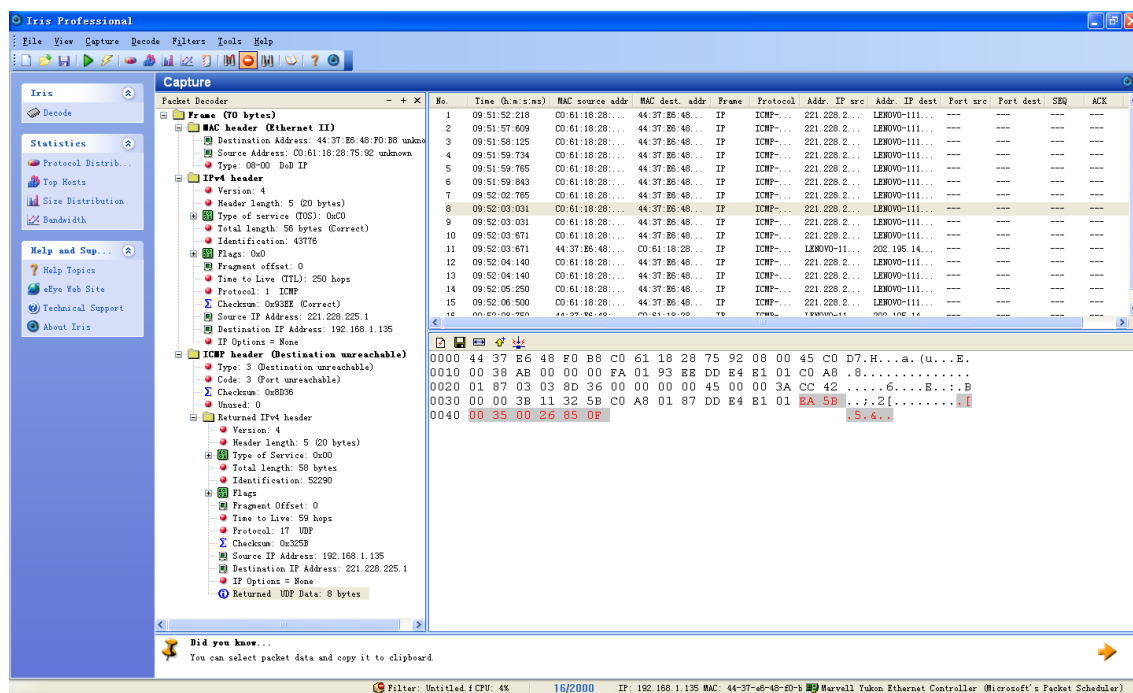


图 4 Iris 报文捕获开始/终止

3. ICMP 报文捕获与分析

- 设置过滤规则，仅捕获 ICMP 报文，并启动报文捕获；
- 运行“Ping www.jiangnan.edu.cn”；（或者其他网址）
- 针对所捕获的报文，选出 1 个“Ping www.jiangnan.edu.cn”所获得的 ICMP 报文，并结合“以太网 MAC 帧格式”；“IP 数据报的格式”；“ICMP 协议报文的格式”；并对其各字段进行分析，给出每一个域的 16 进制码，以及所对应的含义。

```
C0 61 18 28 75 92 44 37 E6 48 F0 B8 08 00 45 00
00 3C CC 7F 00 00 40 01 90 C7 C0 A8 01 87 CA C3
90 87 08 00 47 5C 02 00 04 00 61 62 63 64 65 66
67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76
77 61 62 63 64 65 66 67 68 69
```

图 5 ICMP 报文 16 进制码

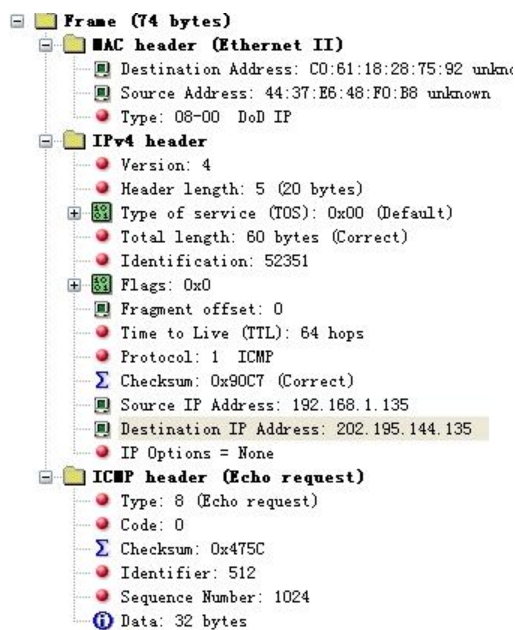


图 6 ICMP 报文解析

4. TCP 三次握手报文捕获与分析

- 设置过滤规则，仅捕获 TCP 协议的 80 端口报文，并启动报文捕获；
- 通过 IE 浏览器浏览江南大学主页 <http://www.jiangnan.edu.cn>；
- 针对所捕获的报文，选出“<http://www.jiangnan.edu.cn>”所对应的 3 次握手报文，参照“TCP 报文段的格式”对前两个报文各字段进行分析。

```

C0 61 18 28 75 92 44 37 E6 48 F0 B8 08 00 45 00
00 34 1D 89 40 00 40 06 FF C0 C0 A8 01 87 CA C3
90 87 0A F7 00 50 EC 4E 81 87 00 00 00 00 80 02
FF FF D8 7D 00 00 02 04 05 B4 01 03 03 03 01 01
04 02

```

图 7 TCP 报文三次握手报文 16 进制码

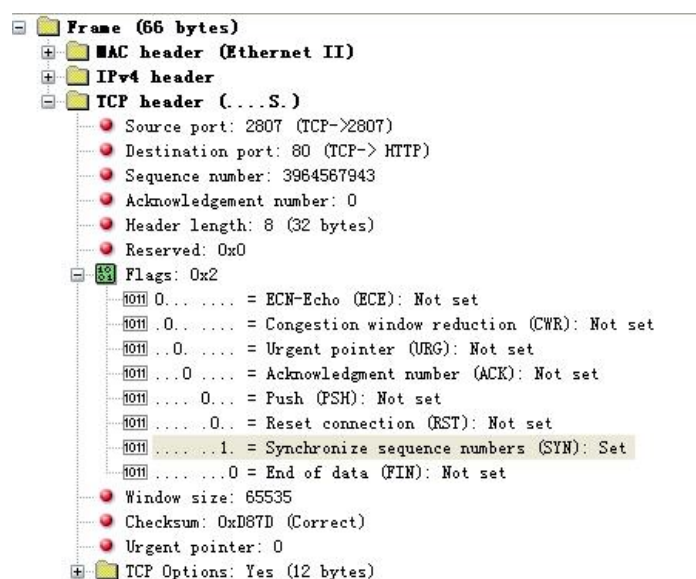


图 8 TCP 报文三次握手报文 16 进制码

5. 用户名与密码分析

- 设置过滤规则，仅捕获 TCP 协议的 80 端口报文，并启动报文捕获；
- 通过 IE 浏览器浏览江南大学主页 <http://bbs.jiangnan.edu.cn>（或者其他需要输入用户名和密码的网页）；并输入用户名和密码；
- 针对所捕获的报文，选出登陆“<http://bbs.jiangnan.edu.cn>”所对应报文，看看你的用户名和密码在哪儿？

```
65 6E 67 74 68 3A 20 37 38 0D 0A 43 6F 6E 6E 65 ength: 78..Conne
63 74 69 6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 76 ction: Keep-Aliv
65 0D 0A 43 61 63 68 65 2D 43 6F 6E 74 72 6F 6C e..Cache-Control
3A 20 6E 6F 2D 63 61 63 68 65 0D 0A 0D 0A 69 64 : no-cache....id
3D 6D 6F 6F 6E 68 65 73 73 26 70 61 73 73 77 64 =moonhess&passwd
3D 31 66 6F 78 33 26 77 65 62 73 65 6C 65 63 74 =lfox3&webselect
3D 31 26 63 6F 6D 65 75 72 6C 3D 25 32 46 69 6E =1&comeurl=%2Fin
64 65 78 2E 70 68 70 26 73 75 62 6D 69 74 31 3D dex.php&submit1=
25 42 35 25 43 37 25 43 32 25 42 43 %B5%C7%C2%BC
```

图 9 BBS 用户名与密码解析