第3章 路由技术实验

随着信息技术的发展，计算机网络在人们的工作和生活中的作用越来越大，路由选择和交换理论是组建可靠网络的基础，路由器在不同网络之间的通信过程中对路由选择起到了关键作用。本章实验主要介绍路由器基本配置、路由器基本维护、系统管理、链路层协议、网络协议、路由协议、组播协议、QoS、语音。通过本章的实验，能够进一步理解常见协议的基本原理，较熟练地掌握配置路由器以组建网络的方法和技能。

实验 3-1 路由器配置基础

【实验背景】

路由器工作在 OSI 参考模型第三层（网络层），用来解决不同网络的数据转发问题，它有“边界路由器”和“中间节点路由器”两种。“边界路由器”处于网络边界的边缘或末端，用于不同网络的连接，如连接企业局域网和广域网（如因特网），这也是目前大多数路由器的类型，这类路由器所支持的网络协议和路由协议比较广，背板带宽非常高，具有较高的吞吐能力，以满足各类不同类型网络的互联；而“中间节点路由器”则处于局域网的内部，通常用于连接不同局域网，起到一个数据转发的桥梁作用。中间节点路由器更注重 MAC 地址的记忆能力，要求较大的缓存。因为所连接的网络基本上是局域网，所以所支持的网络协议比较单一，背板带宽也较小，这些都是为了获得最高的性价比，适应一般企业的随机能力。路由器必须先对其进行正确配置才能正常工作，网络管理员对路由器进行初始配置前，必须通过路由器的 Console 口搭建配置环境。网络管理员通过 Console 口对路由器进行初始配置后，可以通过 Telnet 对路由器进行远程管理。

【实验目的】

（1）掌握路由器的管理特性，学会配置路由器的基本方法。

（2）掌握配置路由器的命令行视图及常用命令的使用方法。

（3）掌握通过 Console 口、Telnet 登录、本地用户 Console 登录并配置路由器的方法。

【实验内容】

（1）在交换机上划分 VLAN。

（2）将交换机配置成 DHCP 服务器，使用户动态获取相应网段的 IP 地址。

【实验设备】

H3C 系列路由器一台,PC 一台或两台,专用配置电缆一根,交叉双绞线一根。配置路由器如图 3.1 所示。

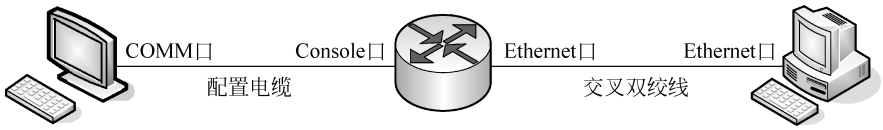

图 3.1　通过 Console 口/Telnet 配置路由器

【实验步骤】

(1) 通过 Console 口配置路由器。

① 按图 3.1 搭建实验环境。

将 PC 终端的 COMM 口通过配置电缆与路由器的 Console 口连接。

② 创建超级终端。

设置终端通信参数,波特率为 9600b/s、数据位为 8 位、停止位为 1 位、无奇偶校验和无数据流控制,如图 3.2 所示。

③ 命令行接口。

启动路由器,单击"确定"按钮,终端上显示路由器自检信息。自检结束后提示用户按 Enter 键,进入路由器命令行视图。

图 3.2　超级终端设置

```
<H3C>
```

(2) 通过 Telnet 配置路由器实验。

① 配置路由器的 IP 地址。

```
<H3C>
<H3C>system-view
[H3C]interface Ethernet 0/0
[H3C-Ethernet 0/0]ip address 192.168.10.10 255.255.255.0
```

② 在路由器上配置 Telnet 用户认证口令。

```
<H3C>system-view
Enter system view , return user view with Ctrl+Z.
[H3C]local-user CQUT                          //创建一个名为 CQUT 的用户
[H3C-luser-CQUT]password simple jsjxy         //用户 CQUT 的密码是 jsjxy
[H3C-luser-CQUT]service-type telnet level 1   //设置用户的类型、级别
```

③ 配置 PC 的 IP 地址和子网掩码,使之与路由器的 IP 地址在同一网段。例如,IP 地址为 192.168.10.15,子网掩码为 255.255.255.0。

④ 在 PC 上运行 Telnet 程序，输入路由器的 IP 地址，然后单击“确定”按钮，如图 3.3 所示。

⑤ 终端上显示“Username：”，提示用户输入用户名，这时输入前面建立的用户名 CQUT；接着出现“Password:”，提示用户输入已设置的登录密码，这时输入前面设置的用户密码 jsjxy，密码输入正确后则出现命令行提示符< H3C >，如图 3.4 所示。注意，输入密码时没有任何显示，包括星号(*)。

图 3.3　运行 Telnet

```
**************************************************************
*          All rights reserved (1997-2004)                   *
*      Without the owner's prior written consent,            *
*no decompiling or reverse-engineering shall be allowed.*
**************************************************************


Login authentication


Username:CQUT
Password:
```

图 3.4　Telnet 登录界面

注意：

① 通过 Telnet 配置路由器时，不要删除或修改对应本 Telnet 连接路由器上接口的 IP 地址，否则会导致 Telnet 连接断开。

② 上面 Telnet 用户登录时，可以访问命令级别为 1 级的命令。如果在路由器执行下列命令后断开 Telnet，再重新连接，比较一下前后的差异：

```
[H3C-luser-CQUT]service-type telnet level 3
```

(3) 命令行接口视图。

路由器命令行提供多种视图，针对不同的命令细则，需要在相应的视图中进行配置。

路由器常见命令视图如表 3.1 所示。

表 3.1　路由器命令行视图

命令视图	功　能	提　示　符	进入命令	退出命令
用户视图	查看路由器状态	< H3C >	与路由器建立连接即进入	Quit
系统视图	配置系统参数	[H3C]	System-view	Quit
RIP 视图	配置 RIP 协议	[H3C-rip]	rip	Quit
OSPF 视图	配置 OSPF 协议	[H3C-ospf-1]	ospf 1	Quit
BGP 视图	配置 BGP 协议	[H3C-bgp]	bgp 1	Quit
路由策略视图	配置路由策略	[H3C-route-policy]	route-policy abc permit node 1	Quit
PIM 视图	配置组播路由	[H3C-pim]	multicast routing-enable,pim	Quit
同步串口视图	配置同步串口	[H3C-Serial0/0]	interface Serial0/0	Quit
以太网接口	配置以太网接口	[H3C-Ethernet0/0]	interface Ethernet0/0	Quit
AUX 接口视图	配置 AUX 接口	[H3C-Aux0]	interface Aux 0	Quit
LoopBack 接口	配置 LoopBack 接口	[H3C-LoopBack1]	interface LoopBack 1	Quit

(4) 实验常用命令。

① 查看当前设备配置。

```
<H3C>display current-configuration
```

② 保存当前设备配置。

```
<H3C>save
```

③ 查看 Flash 中的配置信息。

```
<H3C>display saved-configuration
```

④ 删除 Flash 中的配置信息。

```
<H3C>reset saved-configuration
```

⑤ 重启路由器。

```
<H3C>reboot
```

⑥ 显示系统版本信息。

```
<H3C>display version
```

⑦ 显示历史命令,命令行接口为每个用户默认保存 10 条历史命令。

```
[H3C]display history-command
```

⑧ 查看接口状态。

```
[H3C]display interface
```

⑨ 查看路由表。

```
[H3C]display ip routing-table
```

⑩ 关闭/启用端口。

```
[H3C-Serial3/0]shutdown
[H3C-Serial3/0]undo shutdown
```

注意:串口的配置需要在接口配置视图下完成上述命令后才生效。

⑪ 设备重新命名,设备的默认名为 H3C。

```
[H3C]sysname CQUT                                    //把设备的名字更改为 CQUT
```

(5) 路由器编辑特性介绍,在对路由器的配置过程中可以进行下列操作:

- 普通按键:输入字符到当前光标位置。
- 退格键 BackSpace:删除光标位置的前一个字符。
- 左光标键←:光标向左移动一个字符位置。
- 右光标键→:光标向右移动一个字符位置。
- 上下光标键↑↓:显示历史命令。
- Tab 键:系统用完整的关键字替代原输入并换行显示。

输入关键字时，可以不必输入关键字的全部字符而只输入关键字的前几个字符，只要设备能唯一识别，如 display 可以只输入 dis。

(6) 显示特性介绍：

Language-mode：在用户视图下使用该命令可以实现中英文显示方式切换。

暂停显示时输入“Ctrl＋C”：当信息一屏显示不完时，按此键可以停止显示和命令执行。

暂停显示时输入空格键：当信息一屏显示不完时，按此键可以继续显示下一屏信息。

暂停显示时输入 Enter 键：当信息一屏显示不完时，按此键可以继续显示下一行信息。

(7) 在线帮助介绍：

① 完全帮助：在任何视图下，输入<?>获取该视图下所有命令及其简单描述。

② 部分帮助：

输入一命令，后接以空格间隔的<?>，如< H3C > display ?，如果该位置是关键字，则列出全部关键字及其简单描述；如果该位置为参数，则列出有关的参数及其描述。

输入一字符串，其后紧跟<?>，如< H3C > p? 则列出以该字符串开头的所有命令。

输入一命令，其后紧接一“?”的字符串，如< H3C > display ver?，则列出该字符串开头的所有关键字。

(8) 错误提示：当输入有误时将给以相应的错误提示。

```
[H3C] dispaly
          ^
         % Unrecognized command found at '^' position.
[H3C] display
                  ^
         % Incomplete command found at '^' position.
[H3C] display interface serial 0 0
                                ^
         % Wrong parameter found at '^' position.
```

(9) 使用本地用户进行 Console 登录的认证实验。

```
< H3C > system - view
Enter system view , return user view with Ctrl + Z.
[H3C] user - interface console 0                          //进入 console 视图
[H3C - ui - console0] authentication - mode scheme        //设置 scheme 认证
[H3C - ui - console0] quit
[H3C] local - user CQUT                                   //创建一个名为 CQUT 的用户
[H3C - luser - CQUT] password simple jsjxy                //用户 CQUT 的密码是 jsjxy
[H3C - luser - CQUT] service - type terminal level 3      //设置用户的类型、级别
[H3C - luser - CQUT] quit
[H3C] quit
< H3C > save                                              //保存配置
< H3C > reboot                                            //重启路由器
```

然后再按步骤(1)的实验过程继续，当路由器上显示“Username:”，提示用户输入用户名，这时输入刚刚建立的用户 CQUT；接着出现“Password:”，提示用户输入已设置的登录

密码,这时又输入设置的用户密码 jsjxy,密码输入正确后则出现命令行提示符< H3C >。注意,输入密码时没有任何显示,包括星号(*)。

【思考题】

(1) 如何将路由器还原为出厂配置?

(2) 路由器和三层交换机的区别是什么?

实验 3-2　路由器维护技术

【实验背景】

一般情况下,路由器有以下 4 种存储介质:

(1) DRAM/SDRAM(动态随机存取存储器/同步动态随机存取存储器):作为主存储器,VRP 主程序在它上面运行。

(2) Flash(闪速存储器):主要保存 VRP 主程序及配置文件等。

(3) BOOTROM(引导只读存储器):用来存储引导程序。

(4) NVRAM(非易失性随机存取存储器):用于保存配置文件。

路由器的启动和工作都是靠存储在这些介质上的程序和相关配置文件进行的。当路由器的 VRP 或 BOOTROM 出现 BUG 或进行修改后需要对其进行升级,忘记或要修改 Console 配置口的密码时需要进行相关的维护操作。

【实验目的】

(1) 掌握用 CLI FTP 对 BOOTROM 进行升级的方法。

(2) 掌握用 CLI FTP 对 VRP 进行升级的方法。

(3) 掌握清除进入 console 配置口的密码的方法。

【实验内容】

(1) 用 CLI FTP 对 BOOTROM 进行升级;

(2) 用 CLI FTP 对 VRP 进行升级;

(3) 清除进入 Console 配置口的密码。

【实验设备】

H3C 系列路由器一台,PC 两台,交叉双绞线一根,专用配置电缆一根。路由器基本维护拓扑结构如图 3.5 所示。

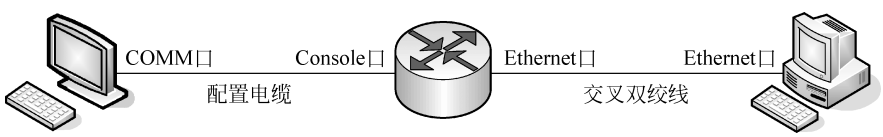

图 3.5　路由器基本维护拓扑结构图

【实验步骤】

(1) 用 CLI FTP 对 BOOTROM 进行升级：

① 在路由器上启动 FTP server，并配置账号和密码、以太网接口地址：

```
<H3C>system-view
[H3C]ftp server enable
[H3C]local-user CQUT
[H3C-luser-CQUT]password simple jsjxy
[H3C-luser-CQUT]service-type ftp
[H3C-Ethernet0/0]ip address 10.0.101.253 24
```

② 配置另一台计算机的地址和路由器的地址在同一网段，设 IP 地址为 10.0.101.111，子网掩码为 255.255.255.0，再在此计算机上运行 FTP，按照提示依次输入用户名 CQUT 和密码 jsjxy，并设置本地目录为 C:\和更改为二进制传输方式即 bin，设置显示传输进度即 hash，如图 3.6 所示。

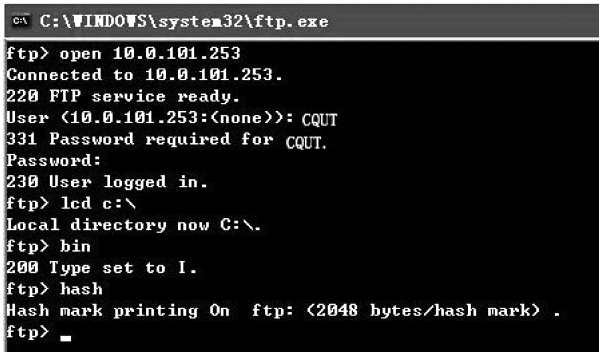

图 3.6　FTP 登录路由器示意图

③ 上载 Bootrom 9.07 的 full 升级文件(假设文件名称为 907bootromfull，大小为 512KB，在计算机的 C:\目录下)。

```
ftp>put 907bootromfull bootromfull
200 Port command okay.
150 Server okay , now receive file.
226 file transmit success.
ftp: 524288 bytes sent in 6.66Seconds 78.77Kbytes/sec.
ftp>
```

之后路由器提示：

```
Ftp server is currently writing to flash , please wait...
Ftp server writing to flash is done.
```

④ 执行 upgrade bootrom full 升级 BOOTROM。

```
<H3C>upgrade bootromfull
  WARNING: The operation is to update the Boot ROM.
       It may result in booting failure.
```

```
Caution!!! upgrade bootrom [Y/N]?y
Please wait, it may take a long time
upgrade succeeds!
```

⑤ 重启路由器,查看 BOOTROM 版本,确认升级成功。

```
Starting at 0x1c00000...
    ********************************************
    *                      *
    *   H3C Series Routers Boot ROM, V9.07   *
    *                      *
    ********************************************
  Copyright(C) 1997 - 2004 by H3C TECH CO., LTD.
  Compiled at 18:10:29 , Oct 14 2004.
   Testing memory...OK!
  128M  bytes  SDRAM
  32768k  bytes  flash memory
  Hardware Version is MTR 1.0
  CPLD Version is CPLD 1.0
  Press Ctrl - B to enter Boot Menu
```

(2) 用 CLI FTP 对 VRP 进行升级。

VRP 采用 FTP 方式进行升级存在两种方式:路由器作为 FTP Server 和路由器作为 FTP Client,路由器作为 FTP Server 升级 VRP 的方法与升级 BOOTROM 的方法类似,只需将步骤④修改为下列命令即可:

```
[H3C]boot main 340 - 0006.bin
Set main boot file successfully!
```

这里假设上传的目标文件名为 340-0006.bin。

(3) 清除进入 Console 配置口的密码。

可以通过从 BOOTROM 中选择"忽略配置"启动路由器来获取和重新设置 Console 的密码,具体操作如下:

① 重启路由器,按 Ctrl+B 键进入 BOOTROM 菜单。

```
Starting at 0x1c00000...
   ********************************************
   *                      *
   *   H3C Series Routers Boot ROM, V9.07   *
   *                      *
   ********************************************
  Copyright(C) 1997 - 2004 by H3C TECH CO., LTD.
 Compiled at 18:10:29 , Oct 14 2004.
  Testing memory...OK!
  128M bytes SDRAM
  32768k bytes flash memory
  Hardware Version is MTR 1.0
  CPLD Version is CPLD 1.0
 Press Ctrl - B to enter Boot Menu
 Please input Bootrom password:   /* 默认密码为空,直接回车 */
```

```
Boot Menu:
  1: Download application program with XMODEM
  2: Download application program with NET
  3: Set application file type
  4: Display applications in Flash
  5: Clear application password
  6: Start up and ignore configuration
  7: Enter debugging environment
  8: Boot Rom Operation Menu
  9: Do not check the version of the software
  a: Exit and reboot
Enter your choice(1 - a):
```

② 选择第六项“6：Start up and ignore configuration”，并按 Enter 键确认。

```
Enter your choice(1 - a): 6
Start up and ignore configuration, Are you sure?[Y/N]y
Set Succeeds
```

③ 选择 a 项重启系统，并按 Enter 键确认。

```
Enter your choice(1 - a): a
Exit and reboot,are you sure?[Y/N]y
Start to reboot...
```

④ 当系统以空配置起来以后，使用 more config.cfg 查看配置脚本。

```
<H3C>dir
Directory of flash:/
  0   - rw -   5748224 Nov 19 2004 17:23:05   main.bin
  1   - rw -   5746199 Nov 30 2004 14:51:21   v330 - 0008.bin
  2   - rw -   8650414 Nov 22 2004 12:26:57   system
  3   - rw -      1053 Dec 15 2004 18:46:41   config.cfg
  4   - rw -   8695261 Dec 15 2004 09:59:45   340 - 0006.bin
31877 KB total (3706 KB free)
<H3C>more config.cfg
/* 这里省略了部分显示内容 */
local - user admin
 password cipher .]@USE = B,53Q = ^SymbolYCpQMAF4 < 1!!
 service - type telnet terminal
 level 3
/* 这里省略了部分显示内容 */
```

如果是采用 simple 方式配置口令，则可以直接显示出密码。

如果是采用 cipher 方式配置口令，按照以下方法处理：

a. 将查看到的配置文件复制保存成一个文本文件。

b. 修改该文件中对应账号的密码“password cipher ;)< 01%^ &.;YGQ=^QMAF4 < 1!!”为类似 password simple aaa 的口令，其中 aaa 为设置的密码。

c. 将修改过的脚本，复制粘贴到当前路由器中。

d. <H3C>display current-configuration 确认当前配置和以前的配置一致后，save 配

置后重新启动系统。

e. 重启后,就可以通过修改过的账号口令登录系统。

【思考题】

(1) 对于软件版本的降级该怎么样操作?

(2) 本实验中路由器是作为 FTP Server 对 VRP 升级的,路由器作为 FTP Client 的对 VRP 升级,该怎么样操作?

实验 3-3　系统管理

【实验背景】

路由器的登录认证有多种方法:

(1) 使用本地用户进行 Console 登录的认证,要求用户从 Console 登录时输入已配置的用户名和对应的口令,用户名和口令正确才能登录成功。

(2) 使用本地用户进行 Telnet 登录的认证,要求用户 Telnet 登录时输入已配置的用户名和对应的口令,用户名和口令正确才能登录成功。

(3) 使用 SSH(Secure Shell)方式登录路由器。用户通过一个不能保证安全的网络环境远程登录到路由器时,SSH 特性可以提供安全保障和强大的认证功能,以保护路由器不受诸如 IP 地址欺诈、明文密码截取等的攻击。

(4) 使用 RADIUS 进行 Telnet 登录的认证要求用户 Telnet 登录时输入用户名和对应的口令,用户名和口令在 RADIVS Server 上验证通过后才能登录路由器。

(5) 使用 TACACS+进行 Telnet 登录的认证要求用户 Telnet 登录时输入用户名和对应的口令,用户名和口令在 TACACS+上验证通过后才能登录路由器。

为了网络正常运行,防止非法访问路由器,需要对路由器做有效的管理。通常,路由器并不在网络管理员身边,到路由器旁边管理路由器很不方便,这时还要建立远程登录用户。还有的时候需要查看路由器的运行日志,通过设定日志主机,路由器将日志发送到日志主机上,便于管理员的管理。

【实验目的】

(1) 掌握 SSH 方式登录认证的配置方法。

(2) 掌握 RADIUS 方式登录认证的配置方法。

(3) 掌握 TACACS+方式登录认证的配置方法。

(4) 掌握日志主机及 SNMP 网管的配置方法。

【实验内容】

(1) 使用 SSH 方式登录路由器。

(2) 使用 RADIUS 方式登录路由器。

(3) 使用 TACACS+方式登录路由器。

(4) 日志主机及 SNMP 网管的配置。

【实验设备】

H3C 系列交换机和路由器各一台，PC 两台或三台，其中一台安装网管软件 AdventNetSNMPv3.3Cdaemon、PUTTY、SSHKey、TekRadius、Cisco Secure ACS 等软件，直连双绞线三条，专用配置电缆一根。路由器系统管理拓扑结构如图 3.7 所示。

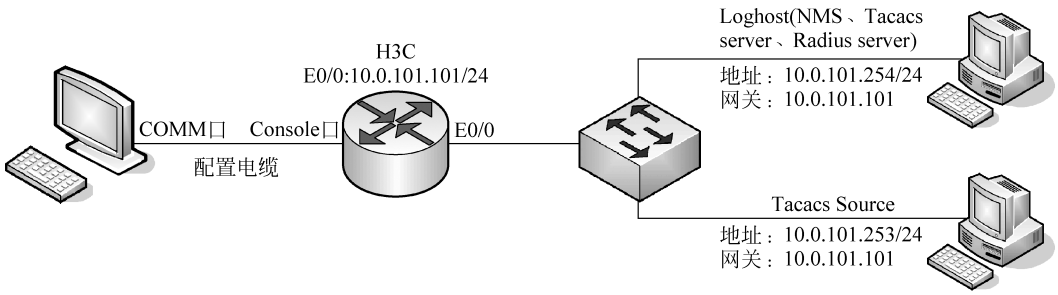

图 3.7　路由器系统管理拓扑结构图

【实验步骤】

(1) 将网络搭建好并配置路由器接口地址：

```
[H3C-Ethernet0/0]ip address 10.0.101.101 24
```

(2) RADIVS 进行 Telnet 登录认证实验。

① 对路由器做如下配置：

```
[H3C] radius scheme experiment                                    //创建 RADIUS 方案
[H3C-radius-experiment] primary authentication 10.0.101.254 1812
                                                                  //配置主验证服务器地址和端口号
[H3C-radius-experiment] key authentication jsjxy                  //配置共享密钥
[H3C-radius-experiment] user-name-format without-domain           //账号格式为不带域名方式
[H3C-radius-experiment] domain system
[H3C-isp-system] scheme radius-scheme experiment                  //引用 RADIUS 方案
[H3C-isp-system] accounting optional                              //打开计费可选开关
[H3C-isp-system] quit
[H3C] user-interface vty 0 4                                      //进入 vty 视图
[H3C-ui-vty0-4] authentication-mode scheme                        //设置 scheme 认证
[H3C-ui-vty0-4] quit
```

② 在 RADIVS Server 上创建用户名和密码分别为 CQUT、jsjxy 的账号后，设置 RADIUS server 和路由器上的 key 一致，就可以使用该账号 Telnet 到路由器。

(3) TACACS+进行 Telnet 登录认证实验。

① 对路由器做如下配置：

```
[H3C] hwtacacs nas-ip 10.0.101.253                                //设置 tacacs+的源地址
[H3C] hwtacacs scheme experiment                                  //创建 hwtacacs 方案
[H3C-hwtacacs-experiment] primary authentication 10.0.101.254     //配置主验证服务器地址
```

```
[H3C-hwtacacs-experiment] primary authorization 10.0.101.254  //配置主授权服务器地址
[H3C-hwtacacs-experiment] key authentication jsjxy      //配置认证密钥
[H3C-hwtacacs-experiment] key authorization jsjxy       //配置授权密钥
[H3C-hwtacacs-experiment] user-name-format without-domain  //账号格式为不带域名方式
[H3C-hwtacacs-experiment] domain system
[H3C-isp-system] scheme hwtacacs-scheme experiment      //引用 hwtacacs 方案"experiment"
[H3C-isp-system] accounting optional                    //打开计费可选开关
[H3C-isp-system] quit
[H3C] user-interface vty 0 4                            //进入 vty 视图
[H3C-ui-vty0-4] authentication-mode scheme              //设置 scheme 认证
[H3C-ui-vty0-4] quit
```

② 在 RADIVS Server 上创建用户名和密码分别为 CQUT、jsjxy 的账号后,设置 hwtacacs server 和路由器上的 key 一致,就可以使用该账号登录到路由器。

(4) SSH 用户通过 password 的验证方式登录路由器。

① 对路由器做如下配置:

```
[H3C] rsa local-key-pair create  //生成本地 RSA 主机密钥对和服务器密钥对,按照提示输入主机密钥的位数,此命令只需执行一遍,即使路由器重新启动后也不必再次执行。
[H3C] user-interface vty 0 4                            //进入 vty 视图
[H3C-ui-vty0-4] authentication-mode scheme              //设置 scheme 认证
[H3C-ui-vty0-4] protocol inbound ssh
[H3C-ui-vty0-4] quit
[H3C] local-user CQUT                                   //创建本地账号 CQUT
[H3C-luser-CQUT] password simple jsjxy                  //设置密码为 jsjxy
[H3C-luser-CQUT] service-type ssh                       //设置服务类型为 ssh
[H3C-luser-CQUT] level 3                                //设置用户优先级为 3
[H3C-luser-CQUT] quit
[H3C] ssh user CQUT authentication-type password        //配置 SSH 用户验证方式为 password
[H3C] domain system                                     //进入 domain system 视图
[H3C-isp-system] scheme local                           //使用本地认证方案
```

② 使用 SSH client 软件 PuTTY,输入用户名 CQUT 和对应的密码 jsjxy 就可以成功登录系统。

(5) SSH 用户通过 RSA 的验证方式登录路由器。

① 使用 puttygen.exe 软件生成公钥和私钥对,并分别保存。

② 使用 SSHkey.exe 软件对生成的公钥进行格式转换。

③ 对路由器的配置只需将步骤(4)配置过程中的加粗部分修改为以下命令即可:

```
[H3C] ssh user CQUT authentication-type rsa             //配置 SSH 用户验证方式为 RSA
[H3C] rsa peer-public-key jsjxy                         //进入公共密钥视图
[H3C-rsa-public-key] public-key-code begin              //进入公共密钥编辑视图
[H3C-rsa-key-code]          //将预先生成并转换格式后的 RSA 公钥粘贴进来
[H3C-rsa-key-code] public-key-code end                  //退出公共密钥编辑视图
[H3C-rsa-public-key] peer-public-key end                //退出公共密钥视图
[H3C] ssh user CQUT assign rsa-key jsjxy                //为用户指定使用的 RSA 密钥
```

④ 使用 putty 软件,对通过 puttygen 生成的私钥进行验证。

⑤ 指定地址,建立 SSH 连接。

⑥ 输入账号，不需要输入密码即可登录，过程如图 3.8 所示。

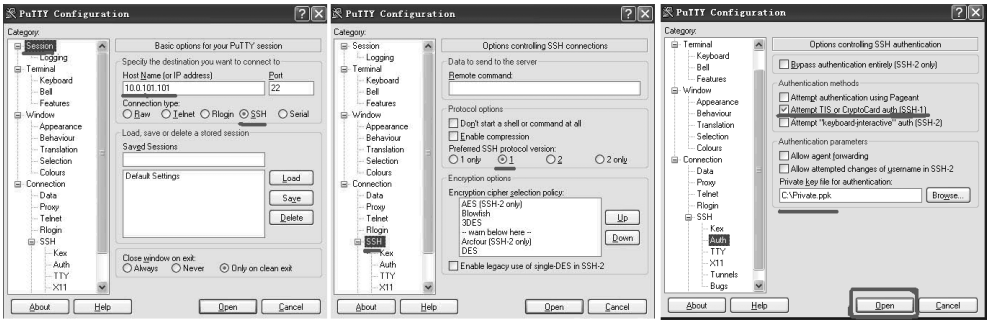

图 3.8　SSH 登录路由器过程示意图

注意：

① 如果用户需要 RSA 认证，就必须指定 RSA 私钥文件，输入账号，不需要输入密码即可登录；如果用户只需要 password 认证，则不需要指定 RSA 私钥文件，输入账号和对应的密码即可登录。

② 相关的软件可以从网站：

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html 下载。

③ 步骤(5)的实验需要手工对公钥进行格式转换，有的设备也支持将公钥文件通过 FTP 上传到路由器(具体方法见路由器基本维护实验)，然后将其中步骤②和③通过下面的命令实现公共密钥格式转换及公共密钥的配置：

```
[H3C] rsa peer-public-key jsjxy import sshkey jsjxy.pk //假设上传的公钥文件名为 jsjxy.pk
```

(6) 日志主机的配置。

```
<H3C>system-view
[H3C]interface loopback 0
[H3C-LoopBack0]ip address 1.1.1.1 32
[H3C-LoopBack0]quit
[H3C]info-center enable                                    //开启信息中心
[H3C]info-center loghost source LoopBack0
                                    //指定 loopback0 作为发送日志信息的源地址
[H3C]info-center loghost 10.0.101.254                      //配置日志主机
```

Windows 平台上的 3Cdaemon 软件可以用来实现日志主机功能，该软件可以从论坛 http://forum.h3c.com/viewthread.php?tid=1057&highlight=3CDaemon 下载，使用非常简单。

(7) SNMP 网管的配置。

① 对路由器做如下配置：

```
<H3C>system-view
[H3C]snmp-agent                                            //使能 SNMP 服务
[H3C]snmp-agent community read CQUT                        //设置读团体名:CQUT
[H3C]snmp-agent community write jsjxy                      //设置写团体名:jsjxy
[H3C]snmp-agent sys-info contact Mr.cui-Tel:62563076       //设置联系方式
```

```
[H3C]snmp-agent sys-info location 3rd-floor                    //设置设备位置
[H3C]snmp-agent sys-info version v1 v3                         //配置 SNMP 版本(默认只允许 v3)
[H3C]snmp-agent trap enable
[H3C]snmp-agent target-host trap address udp-domain 10.0.101.254 udp-port 5000 params
securityname CQUT
    //允许向网管工作站(NMS)10.0.101.254 发送 Trap 报文,使用的团体名为 CQUT
```

② 安装好 MIB Browser 程序后,配置 Host 为 10.0.101.101,Community 为 CQUT

注意:

① 设备默认的 SNMP 版本为 V3,必须修改为和 NMS 上使用版本一致,或设置为 all。

② 网管的 community name 应该与路由器上配置一致。

③ 默认配置下 community read name 为 public, community write name 为 private。

【思考题】

(1) 不同登录认证方式的异同是什么?

(2) TACACS+和 RADIUS 的区别是什么?

实验 3-4　链路层协议

【实验背景】

数据链路层基于物理层的服务,为网络层提供透明的、正确有效的传输链路,有成帧与传输、流量控制、差错控制、链路管理 4 大功能。点对点协议(Point to Point Protocol,PPP)为在点对点连接上传输多协议数据包提供了一个标准方法,PPP 协议是目前广域网上应用最广泛的协议之一,它的优点在于简单、具备用户认证能力、可以解决 IP 分配等问题。它定义了一整套的协议,包括链路层控制协议、网络层控制协议、认证协议。其中认证协议有密码认证协议(Password Authentication Protocol,PAP)和挑战握手认证协议 (Challenge Handshake Authentication Protocol,CHAP)两种,前者采用明文认证,而后者采用密文认证。帧中继(Frame-relay)协议是在 x.25 分组交换技术的基础上发展起来的用简化方法转发和交换数据单元的一种快速分组交换技术,是对 x.25 协议的简化,采用虚电路技术,能充分地利用网络资源,因此处理效率很高,网络吞吐量高,通信时延低,它正在代替传统复杂低速的报文交换服务。家庭拨号上网就是通过 PPP 在用户端和运营商的接入服务器之间建立通信链路。现在,宽带接入呈现出取代拨号上网的趋势,在宽带接入技术日新月异的今天,PPP 也衍生出新的应用。典型的应用是在非对称数据用户环线(Asymmetrical Digital Subscriber Loop,ADSL)接入方式当中,PPP 与其他的协议共同派生出了符合宽带接入要求的新的协议,如 PPPoE(PPP over Ethernet)、PPPoA(PPP over ATM)。利用以太网(Ethernet)资源,在以太网上运行 PPP 来进行用户认证接入的方式称为 PPPoE,是现在 ADSL 接入方式中应用最广泛的技术标准。同样,在异步传输模式(Asynchronous Transfer Mode,ATM)网络上运行 PPP 协议来管理用户认证的方式称为 PPPoA。帧中继用户的接入速率在 64kb/s～2Mb/s,甚至可达到 34Mb/s。它使用的是逻辑连接,而不是物理连接,在一个物理连接上可复用多个逻辑连接(即可建立多条逻辑信道),可实现带宽的复

用和动态分配。帧中继的帧信息长度远比 x.25 分组长度要长，最大帧长度可达 1600 字节/帧，适合于封装局域网的数据单元和传送突发业务（如压缩视频业务、WWW 业务等）。

【实验目的】

（1）掌握 PPP 协议的原理及配置方法。
（2）掌握 PPP 协议进行 PAP 认证的原理及配置方法。
（3）掌握 PPP 协议进行 CHAP 认证的原理及配置方法。
（4）掌握 Frame-relay 协议的原理及配置方法。

【实验内容】

（1）PPP 协议的配置。
（2）PPP 协议进行 PAP 认证的配置。
（3）PPP 协议进行 CHAP 认证的配置。
（4）Frame-relay 协议的配置。

【实验设备】

H3C 系列交换机一台，H3C 系列路由器两台，PC 两台，专用配置电缆一根，网线四条，标准 V35 电缆一对。链路层协议实验网络拓扑图如图 3.9 所示。

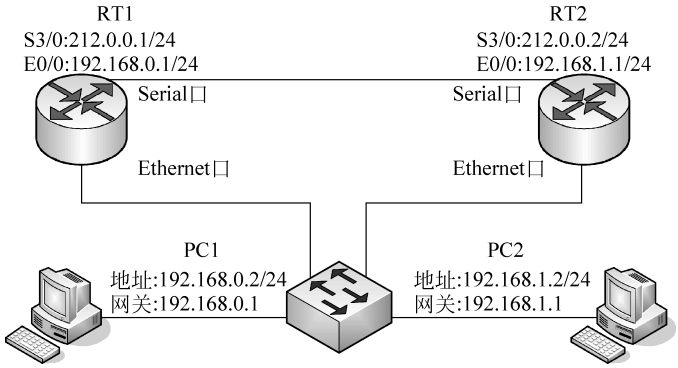

图 3.9　链路层协议实验网络拓扑图

【实验步骤】

（1）按照图 3.9 所示，将网络拓扑结构搭建好。
（2）在路由器 RT1 的接口上配置地址：

```
<H3C>system-view
[H3C]sysname RT1                                          //修改路由器的名字
[RT1]interface Ethernet0/0
[RT1-Ethernet0/0]ip address 192.168.0.1 255.255.255.0    //配置 Ethernet 口的地址
[RT1-Ethernet0/0]interface Serial3/0
[RT1-Serial3/0]ip address 212.0.0.1 255.255.255.0        //配置 Serial 口的地址
[RT1-Serial3/0]rip
```

```
[RT1 - rip]network 192.168.0.0
[RT1 - rip]network 212.0.0.0
```

(3) 对另一个路由器做类似的配置。

(4) 进行 PAP 认证的实验。

① 在主认证方的接口上封装 PPP 协议,并设置认证方式:

```
[RT1 - rip] interface Serial3/0
[RT1 - Serial3/0]link - protocol PPP                    // H3C 的路由器已默认封装了该协议
[RT1 - Serial3/0]ppp authentication - mode pap
[RT1 - Serial3/0]shutdown
[RT1 - Serial3/0]undo shutdown
[RT1 - Serial3/0]quit
```

② 在主认证方将对端用户名和密码加入本地用户列表:

```
[RT1]local - user CQUT
[RT1 - luser - CQUT]password simple jsjxy
[RT1 - luser - CQUT]service - type ppp
```

③ 被认证方配置以 PAP 方式认证时本地发送的 PAP 用户名和密码:

```
[RT2]interface Serial3/0
[RT2 - Serial3/0]ppp pap local - user CQUT password simple jsjxy
[RT2 - Serial3/0]shutdown
[RT2 - Serial3/0]undo shutdown
```

(5) 进行 CHAP 认证的实验。

① 在主认证方配置本地认证对端的方式为 CHAP:

```
[RT1 - luser - CQUT]interface Serial3/0
[RT1 - Serial3/0]ppp authentication - mode chap
```

② 配置主认证方的用户名:

```
[RT1 - Serial3/0]ppp chap user CQUT1
[RT1 - Serial3/0]ppp chap password simple jsjxy
[RT1 - Serial3/0]shutdown
[RT1 - Serial3/0]undo shutdown
[RT1 - Serial3/0]quit
```

③ 在主认证方将对端用户名和密码加入本地用户列表:

```
[RT1]local - user CQUT2
[RT1 - luser - CQUT2]password simple jsjxy
[RT1 - luser - CQUT2]service - type ppp
```

④ 配置被认证方的用户名:

```
[RT2 - Serial3/0]ppp chap user CQUT2
[RT2 - Serial3/0]ppp chap password simple jsjxy
[RT2 - Serial3/0]shutdown
[RT2 - Serial3/0]undo shutdown
```

⑤ 在被认证方配置本地用户名和密码：

```
[RT2 - Serial3/0]quit
[RT2]local - user CQUT1
[RT2 - luser - CQUT1]password simple jsjxy
[RT2 - luser - CQUT1]service - type ppp
```

(6) Frame-relay 协议配置实验。

① 对 RT1 在第 2 步的基础上做如下配置：

```
[RT1 - Serial3/0]link - protocol fr                    //封装帧中继接口,其余使用默认配置
```

② 对 RT2 在第 3 步的基础上做如下配置：

```
[RT2]fr switching                                      //使能帧中继交换
[RT2]interface Serial3/0
[RT2 - Serial3/0]link - protocol fr                    //封装帧中继接口
[RT2 - Serial3/0]fr interface - type dce               //帧中继接口类型,默认是 DTE
[RT2 - Serial3/0]fr lmi type q933a                     //帧中继 LMI 类型,默认是 q933a
[RT2 - Serial3/0]fr dlci 20          //为接口分配 DLCI,默认情况下没有本地可用的虚电路
[RT2 - Serial3/0]fr inarp            //启用逆向地址解析协议(inverse - arp,默认已经启动)
[RT2 - Serial3/0]rip
[RT2 - rip]peer 212.0.0.1
```

【思考题】

以上 PAP 认证实验和 CHAP 认证实验都是主认证方 RT1 认证被认证方 RT2，请考虑 RT1 和 RT2 都同时作为主认证方和被认证方应怎样配置？

实验 3-5　网络协议

【实验背景】

动态主机配置协议(Dynamic Host Configuration Protocol，DHCP)是一种使网络管理员能够集中管理和自动分配 IP 网络地址的通信协议。在 IP 网络中，每个连接 Internet 的设备都需要分配唯一的 IP 地址。DHCP 使网络管理员能从中心节点监控和分配 IP 地址。当某台计算机移到网络中的其他位置时，能自动收到新的 IP 地址。DHCP 使用了租约的概念，或称为计算机 IP 地址的有效期。租用时间是不定的，主要取决于用户在某地连接 Internet 需要多久，这对于教育行业和其他用户频繁改变的环境是很实用的。通过较短的租期，DHCP 能够在一个计算机比可用 IP 地址多的环境中动态地重新配置网络，DHCP 支持为计算机分配静态地址。

网络地址转换(Network Address Translation，NAT)是通过将专用网络地址(如企业内部网 Intranet)转换为公用地址(如互联网 Internet)，从而对外隐藏了内部管理的 IP 地址。这样，通过在内部使用非注册的 IP 地址，并将它们转换为一小部分外部注册的 IP 地址，从而减少了 IP 地址注册的费用以及节省了目前越来越缺乏的地址空间(即 IPv4)。同时，也隐藏了内部网络结构，从而降低了内部网络受到攻击的风险。NAT 分为三种类型：

静态 NAT(Static NAT)、NAT 池(Pooled NAT)和端口 NAT(PAT)。其中静态 NAT 将内部网络中的每个主机都永久映射成外部网络中某个合法的地址,而 NAT 池则是在外部网络中定义了一系列的合法地址,采用动态分配的方法映射到内部网络,端口 NAT 则是把内部地址映射到外部网络的一个 IP 地址的不同端口上。

通过 DHCP 服务器的协助控管各个客户机(执行中的用户端)上不可缺少的网络配置参数,包括域名服务(Domain Name Service,DNS)、Windows 互联网名字服务(Windows Internet Name Service,WINS)等。内网用户通过路由器的 NAT 功能访问 Internet。为了限制局域网内主机对外发起的连接数,路由器上配置 NAT 限制最大连接数特性,可以对源地址发起的连接数进行限制。

【实验目的】

(1) 掌握路由器作为 DHCP 服务器的配置方法。

(2) 掌握路由器用出口地址做 Easy NAT、地址池做 NAT、一个以太网口做 NAT 的配置方法。

(3) 掌握对外提供 WEB 服务的配置方法。

(4) 掌握 NAT 限制每个源地址最大 TCP 连接数的配置方法。

【实验内容】

(1) DHCP 服务器的配置。

(2) NAT 的配置。

(3) 对外提供 Web 服务的配置。

(4) NAT 限制每个源地址最大 TCP 连接数的配置。

【实验设备】

H3C 系列交换机和路由器各一台,PC 一台,专用配置电缆一根,网线两条。网络协议实验拓扑如图 3.10 所示。

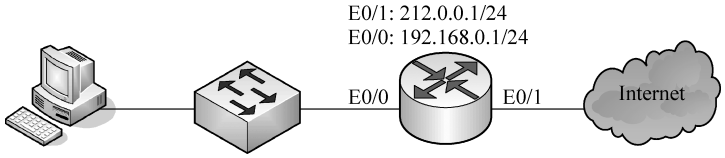

图 3.10　网络协议实验网络拓扑图

【实验步骤】

(1) 按照图 3.10 所示将网络拓扑结构搭建好。

(2) 配置路由器为 DHCP Server。

① 使能 DHCP。

```
[H3C]dhcp enable
```

② 创建 DHCP 地址池，指定可以分配的地址段、网关、DNS Server 地址、域名。

```
[H3C] dhcp server ip - pool 1
[H3C - dhcp - pool - 1]network 192.168.0.0 mask 255.255.255.0
[H3C - dhcp - pool - 1]gateway - list 192.168.0.1
[H3C - dhcp - pool - 1]dns - list 202.202.145.5
[H3C - dhcp - pool - 1]domain - name CQUT
```

③ 配置网关地址。

```
[H3C - dhcp - pool - 1]interface ethernet0/0
[H3C - Ethernet0/0] ip address 192.168.0.1 255.255.255.0
```

④ 保留网关的地址，以防止分配给其他客户机。

```
[H3C] dhcp server forbidden - ip 192.168.0.1
```

⑤ 在 PC 上执行 ipconfig/all 命令，查看该 PC 通过 DHCP 获取的 IP 地址、网关等信息。

```
C:\> ipconfig/all
```

(3) 出接口地址做 Easy NAT：

① 启用防火墙：

```
[H3C]firewall enable
```

② 配置允许进行 NAT 转换的内网地址段：

```
[H3C]acl number 2000
[H3C - acl - basic - 2000] rule 0 permit source 192.168.0.0 0.0.0.255
[H3C - acl - basic - 2000]rule 1 deny
[H3C - acl - basic - 2000]interface ethernet0/0
[H3C - Ethernet0/0]firewall packet - filter 2000 inbound      //将规则应用于接口上
```

③ 配置内部网关：

```
[H3C - Ethernet0/0] ip address 192.168.0.1 255.255.255.0
```

④ 配置出口地址，并做地址转换：

```
[H3C - Ethernet0/0]interface Ethernet0/1
[H3C - Ethernet0/1]ip address 212.0.0.1 255.255.255.0
[H3C - Ethernet0/1]nat outbound 2000
```

⑤ 配置动态路由：

```
[H3C - Ethernet0/1]rip
[H3C - rip]network 212.0.0.0
[H3C - rip]network 192.168.0.0
```

(4) 地址池方式做 nat：

① 配置用户 NAT 的地址池：

```
[H3C]nat address - group 0 212.0.0.3 212.0.0.10
```

② 配置允许进行 NAT 转换的内网地址段,方法同上。

③ 配置出口地址,并做地址转换:

```
[H3C] interface Ethernet0/1
[H3C-Ethernet0/1]ip address 212.0.0.1 255.255.255.0
[H3C-Ethernet0/1]nat outbound 2000 address-group 0
```

④ 配置内部网关、动态路由,方法同上。

(5) 一个以太网口做 NAT 是指局域网和广域网都接在路由器的以太网口上。

① 配置用户 NAT 的地址池,方法同上。

② 配置允许进行 NAT 转换的内网地址段:

```
[H3C-Ethernet0/1]acl number 3000
[H3C-acl-adv-3000]rule 0 deny ip source 192.168.0.0 0.0.0.255 destination 192.168.0.1 0
[H3C-acl-adv-3000]rule 1 permit ip source 192.168.0.0 0.0.0.255
[H3C-acl-adv-3000]rule 2 deny ip
[H3C-acl-adv-3000]interface ethernet0/0
[H3C-Ethernet0/0]firewall packet-filter 3000 inbound
```

③ 配置内部网关,出口地址,并做地址转换:

```
[H3C-Ethernet0/0] ip address 212.0.0.1 255.255.255.0
[H3C-Ethernet0/0] ip address 192.168.0.1 255.255.255.0 sub
[H3C-Ethernet0/0] nat outbound 3000
```

④ 配置动态路由方法同上。

(6) 对外提供 WWW 服务:

如果内部服务器 192.168.0.2 对外提供 WWW 服务,还需要做如下配置。

```
[H3C-Ethernet0/0]nat server protocol tcp global 212.0.0.2 www inside 192.168.0.2 www
```

(7) NAT 限制每个源地址最大 TCP 连接数需要做上述配置外,还要做如下配置。

① 创建连接数限制策略,并配置子规则,对源地址发起的连接数进行限制:

```
[H3C]connection-limit enable
[H3C]connection-limit policy 0
[H3C-connection-limit-policy-0] limit 0 acl 2000 per-source amount 50 20
                                                    //连接的上下限分别为 50 和 20
```

② NAT 引用连接数限制策略 0:

```
[H3C]nat connection-limit-policy 0      //此功能在 VRP3.4-E0201 及以后的版本中实现.
```

【思考题】

(1) 上述的连接限制对每个源地址都限制,如果只对某一个源地址进行限制,应怎么做?

(2) 以上实验内网只有一个出口,若有多个出口做 NAT 实现负载分担,又应怎么做?

(3) 如果对外提供 FTP 服务,路由器应怎样配置?

(4) 如果需要其他用户可以 ping 通内部对外提供服务的服务器,路由器应怎样配置?

实验 3-6　路由协议

【实验背景】

静态路由是指由网络管理员手工配置的路由信息。当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手工修改路由表中相关的静态路由信息。静态路由信息在默认情况下是私有的，不会传递给其他的路由器。当然，网管员也可以通过对路由器进行设置使之成为共享的。静态路由一般适用于比较简单的网络环境，在这样的环境中，网络管理员易于清楚地了解网络的拓扑结构，便于设置正确的路由信息。

动态路由是指路由器能够自动地建立自己的路由表，并且能够根据实际情况的变化适时地进行调整。动态路由机制的运作依赖路由器的两个基本功能：对路由表的维护和路由器之间适时的路由信息交换。

路由选择信息协议(Routing Information Protocol，RIP)是一种在网关与主机之间交换路由选择信息的标准。RIP 是一种内部网关协议，在国家性网络中如当前的因特网，拥有很多用于整个网络的路由选择协议。作为形成网络的每一个自治系统，都有属于自己的路由选择技术，不同的 AS 系统，路由选择技术也不同。RIP 2 由 RIP 而来，属于 RIP 协议的补充协议，主要用于扩大信息装载的有用信息的数量，同时增加其安全性能。RIP 2 是一种基于 UDP 的协议。在 RIP 2 下，每台主机通过路由选择进程发送和接收来自 UDP 端口 520 的数据包。RIP 和 RIP 2 主要适用于 IPv4 网络，而 RIPng 主要适用于 IPv6 网络。

开放最短路径优先(Open Shortest Path First，OSPF)也是一个内部网关协议，用于属于单个自治体系(AS)的路由器之间的路由选择。OSPF 采用链路状态技术，路由器互相发送直接相连的链路信息和它所拥有的到其他路由器的链路信息。每个 OSPF 路由器都维护相同自治系统拓扑结构的数据库。从这个数据库里，构造出最短路径树来计算路由表。当拓扑结构发生变化时，OSPF 能迅速重新计算路径，而只产生少量的路由协议流量。OSPF 支持开销的多路径。区域路由选择功能使添加路由选择保护和降低路由选择协议流量均成为可能。此外，所有的 OSPF 路由选择协议的交换都是经过验证的。

当连接不同网络的路由器之间通过静态路由、动态路由 RIP、动态路由 OSPF 实现互连互通时，需要做这些配置。

【实验目的】

(1) 掌握静态路由和默认路由的工作原理和配置方法。

(2) 掌握动态路由 RIP 的工作原理和配置方法。

(3) 掌握动态路由 OSPF 的工作原理和配置方法。

【实验内容】

(1) 静态路由的配置。

(2) 动态路由 RIP 的配置。

(3) 动态路由 OSPF 的配置。

【实验设备】

H3C 系列交换机一台,H3C 系列路由器两台,PC 两台,专用配置电缆一根,网线四条,标准 V35 电缆一对。路由协议实验网络拓扑图如图 3.11 所示。

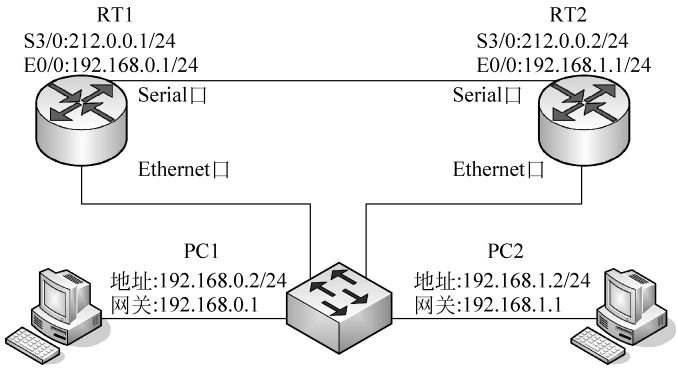

图 3.11　路由协议实验网络拓扑图

【实验步骤】

(1) 按照图 3.11 所示,将网络拓扑结构搭建好。

(2) 在路由器 RT1 的接口上配置地址;

```
<H3C>system-view
[H3C]sysname RT1                                          //修改路由器的名字
[RT1]interface Ethernet0/0
[RT1-Ethernet0/0]ip address 192.168.0.1 255.255.255.0  //配置 Ethernet 口的地址
[RT1-Ethernet0/0]interface Serial3/0
[RT1-Serial3/0]ip address 212.0.0.1 255.255.255.0      //配置 Serial 口的地址
[RT1-Serial3/0]shutdown
[RT1-Serial3/0]undo shutdown
```

(3) 对另一个路由器做类似的配置。

(4) 静态路由的配置:

```
[H3C] ip route-static ip-address { mask | masklen } { interface-type interface-name |
nexthop-address } [ preference value ] [ reject | blackhole ]
[RT1]ip route-static 192.168.1.0 255.255.255.0 212.0.0.2 preference 60
```

对另一个路由器做类似的配置。

注意:

① 在配置静态路由时,一定要保证路由的双向可达。

② 如果必须配置静态路由,请尽量使用具体网段的静态路由,避免使用 ip route-static 0.0.0.0 0.0.0.0 {*interface-type interface-name* | *nexthop-address*} [preference *value*] 默认路由,以防止路由环的产生。

③ 如果接口封装 PPP 或 HDLC 协议,这时可以不用指定下一跳地址,只需指定发送接口即可;对于封装了非点到点协议(如 fr、x25 等)必须配置下一跳的 IP 地址。

(5) 动态路由 RIP 协议的配置：

① 启动 RIP 协议：

```
[RT1] rip
```

② 在指定的网络上使能 RIP：

```
[H3C - rip] network { network - number }
[RT1 - rip]network 192.168.0.0
[RT1 - rip]network 212.0.0.0
```

③ 对另一个路由器做类似的配置。

注意：

① RIP 有 RIP 1 和 RIP 2 两个版本，可以在接口视图下指定接口所处理的 RIP 报文版本，默认情况下启动的是 RIP Version 1。

```
[RT1 - Serial3/0] rip version 2[broadcast | multicast]
```

② RIP 1 的报文传送方式为广播方式，而 RIP 2 有广播方式和组播方式两种报文传送方式，默认将采用组播方式发送报文，其组播地址为 224.0.0.9。

③ RIP 1 对路由聚合不起作用，RIP 2 支持无类地址域间路由和路由选择，默认情况下 RIP 2 支持路由聚合，当需要将所有子网路由广播出去时，可关闭 RIP 2 路由聚合功能。

(6) 动态路由 OSPF 协议的配置：

① 配置路由器的 Router ID：

```
[H3C]router id 1.1.1.1
```

② 启动 OSPF 协议：

```
[H3C] ospf 1
```

③ 配置 OSPF 区域：

```
[H3C - ospf - 1]area 0
```

④ 在指定网段使能 OSPF。

```
[H3C - ospf - 1 - area - 0.0.0.0] network ip - address wildcard - mask
[H3C - ospf - 1 - area - 0.0.0.0] network 192.168.0.0 0.0.0.255
[H3C - ospf - 1 - area - 0.0.0.0] network 212.0.0.0 0.0.0.255
```

⑤ 对另一个路由器做类似的配置。

注意：

Router ID 是一个 32b 的无符号整数，是一台路由器的唯一标识，在整个自治系统内唯一。

【思考题】

(1) 上述的实验是两个路由器背对背地连接模拟广域网的配置内容，如果在两个路由器之间再加一个路由器该如何配置？

(2) 如果一个网络要配置多种路由协议，该怎么配置路由器？

(3) 在动态路由 RIP 协议的配置实验里,如果将 RT1. RT2 的 E0/0 接口地址分别配置为 10.0.101.1/24、10.0.102.1/24,再做相应的配置,则 RT1 的路由表有 10.0.102.0 这条路由吗? 如果再在两个路由器上分别配置[RT1-Serial3/0] rip version 2 broadcast 呢? 如果分别配置为[RT1-Serial3/0] rip version 2 multicast 呢? 如果再在两个路由器上分别配置[RT1-rip]undo summary,再分别做上述改变呢? 为什么?

实验 3-7　组播协议

【实验背景】

在 Internet 上,诸如流媒体、视频会议、视频点播等多媒体业务,正在成为信息传送的重要组成部分。点对点传输的单播方式不能适应单点发送多点接收业务传输特性,因为服务器必须为每一个接收者提供一个相同内容的 IP 报文备份,同时网络上也重复地传输相同内容的报文,占用了大量资源。单个数据流可以发送到多个客户端的组播能力已成为大多数多媒体应用的传输手段。组播技术利用一个 IP 地址使 IP 数据包文发送到用户组。IP 组播采用了特殊定义的目的 IP 地址和目的 MAC 地址。组播路由协议有协议无关组播-密集模式(Protocol Independent Multicast-Dense Mode, PIM-DM)、协议无关组播-稀疏模式(Protocol Independent Multicast-Sparse Mode, PIM-SM)、距离矢量组播路由协议(Distance Vector Multicast Routing Protocol, DVMRP)、开放式组播最短路径优先(Multicast Open Shortest Path First, MOSPF)、核树组播路由协议等。

PIM-DM 利用单播路由表,从源端 PIM 路由器(三层交换机)构建一棵到所有端节点的组播转发树(Distribution Tree, DT)。在发送组播报文时,PIM-DM 认为网络上所有主机都准备接收组播报文,组播源一开始将向网络所有下游节点转发组播报文,无组播组成员的节点将剪枝报文通知上游交换机不用再向下游节点转发数据。当新的成员在剪枝区域中出现时,PIM-DM 发送嫁接消息,使被剪枝的路径重新变成转发状态。该机制称为广播-剪枝过程,PIM-DM 广播-剪枝机制将周期性地不断进行。PIM-DM 在广播-剪枝过程中采用了逆向路径转发(Reverse Path Forwarding, RPF)技术:当一个组播报文到达时,交换机首先判断到达路径的正确性。若到达接口是由单播路由指示的通往组播源的接口,那么该组播报文被认为是从正确路径而来;否则,该组播报文将作为冗余报文而被丢弃,不进行组播转发。

PIM-SM 假设某个共享网段上的所有交换机都不需要发送组播报文,交换机只有在主动请求加入某个组播组后,才能收发组播报文。PIM-SM 通过设置汇聚点(Rendezvous Point, RP)和自举路由器(Bootstrap Router, BSR)向所有支持 PIM-SM 的交换机通告组播信息。在 PIM-SM 中,交换机显式地加入和退出组播组,可以减少数据包文和控制报文占用的网络带宽。PIM-SM 构造以 RP 为根的共享树(RP Path Tree, RPT),使组播报文能沿着共享树发送。当主机加入一个组播组时,直接连接的交换机便向 RP 发送 PIM 加入报文;发送者的第一跳交换机把发送者注册到 RP 上;接收者的指定路由器(Designated Router, DR)将接收者加入到共享树。使用以 RP 为根的 RPT 进行报文转发,可以减少交换机需要维护的协议状态、提高协议的可伸缩性,降低交换机处理开销。当数据流量达到一定程度时,数据可从 RPT 切换到基于源的最短路径树(Short Path Tree, SPT),以减少网络延迟。

随着 Internet 和 Intranet 应用日益丰富，视频点播也逐渐应用于宽带网和局域网。人们已不再满足于浏览文字和图片，越来越多的人更喜欢在网上看电影、听音乐。而视频点播和音频点播功能的实现，则必须依靠流媒体服务技术。PIM 是应用层协议，PIM-DM 主要被设计用于组播局域网应用程序，当发送者和接收者彼此非常接近并且网络中组播组接收成员的数量很大、组播报文的流量很大、组播报文的流量是持续的情况下使用，而 PIM-SM 是一种能有效地路由到跨越大范围网络（WAN 和域间）组播组的协议，在组成员分布相对分散，范围较广、网络带宽资源有限的情况下使用。

【实验目的】

（1）掌握在 Windows Server 2003 中搭建视频服务器的方法。

（2）掌握 PIM-DM 的原理及配置方法。

（3）掌握 PIM-SM 的原理及配置方法。

【实验内容】

（1）Windows Server 2003 中视频服务器的搭建。

（2）PIM-DM 的配置。

（3）PIM-SM 的配置。

【实验设备】

H3C 系列路由器三台，PC 三台（其中一台安装 Windows Server 2003），专用配置电缆一根，交叉双绞线三条，标准 V35 电缆三对。组播协议实验网络拓扑图如图 3.12 所示。

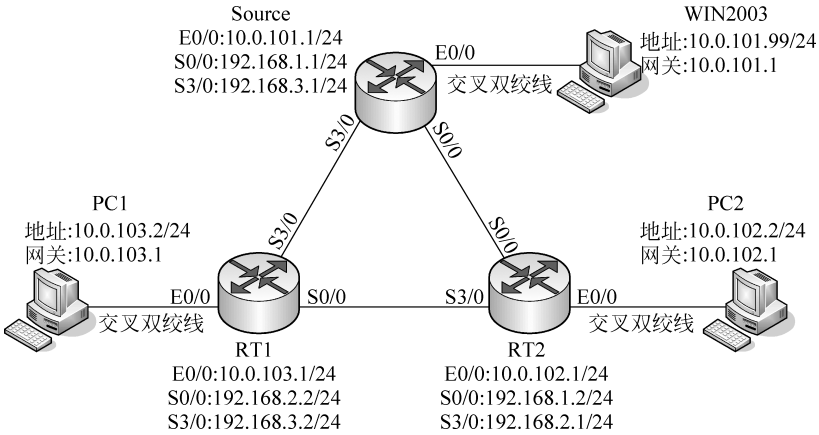

图 3.12　组播协议实验网络拓扑图

【实验步骤】

（1）在 Windows Server 2003 中搭建视频服务器：

① 安装 Windows Media 服务器。Windows Media 服务是 Windows Server 2003 系统的组件之一，但是在默认情况下并不会自动安装，需要用户手工添加，可以使用“Windows

组件向导”和“配置您的服务器向导”安装 Windows Media 服务,这里不再描述。

② 制作流式文件。Windows Media 服务使用的流文件是以 asf、wma 和 wmv 为扩展名的标准的 Windows Media 文件格式。其中 asf 文件通常用于使用 Windows Media Tools 4.0 创建的基于 Microsoft Media 的内容。而 wma 和 wmv 文件是作为 Windows Media 编码器的标准命名约定引入的。而对于 avi、wav、mpg 等文件可以使用 Windows Media 编码器转换成为 Windows Media 服务使用的流文件,Windows Media 编码器可以到微软公司官方网站上下载安装。Windows Media 编码器还可对实况信息源即将音频或视频设备录入的音频、视频或图片等源信息进行编码运算,以将它们转换为流或流文件的过程。另外,Windows Media 编码器还可以用来捕获屏幕、窗口,并且还可以把屏幕、屏幕中的特定区域或窗口在一段时间内的活动信息捕获并做成演示文件,以供其他用户观看或下载,这里不再介绍。

(3) PIM-DM 的配置。

① 按照图 3.12,将网络拓扑结构搭建好。

② 按图 3.12 要求配置各个路由器各接口的地址。

③ 按图 3.12 要求配置各个计算机的 IP 地址、子网掩码及网关。

④ 在路由器上配置相关的路由协议,静态路由或动态路由。

⑤ 在路由器上启动组播路由协议:

```
[Source] multicast routing-enable
```

其他路由器也要做类似的配置。

⑥ 在路由器的各个接口上配置 PIM-DM:

```
[Source-Ethernet0/0]pim dm
[Source-Serial0/0]pim dm
[Source-Serial3/0]pim dm
[Source-Serial3/0]shutdown
[Source-Serial3/0]undo shutdown
```

其他路由器也要做类似的配置。

(4) PIM-SM 的配置。

PIM-SM 的配置和 PIM-DM 的配置类似,只是在 PIM-SM 的配置中,至少一台路由器为 BSR 候选者和 RP 候选者。

```
[Source]pim
[Source-pim]
[Source-pim]c-bsr Serial 3/0 10 20          //10 是 RP Hash 函数的掩码长度(0～32)
                                            //20 是候选自举路由器的优先级(0～255)
[Source-pim]c-rp Serial 3/0 10              //10 是候选 RP 优先级
```

【思考题】

(1) 如何查看路由器的组播路由表?

(2) 如何配置某个路由器的接口为组播边界?

(3) 哪些地址是组播地址? 比较重要的组播地址有哪些?

实验 3-8　QoS

【实验背景】

QoS(Quality of Service,服务质量)是网络的一种安全机制，是一种技术用来解决网络延迟和阻塞等问题的技术。在正常情况下,如果网络只用于特定的无时间限制的应用系统，并不需要 QoS,如 Web 应用、E-mail 等。但是对关键应用和多媒体应用就十分必要。当网络过载或拥塞时,QoS 能确保重要业务量不受延迟或丢弃,同时保证网络的高效运行。拥塞管理是指网络在发生拥塞时,如何进行管理和控制。处理的方法是使用队列技术,将所有要从一个接口发出的报文进入多个队列,按照各个队列的优先级进行处理。不同的队列算法用来解决不同的问题,并产生不同的效果。常用的队列有先进先出队列(First In First Out Queueing,FIFO)、优先队列(Priority Queueing,PQ)、定制队列(Custom Queueing,CQ)、加权公平队列(Weighted Fair Queueing,WFQ)、基于类的队列(Class-Based Queuing,CBQ,这是华为公司的称呼。思科公司称其为基于类的加权公平队列(Class Based Weighted Fair Queueing,CBWFQ))等。

网络管理者可以使用约定访问速度(Committed Access Rate,CAR)对流量进行控制，CAR 利用令牌桶(Tocken Bucket,TB)进行流量控制。CAR 可以为不同类别的报文设置不同的流量特性和标记特性。首先对报文进行分类,然后不同类别的报文有不同的流量特性和标记特性。此外 CAR 的策略还可以进行串联处理。例如,可以对所有的报文限制一个总的流量,然后在总的流量中,再限制部分报文的流量符合某个流量特性。

但是设置 CAR 之后每个数据流都有较大比例的丢包,为了减少报文的无谓丢失,应在上游路由器出口对报文进行通用流量整形(Generic Traffic Shaping,GTS),它可以对不规则或不符合预定流量特性的流量进行整形,以利于网络上下游之间的带宽匹配。GTS 与 CAR 一样,均采用了令牌桶技术控制流量。GTS 与 CAR 的主要区别在于：利用 CAR 进行报文流量控制时,对不符合流量特性的报文进行丢弃；而 GTS 对于不符合流量特性的报文则是进行缓冲,当网络拥塞消除后,GTS 再从缓冲队列中取出报文继续发送,这样就减少了报文的丢弃,同时满足报文的流量特性。

PQ 对报文进行分类,将所有报文分成最多至 4 类,分别属于 PQ 的 4 个队列中的一个，然后,按报文的类别将报文送入相应的队列。PQ 的 4 个队列分别为高优先队列(Top)、中优先队列(Middle)、正常优先队列(Normal)和低优先队列(Bottom),它们的优先级依次降低。在报文出队时,PQ 首先让高优先队列中的报文出队并发送,直到高优先队列中的报文发送完,然后依次对中优先队列、正常优先队列和低优先队列中的报文做同样处理。

CQ 对报文进行分类,将所有报文分成最多至 17 类,分别属于 CQ 的 17 个队列中的一个,按报文的类别将报文送入相应的队列。CQ 的 17 个队列中,0 号队列是优先队列,路由器总是先把 0 号队列中的报文发送完,然后才处理 1～16 号队列中的报文,所以 0 号队列一般作为系统队列,把实时性要求高的交互式协议报文放到 0 号队列。1～16 号队列中的报文可以按用户的定义分配它们能占用接口带宽的比例,这样就可以让不同业务的报文获得合理的带宽,从而既保证关键业务能获得较多的带宽,又不至于使非关键业务得不到带宽。在报

文出队时,CQ 按定义的带宽比例分别从 1～16 号队列取一定量的报文在接口上发送出去。

CBQ 首先根据报文进入网络设备的接口、报文的协议,报文是否匹配访问控制列表(Access Control List,ACL)来对报文进行分类,然后让不同类别的报文进入不同的队列。对于不匹配任何类别的报文,报文被送入默认队列,按 WFQ 进行处理,即按照流的方式进行处理。不同类别的报文可设定占用不同的带宽。在调度出队时,若优先队列中有报文,则调度器总是优先发送优先队列中的报文,直到优先队列中没有报文时,才调度发送其他队列中的报文。每个队列被分配了一定的带宽,调度器会按照每个队列分配到的带宽进行报文出队发送。进入优先队列的报文在接口没有发生拥塞时(此时所有队列中都没有报文),所有属于优先队列的报文都可以被发送。在接口发生拥塞时(队列中有报文时),进入优先队列的报文被限速,超出规定流量的报文将被丢弃。CBQ 最多允许将报文分为 64 类(其中包括默认类)。所以 N_1 的最大值为 63。默认队列的个数 N_2 可以由用户设定。对于优先队列,由于在接口拥塞的时候流量限制开始起作用,所以用户不必设置队列的长度(也就没有了尾丢弃)。另外,由于优先队列中的报文一般是语音报文(Voice over IP, VoIP),采用的是 UDP 报文,所以 WRED 的丢弃策略也不需要。对于其他队列,用户可以设定队列的最大长度。当队列的长度达到队列的最大长度时,默认采用尾丢弃的策略,但用户还可以选择用加权随机早期检测(Weighted Random Early Detection,WRED)的丢弃策略。

WFQ 对报文按流进行分类(相同源 IP 地址、目的 IP 地址、源端口号、目的端口号、协议号、TOS 的报文属于同一个流),每一个流被分配到一个队列,该过程称为散列,采用 HASH 算法完成,尽量将不同的流分入不同的队列。WFQ 的队列数目 N 可以配置。在出队时,WFQ 按流的优先级分配每个流应占有出口的带宽。优先级数值越小,所得的带宽越小;优先级的数值越大,所得的带宽越大。这样就保证了相同优先级业务之间的公平,体现了不同优先级业务之间的权值。带宽的总配额将是所有(流的优先级+1)之和,每个流所占带宽比例为(自己的优先级数+1)/(所有(流的优先级+1)之和)。WFQ 在保证公平的基础上对不同优先级的业务体现权值,而权值依赖于 IP 报文头中所携带的 IP 优先级。

由于内存资源的有限,按照传统的处理方法,当队列的长度达到规定的最大长度时,所有到来的报文都被丢弃。对于 TCP 报文,如果大量的报文被丢弃,将造成 TCP 超时,从而引发 TCP 的慢启动和拥塞避免机制,使 TCP 减少报文的发送。当队列同时丢弃多个 TCP 连接的报文时,将造成多个 TCP 连接同时进入慢启动和拥塞避免,称为 TCP 全局同步。这样多个 TCP 连接发向队列的报文将同时减少,使得发向队列的报文的量不及线路发送的速度,减少了线路带宽的利用。并且,发向队列的报文的流量总是忽大忽小,使线路上的流量总在极少和饱满之间波动。为了避免这种情况的发生,队列可以采用 WRED 的报文丢弃策略(WRED 与 RED 的区别在于前者引入 IP 优先权来区别丢弃策略)。采用 WRED 时,用户可以设定队列的低限和高限。当队列的长度小于低限时,不丢弃报文;当队列的长度在低限和高限之间时,WRED 开始随机丢弃报文(队列的长度越长,丢弃的概率越高);当队列的长度大于高限时,丢弃所有的报文。由于 WRED 随机地丢弃报文,将避免使多个 TCP 连接同时降低发送速度,从而避免了 TCP 的全局同步现象。当某个 TCP 连接的报文被丢弃,开始减速发送时,其他的 TCP 连接仍然有较高的发送速度。如果直接采用队列的长度与用户设定的低限、高限比较并进行丢弃(这是设置队列门限的绝对长度),将会对突发性的数据流造成不公正的待遇,不利于数据流的传输。所以,在与低限、高限比较并进行丢弃时,

采用队列的平均长度(这是设置队列门限与平均长度比较的相对值)。队列的平均长度是队列长度被低通滤波后的结果。它既反映了队列的变化趋势,又对队列长度的突发变化不敏感,避免了对突发性的数据流造成不公正的待遇。当队列机制采用 WFQ 时,可以为不同优先级的报文设定不同的队列长度滤波系数、低限、高限、丢弃概率。从而对不同优先级的报文提供不同的丢弃特性;当队列机制采用 FIFO、PQ、CQ 时,可以为每个队列设定不同的队列长度滤波系数、低限、高限、丢弃概率,为不同类别的报文提供不同的丢弃特性。当 WRED 和 WFQ 配合使用时,还可以实现基于流的 WRED。

拥塞管理技术对比如表 3.2 所示。

表 3.2　拥塞管理技术对比

对列名称	队列数	特　　点
FIFO	1	• 所有报文同等对待,报文到来的次序决定了报文可占用的带宽、报文延迟、报文丢失; • 对不配合的数据源(如 UDP 报文发送)无约束力,不配合的数据源会造成配合的数据源(如 TCP 报文发送)带宽受损失; • 不需要配置,易于使用; • 对时间敏感的实时应用(如 VoIP)的延迟得不到保证; • 处理简单,处理延迟小
PQ	4	• 如果不对高优先级的报文的带宽加限制,会造成低优先级的报文得不到带宽; • 可对不同业务数据提供绝对的优先,对时间敏感的实时应用(如 VoIP)的延迟可以得到保证。对优先业务的报文的带宽占用可以绝对优先; • 需配置,处理速度慢
CQ	17	• 当没有某些类别的报文时,能自动增加现存类别的报文可占的带宽; • 可对不同业务的报文按带宽比例分配带宽; • 需配置,处理速度慢
WFQ	用户决定	• 当流的数目减少时,能自动增加现存流可占的带宽; • 配置容易; • 处理速度比 FIFO 要慢,但比 PQ、CQ 要快; • 可以使延迟的抖动减小; • 可以为不同优先级的流分配不同的带宽; • 可以减小数据量小的交互式应用的延迟; • 可以保护配合(交互)的数据源(如 TCP 报文发送)的带宽
CBQ	用户决定(0～63)	• 对报文进行分类,为每类报文提供确保带宽; • 处理速度比 FIFO 要慢; • 可为部分报文提供快速转发服务,使延迟降低为最小; • 各类数据流确保带宽的总和小于接口带宽时,能自动增加各类流的带宽,从而充分利用线路的带宽; • 可以为非优先类的报文提供 WRED 的丢弃策略; • 为默认类报文提供 WFQ 服务

QoS 带宽管理是网络管理中一种必不可少的手段,可以有效地提高带宽的使用率,特别是针对企业的关键应用,使之得到优先的带宽保证,使企业网络的商务行为更加稳定与顺畅。

【实验目的】

(1) 掌握 QoS 中 CAR 的原理及配置方法。

(2) 掌握 QoS 中 GTS 的原理及配置方法。

(3) 掌握 QoS 中 PQ、CQ、WFQ、CBQ 的原理及配置方法。

(4) 掌握 QoS 中 WRED 的原理及配置方法。

【实验内容】

(1) 约定访问速度(CAR)的配置。

(2) 通用流量整形(GTS)的配置。

(3) 拥塞队列(PQ、CQ、WFQ、CBQ)的配置。

(4) 加权随机早期检测(WRED)的配置。

【实验设备】

H3C 系列交换机一台,H3C 系列路由器两台,安装有 FTP Server 的 PC 一台,安装有 FTP Client 的 PC 两台,专用配置电缆一根,网线五条,标准 V35 电缆一对。QoS 实验网络拓扑图如图 3.13 所示。

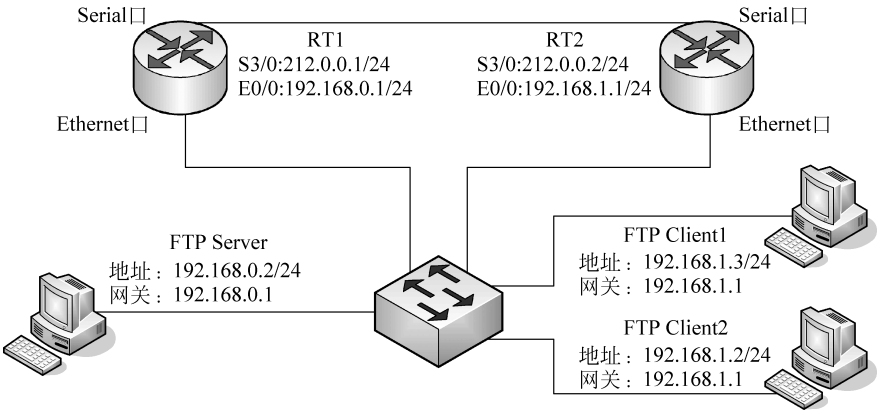

图 3.13　QoS 实验网络拓扑图

【实验步骤】

(1) 按照图 3.13 所示将网络拓扑结构搭建好,并将各个计算机配置好。

(2) 配置各个路由器的接口地址、路由协议、访问控制列表并设置相应的规则,将网络连通为后面的实验做准备。

① 对 RT1 做如下配置:

```
<H3C>system-view
[H3C]sysname RT1
[RT1]interface ethernet0/0
[RT1-Ethernet0/0]ip address 192.168.0.1 255.255.255.0
```

```
[RT1 - Ethernet0/0]interface serial3/0
[RT1 - serial3/0]ip address 212.0.0.1 255.255.255.0
[RT1 - Serial3/0]shutdown
[RT1 - Serial3/0]undo shutdown
[RT1 - serial3/0]acl number 3001
[RT1 - acl - adv - 3001]rule 0 permit ip source 192.168.0.2 0 destination 192.168.1.2 0
[RT1 - acl - adv - 3001]rule 1 deny ip
[RT1 - acl - adv - 3001] acl number 3002
[RT1 - acl - adv - 3002]rule 0 permit ip source 192.168.0.2 0 destination 192.168.1.3 0
[RT1 - acl - adv - 3002] rule 1 deny ip
[RT1 - acl - adv - 3002] rip
[RT1 - rip]network 192.168.0.0
[RT1 - rip]network 212.0.0.0
[RT1 - rip]quit
```

② 对 RT2 做如下配置：

```
< H3C > system - view
[H3C]sysname RT2
[RT2]interface ethernet0/0
[RT2 - Ethernet0/0]ip address 192.168.1.1 255.0.0.0
[RT2 - Ethernet0/0]interface serial3/0
[RT2 - serial3/0]ip address 212.0.0.2 255.255.255.0
[RT2 - serial3/0]shutdown
[RT2 - serial3/0]undo shutdown
[RT2 - serial3/0] acl number 3001
[RT2 - acl - adv - 3001]rule 0 permit ip source 192.168.0.2 0 destination 192.168.1.2 0
[RT2 - acl - adv - 3001]rule 1 deny ip
[RT2 - acl - adv - 3001] acl number 3002
[RT2 - acl - adv - 3002]rule 0 permit ip source 192.168.0.2 0 destination 192.168.1.3 0
[RT2 - acl - adv - 3002] rule 1 deny ip
[RT2 - acl - adv - 3002]rip
[RT2 - rip]network 192.168.1.0
[RT2 - rip]network 212.0.0.0
[RT2 - rip]quit
```

(3) CAR 实验。通过 ACL 设置 CAR 规则对数据流进行分类，对不同的数据流设置不同的 CAR，本实验是在步骤(2)的基础上进行的。

① 启动 FTPServer、FTPClient，两台计算机同时从服务器 FTPServer 上下载同一个大约 20MB 的文件，比较两台计算机的下载速率。

② 在接口上应用承诺访问速率策略进行流量监管。

```
[RT2] interface serial3/0
[RT2 - serial3/0]qos car inbound acl 3001 cir 800000 cbs 150000 ebs 0 green pass red discard
[RT2 - serial3/0]qos car inbound acl 3002 cir 80000 cbs 15000 ebs 0 green pass red discard
[RT2 - serial3/0]shutdown
[RT2 - serial3/0]undo shutdown
[RT2 - serial3/0]quit
```

③ 查看配置的 CAR 状态。

```
[RT2]display qos car interface
```

④ 两台计算机再次同时下载同一文件并比较它们的速率,分析其中的原因。

⑤ 比较和上一步显示的信息的差异。

```
[RT2]display qos car interface
```

(4) GTS 实验是在 CAR 实验的基础上进行的,RT2 配置不变,在 RT1 上增加配置。

① 在接口上应用通用流量整形策略。

```
[RT1] interface serial3/0
[RT1 - serial3/0]qos gts acl 3001 cir 800000 cbs 150000 ebs 0 queue - length 20
[RT1 - serial3/0]qos gts acl 3002 cir 80000 cbs 15000 ebs 0 queue - length 20
[RT1 - Serial3/0]shutdown
[RT1 - Serial3/0]undo shutdown
```

② 查看配置的 GTS 状态。

```
[RT1]display qos gts interface
```

③ 两台计算机再次同时下载同一文件并比较它们的速率,分析其中的原因。

④ 比较和上一步显示的信息的差异。

```
[RT1]display qos gts interface
```

⑤ 比较和 CAR 实验显示信息的差异。

```
[RT2]display qos car interface
```

(5) PQ 实验是在步骤(2)的基础上进行的。注意,PQ 只对接口出流量起作用,对入流量无法控制。

① 指定 SNMP 的配置信息,设备 SNMP 版本为 V3。

```
[RT1] snmp - agent sys - info version v3
```

② 设置优先级队列。

```
[RT1]qos pql 1 queue middle queue - length 20
[RT1]qos pql 1 queue normal queue - length 20
[RT1]qos pql 1 queue bottom queue - length 10
[RT1]qos pql 1 protocol ip acl 3001 queue top
[RT1]qos pql 1 protocol ip acl 3002 queue bottom
```

③ 设置接口发送令牌的速率为 1,用以在接口上产生拥塞,范围是 1～50,默认为 50。

```
[RT1] interface serial3/0
[RT1 - serial3/0]qmtoken 1
[RT1 - serial3/0]undo ip fast - forwarding
```

④ 在接口上应用优先队列调度机制。

```
[RT1 - serial3/0]qos pq pql 1
[RT1 - serial3/0]shutdown
[RT1 - serial3/0]undo shutdown
[RT1 - serial3/0]quit
```

⑤ 设置另一个路由器的接口的波特率为一较小值,用以产生拥塞。

```
[RT2] interface serial3/0
[RT2 - serial3/0]baudrate 19200
[RT2 - serial3/0]shutdown
[RT2 - serial3/0]undo shutdown
[RT2 - serial3/0]quit
```

⑥ 两台计算机同时从 FTPServer 下载同一个文件并查看 PQ 状态。

```
[RT1]display qos pq interface serial3/0
```

(6) CQ 实验是在步骤(2)的基础上进行的。

① 指定 SNMP 的配置信息,设备 SNMP 版本为 V3。

```
[RT1] snmp - agent sys - info version v3
```

② 设置定制队列,将 acl3001 定义的数据流入 1 队列,每次轮询的字节数为 1000,将 acl3002 定义的数据流入 2 队列,每次轮询的字节数为 3000。

```
[RT1]qos cql 1 queue 1 queue - length 10
[RT1]qos cql 1 queue 1 serving 1000
[RT1]qos cql 1 queue 2 queue - length 30
[RT1]qos cql 1 queue 2 serving 3000
[RT1]qos cql 1 protocol ip acl 3001 queue 1
[RT1]qos cql 1 protocol ip acl 3002 queue 2
```

③ 在接口上应用定制队列调度机制。

```
[RT1 - serial3/0]qos cq cql 1
[RT1 - serial3/0]shutdown
[RT1 - serial3/0]undo shutdown
[RT1 - serial3/0]quit
```

④ 对另一个路由器做相应的配置,与 PQ 实验中 RT2 的配置相同。

⑤ 两台计算机同时从 FTPServer 下载同一个文件并查看 CQ 状态及速率的差异。

```
[RT1]display qos cq interface serial3/0
```

(7) CBQ 配置实验是在步骤(2)的基础上进行的。

① 配置分类。

```
[RT1]traffic classifier 1 operator and
[RT1 - classifier - 1]if - match acl 3001
[RT1 - classifier - 1]traffic classifier 2 operator and
[RT1 - classifier - 2]if - match acl 3002
[RT1 - classifier - 2]quit
```

② 定义不同的行为以便对定义的数据流进行控制。

```
[RT1]traffic behavior 1
[RT1 - behavior - 1]car cir 80000 cbs 150000 ebs 0 green pass red discard
```

```
[RT1 - behavior - 1]traffic behavior 2
[RT1 - behavior - 2]car cir 800000 cbs 1500000 ebs 0 green pass red discard
[RT1 - behavior - 2]quit
```

③ 定义 QoS 策略。

```
[RT1]qos policy 1
[RT1 - qospolicy - 1]classifier 1 behavior 1
[RT1 - qospolicy - 1]classifier 2 behavior 2
```

④ 在以太网接口上应用定义的策略。

```
[RT1 - qospolicy - 1]interface ethernet0/0
[RT1 - Ethernet0/0]qos apply policy 1 inbound
[RT1 - Ethernet0/0]quit
```

⑤ 指定 SNMP 的配置信息,设备 SNMP 版本为 V3。

```
[RT1] snmp - agent sys - info version v3
```

⑥ 对另一个路由器做相应的配置,与 PQ 实验中 RT2 的配置相同。

⑦ 两台计算机同时从 FTPServer 下载同一个文件并查看 CBQ 状态及速率的差异。

```
[RT1]display qos policy interface
```

(8) WFQ 配置实验是在步骤(2)的基础上进行的。

① 指定 SNMP 的配置信息,设备 SNMP 版本为 V3。

```
[RT1] snmp - agent sys - info version v3
```

② 在接口上应用承诺访问速率策略进行流量监管。

```
[RT1]interface ethernet0/0
[RT1 - Ethernet0/0]qos car inbound acl 3001 cir 80000 cbs 150000 ebs 0 green remark - prec - pass
7 red discard
[RT1 - Ethernet0/0]qos car inbound acl 3002 cir 80000 cbs 150000 ebs 0 green remark - prec - pass
1 red discard
```

③ 在广域网接口上应用加权公平队列调度机制。

```
[RT1 - Ethernet0/0]interface serial3/0
[RT1 - serial3/0]qos wfq queue - length 64 queue - number 256
[RT1 - serial3/0]shutdown
[RT1 - serial3/0]undo shutdown
[RT1 - serial3/0]quit
[RT1]snmp - agent
```

④ 对另一个路由器做相应的配置,与 PQ 实验中 RT2 的配置相同。

⑤ 两台计算机同时从 FTPServer 下载同一个文件并查看 WFQ 状态及速率的差异。

```
[RT1]display qos wfq interface
```

(9) WRED 配置实验。这里考虑 WRED 和 WFQ 配合使用,对 RT1 的配置只需在

WFQ 实验的基础上加上下列命令即可。

```
[RT1 - serial3/0]qos wfq queue - length 10 queue - number 16
[RT1 - serial3/0]qos wred                    //在接口上应用加权随机早期检测丢弃机制
```

【思考题】

比较不同的拥塞队列的异同。

实验 3-9　网络可靠性

【实验背景】

随着 Internet 的迅猛发展，基于网络的应用逐渐增多。这就对网络的可靠性提出了越来越高的要求。斥资对所有网络设备进行更新当然是一种很好的可靠性解决方案；但本着保护现有投资的角度考虑，可以采用廉价冗余的思路，在可靠性和经济性方面找到平衡点。

虚拟路由冗余协议（Virtual Router Redundancy Protocol，VRRP）就是一种很好的解决方案。在该协议中，对共享多存取访问介质（如以太网）上终端 IP 设备的默认网关（Default Gateway）进行冗余备份，从而在其中一台路由设备宕机时，备份路由设备及时接管转发工作，向用户提供透明的切换，提高了网络服务质量。一个 VRRP 路由器有唯一的标识：VRID，范围为 0～255。该路由器对外表现为唯一的虚拟 MAC 地址，地址的格式为 00-00-5E-00-01-[VRID]。主控路由器负责对 ARP 请求用该 MAC 地址做应答。这样，无论如何切换，保证给终端设备的是唯一一致的 IP 和 MAC 地址，减少了切换对终端设备的影响。VRRP 控制报文只有一种：VRRP 通告（Advertisement）。它使用 IP 多播数据包进行封装，组地址为 224.0.0.18，发布范围只限于同一局域网内。这保证了 VRID 在不同网络中可以重复使用。为了减少网络带宽消耗，只有主控路由器才可以周期性地发送 VRRP 通告报文。备份路由器在连续三个通告间隔内收不到 VRRP 或收到优先级为 0 的通告后启动新的一轮 VRRP 选举。在 VRRP 路由器组中，按优先级选举主控路由器，VRRP 协议中优先级范围是 0～255。若 VRRP 路由器的 IP 地址和虚拟路由器的接口 IP 地址相同，则称该虚拟路由器作 VRRP 组中的 IP 地址所有者；IP 地址所有者自动具有最高优先级：255。优先级 0 一般用在 IP 地址所有者主动放弃主控者角色时使用。可配置的优先级范围为 1～254。优先级的配置原则可以依据链路的速度和成本、路由器性能和可靠性以及其他管理策略设定。主控路由器的选举中，高优先级的虚拟路由器获胜，因此，如果在 VRRP 组中有 IP 地址所有者，则它总是作为主控路由的角色出现。对于相同优先级的候选路由器，按照 IP 地址大小顺序选举。VRRP 还提供了优先级抢占策略，如果配置了该策略，高优先级的备份路由器便会剥夺当前低优先级的主控路由器而成为新的主控路由器。为了保证 VRRP 协议的安全性，提供了两种安全认证措施：明文认证和 IP 头认证。明文认证方式要求：在加入一个 VRRP 路由器组时，必须同时提供相同的 VRID 和明文密码。明文认证能避免在局域网内的配置错误，但不能防止通过网络监听方式获得密码。IP 头认证的方式提供了更高的安全性，能够防止报文重放和修改等攻击。

【实验目的】

(1) 了解常用的提高网络可靠性的方法。

(2) 掌握虚拟路由冗余协议的运用技术。

【实验内容】

在路由器上配置虚拟路由冗余协议,以提高网络的可靠性。

【实验设备】

H3C 系列路由器两台、H3C 系列交换机一台、PC 三台、网线五根、配置电缆一根、V35 电缆两对。网络可靠性实验拓扑结构如图 3.14 所示。

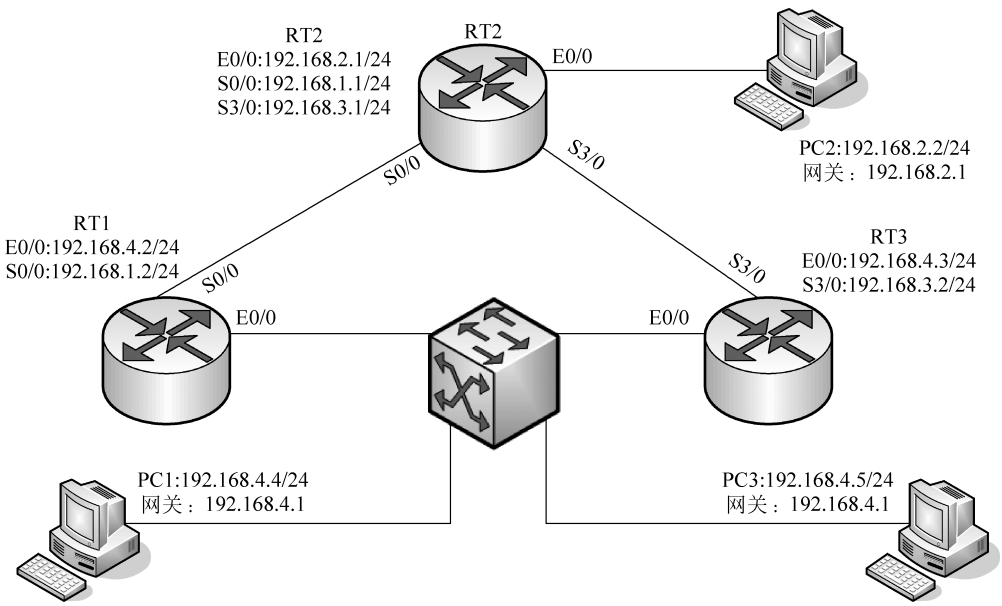

图 3.14　网络可靠性实验拓扑结构图

【实验步骤】

(1) 首先按照图 3.14 要求将网络搭建起来。

(2) 按照图 3.14 配置好各个就算机的 IP 地址、子网掩码、默认网关。

(3) 对路由器 RT1 做如下配置:

```
<H3C>system-view
[H3C]sysname RT1
[RT1]interface ethernet0/0
[RT1-Ethernet0/0]ip address 192.168.4.2 255.255.255.0
[RT1-Ethernet0/0]vrrp vrid 1 virtual-ip 192.168.4.1
[RT1-Ethernet0/0]interface serial0/0
[RT1-Serial0/0]ip address 192.168.1.2 255.255.255.0
```

```
[RT1-Serial0/0]shutdown
[RT1-Serial0/0]undo shutdown
[RT1-Serial0/0]quit
[RT1]router id 192.168.4.2
[RT1]ospf 1
[RT1-ospf-1]area 0
[RT1-ospf-1-area-0.0.0.0]network 192.168.1.0 0.0.0.255
[RT1-ospf-1-area-0.0.0.0]network 192.168.4.0 0.0.0.255
[RT1-ospf-1-area-0.0.0.0]quit
[RT1-ospf-1]quit
[RT1]
```

(4) 对路由器 RT2 做如下配置：

```
<H3C>system-view
[H3C]sysname RT2
[RT2]interface ethernet0/0
[RT2-Ethernet0/0]ip address 192.168.2.1 255.255.255.0
[RT2-Ethernet0/0]interface serial0/0
[RT2-Serial0/0]ip address 192.168.1.1 255.255.255.0
[RT2-Serial0/0]shutdown
[RT2-Serial0/0]undo shutdown
[RT2-Serial0/0]interface serial3/0
[RT2-Serial3/0]ip address 192.168.3.1 255.255.255.0
[RT2-Serial3/0]shutdown
[RT2-Serial3/0]undo shutdown
[RT2-Serial3/0]quit
[RT2]router id 192.168.2.1
[RT2]ospf 1
[RT2-ospf-1]area 0
[RT2-ospf-1-area-0.0.0.0]network 192.168.1.0 0.0.0.255
[RT2-ospf-1-area-0.0.0.0]network 192.168.2.0 0.0.0.255
[RT2-ospf-1-area-0.0.0.0]network 192.168.3.0 0.0.0.255
[RT2-ospf-1-area-0.0.0.0]quit
[RT2-ospf-1]quit
[RT2]
```

(5) 对路由器 RT3 做如下配置：

```
<H3C>system-view
[H3C]sysname RT3
[RT3]interface ethernet0/0
[RT3-Ethernet0/0]ip address 192.168.4.3 255.255.255.0
[RT3-Ethernet0/0]vrrp vrid 1 virtual-ip 192.168.4.1
[RT3-Ethernet0/0]interface serial3/0
[RT3-Serial3/0]ip address 192.168.3.2 255.255.255.0
[RT3-Serial3/0]shutdown
[RT3-Serial3/0]undo shutdown
[RT3-Serial3/0]quit
[RT3]router id 192.168.4.3
[RT3]ospf 1
[RT3-ospf-1]area 0
[RT3-ospf-1-area-0.0.0.0]network 192.168.3.0 0.0.0.255
```

```
[RT3-ospf-1-area-0.0.0.0]network 192.168.4.0 0.0.0.255
[RT3-ospf-1-area-0.0.0.0]quit
[RT3-ospf-1]quit
[RT3]
```

(6) 在 VRRP 中,允许一台路由器加入多个备份组,通过多备份组设置可以实现负荷分担。路由器 RT1 作为备份组 1 的主路由器,同时又为备份组 2 的备份路由器。而路由器 RT3 正好相反,作为备份组 2 的主路由器,并为备份组 1 的备份路由器。PCA 使用备份组 1 的虚拟 IP 作网关,PCC 使用备份组 2 的虚拟 IP 作为网关。这样,能达到既分担数据流,又实现相互备份的目的。在做该实验前,需要先修改 PCC 的默认网关为 192.168.4.10。对路由器 RT2 的配置没有发生改变,对 RT1.RT3 的配置分别做如下改变:

将 RT1 中的配置命令:

```
[RT1-Ethernet0/0]vrrp vrid 1 virtual-ip 192.168.4.1
```

改为命令:

```
[RT1-Ethernet0/0]vrrp vrid 1 virtual-ip 192.168.4.1
[RT1-Ethernet0/0]vrrp vrid 1 priority 120                //设置优先级为 120
[RT1-Ethernet0/0]vrrp vrid 2 virtual-ip 192.168.4.10   //默认优先级为 100
```

将 RT3 中的配置命令:

```
[RT3-Ethernet0/0]vrrp vrid 1 virtual-ip 192.168.4.1
```

改为命令:

```
[RT3-Ethernet0/0]vrrp vrid 1 virtual-ip 192.168.4.1
[RT3-Ethernet0/0]vrrp vrid 2 virtual-ip 192.168.4.10
[RT3-Ethernet0/0]vrrp vrid 2 priority 120
```

(7) 在实际网络运行中,为了更进一步地保证网络可靠性,还需要保证网络设备的出口出现故障时,局域网用户的数据流量能够通过其他设备转发,VRRP 的监控功能可以达到该要求。当网络出口发生故障时,自动降低在备份组中的优先级,从而让高优先级的设备担当主路由器转发局域网内的数据。要实现该功能,只需在步骤(6)的基础上分别在 RT1.RT3 上增加如下配置即可:

RT1:

```
[RT1-Ethernet0/0]vrrp vrid 1 track serial0/0 reduced 30
[RT1-Ethernet0/0]vrrp vrid 2 track serial0/0 reduced 30
```

RT3:

```
[RT3-Ethernet0/0]vrrp vrid 1 track serial3/0 reduced 30
[RT3-Ethernet0/0]vrrp vrid 2 track serial3/0 reduced 30
```

【思考题】

如果一个路由器有两个接口作为出口,正常情况下,路由器使用主线路连入网络,当主线路出现故障时启用备份线路进行接入,该怎么操作?

实验 3-10　路由综合实验

【实验背景】

对于一个大型企业集团来说，其各个分支机构往往分布在多个城市，甚至多个国家，网络拓扑结构也比较复杂，实现集团内设备的互连互通需要综合运用多种技术，而不是单纯的某一种技术。

【实验目的】

（1）掌握在一个网络中综合运用多种链路层协议的方法。
（2）掌握在一个网络中综合运用多种路由协议的方法。
（3）掌握综合运用多种技术方法。

【实验内容】

（1）在一个网络中同时配置 PPP 协议、x.25 协议、Frame-relay 等多种链路层协议。
（2）在一个网络中同时配置静态路由、RIP、OSPF 等多种路由协议。

【实验设备】

H3C 路由器四台、H3C 交换机四台、PC 四台、网线八根、配置电缆一根、V35 电缆三对。路由综合实验网络拓扑图如图 3.15 所示。

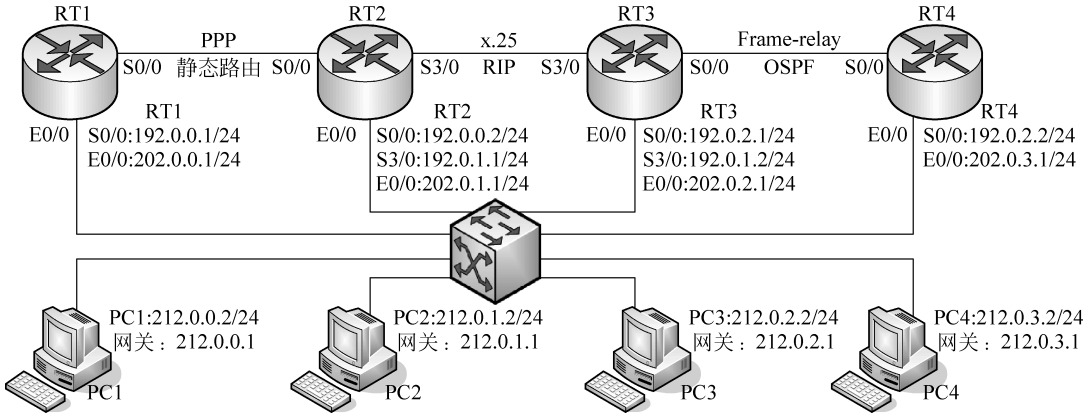

图 3.15　路由综合实验网络拓扑图

【实验步骤】

（1）首先按照图 3.15 要求将网络搭建起来。
（2）按照图 3.15 的要求将各计算机的 IP 地址、子网掩码、网关设置好。
（3）对 RT1 做如下配置：

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

```
[H3C]sysname RT1
[RT1]interface Ethernet0/0
[RT1-Ethernet0/0]ip address 212.0.0.1 255.255.255.0
[RT1-Ethernet0/0]interface Serial0/0
[RT1-Serial0/0]link-protocol ppp
[RT1-Serial0/0]ip address 192.0.0.1 255.255.255.0
[RT1-Serial0/0]shutdown
[RT1-Serial0/0]undo shutdown
[RT1-Serial0/0]quit
[RT1]ip route-static 0.0.0.0 0 192.0.0.2
```

(4) 对 RT2 做如下配置:

```
<H3C>system-view
[H3C]sysname RT2
[RT2]interface Ethernet0/0
[RT2-Ethernet0/0]ip address 212.0.0.2 255.255.255.0
[RT2-Ethernet0/0]interface Serial0/0
[RT2-Serial0/0]link-protocol ppp
[RT2-Serial0/0]ip address 192.0.0.2 255.255.255.0
[RT2-Serial0/0]shutdown
[RT2-Serial0/0]undo shutdown
[RT2-Serial0/0]interface Serial3/0
[RT2-Serial3/0]link-protocol x25
[RT2-Serial3/0]x25 x121-address 1111111111
[RT2-Serial3/0]x25 map ip 192.0.1.2 x121-address 2222222222
[RT2-Serial3/0]ip address 192.0.1.1 255.255.255.0
[RT2-Serial3/0]shutdown
[RT2-Serial3/0]undo shutdown
[RT2-Serial3/0]quit
[RT2]ip route-static 212.0.0.0 24 192.0.0.1
[RT2]rip
[RT2-rip]network 192.0.1.0
[RT2-rip]network 212.0.1.0
[RT2-rip]import direct cost 2
[RT2-rip]import static cost 2
[RT2-rip]peer 192.0.1.2
[RT2-rip]quit
```

(5) 对 RT3 做如下配置:

```
<H3C>system-view
[H3C]sysname RT3
[RT3]interface Ethernet0/0
[RT3-Ethernet0/0]ip address 212.0.2.1 255.255.255.0
[RT3-Ethernet0/0]interface Serial3/0
[RT3-Serial3/0]link-protocol x25 dce
[RT3-Serial3/0]x25 x121-address 2222222222
[RT3-Serial3/0]x25 map ip 192.0.1.1 x121-address 1111111111
[RT3-Serial3/0]ip address 192.0.1.2 255.255.255.0
```

```
[RT3 - Serial3/0]shutdown
[RT3 - Serial3/0]undo shutdown
[RT3 - Serial3/0]interface Serial0/0
[RT3 - Serial0/0]link - protocol fr
[RT3 - Serial0/0]fr lmi type ansi
[RT3 - Serial0/0]fr dlci 100
[RT3 - fr - dlci - Serial0/0 - 100]ip address 192.0.2.1 255.255.255.0
[RT3 - Serial0/0]fr map ip 192.0.2.2 100
[RT3 - Serial0/0]shutdown
[RT3 - Serial0/0]undo shutdown
[RT3 - Serial0/0]quit
[RT3]rip
[RT3 - rip]network 192.0.1.0
[RT3 - rip]network 212.0.2.0
[RT3 - rip]import direct cost 2
[RT3 - rip]import ospf cost 2
[RT3 - rip]peer 192.0.1.1
[RT3 - rip]peer 192.0.2.2
[RT3 - rip]quit
[RT3]router id 1.1.1.1
[RT3]ospf
[RT3 - ospf - 1]area 0
[RT3 - ospf - 1 - area - 0.0.0.1]network 212.0.2.0 0.0.0.255
[RT3 - ospf - 1 - area - 0.0.0.1]network 192.0.2.0 0.0.0.255
[RT3 - ospf - 1 - area - 0.0.0.0]quit
[RT3 - ospf - 1]import direct cost 2
[RT3 - ospf - 1]import rip cost 2
[RT3 - ospf - 1]quit
```

(6) 对 RT4 做如下配置：

```
< H3C > system - view
[H3C]sysname RT4
[RT4]fr switching
[RT4]interface Ethernet0/0
[RT4 - Ethernet0/0]ip address 212.0.3.1 255.255.255.0
[RT4 - Ethernet0/0]interface Serial0/0
[RT4 - Serial0/0]link - protocol fr
[RT4 - Serial0/0]fr interface - type dce
[RT4 - Serial0/0]fr map ip 192.0.2.1 100
[RT4 - Serial0/0]fr dlci 100
[RT4 - fr - dlci - Serial0/0 - 100]ip address 192.0.2.2 255.255.255.0
[RT4 - Serial0/0]shutdown
[RT4 - Serial0/0]undo shutdown
[RT4 - Serial0/0]quit
[RT4]router id 2.2.2.2
[RT4]ospf
[RT4 - ospf - 1]area 0
[RT4 - ospf - 1 - area - 0.0.0.1]network 212.0.3.0 0.0.0.255
```

```
[RT4-ospf-1-area-0.0.0.1]network 192.0.2.0 0.0.0.255
[RT4-ospf-1-area-0.0.0.0]quit
[RT4-ospf-1]quit
```


注意:

① 在 x.25 和 frame-relay 协议上启动 RIP 协议必须配置 peer 命令,否则不能正常工作,但在 PPP 协议上不需要配置。

② 路由器的不同协议交换路由信息需要引入其他路由协议拥有的路由信息。

【思考题】

路由器的不同路由协议如何交换路由信息?