实验1 网络设备基本操作

实验任务一：通过 Console 登录

本实验的主要任务是练习通过 Console 电缆连接进行设备配置的方法。试验前请保证路由器（交换机）的所有配置已经清空。

步骤一：连接配置电缆

步骤二：启动 PC，运行超级终端

在 PC 桌面上运行【开始】->【程序】->【附件】->【通信】->【超级终端】。填入一个任意名称，点击【确定】。

每秒位数为 9600bps、8 位数据位、1 位停止位、无奇偶校验和无流量控制

步骤三：进入 Console 配置界面

用户视图的提示符为<系统名>

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

执行 system-view 命令进入系统视图。系统视图的提示符为[系统名]。执行 quit 命令可以从系统视图切换到用户视图。

步骤二：练习使用帮助特性和补全键

s?　　sysname ?　　<Tab>　　<Tab>

步骤三：更改系统名称

```
 [H3C]sysname YourName
[YourName]
```

步骤四：更改系统时间

```
 [YourName]display clock
17:28:07 UTC Mon 09/08/2008
[YourName]quit
<YourName>clock datetime 10:20:30 10/01/2008
<YourName>display clock
10:20:32 UTC Wed 10/01/2008
```

步骤五：显示系统运行配置

```
<YourName>display current-configuration
```

<Space>　　<Enter>　　<Ctrl+C>

步骤六：显示保存的配置

```
<YourName>display saved-configuration
```

此时尚未保存配置，因此不存在 saved-configuration

步骤七：保存配置

默认配置文件名通常为 startup.cfg，某些版本为 config.cfg。

```
<YourName>save
The current configuration will be written to the device. Are you sure? [Y/N]:
Please input the file name(*.cfg)[cf:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
Now saving current configuration to the device.
Saving configuration cf:/startup.cfg. Please wait...
.
Configuration is saved to cf successfully.........
<YourName>save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[cf:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
cf:/startup.cfg exists, overwrite? [Y/N]:y

Validating file. Please wait...
Now saving current configuration to the device.
Saving configuration cf:/startup.cfg. Please wait...
.
Configuration is saved to cf successfully.
```

由于执行了 save 命令，保存配置与运行配置一致。

步骤八：删除和清空配置

```
[YourName]undo sysname


<YourName>reset saved-configuration
The saved configuration file will be erased. Are you sure? [Y/N]:y
Configuration file in cf is being cleared.
Please wait ...
.........
 Configuration file in cf is cleared.
<YourName>reboot
  Start to check configuration with next startup configuration file, please wait
.......
  This command will reboot the device. Current configuration may be lost in next
 startup if you continue. Continue? [Y/N]:Y
```

步骤九：显示文件目录

```
<YourName> pwd
cf:

<YourName>dir
Directory of cf:/

   0   drw-        -   Jan 19 2007 18:26:34   logfile
   1   -rw-  16337860  Aug 03 2007 17:59:36   msr30-cmw520-r1206p01-si.bin
   2   -rw-      739   Oct 01 2008 10:15:54   startup.cfg

249852 KB total (221648 KB free)
```

```
File system type of cf: FAT32
```

步骤十：显示文本文件内容

用 more 命令

步骤十一：改变当前工作路径

使 cd 命令

步骤十二：文件删除

用 save、dir、delete、dir 命令

虽然删除了该文件，但是在删除该文件前后，为什么 CF 卡的可用内存空间却没有变化呢。那是因为使用 delete 命令删除文件时，被删除的文件被保存在回收站中，仍会占用存储空间。如果用户经常使用该命令删除文件，则可能导致设备的存储空间不足。如果要彻底删除回收站中的某个废弃文件，必须在文件的原归属目录下执行 reset recycle-bin 命令，才可以将回收站中的废弃文件彻底删除，以回收存储空间。

dir /all 命令显示内容包括隐藏文件、隐藏子文件夹以及回收站中的原属于该目录下的文件的信息，回收站里的文件会以方括号“[ ]”标出。文件 myconfig.cfg 应该仍然存在于 CF 卡的回收站中。

用 reset recycle-bin 命令清空回收站后，可发现文件列表中已经找不到 myconfig.cfg 文件，并且可用内存空间已经增加。

使用 delete /unreserved 命令删除一个文件，则该文件将被彻底删除，不能再恢复。其效果等同于执行 delete 命令之后，再在同一个目录下执行了 reset recycle-bin 命令。

实验任务三：通过 Telnet 登录

步骤一：通过 Console 口配置 Telnet 用户

```
[YourName-luser-test] password simple test
[YourName-luser-test] service-type telnet
[YourName-luser-test] level 0
[YourName-luser-test] quit
```

在某些 CMW 版本中需用命令 authorization-attribute level 0 替代命令 level 0。

步骤二：配置 super 口令

```
[YourName] super password  level 3 simple H3C
```

步骤三：配置登录欢迎信息

```
[YourName]header login
Please input banner content, and quit with the character '%'.
Welcome to H3C world!%
[YourName]
```

步骤四：配置对 Telnet 用户使用缺省的本地认证

```
[YourName]user-interface vty 0 4
[YourName-ui-vty0-4]authentication-mode scheme
```

步骤五：进入接口视图，配置以太口和 PC 网卡地址

```
[YourName]interface GigabitEthernet 0/1
[YourName-GigabitEthernet0/1]ip add 192.168.0.1 255.255.255.0
[YourName-GigabitEthernet0/1]
```

步骤六：打开 Telnet 服务

```
[YourName]telnet server enable
% Telnet server has been started
```

步骤七：使用 Telnet 登录

```
telnet 192.168.0.10
```

由于此时登录用户处于访问级别，所以只能看到并使用有限的几个命令。同时，超级终端上会有如下信息显示，表明源 IP 为 192.168.0.10 的设备远程登入到路由器上。

```
<YourName>
%Oct  2 10:27:13:325 2008 YourName SHELL/4/LOGIN: test login from 192.168.0.10
```

步骤八：更改登录用户级别

```
super 3
```

能使用的命令明显多于 level0

步骤九：保存配置，重新启动

使用 save 和 reboot 命令

实验任务四：使用 FTP 上传下载系统文件

步骤一：通过 Console 口配置 FTP 用户

```
[YourName]local-user test_ftp
[YourName-luser-test_ftp] password simple test_ftp
[YourName-luser-test_ftp] service-type ftp
[YourName-luser-test_ftp] level 3
```

步骤二：打开 FTP 服务

```
[YourName]ftp server enable
Info: Start FTP server.
```

步骤三：使用 FTP 登录

步骤四：使用 FTP 上传文件

如果用户以 Administrator 登录 PC，则默认的本地目录是 C:\Documents and Settings\Administrator。

步骤五：使用 FTP 下载文件

dir　　通常为 startup.cfg 或 config.cfg

实验任务五：使用 TFTP 上传下载系统文件

本实验以 3CDaemon 程序作为 TFTP 的服务器端。实际上任何支持 TFTP 服务的程序均可以使用。

步骤一：启动 TFTP 服务器端程序

步骤二：使用 TFTP 下载文件

```
<YourName>tftp 192.168.0.10 get mysystem.sys
The file mysystem.sys exists. Overwrite it? [Y/N]:y
  Verifying server file...
  Deleting the old file, please wait...

  File will be transferred in binary mode
  Downloading file from remote tftp server, please wait...
  TFTP:     913 bytes received in 0 second(s)
  File downloaded successfully.
```

步骤三：使用 TFTP 上传文件

```
<YourName>tftp 192.168.0.10 put config.cfg

  File will be transferred in binary mode
  Sending file to remote tftp server. Please wait... \
  TFTP:     940 bytes sent in 0 second(s).
  File uploaded successfully.
```

实验2 网络设备基本调试

实验任务一：搭建基本连接环境

步骤一：完成 PC、交换机、路由器互连

在教师指导下，完成实验环境的搭建。

步骤二：配置 IP 地址

RTA 的配置如下：

```
[H3C]sysname RTA
[RTA]interface GigabitEthernet 0/0
[RTA-GigabitEthernet0/0]ip add 192.168.0.1 24
[RTA]interface GigabitEthernet 0/1
[RTA-GigabitEthernet0/1]ip add 192.168.1.1 24
```

实验任务二：检查连通性

步骤一：检测 RTA 与 PCA 的连通性

```
[RTA]ping 192.168.0.10
 PING 192.168.1.2: 56  data bytes, press CTRL_C to break
   Reply from 192.168.0.10: bytes=56 Sequence=1 ttl=255 time=27 ms
   Reply from 192.168.0.10: bytes=56 Sequence=2 ttl=255 time=27 ms
   Reply from 192.168.0.10: bytes=56 Sequence=3 ttl=255 time=27 ms
   Reply from 192.168.0.10: bytes=56 Sequence=4 ttl=255 time=26 ms
   Reply from 192.168.0.10: bytes=56 Sequence=5 ttl=255 time=26 ms

 --- 192.168.0.10 ping statistics ---
   5 packet(s) transmitted
   5 packet(s) received
   0.00% packet loss
   round-trip min/avg/max = 26/26/27 ms
```

结果显示，RTA 收到了 ICMP 的 Echo Reply 报文，RTA 可以 ping 通 PCA。反之亦然。

这里路由器默认是发送 5 个 ICMP 请求报文，大小是 56bytes，所以 PING 成功后，会收到 5 个 Reply 报文。而 Windows 默认是发送 4 个 ICMP 请求报文，大小是 32bytes。

查看路由器 ping 命令可携带的参数。使用的完整命令为：

```
<RTA>ping ?
```

再次检查对 PCA 的连通性，使用的完整命令依次为：

```
<RTA>ping -c 50 192.168.0.10
<RTA>ping -s 512 192.168.0.10
<RTA>ping -a 192.168.1.1 192.168.0.10
```

步骤二：检测 RTA 与 PCB 的连通性

```
ping 192.168.1.1
```

实验任务三：检查数据包转发路径

步骤一：检查从 PCA 到 PCB 的数据包转发路径

```
tracert 192.168.1.10
```

总共 2 跳，第一跳为 RTA，第二跳到达 PCB。

步骤二：检查从 RTA 到 PCB 的数据包转发路径

```
<RTA>tracert 192.168.1.10
```

总共 1 跳，第一跳到达 PCB。

查看路由器 tracert 命令携带的参数。使用的完整命令为：

```
<RTA>tracert ?
```

实验任务四：练习使用察看调试信息

步骤一：开启 RTA 终端对信息的监视和显示功能

```
<RTB>terminal monitor
% Current terminal monitor is on.

<RTB>terminal debugging
% Current terminal debugging is on.
```

步骤二：打开 RTA 上 ICMP 的调试开关

```
<RTB>debugging ip icmp
```

步骤三：在 PCA 上 ping RTA，观察 RTB 调试信息输出

```
ping -n 10 192.168.0.1
```

在 RTA 上的 debugging 信息输出类似于：

```
*Sep 12 08:07:17:460 2008 RTB IPDBG/7/debug_icmp:
ICMP Receive: echo(Type=8, Code=0), Src = 192.168.0.10, Dst = 192.168.0.1

*Sep 12 08:07:17:460 2008 RTB IPDBG/7/debug_icmp:
ICMP Send: echo-reply(Type=0, Code=0), Src = 192.168.0.1, Dst = 192.168.0.10

*Sep 12 08:07:17:686 2008 RTB IPDBG/7/debug_icmp:
ICMP Receive: echo(Type=8, Code=0), Src = 192.168.0.10, Dst = 192.168.0.1

*Sep 12 08:07:17:686 2008 RTB IPDBG/7/debug_icmp:
ICMP Send: echo-reply(Type=0, Code=0), Src = 192.168.0.1, Dst = 192.168.0.10
```

步骤四：关闭调试开关

```
<RTA>undo debugging all
```

实验3 以太网基础

实验任务一：网线制作

本实验的主要任务是学员掌握网线的制作方法

步骤一：双绞线线序

双绞线由根有色导线绞合而成，按橙白、橙、绿白、蓝、蓝白、绿、棕白、棕顺时针排列，一次编号为：1、2、3、4、5、6、7、8

如果要制作直连网线，双绞线一端的线序为 1、2、3、4、5、6、7、8.那么另一端的线序应当为 1、2、3、4、5、6、7、8；如果要制作交叉网线，那么另一端的线序应当为 3、6、1、4、5、2、7、8

步骤二：制作直连网线并检测连通性

按照步骤一的直连网线的制作线序，制作一条直连网线。

制作完成后，使用电缆测试仪检测电缆的连通性，检测时将双绞线两端分别插入信号发射器和接收器，打开电源，只有同一条线的指示灯一起亮一起来的情况下，才能说明线缆连通性良好。

步骤三：制作交叉网线并检测连通性

按照步骤一的直连网线的制作线序，制作一条交叉网线。

制作完成后，使用电缆测试仪检测电缆的连通性。

实验任务二：配置以太网双工与速率

步骤一：建立物理连接并运行超级终端

将 PC（或终端）的串口通过标准 Console 电缆与交换机的 Console 口连接。电缆的 RJ-45 头一端连接交换机的 Console 口；9 针 RS-232 接口一端连接计算机的串行口。

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，请学员在用户视图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：查看端口双工与速率

按照组网图，将 PCA 与 SWA 的端口 E1/0/5 相连，连接后，在 SWA 上通过 display interface Ethernet 1/0/5 查看接口显示状态，根据该命令输出请补充如下的空格：

Ethernet1/0/5 current state: UP

IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-e23e-f9b0

Media type is twisted pair, Port hardware type is 100_BASE_TX

100Mbps-speed mode, full-duplex mode

Link speed type is autonegotiation, link duplex type is autonegotiation

从如上显示信息可以看到端口的状态、物理 MAC 地址、连接的线缆类型以及端口的双工与速率。

如上信息显示目前交换机默认情况下端口的双工与速率是自协商模式，协商的结果是：速率：100M，双工模式：全双工

步骤三：修改端口速率

在 SWA 上将端口 E1/0/5 的速率修改为 100M，请在如下的空格中填写完整的配置命令：

[SWA-Ethernet1/0/5]speed 100

修改完成后，再次通过命令 display interface Ethernet 1/0/5 查看端口 Ethernet1/0/5 的状态，根据该命令输出请补充如下的空格：

100Mbps-speed mode, full-duplex mode

Link speed type is force link, link duplex type is autonegotiation

从如上显示信息可以看到，虽然端口的速率仍然是 100M，但是速率模式已经是强制模式，而不是自协商模式，而此时双工的工作模式依然是自协商。

步骤四：修改端口双工模式

在 SWA 上将端口 E1/0/5 的的双工模式配置为全双工模式，请在如下的空格中填写完整的配置命令：

[SWA-Ethernet1/0/5]duplex full

修改完成后，再次通过命令 display interface Ethernet 1/0/5 查看端口 Ethernet1/0/5 的状态，根据该命令输出请补充如下的空格：

100Mbps-speed mode, full-duplex mode

Link speed type is force link, link duplex type is force link

从如上显示信息可以看到，端口虽然依然是全双工模式，但是其协商模式已经是强制模式，而不是自协商模式。

同时也可以看到，修改端口的双工模式不对端口的速率有影响。

步骤五：同时修改端口的速率与双工

在 SWA 上将端口 Ethernet1/0/5 的速率修改为 10M，双工模式修改为半双工，请在如下的空格中补充完整的配置命令：

[SWA-Ethernet1/0/5]speed 10

[SWA-Ethernet1/0/5]duplex half

修改完成后，再次通过命令 display interface Ethernet 1/0/5 查看端口 Ethernet1/0/5 的状态，根据该命令输出请补充如下的空格：

10Mbps-speed mode, half-duplex mode

Link speed type is force link, link duplex type is force link

步骤六：关闭端口

在 SWA 上通过在接口视图下执行 shutdown 命令可以将端口 Ethernet1/0/5 关闭，

配置完成后，再次通过命令 display interface Ethernet 1/0/5 查看端口 Ethernet1/0/5 的状态，根据该命令输出请补充如下的空格：

Ethernet1/0/5 current state: Administratively DOWN

10Mbps-speed mode, half-duplex mode

Link speed type is force link, link duplex type is force link

可以看到端口被关闭，但是步骤五配置的双工模式和速率模式没有改变。该命令只是影响了端口的物理状态。

可以通过在接口视图下配置 undo shutdown 命令将端口 Ethernet1/0/5 开启。

实验4 WLAN 基本配置

实验任务一：配置 AP 使终端设备可以接入

步骤一：创建服务模版

[WA2210-AG]wlan service-template　2　crypto

步骤二：命名 ssid 为 test

[WA2210-AG-wlan-st-2]ssid test

步骤三：使用 wep40 方式加密

[WA2210-AG-wlan-st-2]cipher-suite wep40

步骤四：设置 wep 的密钥为 12345

[WA2210-AG-wlan-st-2]wep default-key 1 wep40 pass-phrase 12345

步骤五：使能服务模版

[WA2210-AG-wlan-st-2]service-template enable

步骤六：创建 WLAN-BSS2

[WA2210-AG]int WLAN-BSS2

步骤七：进入 WLAN-Radio 1/0/2 接口

[WA2210-AG]int WLAN-Radio 1/0/2

步骤八：关联服务模版 2 和 wlan-bss 2

[WA2210-AG-WLAN-Radio1/0/2] service-template 2 interface wlan-bss 2

步骤九：保存配置

[WA2210-AG]save

步骤十：配置 DHCP SERVER

使能 DHCP

[H3C] dhcp enable

保留网关和 DNS 地址

[H3C] dhcp server forbidden-ip 192.168.0.1

[H3C] dhcp server forbidden-ip 192.168.0.2

创建 DHCP 地址池

[H3C] dhcp server ip-pool 1

指定地址段、指定网关、指定 DNS server

[H3C] network 192.168.0.0 mask 255.255.255.0

[H3C] gateway-list 192.168.0.1

[H3C] dns-list 192.168.0.2

进入路由器以太网接口

[H3C] interface Ethernet0/0

配置网关地址

[H3C- Ethernet0/0] ip address 192.168.0.1 255.255.255.0

步骤十一：配置无线客户端软件接入 AP

打开 windows 操作系统中的“无线网络联接”，选择 SSID 为 WEP 的无线连接，输入密码 12345 便可连上。


无线网络连接
网络任务
刷新网络列表
为家庭或小型办公室设置无线网络
相关任务
了解无线网
更改首选网
更改高级设
选择无线网络
单击以下列表中的项目以连接到区域内的无线网络或获得更多信息(W)。
BHC_TRAVEL
无线网络连接
网络“wep”要求网络密钥(也称作 WEP 密钥或 WPA 密钥)。网络密钥帮助阻止未知的入侵连接到此网络。
网络密钥(K):
*****
确认网络密钥(O):
*****
连接(C)
取消
信息。
reachel2620
启用安全的无线网络 (WPA2)
连接(C)

.....- 3 -

实验5 广域网接口和线缆

实验任务一：广域网接口线缆

步骤一：连接广域网接口线缆

通过 V.35 电缆将路由器 RTA 和 RTB 广域网接口 S1/0 实现互联，其中连接 RTA 的 V.35 电缆外接网络侧为 34 孔插座，而连接 RTB 的 V.35 电缆外接网络侧为 34 针插头（虽然通常只保留在用的针），由此可以得知路由器 RTB 的接口 S1/0 是 DTE 端，而路由器 RTA 的接口 S1/0 是 DCE 端

步骤二：查看广域网接口信息

在 RTA 上通过 display interface Serial 1/0 命令查看接口 Serial 1/0 的信息，根据其输出信息可以看到：

Physical layer is synchronous，Virtual Baudrate is 64000 bps

Interface is DCE, Cable type is V35

在 RTB 上通过 display interface Serial 1/0 命令查看接口 Serial 1/0 的信息，根据其输出信息可以看到：

Physical layer is synchronous，Baudrate is 64000 bps

Interface is DTE., Cable type is V35

由以上信息可以看到，RTA 和 RTB 的广域网 V.35 电缆接口工作在同步模式下，目前的传输速率是 64000 bps 或者 64K bps

步骤三：配置广域网接口参数

配置将 RTB 的接口 S1/0 的传输速率修改为 2Mbps，请在如下的空格中补充完整的配置命令：

[RTB-Serial1/0]baudrate 2048000

在 RTB 上执行该命令后，有信息提示：Serial1/0: Baudrate can only be set on the DCE，意思即为只能在 DCE 侧修改接口的波特率即传输速率

然后配置将 RTA 的接口 S1/0 的传输速率修改为 2Mbps，请在如下的空格中补充完整的配置命令：

[RTA-Serial1/0]baudrate 2048000

配置完成后通过 display interface Serial 1/0 命令查看接口 Serial1/0 的信息，根据其输出信息可以看到

Physical layer is asynchronous，Baudrate is 2048000 bps

在 RTA 的接口 Serial 1/0 下作如下配置：

[RTA-Serial1/0]physical-mode async

如上配置命令的含义是配置该物理接口工作在异步方式下

一般情况下，V.35 电缆一般只用于同步方式传输数据。

实验6 HDLC

本实验中的 PC 以及路由器的 IP 地址规划如表 6-1所示。

表6-1 IP 地址规划

设备	接口	IP 地址/掩码	备注
RTA	S1/0	10.1.1.1/30	
RTB	S1/0	10.1.1.2/30	

实验任务一：通过 HDLC 协议实现 RTA 与 RTB 广域网互通

步骤一：运行超级终端并初始化路由器配置

将 PC（或终端）的串口通过标准 Console 电缆与交换机的 Console 口连接。电缆的 RJ-45 头一端连接路由器的 Console 口；9 针 RS-232 接口一端连接计算机的串行口。

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，请学员在用户视图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：依据规划建立两台路由器之间的物理连接

将两台路由器的 S1/0 接口通过 V35 电缆连接，然后在 RTA 上执行命令 display interface serial1/0，根据其输出信息可以看到：

```
Serial1/0 current state: up Line protocol current state:up
Link layer protocol is ppp
```

在 RTB 上执行同样的命令并查看如上信息

注意：

如果 Line protocol 的状态是 DOWN，此时要检查物理电缆的状态，比如插头是否插牢，线缆的针脚是否有脱落等

步骤三：配置路由器广域网上封装 HDLC 协议

在 RTA 上配置广域网接口 S1/0 封装 HDLC 协议，请补充完整的配置命令：

```
[RTA]interface Serial 1/0
[RTA-Serial1/0]link-protocol hdlc
```

在 RTB 上完成广域网接口 HDLC 协议封装的配置

然后在 RTA 上执行命令 display interface serial1/0，根据其输出信息可以看到：

Serial1/0 current state: up　Line protocol current state: up

Link layer protocol is hdlc

在 RTB 上执行同样的命令并查看如上信息

步骤四：配置路由器广域网接口 IP 地址

在 RTA 上配置广域网接口 S1/0 的 IP 地址。请补充完整的配置命令：

```
[RTA]interface Serial 1/0
[RTA-Serial1/0]ip address 10.1.1.1 30 或 10.1.1.1 255.255.255.252
```

在 RTB 上也完整广域网接口 IP 地址配置

在 RTA 的 S1/0 接口模式视图下，执行命令 display this,可以看到

```
interface Serial1/0
 link-protocol hdlc
 ip address 10.1.1.1 255.255.255.252
```

,根据此信息检查并核实配置的正确性。

在 RTB 的 S1/0 接口模式下，执行同样的命令并查看核实配置的正确性。

步骤五：检查路由器广域网之间的互通性

在 RTA 上通过 ping 命令检查 RTA 与 RTB 广域网之间的互通性，其结果是：可以互通

实验7 PPP

实验任务一：PPP 协议基本配置

步骤一：运行超级终端并初始化路由器配置

将 PC（或终端）的串口通过标准 Console 电缆与交换机的 Console 口连接。电缆的 RJ-45 头一端连接路由器的 Console 口；9 针 RS-232 接口一端连接计算机的串行口。

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，请学员在用户视图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：依据规划建立两台路由器之间的物理连接

将两台路由器的 S1/0 接口通过 V35 电缆连接，然后在 RTA 上执行命令 display interface serial1/0，根据其输出信息可以看到：

Serial1/0 current state：up Line protocol current state：up

Link layer protocol is：ppp

在 RTB 上执行同样的命令并查看如上信息

通过如上输出信息可以得知，路由器串口默认的链路层封装协议是 ppp

步骤三：配置路由器广域网接口 IP 地址

在 RTA 上配置广域网接口 S1/0 的 IP 地址。请补充完整的配置命令：

```
[RTA]interface Serial 1/0
[RTA-Serial1/0]ip address 10.1.1.1 30 或者 ip address 10.1.1.1 255.255.255.252
```

在 RTB 上也完成广域网接口 IP 地址配置

在 RTA 的 S1/0 接口模式下，执行命令 display this,可以看到：

```
interface Serial1/0
 link-protocol ppp
 ip address 10.1.1.2 255.255.255.252 
```

,根据此信息检查并核实配置的正确性。

在 RTB 的 S1/0 接口模式下，执行同样的命令并查看核实配置的正确性

在 RTA 路由器上执行命令 display interface serial1/0，根据其输出信息可以看到：

```
Serial1/0 current state：up Line protocol current state：up
Link layer protocol is ppp
LCP opened, IPCP opened
```

步骤四：检查路由器广域网之间的互通性

在 RTA 上通过 ping 命令检查 RTA 与 RTB 广域网之间的互通性，其结果是：可以互通

实验任务二：PPP PAP 认证配置

在开始实验前，将路由器配置恢复到默认状态。

步骤一：配置路由器广域网接口 IP 地址并确认互通性

依据本实验 IP 地址规划表，在 RTA 和 RTB 上配置广域网接口的 IP 地址

从实验任务一得知,MSR 路由器广域网接口默认的链路层封装协议是 ppp。因此只要在广域网接口配置正确的 IP 地址后，RTA 与 RTB 的广域网接口之间是能 ping 通的

步骤二：在 RTA 上配置以 PAP 方式验证对端 RTB

RTA 为主验证方验证 RTB，那么首先要在系统视图下配置将对端 RTB 的用户名和密码加入本地用户列表并设置用户的服务类型，请在 RTA 上完成添加对端用户名 rtb，密码 pwdpwd 到本地用户列表，在如下空格中填写完整的命令：

```
[RTA] local-user rtb
[RTA-luser-rtb] service-type ppp
[RTA-luser-rtb] password simple  pwdpwd
```

其次在接口视图下设置本地验证对端 RTB 的方式为 PAP，请在如下空格中填写完整的命令：

```
[RTA- Serial1/0] ppp authentication-mode pap
```

步骤三：查看接口状态并验证互通性

在 RTA 上执行命令 display interface serial 1/0，根据输出信息可以看到：

```
Serial1/0 current state：up  Line protocol current state：down
Link layer protocol is ppp
LCP closed
```

在 RTA 上 ping RTB 广域网接口地址，其结果为 不通，返回 Request time out

步骤四：配置 RTB 为被验证方

在 RTB 上配置本地被对端 RTA 以 PAP 方式验证时发送的 PAP 用户名（rtb）和密码（pwdpwd），该配置需要在接口视图下完成，请在下面的空格中填写完整的命令：

```
[RTB- Serial1/0] ppp pap local-user rtb password simple pwdpwd
```

步骤五：查看接口状态以及验证 RTA 与 RTB 的互通性

在 RTA 上执行命令 display interface serial 1/0，根据输出信息可以看到：

```
Serial1/0 current state: up  Line protocol current state: up
Link layer protocol is ppp
LCP opened，IPCP opened
```

在 RTB 上完成同样的信息查看

在 RTA 上 ping RTB 广域网接口地址，结果是：可以互通

实验任务三：PPP CHAP 认证配置

在开始实验前，将路由器配置恢复到默认状态。

步骤一：配置路由器广域网接口 IP 地址并确认互通性

依据本实验 IP 地址规划表，在 RTA 和 RTB 上配置广域网接口的 IP 地址

从实验一得知,MSR 路由器广域网接口默认的链路层封装协议是 ppp。因此只要在广域网接口配置正确的 IP 地址后，RTA 与 RTB 的广域网接口之间是能 ping 通的

步骤二：在 RTA 上配置以 CHAP 方式验证对端 RTB

RTA 为主验证方验证 RTB，那么在 RTA 上完成了如下配置：

```
[RTA] local-user rtb
[RTA-luser-user2] password simple pwdpwd
[RTA-luser-user2] service-type ppp
```

如上配置的含义是:将对端 RTB 的用户名和密码加入本地用户列表并设置用户的服务类型

其次在接口视图下设置本地验证对端 RTB 的方式为 CHAP，请在如下空格中填写完整的命令：

```
[RTA-Serial1/0] ppp authentication-mode chap
```

步骤三：查看接口状态并验证互通性

在 RTA 上执行命令 display interface serial 1/0，根据输出信息可以看到：

```
Serial1/0 current state：up  Line protocol current state： down
Link layer protocol is ppp
LCP closed
```

在 RTA 上 ping RTB 广域网接口地址，其结果为 不通，返回 Request time out

步骤四：配置 RTB 为被验证方

在 RTB 上配置如下命令：

```
[RTB-Serial1/0] ppp chap user rtb
```

该配置命令的含义是：配置本地用户名，该用户名是发送到对端惊醒 CHAP 验证使用的用户名

```
[RTB-Serial1/0] ppp chap password simple pwdpwd
```

该配置命令的含义是配置默认的 CHAP 密码，在进行 CHAP 验证的时候使用此密码

步骤五：查看接口状态以及验证 RTA 与 RTB 的互通性

在 RTA 上执行命令 display interface serial 1/0，根据输出信息可以看到：

```
Serial1/0 current state：up  Line protocol current state：up
Link layer protocol is ppp
LCP opened，IPCP opened
```

在 RTB 上完成同样的信息查看

在 RTA 上 ping RTB 广域网接口地址，结果是：可以互通

实验任务四：PPP MP 配置

在开始实验前，将路由器配置恢复到默认状态。

步骤一：依据要求，使用两对 V.35 电缆分别连接 RTA 和 RTB

步骤二：在 RTA 和 RTB 上创建 Mp-group 接口并配置 IP 地址

分别在 RTA 和 RTB 上创建 Mp-group 接口，并配置相应的 IP 地址。

在 RTA 上配置如下：

```
[RTA] interface mp-group 1
```

在该命令中，数字 1 的含义是表示 MP-group 接口的编号是 1

```
[RTA-Mp-group1] ip address 10.1.1.1 30
```

在 RTB 上完成类似的配置，只是 iP 地址为 10.1.1.2。

步骤三：在 RTA 和 RTB 上将相应物理接口加入 Mp-group 接口

分别在 RTA 和 RTB 上将相应的物理接口加入到 Mp-group 接口中，并将相应的物理接口封装 PPP 协议。

在 RTA 上配置如下，请在空格处补全配置：

```
[RTA] interface serial 1/0
[RTA-Serial1/0] link-protocol ppp
[RTA-Serial1/0] ppp mp mp-group 1
[RTA] interface serial 2/0
[RTA-Serial2/0] link-protocol ppp
[RTA-Serial2/0] ppp mp mp-group 1
```

在 RTB 上完成如上同样的配置。

步骤四： 验证并查看 MP 效果

在 RTA 上执行命令 display ppp mp，根据其输出信息可以看到：

```
The member channels bundled are:_
Serial1/0              Up-Time:2009/06/10  08:07:14:496
Serial2/0              Up-Time:2009/06/10  08:07:14:497
```

在 RTA 上执行命令 display interface Mp-group 1，根据其输出信息可以看到：

```
Mp-group1 current state: up  Line protocol current state: up
Link layer protocol is ppp
LCP opened, MP opened, IPCP opened
```

在 RTA 上 ping RTB 上的 MP 接口 ip 地址，其结果为：可以互通

实验8 帧中继

实验任务一：帧中继物理接口静态映射互通配置

实验任务一中的 PC 以及路由器的 IP 地址规划如表 8-1所示。

表8-1 实验任务一 IP 地址规划

设备	接口	IP 地址/掩码	本地 DLCI
RTA	S1/0	10.1.1.1/24	30、40
RTB	S1/0	10.1.1.2/24	70
RTC	S1/0	10.1.1.3/24	80

步骤一：运行超级终端并初始化路由器配置

将 PC（或终端）的串口通过标准 Console 电缆与路由器的 Console 口连接。电缆的 RJ-45 头一端连接路由器的 Console 口；9 针 RS-232 接口一端连接计算机的串行口。

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，请学员在用户视图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：依据规划，配置相关的 IP 地址

依据表 8-1规划的 IP 地址，为路由器的接口配置 IP 地址。

步骤三：配置广域网接口封装

在 RTA 上做如下配置:

[RTA-Serial1/0] link-protocol fr ietf，该命令的含义是封装接口的链路层协议为帧中继，命令中 IETF 的含义是选择 IETF 标准（ietf）格式进行帧中继封装

在 RTB、RTC 上完成同样的配置

步骤四：配置 RTA 上帧中继相关参数

在 RTA 的 Serial 1/0 接口上配置如下：

[RTA-Serial1/0] fr interface-type dte

该命令的含义是 配置帧中继接口类型是 DTE

[RTA-Serial1/0] fr lmi type Q933a

该命令的含义是 配置帧中继接口的 LMI 协议类型为 Q933a

[RTA-Serial1/0] fr map ip 10.1.1.2 30

[RTA-Serial1/0] fr map ip 10.1.1.3 40

请在空格处补充完整的配置并说明该配置命令的含义

配置帧中继的地址映射，其中 IP 地址是对端的 IP 地址，DLCI 是本地虚电路号

[RTA-Serial1/0] ip address 10.1.1.1 24

步骤五：配置 RTB、RTC 上帧中继相关参数

请在如下空格处补充完全 RTB 上帧中继相关的配置：

```
[RTB-Serial1/0] fr interface-type dte
[RTB-Serial1/0] fr lmi type Q933a
[RTB-Serial1/0] fr map ip 10.1.1.1 70
[RTB-Serial1/0] ip address 10.1.1.2 24
```

请在如下空格处填写完整的 RTC 上帧中继相关的配置：

```
[RTC-Serial1/0] fr interface-type dte
[RTC-Serial1/0] fr lmi type Q933a
[RTC-Serial1/0] fr map ip 10.1.1.1 80
[RTC-Serial1/0] ip address 10.1.1.3 24
```

步骤六：配置路由器模拟帧中继交换机

配置路由器 FR-Switch 实现帧中继交换机功能：

```
[fr switch]fr switching   //启用帧中继交换机功能

[fr switch]interface s6/0                //连接 RTA
[fr switch-Serial6/0]link-protocol fr
[fr switch-Serial6/0]fr interface-type dce
[fr switch-Serial6/0]fr dlci 30
[fr switch-fr-dlci-Serial6/0-30]quit
[fr switch-Serial6/0]fr dlci 40
[fr switch-fr-dlci-Serial6/0-40]quit

[fr switch]interface s5/0                //连接 RTB
[fr switch-Serial5/0]link-protocol fr
[fr switch-Serial5/0]fr interface-type dce
[fr switch-Serial5/0]fr dlci 70
[fr switch-fr-dlci-Serial5/0-70]quit

[fr switch]interface s5/1                //连接 RTC
[fr switch-Serial5/1]link-protocol fr
[fr switch-Serial5/1]fr interface-type dce
[fr switch-Serial5/1]fr dlci 80
[fr switch-fr-dlci-Serial5/0-80]quit

[fr switch]fr switch a-b interface Serial6/0 dlci 30 interface Serial5/0 dlci 70
[fr switch-fr-switching-a-b]quit
[fr switch]fr switch a-c interface Serial6/0 dlci 40 interface Serial5/1 dlci 80
[fr switch-fr-switching-a-c]quit
```

检测帧中继交换机配置是否成功：

```
<fr switch>display fr switch-table all
Total PVC switch records:2
PVC-Name                  Status   Interface(Dlci) <-----> Interface(Dlci)
a-b                      Active   Serial6/0(30)         Serial5/0(70)
a-c                      Active   Serial6/0(40)         Serial5/1(80)
```

发现两个通道都已经 active，通道配置成功。

步骤七：查看验证接口配置的正确性

在 RTA 上执行命令 display fr map-info，根据该其输出信息可以看到：

DLCI = 30, IP 10.1.1.2, Serial1/0　　status = active

DLCI = 40, IP 10.1.1.3, Serial1/0　　status = active

在 RTB、RTC 上执行同样的命令查看相关信息

在 RTA 上执行命令 display fr lmi-info，根据其输出信息可以看到：

out status enquiry = 243, in status = 243

30 秒之后，在 RTA 上重复执行命令 display fr lmi-info，根据其输出信息可以看到

out status enquiry 数值 增加 (增加/减少)，in status 数值 增加（增加/减少）

在 RTB、RTC 上完成同样如上的操作

注意：

步骤八中 out status enquiry 显示的数值只作为参考，具体数值以实验室的执行命令 display fr lmi-info 后的显示值为准。

步骤八：验证互通性

在 RTA 上 ping RTB、RTC 的 S1/0 接口 IP 地址，其结果是 可以互通

实验任务二：帧中继子接口静态映射互通配置

实验任务二中的 PC 以及路由器的 IP 地址规划如表 8-2所示。

表8-2 实验任务二 IP 地址规划

设备	接口	IP 地址/掩码	本地 DLCI
RTA	S1/0.1	10.1.1.1/30	30
	S1/0.2	10.1.2.1/30	40

RTB	S1/0	10.1.1.2/30	70
RTC	S1/0	10.1.2.2/30	80

步骤一：运行超级终端并初始化路由器配置

将 PC（或终端）的串口通过标准 Console 电缆与交换机的 Console 口连接。电缆的 RJ-45 头一端连接路由器的 Console 口；9 针 RS-232 接口一端连接计算机的串行口。

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，请学员在用户视图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：依据规划，配置相关的 IP 地址

依据表 8-2规划的 IP 地址，为路由器的接口配置 IP 地址。

步骤三：配置路由器上帧中继相关参数

实现帧中继协议的封装标准为 IEF 格式，帧中继接口的终端类型为 DTE，接口的 LMI 类型为 Q933a，请在 RTA 接口 S1/0 上完成满足如上要求的配置：

```
[RTA] interface serial 1/0
[RTA-Serial1/0] link-protocol fr ietf.
[RTA-Serial1/0] fr interface-type dte
[RTA-Serial1/0] fr lmi type Q933a
```

在 RTB、RTC 的接口 S1/0 上完成同样的配置

步骤四：为 RTA 建立子接口，并配置子接口上的帧中继相关参数

在 RTA 上建立子接口，请在如下空格处补充完整的命令

[RTA]interface Serial 1/0.1 p2p

该命令中 P2P 的含义是定义帧中继点到点类型子接口

[RTA-Serial0/0.1]ip address 10.1.1.1 30

[RTA-Serial0/0.1]fr dlci 30

[RTA]interface Serial 1/0.2 p2p

[RTA-Serial0/0.1]ip address 10.1.2.1 30

[RTA-Serial0/0.1]fr dlci 40

步骤五：配置 RTB、RTC 接口上的帧中继相关信息

在 RTB 上配置帧中继子接口，请补充空格中完整的命令：

interface Serial1/0.1 p2p

fr dlci 70

ip address 10.1.1.2 255.255.255.252

请在如下的空格中完成 RTC 上帧中继子接口的配置：

interface Serial 1/0.1 p2p

fr dlci 80

ip address 10.1.2.2 255.255.255.252

步骤六：配置路由器模拟帧中继交换机

本步骤中 FR-Switch 的配置与实验任务一相同，保留其配置不变即可。

步骤七：查看 RTA 子接口上的相关信息

在 RTA 上执行命令 display fr map-info，根据该其输出信息可以看到：

DLCI 30, Point-to-Point DLCI, Serial1/0.1, status = active

DLCI 40, Point-to-Point DLCI, Serial1/0.2, status = active

在 RTB、RTC 上执行同样的命令查看相关信息

在 RTA 上执行命令 display fr lmi-info，根据其输出信息可以看到：

out status enquiry = 451, in status = 451

30 秒之后，在 RTA 上重复执行命令 display fr lmi-info，根据其输出信息可以看到

out status enquiry 数值 增加 (增加/减少)，in status 数值 增加（增加/减少）

在 RTB、RTC 上完成同样如上的操作

步骤八：验证互通性

在 RTA 上 ping RTB、RTC 的 S1/0.1 接口 IP 地址，其结果是 可以互通

实验9 IP 基础

实验任务一：基本的 IP 网段内通信

步骤一：划分 IP 子网

本实验中给定的一个 C 类网段地址 192.168.1.0.该地址段有 8 个地址位，一共有 256 个 ip 地址，其网络地址是 192.168.1.0，广播地址是 192.168.1.255，一共有 254 个可用主机地址

现在要求将该网段地址划分子网实现每个网段内可用的主机地址数是 25，请在下面的空格中写出最佳的子网划分结果（包括网段和掩码）：

IP：192.168.1.0　掩码：255.255.255.224

IP：192.168.1.32　掩码：255.255.255.224

IP：192.168.1.64　掩码：255.255.255.224

IP：192.168.1.96　掩码：255.255.255.224

IP：192.168.1.128　掩码：255.255.255.224

IP：192.168.1.160　掩码：255.255.255.224

IP：192.168.1.192　掩码：255.255.255.224

IP：192.168.1.224　掩码：255.255.255.224

步骤二：配置 IP 地址

在 PCA 上配置其 IP 地址为 192.168.1.10/255.255.255.240，在 RTA 的 G0/0 接口上配置 IP 地址为 192.168.1.19/255.255.255.240。

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，根据其输出信息回答下面的问题：

PCA 的显示结果是：

IP Address192.168.1.10; Subnet　Mask 255.255.255.240;

Default Gateway 空，没有

在 RTA 上通过 display interface GigabitEthernet 0/0 命令可以查看接口 G0/0 的信息，根据其输出信息可以看到 Internet Address is192.168.1.19 Primary

步骤三：验证相同 IP 网段内通信

在 PCA 上通过 ping 命令检测 PCA 与 RTA 之间的互通，其结果是不能 ping 通 RTA 的 G0/0 接口地址，ping 结果返回信息 Destination host unreachable

产生这种情况的原因是 PCA 与 RTA G0/0 接口直连但是 PCA 与 RTA 接口 G0/0 的 IP 地址不在一个网段，因此无法互通

在不修改 PCA 的 IP 地址以及掩码情况下，修改 RTA 的 G0/0 接口地址为：192.168.1.16/28，该地址中数字 28 的含义是掩码是 28 位，即 255.255.255.240，在 RTA 的 G0/0 接口下不能成功的配置该 IP 地址，产生这种情况的原因是 192.168.1.16/28 是网络地址，不可用

要解决该问题，在不修改 PCA 的 IP 地址以及掩码的情况下，RTA 的 G0/0 接口 ip 地址可以配置范围是 192.168.1.1~192.168.1.9；192.168.1.11~192.168.1.14 掩码：255.255.255.240

步骤四：配置网关

配置 RTA 上接口 G0/1 的 ip 地址为 2.2.2.1/30，要确保 PCB 与 G0/1 能够互通，那么 PCB 的 IP 地址应该配置为 2.2.2.2/30

配置完成后，在 PCA 上 ping RTA 接口 G0/1 的地址 2.2.2.1，其结果是无法互通

产生这种结果的原因是 PCA 上没有配置网关，不能通过网关实现跨网段路由

保持步骤二中配置的 PCA 的 IP 地址不变，配置 RTA 的 G0/0 接口的 IP 地址为 192.168.1.1/28，那么要实现 PCA 可以和 RTA 接口 G0/1 互通，那么 PCA 的网关地址应该配置为 192.168.1.1

配置完成后，在 PCA 上 ping RTA 接口 G0/1 的地址 2.2.2.1，其结果是可以互通

由此可以理解，PC 上网关的含义是相当于一个中转器，所有发往与自己不同网段的 IP 数据包都会被发送给网关，由网关来完成数据包的下一步转发

步骤五：验证不同网段 IP 互通

完成步骤四后，在 PCA 上 ping PCB,其结果是无法 ping 通

要解决该问题，需要给 PCB 配置网关地址 2.2.2.1

按照上述解决办法完成配置修改后，在 PCA 上再次 ping PCB， 其结果是可以 ping 通

实验10 ARP

实验任务一：ARP 表项观察

步骤一：运行超级终端并初始化路由器配置

将 PC（或终端）的串口通过标准 Console 电缆与路由器的 Console 口连接。电缆的 RJ-45 头一端连接路由器的 Console 口；9 针 RS-232 接口一端连接计算机的串行口。

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，请学员在用户视图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10-1 IP 地址列表

设备名称	接口	IP 地址
PCA	--	172.16.0.1/24
PCB	--	172.16.1.1/24
RTA	G0/0	172.16.0.254/24
RTA	G0/1	172.16.1.254/24

据表 10-1所示在 PC 上配置 IP 地址和掩码。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，根据其输出信息回答下面的问题：

PCA 的显示结果是：

IP Address 172.16.0.1 ; Subnet Mask 255.255.255.0 ;

Default Gateway 空

PCB 的显示结果是：

IP Address 172.16.1.1 ; Subnet Mask 255.255.255.0;

Default Gateway 空

然后在 RTA 的接口上配置 IP 地址及掩码，请在下面的空格中补充完整的命令：

[RTA]interface GigabitEthernet0/0

[RTA-GigabitEthernet0/0] ip address 172.16.0.254 24

[RTA]interface GigabitEthernet0/1

[RTA-GigabitEthernet0/1] ip address 172.16.1.254 24

步骤三：查看 ARP 信息

在 RTA 上执行执行命令 display interface GigabitEthernet 0/0，根据该命令的输出信息，填写如下空格：

Internet Address is 172.16.0.254/24 Primary

IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-e2d1-bf50

在 RTA 上执行命令 display interface GigabitEthernet 0/1，根据该命令的输出信息，填写如下空格：

Internet Address is 172.16.1.254/24 Primary

IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-e2d1-bf51

在 PC 的“命令提示符”窗口下，键入命令 ipconfig /all 来查看 PC 的接口 MAC 与 IP 地址

根据该命令的输出信息，请填写如下空格 PC 的 MAC 地址

PCA： Physical Address. . . . . : 00-1C-23-3D-56-95

PCB： Physical Address. . . . . : 00-13-72-8E-47-51

根据以上信息，我们做一张表，表的内容是 PC 及 RTA 的 IP 地址与 MAC 地址对应关系，请补充表中空格处的 MAC 地址如下所示：

表10-2 IP 地址与 MAC 地址对应关系列表

设备名称	接口	IP 地址	MAC 地址
PCA	--	172.16.0.1/24	00-1C-23-3D-56-95
PCB	--	172.16.1.1/24	00-13-72-8E-47-51
RTA	G0/0	172.16.0.254/24	000f-e2d1-bf50
RTA	G0/1	172.16.1.254/24	000f-e2d1-bf51

然后，分别在 PCA 和 PCB 的“命令提示符”窗口下用 ping 命令来测试 PC 到 RTA 的可达性，以使 PC 及 RTA 建立 ARP 表项。

测试完成后，分别在 PCA、PCB 和 RTA 上查看 ARP 表项信息，分别在 PCA 和 PCB 的“命令提示符”窗口下用 arp –a 来查看 ARP 表象信息，根据该命令的输出信息，请填写如下的空格：

PCA 的输出信息：

Internet Address	Physical Address	Type
172.16.0.254	000f-e2d1-bf50	dynamic

PCB 的输出信息：

Internet Address	Physical Address	Type
172.16.1.254	000f-e2d1-bf51	dynamic

在 RTA 上可以在任何视图下执行 display arp all 命令查看路由器所有的 ARP 表项，请执行该命令并根据其输出信息补充如下的空格：

IP Address	MAC Address	VLAN ID	Interface	Aging	Type
172.16.0.1	001c-233d-5695	N/A	GE0/0	13	D
172.16.1.1	0013-728e-4751	N/A	GE0/1	15	D

如上输出信息中，type 字段的含义是 ARP 表项类型：动态，用 D 表示；静态，用 S 表示；授权，用 A 表示;

Aging 字段的含义是动态 ARP 表项的老化时间。

把我们所做的表 1-2 与 PC 及 RTA 上的 ARP 表项对比一下。可知，PC 及 RTA 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。

注意:

学员实验过程中所显示的 MAC 地址与本指导手册中的不同，是正常现象。

实验任务二：ARP 代理配置

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

步骤一：运行超级终端并初始化路由器配置

将 PC（或终端）的串口通过标准 Console 电缆与路由器的 Console 口连接。电缆的 RJ-45 头一端连接路由器的 Console 口；9 针 RS-232 接口一端连接计算机的串行口。

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，请学员在用户视图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10-3 IP 地址列表

设备名称	接口	IP 地址
PCA	--	172.16.0.1/16
PCB	--	172.16.1.1/16
RTA	G0/0	172.16.0.254/24

RTA	G0/1	172.16.1.254/24

根据上表所示在 PC 上配置 IP 地址和掩码。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。根据其输出信息回答下面的问题：

PCA 的显示结果是：

IP Address172.16.0.1; Subnet Mask 255.255.0.0;

Default Gateway 空

PCB 的显示结果是：

IP Address172.16.1.1; Subnet Mask 255.255.0.0;

Default Gateway 空

然后在 RTA 的接口上配置 IP 地址及掩码，请在下面的空格中补充完整的命令：

[RTA]interface GigabitEthernet0/0

[RTA-GigabitEthernet0/0] ip address 172.16.0.254 24

[RTA]interface GigabitEthernet0/1

[RTA-GigabitEthernet0/1] ip address 172.16.1.254 24

步骤三：配置 ARP 代理

在 PCA 和 PCB 上通过 ping 来检测他们之间是否可达，检测的结果是不能互通

导致这种结果的原因是因为尽管 PCA 和 PCB 处于同一个子网内（掩码都是 255.255.0.0），但 RTA 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），所以它不会在两个不同子网之间转发 ARP 报文

在 RTA 上配置 ARP 代理，请在下面的空格处补充完整的命令

[RTA]interface GigabitEthernet0/0

[RTA-GigabitEthernet0/0] proxy-arp enable

[RTA]interface GigabitEthernet0/1

[RTA-GigabitEthernet0/1] proxy-arp enable

配置完成后，在 PCA 上用 ping 命令测试到 PCB 得可达性，其结果是 可以互通

步骤四：查看 ARP 信息

在 PCA 上查看 ARP 表项，根据其输出信息补充如下的空格

Internet Address	Physical Address	Type
172.16.1.1	000f-e2d1-bf50	dynamic

ARP 表项中 PCB 的 IP 地址对应的 MAC 地址与 RTA 接口 G0/0 的 MAC 地址相同,由此可以看出，是 RTA 的接口 G0/0 接口执行了 ARP 代理功能，为 PCA 发出的 ARP 请求提供了代理应答。

在 PCB 上查看 ARP 表项,可以看到 ARP 表项中 PCA 的 IP 地址对应的 MAC 地址与 RTA 的接口 G0/1 的 MAC 地址相同

在 RTA 上通过可以通过 display arp all 命令查看 ARP 表项，其输出结果与实验一的结果一样

实验11 DHCP

实验任务一：PCA 直接通过 RTA 获得 IP 地址

步骤一：建立物理连接并初始化路由器配置

按实验组网图进行物理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，请学员在用户视图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

在如下空格中补充完整命令，配置 RTA 接口 G0/0 IP 地址为 172.16.0.1/24

[RTA-GigabitEthernet0/0] ip address 172.16.0.1 24

交换机 S3610 采用出厂默认配置，不做任何配置，在这种情况下，交换机所有的端口都属于 VLAN 1

步骤三：配置 RTA 作为 DHCP 服务器

配置 RTA 为 DHCP 服务器，给远端的 PCA 分配 IP 网段为 172.16.0.0/24 的地址。请补充下面空格中缺省的命令：

配置 RTA：

[RTA] dhcp enable 启动 DHCP 服务

[RTA]dhcp server forbidden-ip 172.16.0.1

如上配置命令的含义是配置 DHCP 地址池中不参与自动分配的 IP 地址，也即，172.16.0.1 不参与地址分配

[RTA]dhcp server ip-pool 1

如上命令中数值 1 的含义是：DHCP 地址池名称，是地址池的唯一标识

[RTA-dhcp-pool-pool1]network 172.16.0.0 mask 255.255.255.0

[RTA-dhcp-pool-pool1]gateway-list 172.16.0.1

配置完成后，通过 display current-configuration 命令查看配置的正确性

步骤四：PCA 通过 DHCP 服务器获得 IP 地址

在 Windows 操作系统的“控制面板”中选择“网络和 Internet 连接”，选取“网络连接”中的“本地连接”，点击【属性】，在弹出的窗口中选择“Internet 协议（TCP/IP）”，点击【属性】，出现界面如下：

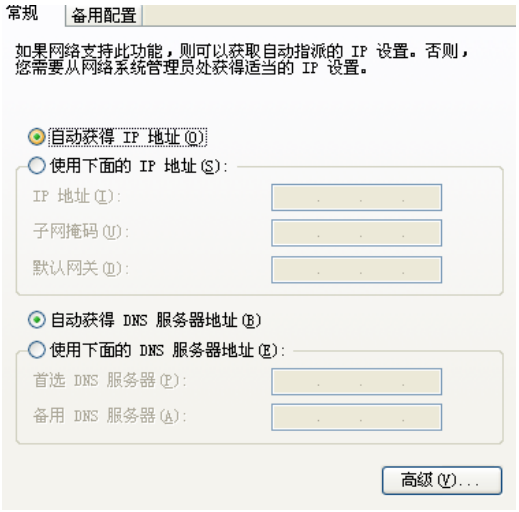


图11-1 Internet 协议（TCP/IP）属性

如图 11-1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 PCA 配置为 DHCP 客户端。在 PCA 的“命令提示符”窗口下，键入命令 ipconfig 来验证 PCA 能否获得 IP 地址和网关等信息。其输出的显示结果是：

IP Address 172.16.0.2; Subnet Mask 255.255.255.0;

Default Gateway 172.16.0.1

如果无法获得 IP，请检查线缆连接是否正确，然后在“命令提示符”窗口下用 ipconfig /renew 命令来使 PCA 重新发起 DHCP 请求。

步骤五：查看 DHCP 服务器相关信息

在 RTA 上用 display dhcp server forbidden-ip 命令来查看 DHCP 服务器禁止分配的 IP 地址，执行该命令根据其输出信息可以看到 172.16.0.1 地址被服务器禁止分配。

在 RTA 上用 display dhcp server free-ip 来查看 DHCP 服务器可供分配的 IP 地址资源

在 RTA 上用 display dhcp server ip-in-use all 来查看 DHCP 地址池的地址绑定信息，执行该命令，根据其输出信息可以看到 PCA 的 MAC 地址绑定的 IP 地址为 172.16.0.2

实验任务二：PCA 通过 DHCP 中继方式获得 IP 地址

步骤一：建立物理连接并初始化路由器配置

按实验组网图进行物理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，请学员在用户视图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11-1 设备 IP 地址列表

设备名称	物理接口	IP 地址	
RTB	G0/0	172.16.1.1/24	
	G0/1	172.16.0.1/24	
RTA	G0/0	172.16.0.2/24	

按表 11-1所示在路由器上配置 IP 地址。

在 RTB 上配置 IP 地址：

```
[RTB-GigabitEthernet0/0]ip address 172.16.1.1 24
[RTB-GigabitEthernet0/1]ip address 172.16.0.1 24
```

在 RTB 上配置缺省路由，下一跳指向 RTA：

```
[RTB]ip route-static 0.0.0.0 0 172.16.0.2
```

在 RTA 上配置接口 IP 及静态路由：

```
[RTA-GigabitEthernet0/0]ip address 172.16.0.2 24
[RTA]ip route-static 172.16.1.0 24 172.16.0.1
```

步骤三：在 RTA 上配置 DHCP 服务器及在 SWA 上配置 DHCP 中继

配置 RTA 为 DHCP 服务器，给远端的 PCA 分配 IP 网段为 172.16.1.0/24 的地址，在如下的空格中补充完整的配置命令：

[RTA] dhcp enable

[RTA]dhcp server forbidden-ip 172.16.1.1

[RTA]dhcp server ip-pool pool1

[RTA-dhcp-pool-pool1]network 172.16.1.0 mask 255.255.255.0

[RTA-dhcp-pool-pool1]gateway-list 172.16.1.1

配置 RTB 提供 DHCP Relay 服务，请在如下的空格中补充完整的配置命令

[RTB] dhcp enable 启动 DHCP 服务

[RTB]dhcp relay server-group 1 ip 172.16.0.2

如上命令中，数字 1 的含义是 DHCP 服务器组号是 1

[RTB]interface GigabitEthernet0/0

[RTB-GigabitEthernet0/0]dhcp select relay

[RTB-GigabitEthernet0/0]dhcp relay server-select 1

步骤四：PCA 通过 DHCP 中继获取 IP 地址

断开 PCA 与 RTA 之间的连接电缆，再接上，以使 PCA 重新发起 DHCP 请求。

完成重新获取地址后，在 PCA 的“命令提示符”窗口下，键入命令 ipconfig 来验证 PCA 能否获得 IP 地址和网关等信息，其输出信息显示为：

IP Address 172.16.1.2; Subnet Mask 255.255.255.0;

Default Gateway 172.16.1.1

步骤五：查看 DHCP 中继相关信息

在 RTA 上通过命令 display dhcp relay server-group 1 查看 DHCP 中继服务器组的信息，

通过命令 display dhcp relay interface GigabitEthernet0/0 查看接口对应的 DHCP 中继服务器组信息

实验12 IPv6 基础

实验任务一：IPv6 地址配置及查看

步骤一：建立物理连接

按照拓扑进行连接，并检查路由器的软件版本及配置信息，确保路由器软件版本符合要求，所有配置为初始状态。如果配置不符合要求，请读者在用户模式下擦除设备中的配置文件，然后重启路由器以使系统采用缺省的配置参数进行初始化。

以上步骤可能会用到以下命令：

```
<RTA> display version
<RTA> reset saved-configuration
<RTA> reboot
```

步骤二：配置接口自动生成链路本地地址及测试可达性，查看邻居信息

请在路由器 RTA 和 RTB 的系统视图下，使能路由器的 IPv6 报文转发功能，并在下面的空格中写出完整的命令。

__ipv6_____

然后在路由器 G0/0 接口视图下，配置接口自动生成链路本地地址，并在下面的空格中写出完整的命令。

RTA 上的命令：___[RTA-GigabitEthernet0/0]ipv6 address auto link-local_____

RTB 上的命令：___[RTB-GigabitEthernet0/0]ipv6 address auto link-local_____

以上配置完成后，路由器会自动生成前缀为 FE80::的链路本地地址。请用命令来查看生成的链路本地地址，并在下面的空格中写出完整的命令。

____display ipv6 interface GigabitEthernet 0/0_____

请在下面填入所看到的地址。

RTA 的接口 G0/0 链路本地地址是：_____ FE80::20F:E2FF:FED1:BDF8_____

RTB 的接口 G0/0 链路本地地址是：_____ FE80::20F:E2FF:FED1:BFB8_____

说明：

链路本地地址和 MAC 地址相关，每台设备会有所不同。

在 RTA 上用命令来进行 RTA 与 RTB 之间的 IPv6 可达性测试，并在下面的空格中写出完整的命令。

_____ ping ipv6 FE80::20F:E2FF:FED1:BFB8 -i GigabitEthernet 0/0___

可达性测试的结果是： 成功 □ 失败 □

如果可达性测试失败，请分析原因。

在 RTA 和 RTB 上通过命令来查看路由器的邻居信息，并在下面的空格中写出完整的命令。

_____ display ipv6 neighbors all_____

RTA 上看到的邻居地址信息是：_____ FE80::20F:E2FF:FED1:BFB8 _____

RTB 的看到的邻居地址信息是：_____ FE80::20F:E2FF:FED1:BDF8_____

步骤三：配置接口生成 EUI-64 地址并测试可达性，查看邻居信息

请在 RTA 及 RTB 的 G0/0 接口视图下，配置接口生成符合 EUI-64 格式的全球单播地址，并设定其前缀为 1::/64。在下面的空格中写出完整的命令。

RTA 上的命令：_____ ipv6 address 1::/64 eui-64_____

RTB 上的命令：_____ ipv6 address 1::/64 eui-64_____

以上配置完成后，路由器接口会生成符合 EUI-64 规范的全球单播地址。用命令来查看生成的 EUI-64 地址并测试可达性。请在下面填入实验结果：

RTA 的接口 G0/0 全球单播地址是：_____ 1::20F:E2FF:FED1:BDF8_____

RTB 的接口 G0/0 全球单播地址是：_____ 1::20F:E2FF:FED1:BFB8_____

在 RTA 上用命令来进行 RTA 与 RTB 之间的 IPv6 可达性测试，并在下面的空格中写出完整的命令。

_____ping ipv6 1::20F:E2FF:FED1:BFB8_____

可达性测试的结果是： 成功 □ 失败 □

在 RTA 和 RTB 上通过命令来查看路由器的邻居信息。

RTA 上看到的邻居地址信息是：

_1::20F:E2FF:FED1:BFB8，FE80::20F:E2FF:FED1:BFB8__

RTB 的看到的邻居地址信息是：

_1::20F:E2FF:FED1:BDF8，FE80::20F:E2FF:FED1:BDF8__

步骤四：配置接口生成全球单播地址并测试可达性，查看邻居信息

请在 RTA 及 RTB 的 G0/0 接口视图下，分别配置全球单播地址 2::1/64 及 2::2/64，并在下面的空格中写出完整的命令。

RTA 上的命令：____ [RTA-GigabitEthernet0/0]ipv6 address 2::1/64_____

RTB 上的命令：_____ [RTB-GigabitEthernet0/0]ipv6 address 2::2/64_____

以上配置完成后，路由器接口会生成全球单播地址。用命令 display ipv6 interface g0/0 verbose 来查看全球单播地址。请在下面填入实验结果：

RTA 的接口 G0/0 全球单播地址是：_____2::1/64_____

RTB 的接口 G0/0 全球单播地址是：_____ 2::2/64_____

在 RTA 上用命令来进行 RTA 与 RTB 之间的 IPv6 可达性测试，并在下面的空格中写出完整的命令。

_____<RTA>ping ipv6 2::2_____

可达性测试的结果是： 成功 □ 失败 □

在 RTA 和 RTB 上通过命令来查看路由器的邻居信息。

RTA 上看到的邻居地址信息是：_____1::20F:E2FF:FED1:BFB8，FE80::20F:E2FF:FED1:BFB8，2::2____

RTB 的看到的邻居地址信息是：___1::20F:E2FF:FED1:BDF8，FE80::20F:E2FF:FED1:BDF8，2::1____

实验13 FTP/TFTP

实验任务一：FTP 操作与分析

本实验通过将路由器配置为 FTP 服务器端，然后在 PC 上使用 FTP 客户端连接到路由器并传输文件。期间通过报文分析软件对 FTP 协议的连接建立和文件传输过程进行观察，从而掌握 FTP 协议的工作原理。

步骤一：建立物理连接

按照实验组网图进行连接，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，请读者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。

以上步骤可能会用到以下命令：

```
<RTA> display version
<RTA> reset saved-configuration
<RTA> reboot
```

步骤二：IP 地址配置

表13-1 IP 地址列表

设备名称	接口	IP 地址	网关
PCA	--	10.0.0.2/24	10.0.0.1
RTA	G0/0	10.0.0.1/24	--

按表 13-1所示在 PC 及路由器上配置 IP 地址。

步骤三：报文分析软件配置

因为在本实验中，需要对 PC 与路由器间的 FTP 协议交互报文进行观察，所以首先要会利用报文分析软件进行相应的报文截获。报文分析软件有多种，较多使用的有 Ethereal、Sniffer 等。本实验以较常用的开源软件 Ethereal 为例，简单描述相关配置。

首先从网站 http://www.ethereal.com/上获取相关软件，安装在 PC 上。然后打开软件，按照下述步骤操作：

1) 在主菜单下选取【Capture】，在弹出的下拉式菜单中单击【Start】，系统会弹出一个配置界面。

2) 在【Interface】对话框中选择使用当前的网卡，然后单击【OK】。软件开始进行报文截获。

3) 截获到所需报文后，单击【Stop】以停止截获，然后查看报文的详细信息。

熟悉软件操作后，请先关闭软件。

步骤四：FTP 服务器端配置

请在路由器 RTA 的系统视图下，使能路由器的 FTP 服务器功能，并在下面的空格中写出完整的命令。

ftp server enable

然后在路由器上创建本地用户并设置相应的密码、服务类型、权限等参数，并在下面的空格中写出完整的命令。

local-user abc

password simple 123456

service-type ftp

level 3

配置完成后要注意保存。

步骤五：使用 FTP 下载文件

在 PCA 的 Windows 操作系统上单击【开始】，单击【命令提示符】，在弹出的对话框中输入命令“CMD”，进入命令行界面下。同时，按照步骤二中的方法，将报文分析软件打开，并开始进行报文捕获。

在命令行界面下，键入命令“ftp 10.0.0.1”，来连接到 FTP 服务器。请按照系统的提示来输入相应的用户名和密码。

用户名： abc

密码： 123456

正常情况下，PCA 现在已经通过 FTP 协议连接到 RTA 上。现在需要把 RTA 上的文件下载到 PCA 上。在命令行下输入命令“ls”来查看 RTA 上的文件名，并在下面的空格中写出看到的后缀名称为.cfg 的文件名。

startup.cfg

说明：

此处可能会有多个文件。

将上述后缀名称为.cfg 的文件来下载到本地。在下面的空格中写出所使用的命令：

get startup.cfg

待系统提示下载完成后，退出 FTP 命令行会话。在下面的空格中写出所使用的命令：

bye

步骤六：TCP 及 FTP 协议分析

停止报文分析软件 Ethereal，然后查看所截获报文的详细信息。请在下面的表格中填入所截获的前三个 TCP 报文的相关信息。

表13-2 TCP 报文信息表

报文序号	源 IP	目的 IP	源端口	目的端口	标志位（Flag）	序列号（Sequence number）	确认号（Acknowledgement number）	Window Size
1	10.0.0.2	10.0.0.1	1109	21	syn	0	0	65535
2	10.0.0.1	10.0.0.2	21	1109	Syn,ack	0	1	8192
3	10.0.0.2	10.0.0.1	1109	21	ack	1	1	65535

根据表 13-2TCP 报文信息表中内容，思考并回答以下问题：

在 TCP 连接中，第一个报文的标志位是 SYN，表示 客户端同步连接服务器 ；确认号是 0 ，表示 此为第一个报文，不需要确认 ；

第二个报文的标志位是 SYN，ACK ，表示 服务器端同步连接客户端，并对客户端回应 ；Acknowledgement number 是 1 ，表示 要求回应报文的 Sequence number 是 1。

在 TCP 建立完成后，客户端与服务器端之间建立 FTP 连接并开始传输文件。请观察 FTP 报文，并在下面的空格中填入以下结果：

PCA 上的 FTP 客户端端口号： 5001

RTA 上的 FTP 服务器端端口号： 20

FTP 文件传输模式是： ASCII

FTP 数据传输方式是： 主动方式（PORT 方式）

实验任务二：TFTP 操作与分析实验

本实验将 PC 配置为 TFTP 服务器端，然后在路由器上使用 FTP 客户端连接到 TFTP 服务器并传输文件。期间通过报文分析软件对 TFTP 协议的连接建立和文件传输过程进行观察，从而掌握 TFTP 协议的工作原理。

步骤一：TFTP 服务器软件配置

本实验中需要用到 TFTP 服务器。TFTP 服务器软件有多种，本实验以较常用的 3CDaemon 软件为例，简单描述相关配置。

首先从网站上下载 3CDaemon 并安装。安装成功后，打开 3CDaemon 软件，其缺省界面如图 13-1：

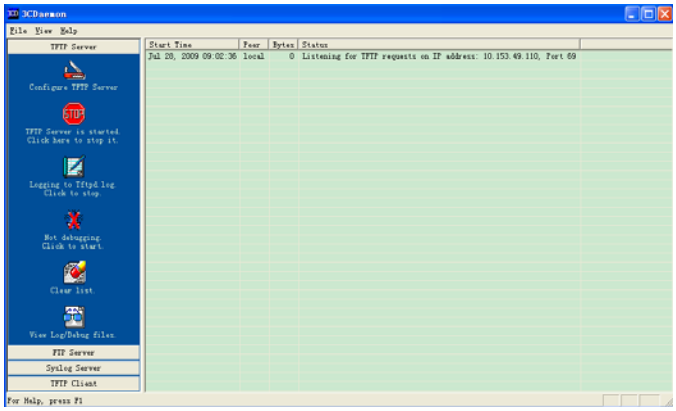


图13-1 3CDaemon 缺省界面

界面的左边是状态栏，表示所能配置的服务器，缺省就是 TFTP 服务器。单击状态栏中的“Configure TFTP Server”，弹出如图 13-2界面：

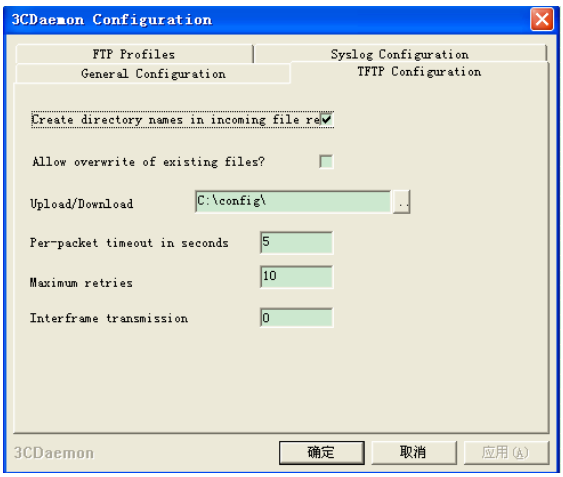


图13-2 TFTP 服务器配置界面

此界面上主要配置 TFTP 服务器的参数。在【Upload/Download】对话框键入所需要上传或下载文件的目录，或单击右边的图标，在弹出的菜单中进行目录选择。

将所需要上传或下载的文件放置于目录中，以备后续操作。考虑到路由器的存储空间有限，文件不宜太大。请读者在下面的空格中填入所放置的文件名称：

test.bin

步骤二：使用 TFTP 下载文件

在路由器的用户视图下，使用命令来查看路由器中的存储空间。在下面的空格中填入所使用的命令和所显示的剩余存储空间：

命令： dir

剩余空间：_____

确保剩余空间大于所需要下载的文件后，使用 TFTP 命令来将文件下载到路由器中。与此同时，打开报文分析软件，来截获 TFTP 操作的报文。

在下面的空格中填入所使用的命令：

tftp 10.0.0.2 get test.bin

步骤三：TFTP 协议分析

停止报文分析软件 Ethereal，然后查看所截获报文的详细信息。请在下面的表格中填入所截获的前三个 TFTP 报文的相关信息。

表13-3 TFTP 报文信息表

报文序号	源 IP	目的 IP	源端口	目的端口	块编号（Block）	确认块编号（Acknowledgement Block）	数据块大小
1	10.0.0.1	10.0.0.2	1028	69	--	--	--
2	10.0.0.2	10.0.0.1	1444	1028	1	--	512
3	10.0.0.1	10.0.0.2	1028	1444	--	1	512

根据 TFTP 报文信息表中内容，思考并回答以下问题：

在 TFTP 传输中，第一个报文是 读请求(Read Request) ，表示 TFTP 客户端需要从 TFTP 服务器下载文件 ；

第二个报文的块编号是 1 ，表示 所传输的第一个文件块 ；

第三个报文的确认块编号是 1 ，表示 确认收到所传输的第一个文件块 。

在 TFTP 传输中，报文数据块的大小是： 512 字节

另外，最后一个 TFTP 报文块的大小是：_____

实验14 以太网交换基础

实验任务一：MAC 地址学习

本实验的主要任务是学员掌握 MAC 地址学习机制以及理解 MAC 地址表

步骤一：运行超级终端并初始化交换机配置

将 PC（或终端）的串口通过标准 Console 电缆与交换机的 Console 口连接。电缆的 RJ-45 头一端连接交换机的 Console 口；9 针 RS-232 接口一端连接计算机的串行口。

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，请学员在用户视图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：连接 PC 并查看 MAC 地址表

按照实验组网图先将 PCA 与交换机连接，然后在交换机上通过 display mac-address 命令查看地址表项；然后再将 PCB 与交换机连接，再次在交换机上通过 display mac-address 命令查看地址表项。然后根据此输出结果完成补充如下表格：

MAC ADDR	VLAN ID	STATE	PORT INDEX	AGING TIME(s)
00-11-43-51-C5-A7	1	LEARNED	Ethernet1/0/1	AGING
00-10-5C-E5-F4-80	1	LEARNED	Ethernet1/0/11	AGING

从如上表格中可以看到，MAC 地址对应的 port index 表示

该 MAC 地址对应的二层以太网端口，也即表示该 MAC 地址是从该端口学习到的，那么同时发往该 MAC 地址的报文将从此端口发出

那么此时，如果 PCA 要给 PCB 发送一个数据帧，其转发流程为

由于在 SWA 的 MAC 地址表汇中已经有 PCA、PCB 的 MAC 地址表项记录，因此 PCA 发送给 PCB 的数据包，会直接查询 SWA 上的 MAC 地址表项，根据该表项记录的 PCB 对应的端口号，直接将数据帧转到该端口，不再向其他端口转发数据帧

步骤三：配置静态 MAC 地址

在交换机上将 PCA 的 MAC 地址配置为静态 MAC 地址表项，请在如下空格中补充完整的配置命令：

[SWA]mac-address static 0011-4351-C5A7 interface Ethernet 1/0/1 vlan 1

配置完成后，在 SWA 上查看 MAC 地址表项，可以看到 PCA 的 MAC 地址表项中 State 项为 Config static，Aging time 项为 NOAGED，port index 项为 Ethernet1/0/1

此时将 PCA 连接 SWA 的网线断开，将 PCA 连接到 SWA 的 Ethernet 1/0/15 端口上，然后再次在 SWA 上查看 MAC 地址表项，此时看到的地址表项 State 项为 Config static，Aging time 项为 NOAGED，port index 项为 Ethernet1/0/1；可以看到 SWA 的 MAC 地址没有学习到端口 Ethernet1/0/15 上，造成这种情况的原因是交换机的 MAC 地址表中对于同一个 MAC 地址同一 VLAN 中只有一个记录，如果静态配置了 PCA 的 MAC 地址和端口好的映射关系以后，交换机就不能也不再在同一 VLAN 中动态学习这个主机的 MAC 地址了。

实验15 VLAN

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 处于不同 VLAN，隔离 PC 间的访问，从而使学员加深对 Access 链路端口的理解。

步骤一：建立物理连接并运行超级终端

将 PC（或终端）的串口通过标准 Console 电缆与交换机的 Console 口连接。电缆的 RJ-45 头一端连接交换机的 Console 口；9 针 RS-232 接口一端连接计算机的串行口。

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，请学员在用户视图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：观察缺省 VLAN

可以在任意视图下通过 display vlan 命令查看交换机上的 VLAN 相关信息。

从以上输出可知，交换机上的缺省 VLAN 是 1。

请执行合适的命令以查看缺省 VLAN 的信息，并在下面的空格中写出完整的命令

```
display vlan 1
```

步骤三：配置 VLAN 并添加端口

分别在 SWA 和 SWB 上创建 VLAN 2，并将 PCA 和 PCC 所连接的端口 Ethernet1/0/1 添加到 VLAN 2 中。

配置 SWA：

请执行合适的命令在 SWA 上创建 VLAN 2 并将端口 Ethernet1/0/1 添加到 VLAN 2 中，在下面的空格中写出完整的命令：

```
[SWA]vlan 2
[SWA-vlan2]port Ethernet 1/0/1
```

配置 SWB：

请执行合适的命令创建 VLAN 2 并将端口 Ethernet1/0/1 添加到 VLAN 2 中，在下面的空格中写出完整的命令：

```
[SWB]vlan 2
[SWB-vlan2]port Ethernet 1/0/1
```

在交换机上查看有关 VLAN 以及 VLAN 2 的信息：

在 SWA 上查看配置的 Vlan 信息，请在下面空格中填写完整的命令：

```
[SWA]display vlan
```

在 SWA 上查看 VLAN 2 的信息，请在下面空格中填写完整的命令：

```
[SWA]display vlan 2
```

步骤四：查看物理端口链路类型

请执行合适的命令查看交换机的物理端口 Ethernet1/0/1 的信息，在下面的空格中写出完整命令：

[SWA]display interface Ethernet 1/0/1

执行上述命令，从命令的输出信息中可以发现，端口 Ethernet1/0/1 的 PVID 是 2，端口 Ethernet1/0/1 的链路类型是 access，该端口 Tagged VLAN ID 是 none，该端口 Untagged VLAN ID 是 2

步骤五：测试 VLAN 间的隔离

我们在 PC 上配置 IP 地址，通过 Ping 命令来测试处于不同 VLAN 间的 PC 能否互通。

表15-1 IP 地址列表

设备名称	IP 地址	网关
PCA	172.16.0.1/24	--
PCB	172.16.0.2/24	--
PCC	172.16.0.3/24	--
PCD	172.16.0.4/24	--

按表 15-1所示在 PC 上配置 IP 地址。

配置完成后，在 PCA 上用 Ping 命令来测试到其它 PC 的互通性。其结果应该是 PCA 与 PCB 不能(能/不能)互通，PCC 和 PCD 不能(能/不能)互通。

实验任务二：配置 Trunk 链路端口

本实验是在交换机间配置 Trunk 链路端口，使同一 VLAN 中的 PC 能够跨交换机访问。通过本实验，学员应该能够掌握 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，PCA 和 PCC 表面上都属于 VLAN 2，从整个网络环境考虑，它们并不在一个广播域，即本质上不在一个 VLAN 中，因为两个交换机上的 VLAN 目前只是各自在本机起作用，还没有发生关联。在 PCA 上用 Ping 命令来测试与 PCC 能否互通。其结果应该是不能互通。

PCA 与 PCC 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。

步骤二：配置 Trunk 链路端口

在 SWA 和 SWB 上配置端口 Ethernet 1/0/24 为 Trunk 链路端口并设置允许需要的 VLAN 数据帧通过。

配置 SWA 上端口 Ethernet 1/0/24 的 Trunk 相关属性：

[SWA]interface Ethernet 1/0/24

[SWA-Ethernet1/0/24]port link-type trunk

请在如上空格中补充完整的配置命令并说明该配置命令的含义：

如上命令设置端口的 Ethernet 1/0/24 链路类型为 Trunk 类型

[SWA-Ethernet1/0/24]port trunk permit vlan all

请在空格处说明该配置命令的含义：

如上配置命令配置允许所有的 VLAN 通过当前 Trunk 端口

完成 SWB 上端口 Ethernet 1/0/24 的 Trunk 相关配置，请在下面空格中填写完整的命令：

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

步骤三：查看 Trunk 相关信息

在 SWA 上执行 display interface Ethernet 1/0/24 命令可以查看端口 Ethernet 1/0/24 的信息，通过执行该命令后的输出的信息显示可以看到，端口的 PVID 值是 1，端口类型是 trunk，允许 VLAN 1~4094(VLAN 号)通过

在 SWA 上执行 display vlan 2 命令可以查看 VLAN 2 的相关信息，通过执行该命令后的输出的信息显示可以看到 VLAN 2 中包含了端口 Ethernet 1/0/24, 且数据帧是以 tagged(tagged/untagged)的形式通过端口的。

步骤四：跨交换机 VLAN 互通测试

在 PCA 上用 Ping 命令来测试与 PCC 能否互通。其结果应该是可以互通

实验任务三：配置 Hybrid 链路端口

本实验任务是利用 Hybrid 端口的特性－－一个端口可以属于多个不同的 VLAN，来完成分属不同 VLAN 内的同网段 PC 机的访问需求.通过本实验，学员应该能够掌握 Hybrid 链路端口的配置及作用。

步骤一：配置 PC 属于不同的 VLAN

保持实验一中配置的 PC 的 IP 地址不变，在实验二的基础上，修改 PCA、PCB、PCC、PCD 分别属于 VLAN 10、VLAN 20、VLAN 30、VLAN 40，同时保持设置端口 Ethernet 1/0/24 为 Trunk 链路端口并设置允许所有的 VLAN 数据帧通过。然后在 PC 上使用 PING 测试 PCA、PCB、PCC、PCD 之间的互通性，发现四台 PC 之间不能互通（能/不能）

然后在 SWA、SWB 上增加如下配置：

[SWA]vlan 30

[SWA]vlan 40

[SWB]vlan 10

[SWB]vlan 20

如上配置命令的作用是为后面配置 hybrid 属性做准备，因为只有在本机存在的 VLAN，在配置端口 hybrid 属性时才能配置该 VLAN 的 tagged 或者 untagged 属性。

步骤二：配置 Hybrid 链路端口

在 SWA 上配置 PCA 所连接的端口 Ethernet 1/0/1 为 Hybrid 端口，并允许 VLAN 30、VLAN 40 的报文以 untagged 方式通过：

[SwitchA]interface Ethernet1/0/1

[SwitchA-Ethernet0/1]port link-type hybrid

请在如上空格中补充完整的配置命令并说明该配置命令的含义：

设置端口 Ethernet 1/0/1 的链路类型为 Hybrid 类型

[SwitchA-Ethernet0/1]port hybrid vlan 30 40 untagged

请在空格处说明该配置命令的含义：

端口 Ethernet 1/0/1 能够接收 VLAN 30 和 40 发过来的报文并且发送这些 VLAN 的报文时不带 VLAN 标签

在 SWA 上配置 PCB 所连接的端口 Ethernet 1/0/2 为 Hybrid 端口，并允许 VLAN 30、VLAN 40 的报文以 untagged 方式通过，请在下面空格中填写完整的命令：

```
[SwitchA]interface Ethernet 1/0/2
[SwitchA-Ethernet0/2]port link-type hybrid
[SwitchA-Ethernet0/2]port hybrid vlan 30 40 untagged
```

在 SWB 上配置 PCC 所连接的端口 Ethernet 1/0/1 为 Hybrid 端口，并允许 VLAN 10、VLAN 20、VLAN 40 的报文以 untagged 方式通过，请在下面空格中填写完整的命令：

```
[SwitchB]interface Ethernet 1/0/1
```

```
[SwitchB-Ethernet0/1]port link-type hybrid
[SwitchB-Ethernet0/1]port hybrid vlan 10 20 40 untagged
```

在 SWB 上配置 PCD 所连接的端口 Ethernet 1/0/2 为 Hybrid 端口，并允许 VLAN 10、VLAN 20、VLAN 30 的报文以 untagged 方式通过，请在下面空格中填写完整的命令：

```
[SwitchB]interface Ethernet 1/0/2
[SwitchB-Ethernet0/2]port link-type hybrid
[SwitchB-Ethernet0/2]port hybrid vlan 10 20 30 untagged
```

步骤三：查看 Hybrid 相关信息

在 SWA 上执行 display vlan 10 命令可以查看 VLAN 10 的相关信息，通过执行该命令后的输出的信息显示可以看到 VLAN 10 中 tagged 的端口为 Ethernet1/0/24， untagged 的端口为 Ethernet1/0/1

在 SWA 上执行 display vlan 20 命令可以查看 VLAN 20 的相关信息，通过执行该命令后的输出的信息显示可以看到 VLAN 20 中 tagged 的端口为 Ethernet1/0/24， untagged 的端口为 Ethernet1/0/2

在 SWA 上执行 display vlan 30 命令可以查看 VLAN 30 的相关信息，通过执行该命令后的输出的信息显示可以看到 VLAN 30 中 tagged 的端口为 Ethernet1/0/24， untagged 的端口为 Ethernet1/0/1、Ethernet1/0/2

在 SWA 上执行 display vlan 40 命令可以查看 VLAN 40 的相关信息，通过执行该命令后的输出的信息显示可以看到 VLAN 40 中 tagged 的端口为 Ethernet1/0/24， untagged 的端口为 Ethernet1/0/1、Ethernet1/0/2。

在 SWB 上执行如上同样的命令查看相关的 VLAN 信息

在 SWA 上执行 display interface ethernet 1/0/1 命令可以查看端口 Ethernet 1/0/1 的信息，通过执行该命令后的输出的信息显示可以看到，端口的 PVID 值是 10，端口类型是 hybrid，Tagged VLAN ID 号是 none， Untagged VLAN ID 号是 10、30、40

在 SWA 上执行 display interface ethernet 1/0/2 命令可以查看端口 Ethernet 1/0/2 的信息，通过执行该命令后的输出的信息显示可以看到，端口的 PVID 值是 20，端口类型是 hybrid，Tagged VLAN ID 号是 none， Untagged VLAN ID 号是 20、30、40

在 SWB 上执行 display interface ethernet 1/0/1 命令可以查看端口 Ethernet 1/0/1 的信息，通过执行该命令后的输出的信息显示可以看到，端口的 PVID 值是 30，端口类型是 hybrid，Tagged VLAN ID 号是 none， Untagged VLAN ID 号是 10、20、30、40

在 SWB 上执行 display interface ethernet 1/0/2 命令可以查看端口 Ethernet 1/0/2 的信息，通过执行该命令后的输出的信息显示可以看到，端口的 PVID 值是 40，端口类型是 hybrid，Tagged VLAN ID 号是 none， Untagged VLAN ID 号是 10、20、30、40

步骤四：检查不同 VLAN 之间的互通性

完成步骤三的配置后，在 PC 上通过 PING 检测 PC 之间的互通性，检查发现：

PCA 和 PCB 不能互通

PCA 和 PCC 可以互通

PCA 和 PCD 可以互通

PCB 和 PCC 可以互通

PCB 和 PCD 可以互通

PCC 和 PCD 可以互通

实验16 生成树协议

实验任务一：STP 基本配置

步骤一：连接配置电缆

步骤二：配置 STP

配置 SWA：

在系统视图下启动 STP，

[SWA]stp enable

然后完成了如下配置命令：

[SWA]stp priority 0

如上配置命令的含义和作用是：设置 SWA 的优先级为 0，以使 SWA 为根桥

[SWA]interface Ethernet 1/0/1

[SWA-Ethernet1/0/1] stp edged-port enable

如上配置命令的含义是：配置连接 PC 的端口为边缘端口

配置 SWB：

在 SWB 上启动 STP 并设置 SWB 的优先级为 4096；并且配置 SWB 连接 PC 的端口为边缘端口。请下面的空格中写出完整的配置命令：

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

步骤三：查看 STP 信息

在 SWA 上执行 display stp 命令查看 STP 信息，执行 display stp brief 命令查看 STP 简要信息，依据该命令输出的信息，可以看到 SWA 上所有端口的 STP 角色是 DESI 即角色为指定端口，都处于 FORWARDING 转发状态

在 SWB 上执行 display stp 命令查看 STP 信息，执行 display stp brief 命令查看 STP 简要信息，依据该命令输出的信息，可以看到 SWB 端口 E1/0/23 的 STP 角色是根端口，处于 FORWARDING 转发状态，端口 E1/0/24 的 STP 角色是备份根端口，处于 DISCARDING 阻塞状态；连接 PC 的端口 E1/0/1STP 角色是指定端口，处于转发状态

从上可以得知，STP 能够发现网络中的环路，并有选择的对某些端口进行阻塞，最终将环路网络结构修剪成无环路的树型网络结构

步骤四：STP 冗余特性验证

分别配置 PCA、PCB 的 IP 地址为 172.16.0.1/24、172.16.0.2/24，配置完成后，在 PCA 上执行命令“Ping 172.16.0.2 –t”，以使 PCA 向 PCB 不间断发送 ICMP 报文

然后依据步骤三查看的 SWB 上看 STP 端口状态，确定交换机间端口 E1/0/23 处于转发状态。在 SWB 上将交换机之间处于 STP 转发状态端口的电缆断开，然后再次在 SWB 上查看 STP 端口状态，查看发现 SWB 端口 E1/0/24 处于转发状态。

通过如上操作以及显示信息可以看出，STP 不但能够阻断冗余链路，并且能够在活动链路断开时，通过激活被阻断的冗余链路而恢复网络的连通。

步骤五：端口状态迁移查看

在交换机 SWA 上断开端口 E1/0/1 的电缆，再重新连接，并且在 SWA 上查看交换机输出信息。如下：

```
[SWA]
……
 Ethernet1/0/1: link status is UP
%Apr 26 14:04:53:880 2000 SWA MSTP/2/PFWD:Instance 0's 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。出现这种情况的原因是因为端口被配置成边缘端口，无须延迟而进入转发状态，这也是 RSTP/MSTP 相对于 STP 的改进之一

为了清晰观察端口状态，我们在连接 PC 的端口 E1/0/1 上取消边缘端口配置，请在如下空格中填写完整的配置命令：

配置 SWA 取消边缘端口配置：

```
[SWA]interface Ethernet 1/0/1
[SWA-Ethernet1/0/1] undo stp edged-port
```

配置完成后，断开端口 E1/0/1 的电缆，再重新连接，并且在 SWA 上通过命令 display stp brief 查看端口 E1/0/1 的状态. 注意每隔几秒钟执行命令查看一次，以能准确看到端口状态的迁移过程. 可知，端口 E1/0/1 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

注意：

如果在 PCA 上 Ping 172.16.0.2 –t 时出现 “Request timed out.”，表明 PCB 无回应，需要检查 PCB 是否开启了防火墙或交换机配置是否有问题。

实验17 链路聚合

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，使学员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：连接配置电缆

将 PC（或终端）的串口通过标准 Console 电缆与交换机的 Console 口连接。电缆的 RJ-45 头一端连接路由器的 Console 口；9 针 RS-232 接口一端连接计算机的串行口。

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，请读者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

配置 SWA，在 SWA 上完成如下配置：

[SWA] interface bridge-aggregation 1

如上配置命令的含义是：创建二层聚合端口，并进入二层聚合端口视图，数字 1 表示聚合组编号为 1

[SWA] interface Ethernet 1/0/23

[SWA-Ethernet1/0/23] port link-aggregation group 1

补充如上空格中的配置命令并说明该命令的含义：将端口 E1/0/23 加入聚合组 1

[SWA] interface Ethernet 1/0/24

[SWA-Ethernet1/0/24] port link-aggregation group 1

配置 SWB，将端口 E1/0/23 和端口 E1/0/24 进行聚合，请在如下空格中补充完整的配置命令：

```
[SWB] interface bridge-aggregation 1
[SWB] interface Ethernet 1/0/23
[SWB-Ethernet1/0/23] port link-aggregation group 1
[SWB] interface Ethernet 1/0/24
[SWB-Ethernet1/0/24] port link-aggregation group 1
```

步骤三：查看聚合组信息

分别在 SWA 和 SWB 上通过 display link-aggregation summary 命令查看二层聚合端口所对应的聚合组摘要信息，通过 display link-aggregation verbose 命令查看二层聚合端口所对应聚合组的详细信息

通过执行查看聚合组摘要信息命令，可以得知该聚合组聚合端口类型是：BAGG 代表二层聚合端口，聚合模式是 S 静态聚合，负载分担类型是 share 为负载分担类型，Select Ports 数是 2，Unselect Ports 数是 0。

步骤四：链路聚合组验证

表17-1 IP 地址列表

设备名称	IP 地址	网关
PCA	172.16.0.1/24	--
PCB	172.16.0.2/24	--

按表 17-1所示在 PC 上配置 IP 地址。

配置完成后，在 PCA 上执行 **ping** 命令，以使 PCA 向 PCB 不间断发送 ICMP 报文。

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 PCA 上发送的 ICMP 报文无（有/无）丢失。（注意：丢失一个 ping 包也属于正常）

如上测试说明聚合组中的两个端口之间是互为备份的关系。

实验18 直连路由和静态路由

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

实验任务一：直连路由与路由表查看

步骤一：建立物理连接并运行超级终端

将 PC（或终端）的串口通过标准 Console 电缆与路由器的 Console 口连接。电缆的 RJ-45 头一端连接路由器的 Console 口；9 针 RS-232 接口一端连接计算机的串行口。

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，请学员在用户视图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，在路由器上在任意视图下通过执行 display ip routing-table 命令查看路由器全局路由表，执行该命令，从输出信息可知，目前路由器只有目的地址是 127.0.0.0/127.0.0.1 的路由

表18-1 IP 地址列表

设备名称	接口	IP 地址	网关
RTA	S6/0	192.168.1.1/24	--
	G0/0	192.168.0.1/24	--
RTB	S6/0	192.168.1.2/24	--
	G0/0	192.168.2.1/24	--
PCA	--	192.168.0.2/24	192.168.0.1
PCB	--	192.168.2.2/24	192.168.2.1

按表 18-1所示在路由器接口上分别配置 IP 地址。

配置完成后，再次通过 display ip routing-table 查看 RTA 路由表，从该命令的输出信息可以看出，路由表中的路由类型为直连路由，这种类型的路由是由链路层协议发现的路由，链路层协议 UP 后，路由器会将其加入路由表中。如果我们关闭链路层协议，则相关直连路由也消失。

在 RTA 上通过在接口视图下执行 shutdown 命令关闭接口 GigabitEthernet0/0，然后再次查看 RTA 路由表，可以看到与该接口网段相关的路由消失（存在/消失）

继续在 RTA 上在接口视图下执行 undo shutdown 命令开启接口 GigabitEthernet0/0，然后再次查看 RTA 路由表，可以看到与该接口网段相关的路由存在（存在/消失）

实验任务二：静态路由配置

本实验主要是通过在路由器上配置静态路由，从而达到 PC 之间能够互访的目的。通过本次实验，学员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：配置 PC IP 地址

按表 18-1所示在 PC 上配置 IP 地址和网关。配置完成后，在 PC 上用 Ping 命令来测试可达性。

在 PCA 上测试到网关（192.168.0.1）的可达性，PING 的结果是可以互通

在 PCA 上用 Ping 命令测试到 PCB 的可达性，PING 的结果是不可达,造成该结果的原因是 RTA 没有到达 PCB（192.168.2.2）的路由

步骤二：静态路由配置规划

要解决步骤一中出现的 PCA 与 PCB 之间可达性的问题，需要规划配置静态路由：

1. 规划 RTA 上的静态路由，RTA 上应该配置一条目的网段为 192.168.2.0/24 下一跳为 192.168.1.2 的静态路由

2. 规划 RTB 上的静态路由，RTB 上应该配置一条目的网段为 192.168.0.0/24 下一跳为 192.168.1.1 的静态路由

步骤三：配置静态路由

依据步骤二的规划，在 RTA 上配置如下静态路由：

```
[RTA]ip route-static 192.168.2.0 24 192.168.1.2
```

在 RTB 上配置如下静态路由：

```
[RTB]ip route-static 192.168.0.0 24 192.168.1.1
```

配置完成后，分别在 RTA 和 RTB 上查看路由表，可以看到路由表中有一条路由协议类型为 static 路由优先级为 60 的静态路由，表明路由配置成功。

再次测试 PC 之间的可达性，在 PCA 上用 Ping 命令测试到 PCB 的可达性，结果是 PCA 与 PCB 之间可以互通

要查看 PCA 到 PCB 得数据报文的传递路径，可以在 PCA 上通过 Tracert 命令来查看，查看结果是报文沿 PCA→RTA→RTB→PCB 的路径被转发的

步骤四：路由环路观察

为了人为在 RTA 和 RTB 之间造成环路，可以在 RTA 和 RTB 上分别配置一条缺省路由，该路由的下一跳互相指向对方，因为路由器之间是用串口点到点相连的，所以可以（可以/不可以）配置下一跳为本地接口

在 RTA 上配置该路由：

[RTA]ip route-static 0.0.0.0 0.0.0.0 s6/0

在 RTB 上配置该路由：

[RTB]ip route-static 0.0.0.0 0.0.0.0 s6/0

配置完成后，在路由器上查看路由表。

在 RTA 上查看路由表，可以看到一条优先级为 60，协议类型为 Static 的缺省路由。

在 RTB 上查看路由表，可以看到一条优先级为 60，协议类型为 Static 的缺省路由

可知，缺省路由配置成功。

然后在 PCA 上用 Tracert 命令追踪到目的 IP 地址 3.3.3.3 的数据报文的转发路径，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，报文在 192.168.1.2 和 192.168.1.1 之间循环转发。造成该现象的原因是：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 RTB（192.168.1.2），而 RTB 又根据它的缺省路由，把报文转发回了 RTA（192.168.1.1）。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

实验19 RIP

实验任务一：配置 RIPv1

本实验主要通过在路由器上配置 RIPv1 协议，达到 PC 之间能够互访的目的。通过本次实验，学员应能够掌握 RIPv1 协议的基本配置。

步骤一：建立物理连接并运行超级终端

将 PC（或终端）的串口通过标准 Console 电缆与路由器的 Console 口连接。电缆的 RJ-45 头一端连接路由器的 Console 口；9 针 RS-232 接口一端连接计算机的串行口。

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，请学员在用户视图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19-1 IP 地址列表

设备名称	接口	IP 地址	网关
RTA	S6/0	192.168.1.1/24	--
	G0/0	192.168.0.1/24	--
RTB	S6/0	192.168.1.2/24	--
	G0/0	192.168.2.1/24	--
PCA	--	192.168.0.2/24	192.168.0.1
PCB	--	192.168.2.2/24	192.168.2.1

按表 19-2所示在 PC 上配置 IP 地址和网关。配置完成后用 ping 命令测试网络的可达性。

在 PCA 上用 ping 命令测试到网关 192.168.0.1 的可达性，测试结果是 可以互通

在 PCA 上用 ping 命令测试到 PCB 的可达性，测试结果是目的网段不可达，无法互通,产生该结果的原因是 路由器上没有到达目的主机的路由

步骤三：启用 RIP 协议

在 RTA 上配置 RIP 相关命令如下：

[RTA]rip

如上配置命令的含义是 在 RTA 上启动 RIP 进程

[RTA-rip-1]network 192.168.0.0

如上命令提示符中数字 1 的含义是 RIP 进程 1，在启动 RIP 的时候，没有指定进程号，就采用缺省进程 1

如上配置命令的含义是在网段 192.168.0.0 接口上使能 RIP

[RTA-rip-1]network 192.168.1.0

在 RTB 上创建 RIP 进程并在 RTB 的两个接口上使能 RIP，在如下的空格处填写具体命令：

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

步骤四：查看路由表并检测 PC 之间互通性

完成步骤三后，在路由器上通过 display ip routing-table 命令查看路由表。

在 RTA 上可以看到一条目的网段为 192.168.2.0/24 优先级为 100 的 RIP 路由

在 RTB 上可以看到一条目的网段为 192.168.0.0/24 优先级为 100 的 RIP 路由

在 PCA 上通过 Ping 命令检测 PC 之间的互通性，其结果是可以互通

步骤五：查看 RIP 的运行状态

在 RTA 上通过命令 display rip 查看 RIP 运行状态，从其输出信息可知，目前路由器运行的是 RIPv1，自动聚合功能是打开(打开/关闭)的；路由更新周期（Update time）是 30 秒，network 命令所指定的网段是 192.168.0.0 和 192.168.1.0。

打开 RIP 的 debugging，观察 RIP 收发协议报文的情况，看到如下 debugging 信息：

```
<RTA>terminal debugging
<RTA>terminal monitor
<RTA>debugging rip 1 packet
<RTA>
*Oct 31 02:20:12:490 2008 RTA RM/6/RMDEBUG: RIP 1 : Sending response on interface
GigabitEthernet0/0 from 192.168.0.1 to 255.255.255.255
*Oct 31 02:20:12:490 2008 RTA RM/6/RMDEBUG:   Packet : vers 1, cmd response, length
44
*Oct 31 02:20:12:491 2008 RTA RM/6/RMDEBUG:     AFI 2, dest 192.168.1.0, cost 1
*Oct 31 02:20:12:491 2008 RTA RM/6/RMDEBUG:     AFI 2, dest 192.168.2.0, cost 2
*Oct 31 02:20:12:491 2008 RTA RM/6/RMDEBUG: RIP 1 : Sending response on interface
Serial6/0 from 192.168.1.1 to 255.255.255.255
*Oct 31 02:20:12:491 2008 RTA RM/6/RMDEBUG:   Packet : vers 1, cmd response, length
24
*Oct 31 02:20:12:491 2008 RTA RM/6/RMDEBUG:     AFI 2, dest 192.168.0.0, cost 1
*Oct 31 02:20:19:505 2008 RTA RM/6/RMDEBUG: RIP 1 : Receive response from 192.168.1.2
on Serial6/0
*Oct 31 02:20:19:506 2008 RTA RM/6/RMDEBUG:   Packet : vers 1, cmd response, length
24
*Oct 31 02:20:19:506 2008 RTA RM/6/RMDEBUG:     AFI 2, dest 192.168.2.0, cost 1
```

由以上输出可知，RTA 在接口 GigabitEthernet0/0 上发送的路由更新以及在接口 Serial6/0 上发送的路由更新，目的地址都为 255.255.255.255 也即是以广播方式发送的.同时可以看到发送以及接收的路由更新网段信息都没有携带掩码。

分析以上的路由更新，可以发现，RTA 在接口 Serial6/0 上收到路由 192.168.2.0，而不会再把此路由从接口 Serial6/0 上发出去。原因是路由器启用 RIP 后，水平分割功能缺省是打开的

步骤六：查看水平分割与毒性逆转

在 RTA 上添加如下配置：

```
[RTA-Serial6/0]undo rip split-horizon
```

如上配置命令的含义是在接口 Serial 6/0 上取消水平分割，配置完成后，看到如下 debugging 信息：

```
*Oct 21 09:37:55:171 2008 RTA RM/6/RMDEBUG: RIP 1 : Sending response on interface
Serial6/0 from 192.168.1.1 to 255.255.255.255
*Oct 21 09:37:55:171 2008 RTA RM/6/RMDEBUG:   Packet : vers 1, cmd response, length
64
*Oct 21 09:37:55:171 2008 RTA RM/6/RMDEBUG:     AFI 2, dest 192.168.0.0, cost 1
*Oct 21 09:37:55:171 2008 RTA RM/6/RMDEBUG:     AFI 2, dest 192.168.1.0, cost 1
*Oct 21 09:37:55:172 2008 RTA RM/6/RMDEBUG:     AFI 2, dest 192.168.2.0, cost 2
```

由以上输出可知，在水平分割功能关闭的情况下，RTA 在接口 Serial6/0 上发送的路由更新包含了路由 192.168.0.0、192.168.1.0 和 192.168.2.0。也就是说，路由器把从接口 Serial6/0 学到的路由 192.168.2.0 又从该接口发送了出去。这样容易造成路由环路

另外一种避免环路的方法是毒性逆转。在 RTA 的接口 Serial6/0 上启用毒性逆转，请在如下的空格中补充完整的配置命令

```
[RTA-Serial6/0]rip poison-reverse
```

配置完成后，看到如下 debugging 信息：

```
*Oct 21 09:40:02:143 2008 RTA RM/6/RMDEBUG: RIP 1 : Sending response on interface
Serial6/0 from 192.168.1.1 to 255.255.255.255
*Oct 21 09:40:02:143 2008 RTA RM/6/RMDEBUG:   Packet : vers 1, cmd response, length
44
*Oct 21 09:40:02:143 2008 RTA RM/6/RMDEBUG:     AFI 2, dest 192.168.0.0, cost 1
*Oct 21 09:40:02:143 2008 RTA RM/6/RMDEBUG:    AFI 2, dest 192.168.2.0, cost 16
```

由以上输出信息可知，启用毒性逆转后，RTA 在接口 Serial 6/0 上发送的路由更新包含了路由 192.168.2.0，但度量值为 16（无穷大）。相当于显式地告诉 RTB，从 RTA 的接口 Serial6/0 上不能到达网络 192.168.2.0。

步骤七：配置接口工作在抑制状态

在前面实验中，路由器在所有接口都发送协议报文，包括连接 PC 的接口。实际上，PC 并不需要接收 RIP 协议报文。我们可以在 RIP 视图下配置 silent-interface 命令使接口只接收而不发送 RIP 协议报文。

配置 RTA 接口 GigabitEthernet 0/0 工作在抑制状态，请补充完整的配置命令：

```
[RTA-rip-1]silent-interface GigabitEthernet 0/0
```

配置 RTB 接口 GigabitEthernet 0/0 工作在抑制状态，请补充完整的配置命令：

```
[RTB-rip-1]silent-interface GigabitEthernet 0/0
```

配置完成后，用 debugging 命令来观察 RIP 收发协议报文的情况。可以发现，RIP 不再从接口 GigabitEthernet0/0 发送协议报文了。

这种方法的另外一个好处是防止路由泄漏而造成网络安全隐患。比如，公司某台运行 RIP 的路由器连接到公网，那就可以通过配置 silent-interface 而防止公司内网中的路由泄漏到公网上。

此步骤完成后，在路由器上关闭 debugging，以免影响后续实验。

```
<RTA>undo debugging all
<RTB>undo debugging all
```

实验任务二：配置 RIPv2

本实验首先通过让 RIPv1 在划分子网的情况下不能正确学习路由，从而让学员了解到 RIPv1 的局限性；然后指导学员启用 RIPv2 协议。通过本实验，学员应该能够了解 RIPv1 的局限性，并掌握如何在路由器上配置 RIPv2。

步骤一：建立物理连接并运行超级终端

将 PC（或终端）的串口通过标准 Console 电缆与路由器的 Console 口连接。电缆的 RJ-45 头一端连接路由器的 Console 口；9 针 RS-232 接口一端连接计算机的串行口。

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，请学员在用户视图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19-2 IP 地址列表

设备名称	接口	IP 地址	网关
RTA	S6/0	192.168.1.1/24	--
	G0/0	192.168.0.1/24	--
RTB	S6/0	192.168.1.2/24	--
	G0/0	10.0.0.1/24	--
PCA	--	192.168.0.2/24	192.168.0.1
PCB	--	10.0.0.2/24	10.0.0.1

按上表在路由器接口上以及 PC 上配置 IP 地址。

步骤三：配置 RIPV1，观察路由表

在 RTA 上创建 RIPv1 进程并在 RTA 的两个接口上使能 RIP，具体命令为：

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

在 RTB 上创建 RIPv1 进程并在 RTA 的两个接口上使能 RIP，具体命令为：

```
[RTB]rip
[RTB-rip-1]network 192.168.1.0
[RTB-rip-1]network 10.0.0.0
```

配置完成后，在 RTA 上通过 display ip routing-table 命令查看全局路由表，从路由表输出信息可以看到，RTA 路由表中通过 RIP 协议学习到的路由目的网段为 10.0.0.0/8，该目的网段与实际 RTB 的网络不一致（一致/不一致），导致这种结果的原因是 RIPv1 协议报文中不携带掩码信息所致，路由信息以自然掩码学习.要解决该问题可以将 RIP 运行版本修改为 RIPv2

步骤四：配置 RIPV2

在步骤三的基础上修改 RTA、RTB 的 RIP 版本为 Version 2，在正确的视图下配置 RIP Version 2 的命令：

```
[RTA-rip-1]version 2
[RTB-rip-1]version 2
```

要使得 RIP V2 能够向外发布子网路由和主机路由，而不是按照自然掩码发布网段路由，还需要配置关闭 RIPV2 自动聚合功能，在正确视图下完成该配置的命令：

```
[RTA-rip-1]undo summary
[RTB-rip-1]undo summary
```

配置完成后，在 RTA 上查看路由表，可以看到，RTA 学习到的 RIP 路由的目的网段为 10.0.0.0/24，此时如果路由表中仍然有路由 10.0.0.0/8，其原因可能是 RIP 路由的老化时间是 180 秒。当未收到关于此路由的更新超过 180 秒后，RIP 才会把此路由从 IP 路由表中撤销

在 RTA 上通过命令 display rip 查看 RIP 运行状态，从其输出信息可知，当前 RIP 的运行版本是 RIPv2

步骤五：配置 RIPv2 认证

在 RTA 上添加如下配置：

```
[RTA-Serial6/0]rip authentication-mode md5 rfc2453 aaaaa
```

如上配置命令的含义是在接口 S6/0 下启动 RIPV2 的 MD5 密文验证，验证密钥是 aaaaa 并注定 MD5 认证报文使用 RFC 2453 标准的报文格式

配置 RTB 的 S6/0 启动 RFC 2453 格式的 MD5 认证，密钥为 abcde，请在如下空格中填写完整的配置命令：

```
[RTB-Serial6/0]rip authentication-mode md5 rfc2453 abcde
```

因为原有的路由需要过一段时间才能老化，所以可以将接口关闭再启用，加快重新学习路由的过程。例如，关闭再启用 RTA 的接口 Serial6/0，如下：

```
[RTA-Serial6/0]shutdown
[RTA-Serial6/0]undo shutdown
```

配置完成后，在路由器上查看路由表，在 RTA 的路由表中没有 RIP 路由，在 RTB 的路由表中也没有 RIP 路由可以看到，因认证密码不一致，RTA 不能够学习到对端设备发来的路由

修改 RTB 的 MD5 认证密钥，使其与 RTA 认证密钥一致，请在如下空格中补充完整的配置命令：

```
[RTA-Serial6/0]rip authentication-mode md5 rfc2453 aaaaa
```

配置完成后，等待一段时间后，再查看 RTA 上的路由表，可以看到，RTA 路由表中有了正确的路由 10.0.0.0/24。请在如下空格中说明为什么需要等待一段时间后才能看到正确的路由：需要等到 RIP 的更新周期

实验20 OSPF

实验任务一：单区域 OSPF 基本配置

步骤一：搭建实验环境并完成基本配置

步骤二：检查网络连通性和路由器路由表

在 ClientA 上 ping ClientB (IP 地址为 10.1.0.1)，结果是无法互通，导致这种结果的原因是 RTA 上只有直连路由，没有到达 ClientB 的路由表，故从 ClientA 上来的数据报文无法转发给 ClientB

步骤三：配置 OSPF

在 RTA 上完成 OSPF 如下配置：

[RTA]router id 1.1.1.1

[RTA]ospf 1

如上配置中，数字 1 的含义是 OSPF 进程号，缺省情况下取值为 1

[RTA-ospf-1]area 0.0.0.0

在如下的空格中填写最恰当的配置命令

[RTA-ospf-1-area-0.0.0.0]network 1.1.1.1 0.0.0.0

[RTA-ospf-1-area-0.0.0.0]network 10.0.0.0 0.0.0.255

[RTA-ospf-1-area-0.0.0.0]network 20.0.0.0 0.0.0.255

在 RTB 上配置 OSPF：

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

步骤四：检查路由器 OSPF 邻居状态及路由表

在路由器上可以通过 display ospf peer 命令查看路由器 OSPF 邻居状态。

通过如上命令在 RTA 上查看路由器 OSPF 邻居状态，依据输出信息，可以看到，RTA 与 Router ID 为 2.2.2.2（RTB）的路由器互为邻居，此时，邻居状态达到 FULL，说明 RTA 和 RTB 之间的链路状态数据库同步，RTA 具备到达 RTB 的路由信息。

在 RTA 上可以使用 display ospf routing 命令查看路由器的 OSPF 路由表。

在 RTA 上使用 display ip routing-table 命令查看路由器全局路由表，依据此命令输出信息显示，可以看到，RTA 的路由表中有二条 OSPF 路由，其优先级分别为 10，10 ，Cost 值分别为 2，2 。

步骤五：检查网络连通性

在 ClientA 上 ping ClientB(IP 地址为 10.1.0.1)，其结果是可以互通 。

在 ClientB 上 ping ClientA(IP 地址为 10.0.0.1)，其结果是可以互通 。

实验任务二：单区域 OSPF 增强配置

步骤一：搭建实验环境并完成基本配置

步骤二：OSPF 基本配置

在路由器上完成基本 OSPF 配置，并在相关网段使能 OSPF

1. 在 RTA 上配置 OSPF：

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

2. 在 RTB 上配置 OSPF：

```
[RTB]router id 2.2.2.2
[RTB]ospf 1
[RTB-ospf-1]area 0.0.0.0
[RTB-ospf-1-area-0.0.0.0]network 2.2.2.2 0.0.0.0
[RTB-ospf-1-area-0.0.0.0]network 10.0.0.0 0.0.0.255
[RTB-ospf-1-area-0.0.0.0]network 20.0.0.0 0.0.0.255
```

步骤三：检查路由器 OSPF 邻居状态及路由表

在 RTA 上使用 display ospf peer 命令查看路由器 OSPF 邻居状态，根据输出信息可以看到：RTA 与 Router ID 为 2.2.2.2（RTB）的路由器建立了两个邻居， RTA 的 G0/0 接口与 RTB 配置 IP 地址为 20.0.0.2 的接口建立一个邻居，该邻居所在的网段为 20.0.0.0/24；另外，RTA 的 G0/1 接口与 RTB 配置的 IP 地址为 10.0.0.2 的接口建立一个邻居，该邻居所在的网段为 10.0.0.0/24。

在 RTA 上使用 display ospf routing 查看路由器 OSPF 路由表,根据输出信息可以看到：

在 RTA 的 OSPF 路由表上有两条到达 RTB 的 2.2.2.2/32 网段的路由，分别是邻居 20.0.0.2 发布的，另一条是邻居 10.0.0.2 发布的，这几条路由的 Cost 相同。

在 RTA 上使用 display ip routing-table 查看路由器全局路由表，根据输出信息可以看到，在 RTA 路由器全局路由表内，有两条到达 RTB 的 2.2.2.2/32 网段的等价 OSPF 路由。

步骤四：修改路由器 OSPF 接口开销

修改路由器 OSPF 接口开销需要在接口视图下通过 ospf cost 命令完成。

修改 RTA 的 G0/0 接口的 OSPF 开销为 150，请在如下空格中填写完整的配置命令：

```
[RTA]interface G0/0
[RTA-GigabitEthernet0/0]ospf cost 150
```

步骤五：检查路由器路由表

在 RTA 上使用命令 display ospf routing 查看路由器 OSPF 路由表以及通过 display ip routing-table 命令查看路由器全局路由表，根据输出信息可以看到，在 RTA 的 OSPF 路由表上有一条到达 RTB 的 2.2.2.2/32 网段的路由，导致这种结果的原因是由于 RTA 的 G0/0 接口的开销配置为 150，远高于 G0/1 接口的开销，故在 RTA 的 OSPF 路由表上仅有一条由邻居 10.0.0.2（该邻居与 RTA 的 G0/1 接口连接）发布的到达 RTB 的 2.2.2.2/32 网段的路由。

步骤六：修改路由器 OSPF 接口优先级

配置修改路由器 OSPF 接口优先级需要在接口视图下通过 ospf dr-priority 命令完成。

修改 RTB 的 G0/0 的 OSPF 接口优先级为 0，请在如下空格中填写完整的配置命令：

```
[RTB]interface G0/0
[RTB-GigabitEthernet0/0]ospf dr-priority 0
```

步骤七：在路由器上重启 OSPF 进程

在路由器上重启 OSPF 进程需要在用户视图下通过 reset ospf 命令完成。

将 RTA 的 OSPF 进程重启，具体配置命令为<RTA>reset ospf 1 process

将 RTB 的 OSPF 进程重启，具体配置命令为<RTB>reset ospf 1 process

步骤八：查看路由器 OSPF 邻居状态

OSPF 进程重新启动后，在 RTA、RTB 上使用 display ospf peer 查看路由器 OSPF 邻居状态，依据输出信息可以看到，RTA 接口 G0/0 成为网段 20.0.0.0/24 的 DR，RTB 的 G0/0 成为网段 20.0.0.0/24 的 DRother，导致这种原因是因为由于 RTB 的 G0/0 接口的 dr 优先级为 0，不具备 DR/BDR 选举权 。

实验任务三：多区域 OSPF 基本配置

步骤一： 搭建实验环境并完成基本配置

步骤二：OSPF 基本配置

RTA 的两个接口都属于 OSPF 区域 0，RTB 的两个接口分别属于 OSPF 区域 0 和区域 1，RTC 的两个接口都属于 OSPF 区域 1。依据该区域划分完成基本 OSPF 配置。

在 RTA 完成基本 OSPF 配置，并在相关网段使能 OSPF，其完整命令为：

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

在 RTB 完成基本 OSPF 配置，并配置正确的区域以及在相关网段使能 OSPF，其完整命令为：

```
[RTB]router id 2.2.2.2
[RTB]ospf 1
[RTB-ospf-1]area 0.0.0.0
[RTB-ospf-1-area-0.0.0.0]network 2.2.2.2 0.0.0.0
[RTB-ospf-1-area-0.0.0.0]network 20.0.0.0 0.0.0.255
[RTB-ospf-1-area-0.0.0.0]quit
[RTB-ospf-1-area]area 1
[RTB-ospf-1-area-0.0.0.1]network 30.0.0.0 0.0.0.255
```

在 RTC 上完成基本 OSPF 配置，并在相关网段使能 OSPF，其完整命令为：

```
[RTC]router id 3.3.3.3
[RTC]ospf 1
[RTC-ospf-1]area 1
[RTC-ospf-1-area-0.0.0.1]network 3.3.3.3 0.0.0.0
[RTC-ospf-1-area-0.0.0.1]network 10.1.0.0 0.0.0.255
[RTC-ospf-1-area-0.0.0.1]network 30.0.0.0 0.0.0.255
```

步骤三：检查路由器 OSPF 邻居状态及路由表

在 RTB 上使用 display ospf peer 查看路由器 OSPF 邻居状态，根据输出信息可以得知，在 Area 0.0.0.0 内，RTB 的 G0/0 接口与 RTA 配置 IP 地址为 20.0.0.1 的接口建立邻居关系，该邻居所在的网段为 20.0.0.0/24，RTB 配置 IP 地址为 20.0.0.2 的接口为该网段的 DR 路由器；在 Area 0.0.0.1 内，RTB 的 G0/1 接口与 RTC 配置 IP 地址为 30.0.0.1 的接口建立邻居关系，该邻居所在的网段为 30.0.0.0/24，RTC 配置 IP 地址为 30.0.0.1 的接口为该网段的 DR 路由器。

在 RTB 上使用 display ospf routing 命令查看路由器 OSPF 路由表，使用 display ip routing-table 命令查看路由器全局路由表，

步骤四：检查网络连通性

在 ClientA 上 ping ClientB(IP 地址为 10.1.0.1)，其结果是可以互通；

在 ClientB 上 ping ClientA(IP 地址为 10.0.0.1)，其结果是可以互通。

实验21 ACL 包过滤

实验任务一：配置基本 ACL

本实验任务主要是通过在路由器上实施基本 ACL 来禁止 PCA 访问 PCB，使学员熟悉基本 ACL 的配置和作用

步骤一：建立物理连接并初始化路由器配置

按实验组网图进行物理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，请学员在用户视图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 IP 地址及路由

表21-1 IP 地址列表

设备名称	接口	IP 地址	网关
RTA	S6/0	192.168.1.1/24	--
	G0/0	192.168.0.1/24	--
RTB	S6/0	192.168.1.2/24	--
	G0/0	192.168.2.1/24	--
PCA	--	192.168.0.2/24	192.168.0.1
PCB	--	192.168.2.2/24	192.168.2.1

按表 21-1所示在 PC 上配置 IP 地址和网关。配置完成后，在 Windows 操作系统的【开始】里选择【运行】，在弹出的窗口里输入 CMD，然后在【命令提示符】下用 ipconfig 命令来查看所配置的 IP 地址和网关是否正确。

学员可自己选择在路由器上配置静态路由或任一种动态路由，来达到全网互通

配置完成后，请在 PCA 上通过 Ping 命令来验证 PCA 与路由器、PCA 与 PCB 之间的可达性。其结果应该可达。如果不可达，请参考本教材相关章节来检查路由协议是否设置正确。

步骤三：ACL 应用规划

本实验的目的是使 PCA 不能访问 PCB，也就是 PC 之间不可达。请学员考虑如何在网络中应用 ACL 包过滤的相关问题：

- 需要使用何种 ACL？
- ACL 规则的动作是 deny 还是 permit？
- ACL 规则中的反掩码应该是什么？

- ACL 包过滤应该应用在路由器的哪个接口的哪个方向上？

下面是有关 ACL 规划的答案：

- 本实验目的是要禁止 PCA 访问 PCB，仅使用源 IP 地址就能够识别 PCA 发出的数据报文，因此使用基本 ACL 即可。
- 本实验目的是要使 PC 之间不可达，因此 ACL 规则的动作是 deny。
- 本实验中只需要限制从单台 PC 发出的报文，因此反掩码设置为 0.0.0.0。
- 因为需要禁止 PCA 访问 PCB，所以可以在 RTA 连接 PCA 的接口 G0/0 上应用 ACL，方向为 Inbound。

步骤四：配置基本 ACL 并应用

首先要在 RTA 上配置开启防火墙功能并设置防火墙的缺省过滤方式，请在下面的空格中补充完整的命令：

[RTA] firewall enable

[RTA]firewall default permit

其次配置基本 ACL，基本 ACL 的编号范围是 2000~2999，请在下面的空格中补充完整的命令：

[RTA]acl number 2001

[RTA-acl-basic-2001]rule deny source 192.168.0.2 0.0.0.0

最后要在 RTA 的接口上应用 ACL 才能确保 ACL 生效，请在下面的空格中写出完整的在正确的接口正确的方向上应用该 ACL 的配置命令：

[RTA-GigabitEthernet0/0]firewall packet-filter 2001 inbound

步骤五：验证防火墙作用及查看

在 PCA 上使用 Ping 命令来测试从 PCA 到 PCB 的可达性，结果是 ping 包返回目的网段不可达

同时在 RTA 上通过命令 display acl 2001 查看 ACL 的统计，根据其输出信息显示可以看

Rule 0 8 times matched,根据该显示可以看到有数据报文命中了 ACL 中定义的规则。

在 RTA 上通过 display firewall-statistics all 命令查看所有的火墙的统计信息，依据该命令输出信息可以看到：

Firewall is enable, default filtering method is permit.

Interface: GigabitEthernet0/0

In-bound Policy: acl 2001

实验任务二：配置高级 ACL

本实验任务是通过在路由器上实施高级 ACL 来禁止从 PCA 到网络 192.168.2.0/24 的 FTP 数据流，来使学员熟悉高级 ACL 的配置和作用。

步骤一：建立物理连接并初始化路由器配置

按实验组网图进行物理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，请学员在用户视图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：ACL 应用规划

本实验的目的是禁止从 PCA 到网络 192.168.2.0/24 的 FTP 数据流，但允许其它数据流通过。请学员考虑如何在网络中应用 ACL 包过滤的相关问题：

- 需要使用何种 ACL？
- ACL 规则的动作是 deny 还是 permit？
- ACL 规则中的反掩码应该是什么？
- ACL 包过滤应该应用在路由器的哪个接口的哪个方向上？

下面是有关 ACL 规划的答案：

- 本实验目的是要禁止从 PCA 到网络 192.168.2.0/24 的 FTP 数据流。需要使用协议端口号来识别 PCA 发出的 FTP 数据报文，因此必须使用高级 ACL。
- 本实验目的是要使 PC 之间不可达，因此 ACL 规则的动作是 deny。
- 本实验中只需要限制从单台 PC 发出的到网络 192.168.2.0/24 的报文，因此需要设置源 IP 地址反掩码为 0.0.0.0，目的 IP 反掩码为 0.0.0.255。
- 因为需要禁止 PCA 发出的数据，所以可以在 RTA 连接 PCA 的接口 G0/0 上应用 ACL，方向为 inbound。

步骤三：配置高级 ACL 并应用

首先要在 RTA 上配置开启防火墙功能并设置防火墙的缺省过滤方式，请在下面的空格中补充完整的命令：

[RTA] firewall enable

[RTA]firewall default permit

其次配置高级 ACL，高级 ACL 的编号范围是 3000~3999，请在下面的空格中补充完整的命令：

[RTA]acl number 3002

[RTA-acl-adv-3002] rule deny tcp source 192.168.0.2 0.0.0.0 destination 192.168.2.1 0.0.0.255 destination-port eq ftp

[RTA-acl-adv-3002] rule permit ip source 192.168.0.2 0.0.0.0 destination 192.168.2.0 0.0.0.255

最后要在 RTA 的接口上应用 ACL 才能确保 ACL 生效，请在下面的空格中写出完整的在正确的接口正确的方向上应用该 ACL 的配置命令：

[RTA-GigabitEthernet0/0]firewall packet-filter 3002 inbound

步骤四：验证防火墙作用及查看

在 PCA 上使用 Ping 命令来测试从 PCA 到 PCB 的可达性，结果是可达

在 PCB 上开启 FTP 服务，然后在 PCA 上使用 FTP 客户端软件连接到 PCB,结果应该是

FTP 请求被拒绝

同时在 RTA 上通过命令 display acl 3002 查看 ACL 的统计，根据其输出信息显示可以看

Rule 0 6 times matched, Rule 5 1 times matched,

根据该显示可以看到有数据报文命中了 ACL 中定义的规则。

在 RTA 上通过 display firewall-statistics all 命令查看所有的火墙的统计信息,根据其输出信息可以看到数据报文被 permitted、denied 的百分比。

注意：

学员实验过程中所显示的 times matched 可能都不相同，是正常现象。

实验22 网络地址转换

实验任务一：配置 Basic NAT

本实验中，私网客户端 Client_A、 Client_B 需要访问公网服务器 Server，而 RTB 上不能保有私网路由，因此将在 RTA 上配置 Basic NAT，动态地为 Client_A、Client_B 分配公网地址。

步骤一：建立物理连接并初始化路由器配置

按实验组网图进行物理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，请学员在用户视图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：基本 IP 地址和路由配置

依据实验组网图，完成 RTA 和 RTB 上接口 IP 地址的配置，

需要在 RTA 上配置缺省路由去往公网路由器 RTB，请在下面的空格中补充完整的路由配置：

```
[RTA]ip route-static 0.0.0.0 0 198.76.28.2
```

交换机 SW1 采用出厂缺省配置即可。

步骤三：检查连通性

分别在 Client_A 和 Client_B 上 ping Server（IP 地址为 198.76.29.4），其结果为无法 ping 通

产生这种结果的原因是在公网路由器上不可能有私网的路由，从 Server 回应的 ping 响应报文到 RTB 的路由表上无法找到 10.0.0.0 网段的路由

步骤四：配置 Basic NAT

在 RTA 上配置 Basic NAT：

首先通过 ACL 定义允许源地址属于 10.0.0.0/24 网段的流做 NAT 转换，请在如下的空格中填写完整的 ACL 配置命令

```
[RTA]acl number 2000
[RTA-acl-basic-2000]rule 0 permit source 10.0.0.0 0.0.0.255
```

其次配置 NAT 地址池，设置地址池中用于地址转换的地址范围为：198.76.28.11 到 198.76.28.20，请在下面的空格中填写完成的 NAT 地址池配置命令：

```
[RTA]nat address-group 1 198.76.28.11 198.76.28.20
```

在该命令中，数字 1 的含义是：地址池的索引号是 1

最后将地址池与 ACL 关联，并在正确的接口的正确方向上下发，请在下面的空格中填写完整的命令：

[RTA] interface G0/1

[RTA- G0/1] nat outbound 2000 address-group 1 no-pat

在该命令中，参数 no-pat 的含义是：

表示不使用 TCP/UDP 端口信息实现多对多地址转换，也即表示使用一对一地址转换，只转换数据包的地址而不转换端口信息

步骤五：检查连通性

从 Client_A、Client_B 分别 ping Server，其结果是可以 Ping 通

步骤六：检查 NAT 表项

完成步骤五后立即在 RTA 上通过 display nat session 命令查看 NAT 会话信息，依据该信息输出，可以看到该 ICMP 报文的源地址 10.0.0.1 已经转换成公网地址 198.76.28.12，目的端口号和源端口号均为 1024。源地址 10.0.0.2 已经转换成公网地址 198.76.28.11，目的端口号和源端口号均为 512。五分钟后再次通过该命令查看表项，发现 NAT 表项全部消失，产生这种现象的原因是 NAT 表项具有一定的老化时间（aging-time），一旦超过老化时间，NAT 会删除表项。

可以通过 display nat aging-time 命令查看路由器的 NAT 默认老化时间

注意：

步骤六中不同学员实验结果中的 NAT 会话信息中的显示的转换后的公网地址和端口号可能不同，这是正常现象，以实际显示结果为准。

实验任务二：NAPT 配置

私网客户端 Client_A、 Client_B 需要访问公网服务器 Server，但由于公网地址有限，在 RTA 上配置的公网地址池范围为 198.76.28.11～198.76.28.11，因此配置 NAPT，动态地为 Client_A、Client_B 分配公网地址和协议端口。

步骤一：建立物理连接并初始化路由器配置

按实验组网图进行物理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，请学员在用户视图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：基本 IP 地址和路由配置

与实验任务一同样，配置 RTA 和 RTB 相关接口的 IP 地址以及路由

SW1 同样采用出厂缺省配置即可

步骤三：检查连通性

从 Client_A、Client_B ping Server（IP 地址为 198.76.29.4），其结果是 不能 ping 通

步骤四：配置 NAPT

在 RTA 上配置 NAPT：

首先通过 ACL 定义允许源地址属于 10.0.0.0/24 网段的流做 NAT 转换，请在如下的空格中填写完整的 ACL 配置命令

[RTA]acl number 2000

[RTA-acl-basic-2000]rule 0 permit source 10.0.0.0 0.0.0.255

其次配置 NAT 地址池 1，设置地址池中用于地址转换的地址为：198.76.28.11

[RTA-acl-basic-2000]nat address-group 1 198.76.28.11 198.76.28.11

在接口视图下将 NAT 地址池与 ACL 绑定并下发，在配置命令中不需要（需要/不需要）携带 no-pat 参数，意味着 NAT 要对数据包进行端口的转换,请在下面的空格中填写完整的命令：

[RTA] interface G0/1

[RTA- G0/1] nat outbound 2000 address-group 1

步骤五：检查连通性

从 Client_A、Client_B 上分别 ping Server，其结果是 可以 ping 通

步骤六：检查 NAT 表项

完成步骤五后立即在 RTA 上通过 display nat session 命令查看 NAT 会话信息，依据该信息输出，可以看到源地址 10.0.0.1 和 10.0.0.2 转换成的公网地址分别为 198.76.28.11 和 198.76.28.11，10.0.0.1 转换后的端口为 12289，10.0.0.2 转换后的端口为 12288。当 RTA 出接口收到目的地址为 198.76.28.11 的回程流量时，正是用当初转换时赋予的不同的端口来分辩该流量是转发给 10.0.0.1 还是 10.0.0.2。NAPT 正是靠这种方式，对数据包的 IP 层和传输层信息同时进行转换，显著地提高公有 IP 地址的利用效率。

注意：

步骤六中不同学员实验结果中的 NAT 会话信息中的显示的转换后的端口号可能不同，这是正常现象，以实际显示结果为准。

实验任务三：Easy IP 配置

私网客户端 Client_A、Client_B 需要访问公网服务器 Server，使用公网接口 IP 地址动态为 Client_A、Client_B 分配公网地址和协议端口。

步骤一：建立物理连接并初始化路由器配置

按实验组网图进行物理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，请学员在用户视图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：基本 IP 地址和路由配置

与实验任务一同样，配置 RTA 和 RTB 相关接口的 IP 地址以及路由

SW1 同样采用出厂缺省配置即可

步骤三：检查连通性

从 Client_A、Client_B ping Server（IP 地址为 198.76.29.4），其结果是 无法 ping 通

步骤四：配置 Easy IP

在 RTA 上配置 Easy IP:

首先通过 ACL 定义允许源地址属于 10.0.0.0/24 网段的流做 NAT 转换，请在如下的空格中填写完整的 ACL 配置命令

[RTA]acl number 2000

[RTA-acl-basic-2000]rule 0 permit source 10.0.0.0 0.0.0.255

然后在接口视图下江 ACL 与接口关联并下发 NAT，请在如下的空格中填写完整的配置命令：

[RTA] interface G0/1

[RTA- G0/1] nat outbound 2000

步骤五：检查连通性

从 Client_A、Client_B 分别 ping Server，其结果是 能够 ping 通

步骤六：检查 NAT 表项

完成步骤五后立即在 RTA 上通过 display nat session 命令查看 NAT 会话信息，依据该信息输出，可以看到源地址 10.0.0.1 和 10.0.0.2 转换成的公网地址分别为 198.76.28.1 和 198.76.28.1

请思考一个问题：在步骤五中，从 Client_A 能够 ping 通 Server，但是如果从 Server 端 ping Client_A 呢？其结果是无法 ping 通。 导致这种情况的原因是：在 RTA 上始终没有 10.0.0.0/24 网段的路由，所以 Server 直接 ping Client_A 是不可达的。而 Client_A 能 ping 通 Server 是因为，由 Server 回应的 ICMP 回程报文源地址是 Server 的地址 198.76.29.4，但是目的地址是 RTA 的出接口地址 198.76.28.1，而不是 Client_A 的实际源地址 10.0.0.1。也就是说这个 ICMP 连接必须是由 Client 端来发起连接，触发 RTA 做地址转换后转发。还记得我们在 RTA 出接口 Eth 0/1 下发 NAT 配置时的那个 outbound 吗？NAT 操作是在出方向使能有效。所以，如果从 Server 端始发 ICMP 报文 ping Client 端，是无法触发 RTA 做地址转换的。

实验任务四：NAT Server 配置

想让 Server 端能够 ping 通 Client_A，以便 Client_A 对外提供 ICMP 服务，在 RTA 上为 Client_A 静态映射公网地址和协议端口，公网地址为 198.76.28.11

在实验三的基础上继续如下实验

步骤一：检查连通性

从 Server ping Client_A 的私网地址 10.0.0.1，其结果是无法 ping 通。

步骤二：配置 NAT Server

在 RTA 上完成 NAT Server 配置，允许 Client_A 对外提供 ICMP 服务。请在如下空格中完成完整的配置命令：

[RTA] interface G0/1

[RTA- G0/1] nat server protocol icmp global 198.76.28.11 inside 10.0.0.1

步骤三：检查连通性并查看 NAT 表项

从 Server 主动 ping Client_A 的公网地址 198.76.28.11，其结果是可以 ping 通

在 RTA 上通过 display nat server 命令查看 NAT Server 表项，表项信息中显示出地址 198.76.28.11 和地址 10.0.0.1 的一对一的映射关系。

实验23 AAA/SSH

23.1 实验过程

实验任务一：Telnet 用户本地认证、授权、计费配置

步骤一：建立物理连接并运行超级终端

步骤二：配置相关 IP 地址并验证互通性

步骤三：配置 telnet

首先要在路由器上开启设备的 Telnet 服务器功能，请在如下的空格中填写完整的配置命令：

[RTA]telnet server enable

接下来在路由器上完成了如下配置：

[RTA] user-interface vty 0 4

[RTA-ui-vty0-4] authentication-mode scheme

如上配置命令的含义和作用是指定 Telnet 用户进行 AAA 授权认证方式

最后在路由器上创建本地 telnet 用户：用户名 telnet，明文密码 aabbcc，并设置用户的服务类型。请在如下的空格中填写完整的配置命令：

[RTA] local-user telnet

[RTA-luser-telnet] service-type telnet

[RTA-luser-telnet] password simple aabbcc

在配置 Telnet 用户时同时配置如下命令：

[RTA -luser- telnet]level 3

该命令的含义是：指定本地用户的授权级别为 3，也即管理级别。在某些版本上需使用 authorization-attribute level 命令替代 level 命令。

步骤四：配置 AAA

在路由器上配置相关的 AAA 方案为本地认证、授权和计费，请在如下空格中补充完整的配置命令：

[RTA] domain data

如上配置命令的含义是创建名为 data 的域，telnet 用户登录的时候，用户名为 telnet@data

[RTA -isp-data] authentication login local

[RTA -isp-data] authorization login local

[RTA -isp-data] accounting login local

步骤五：验证

在 PCA 上使用 Telnet 登录时输入用户名为 telnet@data，其结果是登录成功而且登录后具有管理员权限

实验任务二：Telnet 用户通过 RADIUS 服务器认证、授权、计费的应用配置

步骤一：建立物理连接并运行超级终端

步骤二：配置相关 IP 地址并验证互通性

步骤三：配置 telnet

首先要在路由器上开启设备的 Telnet 服务器功能，请在如下的空格中填写完整的配置命令：

[RTA] telnet server enable

接下来在路由器上配置 Telnet 用户登录采用 AAA 认证方式，请在如下的空格中补充完整的配置命令：

[[RTA] user-interface vty 0 4

[RTA-ui-vty0-4] authentication-mode scheme

步骤四：配置 Radius 方案

在 RTA 上完成如下配置：

[RTA] radius scheme rad

该配置命令的含义是创建名为 rad 的 RADIUS 方案并进入其视图，在该方案中将指明 RADIUS 认证/授权/计费服务器的 IP 地址、UDP 端口号以及 RADIUS 客户端与之交互所需的一些参数

接下来配置主 RADIUS 认证/授权和计费服务器，其端口号分别为 1812、1813，请在如下空格中补充正确的完整的配置命令：

[RTA-radius-rad] primary authentication 10.10.10.2 1812

[RTA-radius-rad] primary accounting 10.10.10.2 1813

然后配置指定 RADIUS 认证/授权报文/计费报文的共享密钥均为 expert，请在如下空格中补充正确的完整的配置命令：

[RTA-radius-rad] key authentication expert

[RTA-radius-rad] key accounting expert

由于通过 RADIUS 服务器对 MSR 路由器的 telnet 用户进行验证、授权和计费要使用私有的 RADIUS 协议的规程和报文格式进行交互，因此需要配置指定 **extended** 类型的 RADIUS 服务器，请在如下空格中补充正确的配置命令：

[RTA-radius-rad] server-type extended

最后在路由器上配置了如下命令：

[RTA-radius-rad] user-name-format with-domain

如上配置命令的含义是来设置发送给 RADIUS 服务器的用户名格式为*"userid@isp-name"* 的格式，也即要求发送给 RADIUS 服务器的用户名带 ISP 域名

在路由器上配置 NAS 的 IP 地址，也即指定发送 RADIUS 报文使用的源地址，请在如下的空格中补充正确的配置命令：

[RTA-radius-rad] nas-ip 10.10.10.1

步骤五：配置 ISP 域的 AAA 方案

在 ISP 域 aaa 下为 login 用户配置认证、授权和计费方案为 RADIUS 的方案，方案名为 rad，请在如下空格中补充完整的配置命令：

[RTA] domain aaa

[RTA-isp-aaa] authentication default radius-scheme rad

[RTA-isp-aaa] authorization default radius-scheme rad

[RTA-isp-aaa] accounting default radius-scheme rad

步骤六：配置 RADIUS 服务器

需要在 RADIUS 服务器上配置 TELNET 登录用户名，并设定其管理权限，同时还要设置与交换机交互 RADIUS 报文的共享密钥等，相关 RADIUS 服务器的配置请参考本书附录。

本实验中，设定 Telnet 用户名为 123，密码为 456，管理权限为 3，也即具有管理员权限。

步骤七：验证

在 Telnet 客户端按照提示输入用户名及密码，其结果是成功登录并具有管理员权限

实验任务三：SSH password 认证配置

步骤一：建立物理连接并初始化路由器配置

步骤二：配置基本 IP 地址

将路由器连接 PC 的接口 G0/0 配置 IP 地址 192.168.1.1/30，那么这种情况下，PC 的 IP 地址应该正确配置为 192.168.1.2/30

步骤三：创建本地 SSH 登录用户

在路由器上创建本地用户 client，密码使用明文 pwdpwd,如果要确保该用户在通过 SSH 认证登录后具有管理员的权限，那么该用户的访问命令级别为 3，请在下面的空格中补充完整的本地用户配置命令：

[RTA] local-user client

[RTA -luser-client] password simple pwdpwd

[RTA -luser-client] service-type ssh

[RTA -luser-client] level 3

步骤四：配置登录用户界面的 AAA 认证方式

配置 SSH 客户端登录用户界面的认证方式为 AAA 认证，同时设置路由器上远程用户登录协议为 SSH，请在下面的空格中补充完整的配置命令：

```
[RTB]user-interface vty 0 4
[RTB-ui-vty0-4]authentication-mode scheme
[RTB-ui-vty0-4]protocol inbound ssh
```

步骤五：配置生成 DSA 或 RSA 密钥

服务器端的 DSA 或 RSA 密钥对，用于在密钥和算法协商阶段生成会话 ID，以及客户端认证服务器，请在正确的视图下配置服务器端生成 DSA 以及 RSA 密钥。

配置生成 RSA 密钥对：

[RTA] public-key local create rsa

配置生成 DSA 密钥对：

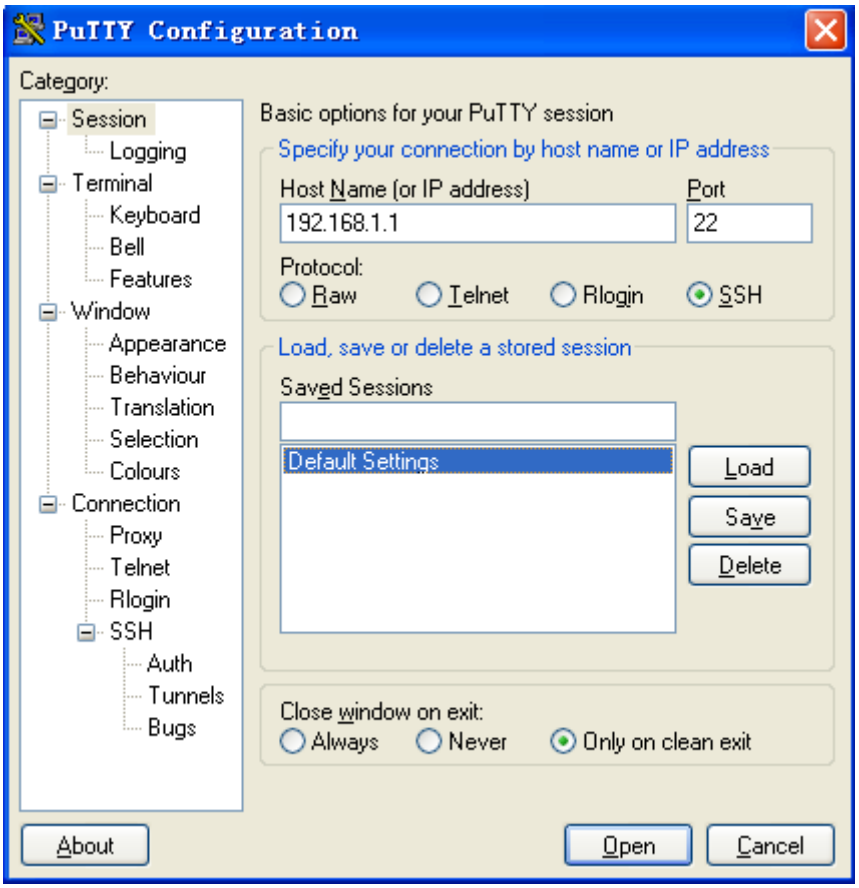
[RTA] public-key local create dsa

配置使能 SSH 服务器功能：

[RTA] ssh server enable

步骤六：SSH 登录验证

使用 SSH client 软件 PuTTY，打开 PuTTY.exe 程序，出现所示的客户端配置界面。在“Host Name（or IP address）”文本框中输入 SSH 服务器的 IP 地址为 192.168.1.1，如下：



然后单击【Open】按钮。按提示输入登录用户名及密码，其结果是：

可以成功登录路由器，登录后具有管理员权限

实验24 交换机端口安全技术

实验任务一：配置 802.1X

步骤一：建立物理连接并初始化交换机配置

步骤二：检查互通性

步骤三：配置 802.1X 协议

实现在交换机 SWA 上启动 802.1X 协议：

首先需要分别在全局和端口开启 802.1X 认证功能，请在下面的空格中补充完整的命令：

[SWA] dot1x

[SWA]dot1x interface e1/0/1 e1/0/2

其次在 SWA 上创建本地 802.1X 用户，用户名为 abcde”，密码为明文格式的 12345，该用户的服务类型 service-type 是 lan-access。请在如下的空格中完成该本地用户的配置命令：

[SWA]local-user abcde

[SWA-luser-h3c]service-type lan-access

[SWA-luser-h3c]password simple 12345

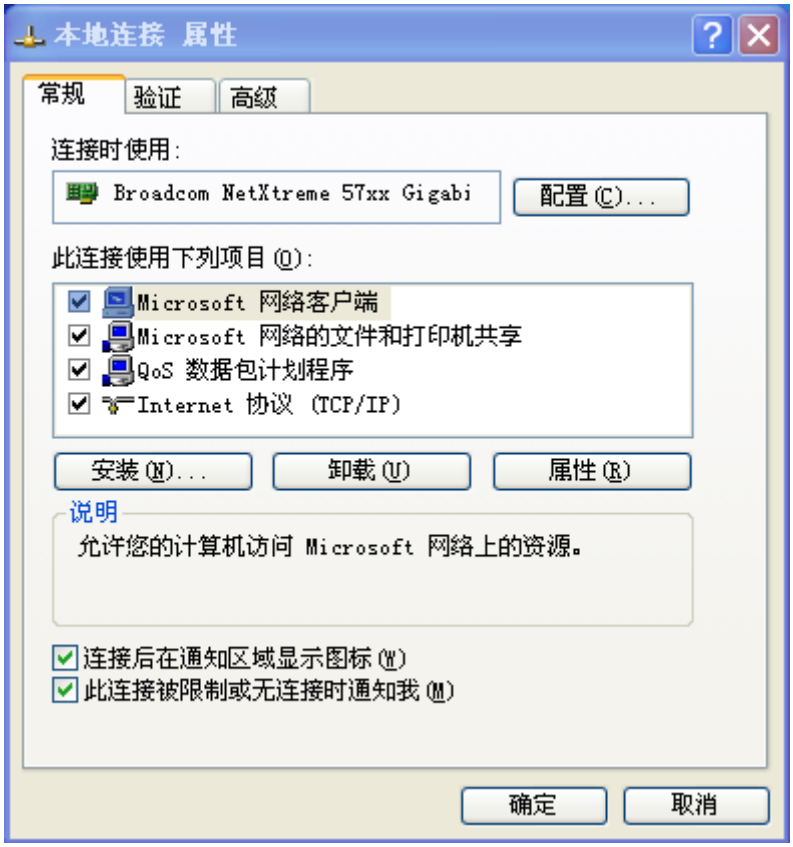
步骤四：802.1X 验证

配置完成后，再次在 PCA 上用 ping 命令来测试到 PCB 的互通性，其结果是 PCA 与 PCB 不能够互通。

导致如上结果的原因是交换机上开启了 802.1X 认证，需要在客户端配置 802.1X 认证相关属性。

PC 可以使用 802.1X 客户端软件或 Windows 系统自带客户端接入交换机。本实验以 Windows 系统自带客户端为例说明如何进行设置。

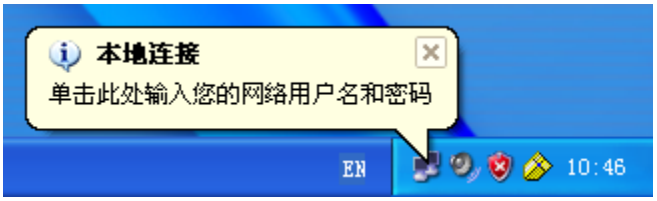
在 Windows 操作系统的【控制面板】中选择【网络和 Internet 连接】，选取【网络连接】中的【本地连接】，点击【属性】，如下所示：



再选取【验证】，并勾选【启用此网络的 IEEE802.1x 验证】，如下所示：

然后点击【确定】，保存退出。

等待几秒钟后，屏幕右下角会自动弹出要求认证的相应提示，如下所示：



按提示要求点击，系统弹出对话框，要求输入用户名和密码，如下所示：

在对话框中输入用户名 abcde 和密码 12345 后，点击【确定】，系统提示通过验证。

在 PCA 与 PCB 都通过验证后，在 PCA 上用 ping 命令来测试到 PCB 的互通性。结果是 PCA 与 PCB 能够互通

注意：

如果 Windows 系统长时间没有自动弹出要求认证提示，或认证失败需要重新认证，可以将电缆断开再连接，以重新触发 802.1X 认证过程。

实验任务二：配置端口隔离

步骤一：建立物理连接并初始化交换机配置

步骤二：检查互通性

步骤三：配置端口隔离

在交换机上启用端口隔离，设置端口 Ethernet1/0/1、Ethernet1/0/2 为隔离组的普通端口，端口 Ethernet1/0/24 为隔离组的上行端口。

配置 SWA：

[SWA] interface Ethernet 1/0/1

[SWA-Ethernet1/0/1] port-isolate enable

[SWA] interface Ethernet 1/0/2

[SWA-Ethernet1/0/2] port-isolate enable

[SWA] interface Ethernet 1/0/24

[SWA-Ethernet1/0/2] port-isolate uplink-port

配置完成后，通过 display port-isolate group 命令查看显示隔离组的信息。

步骤四：端口隔离验证

配置完成后，再次在 PCA 上用 ping 命令测试到 PCB 得互通性，其结果是 PCA 与 PCB 不能互通

然后将 PCB 从端口 Ethernet1/0/2 断开，把 PCB 连接到隔离组的上行端口 Ethernet1/0/24 上，再用 ping 命令测试，其结果是 PCA 与 PCB 可以互通

实验任务三：配置端口绑定

步骤一：建立物理连接并初始化路由器配置

步骤二：配置端口绑定

配置 PCA 的 IP 地址为 172.16.0.1/24，PCB 的 IP 地址为 172.16.0.2/24

分别查看并记录 PCA 和 PCB 的 MAC 地址，

之后在交换机 SWA 上启用端口绑定，设置端口 Ethernet1/0/1 与 PCA 的 MAC 地址绑定，端口 Ethernet1/0/2 与 PCB 的 MAC 地址绑定， 请在如下空格中补充完整的命令：

[SWA] interface ethernet 1/0/1

[SWA-Ethernet1/0/1] user-bind mac-addr 001C-233D-5695

[SWA] interface ethernet 1/0/2

[SWA-Ethernet1/0/2] user-bind mac-addr 0013-728E-4751

配置完成后，通过执行 display user-bind 命令查看已设置绑定的信息。

步骤三：端口绑定验证

在 PCA 上用 ping 命令来测试到 PCB 的互通性，其结果是 PCA 与 PCB 可以互通

断开 PC 与交换机间的连接，然后将 PCA 连接到端口 Ethernet1/0/2，PCB 连接到端口 Ethernet1/0/1。再重新用 ping 命令来测试 PCA 到 PCB 的互通性。其结果是 PCA 与 PCB 不能互通

注意：

未配置端口绑定的端口允许所有报文通过。

步骤二中的 MAC 地址以学员实际操作的 PC 的 MAC 地址为准。

实验25 IPSec

实验任务一：配置采用 IKE 方式建立 IPsec SA

步骤一：建立物理连接并初始化路由器配置

步骤二：基本 IP 地址和路由配置

依据实验组网图完成 RTA、RTB、RTC、PCA、PCB 的 IP 地址配置。

在 RTA 上要配置去往 PCB 的静态路由，请在下面的空格中补充完整的配置：

[RTA]ip route-static 0.0.0.0 0.0.0.0 2.2.2.2

在 RTB 上要配置去往 PCA 的静态路由，请在下面的空格中补充完整的配置：

[RTB]ip route-static 0.0.0.0 0.0.0.0 3.3.3.2

在 RTC 上需要配置两条静态路由才能确保网络互通，请在下面的空格中补充完整的配置：

[RTC] ip route-static192.168.1.0 255.255.255.0 2.2.2.1

[RTC] ip route-static192.168.2.0 255.255.255.0 3.3.3.1

配置完成后，在 PCA 和 PCB 上使用 PING 测试他们之间的互通性，其结果是可以互通。

步骤三：定义访问控制列表

要对 PCA 代表的子网与 PCB 代表的子网之间的数据流进行安全保护，那么需要定义访问控制列表识别 PCA 与 PCB 之间的数据流。

在 RTA 和 RTB 上配置高级（基本/高级）访问控制列表，定义子网 192.168.1.0/24 与 192.168.2.0/24 子网之间的数据流。

配置 RTA 访问控制列表，请在下面空格补充完整配置：

[RTA] acl number 3101

[RTA-acl-adv-3101] rule permit ip source 192.168.1.0 0.0.0.255 destination

192.168.2.0 0.0.0.255

配置 RTB 访问控制列表，请在下面空格补充完整配置：

[RTB] acl number 3101

[RTB-acl-adv-3101] rule permit ip source 192.168.2.0 0.0.0.255 destination

192.168.1.0 0.0.0.255

步骤四：定义安全提议

安全提议保存 IPSec 需要使用的特定安全协议、加密/认证算法以及封装模式，为 IPSec 协商 SA 提供各种安全参数。

在 RTA 上配置定义安全提议，请在空格处补充完整的配置命令。

创建名为 tran1 的安全提议：

[RTA] ipsec proposal tran1

定义报文封装形式采用隧道模式：

[RTA-ipsec-proposal-tran1] encapsulation-mode tunnel

定义安全协议采用 ESP 协议：

[RTA-ipsec-proposal-tran1] transform esp

定义加密算法采用 DES，认证算法采用 HMAC-SHA-1-96：

[RTA-ipsec-proposal-tran1] esp encryption-algorithm des

[RTA-ipsec-proposal-tran1] esp authentication-algorithm sha1

在 RTB 上完成如上同样的安全参数配置，除安全提议名称配置可以不同，其他参数配置均和 RTA 配置一致。

步骤五：配置 IKE 对等体

1. 在 RTA 上创建名为 test 的对等体：

[RTA] ike peer test

配置预共享密钥为 abcde：

[RTA-ike-peer-test] pre-shared-key abcde

指定对端网关设备的 IP 地址：

[RTA-ike-peer-test] remote-address 3.3.3.1

2. 在 RTB 上创建名为 test 的对等体：

[RTB] ike peer test

配置预共享密钥为 abcde：

[RTB-ike-peer-test] pre-shared-key abcde

指定对端网关设备的 IP 地址：

[RTB-ike-peer-test] remote-address 2.2.2.1

步骤六：创建安全策略

安全策略规定了对什么样的数据流采用什么样的安全提议。

1. 在 RTA 上创建安全策略：

[RTA] ipsec policy RT 10 isakmp

如上配置命令中 RT 、10、isakmp 的含义分别为：

RTA 是安全策略的名字 ，10 是安全策略的顺序号，isakmp 表示通过 IKE 协商方式建立安全联盟。

定义安全策略引用访问控制列表：

[RTA-ipsec-policy-isakmp-RT-10] security acl 3101

定义安全策略引用安全提议，在空格处补充完整配置：

[RTA-ipsec-policy-isakmp-RT-10] proposal tran1

定义安全策略引用 IKE 对等体，在空格处补充完整配置：

[RTA-ipsec-policy-isakmp-RT-10] ike-peer test

2. 在 RTB 上完成同样如上配置。

步骤七：在接口上引用安全策略组

在 RTA 的 G0/1 接口上引用安全策略组才能使 IPSEC 配置生效，请在下面的空格中补充完整的配置：

[RTA] interface g0/1

[RTA-GigabitEthernet0/1]ipsec policy RT

配置 RTB 接口上引用安全策略组：

[RTB] interface g0/1

[RTB-GigabitEthernet0/1]ipsec policy RT

步骤八：验证 IPSec 加密

在 RTB 上执行 ping -a 192.168.2.1 192.168.1.1，其结果是可以 ping 通。

然后在 RTB 上使用 display ipsec sa 命令查看安全联盟的相关信息，根据输出信息补充如下空格：

IPsec policy name: "rt"

sequence number: 10

mode: isakmp

---

connection id: 3

encapsulation mode: tunnel

perfect forward secrecy: None

tunnel:

local address: 3.3.3.1

remote address: 2.2.2.1

Flow :

sour addr: 192.168.2.0/255.255.255.0 port: 0 protocol: IP

dest addr: 192.168.1.0/255.255.255.0 port: 0 protocol: IP

可以在 RTB 上通过命令 display ike sa 查看 IKE SA 的详细信息，根据该命令的输出信息可以看到：peer 的 ip 地址为 2.2.2.1，结果显示中 phase 1 和 phase 2 的 flag 标志为 RD|ST。

通过如上命令输出信息表明数据流已经匹配 IPSEC 安全隧道。

可以在 RTB 上执行 display ipsec statistics 来查看 IPSec 处理报文的统计信息，执行该命令后，记录下输出信息中的 input/output security packets、input/output security bytes 项目数值，然后再次在 RTB 上执行 ping -a 192.168.2.1 192.168.1.1，待该 ping 操作结束后，再次查看输出信息中的 input/output security packets、input/output security bytes 项目数值，发现数值增加。说明已经匹配 IPSEC 安全隧道。

可以通过执行 display ipsec session 命令来查看 IPSec 会话的信息，根据其输出结果，可以看到 session flow 的匹配次数以及该 session 得 Sour addr 和 Dest Addr。

通过执行 display ipsec tunnel 命令来查看 IPSec 隧道的信息 。

注意：

步骤八中 display ipsec sa 命令查看安全联盟的相关信息的输出信息中，sequence number 以及 connection id 可能会与本例中显示不同，这是正常现象，以实际实验输出结果为准。

实验26 VRRP

实验任务一：VRRP 单备份组配置

步骤一：建立物理连接并初始化路由器与交换机配置

步骤二：基本 IP 地址和路由配置

依据实验组网图的标识完成 RTA、RTB、RTC、PCA、PCB 的 IP 地址配置，要实现 VRRP 备份的要求，那么 PCA 的网关地址应设置为 192.168.1.3,PCB 的网关地址应设置为 192.168.2.1

为了配置简单，在 RTA、RTB、RTC 上运行 OSPF，所有接口网段都在 OSPF area 0 中发布。

SWA 采取出厂默认配置。

完成如上配置后，用 ping 命令检查互通性：

PCA ping RTA 上 G0/0 接口 IP 地址，其结果是 可以 ping 通

PCA ping RTB 上 G0/0 接口 IP 地址，其结果是 可以 ping 通

步骤三：配置 VRRP

创建 VRRP 备份组的同时，需要在接口视图下配置备份组的虚拟 IP 地址，并且保证配置的虚拟 IP 地址与 RTA 和 RTB G0/0 接口的 IP 地址在（在/不在）同一网段，请在如下空格中补充完整的配置虚拟 IP 地址的命令：

配置 RTA 虚拟 IP 地址：

[RTA- GigabitEthernet0/0] vrrp vrid 1 virtual-ip 192.168.1.3

配置 RTB 虚拟 IP 地址：

[RTB- GigabitEthernet0/0] vrrp vrid 1 virtual-ip 192.168.1.3

PCA ping 自己的网关地址，其结果是不能 ping 通,产生这种结果的原因是 MSR 路由器在缺省情况下不允许能够 ping 通 VRRP 虚地址，要改变这种结果，需要在 RTA、RTB 上增加配置命令，请在下面的空格中填写完整的配置命令：

[RTA]vrrp ping-enable

[RTB]vrrp ping-enable

接下来配置备份组优先级以确保在初始情况下，RTA 为 Master 路由器承担业务转发，在 MSR 路由器上 VRRP 备份组的缺省优先级是 100，要确保 RTA 为 VRRP 备份组 Master 路由器，那么 RTA 在该备份组中的优先级应该大于（大于/小于）RTB 在该备份组中的优先级。请在如下空格中补充完整的命令配置路由器备份组优先级

配置 RTA 备份组优先级为 120：

[RTA- GigabitEthernet0/0] vrrp vrid 1 priority 120

配置 RTB 备份组优先级为 100：

[RTB- GigabitEthernet0/0] vrrp vrid 1 priority 100 RTB 不需此配置也可以，缺省的备份组优先级就是 100.

步骤四：验证 VRRP

在 PCA 上用 ping 检测到 PCB 得可达性，其结果是可以 ping 通

在 RTA 上通过命令 display vrrp 查看 VRRP 备份组状态的摘要信息，通过命令 display vrrp verbose 可以查看 VRRP 备份组状态的详细信息，根据该命令输出，可以看出 RTA 的 VRRP 状态是 Master

在 RTB 上执行同样的命令，可以看到 RTB 的 VRRP 状态是 Backup

此时将 RTA 关机，再次在在 PCA 上用 ping 检测到 PCB 得可达性，其结果是依然可以 ping 通，此时在 RTB 上查看 VRRP 状态，可以看到 RTB 的 VRRP 状态是 Master

实验任务二：VRRP 监视接口配置

步骤一：建立物理连接并初始化路由器与交换机配置

步骤二：基本 IP 地址和路由配置

依据实验组网图的标识完成 RTA、RTB、RTC、PCA、PCB 的 IP 地址配置，要实现 VRRP 备份的要求，那么 PCA 的网关地址应设置为 192.168.1.3,PCB 的网关地址应设置为 192.168.2.1

为了配置简单，在 RTA、RTB、RTC 上运行 OSPF，所有接口网段都在 OSPF area 0 中发布。

SWA 采取出厂默认配置

完成如上配置后，用 ping 命令检查互通性：

PCA ping RTA 上 G0/0 接口 IP 地址，其结果是 可以 ping 通

PCA ping RTB 上 G0/0 接口 IP 地址，其结果是 可以 ping 通

步骤三：配置 VRRP

创建 VRRP 备份组的同时，需要在接口视图下配置备份组的虚拟 IP 地址，并且保证配置的虚拟 IP 地址与 RTA 和 RTB G0/0 接口的 IP 地址在（在/不在）同一网段，请在如下空格中补充完整的配置虚拟 IP 地址的命令：

配置 RTA 虚拟 IP 地址：

[RTA- GigabitEthernet0/0] vrrp vrid 1 virtual-ip 192.168.1.3

配置 RTB 虚拟 IP 地址：

[RTB- GigabitEthernet0/0] vrrp vrid 1 virtual-ip 192.168.1.3

PCA ping 自己的网关地址，其结果是不能 ping 通,产生这种结果的原因是 MSR 路由器在缺省情况下不允许能够 ping 通 VRRP 虚地址，要改变这种结果，需要在 RTA、RTB 上增加配置命令，请在下面的空格中填写完整的配置命令：

[RTA]vrrp ping-enable

[RTB]vrrp ping-enable

接下来配置备份组优先级以确保在初始情况下，RTA 为 Master 路由器承担业务转发，在 MSR 路由器上 VRRP 备份组的缺省优先级是 100，要确保 RTA 为 VRRP 备份组 Master 路由器，那么 RTA 在该备份组中的优先级应该大于（大于/小于）RTB 在该备份组中的优先级。请在如下空格中补充完整的命令配置路由器备份组优先级

配置 RTA 备份组优先级为 120：

[RTA- GigabitEthernet0/0] vrrp vrid 1 priority 120

配置 RTB 备份组优先级为 100：

[RTB- GigabitEthernet0/0] vrrp vrid 1 priority 100 RTB 不需此配置也可以，缺省的备份组优先级就是 100.

步骤四：配置 VRRP 指定被监视的接口

在 RTA 和 RTB 上的 GigabitEthernet0/0 接口下配置 VRRP 监视上行出口 Serial1/0，当上行出口 Serail 1/0 出现故障时，路由器的优先级自动降低 30，以低于处于备份组的路由器优先级，从而实现主备倒换。请在下面的空格中补充完整的命令：

配置 RTA：

[RTA- GigabitEthernet0/0] vrrp vrid 1 track interface Serial1/0 reduced 30

配置 RTB：

[RTB- GigabitEthernet0/0] vrrp vrid 1 track interface Serial1/0 reduced 30

然后在 RTA、RTB 上都做了如下的配置：

[RTA- GigabitEthernet0/0] vrrp vrid 1 timer advertise 5

[RTB- GigabitEthernet0/0] vrrp vrid 1 timer advertise 5

该配置命令的含义是设置备份组中的 Master 路由器发送 VRRP 通告报文的时间间隔为 5 秒

[RTA- GigabitEthernet0/0] vrrp vrid 1 preempt-mode timer delay 5

[RTB- GigabitEthernet0/0] vrrp vrid 1 preempt-mode timer delay 5

该配置命令的含义是配置备份组中的路由器工作在抢占方式，并配置抢占延迟时间为 5 秒

步骤五：验证 VRRP

在 PCA 上用 ping 检测到 PCB 得可达性，其结果是 可以 ping 通

在 RTA 上通过命令 display vrrp 查看 VRRP 备份组状态的摘要信息，通过命令 display vrrp verbose 可以查看 VRRP 备份组状态的详细信息，根据该命令输出，可以看出 RTA 的 VRRP 状态是 Maste，路由器优先级是 120

在 RTB 上执行同样的命令，可以看到 RTB 的 VRRP 状态是 BACKUP,路由器优先级是 100

此时将 RTA 连接 RTC 的接口 Serail 1/0 线缆断开，再次在在 PCA 上用 ping 检测到 PCB 得可达性，其结果是依然可以 ping 通，此时在 RTA 上查看 VRRP 状态，可以看到 RTA 的 VRRP 状态是 Backup，路由器优先级是 90； 在 RTB 上查看 VRRP 状态，可以看到 RTB 的 VRRP 状态是 Master，路由器优先级是 100。

从如上显示信息可以看出，由于上行接口 Serail 1/0 出现故障 VRRP 备份主进行了主备倒换。

实验27 链路备份和路由备份

实验任务一：配置链路备份

本实验主要目标是实现 PCA 与 PCB 通过 RTA 和 RTB 互 1 通，同时把 RTA 的接口 Serial2/1 和 G0/0 配置为主接口 Serial2/0 的备份接口，并优先使用备份接口 Serial2/1。而且设置主接口与备份接口相互切换的延时

步骤一：建立物理连接并初始化路由器配置

按实验组网图进行物理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，请学员在用户视图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：基本 IP 地址和路由配置

依据实验组网图的标识完成 RTA、RTB、PCA、PCB 的 IP 地址配置，其中 PCA 的网关地址应设置为 192.168.1.1,PCB 的网关地址应设置为 192.168.2.1

配置 RTA 和 RTB 的路由，依据组网图，在 RTA 和 RTB 上需要配置三条下一跳不相同(相同/不相同)的静态路由，请在如下空格中补充完整的 RTA 和 RTB 的静态路由配置：

配置 RTA 静态路由：

[RTA]ip route-static 192.168.2.0 24 2.2.2.2

[RTA]ip route-static 192.168.2.0 24 3.3.3.2

[RTA]ip route-static 192.168.2.0 24 4.4.4.2

配置 RTB 静态路由：

[RTB]ip route-static 192.168.1.0 24 2.2.2.1

[RTB]ip route-static 192.168.1.0 24 3.3.3.1

[RTB]ip route-static 192.168.1.0 24 4.4.4.1

配置完成后，在 PCA 上 ping PCB，其结果应该是可达

步骤三：配置链路备份

要在 RTA 上实现链路备份配置，需要在接口视图下通过 standby interface 命令完成；而要实现优先使用备份接口 Serial 2/1,也即备份接口 Serial2/1 和 G0/0 有不同的备份优先级，那么在配置如上命令时需要加入 priority 参数。请在如下空格中补充完整的配置命令实现 RTA 的接口 Serial2/1 和 G0/0 配置为主接口 Serial2/0 的备份接口，并优先使用备份接口 Serial2/1：

[RTA] interface serial 2/0

[RTA -Serial2/0] standby interface serial 2/1 30

[RTA -Serial2/0] standby interface g0/0 20

同时在 RTA 上做了如下配置：

[RTA-Serial2/0] standby timer delay 10 10

如上配置命令的含义是：设置主备接口切换的延时均为 10 秒，即从主接口切换到备份接口的延时和从备份接口切换到主接口的延时都是 10 秒。

步骤四：验证链路备份

完成步骤三后，在 PCA 上 ping　PCB，其结果是 可以 ping 通

在 PCA 上可以通过 display standby state 命令查看主接口与备份接口的状态，根据该命令的输出信息补充下面的空格信息：

Interface	Interfacestate	Standbystate	Pri
Serial2/0	UP	MUP	
Serial2/1	STANDBY	STANDBY	30
GigabitEthernet0/0	STANDBY	STANDBY	20

此时在 RTA 上通过 shutdown 命令将端口 Serial2/0 手工关闭，然后 10 秒后，继续查看主接口与备份接口的状态，根据该命令的输出信息补充下面的空格信息：

Interface	Interfacestate	Standbystate	Pri
Serial2/0	DOWN	MDOWN	
Serial2/1	UP	UP	30
GigabitEthernet0/0	STANDBY	STANDBY	20

此时，在 PCA 上 ping PCB,其结果是依然可以 ping 通

然后在保持端口 Serial2/0 关闭，将端口 Serial2/1 手动关闭，然后 10 秒后，继续查看主接口与备份接口的状态，根据该命令的输出信息补充下面的空格信息：

Interface	Interfacestate	Standbystate	Pri
Serial2/0	DOWN	MDOWN	
Serial2/1	DOWN	DOWN	30

GigabitEthernet0/0	UP	UP	20

此时，在 PCA 上 ping PCB,其结果是依然可以 ping 通

注意：

步骤三种配置的接口备份优先级数值仅供参考，学员配置的时候只需要确保 Serial2/1 的备份优先级数值大于 G0/0 即可。

实验任务二：配置路由备份

依据实验组网图，在 RTA—RTC--RTB 之间的通过运行 RIP 动态路由协议，而 RTA—RTB 之间运行静态路由协议，通过配置实现 PCA 访问 PCB 优先选择静态路由路径，其次选择 RIP 路由路径

步骤一：建立物理连接并初始化路由器配置

按实验组网图进行物理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，请学员在用户视图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：基本 IP 地址配置

依据实验组网图的标识完成 RTA、RTB、RTC、PCA、PCB 的 IP 地址配置，其中 PCA 的网关地址应设置为 192.168.1.1,PCB 的网关地址应设置为 192.168.2.1

配置完成后，使用 ping 命令检测任意两台直连的设备之间的互通性，其结果应当是直连的设备互连接口之间可以 ping 通。

步骤三：配置 RIP

在 RTA---RTC—RTB 的互连接口以及 RTA 和 RTB 的 G1/0 接口上运行 RIP V2，

在如下的空格中完成 RTA 上 RIP V2 的配置：

```
[RTA] rip
[RTA-rip-1] network 192.168.1.0
[RTA-rip-1] network 3.3.3.0
[RTA-rip-1] undo summary
[RTA-Serial5/0]rip version 2
[RTA-GigabitEthernet0/1]rip version 2
```

在如下的空格中完成那个 RTB 上 RIPV2 的配置：

```
[RTB] rip
[RTB-rip-1] network 192.168.2.0
[RTB-rip-1] network 2.2.2.0
[RTB-rip-1] undo summary
[RTB-Serial5/0]rip version 2
[RTB-GigabitEthernet0/1]rip version 2
```

在如下的空格中完成那个 RTC 上 RIPV2 的配置：

```
[RTC] rip
[RTC-rip-1] network 2.2.2.0
[RTC-rip-1] network 3.3.3.0
[RTC-rip-1] undo summary
[RTA-Serial5/0]rip version 2
[RTA-Serial5/1]rip version 2
```

配置完成后，在 RTA 上查看全局路由表，可以看到 RTA 的路由表中，有目的网段为 192.168.2.0/24 的路由，其协议优先级为 100，花费 Cost 值为 2。在 RTB 上查看全局路由表，可以看到目的网段为 192.168.1.0/24 的 RIP 路由

PCA 通过 ping 命令检测与 PCB 的互通，其结果是可以 Ping 通

步骤四：配置静态路由

RTA 与 RTB 之间通过 G0/0 互连，在 RTA 与 RTB 上配置静态路由，

要实现 PCA 访问 PCB 优先选择该静态路由，那么应当配置同一目的网段的静态路由的优先级数值小于 RIP 路由协议的优先级值。MSR 上静态路由的优先级缺省是 60，因此缺省值即可满足要求。

[RTA]ip route-static 192.168.2.0 24 4.4.4.2

[RTB]ip route-static 192.168.1.0 24 4.4.4.1

配置完成后在 RTA 上查看全局路由表，可以看到目的网段为 192.168.2.0/24 的路由有 一 条，是静态路由，其优先级是 60 ；在 RTB 上查看全局路由表，可以看到目的网段为 192.168.1.0/24 的路由有 一 条，是 静态 路由，其优先级是 60 。

PCA 通过 ping 命令检测与 PCB 的互通，其结果是可以 Ping 通

步骤五：路由备份验证

步骤四中，PCA 可以 ping 通 PCB 是通过静态路由实现的，因为 RTA 的路由表中没有去往 PCB 网段的 RIP 路由，同理，RTB 的路由表中也没有去往 PCA 网段的 RIP 路由

断开 PCA 与 PCB 之间的 G0/0 的链路，然后在 RTA 上查看全局路由表，可以看到目的网段为 192.168.2.0/24 的路由是一条 RIP 路由，在 RTB 上查看全局路由表，可以看到目的网段为 192.168.1.0/24 的路由也是一条 RIP 路由。然后 PCA 通过 ping 命令检测与 PCB 的胡同，其结果是可以 ping 通

然后再次连接 RTA 与 RTB 之间的 G0/0 链路，然后在 RTA 上查看全局路由表，可以看到目的网段为 192.168.2.0/24 的路由是一条静态路由，在 RTB 上查看全局路由表，可以看到目的网段为 192.168.1.0/24 的路由也是一条静态路由。然后 PCA 通过 ping 命令检测与 PCB 的胡同，其结果是可以 ping 通

如上的实验验证了静态路由与 RIP 之间的备份

实验28 网络管理基本操作

本实验主要内容为观察网管系统软件显示信息，并记录之。具体信息以网管软件显示信息为准，无特别参考内容。

实验29 综合组网

实验任务一：内网部署

步骤一：总部内网部署

第1步： 按照前期的命名规划及端口描述个给每台设备命名并添加端口描述，此处只给出单台设备的命名及端口描述，命令如下：

[H3C]sysname BJ-MSR3020-0

进入互连端口，按照设计要求添加端口描述

[BJ-MSR3020-0] interface GigabitEthernet0/0

[BJ-MSR3020-0-GigabitEthernet0/0] description Link-To-BJ-S5626-0-G1/0/1

第2步： 配置核心交换机与服务器区交换机的端口聚合，参与聚合的端口为 G1/0/2 与 G1/0/3，使用基于手工方式的链路聚合。具体配置如下：

核心交换机 BJ-S5626C-0 配置：

创建手工聚合组 1

[BJ-S5626C-0]link-aggregation group 1 mode manual

将 G1/0/2 和 G1/0/3 加入聚合组 1

[BJ-S5626C-0] interface GigabitEthernet 1/0/2

[BJ-S5626C-0-GigabitEthernet1/0/2] port link-aggregation group 1

[BJ-S5626C-0-GigabitEthernet1/0/2] interface GigabitEthernet 1/0/3

[BJ-S5626C-0-GigabitEthernet1/0/3] port link-aggregation group 1

服务器区交换机 BJ-S5116P-0 配置：

创建手工聚合组 1

[BJ-S5116P-0]link-aggregation group 1 mode manual

将 G1/0/1 和 G1/0/2 加入聚合组 1

[BJ-S5116P-0] interface GigabitEthernet 1/0/1

[BJ-S5116P-0-GigabitEthernet1/0/1] port link-aggregation group 1

[BJ-S5116P-0-GigabitEthernet1/0/1] interface GigabitEthernet 1/02

[BJ-S5116P-0-GigabitEthernet1/0/2] port link-aggregation group 1

查看端口聚合摘要信息，验证链路聚合是否成功

```
<BJ-S5116P-0>dis link-aggregation summary
Aggregation Group Type:D -- Dynamic, S -- Static , M -- Manual
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor ID: 0x8000, 000f-e254-49d5
  AL  AL   Partner ID          Select Unselect Share Master
  ID  Type                   Ports  Ports    Type  Port
--------------------------------------------------------------------------------
----------------------------
  1   M    none               2      0      Shar  GigabitEthernet 1/0/1
```

第3步：　根据前期的 VLAN 及端口分配规划，在各接入交换机上配置 VLAN，并将上行接口配置为 Trunk 链路，允许相关 VLAN 通过。本步骤以 BJ-S3152TP-0 为例演示如何配置。

创建 VLAN 10

[BJ-S3152TP-0]vlan 10

将 E1/0/1 到 E1/0/30 端口分配给 VLAN 10

[BJ-S3152TP-0-vlan10]port e1/0/1 to e1/0/30

创建 VLAN 20

[BJ-S3152TP-0-vlan10]vlan 20

将 E1/0/31 到 E1/0/48 端口分配给 VLAN 20

[BJ-S3152TP-0-vlan10]port e1/0/31 to e1/0/48

进入上行端口 G1/1/1

[BJ-S3152TP-0-vlan10]int g1/1/1

设置上行端口类型为 Trunk

[BJ-S3152TP-0-GigabitEthernet1/1/1] port link-type trunk

设置上行 G1/1/1 端口允许 VLAN 10、VLAN 20 通过

[BJ-S3152TP-0-GigabitEthernet1/1/1] port trunk permit trunk vlan 10 20

第4步：　为了让 VLAN 之间能够通信，在核心交换机 BJ-S5626C-0 上为每个 VLAN 配置 IP 地址，启动 VLAN 间路由功能，具体 IP 地址见前期规划。

进入 VLAN 10 的三层虚接口

[BJ-S5626C-0]int vlan 10

为 VLAN 10 三层接口配置 IP 地址

[BJ-S5626C-0-Vlan-interface10]ip add 192.168.1.254　24

进入 VLAN 20 的三层虚接口

[BJ-S5626C-0-Vlan-interface10]int vlan 20

为 VLAN 20 三层接口配置 IP 地址

[BJ-S5626C-0-Vlan-interface20]ip add 192.168.2.254　24

进入 VLAN 30 的三层虚接口

[BJ-S5626C-0-Vlan-interface20]int vlan 30

为 VLAN 30 三层接口配置 IP 地址

[BJ-S5626C-0-Vlan-interface30]ip add 192.168.3.254　24

进入 VLAN 40 的三层虚接口

[BJ-S5626C-0-Vlan-interface30]int vlan 40

为 VLAN 40 三层接口配置 IP 地址

[BJ-S5626C-0-Vlan-interface40]ip add 192.168.4.254　24

进入 VLAN 50 的三层虚接口

[BJ-S5626C-0-Vlan-interface40]int vlan 50

为 VLAN 50 三层接口配置 IP 地址

[BJ-S5626C-0-Vlan-interface50]ip add 192.168.0.1 30

以上配置完成之后，可以通过 ping 命令验证前期的配置是否正确，验证的方法是将 PC 机接入任意一个 VLAN，将 PC 机的 IP 地址修改为所在 VLAN 的 IP 地址。

第5步：　配置 DHCP 协议

开启 DHCP 功能

[BJ-S5626C-0]dhcp enable

创建 VLAN 10　对应的 DHCP 地址池

[BJ-S5626C-0]dhcp server ip-pool vlan10

配置 VLAN 10 地址池动态分配的地址范围

[BJ-S5626C-0-dhcp-pool-vlan10]network 192.168.1.0 mask 255.255.255.0

指定为 VLAN 10 内客户端分配的的网关地址

[BJ-S5626C-0-dhcp-pool-vlan10]gateway-list 192.168.1.254

指定为 VLAN 10 内客户端分配的 DNS 服务器地址

[BJ-S5626C-0-dhcp-pool-vlan10]dns-list 202.102.99.68

[BJ-S5626C-0-dhcp-pool-vlan10]quit

创建 VLAN 20 对应的 DHCP 地址池

[BJ-S5626C-0]dhcp server ip-pool vlan20

配置 VLAN 20 地址池动态分配的地址范围

[BJ-S5626C-0-dhcp-pool-vlan20]network 192.168.2.0 mask 255.255.255.0

指定为 VLAN 20 内客户端分配的 DNS 服务器地址

[BJ-S5626C-0-dhcp-pool-vlan20]dns-list 202.102.99.68

指定为 VLAN 20 内客户端分配的的网关地址

[BJ-S5626C-0-dhcp-pool-vlan20]gateway-list 192.168.2.254

[BJ-S5626C-0-dhcp-pool-vlan20]quit

创建 VLAN 30 对应的 DHCP 地址池

[BJ-S5626C-0]dhcp server ip-pool vlan30

配置 VLAN 30 地址池动态分配的地址范围

[BJ-S5626C-0-dhcp-pool-vlan30]network 192.168.3.0 mask 255.255.255.0

指定为 VLAN 30 内客户端分配的的网关地址

[BJ-S5626C-0-dhcp-pool-vlan30]gateway-list 192.168.3.254

指定为 VLAN 30 内客户端分配的 DNS 服务器地址

[BJ-S5626C-0-dhcp-pool-vlan30]dns-list 202.102.99.68

[BJ-S5626C-0-dhcp-pool-vlan30]quit

配置 DHCP 地址池中不参与自动分配的 IP 地址（网关地址）

[BJ-S5626C-0]dhcp server forbidden-ip 192.168.1.254

[BJ-S5626C-0]dhcp server forbidden-ip 192.168.2.254

[BJ-S5626C-0]dhcp server forbidden-ip 192.168.3.254

如果要在 PC 上测试 DHCP 配置是否成功，需在 PC 机的【开始】|【运行】处输入 CMD 命令进入命令行模式，在此模式下输入 命令可以查看本机 Ipconfig 地址的详细情况。

第6步： 配置交换机的管理地址，在本例中使用 VLAN 1 作为管理 VLAN，接入交换机以 BJ-S5116P-0 为例，其他交换机本部分配置与此类似。

BJ-S5626C-0 交换机：

进入 VLAN 1 的三层虚接口

[BJ-S5626C-0]int vlan 1

为 VLAN 1 三层接口配置 IP 地址

[BJ-S5626C-0-Vlan-interface1]ip add 192.168.0.25 29

BJ-S5116P-0 交换机：

进入 VLAN 1 的三层虚接口

[BJ-S5116P-0]int vlan 1

为 VLAN 1 三层接口配置 IP 地址

[BJ-S5116P-0-Vlan-interface1]ip add 192.168.0.26 29

[BJ-S5116P-0-Vlan-interface1]quit

配置到达上层交换机的路由，下一跳指向核心交换机的管理地址

[BJ-S5116P-0]ip route-static 0.0.0.0 0.0.0.0 192.168.0.25

步骤二：深圳办事处内网部署

第1步： 给设备命名并添加端口描述

SZ-MSR2020-0 路由器：

[H3C]sysname SZ-MSR2020-0

进入各互连端口，按照设计要求添加端口描述

[SZ-MSR2020-0] interface Ethernet0/0

[SZ-MSR2020-0-GigabitEthernet0/0] description Link-To-SZ-S3152TP-0-E1/0/1

SZ-S3152TP-0 交换机：

[H3C]sysname SZ-S3152TP-0

进入各互连端口，按照设计要求添加端口描述

[SZ-S3152TP-0] interface Ethernet 1/0/1

[SZ-S3152TP-0-Ethernet1/0/1] description Link-To-SZ-MSR2020-0-E0/0

第2步： DHCP 配置

在深圳办事处，也使用 DHCP 方式为接入 PC 机分配 IP 地址，DHCP 服务器为 MSR2020 路由器，具体 DHCP 的配置如下：

为 E0/0 接口配置 IP 地址，此地址为内网所有 PC 机的网关

[SZ-MSR2020-0-Ethernet0/0]ip add 192.168.5.254 24

[SZ-MSR2020-0-Ethernet0/0]quit

开启 DHCP 功能

[SZ-MSR2020-0]dhcp enable

创建 DHCP 地址池 1

[SZ-MSR2020-0]dhcp server ip-pool 1

配置地址池动态分配的地址范围

[SZ-MSR2020-0-dhcp-pool-1]network 192.168.5.0 mask 255.255.255.0

指定为客户端分配的的网关地址

[SZ-MSR2020-0-dhcp-pool-1]gateway-list 192.168.5.254

指定为客户端分配的 DNS 服务器地址

[SZ-MSR2020-0-dhcp-pool-1]dns-list 202.102.99.68

[SZ-MSR2020-0-dhcp-pool-1]quit

配置 DHCP 地址池中不参与自动分配的 IP 地址

[SZ-MSR2020-0]dhcp server forbidden-ip 192.168.5.254

[SZ-MSR2020-0]dhcp server forbidden-ip 192.168.5.250

第3步： 交换机管理地址配置

进入 VLAN 1 的三层虚接口

[SZ-S3152TP-0]int vlan 1

为 VLAN 1 三层接口配置 IP 地址

[SZ-S3152TP-0-Vlan-interface1]ip add 192.168.5.250 24

[SZ-S3152TP-0-Vlan-interface1]quit

配置到达上层路由器的路由，下一跳指向路由器接口地址

[SZ-S3152TP-0]ip rout 0.0.0.0 0.0.0.0 192.168.5.254

步骤三：上海研究所内网部署

第1步：　给设备命名并添加端口描述

SH-MSR2020-0 路由器：

[H3C]sysname SH-MSR2020-0

进入各互连端口，按照设计要求添加端口描述

[SH-MSR2020-0] interface Ethernet0/0

[SH-MSR2020-0-GigabitEthernet0/0] description Link-To-SH-S3152TP-0-E1/0/1

SH-S3152TP-0 交换机：

[H3C]sysname SH-S3152TP-0

进入各互连端口，按照设计要求添加端口描述

[SH-S3152TP-0] interface Ethernet 1/0/1

[SH-S3152TP-0-Ethernet1/0/1] description Link-To-SH-MSR2020-0-E0/0

第2步：　DHCP 配置

在上海研究所，也使用 DHCP 方式为接入 PC 机分配 IP 地址，DHCP 服务器为 MSR2020 路由器，具体 DHCP 的配置如下：

为 E0/0 接口配置 IP 地址，此地址为内网所有 PC 机的网关

[SH-MSR2020-0-Ethernet0/0]ip add 192.168.6.254 24

[SH-MSR2020-0-Ethernet0/0]quit

开启 DHCP 功能

[SH-MSR2020-0]dhcp enable

创建 DHCP 地址池 1

[SH-MSR2020-0]dhcp server ip-pool 1

配置地址池动态分配的地址范围

[SH-MSR2020-0-dhcp-pool-1]network 192.168.6.0 mask 255.255.255.0

指定为客户端分配的的网关地址

[SH-MSR2020-0-dhcp-pool-1]gateway-list 192.168.6.254

指定为客户端分配的 DNS 服务器地址

[SH-MSR2020-0-dhcp-pool-1]dns-list 202.102.99.68

[SH-MSR2020-0-dhcp-pool-1]quit

配置 DHCP 地址池中不参与自动分配的 IP 地址

[SH-MSR2020-0]dhcp server forbidden-ip 192.168.6.254

[SH-MSR2020-0]dhcp server forbidden-ip 192.168.6.250

第3步：　交换机管理地址配置

进入 VLAN 1 的三层虚接口

[SH-S3152TP-0]int vlan 1

为 VLAN 1 三层接口配置 IP 地址

[SH-S3152TP-0-Vlan-interface1]ip add 192.168.6.250 24

[SH-S3152TP-0-Vlan-interface1]quit

配置到达上层路由器的路由，下一跳指向路由器接口地址

[SH-S3152TP-0]ip rout 0.0.0.0 0.0.0.0 192.168.6.254

实验任务二：广域网部署

第1步：　BJ-MSR3020-0 配置

[BJ-MSR3020-0]int s1/0

按照规划为 S1/0 接口添加描述

[BJ-MSR3020-0 Serial1/0]description Link-To-SZ-MSR2020-0-S1/0

给 S1/0 接口配置 IP 地址

[BJ-MSR3020-0-Serial1/0]ip add 192.168.0.5 30

[BJ-MSR3020-0]int s1/1

按照规划为 S1/1 接口添加描述

[BJ-MSR3020-0 Serial1/1]description Link-To-SH-MSR2020-0-S1/0

进入 S1/2 接口

[BJ-MSR3020-0-Serial1/1]int s1/2

按照规划为 S1/2 接口添加描述

[BJ-MSR3020-0 Serial1/2]description Link-To-SH-MSR2020-0-S1/1

[BJ-MSR3020-0 Serial1/2]quit

创建并进入 MP-group 0 接口

[BJ-MSR3020-0] interface Mp-group 0

给 MP-group 0 接口配置 IP 地址

[BJ-MSR3020-0- Mp-group0] ip add 192.168.0.9　30

[BJ-MSR3020-0- Mp-group0]int s1/1

将 S1/1 接口加入 MP-group 0

[BJ-MSR3020-0-Serial1/1]ppp mp mp-group 0

进入 S1/2 接口

[BJ-MSR3020-0-Serial1/1] int s1/2

将 S1/1 接口加入 MP-group 0

[BJ-MSR3020-0-Serial1/2]ppp mp mp-group 0

第2步：　SZ-MSR2020-0 配置

[SZ-MSR2020-0]int s1/0

按照规划为 S1/0 接口添加描述

[SZ-MSR2020-0 Serial1/0]description Link-To-BJ-MSR2020-0-S1/0

给 S1/0 接口配置 IP 地址

[SZ-MSR2020-0-Serial1/0]ip add 192.168.0.6 30

第3步：　SH-MSR2020-0 配置

[SH-MSR2020-0]int s1/0

按照规划为 S1/0 接口添加描述

[SH-MSR2020-0 Serial1/0]description Link-To-BJ-MSR3020-0-S1/1

[SH-MSR2020-0-Serial1/0]int s1/1

按照规划为 S1/1 接口添加描述

[SH-MSR2020-0 Serial1/1]description Link-To-BJ-MSR3020-0-S1/2

[SH-MSR2020-0 Serial1/1]quit

创建并进入 MP-group 0 接口

[SH-MSR2020-0] interface Mp-group0

给 MP-group 0 接口配置 IP 地址

[SH-MSR2020-0- Mp-group0] ip add 192.168.0.10 30

将 S1/0 接口加入 MP-group 0

[SH-MSR2020-0- Mp-group0]int s1/0

[SH-MSR2020-0-Serial1/0]ppp mp mp-group 0

将 S1/1 接口加入 MP-group 0

[SH-MSR2020-0-Serial1/0] int s1/1

[SH-MSR2020-0-Serial1/1]ppp mp mp-group 0

实验任务三：路由部署

第1步：　BJ-S5626C-0 交换机路由配置

手工指定 router id，为 VLAN 1 的接口地址

[BJ-S5626C-0]router id 192.168.0.25

[BJ-S5626C-0]ospf

[BJ-S5626C-0-ospf-1]area 1

在区域里发布网段，后面跟的是反掩码，但有些地址我们很难口算出它的反掩码，CMW 提供了这样一个特性：可以将掩码自动转化为反掩码；为此我们演示一下，发布网段时使用掩码，并验证是否能自动转换。

[BJ-S5626C-0-ospf-1-area-0.0.0.1]net 192.168.1.0 255.255.255.0

验证是否能自动将掩码转换成反掩码

[BJ-S5626C-0-ospf-1-area-0.0.0.1]dis this

#

area 0.0.0.1

network 192.168.1.0 0.0.0.255

#

return

继续发布 VLAN 20、VLAN 30、VLAN 40 所在的网段

[BJ-S5626C-0-ospf-1-area-0.0.0.1]net 192.168.2.0　0.0.0.255

[BJ-S5626C-0-ospf-1-area-0.0.0.1]net 192.168.3.0　0.0.0.255

[BJ-S5626C-0-ospf-1-area-0.0.0.1]net 192.168.4.0　0.0.0.255

#发布同 BJ-MSR3020-0 路由器互连接口地址

[BJ-S5626C-0-ospf-1-area-0.0.0.1]net 192.168.0.1　0.0.0.3

#发布交换机管理 VLAN 地址网段

[BJ-S5626C-0-ospf-1-area-0.0.0.1]net 192.168.0.24　0.0.0.7

第2步：　BJ-MSR3020-0 路由器路由配置

创建并进入 loopback 0 接口

[BJ-MSR3020-0]int loop 0

为 loopback 0 接口配置 IP 地址，注意掩码为 32 位

[BJ-MSR3020-0-LoopBack0]ip add 192.168.0.17 32

手工指定 router id

[BJ-MSR3020-0]router id 192.168.0.17

[BJ-MSR3020-0]ospf

创建并进入 area 1

[BJ-MSR3020-0-ospf-1]area 1

发布同 BJ-S5626C-0 的互连网段

[BJ-MSR3020-0-ospf-1-area-0.0.0.1]net 192.168.0.0 0.0.0.3

为了便于管理，发布 loopback 接口地址（作为网管地址）

[BJ-MSR3020-0-ospf-1-area-0.0.0.1]net 192.168.0.17 0.0.0.0

创建并进入 area 0

[BJ-MSR3020-0-ospf-1]area 0

#发布同 SZ-MSR2020-0 及 SH-MSR2020-0 的互连网段

[BJ-MSR3020-0-ospf-1-area-0.0.0.0]net 192.168.0.4 0.0.0.3

[BJ-MSR3020-0-ospf-1-area-0.0.0.0]net 192.168.0.8 0.0.0.3

第3步： SZ-MSR2020-0 路由器路由配置

创建并进入 loopback 0 接口

[SZ-MSR2020-0]int loop 0

为 loopback 0 接口配置 IP 地址，注意掩码为 32 位

[SZ-MSR2020-0-LoopBack0]ip add 192.168.0.18 32

手工指定 router id

[SZ-MSR2020-0]router id 192.168.0.18

[SZ-MSR2020-0]ospf

[SZ-MSR2020-0-ospf-1]area 0

发布同 BJ-MSR3020-0 的互连网段

[SZ-MSR2020-0-ospf-1-area-0.0.0.0]net 192.168.0.4　0.0.0.3

[SZ-MSR2020-0-ospf-1]area 2

发布深圳办事处内网网段地址

[SZ-MSR2020-0-ospf-1-area-0.0.0.2]net 192.168.5.0 0.0.0.255

发布 loopback 地址（作为网管地址）

[SZ-MSR2020-0-ospf-1-area-0.0.0.2]net 192.168.0.18　0.0.0.0

第4步：　SH-MSR2020-0 路由器路由配置

[SH-MSR2020-0]int loop 0

为 loopback 0 接口配置 IP 地址，注意掩码为 32 位

[SH-MSR2020-0-LoopBack0]ip add 192.168.0.19　32

[SH-MSR2020-0]router id 192.168.0.19

[SH-MSR2020-0]ospf

[SH-MSR2020-0-ospf-1]area 0

发布同 BJ-MSR3020-0 的互连网段

[SH-MSR2020-0-ospf-1-area-0.0.0.0]net 192.168.0.8 0.0.0.3

[SH-MSR2020-0-ospf-1]area 3

发布上海研究所内网网段地址

[SH-MSR2020-0-ospf-1-area-0.0.0.3]net 192.168.6.0 0.0.0.255

发布 loopback 地址（作为网管地址）

[SH-MSR2020-0-ospf-1-area-0.0.0.3]net 192.168.0.19 0.0.0.0

第5步：　配置访问 Internet 的路由

[BJ-MSR3020-0- GigabitEthernet]0/1]ip add 202.38.160.2 30

配置一条缺省路由，下一跳指向 ISP 给的网关地址

[BJ-MSR3020-0] ip route-static 0.0.0.0 0.0.0.0 202.38.160.1

将缺省路由发布到 OSPF 中

[BJ-MSR3020-0-ospf-1]default-route-advertise

实验任务四：网络安全部署

第1步：　地址转换及服务器发布

创建 ACL 2000

[BJ-MSR3020-0]acl number 2000 match-order auto

[BJ-MSR3020-0- acl-basic-2000]rule 0 permit

进入连接 Internet 的接口

[BJ-MSR3020-0]interface G0/1

使用 Easy IP 方式使能 NAT

[BJ-MSR3020-0-GigabitEthernet0/1]nat outbound 2000

发布 WWW 及 OA 服务器

[BJ-MSR3020-0-GigabitEthernet0/1]nat server protocol tcp global 202.38.160.2 www inside 192.168.4.131 www

[BJ-MSR3020-0- GigabitEthernet0/1]nat server protocol tcp global 202.38.160.2 8080 inside 192.168.4.130 8080

第2步：　攻击防范配置

常见的病毒及攻击端口，如 ACL3001

```
acl number 3001
 rule 0 deny tcp source-port eq 3127
 rule 1 deny tcp source-port eq 1025
 rule 2 deny tcp source-port eq 5554
 rule 3 deny tcp source-port eq 9996
 rule 4 deny tcp source-port eq 1068
 rule 5 deny tcp source-port eq 135
 rule 6 deny udp source-port eq 135
 rule 7 deny tcp source-port eq 137
 rule 8 deny udp source-port eq netbios-ns
 rule 9 deny tcp source-port eq 138
 rule 10 deny udp source-port eq netbios-dgm
 rule 11 deny tcp source-port eq 139
 rule 12 deny udp source-port eq netbios-ssn
 rule 13 deny tcp source-port eq 593
 rule 14 deny tcp source-port eq 4444
 rule 15 deny tcp source-port eq 5800
 rule 16 deny tcp source-port eq 5900
 rule 18 deny tcp source-port eq 8998
 rule 19 deny tcp source-port eq 445
 rule 20 deny udp source-port eq 445
 rule 21 deny udp source-port eq 1434
rule 30 deny tcp destination-port eq 3127
 rule 31 deny tcp  destination-port eq 1025
 rule 32 deny tcp destination-port eq 5554
 rule 33 deny tcp destination-port eq 9996
 rule 34 deny tcp destination-port eq 1068
 rule 35 deny tcp destination-port eq 135
 rule 36 deny udp destination-port eq 135
 rule 37 deny tcp destination-port eq 137
 rule 38 deny udp destination-port eq netbios-ns
 rule 39 deny tcp destination-port eq 138
 rule 40 deny udp destination-port eq netbios-dgm
 rule 41 deny tcp destination-port eq 139
 rule 42 deny udp destination-port eq netbios-ssn
 rule 43 deny tcp destination-port eq 593
 rule 44 deny tcp destination-port eq 4444
 rule 45 deny tcp destination-port eq 5800
 rule 46 deny tcp destination-port eq 5900
 rule 48 deny tcp destination-port eq 8998
 rule 49 deny tcp destination-port eq 445
 rule 50 deny udp destination-port eq 445
 rule 51 deny udp destination-port eq 1434
```

将 ACL 3001 应用与连接外网接口的 IN 方向，阻止外网的入侵

[BJ-MSR3020-0-GigabitEthernet0/1] firewall packet-filter 3001 inbound

实验任务五：网管部署

打开 SNMP 代理功能

[BJ-S5626C-0]snmp-agent

指定 SNMP 的读团体名为 CD-public

[BJ-S5626C-0]snmp-agent community read CD-public

指定 SNMP 的读团体名为 CD- private

[BJ-S5626C-0]snmp-agent community write CD-private

指定 SNMP 的版本为 V2C 版本

[BJ-S5626C-0]snmp-agent sys-info version v2c

打开的告警触发功能

[BJ-S5626C-0]snmp-agent trap enable

设置 Trap 目标主机地址

[BJ-S5626C-0]snmp-agent target-host trap address udp-domain 192.168.4.1 udp-port 5000 params securityname CD-public