路由器实验篇

第六章 路由协议实验

6.1 实验背景知识

6.1.1 路由器简介

路由器是网络的“边缘”设备，路由器的核心作用是实现网络互连。因此路由器必须具备两个或两个以上的接口，协议至少实现到网络层，至少支持两种以上的子网协议，同时具有存储、转发和寻径的功能。路由器能够实现不同速率网络的适配，还能够隔离广播，实施安全策略。路由器能够建立维护路由信息，实现数据包转发、分片与重组，实现数据备份、流量控制等功能。

路由器的结构包括硬件和软件 2 部分。硬件由 CPU(处理器)、RAM(存储正在运行的配置文件)、FLASH（负责保存 OS 的映像和路由器的微码）、NVRAM（保存配置件）、ROM（加载 OS）和接口（完成路由器与其它设备的数据交换）组成；软件由 BOOT ROM 和 VRP (Versatile Routing Platform 通用路由平台）组成。BOOT ROM 的主要功能是路由器加电后完成有关初始化工作，并向内存中加入操作系统代码。

VRP 是华为公司数据通信产品的通用操作系统平台，它以 IP 业务为核心，实现组件化的体系结构，在提供丰富功能特性的同时，提供基于应用的可裁剪能力和可伸缩能力。

路由器要将数据报文从一个网络转发到另一个网络，需要根据所收到的报文的目的地址选择一条合适的路由（通过某一网络），将报文传送到下一个路由器，路由中最后的路由器负责将报文送交目的主机。路由器转发分组的关键是路由表。每个路由器中都保存着一张路由表，表中每条路由项都指明分组到某子网或某主机应通过路由器的哪个物理端口发送，然后就可到达该路径的下一个路由器，或者不再经过别的路由器而传送到直接相连的网络中的目的主机。路由器根据路由表首先进行精确匹配，就是按照子网掩码最长的匹配路由转发 IP 包，如果没有精确匹配的路由表项，则使用缺省路由转发 IP 包。如果无法转发，则发送 ICMP Unreachable 报文给 IP 包来源。

路由表中包含了下列关键项：

- 目的地址：用来标识 IP 包的目的地址或目的网络。
- 网络掩码：与目的地址一起来标识目的主机或路由器所在的网段的地址。将目的地址和网络掩码“逻辑与”后可得到目的主机或路由器所在网段的地址。
- 输出接口：说明 IP 包将从该路由器哪个接口转发。
- 下一跳 IP 地址：说明 IP 包所经由的下一个路由器。
- 本条路由加入 IP 路由表的优先级：针对同一目的地，可能存在不同下一跳的若干条路由，这些不同的路由可能是由不同的路由协议发现的，也可以是手工配置的静态路由。优先级高（数值小）将成为当前的最优路由。

路由表项根据路由的目的地不同，可以划分为：主机路由和子网路由。子网路由的目的地为子网，主机路由的目的地为主机。另外，根据目的地与该路由器是否直接相连，又可分为：直接路由和间接路由。直接路由的目的地所在网络与路由器直接相连。间接路由的目的

地所在网络与路由器不是直接相连。为了不使路由表过于庞大，需要设置一条缺省路由。凡遇到查找路由表失败后的数据包，就选择缺省路由转发。

Destination/Mask	Proto	Pre	Cost	Nexthop	Interface
1.1.1.0/24	DIRECT	0	0	1.1.1.1	Interface Serial1/0/0
1.1.1.1/32	DIRECT	0	0	127.0.0.1	InLoopBack0
2.2.2.0/24	DIRECT	0	0	2.2.2.1	Interface serial2/0/0
2.2.2.1/32	DIRECT	0	0	127.0.0.1	InLoopBack0
3.3.3.0/24	DIRECT	0	0	3.3.3.1	Interface ethernet1/0/0
3.3.3.1/32	DIRECT	0	0	127.0.0.1	InLoopBack0
127.0.0.0/8	DIRECT	0	0	127.0.0.1	InLoopBack0
127.0.0.1/32	DIRECT	0	0	127.0.0.1	InLoopBack0

表 6-1 路由表

6.1.2 RIP 简介

常见的 IP 协议是可路由协议。可路由协议（Routed Protocol）属于网络层，可以封装网络层数据包，以实现数据包转发。常见的可路由协议有 IP 协议、IPX 协议。而路由器中使用的路由协议（Routing Protocol）属于应用层，它与可路由协议协同工作，用于生成路由信息。常见的路由协议包括 RIP、OSPF、IS-IS 等。

RIP 是一种基于距离矢量（Distance-Vector）算法的协议，它使用 UDP 报文进行路由信息的交换。RIP 每隔 30 秒钟发送一次路由刷新报文，如果在 180 秒内收不到从某一网络邻居发来的路由刷新报文，则将该网络邻居的所有路由标记为不可达。如果在 300 秒之内收不到从某一网上邻居发来的路由刷新报文，则将该网上邻居的路由从路由表中清除。RIP 分为 RIP-1 和 RIP-2。RIP-1 不具备报文加密验证功能，而在 RIP-2 中实现了该功能。

RIP 使用跳数（Hop Count）来衡量到达目标机的距离，称为路由权（Routing Metric）。在 RIP 中，路由器到与它直接相连网络的跳数为 0，通过一个路由器可达的网络的跳数为 1，其余依此类推。为限制收敛时间，RIP 规定 metric 取值 0~15 之间的整数，大于或等于 16 的跳数被定义为无穷大，即目的网络或主机不可达。

为提高性能，防止产生路由环，RIP 支持水平分割（Split Horizon）和毒性逆转（Poison Reverse）。RIP 还可引入其它路由协议所得到的路由。

每个运行 RIP 的路由器管理一个路由数据库，该路由数据库包含了到网络所有可达信宿的路由项，这些路由项包含下列信息：

- 目的地址：主机或网络的地址。
- 下一跳地址：为到达目的地，需要经过的相邻路由器的接口 IP 地址。
- 接口：转发报文的接口。
- cost 值：本路由器到达目的地的开销。
- 路由时间：从路由项最后一次被修改到现在所经过的时间，路由项每次被修改时，路由时间重置为 0。

某路由器刚启动 RIP 时，以广播的形式向相邻路由器发送请求报文，相邻路由器的 RIP 收到请求报文后，响应该请求，回送包含本地路由表信息的响应报文。

路由器收到响应报文后，修改本地路由表，同时向相邻路由器发送触发修改报文，广播路由修改信息。相邻路由器收到触发修改报文后，又向其各自的相邻路由器发送触发修改报文。在一连串的触发修改广播后，各路由器都能得到并保持最新的路由信息。

同时，RIP 每隔 30 秒向相邻路由器广播本地路由表，相邻路由器在收到报文后，对本地路由进行维护，选择一条最佳路由，再向其各自相邻网络广播修改信息，使更新的路由最终能达到全局有效。同时，RIP 采用超时机制对过时的路由进行超时处理，以保证路由的实时性和有效性。

6.1.3 OSPF 简介

开放最短路径优先协议 OSPF（Open Shortest Path First）是另一种常用路由协议，它是由 IETF 组织开发的一个基于链路状态的内部网关协议。OSPF 具有下面的特性：

- 适应范围——支持各种规模的网络，最多可支持几百台路由器。
- 快速收敛——在网络的拓扑结构发生变化后立即发送更新报文，使这一变化在自治系统中同步。
- 无自环——由于 OSPF 根据收集到的链路状态用最短路径树算法计算路由，从算法本身保证了不会生成自环路由。
- 区域划分——允许自治系统的网络被划分成区域来管理，区域间传送的路由信息被进一步抽象，从而减少了占用的网络带宽。
- 等值路由——支持到同一目的地址的多条等值路由。
- 路由分级——使用 4 类不同的路由，按优先顺序来说分别是：区域内路由、区域间路由、第一类外部路由、第二类外部路由。

每个支持 OSPF 协议的路由器都维护着一份描述整个自治系统拓扑结构的链路状态数据库 LSDB（Link State Database）。每台路由器根据自己周围的网络拓扑结构生成链路状态广播 LSA（Link State Advertisement），通过相互之间发送协议报文将 LSA 发送给网络中其它路由器。这样每台路由器都收到了其它路由器的 LSA，所有的 LSA 放在一起便组成了链路状态数据库。

由于 LSA 是对路由器周围网络拓扑结构的描述，那么 LSDB 则是对整个网络的拓扑结构的描述。路由器很容易将 LSDB 转换成一张带权的有向图，这张图便是对整个网络拓扑结构的真实反映。显然，各个路由器得到的是一张完全相同的图。

每台路由器都使用 SPF 算法计算出一棵以自己为根的最短路径树，这棵树给出了到自治系统中各节点的路由，外部路由信息为叶子节点，外部路由可由广播它的路由器进行标记以记录关于自治系统的额外信息。显然，各个路由器各自得到的路由表是不同的。

OSPF 协议定义了“指定路由器”DR（Designated Router），所有路由器都只将信息发送给 DR，由 DR 将网络链路状态广播出去。这样就减少了多址访问网络上各路由器之间邻接关系的数量。OSPF 协议支持基于接口的报文验证以保证路由计算的安全性；并使用 IP 多播方式发送和接收报文。

6.2 实验目的

本章节实验共 4 个内容，包括静态路由配置、RIP 配置、OSPF 配置和多域 OSPF 邻居认证 4 个实验。通过本章节实验，能够掌握路由器的工作原理，了解路由表的作用，熟悉路由协议的基本配置方法。

6.3 实验内容

6.3.1 静态路由配置

1、软硬件要求：路由器 2 台，交换机 2 台，计算机 4 台，Console 线 2 根，DTE 和 DCE 电缆 1 对，网线若干。

2、网络拓扑图：

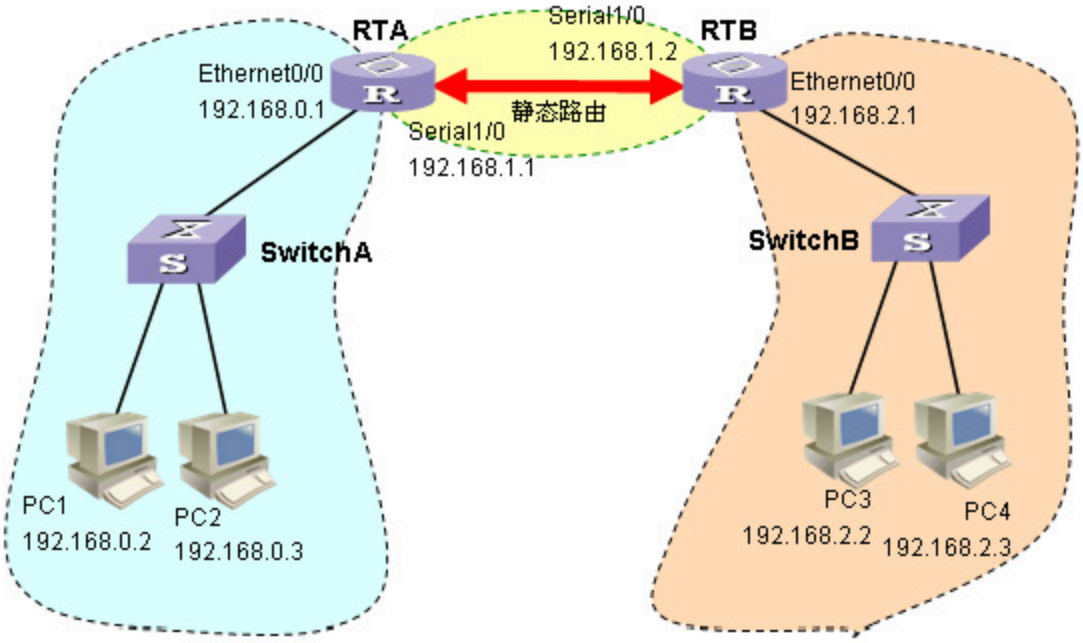

图 6-2 静态路由配置

3、连接设备

按照图 6-2 连线。路由器 RTA 和 RTB 的同/异步串口 Serial1/0 通过 DTE 和 DCE 电缆相连，交换机 SwitchA 的端口 ethernet 1/0/1 与路由器 RTA 的以太网接口 Ethernet 0/0 通过网线相连，交换机 SwitchB 的端口 ethernet 1/0/1 与路由器 RTB 的以太网接口 Ethernet 0/0 通过网线相连。PC1 和 PC2 连接在 SwitchA 的端口 ethernet 1/0/2 、ethernet 1/0/3 上，PC3 和 PC4 连接在 SwitchB 的端口 ethernet 1/0/2 、ethernet 1/0/3 上。

路由器 RTA 的 Ethernet 0/0 接口地址是 192.168.0.1/24，Serial1/0 接口地址是 192.168.1.1/24。路由器 RTB 的 Ethernet 0/0 接口地址是 192.168.2.1/24，Serial1/0 接口地址是 192.168.1.2/24。PC1 和 PC2 的 IP 地址分别是 192.168.0.2/24、192.168.0.3/24，缺省网关地址相同，为 192.168.0.1。PC3 和 PC4 的 IP 地址分别是 192.168.2.2/24、192.168.2.3/24，缺省网关地址相同，为 192.168.2.1。

4、观察

使用 Ping 命令测试各个 PC 之间是否可以通信，测试路由器的各个接口是否可以通信。使用命令 display ip routing-table 显示路由表，记录各个路由表项。

5、在路由器 RTA 上配置静态路由

```
<Quidway> system-view
//进入系统视图
[Quidway] sysname RTA
//修改系统名称
```

[RTA] interface ethernet 0/0
[RTA-Ethernet0/0] ip address 192.168.0.1 24
//指定以太网接口 Ethernet 0/0 的 IP 地址是 192.168.0.1，掩码为 255.255. 255.0

[RTA-Ethernet0/0] interface serial 1/0
[RTA- Serial1/0] ip address 192.168.1.1 24
//指定同/异步串口 Serial1/0 的 IP 地址是 192.168.1.1，掩码为 255.255. 255.0
[RTA- Serial1/0] shutdown
[RTA- Serial1/0] undo shutdown
//关闭后再打开端口，使配置立刻生效
[RTA- Serial1/0] quit

[RTA] ip route-static 192.168.2.0 255.255.255.0 192.168.1.2
//在路由器 RTA 上配置到 192.168.2.0 网段的静态路由

6、在路由器 RTB 上配置静态路由
<Quidway> system-view
//进入系统视图
[Quidway] sysname RTB
//修改系统名称

[RTB] interface ethernet 0/0
[RTB-Ethernet0/0] ip address 192.168.2.1 24
//指定以太网接口 Ethernet 0/0 的 IP 地址是 192.168.2.1，掩码为 255.255. 255.0

[RTB] interface serial 1/0
[RTB- Serial1/0] ip address 192.168.1.2 24
//指定同/异步串口 Serial1/0 的 IP 地址是 192.168.1.2，掩码为 255.255. 255.0
[RTB- Serial1/0] shutdown
[RTB- Serial1/0] undo shutdown
//关闭后再打开端口，使配置立刻生效
[RTB- Serial1/0] quit

[RTB] ip route-static 192.168.0.0 255.255.255.0 192.168.1.1
//在路由器 RTB 上配置到 192.168.0.0 网段的静态路由

7、测试验证

使用 Ping 命令测试。路由器的各个接口可以通信，RTA 能够 Ping 通所有主机，RTB 能够 Ping 通所有主机，主机 1、2 能与主机 3、4 互相 Ping 通。使用命令 display ip routing-table 显示路由表，记录各个路由表项，与前面记录的路由表项对比，比较有何不同。

6.3.2 RIP 配置

1、软硬件要求：路由器 2 台，交换机 2 台，计算机 4 台，Console 线 2 根，DTE 和 DCE 电

缆 1 对，网线若干。

2、网络拓扑图：

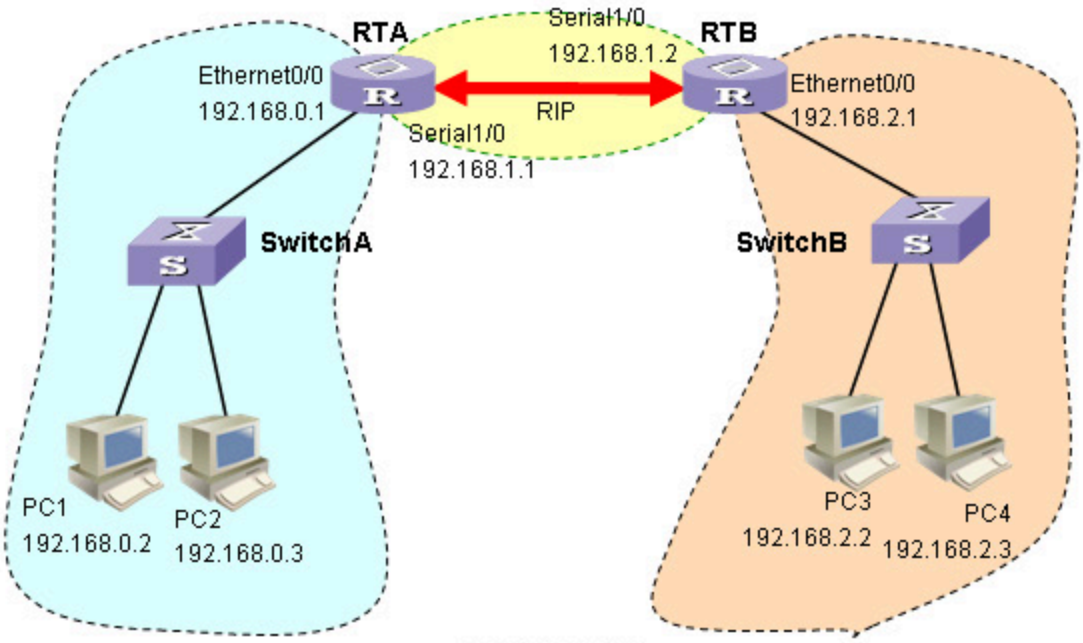

图 6-2 RIP 配置

3、连接设备

按照图 6-2 连线。路由器 RTA 和 RTB 的同/异步串口 Serial1/0 通过 DTE 和 DCE 电缆相连，交换机 SwitchA 的端口 ethernet 1/0/1 与路由器 RTA 的以太网接口 Ethernet 0/0 通过网线相连，交换机 SwitchB 的端口 ethernet 1/0/1 与路由器 RTB 的以太网接口 Ethernet 0/0 通过网线相连。PC1 和 PC2 连接在 SwitchA 的端口 ethernet 1/0/2 、ethernet 1/0/3 上，PC3 和 PC4 连接在 SwitchB 的端口 ethernet 1/0/2 、ethernet 1/0/3 上。

路由器 RTA 的 Ethernet 0/0 接口地址是 192.168.0.1/24，Serial1/0 接口地址是 192.168.1.1/24。路由器 RTB 的 Ethernet 0/0 接口地址是 192.168.2.1/24，Serial1/0 接口地址是 192.168.1.2/24。PC1 和 PC2 的 IP 地址分别是 192.168.0.2/24、192.168.0.3/24，缺省网关地址相同，为 192.168.0.1。PC3 和 PC4 的 IP 地址分别是 192.168.2.2/24、192.168.2.3/24，缺省网关地址相同，为 192.168.2.1。

4、观察

使用 Ping 命令测试各个 PC 之间是否可以通信，测试路由器的各个接口是否可以通信。使用命令 display ip routing-table 显示路由表，记录各个路由表项。

5、在路由器 RTA 上配置 RIP

```
<Quidway> system-view
//进入系统视图
[Quidway] sysname RTA
//修改系统名称

[RTA] interface ethernet 0/0
[RTA-Ethernet0/0] ip address 192.168.0.1 24
//指定以太网接口 Ethernet 0/0 的 IP 地址是 192.168.0.1，掩码为 255.255. 255.0

[RTA-Ethernet0/0] interface serial 1/0
[RTA- Serial1/0] ip address 192.168.1.1 24
```

//指定同/异步串口 Serial1/0 的 IP 地址是 192.168.1.1，掩码为 255.255. 255.0
[RTA- Serial1/0] shutdown
[RTA- Serial1/0] undo shutdown
//关闭后再打开端口，使配置立刻生效

[RTA- Serial1/0] rip
[RTA-rip] network 192.168.0.0
[RTA-rip] network 192.168.1.0
//在路由器 RTA 上启动 RIP，并配置在接口 Ethernet0/0 和 Serial1/0 上运行 RIP

6、在路由器 RTB 上配置 RIP
<Quidway> system-view
//进入系统视图
[Quidway] sysname RTB
//修改系统名称

[RTB] interface ethernet 0/0
[RTB-Ethernet0/0] ip address 192.168.2.1 24
//指定以太网接口 Ethernet 0/0 的 IP 地址是 192.168.2.1，掩码为 255.255.255.0

[RTB-Ethernet0/0] interface serial 1/0
[RTB- Serial1/0] ip address 192.168.1.2 24
//指定同/异步串口 Serial1/0 的 IP 地址是 192.168.1.2，掩码为 255.255.255.0
[RTB- Serial1/0] shutdown
[RTB- Serial1/0] undo shutdown
//关闭后再打开端口，使配置立刻生效

[RTB- Serial1/0] rip
[RTB-rip] network 192.168.1.0
[RTB-rip] network 192.168.2.0
//在路由器 RTB 上启动 RIP，并配置在接口 Ethernet0/0 和 Serial1/0 上运行 RIP

7、测试验证

使用 Ping 命令测试。路由器的各个接口可以通信，RTA 能够 Ping 通所有主机，RTB 能够 Ping 通所有主机，主机 1、2 能与主机 3、4 互相 Ping 通。使用命令 display ip routing-table 显示路由表，记录各个路由表项，与前面记录的路由表项对比，比较有何不同。

6.3.3 配置 OSPF

1、软硬件要求：路由器 2 台，交换机 2 台，计算机 2 台，Console 线 2 根，DTE 和 DCE 电缆 1 对，网线若干。

2、网络拓扑图：

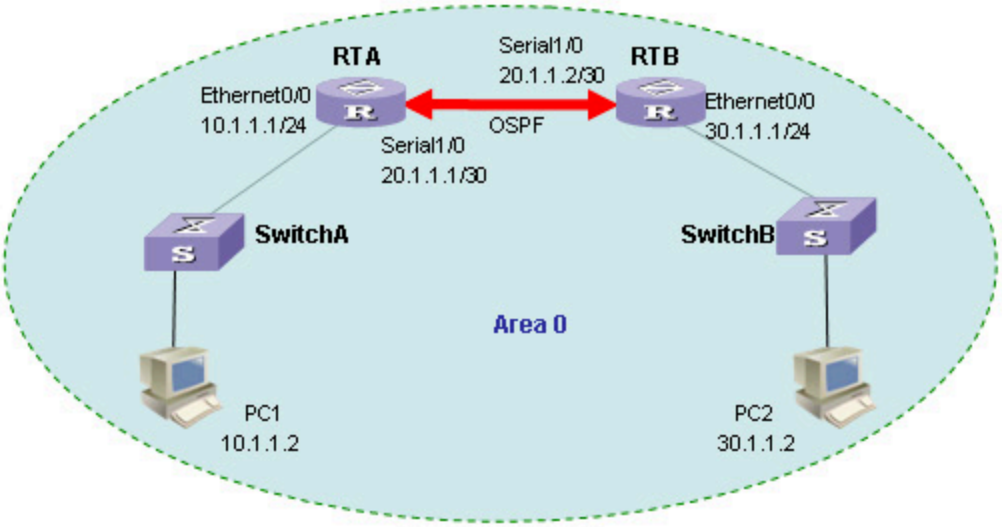

图 6-3 OSPF 配置

3、连接设备

按照图 6-3 连线。路由器 RTA 和 RTB 的同/异步串口 Serial1/0 通过 DTE 和 DCE 电缆相连，交换机 SwitchA 的端口 ethernet 1/0/1 与路由器 RTA 的以太网接口 Ethernet 0/0 通过网线相连，交换机 SwitchB 的端口 ethernet 1/0/1 与路由器 RTB 的以太网接口 Ethernet 0/0 通过网线相连。PC1 在 SwitchA 的端口 ethernet 1/0/2 上，PC2 连接在 SwitchB 的端口 ethernet 1/0/2 上。

路由器 RTA 的 Ethernet 0/0 接口地址是 10.1.1.1/24，Serial1/0 接口地址是 20.1.1.1/30。路由器 RTB 的 Ethernet 0/0 接口地址是 30.1.1.1/24，Serial1/0 接口地址是 20.1.1.2/30。PC1 的 IP 地址是 10.1.1.2/24，缺省网关地址是 10.1.1.1。PC2 的 IP 地址是 30.1.1.2/24，缺省网关地址是 30.1.1.1。

4、观察

使用 Ping 命令测试各个 PC 之间是否可以通信，测试路由器的各个接口是否可以通信。使用命令 display ip routing-table 显示路由表，记录各个路由表项。

5、在路由器 RTA 上配置 OSPF

```
<Quidway> system-view
//进入系统视图
[Quidway] sysname RTA
//修改系统名称

[RTA] router id 1.1.1.1
//设置运行 OSPF 协议的路由器 ID 号

[RTA] interface LoopBack 0
[RTA-LoopBack0] ip address 1.1.1.1 32
//配置 loopback0 和 router id 地址一致

[RTA-LoopBack0] interface Ethernet0/0
[RTA-Ethernet0/0] ip address 10.1.1.1 255.255.255.0

[RTA-Ethernet0/0] interface Serial1/0
[RTA-Serial1/0] link-protocol ppp
```

//封装 ppp 协议
[RTA-Serial1/0] ip address 20.1.1.1 255.255.255.252
[RTA-Serial1/0] quit

[RTA] ospf
//启动 ospf 路由协议

[RTA-ospf-1] area 0
//创建区域 0
[RTA-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
//在接口 LoopBack0 上运行 OSPF 协议
[RTA-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.3
//在接口 Serial1/0 上运行 OSPF 协议
[RTA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
//在接口 Ethernet0/0 上运行 OSPF 协议

6、在路由器 RTB 上配置 OSPF

<Quidway> system-view
//进入系统视图
[Quidway] sysname RTB
//修改系统名称

[RTB] router id 1.1.1.2
//设置运行 OSPF 协议的路由器 ID 号

[RTB] interface LoopBack 0
[RTB-LoopBack0] ip address 1.1.1.2 32
//配置 loopback0 和 router id 地址一致

[RTB-LoopBack0] interface Ethernet0/0
[RTB-Ethernet0/0] ip address 30.1.1.1 255.255.255.0

[RTB-Ethernet0/0] interface Serial1/0
[RTB-Serial1/0] link-protocol ppp
//封装 ppp 协议
[RTB-Serial1/0] ip address 20.1.1.2 255.255.255.252

[RTB-Serial1/0] ospf
//启动 ospf 路由协议

[RTB-ospf-1] area 0
//创建区域 0
[RTB-ospf-1-area-0.0.0.0] network 1.1.1.2 0.0.0.0
//在接口 LoopBack0 上运行 OSPF 协议
[RTB-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.3

//在接口 Serial1/0 上运行 OSPF 协议

[RTB-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255

//在接口 Ethernet0/0 上运行 OSPF 协议

7、测试验证

使用 Ping 命令测试。路由器的各个接口可以通信，RTA 能够 Ping 通所有主机，RTB 能够 Ping 通所有主机，主机 1、2 互相 Ping 通。使用命令 display ip routing-table 显示路由表，记录各个路由表项，与前面记录的路由表项对比，可以发现路由器通过 OSPF 获得了到对方的路由。

6.3.4 多域 OSPF 邻居认证

1、软硬件要求：路由器 3 台，交换机 2 台，计算机 2 台，Console 线 3 根，DTE 和 DCE 电缆 2 对，网线若干。

2、网络拓扑图：

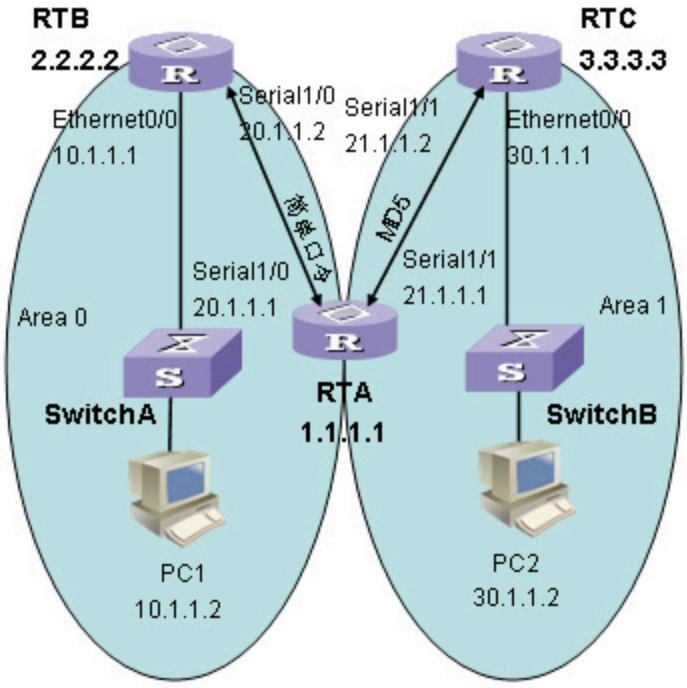

图 6-4 多域 OSPF 邻居认证

3、连接设备

按照图 6-4 连线。路由器 RTA 和 RTB 的同/异步串口 Serial1/0 通过 DTE 和 DCE 电缆相连，路由器 RTA 和 RTC 的同/异步串口 Serial1/1 通过 DTE 和 DCE 电缆相连。交换机 SwitchA 的端口 ethernet 1/0/1 与路由器 RTB 的以太网接口 Ethernet 0/0 通过网线相连，交换机 SwitchB 的端口 ethernet 1/0/1 与路由器 RTC 的以太网接口 Ethernet 0/0 通过网线相连。PC1 连接在 SwitchA 的端口 ethernet 1/0/2 上，PC2 连接在 SwitchB 的端口 ethernet 1/0/2 上。

路由器 RTA 的 Serial1/0 接口地址是 20.1.1.1/24，Serial1/1 接口地址是 21.1.1.1/24。路由器 RTB 的 Ethernet 0/0 接口地址是 10.1.1.1/24，Serial1/0 接口地址是 20.1.1.2/24。路由器 RTC 的 Ethernet 0/0 接口地址是 30.1.1.1/24，Serial1/1 接口地址是 21.1.1.2/24。PC1 的 IP 地址是 10.1.1.2/24，缺省网关地址是 10.1.1.1。PC2 的 IP 地址是 30.1.1.2/24，缺省网关地址是 30.1.1.1。

4、观察

使用 Ping 命令测试各个 PC 之间是否可以通信，测试路由器的各个接口是否可以通信。

使用命令 display ip routing-table 显示路由表，记录各个路由器的路由表项。

5、路由器 RTA 上的配置

```
<Quidway> system-view
//进入系统视图
[Quidway] sysname RTA
//修改系统名称

[RTA] router id 1.1.1.1
//设置运行 OSPF 协议的路由器 ID 号

[RTA] interface Serial1/0
[RTA-Serial1/0] link-protocol ppp
//封装 ppp 协议
[RTA-Serial1/0] ip address 20.1.1.1 255.255.255.0

[RTA-Serial1/0] ospf authentication-mode simple password
//配置接口 Serial1/0 的网段 20.1.1.0 所在的区域 0 支持明文验证，验证字为 password

[RTA-Serial1/0] interface Serial1/1
[RTA-Serial1/1] link-protocol ppp
//封装 ppp 协议
[RTA-Serial1/1] ip address 21.1.1.1 255.255.255.0

[RTA-Serial1/1] ospf authentication-mode md5 1 password
//配置接口 Serial1/1 的网段 21.1.1.0 所在的区域 1 支持 MD5 密文验证
//验证字标识符为 1，验证字为 password

[RTA-Serial1/1] ospf
//启动 ospf 路由协议

[RTA-ospf-1] area 0
//创建区域 0
[RTA-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[RTA-ospf-1-area-0.0.0.0] authentication-mode simple
//在接口 Serial1/0 上运行 OSPF 协议，支持明文验证
[RTA-ospf-1-area-0.0.0.0] quit

[RTA-ospf-1] area 1
//创建区域 0
[RTA-ospf-1-area-0.0.0.1] network 21.1.1.0 0.0.0.255
[RTA-ospf-1-area-0.0.0.1] authentication-mode md5
//在接口 Serial1/1 上运行 OSPF 协议，支持 MD5 密文验证
```

6、路由器 RTB 上的配置

```
<Quidway> system-view
```

//进入系统视图
[Quidway] sysname RTB
//修改系统名称
[RTB] interface Ethernet0/0
[RTB-Ethernet0/0] ip address 10.1.1.1 255.255.255.0

[RTB-Ethernet0/0] interface Serial1/0
[RTB- Serial1/0] ip address 20.1.1.2 255.255.255.0

[RTB- Serial1/0] ospf authentication-mode simple password
//配置接口 Serial1/0 的网段 20.1.1.0 所在的区域 0 支持明文验证

[RTB- Serial1/0] router id 2.2.2.2
//设置运行 OSPF 协议的路由器 ID 号

[RTB] ospf

[RTB-ospf-1] area 0
[RTB-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[RTB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RTB-ospf-1-area-0.0.0.0] authentication-mode simple
//在接口 Serial1/0 上运行 OSPF 协议，支持明文验证

7、路由器 RTC 上的配置

<Quidway> system-view
//进入系统视图
[Quidway] sysname RTC
//修改系统名称
[RTC] interface Ethernet0/0
[RTC-Ethernet0/0] ip address 30.1.1.1 255.255.255.0

[RTC-Ethernet0/0] interface Serial1/1
[RTC-Serial1/1] ip address 21.1.1.2 255.255.255.0

[RTC-Serial1/1] ospf authentication-mode md5 1 password
//配置接口 Serial1/1 的网段 21.1.1.0 所在的区域 1 支持 MD5 密文验证

[RTC-Serial1/1] router id 3.3.3.3
//设置运行 OSPF 协议的路由器 ID 号

[RTC] ospf

[RTC-ospf-1] area 1
[RTC-ospf-1-area-0.0.0.1] network 21.1.1.0 0.0.0.255
[RTC-ospf-1-area-0.0.0.1] network 30.1.1.0 0.0.0.255

[RTC-ospf-1-area-0.0.0.1] authentication-mode md5

//在接口 Serial1/1 上运行 OSPF 协议，支持 MD5 密文验证

8、测试验证

路由器 A 与路由器 B 交换路由更新信息时采用纯文本认证，而在与路由器 C 交换路由更新时使用 MD5 密文认证。路由器 A 的 Serial1/0 接口与路由器 B 的 Serial1/1 接口在 OSPF 区域 0 内。路由器 A 的 Serial1/1 接口与路由器 C 的 Serial1/1 接口都在区域 1 内，它们都为区域 1 配置了 MD5 认证。

使用命令 display ospf routing 显示 OSPF 路由表的信息，可以发现路由器通过 OSPF 获得了到对方的路由，查看不同域间学到的路由的标识。使用命令 display ospf lsdb brief 观察 OSPF 连接状态数据库，可看到不同的 LSA。如果 PC1 和 PC2 能够互相 Ping 通,代表设置正确。

6.4 思考题

（1）路由器工作在网络模型的哪一层？有哪些配置方式？有哪些接口？主要功能是什么？

（2）如果把主机 IP 地址设成与路由器端口不同网段的 IP 地址，主机间能否互通？为什么？

（3）静态路由有什么作用？在哪些情况下使用？

（4）写出路由表各项以及其含义。

（5）RIP 协议最多支持多少跳？

（6）RIP 协议和 OSPF 协议的区别有哪些？

第七章 链路层协议实验

7.1 实验背景知识

7.1.1 PPP

PPP（Point to Point Protocol）协议是在点到点链路上承载网络层数据包的一种链路层协议，由于它能够提供用户验证、易于扩充，并且支持同异步通信，因而获得广泛应用。

PPP 定义了一整套的协议，包括链路控制协议（LCP）、网络层控制协议（NCP）和验证协议（PAP 和 CHAP）等。其中，链路控制协议（Link Control Protocol）简称 LCP，主要用来建立、拆除和监控数据链路。网络层控制协议（Network Control Protocol）简称 NCP，主要用来协商在该数据链路上所传输的数据包的格式与类型。

PAP 和 CHAP 都是用于网络安全方面的验证协议族。

PAP 验证为两次握手验证，口令为明文。在 PAP 验证的过程中，被验证方发送用户名和口令到验证方；验证方根据本端用户表查看是否有此用户以及口令是否正确，然后返回不同的响应。

CHAP 验证为三次握手验证，口令为密文（密钥）。在 CHAP 验证过程中，验证方主动发起验证请求，验证方向被验证方发送一些随机产生的报文（Challenge），并同时将本端的用户名附带上一起发送给被验证方；被验证方接到验证方的验证请求后，被验证方根据此报文中验证方的用户名和本端的用户表查找用户口令字，如找到用户表中与验证方用户名相同的用户，便利用报文 ID、此用户的密钥（口令字）和 MD5 算法对该随机报文进行加密，将生成的密文和自己的用户名发回验证方（Response）；验证方用自己保存的被验证方口令字和 MD5 算法对原随机报文加密，比较二者的密文，根据比较结果返回不同的响应。

7.1.2 HDLC

高级数据链路控制（High-level Data Link Control）简称 HDLC，是一种面向比特的链路层协议。其最大特点是不需要规定数据必须是字符集，对任何一种比特流，均可以实现透明的传输。标准 HDLC 协议族中的协议都是运行于同步串行线路之上，如 DDN。HDLC 的地址字段是 8 个字节，控制字段是 8 比特，用来实现 HDLC 协议的各种控制信息，并标识是否是数据。

7.1.3 帧中继

帧中继协议是一种简化的 X.25 广域网协议。帧中继网提供了用户设备（如路由器和主机等）之间进行数据通信的能力，用户设备被称作数据终端设备（即 DTE）；为用户设备提供接入的设备，属于网络设备，被称为数据电路终接设备（即 DCE）。

帧中继协议是一种统计复用的协议，它在单一物理传输线路上能够提供多条虚电路。每条虚电路用 DLCI（数据链路连接标识，Data Link Connection Identifier）来标识的，DLCI 只在本地接口和与之直接相连的对端接口有效，不具有全局有效性，即在帧中继网络中，不

同的物理接口上相同的 DLCI 并不表示是同一个虚连接。帧中继网络用户接口上最多可支持 1024 条虚电路，其中用户可用的 DLCI 范围是 16～1007。

帧中继地址映射是把对端设备的协议地址与对端设备的帧中继地址（本地的 DLCI）关联起来，以便高层协议能通过对端设备的协议地址寻址到对端设备。帧中继主要用来承载 IP 协议，在发送 IP 报文时，根据路由表只知道报文的下一跳地址。发送前必须由该地址确定它对应的 DLCI。这个过程可以通过查找帧中继地址映射表来完成，因为地址映射表中存放的是对端 IP 地址和下一跳的 DLCI 的映射关系。地址映射表可以由手工配置，也可以由 Inverse ARP 协议动态维护。

根据虚电路建立的不同方式，可以将虚电路分为两种类型：永久虚电路和交换虚电路。手工设置产生的虚电路称为永久虚电路，通过协议协商产生的虚电路称为交换虚电路，这种虚电路由协议自动创建和删除。目前在帧中继中使用最多的方式是永久虚电路方式，即手工配置虚电路方式。

7.1.4 网桥

网桥（Bridge）是一种在数据链路层连接局域网（LAN），并在其间传递数据的网络设备。在一些小型网络尤其是分布比较分散的网络中，使用网桥可以减少网络维护成本，网络终端用户也不需要对设备进行特别设置，网络连接就像是 HUB 一样。

“透明”网桥（Transparent Bridging）用于连接物理介质类型相同的局域网，它主要应用在以太网（Ethernet）环境中。透明网桥通常都保存一张网桥表，该网桥表记录目的 MAC 地址与接口之间的对应关系。

网桥依据网桥表进行转发，网桥表由 MAC 地址和接口两部分组成，网桥必须获取 MAC 地址和接口的对应关系。网桥与物理网段相连时，会监测该物理网段上的所有以太网帧，一旦监测到某个接口上节点发来的以太网帧，就提取出该帧的源 MAC 地址，并将该 MAC 地址与接收该帧的接口之间的对应关系加入到网桥地址表中。

7.2 实验目的

本章节共 7 个实验内容，包括 PPP 不验证实验、PAP 单向验证实验、PAP 双向验证实验、CHAP 双向验证实验、HDLC 实验、帧中继实验和 PPP 透明网桥实验。通过这些实验的操作，可以了解 PPP、FR 等协议的工作过程，掌握它们的配置方法。

7.3 实验内容

7.3.1 PPP 不验证实验

1、软硬件要求：路由器 2 台，交换机 2 台，计算机 2 台，Console 线 2 根，DTE 和 DCE 电缆 1 对，网线若干。

2、网络拓扑图：

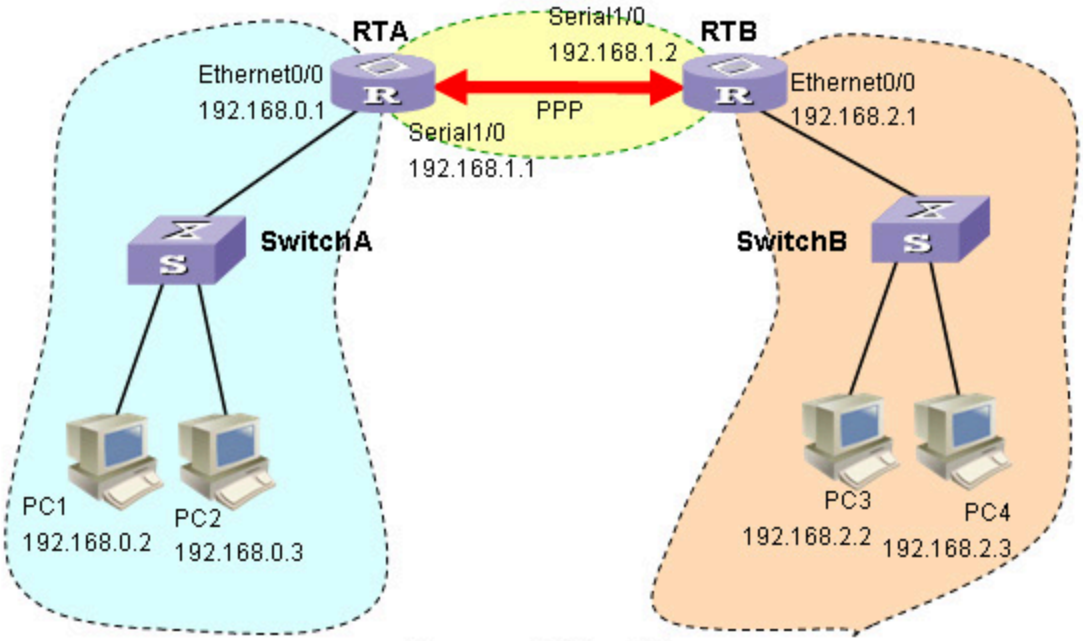

图 7-1 PPP 不验证实验

3、连接设备

按照图 7-1 连线。路由器 RTA 和 RTB 的同/异步串口 Serial1/0 通过 DTE 和 DCE 电缆相连，交换机 SwitchA 的端口 ethernet 1/0/1 与路由器 RTA 的以太网接口 Ethernet 0/0 通过网线相连，交换机 SwitchB 的端口 ethernet 1/0/1 与路由器 RTB 的以太网接口 Ethernet 0/0 通过网线相连。PC1 连接在 SwitchA 的端口 ethernet 1/0/2 上，PC2 连接在 SwitchB 的端口 ethernet 1/0/2 上。

路由器 RTA 的 Ethernet 0/0 接口地址是 192.168.0.1/24，Serial1/0 接口地址是 192.168.1.2/24。路由器 RTB 的 Ethernet 0/0 接口地址是 192.168.2.1/24，Serial1/0 接口地址是 192.168.1.1/24。PC1 的 IP 地址是 192.168.0.2/24，缺省网关地址是 192.168.0.1。PC2 的 IP 地址是 192.168.2.2/24，缺省网关地址是 192.168.2.1。

4、观察

使用 Ping 命令测试，观察各个 PC 之间是否能够通信，路由器的各个接口是否能够通信。

5、在路由器 RTA 上的配置

```
<Quidway> system-view
//进入系统视图
[Quidway] sysname RTA
//修改系统名称

[RTA] interface Ethernet0/0
[RTA-Ethernet0/0] ip address 192.168.0.1 255.255.255.0

[RTA-Ethernet0/0] interface Serial 1/0
[RTA-Serial1/0] ip address 192.168.1.1 255.255.255.0
//为端口 Serial1/0 配置 IP 地址
[RTA-Serial1/0] link-protocol ppp
//在端口 Serial1/0 上启动 ppp 协议
```

[RTA-Serial1/0] rip
[RTA-rip] network 192.168.0.0
[RTA-rip] network 192.168.1.0
//在路由器 RTA 上启动 RIP 协议，与 RTB 交换路由表项

6、在路由器 RTB 上的配置

<Quidway> system-view
//进入系统视图
[Quidway] sysname RTB
//修改系统名称

[RTB] interface Ethernet0/0
[RTB-Ethernet0/0] ip address 192.168.2.1 255.255.255.0

[RTB-Ethernet0/0] interface Serial 1/0
[RTB-Serial1/0] ip address 192.168.1.2 255.255.255.0
//为端口 Serial1/0 配置 IP 地址
[RTB-Serial1/0] link-protocol ppp
//在端口 Serial1/0 上启动 ppp 协议

[RTB-Serial1/0] rip
[RTB-rip] network 192.168.1.0
[RTB-rip] network 192.168.2.0
//在路由器 RTB 上启动 RIP 协议，与 RTA 交换路由表项

7、测试验证

使用 Ping 命令测试，可以发现各个 PC 之间能够通信，路由器的各个接口也能通信。

7.3.2 PAP 单向验证实验

1、软硬件要求：路由器 2 台，交换机 2 台，计算机 2 台，Console 线 2 根，DTE 和 DCE 电缆 1 对，网线若干。

2、网络拓扑图：

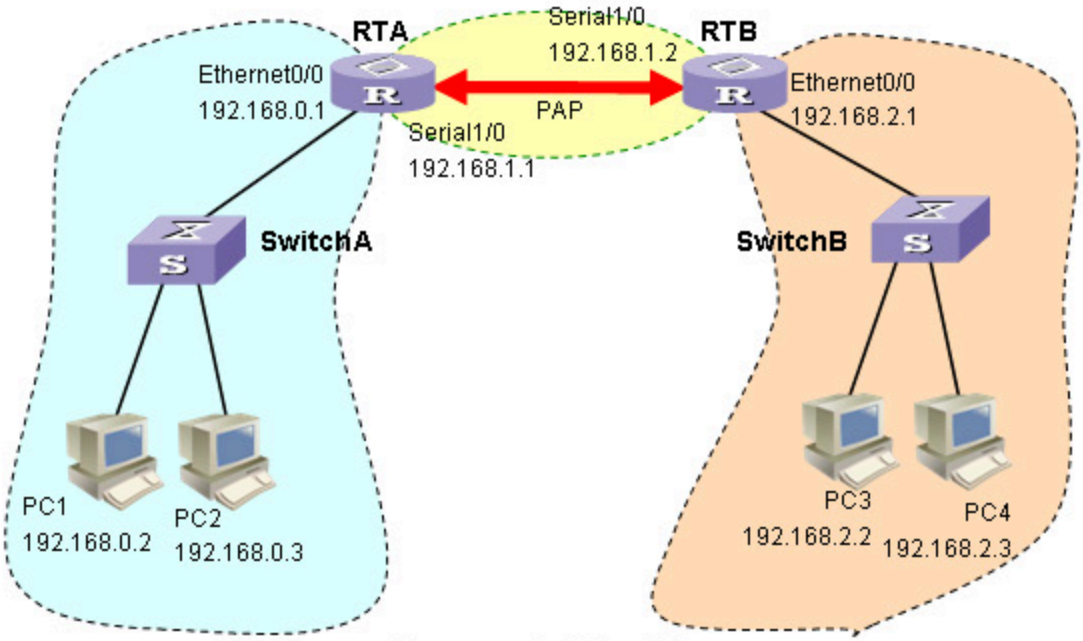

图 7-2 PAP 单向验证实验

3、连接设备

连线方法与上个实验相同，请参见实验 7.3.1 。

4、在路由器 RTA 上的配置

<Quidway> system-view

//进入系统视图

[Quidway] sysname RTA

//修改系统名称

[RTA] int serial1/0

[RTA-serial1/0] ppp authentication-mode pap

//为端口 Serial1/0 配置 PAP 验证

[RTA] local-user rtb

//创建用来验证的本地帐号

[RTA-luser-rtb] service-type ppp

//设置服务类型为 ppp

[RTA-luser-rtb] password simple NWPU

//设置密码为 NWPU

[RTA-luser-rtb] quit

[RTA] rip

[RTA-rip] network 192.168.0.0

[RTA-rip] network 192.168.1.0

//在路由器 RTA 上启动 RIP 协议，与 RTB 交换路由表项

5、在路由器 RTB 上的配置

<Quidway> system-view

//进入系统视图

[Quidway] sysname RTB

//修改系统名称

[RTB] interface Ethernet0/0
[RTB-Ethernet0/0] ip address 192.168.2.1 255.255.255.0
[RTB-Ethernet0/0] interface Serial 1/0
[RTB-Serial1/0] ip address 192.168.1.2 255.255.255.0
//为端口 Serial1/0 配置 IP 地址
[RTB-Serial1/0] link-protocol ppp
//在端口 Serial1/0 上启动 ppp 协议

[RTB-serial1/0] ppp pap local-user rtb password simple NWPU
//在路由器 RTB 上配置自己的验证信息，其发起验证时将把该信息发送给验证方

[RTB-Serial1/0] rip
[RTB-rip] network 192.168.1.0
[RTB-rip] network 192.168.2.0
//在路由器 RTB 上启动 RIP 协议，与 RTA 交换路由表项

6、测试验证

使用 Ping 命令测试，可以发现各个 PC 之间能够通信，路由器的各个接口也能通信。使用命令 display interface 查看接口 serial1/0 状态。RTA 需要对 RTB 送过来的帐号口令进行 PAP 验证，验证通过后 line protocol 才会 up。RTB 不需要对 RTA 进行验证。改变一方路由器上的验证密码，看看会发生什么情况。

7.3.3 PAP 双向验证实验

1、软硬件要求：路由器 2 台，交换机 2 台，计算机 2 台，Console 线 2 根，DTE 和 DCE 电缆 1 对，网线若干。

2、网络拓扑图：

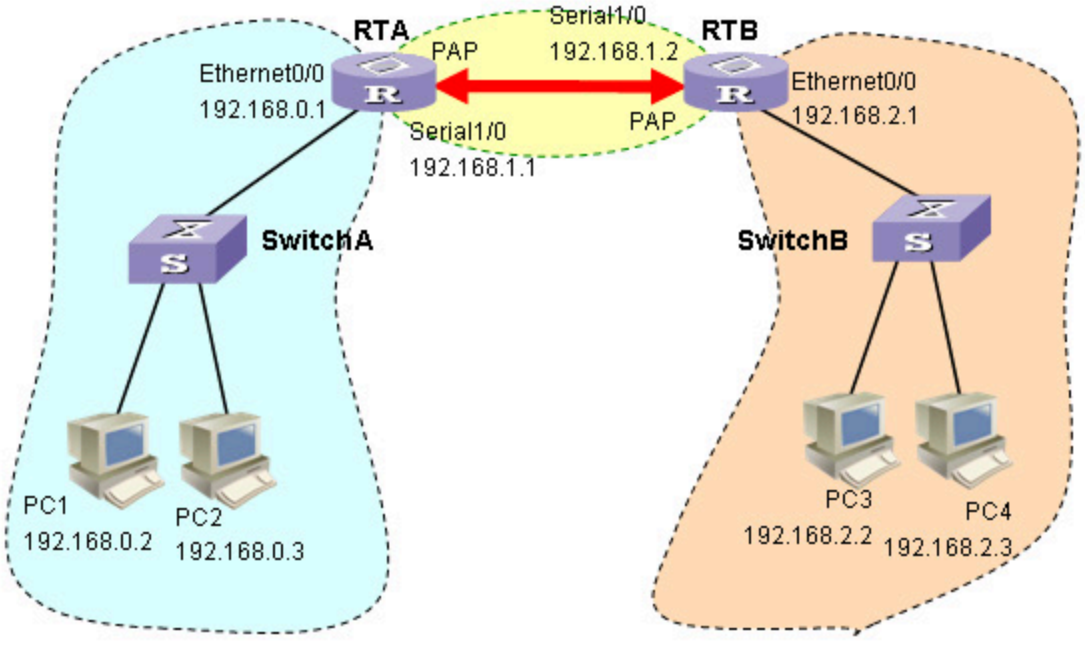

图 7-3 PAP 双向验证实验

3、连接设备

连线方法请参见实验 7.3.1 。

4、在路由器 RTA 上的配置

```
<Quidway> system-view
//进入系统视图
[Quidway] sysname RTA
//修改系统名称

[RTA] interface Ethernet0/0
[RTA-Ethernet0/0] ip address 192.168.0.1 255.255.255.0
[RTA-Ethernet0/0] interface Serial 1/0
[RTA-Serial1/0] ip address 192.168.1.1 255.255.255.0
//为端口 Serial1/0 配置 IP 地址
[RTA-Serial1/0] link-protocol ppp
//在端口 Serial1/0 上启动 ppp 协议

[RTA-serial1/0] ppp authentication-mode pap
//为端口 Serial1/0 配置 PAP 验证
[RTA-Serial1/0]ppp pap local-user rta password simple NWPU
//送给对端的用户名密码
[RTA-Serial1/0] quit

[RTA] local-user rtb
//创建用来验证的本地帐号
[RTA-luser-rtb] service-type ppp
//设置服务类型为 ppp
[RTA-luser-rtb] password simple NWPU
//设置密码为 NWPU
[RTA-luser-rtb] quit

[RTA] rip
[RTA-rip] network 192.168.0.0
[RTA-rip] network 192.168.1.0
//在路由器 RTA 上启动 RIP 协议，与 RTB 交换路由表项
```

5、在路由器 RTB 上的配置

```
<Quidway> system-view
//进入系统视图
[Quidway] sysname RTB
//修改系统名称

[RTB] interface Ethernet0/0
[RTB-Ethernet0/0] ip address 192.168.2.1 255.255.255.0
[RTB-Ethernet0/0] interface Serial 1/0
```

[RTB-Serial1/0] ip address 192.168.1.2 255.255.255.0
//为端口 Serial1/0 配置 IP 地址
[RTB-Serial1/0] link-protocol ppp
//在端口 Serial1/0 上启动 ppp 协议

[RTB-serial1/0] ppp authentication-mode pap
//为端口 Serial1/0 配置 PAP 验证
[RTB-Serial1/0]ppp pap local-user rtb password simple NWPU
//送给对端的用户名密码
[RTB-Serial1/0] quit

[RTB] local-user rta
//创建用来验证的本地帐号
[RTB-luser-rta] service-type ppp
//设置服务类型为 ppp
[RTB-luser-rta] password simple NWPU
//设置密码为 NWPU
[RTB-luser-rta] quit

[RTB-Serial1/0] rip
[RTB-rip] network 192.168.1.0
[RTB-rip] network 192.168.2.0
//在路由器 RTB 上启动 RIP 协议，与 RTA 交换路由表项

6、测试验证

使用 Ping 命令测试，可以发现各个 PC 之间能够通信，路由器的各个接口也能通信。使用命令 display interface 查看接口 serial1/0 状态。RTA 需要对 RTB 送过来的帐号口令进行 PAP 验证，验证通过后 line protocol 才会 up，而 RTB 同样需要对 RTA 送过来的帐号口令进行 PAP 验证，验证通过后 line protocol 才会 up。

7.3.4 CHAP 双向验证实验

1、软硬件要求：路由器 2 台，交换机 2 台，计算机 2 台，Console 线 2 根，DTE 和 DCE 电缆 1 对，网线若干。

2、网络拓扑图：

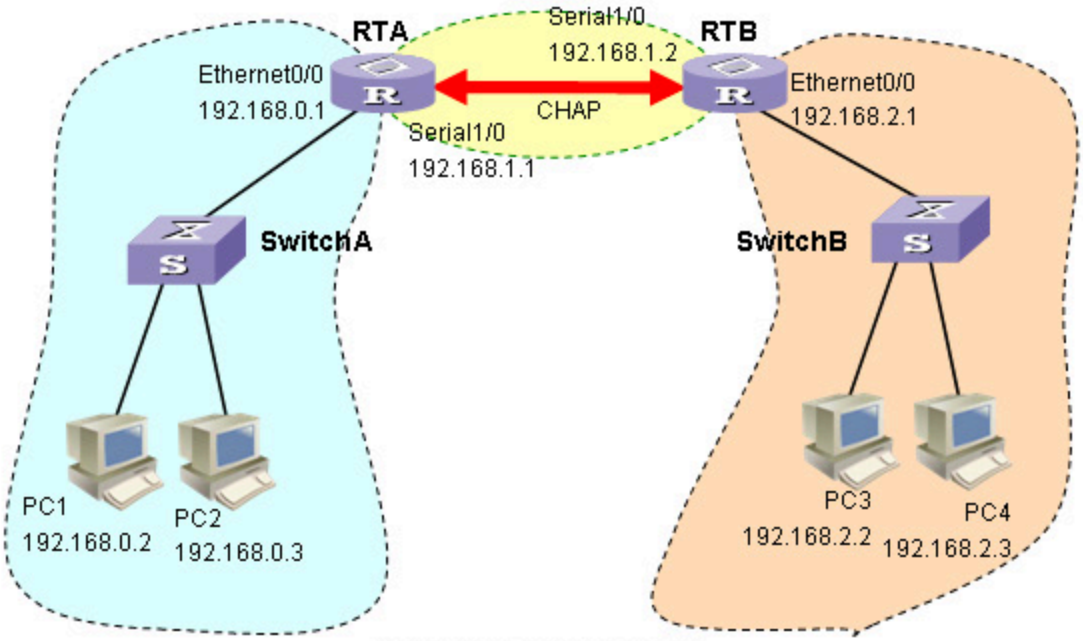

图 7-4 CHAP 双向验证实验

3、连接设备

连线方法请参见实验 7.3.1 。

4、在路由器 RTA 上的配置

<Quidway> system-view

//进入系统视图

[Quidway] sysname RTA

//修改系统名称

[RTA] interface Serial 1/0

[RTA-serial1/0] ppp authentication-mode chap

//为端口 Serial1/0 配置 CHAP 验证

[RTA-Serial1/0] ppp chap user rta

//Chap 认证帐号

[RTA] local-user rtb

//创建用来验证的本地帐号

[RTA-luser-rtb] service-type ppp

//设置服务类型为 ppp

[RTA-luser-rtb] password simple NWPU

//设置密码为 NWPU

[RTA-luser-rtb] quit

[RTA] interface Ethernet0/0

[RTA-Ethernet0/0] ip address 192.168.0.1 255.255.255.0

[RTA-Ethernet0/0] interface Serial 1/0

[RTA-Serial1/0] ip address 192.168.1.1 255.255.255.0

//为端口 Serial1/0 配置 IP 地址

[RTA-Serial1/0] link-protocol ppp

//在端口 Serial1/0 上启动 ppp 协议

[RTA-Serial1/0] rip
[RTA-rip] network 192.168.0.0
[RTA-rip] network 192.168.1.0
//在路由器 RTA 上启动 RIP 协议，与 RTB 交换路由表项

5、在路由器 RTB 上的配置

<Quidway> system-view
//进入系统视图
[Quidway] sysname RTB
//修改系统名称

[RTB] interface Serial 1/0
[RTB-serial1/0] ppp authentication-mode chap
//为端口 Serial1/0 配置 CHAP 验证
[RTB-Serial1/0]ppp chap user rtb
//Chap 认证帐号

[RTB] local-user rta
//创建用来验证的本地帐号
[RTB-luser-rta] service-type ppp
//设置服务类型为 ppp
[RTB-luser-rta] password simple NWPU
//设置密码为 NWPU
[RTB-luser-rta] quit

[RTB] interface Ethernet0/0
[RTB-Ethernet0/0] ip address 192.168.2.1 255.255.255.0
[RTB-Ethernet0/0] interface Serial 1/0
[RTB-Serial1/0] ip address 192.168.1.2 255.255.255.0
//为端口 Serial1/0 配置 IP 地址
[RTB-Serial1/0] link-protocol ppp
//在端口 Serial1/0 上启动 ppp 协议

[RTB-Serial1/0] rip
[RTB-rip] network 192.168.1.0
[RTB-rip] network 192.168.2.0
//在路由器 RTB 上启动 RIP 协议，与 RTA 交换路由表项

6、测试验证

使用 Ping 命令测试，可以发现各个 PC 之间能够通信，路由器的各个接口也能通信。使用命令 display interface 查看接口 serial1/0 状态。RTA 需要对 RTB 送过来的帐号口令进行 CHAP 验证，验证通过后 line protocol 才会 up，而 RTB 同样需要对 RTA 送过来的帐号口令进行 CHAP 验证，验证通过后 line protocol 才会 up。

7.3.5 HDLC 实验

1、软硬件要求：路由器 2 台，交换机 2 台，计算机 2 台，Console 线 2 根，DTE 和 DCE 电缆 1 对，网线若干。

2、网络拓扑图：

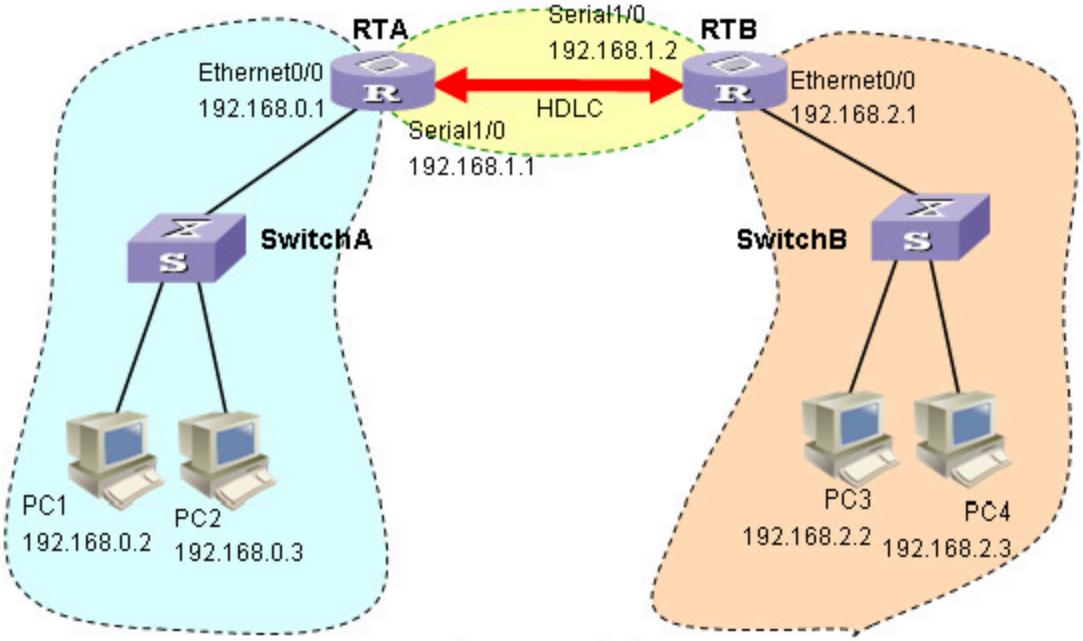

图 7-5 HDLC 实验

3、连接设备

连线方法请参见实验 7.3.1 。

4、在路由器 RTA 上的配置

```
<Quidway> system-view
//进入系统视图
[Quidway] sysname RTA
//修改系统名称

[RTA] interface Ethernet0/0
[RTA-Ethernet0/0] ip address 192.168.0.1 255.255.255.0
[RTA-Ethernet0/0] interface Serial 1/0
[RTA-Serial1/0] ip address 192.168.1.1 255.255.255.0
//为端口 Serial1/0 配置 IP 地址

[RTA-Serial1/0] link-protocol hdlc
//配置接口封装为 hdlc

[RTA-Serial1/0] rip
[RTA-rip] network 192.168.0.0
[RTA-rip] network 192.168.1.0
//在路由器 RTA 上启动 RIP 协议
```

5、在路由器 RTB 上的配置

```
<Quidway> system-view
//进入系统视图
[Quidway] sysname RTB
//修改系统名称
[RTB] interface Ethernet0/0
[RTB-Ethernet0/0] ip address 192.168.2.1 255.255.255.0
[RTB-Ethernet0/0] interface Serial 1/0
[RTB-Serial1/0] ip address 192.168.1.2 255.255.255.0
//为端口 Serial1/0 配置 IP 地址

[RTB-Serial1/0] link-protocol hdlc
//配置接口封装为 hdlc

[RTB-Serial1/0] rip
[RTB-rip] network 192.168.1.0
[RTB-rip] network 192.168.2.0
//在路由器 RTB 上启动 RIP 协议
```

6、测试验证

使用 Ping 命令测试，可以发现各个 PC 之间能够通信，路由器的各个接口也能通信。使用命令 display interface 查看接口 serial1/0 状态。

7.3.6 帧中继实验

1、软硬件要求：路由器 2 台，交换机 2 台，计算机 2 台，Console 线 2 根，DTE 和 DCE 电缆 1 对，网线若干。

2、网络拓扑图：

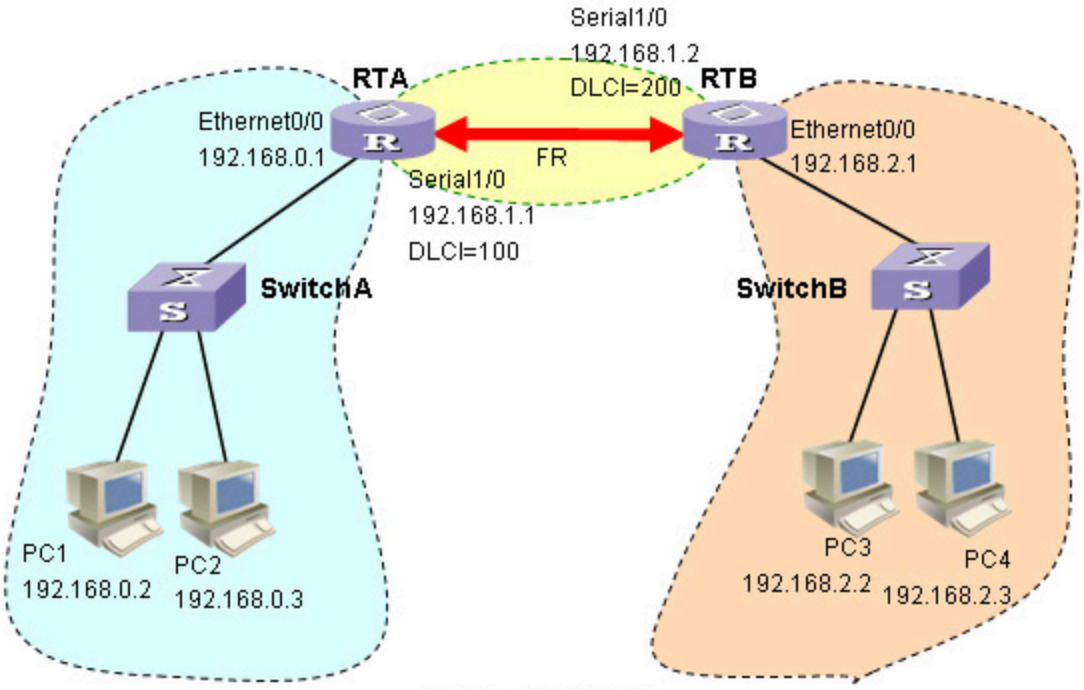

图 7-6 帧中继实验

3、连接设备

连线方法请参见实验 7.3.1 。

4、在路由器 RTA 上的配置

```
<Quidway> system-view
//进入系统视图
[Quidway] sysname RTA
//修改系统名称

[RTA] interface Ethernet0/0
[RTA-Ethernet0/0] ip address 192.168.0.1 255.255.255.0
[RTA-Ethernet0/0] interface Serial 1/0
[RTA-Serial1/0] ip address 192.168.1.1 255.255.255.0
//为端口 Serial1/0 配置 IP 地址

[RTA-Serial1/0] link-protocol fr
//配置封装方式为帧中继
[RTA-Serial1/0] fr interface-type dte
//配置端口类型为 dte
[RTB-Serial1/0] fr dlci 100
//配置数据链路连接标识

[RTA-Serial1/0] rip
[RTA-rip] network 192.168.0.0
[RTA-rip] network 192.168.1.0
//在路由器 RTA 上启动 RIP 协议
```

5、在路由器 RTB 上的配置

```
<Quidway> system-view
//进入系统视图
[Quidway] sysname RTB
//修改系统名称

[RTB] interface Ethernet0/0
[RTB-Ethernet0/0] ip address 192.168.2.1 255.255.255.0
[RTB-Ethernet0/0] interface Serial 1/0
[RTB-Serial1/0] ip address 192.168.1.2 255.255.255.0
//为端口 Serial1/0 配置 IP 地址

[RTB-Serial1/0] link-protocol fr
//配置封装方式为帧中继
[RTB-Serial1/0] fr interface-type dce
//配置端口类型为 dce
[RTB-Serial1/0] fr dlci 200
//配置数据链路连接标识
```

[RTB-Serial1/0] rip
[RTB-rip] network 192.168.1.0
[RTB-rip] network 192.168.2.0
//在路由器 RTB 上启动 RIP 协议

6、测试验证

使用 Ping 命令测试，可以发现各个 PC 之间能够通信，路由器的各个接口也能通信。使用命令 display interface 查看接口 serial1/0 状态。RTA 工作在帧中继的 DTE 方式，RTB 工作在帧中继的 DCE 方式。

7.3.7 PPP 透明网桥实验

1、软硬件要求：路由器 2 台，交换机 2 台，计算机 2 台，Console 线 2 根，DTE 和 DCE 电缆 1 对，网线若干。

2、网络拓扑图：

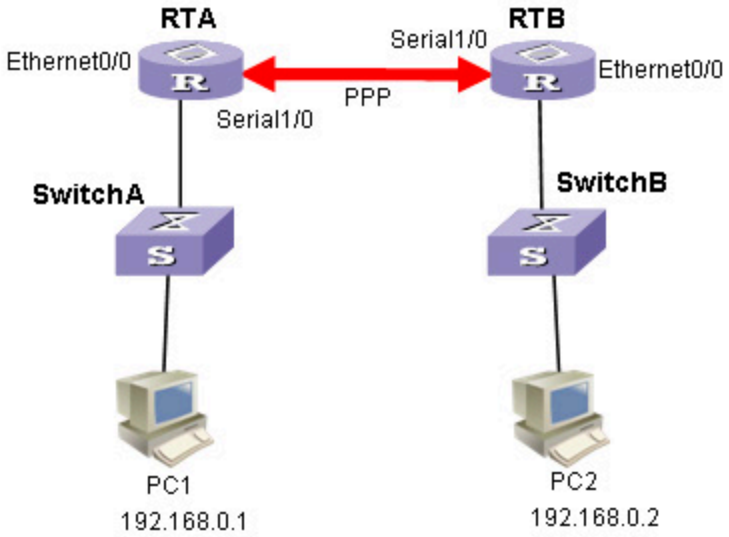

图 7-7 PPP 透明网桥实验

3、连接设备

按照图 7-7 连线。路由器 RTA 和 RTB 的同/异步串口 Serial1/0 通过 DTE 和 DCE 电缆相连，交换机 SwitchA 的端口 ethernet 1/0/1 与路由器 RTA 的以太网接口 Ethernet 0/0 通过网线相连，交换机 SwitchB 的端口 ethernet 1/0/1 与路由器 RTB 的以太网接口 Ethernet 0/0 通过网线相连。PC1 连接在 SwitchA 的端口 ethernet 1/0/2 上，PC2 连接在 SwitchB 的端口 ethernet 1/0/2 上。

PC1 的 IP 地址是 192.168.0.1/24，PC2 的 IP 地址是 192.168.0.2/24。

4、观察

使用 Ping 命令测试，观察各个 PC 之间是否能够通信，路由器的各个接口是否能够通信。

5、在路由器 RTA 上的配置

<Quidway> system-view
//进入系统视图
[Quidway] sysname RTA
//修改系统名称

[RTA] bridge enable
//使能网桥的桥接功能
[RTA] bridge 1 enable
//使能网桥组 1

[RTA] interface ethernet 0/0
[RTA -Ethernet 0/0] bridge-set 1
//接口属于网桥组 1

[RTA-Ethernet0/0] interface Serial 1/0
[RTA-Serial1/0] link-protocol ppp
//在端口 Serial1/0 上启动 ppp 协议

[RTA-Serial1/0] bridge-set 1
//接口属于网桥组 1

6、在路由器 RTB 上的配置

<Quidway> system-view
//进入系统视图
[Quidway] sysname RTB
//修改系统名称

[RTB] bridge enable
//使能网桥的桥接功能
[RTB] bridge 1 enable
//使能网桥组 1

[RTB] interface ethernet 0/0
[RTB -Ethernet 0/0] bridge-set 1
//接口属于网桥组 1

[RTB-Ethernet0/0] interface Serial 1/0
[RTB-Serial1/0] link-protocol ppp
//在端口 Serial1/0 上启动 ppp 协议

[RTB-Serial1/0] bridge-set 1
//接口属于网桥组 1

7、测试验证

使用 Ping 命令测试，各个 PC 之间能够通信。通过路由器的桥接功能，分处桥两端的物理以太网段的计算机可以通过桥接通信，而不需要进行 IP 路由，从而达到透过广域网，进行网上邻居的直接访问和其他应用。

7.4 思考题

（1）说明 CHAP 验证的过程。

（2）简述帧中继的工作原理。

（3）什么是网桥？

第八章 访问控制列表实验

8.1 实验背景知识

8.1.1 防火墙简介

为了保护一个计算机网络免受外来入侵者的攻击，人们在内部网与 Internet 之间设置一个安全网关，在保持内部网与 Internet 连通性的同时，对进入内部网的信息流实行访问控制，只转发合法的信息流，而将非法的信息流阻挡在内部网之外。这种安全网关被形象地称为防火墙。防火墙是设在内部网络和外部网络之间的一道关卡。当一个内部网接入 Internet 时，通常在内部网与 Internet 之间设置一个防火墙，以保护内部网免受非法用户的入侵。

防火墙一方面阻止来自因特网的对受保护网络的未授权或未验证的访问，另一方面允许内部网络的用户对因特网进行 Web 访问或收发 E-mail 等。防火墙也可以作为一个访问因特网的权限控制关口，如允许组织内的特定的人可以访问因特网。

根据不同的保护机制和工作原理，防火墙主要分成三类：分组过滤型、代理服务型和状态检测型。它们在网络性能、安全性和应用透明性等方面各有利弊。

8.1.2 访问控制列表

分组过滤型(Packet Filter) 防火墙，又称包过滤防火墙，一般是对 IP 数据包进行过滤。对路由器需要转发的数据包，先获取包头信息，包括 IP 层所承载的上层协议的协议号、数据包的源地址、目的地址、源端口和目的端口等，然后和设定的规则进行比较，根据比较的结果对数据包进行转发或者丢弃。

为了过滤数据包，路由器需要配置一些规则，规定什么样的数据包可以通过，什么样的数据包不能通过。这些规则就是通过访问控制列表 ACL（Access Control List）体现的。

用户需要根据自己的安全策略来确定访问控制列表，并将其应用到整机或指定接口上，路由器就会根据访问控制列表来检查所有接口或指定接口上的所有数据包，对于符合规则的报文作正常转发或丢弃处理，从而起到防火墙的作用。

一个访问控制列表可以由多条“permit | deny”语句组成，每一条语句描述的规则是不相同，这些规则可能存在重复或矛盾的地方，在将一个数据包和访问控制列表的规则进行匹配的时候，有两种匹配顺序：配置顺序和自动排序。配置顺序是指按照用户配置 ACL 的规则的先后进行匹配。自动排序使用“深度优先”的原则。“深度优先”规则是把指定数据包范围最小的语句排在最前面。这一点可以通过比较地址的通配符来实现，通配符越小，则指定的主机的范围就越小。具体标准为：对于基本访问控制规则的语句，直接比较源地址通配符，通配符相同的则按配置顺序；对于基于接口的访问控制规则，配置了“any”的规则排在后面，其它按配置顺序；对于高级访问控制规则，首先比较源地址通配符，相同的再比较目的地址通配符，仍相同的则比较端口号的范围，范围小的排在前面，如果端口号范围也相同则按配置顺序。

8.1.3 地址转换

地址转换（NAT）又称地址代理，它实现了私有网络访问外部网络的功能。地址转换的机制就是将私有网络内主机的 IP 地址和端口替换为路由器的外部网络地址和端口，以及从路由器的端口转换为私有网络主机的 IP 地址和端口，即<私有地址+端口>与<公有地址+端口>之间的转换。私有地址是指内部网络或主机地址，公有地址是指在因特网上全球唯一的 IP 地址。私有网络预留有三个 IP 地址块：

A 类：10.0.0.0～10.255.255.255

B 类：172.16.0.0～172.31.255.255

C 类：192.168.0.0～192.168.255.255

上述三个范围内的地址不会在因特网上被分配，因而可以不必向 ISP 或注册中心申请而在公司或企业内部自由使用。各企业根据在预见未来内部主机和网络的数量后，选择合适的内部网络地址，不同企业的内部网络地址可以相同。如果一个公司选择上述三个范围之外的其它网段作为内部网络地址，则有可能会造成混乱。地址转换在允许内部网络的主机访问网外资源的同时，为内部主机提供“隐私”（Privacy）保护。

NAT 服务器处于私有网络和公有网络的连接处。当内部计算机向外部计算机发送一个数据报时，数据报将通过 NAT 服务器。NAT 进程查看报头内容，发现该数据报是发往外网的，那么它将数据报的源地址字段的私有地址换成一个可在 Internet 上选路的公有地址，并将该数据报发送到外部计算机，同时在网络地址转换表中记录这一映射；外部计算机给内部计算机发送应答报文，到达 NAT 服务器后，NAT 进程再次查看报头内容，然后查找当前网络地址转换表的记录，用原来的内部 PC 的私有地址替换目的地址。

8.2 实验目的

本章节包括 ACL 实验、包过滤日志实验、地址转换实验和地址池 NAT 实验 4 个内容。通过以上实验，可以了解访问控制列表的作用，熟悉 NAT 的工作原理，掌握一定的配置技巧。

8.3 实验内容

8.3.1 ACL 实验一（按照配置顺序匹配）

1、软硬件要求：路由器 1 台，交换机 2 台，计算机 4 台，Console 线 1 根，网线若干。

2、网络拓扑图：

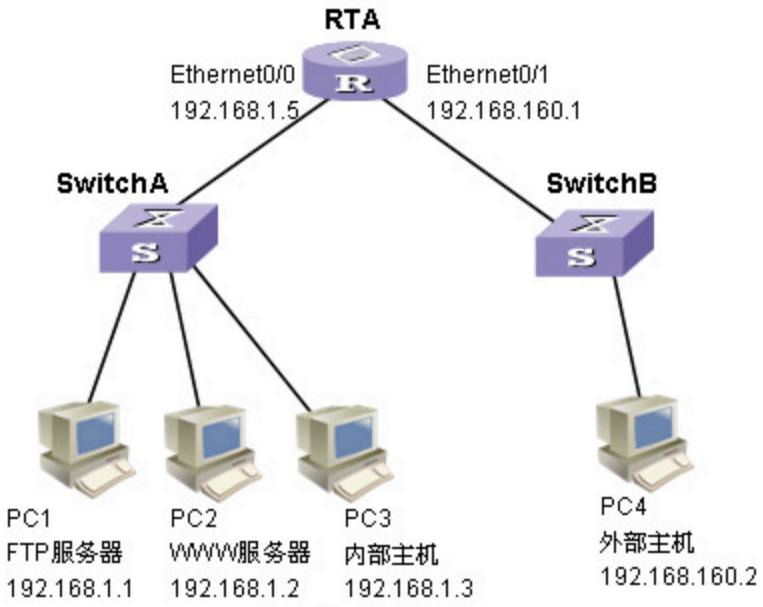

图 8-1 ACL 实验一

3、实验要求

PC1-PC3 属于内部网，PC4 属于外部网。通过配置防火墙，实现 PC4 与 PC3 可以通信，PC4 与 PC1 可以通信，PC4 与 PC2 不能通信。

4、连接设备

按照图 8-1 连线。交换机 SwitchA 的端口 ethernet 1/0/1 与路由器 RTA 的以太网接口 Ethernet 0/0 通过网线相连，交换机 SwitchB 的端口 ethernet 1/0/1 与路由器 RTA 的以太网接口 Ethernet 0/1 通过网线相连。PC1、PC2 和 PC3 连接在 SwitchA 的端口 ethernet 1/0/2 -ethernet 1/0/4 上，PC4 连接在 SwitchB 的端口 ethernet 1/0/2 上。

路由器 RTA 的 Ethernet 0/0 接口地址是 192.168.1.5/24，Ethernet 0/1 接口地址是 192.168.160.1/24。PC1 地址是 192.168.1.1/24，PC2 地址是 192.168.1.2/24， PC3 地址是 192.168.1.3/24，PC1-PC3 的缺省网关地址是 192.168.1.5。PC4 为外部主机，IP 地址是 192.168.160.2/24，缺省网关地址是 192.168.160.1。

5、观察

配置好 IP 地址，使用 Ping 命令测试，观察各个 PC 之间是否能够通信，路由器的各个接口是否能够通信。

6、在路由器 RTA 上配置防火墙

```
<Quidway> system-view
//进入系统视图
[Quidway] sysname RTA
//修改系统名称

[RTA] interface Ethernet 0/0
[RTA-Ethernet0/0] ip address 192.168.1.5 255.255.255.0
[RTA-Ethernet0/0] interface Ethernet 0/1
[RTA-Ethernet0/1] ip address 192.168.160.1 255.255.255.0
[RTA-Ethernet0/1] quit

[RTA] firewall enable
//在路由器 RTA 上允许防火墙
```

[RTA] firewall default permit
//设置防火墙缺省过滤方式为允许包通过

[RTA] acl number 3001
//创建访问控制列表 3001
[RTA-acl-adv-3001] rule permit ip source 192.168.1.1 0
[RTA-acl-adv-3001] rule permit ip source 192.168.1.2 0
[RTA-acl-adv-3001] rule permit ip source 192.168.1.3 0
//配置规则允许内部服务器和特定主机访问外部网
[RTA-acl-adv-3001] rule deny ip
//配置规则禁止所有 IP 包通过

[RTA-acl-adv-3001] interface Ethernet 0/0
[RTA-Ethernet0/0] firewall packet-filter 3001 inbound
//将规则 3001 作用于从接口 Ethernet0/0 进入的包

[RTA-Ethernet0/0] acl number 3002
//创建访问控制列表 3002
[RTA-acl-adv-3002] rule permit ip source 192.168.160.2 0 destination 192.168.1.1 0
[RTA-acl-adv-3002] rule permit ip source 192.168.160.2 0 destination 192.168.1.3 0
//配置规则允许特定用户从外部网访问内部特定主机
[RTA-acl-adv-3002] rule deny ip
//配置规则禁止所有 IP 包通过

[RTA-acl-adv-3002]interface Ethernet 0/1
[RTA-Ethernet0/1] firewall packet-filter 3002 inbound
//将规则 3002 作用于从接口-Ethernet0/1 进入的包

7、测试验证

使用命令 display acl all 显示配置的访问控制列表的规则。防火墙配置完成后，PC4 可以 Ping 通 PC1，但不能访问 PC2。PC3 可以 Ping 通 PC4。改变 PC4 的 IP 地址，则不能访问内部网。改变规则顺序，，将命令 rule deny ip 放在第一条，则内外网之间的 PC 无法通信。删除 ACL 规则的命令为 undo rule <*规则编号*>，这条命令在控制列表视图下完成。

8.3.2 ACL 实验二（按照自动排序匹配）

实验说明：本实验是由两个独立的小实验组成，即标准 ACL 和扩展 ACL。标准 ACL 实验只完成第 1、2、3、4、5、6、7、9、10 步骤，扩展 ACL 实验只完成第 1、2、3、4、5、6、8、9、10 步骤。

1、软硬件要求：路由器 2 台，交换机 2 台，计算机 4 台，Console 线 2 根，网线若干。

2、网络拓扑图：

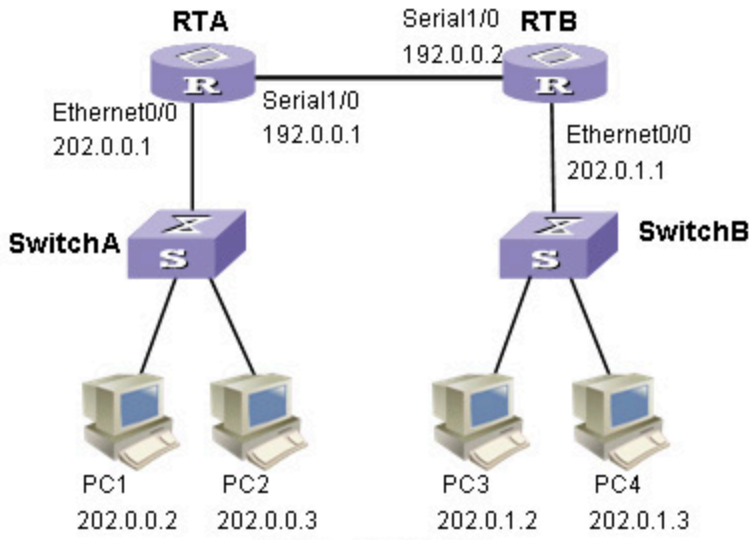

图 8-2 ACL 实验二

3、实验要求

PC1、PC2 属于内部网，PC3、PC4 属于外部网。通过配置防火墙，PC1 可以与外部网的 PC 进行通信，PC2 不能与外部网的 PC 进行通信。

4、连接设备

按照图 8-2 连线。路由器 RTA 和 RTB 的同/异步串口 Serial 1/0 通过 DTE 和 DCE 电缆相连，交换机 SwitchA 的端口 ethernet 1/0/1 与路由器 RTA 的以太网接口 Ethernet 0/0 通过网线相连，交换机 SwitchB 的端口 ethernet 1/0/1 与路由器 RTB 的以太网接口 Ethernet 0/0 通过网线相连。PC1、PC2 和连接在 SwitchA 的端口 ethernet 1/0/2、ethernet 1/0/3 上，PC3、PC4 连接在 SwitchB 的端口 ethernet 1/0/2、ethernet 1/0/3 上。

路由器 RTA 的 Ethernet 0/0 接口地址是 202.0.0.1/24，Serial1/0 接口地址是 192.0.0.1/24。路由器 RTB 的 Ethernet 0/0 接口地址是 202.0.1.1/24，Serial1/0 接口地址是 192.0.0.2/24。PC1 的地址是 202.0.0.2/24，PC2 的地址是 202.0.0.3/24，PC1 和 PC2 的缺省网关地址是 202.0.0.1。PC3 的地址是 202.0.1.2/24，PC4 的地址是 202.0.1.3/24，PC3 和 PC4 的缺省网关地址是 202.0.1.1。

5、观察

配置好 IP 地址，然后在路由器上启动 RIP 协议，使用 Ping 命令测试，观察各个 PC 之间是否能够通信，路由器的各个接口是否能够通信。

6、在路由器 RTA 上配置各端口地址、启动 RIP 协议并打开防火墙

```
<Quidway> system-view
//进入系统视图
[Quidway] sysname RTA
//修改系统名称

[RTA] interface Ethernet 0/0
[RTA-Ethernet0/0] ip address 202.0.0.1 255.255.255.0
[RTA-Ethernet0/0] interface Serial 1/0
[RTA-Serial1/0] ip address 192.0.0.1 255.255.255.0
[RTA-Serial1/0] rip
[RTA-rip] network 202.0.0.0
[RTA-rip] network 192.0.0.0
```

//在路由器 RTA 上启动 RIP 协议

[RTA] firewall enable
//在路由器 RTA 上允许防火墙
[RTA] firewall default permit
//设置防火墙缺省过滤方式为允许包通过

7、 创建标准 ACL
[RTA] acl number 2008 match-order auto
//创建访问控制列表 2008
[RTA-acl-basic-2008] rule deny source 202.0.0.0 0.0.0.255
//禁止 202.0.0.0 网段访问外部网络
[RTA-acl-basic-2008] rule permit source 202.0.0.2 0.0.0.0
//允许特定主机 202.0.0.2 访问外部网络
[RTA-acl- basic-2008] interface Serial 1/0
[RTA- Serial1/0] firewall packet-filter 2008 outbound
//将规则 2008 作用于接口 Serial 1/0，方向为出

8、 创建扩展 ACL
[RTA-acl-basic-2008] acl number 3008 match-order auto
[RTA-acl-adv-3008]rule deny ip source 202.0.0.0 0.0.0.255
destination 202.0.1.0 0.0.0.255
//禁止 202.0.0.0 网段访问外部网络
[RTA-acl-adv-3008] rule permit ip source 202.0.0.2 0.0.0.0
destination 202.0.1.0 0.0.0.255
//允许特定主机 202.0.0.2 访问外部网络
[RTA-acl-adv-3008] interface Serial 1/0
[RTA- Serial1/0] firewall packet-filter 3008 outbound
//将规则 3008 作用于接口 Serial 1/0，方向为出

9、在路由器 RTB 上的配置配置各端口地址并启动 RIP 协议
<Quidway> system-view
//进入系统视图
[Quidway] sysname RTB
//修改系统名称

[RTB] interface Ethernet 0/0
[RTB-Ethernet0/0] ip address 202.0.1.1 24 255.255.255.0
[RTB-Ethernet0/0] interface Serial 1/0
[RTB-Serial1/0] ip address 192.0.0.2 255.255.255.0

[RTB-Serial1/0] rip
[RTB-rip] network 202.0.1.0
[RTB-rip] network 192.0.0.0

//在路由器 RTB 上启动 RIP 协议

10、测试验证

使用命令 display acl all 显示配置的访问控制列表的规则。PC1 可以 Ping 通 PC3、PC4，PC2 不能访问 PC3、PC4。由于自动排序使用“深度优先”的原则，因此改变 ACL 规则的顺序，对防火墙功能没有影响。

8.3.3 包过滤日志实验

1、软硬件要求：路由器 1 台，交换机 1 台，计算机 1 台，Console 线 1 根，网线若干。

2、网络拓扑图：

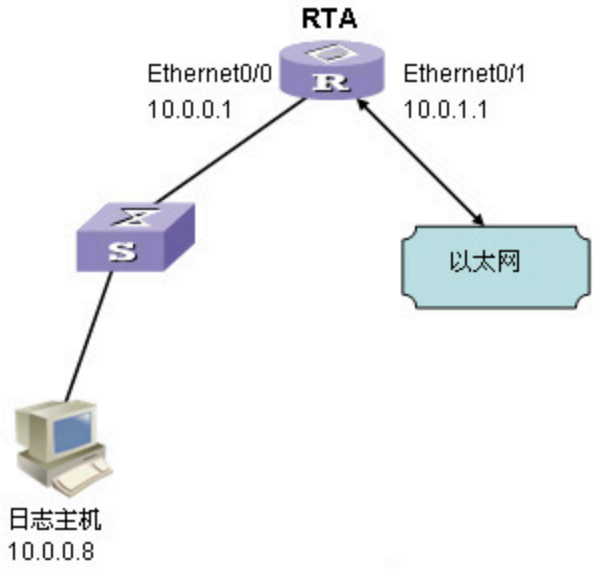

图 8-3 包过滤日志实验

3、实验要求

日志主机地址 10.0.0.8，每天 08:30-18:00 禁止报文送出 ethernet0/1，禁止 PC Telnet 到 Router。

4、连接设备

按照图 8-3 连线。

5、在路由器 RTA 上的配置

<Quidway> system-view

//进入系统视图

[Quidway] sysname RTA

//修改系统名称

[RTA] info-center loghost 10.0.0.8

//记录到日志主机 10.0.0.8 上

[RTA] firewall enable

//启动防火墙

[RTA] acl number 2000

[RTA-acl-basic-2000] rule 0 deny logging

//禁止所有日志

[RTA-acl-basic-2000] acl number 3000
[RTA-acl-adv-3000] rule 0 deny tcp destination 10.0.1.1 0 destination-port eq telnet logging
[RTA-acl-adv-3000] rule 1 deny tcp destination 10.0.0.1 0 destination-port eq telnet logging
//禁止任何源地址 telnet 到 RTA，对违反的报文做日志记录
[RTA-acl-adv-3000] time-range time_range 08:30 to 18:30 daily
//访问控制规则生效的时间段

[RTA] interface Ethernet0/0
[RTA-Ethernet0/0] ip address 10.0.0.1 255.0.0.0
[RTA-Ethernet0/0] firewall packet-filter 3000 inbound
[RTA-Ethernet0/0] firewall packet-filter 2000 outbound

[RTA-Ethernet0/0] interface Serial1/0
[RTA- Serial1/0] ip address 10.0.1.1 255.0.0.0
[RTA- Serial1/0] firewall packet-filter 3000 inbound

8.3.4 地址转换实验

1、软硬件要求：路由器 1 台，交换机 2 台，计算机 4 台，Console 线 1 根，网线若干。
2、网络拓扑图：

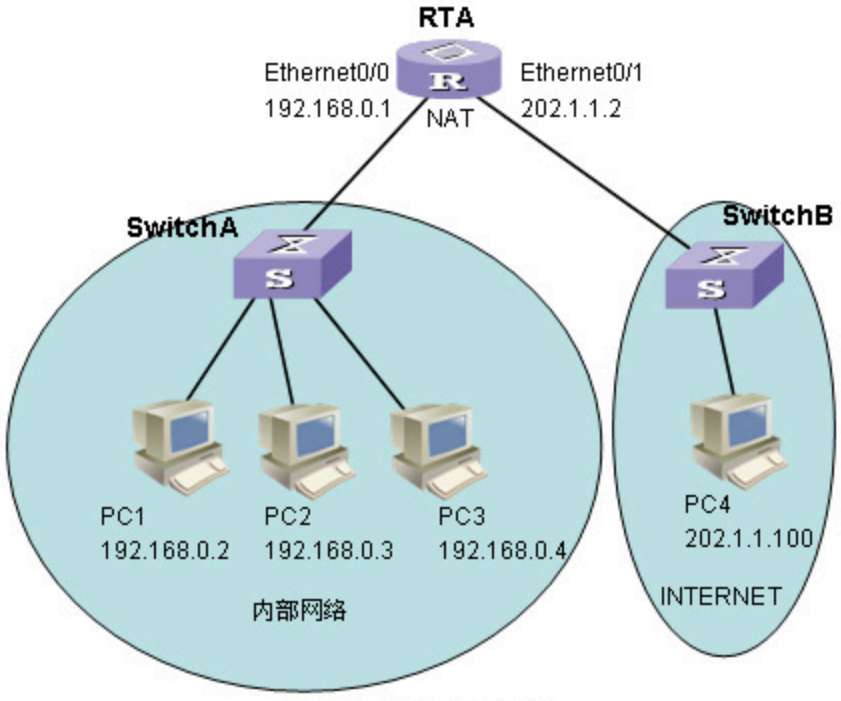

图 8-4 地址转换实验

3、连接设备

按照图 8-4 连线。交换机 SwitchA 的端口 ethernet 1/0/1 与路由器 RTA 的以太网接口 Ethernet 0/0 通过网线相连，交换机 SwitchB 的端口 ethernet 1/0/1 与路由器 RTA 的以太网接口 Ethernet 0/1 通过网线相连。PC1、PC2 和 PC3 连接在 SwitchA 的端口 ethernet 1/0/2 -ethernet

1/0/4 上，PC4 连接在 SwitchB 的端口 ethernet 1/0/2 上。

路由器 RTA 的 Ethernet 0/0 接口地址是 192.168.0.1/24，Ethernet 0/1 接口地址是 202.1.1.2/24。PC1 地址是 192.168.0.2/24，缺省网关地址是 192.168.0.1。PC2 地址是 192.168.0.3/24，缺省网关地址是 192.168.0.1。PC3 IP 地址是 192.168.0.4/24，缺省网关地址是 192.168.0.1。PC4 为外部主机，IP 地址是 202.1.1.3/24，缺省网关地址是 202.1.1.2。

4、在路由器上的配置

```
<Quidway> system-view
//进入系统视图
[Quidway] sysname RTA
//修改系统名称

[RTA] acl number 2000
[RTA-acl-basic-2000] rule permit source 192.168.0.0 0.0.0.255
//配置允许进行 NAT 转换的内网地址段
[RTA-acl-basic-2000] rule deny

[RTA-acl-basic-2000] interface Ethernet0/0
[RTA-Ethernet0/0] ip address 192.168.0.1 255.255.255.0
//内网网关地址

[RTA-Ethernet0/0] interface Ethernet0/1
[RTA-Ethernet0/1] ip address 202.1.1.2 255.255.255.248
//出接口地址

[RTA-Ethernet0/1] nat outbound 2000
//在出接口上进行 NAT 转换
```

5、测试验证

使用命令 display acl all 显示配置的访问控制列表的规则。使用 Ping 命令测试，PC1-PC3 可以 Ping 通 PC4。PC4 上安装抓包软件，捕捉 PC1-PC3 传输的数据包，分析 IP 地址。

8.3.5 地址池 NAT 实验

1、软硬件要求：路由器 1 台，交换机 2 台，计算机 4 台，Console 线 1 根，网线若干。

2、网络拓扑图：

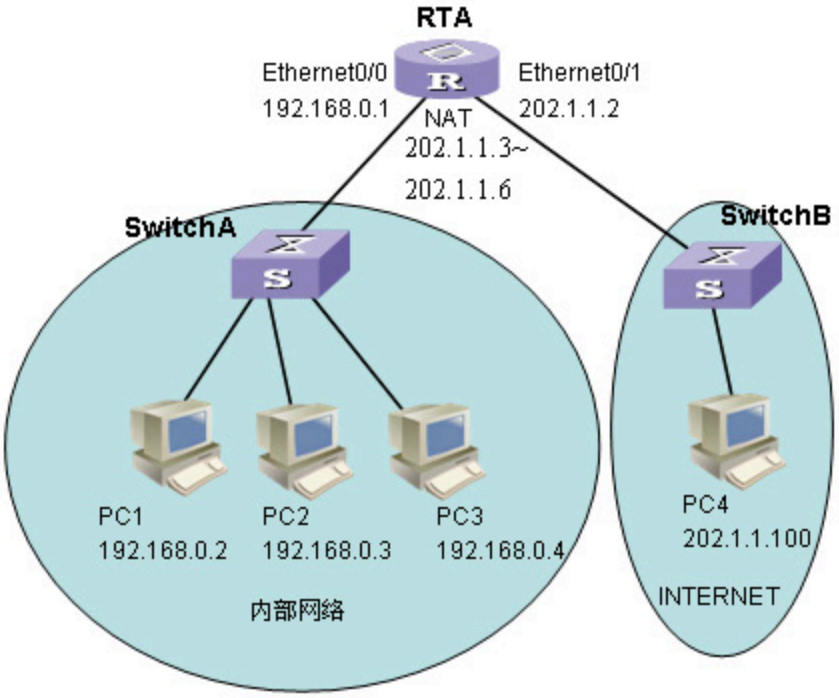

图 8-5 地址池 NAT 实验

3、连接设备

按照图 8-5 连线。交换机 SwitchA 的端口 ethernet 1/0/1 与路由器 RTA 的以太网接口 Ethernet 0/0 通过网线相连，交换机 SwitchB 的端口 ethernet 1/0/1 与路由器 RTA 的以太网接口 Ethernet 0/1 通过网线相连。PC1、PC2 和 PC3 连接在 SwitchA 的端口 ethernet 1/0/2 -ethernet 1/0/4 上，PC4 连接在 SwitchB 的端口 ethernet 1/0/2 上。

路由器 RTA 的 Ethernet 0/0 接口地址是 192.168.0.1/24，Ethernet 0/1 接口地址是 202.1.1.2/24。PC1 地址是 192.168.0.2/24，缺省网关地址是 192.168.0.1。PC2 地址是 192.168.0.3/24，缺省网关地址是 192.168.0.1。PC3 IP 地址是 192.168.0.4/24，缺省网关地址是 192.168.0.1。PC4 为外部主机，IP 地址是 202.1.1.100/24，缺省网关地址是 202.1.1.2。

4、在路由器上的配置

```
<Quidway> system-view
//进入系统视图
[Quidway] sysname RTA
//修改系统名称

[RTA] acl number 2000
[RTA-acl-basic-2000] rule permit source 192.168.0.0 0.0.0.255
//配置允许进行 NAT 转换的内网地址段
[RTA-acl-basic-2000] rule deny
[RTA-acl-basic-2000] nat address-group 0 202.1.1.3 202.1.1.6
//用户 NAT 的地址池

[RTA] interface Ethernet0/0
[RTA-Ethernet0/0] ip address 192.168.0.1 255.255.255.0
//内网网关

[RTA-Ethernet0/0] interface Ethernet0/1
```

[RTA-Ethernet0/1] ip address 202.1.1.2 255.255.255.0

[RTA-Ethernet0/1] nat outbound 2000 address-group 0

//在出接口上进行 NAT 转换

5、测试验证

使用命令 display nat all 查看所有的关于地址转换的信息。使用命令 display acl all 显示配置的访问控制列表的规则。使用 Ping 命令测试，PC1-PC3 可以 Ping 通 PC4。PC4 上安装抓包软件，捕捉 PC1-PC3 传输的数据包，分析 IP 地址。

8.4 思考题

（1）防火墙的作用是什么？

（2）ACL 如何分类？各自用于什么情况？

（3）NAT 的工作原理是怎样的？