6 实验六 RIP 协议分析

6.1 实验目的

1）理解路由协议的分类，掌握静态路由和 RIP 协议的配置方法；
2）分析掌握 RIP 报文结构及各字段的含义；
3）分析两个路由设备之间 RIP 报文的交换及路由表的构建过程。

6.2 实验内容

1）在路由器、三层交换机上依次配置**静态路由、缺省路由和 RIP 协议**，然后分别用 ping 命令测试网络的连通性。

2）在路由器和三层交换机上配置 RIP 协议，在计算机上使用报文分析软件截获 RIP 报文，**分析 RIP 报文各字段的含义**。

3）采用镜像技术，捕获两个路由设备之间交换的 RIP 报文，分析**两个设备中路由表的构建情况**。

6.3 实验原理

路由器以两种基本方式构建非直连路由。一是可以使用预设值的静态路由，二是使用通过任何一种动态路由协议来动态计算路由。路由器使用动态路由协议发现路由，并通过这些路由来转发报文。

动态路由协议按照其所执行的算法不同，可以分为距离矢量路由协议、链路状态路由协议，以及混合型路由协议。

RIP 协议的全称是路由信息协议（Routing Information Protocol），它是一种内部网关协议，用于一个自治系统内的路由信息的传递。RIP 协议是基于距离矢量（Distance Vector）算法的，它使用“跳数”，即 metric 来衡量到达目标地址的路由距离。RIP 协议用于使用同种技术的中型网络，对于更复杂的环境，一般不使用 RIP 协议。

RIP 进程运行于路由器中，负责从网络中的其它路由器接收路由信息，从而对本地 IP 路由表进行动态维护，保证 IP 层发送报文时选择正确的路由，同时广播本路由器的路由信息，通知相邻路由器作相应的修改。RIP 协议使用 UDP 通信，所接收的路由信息都封装在 UDP 的数据报中，RIP 在 520 号端口上接收来

自远程路由器的路由修改信息，并对本地的路由表做相应的修改，同时通知其它路由器。通过这种方式，达到全局路由的有效。

6.4 实验环境与分组

1）DCR5650 三层交换机 2 台(S1，S2)，DCR2626 路由器 1 台(R1)。

2）每 4 人一组，共同配置设备，完成实验。

6.5 实验组网

图 5-1 是本实验的组网图，图中的参数只作为参考，鼓励各小组灵活自定义 IP 地址、端口等参数。

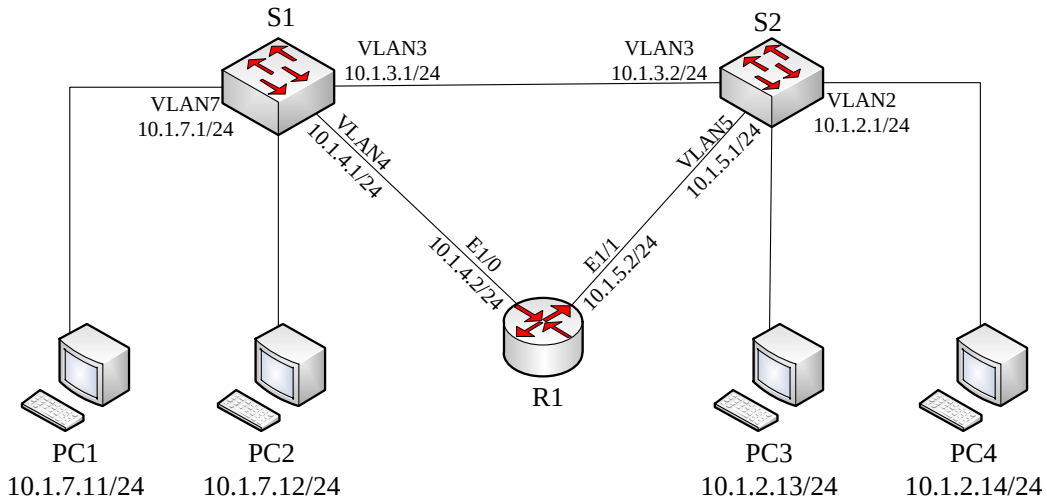

图 5-1 RIP 协议配置组网拓扑图

6.6 RIP 启动与路由分析

将交换机、路由器恢复为出厂设置，参考命令如下：

交换机：

```
Switch> enable   !进入特权用户模式
Switch# set default   !启动初始化
Are you sure? [Y/N] = y   ！确认初始化，显示初始化信息
Switch# write   ！写入初始化信息到启动文件
Switch# reload   ！重新启动交换机
```

路由器：

```
Router>enable              !进入特权用户配置模式
Router#delete              !恢复出厂设置
Router#reboot              !重启路由设备
```

步骤 1：按照图 5-1 所示连接好设备，配置各 PC 的 IP 地址、子网掩码和网关。配置交换机和路由器各接口的 IP 地址。参考命令如下：

配置交换机 S1：

```
switch(Config)# hostname S1       ！改名以方便配置操作
S1(Config)# vlan 3
S1(Config-vlan3)# switchport interface ethernet 0/0/1
S1(Config-vlan3)# exit
S1(Config)# interface vlan 3
S1(Config-If-Vlan3)# ip address 10.1.3.1 255.255.255.0
```

同理配置交换机 S1 其他 vlan。

配置路由器 R1：

```
Router#config
Router(Config)# hostname R1！改名以方便配置操作
R1(config)# interface    e1/0
R1(config-if)#ip    address    10.1.4.2    255.255.255.0
```

同理配置 R1 的接口 e1/1。

此时，测试 PC1、PC2 和 S1 之间是否可以互相通信，测试 R1 和 S1 之间是否可以互相通信。在 R1 上 ping 两台机器 PC1 和 PC2，看能否 ping 通，通过各自的路由表分析原因。

```
R1# show    ip    route        ！查看路由表
```

步骤 2：在 R1 上配置 10.1.7.0/24 的静态路由。命令如下：

```
R1(config)# ip route 10.1.7.0 255.255.255.0 10.1.4.1
```

在 R1 上 ping 各个 PC 看能否 ping 通，查看各自的路由表，分析原因。

步骤 3：删除步骤 2 配置的静态路由：

```
R1(config)# no ip route 10.1.7.0 255.255.255.0 10.1.4.1
```

步骤 4：在 S1 和 R1 分别启动 RIP 协议。命令如下：

在交换机 S1 启动 RIP 协议命令：

```
S1(Config)# router rip                ！激活 RIP 进程
S1(Config-router)#version  2          ！指定 RIP 版本
S1(Config-router)#network vlan3       ！指定 RIP 相关网络号
S1(Config-router)#network vlan4
S1(Config-router)#network vlan7
```

在路由器 R1 启动 RIP 协议命令：

```
R1(config)# router rip
R1(config-rip)# version  2          ！指定 RIP 版本
R1(config-rip)# network 10.1.4.0 255.255.255.0
R1(config-rip)# network 10.1.5.0 255.255.255.0
```

测试 R1 和各个 PC 的连通性，查看 S1 和 R1 的路由表信息，将路由表信息填入检查单的表 5-1 中，分析原因，回答相关问题。

表 5-1 路由表信息

设备	Destination/Mask	Protocol	Pref	Cost	Nexthop	Interface
S1						
R1						

Pref：路由表项优先级；Cost：路由表项代价。

常见路由种类及优先级：

路由种类	优先级
D-Direct	0
S-STATIC	1
E-OSPF	110
R-RIPv1、v2	120
B-BGP	200
……	

步骤 5：在 S2 上配置各个 VLAN 以及接口地址，并启动 RIP 协议（命令参考 S1 的配置），并测试各个 PC 机之间的连通性。在 PC1 上用 ***tracert -d 10.1.2.14***（PC4 的 IP 地址），查看 PC1-PC4 的路由连通路径。

步骤 6：拔掉 S1 与 S2 的直连线，测试 PC2 与 PC3 的连通性，在 PC2 上用

tracert -d 10.1.2.13，查看 PC2-PC3 的路由连通路径。（如果不能连通，请过一段时间重新测试。）

6.7 RIP 报文结构及路由的更新

6.7.1 RIP 报文结构

RIP 报文可分为请求信息的报文（Request 报文）和应答信息报文（Response 报文），格式相同，由固定的首部和可选的网络的 IP 地址和到该网络的跳数组成，RIP 协议有两个版本，即版本 1（RFC 1058）和版本 2（RFC 2453），实验是以版本 2 为例进行测试实验。图 5-3 是 RIP 版本 2 的报文格式：

0 8 16 32

命令 Command	版本 Version	必须为 0
地址类型标志符 Address family identifier		路由标签 Route Tag
IP 地址		
子网掩码 Subnet mask		
下一跳 Next Hop		
metric		

图 5-3 RIP（版本 2）报文的格式

命令 Command 字段为 1 时表示 RIP 请求，为 2 时表示 RIP 应答。地址类型标志符在实际应用中总是为 2，即地址类型为 IP 地址。“IP 地址”字段表明目的网络地址，“Metric”字段表明了到达目的网络所需要的“跳数”。距离度量值用跳数来衡量，取值范围是 1－16，其中 16 表示无限远（不可达路由）。路由器每经过 30 秒发送一次 Response 报文，这种报文用广播方式传播。

RIP 版本 1 对 RIP 报文中“版本”字段的处理：

“版本”字段为 0，忽略该报文；“版本”字段为 1 表示是 RIP 版本 1 报文，检查报文中“必须为 0”的字段，若不符合规定，忽略该报文。

“版本”字段>1 时，不检查报文中“必须为 0”的字段，仅处理 RFC 1058 中规定的有意义的字段。因此，运行 RIP 版本 1 的机器能够接收处理 RIP 版本 2 的报文，但会丢失其中的 RIP 版本 2 新规定的那些信息。

RIP 版本 1 不能识别子网网络地址，因为在其传送的路由更新报文中不包含子网掩码，因此 RIP 路由信息要么是主机地址，用于点对点链路的路由；要么是 A、B、C 类网络地址，用于以太网等的路由；另外，还可以是 0.0.0.0，即缺省路由信息。RIP 版本 2 使用了版本 1 中“必须为 0”的字段，增加了一些对于路由

的有用信息，其主要新添的特性有①报文中包含子网掩码，可以进行子网路由；②支持明文/MD5 验证；③报文中包含了下一跳 IP，为路由的选优提供了更多的信息。路由标签 Route Tag 用于区分或者过滤路由。

6.7.2 RIP 路由表的更新

路由器最初启动时只包含了其直连网络的路由信息，并且其直连网络的 metric 值为 1，然后它向周围的邻居路由器发出完整路由表的 RIP 请求。路由器根据接收到的 RIP 应答来更新其路由表。若接收到与已有表项的目的地址相同的路由信息，则分别对待①已有表项的来源端口与新表项的来源端口相同，那么无条件根据最新的路由信息更新其路由表；②已有表项与新表项来源于不同的端口，那么比较它们的 metric 值，将 metric 值较小的一个最为自己的路由表项；③新旧表项的 metric 值相等，普遍的处理方法是保留旧的表项。

路由器每 30 秒发送一次自己的路由表（以 RIP 应答的方式广播出去）。针对某一条路由信息，如果 180 秒以后都没有接收到新的关于它的路由信息，那么将其标记为**失效，即 metric 值标记为 16。**在另外的 120 秒以后，如果仍然没有更新信息，该条失效信息被**删除**。

6.8 RIP 报文捕获及结果分析

步骤 7：在前面配置的基础上，将交换机 S1 与 R1 相连接的端口镜像到 S1 与 PC1 相连接的端口。参考命令如下（配置端口以实际连接端口为准）：

```
S1(Config)#monitor session 1 source interface ethernet 0/0/1 both
S1(Config)#monitor session 1 destination interface ethernet 0/0/3
```

步骤 8：停止交换机 S1 上的 RIP 协议；

```
S1(config)# no router rip
```

步骤 9：在 PC1 上运行 WireShark 截获报文，然后在 S1 上启动 RIP 协议（配置命令参考步骤 4）。观察截获的请求报文和应答报文，选择一对 RIP 的请求/应答报文填写在表 5-2 和 5-3 中并理解其含义。

表 5-2 RIP 协议的请求报文

观察点：		字段	值	含义
IP		目的地址		
UDP		端口号		
RIP	头部	命令字段		

		版本号		
	路由信息	地址族标识		
		网络地址		
		跳数		

表 5-3 RIP 协议的应答报文

观察点：		字段	值	含义
IP		目的地址		
UDP		端口号		
RIP	头部	命令字段		
		版本号		
	路由信息	地址族标识		
		网络地址		
		跳数		

互动讨论主题

1）解释名词术语：缺省路由、直连路由、静态路由与动态路由；

2）RIP 构建路由的条件与好处；

3）理解 RIP 构建的路由表及其使用；

4）RIP 报文如何构建路由表；

5）RIP 报文的启动与报文形成次序的关系。

6.9 进阶自设计

在上述实验结果的基础上，自主设计实验（例：把 S1-S2 之间的网线各插拔一次）获取 S1 和 R1 之间的 RIP 交互报文，结合报文分析 S1 和 R1 路由表项的**生成、更新、失效和删除**等过程。