# 实验六 RIP协议分析

## 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。

## 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**。

## 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。

## 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。

## 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

## 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 | 10.1.3.0/24 | RIP | [120,1] | 2 | 10.1.4.1 | Ethernet1/0[0] |
| 10.1.7.0/24 | RIP | [120,1] | 2 | 10.1.4.1 | Ethernet1/0[0] |
| 10.1.4.0/24 | D-Direct | 0 | 1 | 10.1.4.1 | Ethernet1/0[0] |
| 10.1.5.0/24 | D-Direct | 0 | 1 | 10.1.5.1 | Ethernet1/1[0] |

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。）

## RIP报文结构及路由的更新

### 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。

### 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**。

## 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。

## 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。