实验十九 RIP 路由报文结构分析

【实验目的】

1. 掌握动态路由协议 RIP 的报文结构，工作原理及工作过程；
2. 掌握 RIP 路由协议两个版本的区别。

【实验学时】

2 学时

【实验环境】

在本实验中需要 3 台路由器、1 台交换机、1 台协议分析仪。3 台路由器运行 RIP 路由协议，使用协议分析仪采集数据包，对采集到的数据进行分析。

将所有的路由器都接入到交换机上，并在交换机上配置端口映像功能，具体 IP 分配如下表：

表 6-1 设备 IP 地址分配表

设备	接口	IP 地址	连接到交换机
RSR-A	FA0/0	192.168.1.1/24	FA0/8
RSR-A	LO0	192.168.10.1/24	--
RSR-B	FA0/0	192.168.1.2/24	FA0/9
RSR-B	FA0/1	192.168.2.1/24	FA0/10
RSR-B	LO0	192.168.20.1/24	--
RSR-C	FA0/0	192.168.2.2/24	FA0/7
RSR-C	LO0	192.168.30.1/24	--
RG-PATS 协议分析仪	Eth 0	172.16.1.4	FA0/24

设备连接如下图所示：

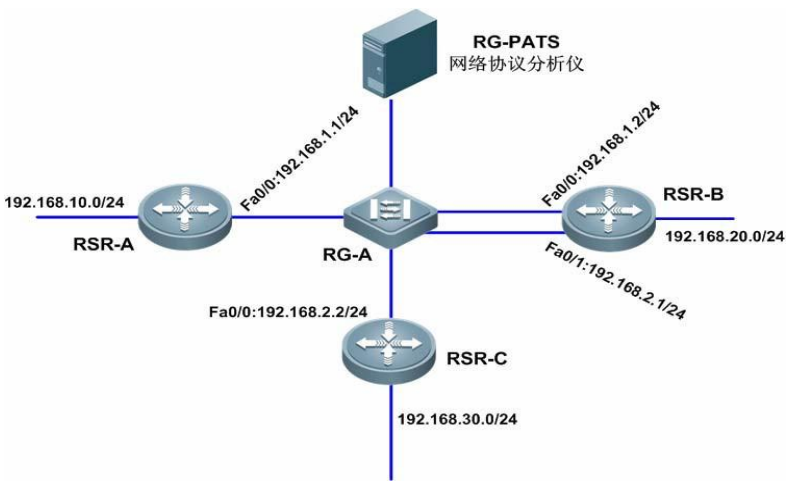
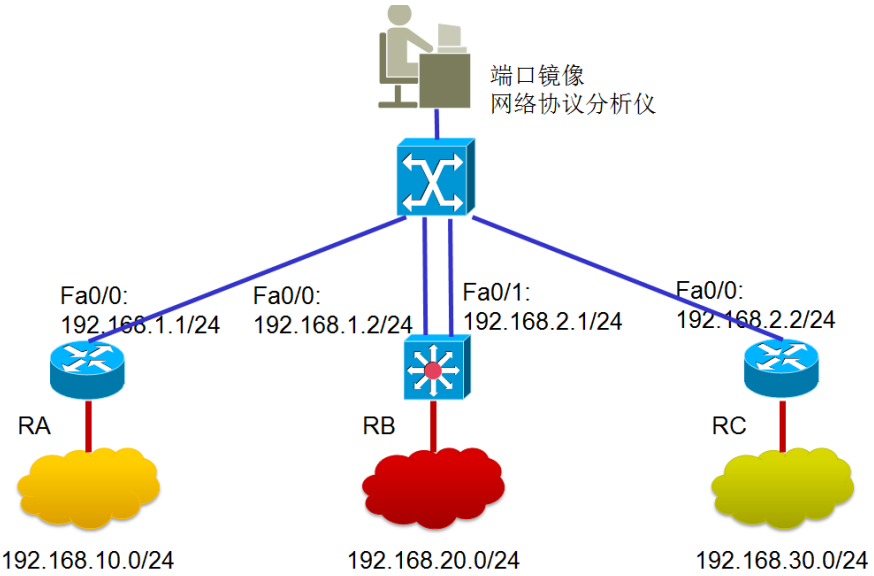


图 6-4 实验拓扑图

注意：在实验室环境下，为了观测路由器之间的交互，将不同路由器都接到同一个交换机上，通过端口镜像将路由器之间的报文转发到指定的主机上，再用网络协议分析仪软件进行观测。同时，由于路由器实际设备的缺乏，我们通过“三层交换机关闭交换功能”来模拟路由器。实验的拓扑示意图为：



【三层交换机配置路由命令】

三层交换机命令：启动某个接口的路由功能/关闭交换功能

```
Switch> enable 14
Switch# configure terminal
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#no switchport
! 关闭 Fa0/1 的交换功能
Switch(config-if)#ip address 192.168.1.2 255.255.255.0
! 配置该接口的 ip 地址
Switch(config-if)#exit
! 退回到上一级配置级别
Switch(config)#
```

注意：不关闭交换功能，交换机接口无法设置 IP

三层交换机/路由器的公共命令：启动 IP 路由，配置 RIP 协议

```
Router(config)#ip routing
! 启动路由功能
Router(config)#router rip
! 进入对 rip 协议的配置
Router(config-router)#version 1
! 设置 rip 协议为版本 1
Router(config-router)#network 192.168.10.0
! 设置 rip 协议为版本 1
Router(config-if)#exit
```

```
！退回到上一级配置级别
Router(config)#
```

三层交换机/路由器的公共命令：观察 IP 层协议状态/路由表

```
Router# show ip protocols
！查看当前使用什么路由协议/及其配置情况
Router# show ip route
！查看当前路由表
Router# debug ip rip packet
！进入调试 rip 协议的状态，每个 rip 报文的收发都将被输出到终端屏幕上
Router# no debug ip rip packet
！关闭 rip 协议的调试状态
```

三层交换机命令：清除路由功能

```
Switch> enable 14
Switch# configure terminal
Switch(config)#no ip routing
！关闭 ip 路由功能，rip 配置将同时被删除
Switch(config)#
```

三层交换机命令：清除各接口的 ip 配置

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport
！启动 Fa0/1 的交换功能
Switch(config-if)#no ip address
！清除该接口的 ip 地址
Switch(config-if)#shutdown
！关闭该接口
Switch(config-if)#exit
！退回到上一级配置级别
Switch(config)#
```

路由器命令：清除路由功能

```
Router> enable 14
Router# configure terminal
Router(config)#no ip routing
！关闭 ip 路由功能，rip 配置将同时被删除
Router(config)#
```

路由器命令：清除各接口的 ip 配置

```
Router(config)#interface fastEthernet 0/1
Router(config-if)#no ip address
！清除该接口的 ip 地址
Router(config-if)#shutdown
！关闭该接口
Router(config-if)#exit
```

```
! 退回到上一级配置级别
Router(config)#
```

【实验内容】

1、学习 RIP 协议的报文格式；
2、掌握 RIP 协议的工作原理，了解 RIP1 和 RIP2 的区别；
3、了解 RIP 协议的缺陷。

【实验流程】

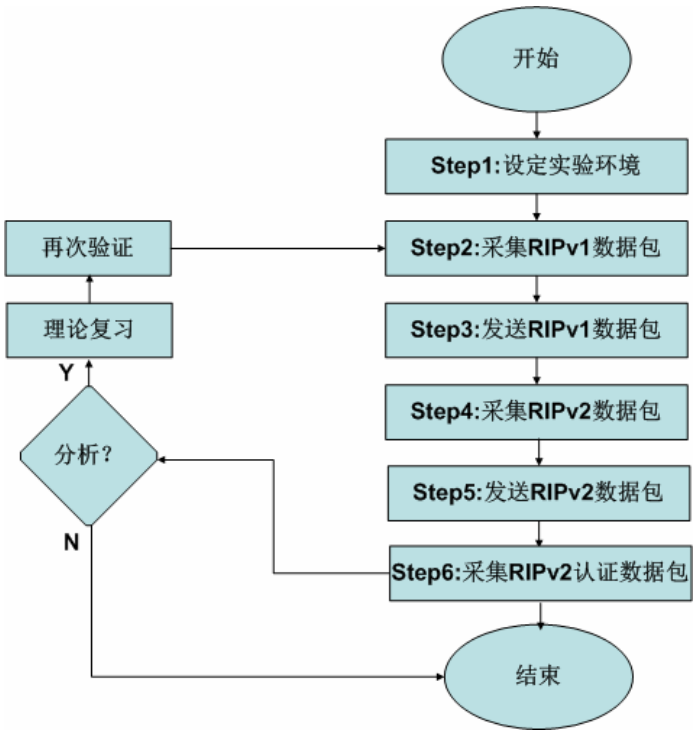


图 6-5 实验流程图

【实验原理】

RIP 协议简介

RIP 路由协议有 RIPv1 和 RIPv2 两个版本，RIPv1 是有类路由协议，其不支持 VLSM， 不支持验证，路由更新采用的广播的方式；而 RIPv2 是无类路由协议，支持 VLSM，支持 验证，路由更新采用组播的方式。RIPv2 首先在 RFC1388“携带额外信息的 RIP 版本 2” 中定义，发布于 1993 年 1 月。该 RFC 在 1732 中做了修订，最终在 1998 年 11 月发布的 RFC2453“RIP 版本 2”中定稿。

为确保 RIP 今后可以和 TCP/IP 一起使用，有必要定义一种能和 IPv6 一起使用的版本，1997 年 RFC2080 发布了标题为“用于 IPv6 的 RIPng”文档。

RIP 路由协议进行路由信息交换是通过发送两种不同类型 RIP 报文实现的：RIP 请求和

响应，这些报文作为常规 TCP/IP 报文，使用 UDP 传输，使用 UDP 端口 520。该端口按照如下方式使用：

- RIP 请求报文发送到UDP 目的端口520，这些报文可以使用520作为源端口，也可以使用一个短暂端口号。
- 为回答RIP 请求面发送的响应报文使用源端口520，其目的端口等于RIP 请求报文使用的端口。
- 未经请求的 RIP 响应报文发送时使用的源端口和目的端口均为 520。

RIP 报文格式

RIP 报文包含在 UDP 数据报中，如下图所示：

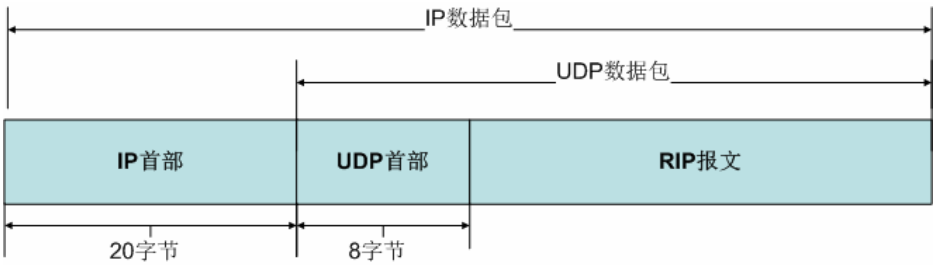


图 6-6 封装在 UDP 数据报的 RIP 报文

下图所示为 RIP 的报文格式：

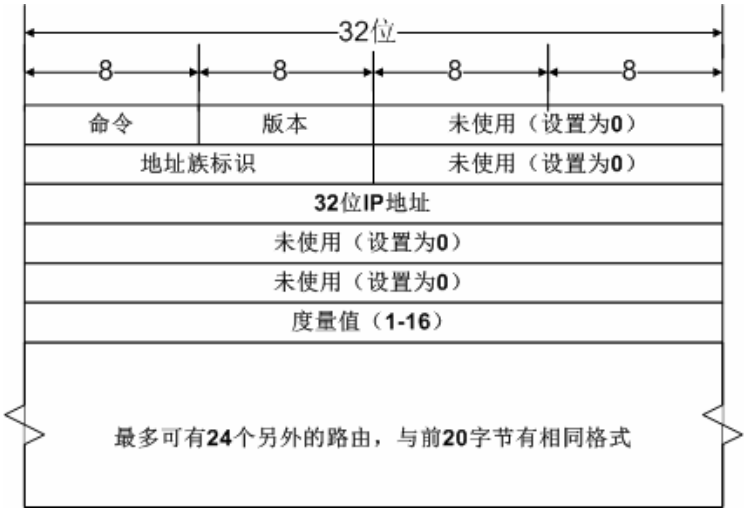


图 6-7 RIP 消息格式

- 命令：命令字段为 1 表示请求，2 表示应答。还有两个舍弃不用的命令（3 和 4），两个非正式的命令：轮询（5）和轮询表项（6）。请求表示要求其他系统发送其全部或部分路由表。应答则包含发送者全部或部分路由表。
- 版本：版本字段通常为1，而第2版RIP将此字段设置为2。

- 地址族标识：紧跟在后面的 20 字节指定地址系列（address family）（对于 IP 地址来说，其值是 2）、IP 地址以及相应的度量。

采用这种 20 字节格式的 RIP 报文可以通告多达 25 条路由。上限 25 条是用来保证 RIP 报文的总长度为 20×25+4=504，小于 512 字节。由于每个报文最多携带 25 个路由，因此为了发送整个路由表，经常需要多个报文。

如下图是使用 RG-PATS 网络协议分析仪采集到的 RIP 报文：

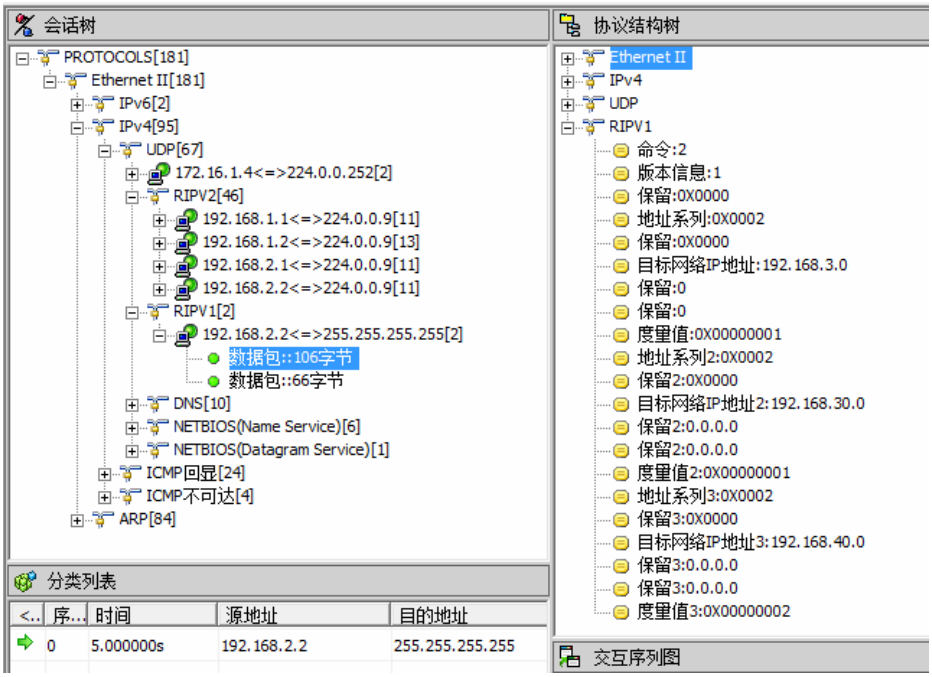


图 6-8 RG-PATS 网络协议分析仪采集 RIP 消息格式

RIP 报文类型

RIP 使用两种报文类型：请求和响应

1、请求报文： 当路由器刚刚接入到网络上，或路由器有一些超时的项目，它就发送请求报文，请求报

文可以询问整个路由表的信息或某个具体的路由信息，如下图所示：

图 6-9 对于特定的路由表信息的请求

图 6-10 对于所有的路由表信息的请求

如下图是使用 RG-PATS 网络协议分析仪采集到的 RIP 请求报文：

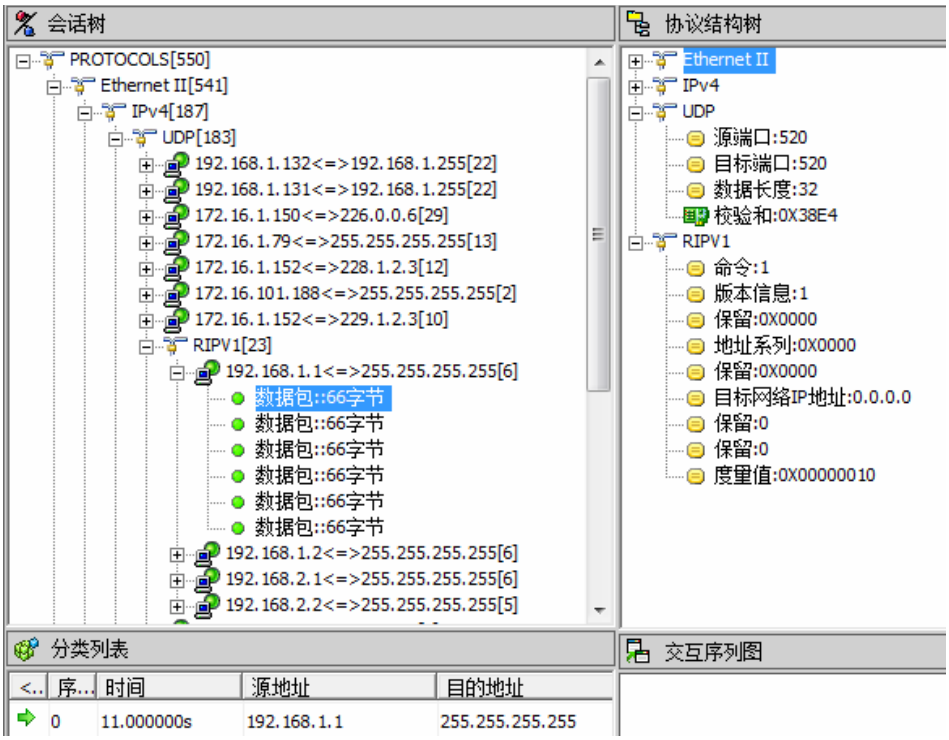


图 6-11 RG-PATS 网络协议分析仪采集 RIP 请求报文

2、响应报文 响应可以是询问的或非询问的，询问的响应仅在回答请求时才发送出来。它包含了在对

应的请求中指明的终点的信息，而非询问的响应则是定期发送，如每隔 30s 或当路由表中有变化时，这种响应有时叫做更新分组，如下图所示：

图 6-12 响应报文

如下图是使用 RG-PATS 网络协议分析仪采集到的 RIP 响应报文：

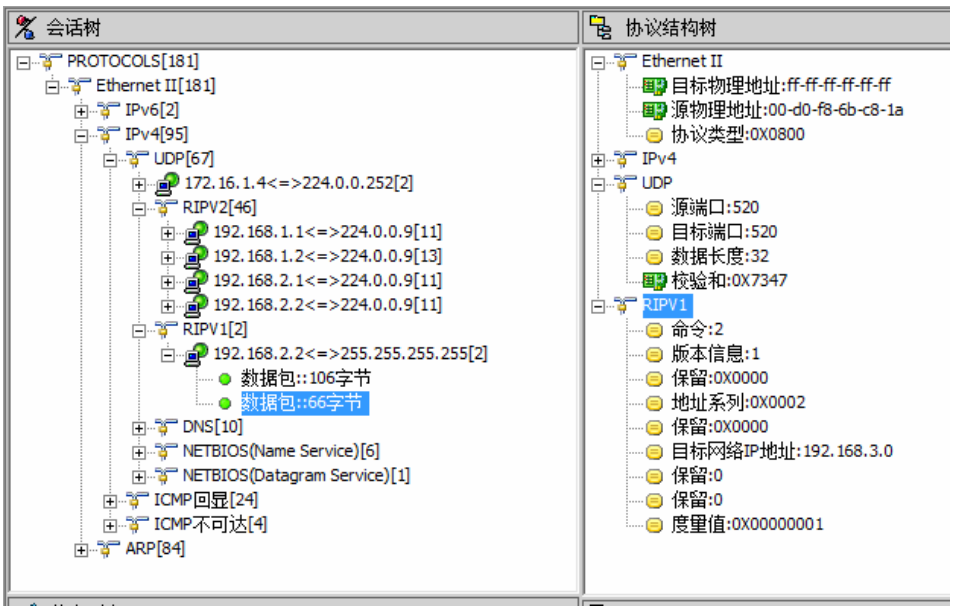


图 6-13 RG-PATS 网络协议分析仪采集 RIP 响应报文

RIPv2 报文格式

设计 RIPv2 版本是为了克服 RIPv1 版本的某些缺点，RIPv2 的设计者没有增大每一个项目的报文长度，他们只是把 RIPv1 中的对 TCP/IP 协议填入 0 的那些字段改为一些新的字段。对其基础上增加了一些扩展特性，以适用于现代网络的路由选择环境，这些扩展我包括：

无类别路由协议：RIPv2 的每一个路由条目都携带子网掩码，因此 RIPv2 支 VLSM。 多播方式路由更新：RIPv1 使用广播方式把 RIP 报文发送给每一个邻居，RIPv2 使用多播的方式向其他使用 RIPv2 的路由器发出更新报文，使用的多播地址是 224.0.0.9，采用多播方式的好处在于，本地网络上和 RIP 路由选择无关的设备不需要花费时间解析路由器广播的更新报文。

与 RIPv1 一样，RIPv2 操作使用的端口号为 UDP520，并且数据报文最大不超过 512 字节。

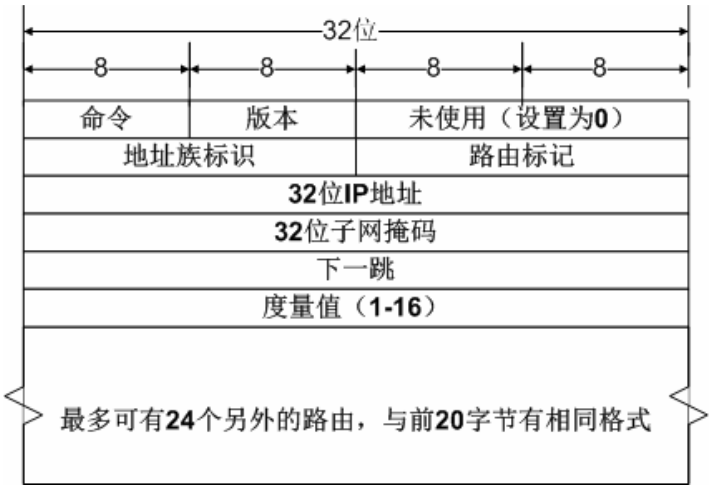


图 6-14 RIPv2 报文格式

- 命令（Command）——只取值 1 或 2，1 表示该消息是请求消息，2 表示该消息是响应消息。其他的取值都不被使用或保留用作私有用途。
- 版本号（Version）——对于 RIPv2，该字段的值设为 2，如果设置为 0 或者虽设置为 1 但消息是无效的 RIPv1 格式，那么这个消息将被丢弃。RIPv2 处理无效的 RIPv1 消息。
- 地址族标识（Address Family Identifier,AFI）------对于 IP 该项设置为 2。只有一个例外的情况，该消息是路由器（或主机）整个路由选择表的请求。
- 路由标记（Route Tag）——提供这个字段用来标记外部外部路由或重分配到 RIPv2 协议中的路由。默认的情况是使用这个 16 位的字段来携带从外部路由选择协议注入到 RIP 中的路由的自治系统号。虽然 RIP 协议自己并不使用这个字段，但是再多个地点和某个 RIP 域相连的外部路由，可能需要使用这个路由标记字段通过 RIP 域来交换路由信息。这个字段也可以用来把外部路由编成“组”，以便在 RIP 域中更容易的控制这些路由。
- IP 地址（IP Address）——路由的目的地址。这一项可以是主网络地址，子网地址或者主机路由地址。
- 子网掩码（Subnet Mask）——是一个确认 IP 地址的网络和子网部分的 32 位的掩码。
- 下一跳（Next Hop）——如果存在的话，它标识一个比通告路由器的地址更好的下一跳地址。换句话说，它指出的下一跳地址，其度量值比在同一个子网上的通告路由器更靠近目的地。如果这个字段设置位全 0（0.0.0.0），说明通告路由器的地址是最好的下一跳地址。
- 度量（Metric）—— Metric 在 RIP 里面指的就是跳数。该字段的取值范围是 1~16 之间。

如下图是使用 RG-PATS 网络协议分析仪采集到的 RIPv2 报文：

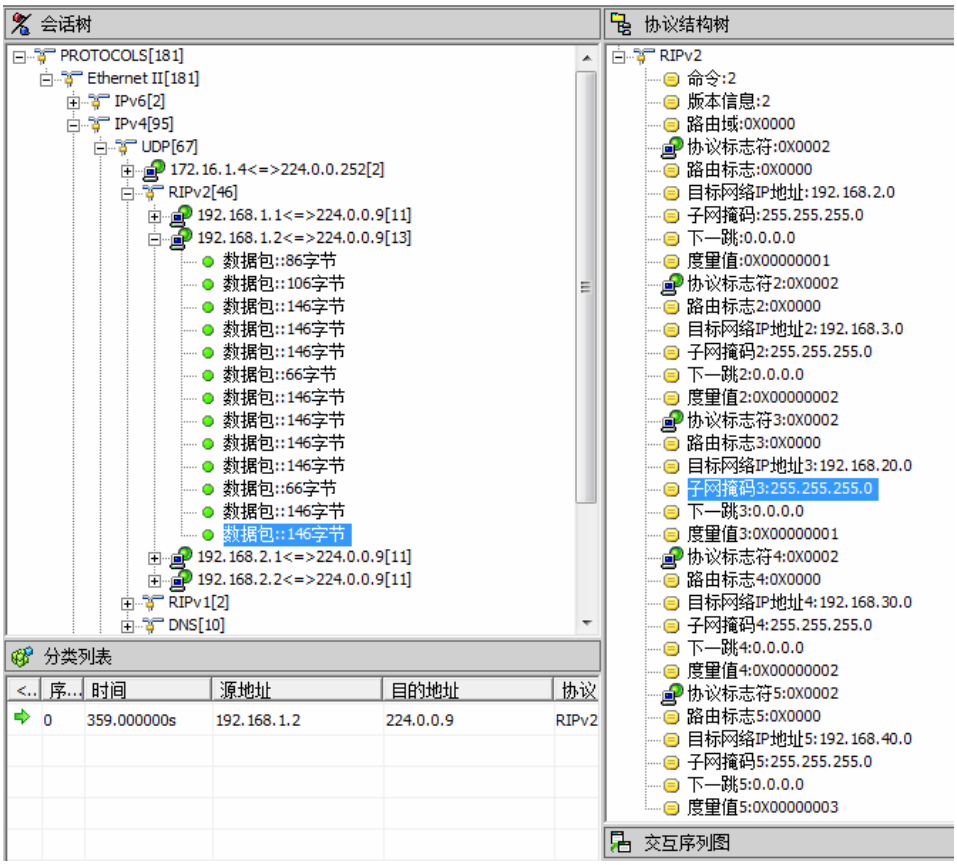


图 6-15 RG-PATS 网络协议分析仪采集 RIPv2 报文

RIP 协议工作原理

每一个路由器定期（每隔 30s）向邻居路由器广播自己的路由表，邻居路由器就是指与其直接相连的所有路由器，如下图所示：路由器 R1 邻居为路由器 R2 和 R4，路由器 R2 的邻居为路由器 R1 和 R3，而路由器 R1 和 R3 不是邻居。RIP 让网络中所有的路由器与其邻居路由器不断交换距离信息，并不断更新路由表。

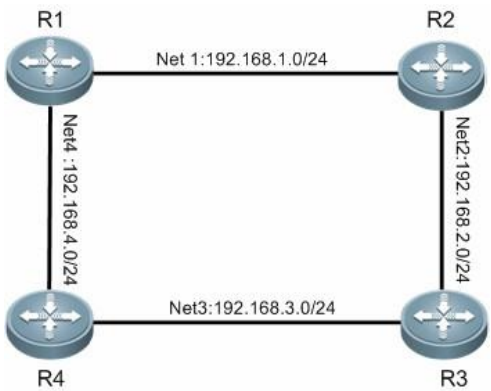


图 6-16 运行 RIP 协议的网络拓扑

1、初始化路由表 当路由器加入到网络时，首先进行路由表初始化，初始状态下，在路由表中只有直连连接的网络，度量值设置为 0，下一跳字段空，下图给出了上图中网络拓扑结构中各个路由器的初始路由表。

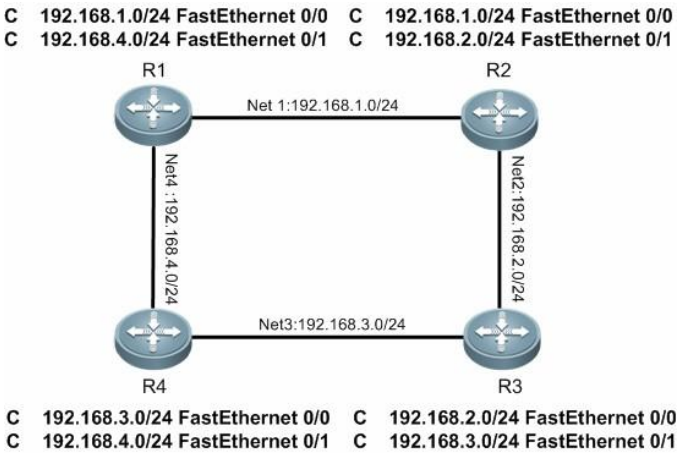


图 6-17 初始状态路由表

2、路由表的更新

下图表示了 RIP 路由算法的流程，根据 RIP 路由更新算法，以路由器 R2 为例，路由器 R2 收到从邻居路由器 R1 和路由器 R3 发来的路由表，这些路由表列出了一些目的网络及相应的跳数。根据 RIP 路由更新算法，首先把邻居站路由表中的跳数增加 1，这是因为，如果路由器 R1 中的路由表项为（192.168.4.0/24），则意味着从路由器 R1 到网络 192.168.4.0 需要 1 跳的距离，那从路由器 R2 经过路由器 R1 到网络 192.168.4.0，就要增加 1 跳的距离。然后根据 RIP 路由更新算法，把邻居路由表中的每一个表项与路由器 R2 中旧的路由表项进行比较，得到路由器 R2 的新路由表。

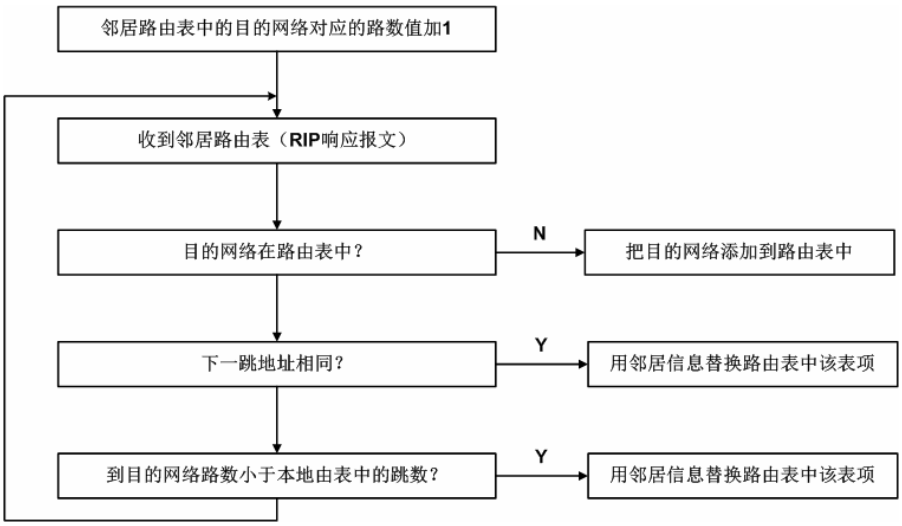


图 6-18 RIP 路由更新算法

3、定期选路更新

每过 30 秒，所有或部分路由器会将其完整路由表发送给相邻路由器。发送路由表可以 是广播形式的（如在以太网上），或是发送给点对点链路的其他终点的。

RIP 优点及缺陷

由于 RIP 路由协议算法简单，所以 RIP 具有操作直接、易于实现且对路由器的处理能力要求很低等优点，这使它对于小型自治系统（AS）特别适合。然而，协议的简单性也导致了一些重大的缺陷。对于数据报的发送而言，跳数经常不是用于选择路由的最佳度量，此外算法本身也存在很多问题，包括收敛（使所有路由器对同一选路信息达成一致所经过的时间）速度慢，以及选路环路、计数到无穷等。RIP 包含了几个专门的特性用来解决其中部分问题，但其他问题则属于协议固有缺陷。

RIP 协议也采用很多特定特性来解决 RIP 的算法问题，比如水平分割、具有毒性逆转 的水平分割、触发更新、抑制等特性。

【实验步骤】

步骤一：设定 RIPv1 路由协议实验环境

注意：对于由三层交换机配置而成的路由器，切记在配置之前先启动其，路由功能，具体命令见实验环境介绍。

1、配置端口映射

```
S3750#
S3750#configure terminal
S3750(config)#monitor session 1 destination interface FastEthernet 0/24
S3750(config)#monitor session 1 source interface FastEthernet 0/1 – 10 both
```

2、在路由器上配置 RIPv1 路由协议

```
RA#configure terminal
RA(config)# interface FastEthernet 0/0
RA(config-if)#ip address 192.168.1.1 255.255.255.0
RA(config)# interface Loopback 0
RA(config-if)#ip address 192.168.10.1 255.255.255.0
RA#configure terminal
RA(config)#router rip
RA(config-router)#network 192.168.1.0
RA(config-router)#network 192.168.10.0
RB#configure terminal
RB(config)# interface FastEthernet 0/0
RB(config-if)#ip address 192.168.1.2 255.255.255.0
RB(config)# interface Loopback 0
RB(config-if)#ip address 192.168.20.1 255.255.255.0
RB#configure terminal
RB(config)# interface FastEthernet 0/1
RB(config-if)#ip address 192.168.2.1 255.255.255.0
RB#configure terminal
```

```
RB(config)#router rip
RB(config-router)#network 192.168.1.0
RB(config-router)#network 192.168.2.0
RB(config-router)#network 192.168.20.0
RC#configure terminal
RC(config)# interface FastEthernet 0/0
RC(config-if)#ip address 192.168.2.2 255.255.255.0
RC(config)# interface Loopback 0
RC(config-if)#ip address 192.168.30.1 255.255.255.0
RC#configure terminal
RC(config)#router rip
RC(config-router)#network 192.168.2.0
RC(config-router)#network 192.168.30.0
```

步骤二：使用 RG-PATS 网络协议分析仪采集 RIPv1 数据包

当拓扑中的所有路由器启动了 RIP 路由进程，这时所有路由器都会以广播的方式通过其接口发送一个请求信息，请求其邻居所有的路由表信息，如下图所示，因为在此拓扑中， 路由器 RA 和路由器 RB 是通过 192.168.1.0 网段相连，路由器 B 与路由器 C 是通过 192.168.2.0 网络相连，所以其向外发送请求时是通过 192.168.1.1、192.168.1.2、192.168.2.1、192.168.2.2 接口发送出去的。

其使用的 UDP 协议的 520 端口与邻居进行交换信息的；在 RIPv1 数据包中其使用的命令为 1，说明其是一个请求报文；版本信息为 1，这说明其运行的 RIPv1；目标地址全为 0，这是路由器请求邻居的所有路由表信息；其它字段全为 0；

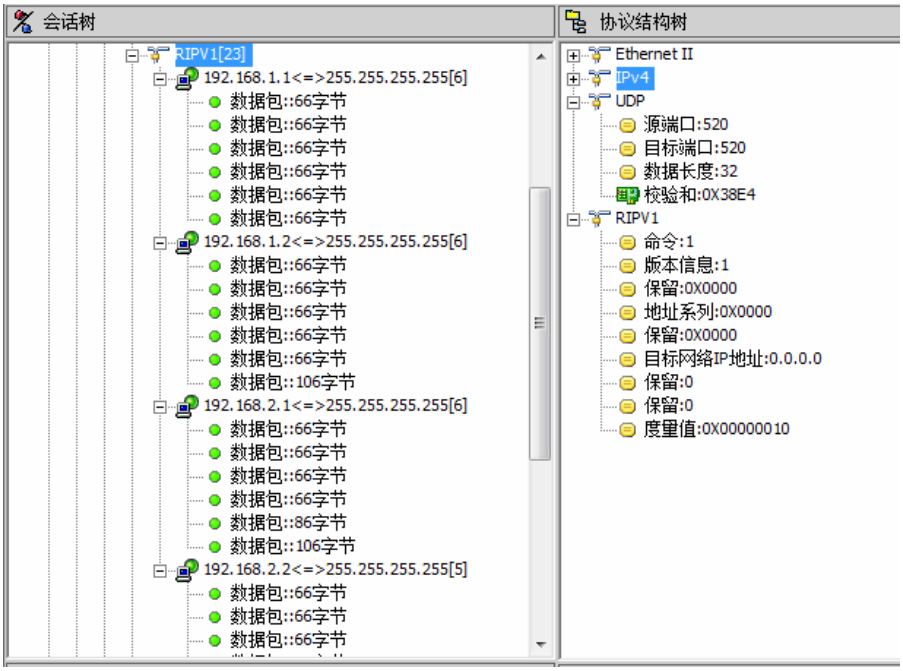


图 6-19 RG-PATS 网络协议分析仪采集 RIPv1 报文

当路由器收到请求信息后，路由器会将其路由表发送给其邻居，如下图所示：

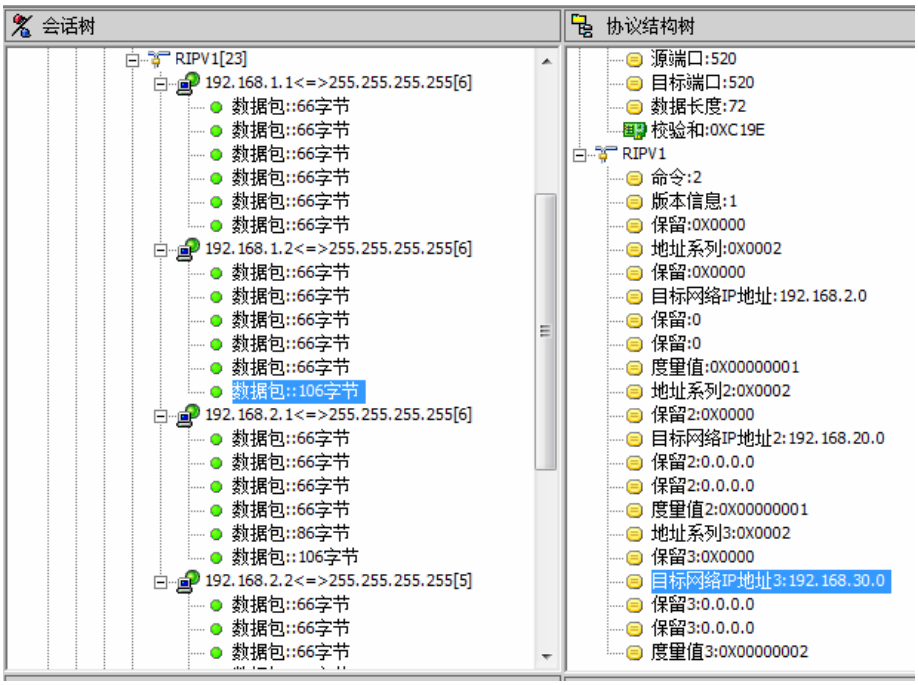


图 6-20 RG-PATS 网络协议分析仪采集 RIPv1 报文

路由器 RB 接收到 RA 的请求报文后，并以响应报文发送给路由器 RA，响应报文中包含了所有的路由表信息，上图中公布了目标网络 192.168.2.0、192.168.30.0、192.168.20.0 信息，并将其度量也公布给邻居路由器 RA；响应报文的命令为 2，则此报文为响应报文；地址系列为 2，由此报文为 IP 报文；目标网络、度量值则为路由表信息；但在此更新报文中没有目标为 192.168.1.0 的路由信息，因为 RIP 路由协议为了防止环路，采用了水平分割的技术。

步骤三：使用 RG-PATS 协议数据发生器发送 RIPv1 数据包

把路由器 RA 关掉，把 RG-PATS 协议仪连接到网络中，使用 RG-PATS 协议仪的协议数据发生器编辑一个数据包，模拟路由器 A 发送路由更新信息。

在 RG-PATS 协议仪上打开数据包发生器，编辑一个 RIPv1 数据包。首先点击菜单栏“添加”，如下图所示：

图 6-21 添加报文

添加一个 RIPv1 协议模板，点击确认添加，如下图所示：

图 6-22 添加 RIPV1 协议模板

修改协议模板的每个值：

Ethernet II 封装：

- 目标物理地址设置为广播地址 FF-FF-FF-FF-FF-FF
- 原物理地址设置为路由器 RA 的 fa0/0 接口 MAC 地址
- 类型：0800

IP 封装：

- 版本信息：4
- IP 头长度：5
- 服务类型：C0
- 总长度：52
- 标识：0
- 标志：2
- 生存时间：64
- 协议类型：17
- 发送 IP 地址：192.168.1.1
- 目标 IP 地址：255.255.255.255

UDP 封装：

- 源端口号：520
- 目标端口号：520
- UDP 长度：32

RIPv1 封装：

- 命令：2
- 版本信息：1
- 地址系列：2
- 目标网络：192.168.10.0
- 度量值：1 编辑完成数据包后，需要点击菜单栏的校验和，进行

数据检验，如下图所示：

图 6-23 校验和计算

下图是编辑完成并经过校验的数据包：

图 6-24 编辑完成的 RIPV1 报文

数据包编辑完成之后，首先在路由器 RB 使用 show ip route 命令查看路由器 RA 没有 关闭前的路由表，如下图所示：

```
Codes:  C - connected, S - static,  R - RIP B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default

Gateway of last resort is no set
C    192.168.1.0/24 is directly connected, FastEthernet 0/0
C    192.168.1.2/32 is local host.
C    192.168.2.0/24 is directly connected, FastEthernet 0/1
C    192.168.2.1/32 is local host.
R    192.168.10.0/24 [120/1] via 192.168.1.1, 00:00:12, FastEthernet 0/0
C    192.168.20.0/24 is directly connected, Loopback 0
C    192.168.20.1/32 is local host.
R    192.168.30.0/24 [120/1] via 192.168.2.2, 00:00:26, FastEthernet 0/1
```

图 6-25 查看路由表

然后关闭路由器 RA，等一会之后，再用 show ip route 命令查看路由器 RB 的路由表，这时去往 192.168.10.0 网络的路由信息不存在了，如下图所示：

```
RB#show ip route

Codes:  C - connected, S - static,  R - RIP B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default

Gateway of last resort is no set
C    192.168.1.0/24 is directly connected, FastEthernet 0/0
C    192.168.1.2/32 is local host.
C    192.168.2.0/24 is directly connected, FastEthernet 0/1
C    192.168.2.1/32 is local host.
C    192.168.20.0/24 is directly connected, Loopback 0
C    192.168.20.1/32 is local host.
R    192.168.30.0/24 [120/1] via 192.168.2.2, 00:00:02, FastEthernet 0/1
```

图 6-26 查看路由表

这时，在路由器 RB 上使用 debug ip rip packet 命令，找开 debug 信息测试，再使用 RG-PATS 协议仪的协议数据发生器发送刚编辑好的数据包，点击协议数据发器的菜单栏的“发送”键，如下图所示：

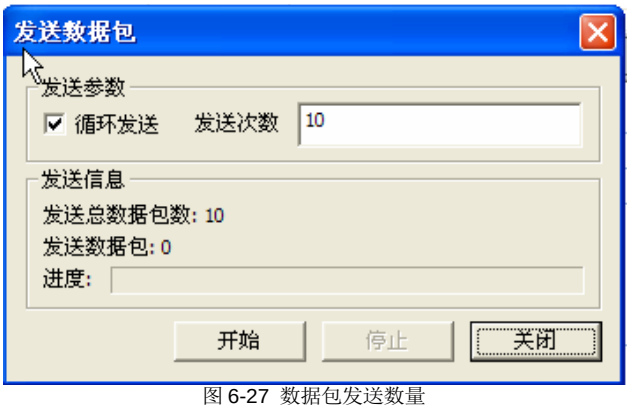


图 6-27 数据包发送数量

选择循环发送，发送次数为 10，点击“开始”按键开始发送。这时路由器 RB 上显示如下信息：

```
RB#
May 13 00:26:39 RB %7: [RIP] RIP recveived packet, sock=2125 src=192.168.1.1 len24
May 13 00:26:39 RB %7: [RIP] Received unknown packet comes from different subnet
May 13 00:26:39 RB %7: [RIP] RIP recveived packet, sock=2125 src=192.168.1.1 len24
May 13 00:26:39 RB %7:         route-entry: family 2 ip 192.168.10.0 metric 1
May 13 00:26:39 RB %7: [RIP] Received version 1 response packet
May 13 00:26:39 RB %7: [RIP] Translate mask to 24
May 13 00:26:39 RB %7: [RIP] Schedule output trigger timer
May 13 00:26:39 RB %7: [RIP] RIP recveived packet, sock=2125 src=192.168.1.1 len24
May 13 00:26:39 RB %7: [RIP] Received unknown packet comes from different subnet
May 13 00:26:39 RB %7: [RIP] RIP recveived packet, sock=2125 src=192.168.1.1 len24
May 13 00:26:39 RB %7:         route-entry: family 2 ip 192.168.10.0 metric 1
May 13 00:26:39 RB %7: [RIP] Received version 1 response packet
May 13 00:26:39 RB %7: [RIP] Translate mask to 24
May 13 00:26:40 RB %7: [RIP] RIP recveived packet, sock=2125 src=192.168.1.1 len24
May 13 00:26:40 RB %7: [RIP] Received unknown packet comes from different subnet
May 13 00:26:40 RB %7: [RIP] RIP recveived packet, sock=2125 src=192.168.1.1 len24
May 13 00:26:40 RB %7:         route-entry: family 2 ip 192.168.10.0 metric 1
May 13 00:26:40 RB %7: [RIP] Received version 1 response packet
May 13 00:26:40 RB %7: [RIP] Translate mask to 24
```

图 6-28 debug 命令测试

在路由器 RB 上使用命令 show ip route 查看是否学习到 192.168.10.0 网络的路由， 如下图所示：

```
RB#show ip route

Codes:  C - connected, S - static,  R - RIP B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default

Gateway of last resort is no set
C    192.168.1.0/24 is directly connected, FastEthernet 0/0
C    192.168.1.2/32 is local host.
C    192.168.2.0/24 is directly connected, FastEthernet 0/1
C    192.168.2.1/32 is local host.
R    192.168.10.0/24 [120/1] via 192.168.1.1, 00:00:10, FastEthernet 0/0
C    192.168.20.0/24 is directly connected, Loopback 0
C    192.168.20.1/32 is local host.
R    192.168.30.0/24 [120/1] via 192.168.2.2, 00:00:00, FastEthernet 0/1
```

图 6-29 查看路由表

通过上图的显示，路由器 RB 学习到了关于 192.168.10.0 网络的路由信息。也可以使用协议数据发生器再编辑一个关于 192.168.50.0 网络的路由信息，开销设置为 3，如下图是经过编辑并校验完成的数据包：

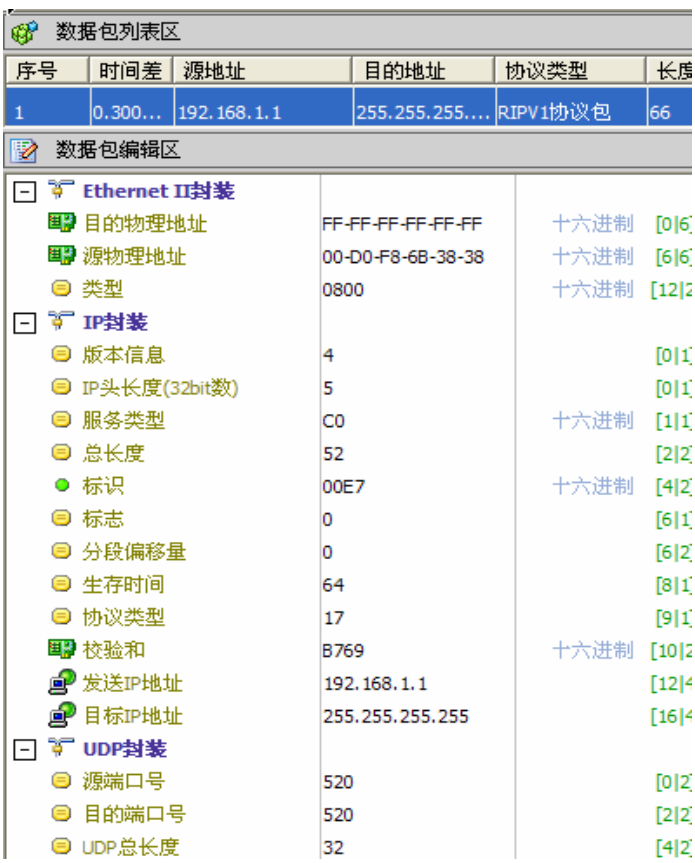


图 6-30 编辑完成的数据包

编辑完成后，点击发送，在路由器 RB 上使用 show ip route 命令查看，学习到关于去往 192.168.50.0 网络的路由信息。如下图所示：

```
RB#show ip route

Codes:  C - connected, S - static,  R - RIP B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default

Gateway of last resort is no set
C    192.168.1.0/24 is directly connected, FastEthernet 0/0
C    192.168.1.2/32 is local host.
C    192.168.2.0/24 is directly connected, FastEthernet 0/1
C    192.168.2.1/32 is local host.
R    192.168.10.0/24 [120/1] via 192.168.1.1, 00:02:19, FastEthernet 0/0
C    192.168.20.0/24 is directly connected, Loopback 0
C    192.168.20.1/32 is local host.
R    192.168.30.0/24 [120/1] via 192.168.2.2, 00:00:04, FastEthernet 0/1
R    192.168.50.0/24 [120/2] via 192.168.1.1, 00:00:10, FastEthernet 0/0
```

图 6-31 查看路由表

步骤四：设定 RIPv2 路由协议实验环境

```
RA#configure terminal
RA(config)# interface FastEthernet 0/0
RA(config-if)#ip address 192.168.1.1 255.255.255.0
RA(config)# interface Loopback 0
RA(config-if)#ip address 192.168.10.1 255.255.255.0
RA#configure terminal
RA(config)#router rip
RA(config-router)#network 192.168.1.0
RA(config-router)#network 192.168.10.0
RA(config-router)#version 2
```

```
RA(config-router)#no  auto-summary

RB#configure  terminal
RB(config)# interface FastEthernet 0/0
RB(config-if)#ip address 192.168.1.2 255.255.255.0
RB(config)# interface Loopback 0
RB(config-if)#ip address 192.168.20.1 255.255.255.0
RB#configure  terminal
RB(config)# interface FastEthernet 0/1
RB(config-if)#ip address 192.168.2.1 255.255.255.0
RB#configure  terminal
RB(config)#router rip
RB(config-router)#network  192.168.1.0
RB(config-router)#network  192.168.2.0
RB(config-router)#network  192.168.20.0
RB(config-router)#version  2
RB(config-router)#no  auto-summary


RC#configure  terminal
RC(config)# interface FastEthernet 0/0
RC(config-if)#ip address 192.168.2.2 255.255.255.0
RC(config)# interface Loopback 0
RC(config-if)#ip address 192.168.30.1 255.255.255.0
RC#configure  terminal
RC(config)#router rip
RC(config-router)#network  192.168.2.0
RC(config-router)#network  192.168.30.0
RC(config-router)#version  2
RC(config-router)#no  auto-summary
```

步骤五、使用 RG-PATS 网络协议分析仪采集 RIPv2 数据包

当拓扑中的所有路由器启动了 RIPv2 路由进程，这时所有路由器都会以组播的方式通过其接口发送路由更新信息，采用的组播地址为 224.0.0.9，其使用的 UDP 协议的 520 端口与邻居进行交换信息的；在 RIPv2 数据包中其使用的命令为 2，说明其是一个响应报文；版本信息为 2，这说明其运行的 RIPv2；报文中还有关于目标网络、子网信息、下一跳、度量值等信息；因为 RIPv2 是无类的路由协议，支持 VLSM，所以在其发送路由信息的时候需求携带子网信息的。如下图所示：

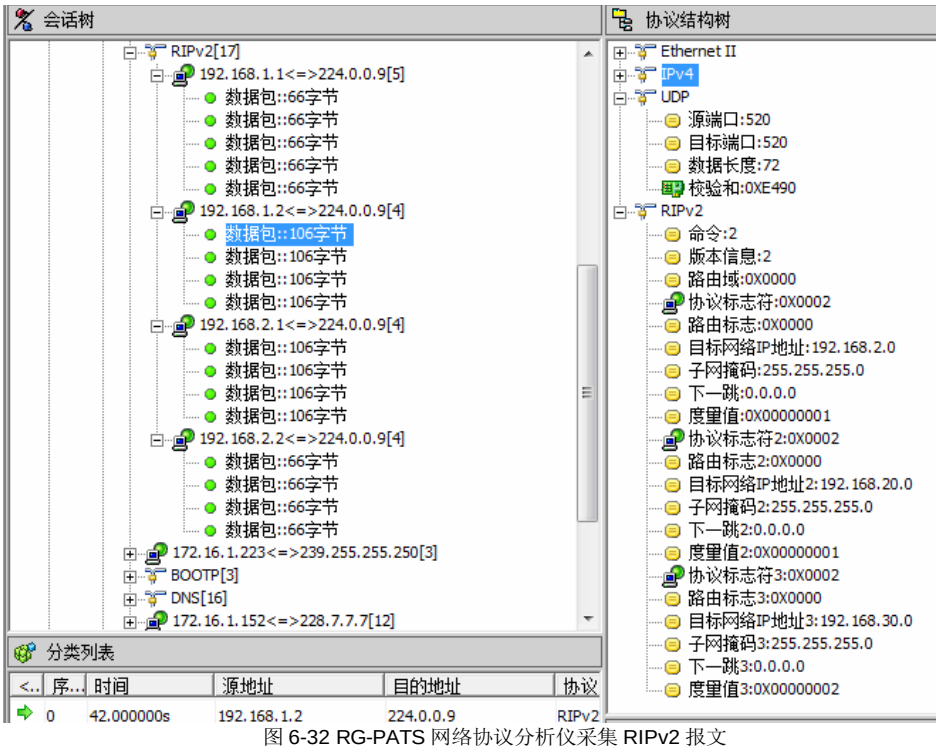


图 6-32 RG-PATS 网络协议分析仪采集 RIPv2 报文

如上图所示，路由器 RB 发送路由信息给路由器 RA，其报文中包含去往目标网络 192.168.2.0、192.168.20.0、192.168.30.0 三个网络的路由信息，并且去往目标度量值分别为 1、1、2 跳。

在路由器 RA 上使用 show ip route 命令查看一下路由表信息，如下所示：

```
RA#sh ip route

Codes:  C - connected, S - static,   R - RIP B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default

Gateway of last resort is no set
C       192.168.1.0/24 is directly connected, FastEthernet 0/0
C       192.168.1.1/32 is local host.
R       192.168.2.0/24 [120/1] via 192.168.1.2, 00:00:24, FastEthernet 0/0
C       192.168.10.0/24 is directly connected, Loopback 0
C       192.168.10.1/32 is local host.
R       192.168.20.0/24 [120/1] via 192.168.1.2, 00:00:24, FastEthernet 0/0
R       192.168.30.0/24 [120/2] via 192.168.1.2, 00:00:24, FastEthernet 0/0
```

图 6-33 show ip route 路由表

步骤六、使用 RG-PATS 协议数据发生器发送 RIPv2 数据包

把路由器 RA 关掉，把 RG-PATS 协议仪连接到网络中，使用 RG-PATS 协议仪的协议数据发生器编辑一个数据包，模拟路由器 A 发送路由更新信息。

在 RG-PATS 协议仪上打开数据包发生器，编辑一个 RIPv2 数据包。首先点击菜单栏“添加”，如下图所示：

图 6-34 添加数据包

添加一个 RIPv1 协议模板，点击确认添加，如下图所示：

图 6-35 添加 RIPV2 协议模板

修改协议模板的每个值：

Ethernet II 封装：

- 目标物理地址设置为 224.0.0.4 组播 MAC 地址 01-00-5E-00-00-09
- 原物理地址设置为路由器 RA 的 fa0/0 接口 MAC 地址
- 类型：0800

IP 封装：

- 版本信息：4
- IP 头长度：5
- 服务类型：C0
- 总长度：52
- 标识：00B2
- 标志：0
- 生存时间：1
- 协议类型：17
- 发送 IP 地址：192.168.1.1
- 目标 IP 地址：224.0.0.9

UDP 封装：

- 源端口号：520
- 目标端口号：520
- UDP 长度：32

RIPv1 封装：

- 命令：2
- 版本信息：2
- 地址系列：2
- 目标网络：192.168.10.0
- 子网掩码：255.255.255.0
- 下一跳：0.0.0.0
- 度量值：1 编辑完成数据包后，需要点击菜单栏的校验和，进行

数据检验，如下图所示：

图 6-36 计算校验和

下图是编辑完成并经过校验的数据包：

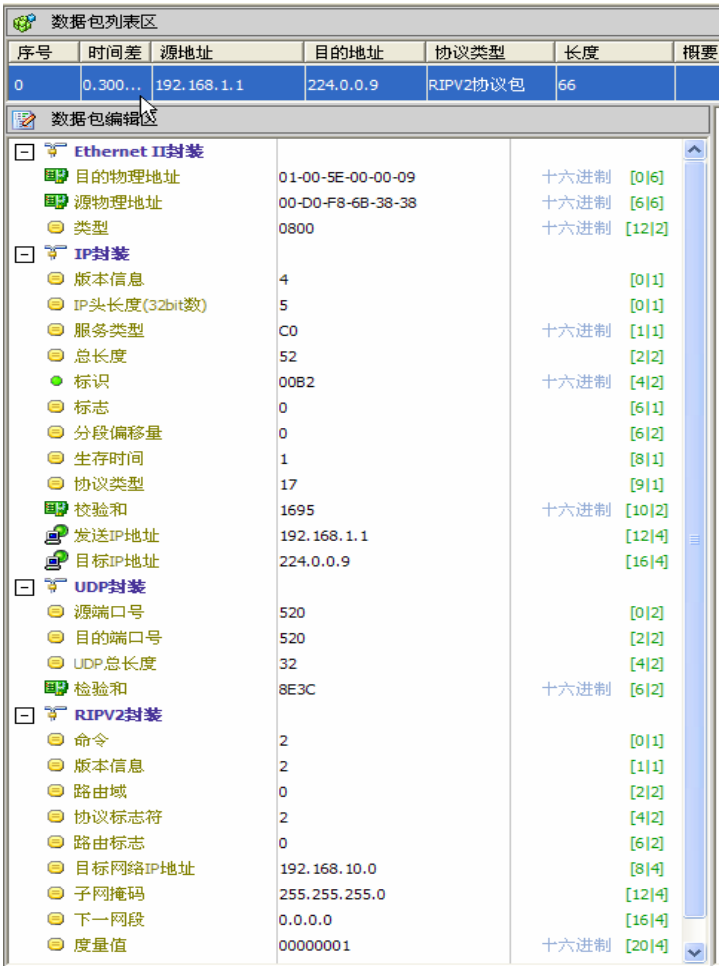


图 6-37 编辑完成的 RIPV2 数据包

数据包编辑完成之后，首先在路由器 RB 使用 show ip route 命令查看路由器 RA 没有 关闭前的路由表，如下图所示：

```
RB#show ip route
Codes:  C - connected, S - static, R - RIP B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default

Gateway of last resort is no set
C       192.168.1.0/24 is directly connected, FastEthernet 0/0
C       192.168.1.2/32 is local host.
C       192.168.2.0/24 is directly connected, FastEthernet 0/1
C       192.168.2.1/32 is local host.
R       192.168.10.0/24 [120/1] via 192.168.1.1, 00:00:45, FastEthernet 0/0
C       192.168.20.0/24 is directly connected, Loopback 0
C       192.168.20.1/32 is local host.
R       192.168.30.0/24 [120/1] via 192.168.2.2, 00:00:11, FastEthernet 0/1
```

图 6-38 show ip route 路由表

然后关闭路由器 RA，等一会之后，再用 show ip route 命令查看路由器 RB 的路由表，这时去住 192.168.10.0 网络的路由信息不存在了，如下图所示：

```
RB#show ip route
Codes:  C - connected, S - static, R - RIP B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default

Gateway of last resort is no set
C       192.168.1.0/24 is directly connected, FastEthernet 0/0
C       192.168.1.2/32 is local host.
C       192.168.2.0/24 is directly connected, FastEthernet 0/1
C       192.168.2.1/32 is local host.
C       192.168.20.0/24 is directly connected, Loopback 0
C       192.168.20.1/32 is local host.
R       192.168.30.0/24 [120/1] via 192.168.2.2, 00:00:09, FastEthernet 0/1
```

图 6-39 show ip route 路由表

这时，在路由器 RB 上使用 debug ip rip packet 命令，找开 debug 信息测试，再使用 RG-PATS 协议仪的协议数据发生器发送刚编辑好的数据包，点击协议数据发器的菜单栏的“发送”键，如下图所示：

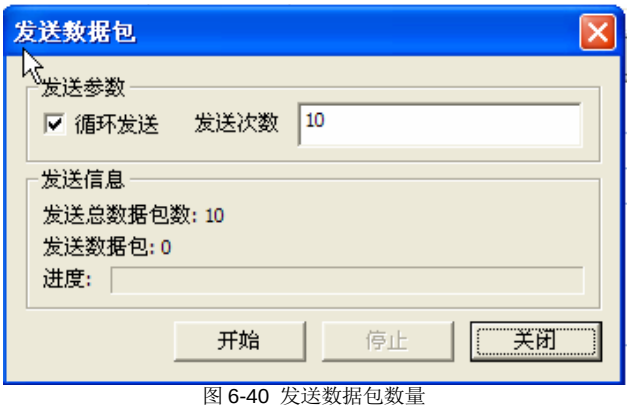


图 6-40 发送数据包数量

选择循环发送，发送次数为 10，点击“开始”按键开始发送。这时路由器 RB 上显示 如下信息：

```
RB#May 12 23:53:46 RB %7: [RIP] RIP recveived packet, sock=2125 src=192.168.1.1 len=24
May 12 23:53:46 RB %7: [RIP] Received unknown packet comes from different subnet
May 12 23:53:46 RB %7: [RIP] RIP recveived packet, sock=2125 src=192.168.1.1 len=24
May 12 23:53:46 RB %7: [RIP] Both do not need auth, Auth ok
May 12 23:53:46 RB %7:          route-entry: family 2 tag 0 ip 192.168.10.0 mask 255.255.255.0 nhop 0.0.0.0 metric 1
May 12 23:53:46 RB %7: [RIP] Received version 2 response packet
May 12 23:53:46 RB %7: [RIP] Schedule output trigger timer
May 12 23:53:47 RB %7: [RIP] RIP recveived packet, sock=2125 src=192.168.1.1 len=24
May 12 23:53:47 RB %7: [RIP] Received unknown packet comes from different subnet
May 12 23:53:47 RB %7: [RIP] RIP recveived packet, sock=2125 src=192.168.1.1 len=24
May 12 23:53:47 RB %7: [RIP] Both do not need auth, Auth ok
May 12 23:53:47 RB %7:          route-entry: family 2 tag 0 ip 192.168.10.0 mask 255.255.255.0 nhop 0.0.0.0 metric 1
May 12 23:53:47 RB %7: [RIP] Received version 2 response packet
May 12 23:53:47 RB %7: [RIP] RIP recveived packet, sock=2125 src=192.168.1.1 len=24
May 12 23:53:47 RB %7: [RIP] Received unknown packet comes from different subnet
May 12 23:53:47 RB %7: [RIP] RIP recveived packet, sock=2125 src=192.168.1.1 len=24
May 12 23:53:47 RB %7: [RIP] Both do not need auth, Auth ok
May 12 23:53:47 RB %7:          route-entry: family 2 tag 0 ip 192.168.10.0 mask 255.255.255.0 nhop 0.0.0.0 metric 1
```

图 6-41 debug 命令测试

在路由器 RB 上使用命令 show ip route 查看是否学习到 192.168.10.0 网络的路由，如 下图所示：

```
RB#show ip route
Codes:  C - connected, S - static, R - RIP B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default

Gateway of last resort is no set
C       192.168.1.0/24 is directly connected, FastEthernet 0/0
C       192.168.1.2/32 is local host.
C       192.168.2.0/24 is directly connected, FastEthernet 0/1
C       192.168.2.1/32 is local host.
R       192.168.10.0/24 [120/1] via 192.168.1.1, 00:00:45, FastEthernet 0/0
C       192.168.20.0/24 is directly connected, Loopback 0
C       192.168.20.1/32 is local host.
R       192.168.30.0/24 [120/1] via 192.168.2.2, 00:00:11, FastEthernet 0/1
```

图 6-42 show ip route 路由表

通过上图的显示，路由器 RB 学习到了关于 192.168.10.0 网络的路由信息。

【思考问题】

1.RIPv1 和 RIPv2 两个版本有什么区别？
2.RIPv2 在 RIPv1 基础上做了那些扩展？
3.试列举 RIP 的缺点及其相应的补救办法？