

第 5 章

IP 路由协议

本章首先介绍 IP 路由的基本原理及路由协议的分类,然后分析三种典型路由协议的基本工作过程,这三种协议是选路信息协议 RIP2、开放最短路径优先协议 OSPF2 以及边界网关协议 BGP4。

5.1 路由协议概述

5.1.1 IP 路由原理及路由表

IP 协议负责为互联网上的任意两台计算机之间的分组传输寻找一条合适的路径。当 IP 协议接收到一个 IP 分组时,首先根据分组中的目的地址查询路由器的转发表(根据路由表生成),获取到达目的主机的下一跳路由器的地址,其次把分组转发给下一跳路由器(如果目的主机连接在路由器所在的网络上,IP 协议就直接把分组转发给目的主机)。最后通过多次转发,分组就可以从源主机传输到目的主机。

IP 协议的工作依赖于路由表中的路由信息。路由表是一种数据结构,为路由器提供了到达不同目的地址的最佳路径。一般情况下,路由表中的每一项路由都包含了目的网络地址、下一跳地址、路由度量值等信息。由于互联网中的计算机数量巨大,因此通常并不是在路由表中存储到达目的主机的路由,而是存储到达主机所在网络的路由(即到达目的网络地址的路由)。路由表也可以存储到达特定 IP 地址的路由。

路由表中的路由信息主要通过以下三种方式获得:

(1) 添加直连路由:直连路由是到达路由器直接连接网络的路由。配置并启用路由器连接网络的接口后,路由器在路由表中添加到达该网络的直连路由。

(2) 添加静态路由:静态路由是网络管理员手动添加的路由,可用于人为指定到达某一网络或某一主机所需经过的路径。

(3) 计算动态路由:动态路由是路由器在路由选择协议控制下,通过与邻居路由器之间交换路由信息而建立的路由。如果网络拓扑发生变化(例如链路或路由器发生故障,增加了新的链路或路由器等),或通信量发生变化,路由器将在路由协议的控制下相互通告这些变化信息,而路由器则根据接收到的路由信息重新运行路由算法,更新各自的路由表,以反映网络的当前状态。

5.1.2 IP 路由协议分类

1. 按自适应性分类

从路由算法能否随网络的通信量或拓扑变化自适应地进行路由调整来划分,路由协

议可分为静态路由协议和动态路由协议。静态路由也叫非自适应路由,其特点是配置简单、开销小,但不能及时适应网络状态的变化,适用于拓扑结构简单且稳定的小规模网络互联。动态路由也叫自适应路由,其特点是能较好地适应网络状态的变化,但实现较为复杂,开销也比较大,适用于规模较大、拓扑结构复杂的网络。动态路由协议的运行会不同程度地消耗网络带宽、路由器 CPU 和内存等资源。

2. 按使用范围分类

互联网规模巨大,如果所有路由器之间都交换路由信息,将会造成很大的通信开销,而且由于路由器数量众多,路由算法也难以收敛。互联网采用了分级的路由策略,即把整个互联网划分为许多较小的自治系统(Autonomous System,AS),在 AS 内部使用内部网关协议(Interior Gateway Protocol,IGP)为 AS 内部网络(及主机)建立路由表,而在 AS 之间使用外部网关协议(External Gateway Protocol,EGP)为不同 AS 的网络(及主机)建立路由表。这种分级方式限制了交换路由信息的路由器数量,降低了动态路由协议运行的开销。自治系统内部的路由选择称为域内路由选择(Intra-Domain Routing),自治系统之间的路由选择称为域间路由选择(Inter-Domain Routing)。

自治系统传统上的定义是指在单一技术管理下的一组路由器,这些路由器使用一种内部网关协议和内部链路代价度量决定在 AS 内部的分组转发路由,使用一种外部网关协议决定如何将分组转发给其他自治系统。随着技术的发展,在一个 AS 内部也可以同时使用多种内部网关协议和多种链路代价度量,而且这个 AS 对外部仍表现出一致的内部路由选择策略,即通过它到达目的网络只有一条统一的路由。

3. 按路由算法工作原理分类

根据路由算法工作原理的不同,路由选择协议大体上可分为距离向量协议、链路状态协议和路径向量协议三种类型。此外,还有具有多种算法特点的混合型路由选择协议。典型的距离向量路由协议有路由信息协议(Routing Information Protocol,RIP)、内部网关路由选择协议(Interior Gateway Routing Protocol,IGRP)等;典型的链路状态路由选择协议有开放最短路径优先(Open Shortest Path First,OSPF)协议、中间系统到中间系统路由选择协议(Intermediate System to Intermediate System Routing Protocol,IS-IS)等;典型的路径向量路由选择协议有边界网关协议(Border Gateway Protocol,BGP)。Cisco 专有的增强型内部网关路由选择协议(Enhanced Interior Gateway Protocol,EIGP)是兼具距离向量和链路状态算法特点的混合型路由协议。在上述协议中,除 BGP 是一种外部网关协议外,其他协议都是内部网关协议。

5.2 RIP 协议分析

选路信息协议(Routing Information Protocol,RIP)是一种广泛使用的内部网关协议。它是一种分布式基于距离向量的路由选择协议,其最大的优点就是简单,适用于小型互联网。最初的 RIP 标准是 RFC 1058,称为 RIP1。RFC 2453 对 RIP1 进行了改进,以支持 CIDR 类型地址,且提供简单的鉴别及组播发送等功能,称为 RIP2。RFC 2080 定义了 RIPng 协议,使得 RIP 协议也能应用到 IPv6 网络中。

5.2.1 RIP 基本工作原理

在 RIP 协议中,每个路由器都维护一张路由表,其中存储了从该路由器到自治系统网络的路由及其距离等。路由用路径上的第一跳路由器的地址表示;距离(Metric)度量了该路径的代价,通常用分组从该路由器到达目的地址要经过的转发次数(跳数)表示。初始时,路由表中只有与路由器直接连接网络的路由项,到直连网络的距离定义为 1。在 RIP 协议中,用距离 16 表示无穷大(Infinity),即网络不可达。因而,RIP 协议只适用于直径不超过 15 的小型互联网。

RIP 协议规定,相邻路由器之间要周期性地交换各自的路由表,这个周期是 30s。通过同一个网络连接的路由器称为相邻路由器。为了避免大量路由器同时发送路由表而造成网络拥塞,这个周期性不是严格的,路由器在每次发送自己的路由表之前会附加一段随机延迟的时间(0~5s)。

接收到邻居发送的路由表后,路由器采用距离向量算法更新自己的路由表(距离向量算法见 5.2.2 节)。在下一个发送周期,路由器将更新后的路由表再发送给自己的邻居路由器。这样,路由信息将在整个自治系统中逐渐扩散开来。在网络拓扑结构不变的情况下,经过有限次的邻居路由器交换路由表后,所有的路由器都将获得了到达自治系统中所有网络的最短路由,此时 RIP 路由协议收敛(Convergence)。

然而,在实际环境中,网络或路由器可能会出现故障。由于 RIP 中邻居路由器间周期性地交换路由表,因此当某个网络或路由器发生故障后,通过该网络连接的邻居路由器或该路由器的邻居将无法接收到这些周期性发送的路由信息。邻居路由器可通过这一现象来发现故障。RIP 协议规定,从上一次接收到邻居发送的路由表起,若经过 180s 后还没有接收到新发送的路由表,就假定连接邻居路由器的网络或邻居路由器发生故障。此时路由器立即更新与故障相关的路由表项,并在随后的发送周期中,将新的路由表发送给其他邻居路由器。最终,经过有限次的邻居路由器交换路由表后,路由协议达到新的收敛状态。

RIP 使用 UDP 协议进行路由信息交换。RIP1 和 RIP2 使用 UDP 的 520 端口发送或接收 RIP 报文。该端口也称为 RIP 端口。

RIP 协议也支持主机路由。

5.2.2 距离向量算法

路由器接收到邻居路由器发送的路由表后,采用距离向量算法(Distance-Vector Algorithm)更新自己的路由表。该算法的基本思想如下:

对接收到的路由表中的每一个路由项(到某个目的网络的路由):

(1) 检查其有效性。基本的检查包括目的 IP 地址是否有效(非保留地址)、距离是否有效(0~16)等。若检测失败,则丢弃该路由项。

(2) 计算从自己出发到达该路由项的目的地址的路由及其距离。在 RIP1 中,路由的第一跳地址(即下一跳地址)就是发送该路由项的邻居路由器的地址,可从携带路由表的 IP 分组的源地址获得;在 RIP2 中,路由项中就可能包含有下一跳地址(该地址也是发送

路由项的路由器和本路由器的一个邻居)。该路由的距离是路由项中携带的距离值(即从发送路由项的邻居或路由项中指定的下一跳地址到目的网络的距离)再加上接收该路由项的网络的代价。若计算所得的距离值超过 16,就记为 16,表示不可达。RIP 协议通常用跳数度量网络的传输代价,即代价为 1。此外,RIP 协议也允许管理员指定网络的代价。

(3) 更新自己的路由表。规则如下:

- 若原来路由表中不存在到达该目的网络的路由项,则添加该路由项。
- 否则,若新路由(第 2 步中计算所得路由)的下一跳地址与路由表中路由项记录的下一跳地址相同,就用新路由替换路由表中的路由项,而不管哪个路由的距离值更小。
- 否则(新路由的下一跳地址与路由表中路由项记录的下一跳地址不同),若新路由的距离小于路由表中路由项的距离,就用新路由替换路由表中的路由项。
- 否则,丢该路由项。

路由器也要检测邻居路由器是否可达。如果从上一次接收到邻居发送的路由表起,180s 后还没有接收到新发送的路由表,就将该邻居路由器标记为不可达,并将路由表中以该邻居路由器为下一跳地址的所有路由表项置为不可达(距离值置为 16)。

5.2.3 RIP 协议的改进

1. 计数到无穷问题

当网络发生故障时,通过邻居路由器之间周期性的路由表交换,RIP 协议最终也能达到收敛状态。然而,这个收敛速度可能很慢,收敛过程可能存在计数到无穷(Counting to Infinity)的问题。这里通过一个例子来说明该问题。

假定有四个路由器 A、B、C 和 D,它们之间的连接关系如图 5.1 所示,其中 C 和 D 之间网络的代价记为 10,其他网络的代价记为 1。为了表述简单,这里只关注每个路由器的路由表中到达目标网络的路由表项,如表 5.1 所示。

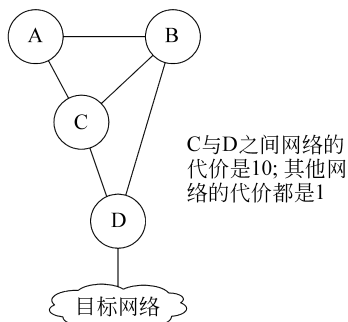


表 5.1 图 5.1 中各路由器到目标网络的路由

路 由 器	(下一跳,距离)
D	(直接连接,1)
B	(D,2)
C	(B,3)
A	(B,3)

图 5.1 RIP 协议的计数到无穷问题

假设某时刻 B 和 D 之间的网络发生了故障,则到达目标网络应通过 C 和 D 之间的网络。相邻路由器之间通过周期性交换路由表能达到这个收敛状态,但收敛过程很慢。每

次交换路由表后的路由器表项变化如表 5.2 所示。

表 5.2 图 5.1 中路由器的路由表项变化

路由器	时 间						
	T0	T1	T2	T3	...	T8	T9
D	(直连,1)	(直连,1)	(直连,1)	(直连,1)	...	(直连,1)	(直连,1)
B	不可达	(C,4)	(C,5)	(C,6)	...	(C,11)	(C,12)
C	(B,3)	(A,4)	(A,5)	(A,6)	...	(A,11)	(D,11)
A	(B,3)	(C,4)	(C,5)	(C,6)	...	(C,11)	(C,12)

在 T0 时刻,路由器 B 通过超时机制发现 B 和 D 之间的网络发生故障,其将自己通过 D 到达目标网络的路由项设置为不可达(Unreachable)。但此时 A 和 C 仍认为可通过 B 到达目标网络。

在 T1 时刻,相邻路由器之间交换路由表,B 接收到 A 和 C 的路由表后,认为可通过 A 或 C 到达目标网络(距离都是 4;实际上不可能,因为通过 A 或 C 到达目标网络又要经过 B,而 B 无法到达目标网络。),表中 B 根据 C 发送的路由项更新了自己到达目标网络的路由项。A 接收到 B 和 C 的路由表后,根据距离向量算法,会选择通过 C 到达目标网络(通过 B 无法到达,通过 C 的距离是 4。)。C 可以接收到 A、B 和 D 发送的路由表,C 会选择通过 A 去往目标网络(通过 B 无法到达目标网络,通过 D 到达目标网络的距离是 11,通过 A 到达目标网络的距离是 4。)。

T2 到 T7 时刻的路由表交换与 T1 时刻类似,在此不再赘述。直到 T8 时刻,路由器 C 才找到正确的去往目标网络的路由(通过 C 和 D 之间的网络)。在下一个交换周期,A 和 B 也找到了正确的路由。

在最坏的情况下,当网络实际不可达时,到达该网络路由的距离要增加到无穷(16),路由才会收敛,此称为计数到无穷问题。因此,RIP 协议中用于表示无穷的距离值不能太大,以便在发生故障情况下路由能尽快收敛。RIP 中采用 16 表示无穷大,这是在网络直径与路由收敛速度之间的一个折中。

RIP 协议采用水平分割技术和触发更新技术来尽量避免此类问题的发生。

2. 水平分割

上述路由收敛慢的原因在于路由器 A 和 C 之间形成了一个循环路由,各自以对方为到达目标网络的下一跳路由器。路由器把从邻居学习到的路由(以邻居路由器为下一跳地址)再发送给邻居就有可能形成循环路由,而且这些路由对邻居的路由发现没有提供任何有意义的信息。简单水平分割(Simple Split Horizon)技术禁止将从邻居学习到的路由再回送给邻居,从而在刚开始形成环路时,双方就不再交换环路路由信息,最终环路路由将在超时机制下被丢弃。这就避免了计数到无穷的问题,加快了路由的收敛。

带毒性逆转的水平分割(Split Horizon with Positioned Reverse)技术允许路由器在发送路由表时包含从邻居学习到的路由,但却将这些路由的距离置为无穷(16)。这样,邻居能立即知道环路路由不可用,而不用等待路由超时后再丢弃。但其缺点是要在路由更

新消息中包含无效的路由项,增加了路由交换开销。

3. 触发更新

循环路由也可能存在于多个路由器之间。例如,路由器 A 认为到达某目标网络可通过路由器 B,B 认为可通过路由器 C,而 C 又认为可通过 A。水平分割技术只能避免在两个邻居路由器之间形成环路,在这种情况下不起作用。此时可采用触发更新(Triggered Updates)技术快速发现在多个路由器之间形成的环路路由,而不必等到环路路由的距离增大到无穷时再发现。

触发更新技术规定,在任何时候,当更新了一条路由的距离时,路由器就立即向其邻居发送路由更新消息,而不必等到下一个发送周期时再发送。邻居路由器更新路由表后,若存在改变距离的路由,也立即向它们的邻居发送路由更新消息,从而引起级联(Cascading)的触发更新,使路由变化尽快在网络中扩散开来,加速路由收敛。

在触发更新扩散的过程中,路由器也会进行正常的周期性路由表交换。如果触发更新尚未扩散到的路由器发送了正常的周期性路由消息,那些已经被触发更新影响的路由器有可能会重新采用旧的路由,从而再次建立一个循环路由。因此,触发更新技术并不能完全避免计数到无穷的问题。当触发更新能在极短时间内完成扩散时,形成环路路由的可能性会很低。

5.2.4 RIP2 报文格式

1. RIP2 报文格式

RIP 协议的报文由固定首部和路由表组成,格式如图 5.2 所示,其中:

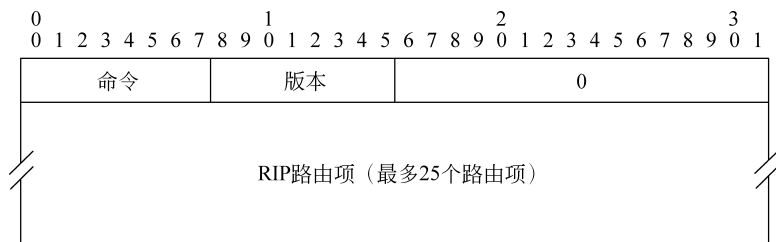


图 5.2 RIP 协议的报文格式

(1) 命令(Command)字段,1 字节,指明了发送该报文的目的。为 1 是请求报文,表明请求报文接收方发送其全部或部分路由表;为 2 是响应报文,表明报文携带有发送方的全部或部分路由表信息。响应报文可以是对请求报文的回应,也可以是发送方周期性的路由表发送(可称为非请求响应)。

(2) 版本(Version)字段,1 字节,RIP 协议版本号,RIP1 设置为 1,RIP2 设置为 2。

(3) 必为 0(Must Be Zero,MBZ)字段,2 字节,必须置为 0。以上 3 个字段组成 RIP 协议的固定首部。

(4) 路由项(RouTe Entry,RTE)字段,20 字节,包含了到达一个目的网络的路由项信息,对应发送方路由表中的一行。每个 RIP 报文中最多可包含 25 个路由项。所有 RIP 协议(RIP1、RIP2 和 RIPng)的固定首部格式都相同,只是路由项格式不同。

RIP2 协议的路由项格式如图 5.3 所示,其中:

(1) 地址族标识符(Address Family Identifier)字段,2 字节,指明解释网络地址时应遵循的协议族。IPv4 协议的地址族标识符定义为 2。

(2) 路由标记(Route Tag)字段,2 字节,是分配给该路由项的一个属性值,主要用于区分内部 RIP 路由(来自自治系统内部)和外部 RIP 路由(来自其他自治系统),例如可用自治系统编号作路由标记。路由器在向邻居通告一个路由时,应当保留该路由的标记不变。

(3) IP 地址(IP Address)字段,4 字节,目的网络的 IPv4 地址。全 0 地址表示默认路由。

(4) 子网掩码(Subnet Mask)字段,4 字节,目的网络的地址掩码。

(5) 下一跳(Next Hop)字段,4 字节,指明报文接收方路由器到达目的网络的下一跳地址。若为 0.0.0.0,表明报文接收方路由器到达目的网络的下一跳的地址就是报文发送方路由器,其地址可从携带 RIP 报文的 IP 分组中获得(源地址)。增加显式的下一跳地址是为了避免额外的分组转发,RFC 2453 的附录(Appendix A)中给出了一个例子。

(6) 距离(Metric)字段,4 字节,指明从报文发送方路由器或下一跳字段地址到达目的网络的路由的距离。

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1																
地址族标识符																路由标记																															
IPv4地址																																															
子网掩码																																															
下一跳																																															
距离																																															

图 5.3 RIP2 协议的路由项格式

2. RIP 请求报文

RIP 路由器除了周期性地向邻居路由器发送自己的路由表外,还可以向邻居路由器显式地请求其全部或部分路由表,这通过向邻居路由器发送 RIP 请求报文(命令字段置为 1)来实现。当一个 RIP 路由器启动时,它可以向其邻居路由器发送 RIP 请求报文,请求邻居把整个路由表发送给自己,以便快速建立起自己的路由表。部分路由表请求主要用于路由监测,此时请求方可以是一台能够发送、接收及处理 RIP 报文的主机(但它不参与 RIP 路由交换)。

在 RIP 请求报文中,若只有一个路由项,且地址族标识符是 0、距离是无穷(16),则表明请求的是整个路由表。报文接收路由器构造一个 RIP 响应报文,在其中逐项填入自己路由表中的有效路由,发送给请求方。若路由数量超过一个 RIP 报文能携带的路由项数,就再构造新的 RIP 响应报文并发送。

在部分路由表请求报文中,路由项列出了所请求的路由。报文接收方在自己的路由表中逐项查找相应路由项,若存在,就填入其距离字段,否则,在距离字段填入 16。最后

把报文命令字段置为 2(生成响应报文),并发送给请求方。

请求报文的接收方路由器对全部路由表请求和部分路由表请求的处理也不同。全部路由请求主要用于快速建立请求方路由器的路由表,必须应用水平分割技术;而部分路由表请求主要用于路由诊断,此时需要获得路由项的确切信息,不能改变或隐藏路由项信息,因而不能应用水平分割技术。

发送部分路由表请求报文时,请求方可不使用 RIP 端口,将请求报文直接发送给特定路由器的 RIP 端口。请求报文接收路由器则相应地将生成的响应报文直接发送给请求方的非 RIP 端口。

3. 鉴别报文

RIP2 中路由器可以对每个接收的 RIP 报文进行鉴别(Authentication)。鉴别信息占用第一个路由项的 20 字节(这意味着若携带鉴别信息,一个 RIP2 报文最多能携带 24 个路由项)。采用鉴别机制时,将第一个路由项的地址族标识符字段设置为 0xFFFF,路由标记字段则被重新命名为鉴别类型(Authentication Type),用于区分鉴别机制的类型。RFC 2453 只定义了一种简单的密码鉴别,其鉴别类型是 2。路由项中剩余的 16 字节包含了鉴别用的明文密码(若密码不足 16 字节,则靠左对齐并补 0)。

4. 报文组播发送

RIP1 中路由器用广播(Broadcast)方式向邻居路由器发送 RIP 报文。为了减少对不参与 RIP 协议主机的影响,RIP2 协议支持路由器以组播(Multicast)方式向邻居路由器发送 RIP 报文,使用的组播地址为 224.0.0.9。需要注意的是,由于 RIP 协议只在相邻路由器之间交换报文,因而这里的组播不需要组播管理协议(IGMP)的支持。RIP2 中是否采用组播是可配置的。

5.2.5 RIP2 协议分析

1. 相关命令

(1) 启用 RIP

```
Router(config)#router rip
```

执行上述命令将进入 RIP 协议配置模式,可配置 RIP 协议的参数。要停止 RIP 路由协议并清除所有 RIP 配置,可在全局配置模式下使用“no router rip”命令。

(2) 指定 RIP 协议版本

```
Router (config-router)#version [1|2]
```

在 RIP 协议配置模式下执行上述命令,指定 RIP 协议的版本。在默认情况下,Cisco 路由器可以接收 RIPv1 和 RIPv2 的路由信息,但只发送 RIPv1 的路由信息。

(3) 指定直连网络

```
Router (config-router)#network address
```

在 RIP 协议配置模式执行上述命令,向 RIP 协议添加路由器的直连网络信息,参数 address 是本路由器直连网络的网络地址。在路由交换过程中,路由器会向其邻居通告配

置的直连网络。执行该命令后,路由器将在指定网络的接口上启用 RIP 路由协议,相关接口随即开始发送和接收路由更新报文。

(4) 指定被动接口

```
Router (config-router)#passive-interface interface
```

如果路由器某个接口所连接的网络上没有其他运行 RIP 协议的路由器,路由器就没有必要从这个接口发送 RIP 路由信息。在 RIP 协议配置模式下执行上述命令可禁止路由器从指定接口发送路由信息,参数 interface 是要禁止发送路由信息的接口。注意,虽然路由器不再从该接口发送路由信息,但该接口所连接的网络仍会被路由器通知给相邻的路由器。我们将这类接口称为被动接口。

2. 网络拓扑及配置

在 GNS3 中搭建如图 5.4 所示的网络,并按图 5.4 中所示关系连接路由器和主机接口。新建一个 GNS3 工程 rip2,并保存该网络拓扑。

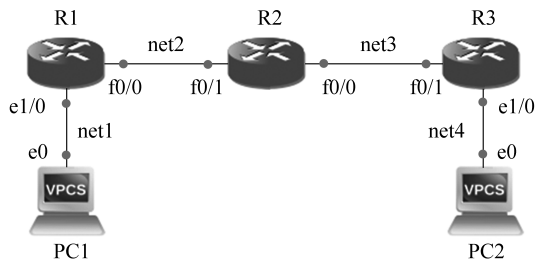


图 5.4 RIP 协议分析的网络拓扑

右击路由器 R1,选择控制台(Console)命令,打开 R1 的控制台窗口,执行下列命令,配置路由器的接口地址及路由协议并保存:

```
1: R1#config t
2: R1(config)#interface e1/0
3: R1(config-if)#ip address 192.168.1.1 255.255.255.0
4: R1(config-if)#no shutdown
5: R1(config-if)#exit
6: R1(config)#interface f0/0
7: R1(config-if)#ip address 192.168.2.1 255.255.255.0
8: R1(config-if)#no shutdown
9: R1(config-if)#exit
10: R1(config)#router rip
11: R1(config-router)#version 2
12: R1(config-router)#network 192.168.1.0
13: R1(config-router)#network 192.168.2.0
14: R1(config-router)#passive-interface e1/0
15: R1(config-router)#end
16: R1#write
```

参照上述过程,配置路由器 R2 和 R3 的接口地址及路由协议,参数见表 5.3。注意设置 R1 的 e1/0 接口和 R3 的 e1/0 接口为被动接口。

打开 PC1 控制台窗口,执行下列命令,配置其接口地址、默认网关并保存:

```
1: PC1> ip 192.168.1.100/24 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.100 255.255.255.0 gateway 192.168.1.1
2: PC1> save
```

在 PC2 的控制台窗口中,执行类似命令配置接口地址和默认网关,参数如表 5.3 所示。

表 5.3 RIP 协议分析的网络配置参数

设 备	接 口	IP 地 址	地 址 掩 码	默 认 网 关
R1	f0/0	192.168.2.1	255.255.255.0	—
	e1/0	192.168.1.1	255.255.255.0	—
R2	f0/0	192.168.3.1	255.255.255.0	—
	f0/1	192.168.2.2	255.255.255.0	—
R3	f0/1	192.168.3.2	255.255.255.0	—
	e1/0	192.168.4.1	255.255.255.0	—
PC1	e0	192.168.1.100	255.255.255.0	192.168.1.1
PC2	e0	192.168.4.100	255.255.255.0	192.168.4.1

3. RIP2 协议分析

在实验中,我们在 R1 和 R2 之间的网络上捕获 RIP2 分组,分析 RIP2 协议的工作过程。在 R1 和 R2 之间的链路上单击右键,选择开始捕获(Start capture)命令,指定在 R1 的 f0/0 接口或 R2 的 f0/1 接口进行分组捕获。

打开捕获的分组文件,输入显示过滤器“rip.version==2”,Wireshark 分组列表窗口显示如图 5.5 所示。

No.	Time	Source	Destination	Protocol	Length	Info
7	24.326304000	192.168.2.1	224.0.0.9	RIPv2	66	Response
8	25.526193000	192.168.2.2	224.0.0.9	RIPv2	86	Response
14	51.801968000	192.168.2.1	224.0.0.9	RIPv2	66	Response
16	53.741223000	192.168.2.2	224.0.0.9	RIPv2	86	Response
23	79.638964000	192.168.2.1	224.0.0.9	RIPv2	66	Response
25	80.501627000	192.168.2.2	224.0.0.9	RIPv2	86	Response

图 5.5 RIP2 分组的周期性交换

观察分组列表窗口中分组的捕获(发送)时间,可以发现 R2(192.168.2.2)和 R1(192.168.2.1)以约 30s 的间隔向组播地址 224.0.0.9 发送 RIPv2 报文。选择一个 R2 发送的分组,在分组首部详细信息窗口查看其分组首部字段值。可看到 RIP 分组封装在