

RIP 协议分析及其实验的设计与实现

刘向东^a, 寇清华^b, 张晓蕊^a, 王德高^a

(大连民族学院 a. 非线性信息技术研究所; b. 图书馆 辽宁 大连 116600)



摘要: 介绍了 RIP 协议的原理以及工作过程,通过设计具体的实验方案,结合协议分析软件捕获 RIP 报文,具体地验证了 RIP 协议的工作原理与工作过程,展示了 RIP 的慢收敛问题,并通过配置水平分割或毒化路由等特性,演示了其对 RIP 慢收敛起到的关键作用,以加深学生对 RIP 协议与路由技术的理解。

关键词: RIP 协议; 协议分析; 水平分割; 慢收敛

中图分类号: TP 393.08

文献标志码: A

文章编号: 1006-7167(2015)01-0122-04

Design and Operation of RIP Protocol Analysis Experiment

LIU Xiang-dong^a, KOU Qing-hua^b, ZHANG Xiao-rui^a, WANG De-gao^a

(a. The Institute of Nonlinear Information Technology; b. Library,

Dalian Nationalities University, Dalian 116600, China)

Abstract: This paper introduces the background, principles and implementation of Routing Information Protocol (RIP), shows the routing process of RIP by specific experiments with the aid of protocol analysis method. The experiment demonstrates slow convergence phenomenon, and the key effect of split horizon technology. The experiment enhances the self-study abilities of students.

Key words: RIP; protocol analysis; split horizon; slow convergence

0 引言

路由技术是因特网体系结构的基础,而动态路由协议又是网络互联的一项重要关键技术。动态路由协议在实际组网中应用十分广泛。也正因为如此,使得路由协议成为网络工程专业学生必需深入理解并掌握的一个重要内容。

在众多的路由协议当中,路由信息协议(Routing Information Protocol, RIP)是一种简单的、采用距离-矢量(Distance-Vector, DV)算法的域内动态路由协议^[1-3],非常适合作为实验内容,以加深学生对路由协议的理解。RIP 协议是 XEROX 的 Palo Alto 研究中心(PARC)在 XEROX 的早期 PDU 和 XNC 路由选择协议

的基础上开发的,但 RIP 协议的广泛应用却主要得益于加利福尼亚大学伯克利分校的 routed 程序实现,并将其和 4BSD UNIX 系统一起分发^[2]。RIP 主要应用于使用同种技术的中小型网络。对于更复杂的网络环境, RIP 受到无限计算问题的困扰,往往收敛得很慢,一般使用不多。

在计算机网络原理课程中,关于动态路由协议的内容普遍不多^[4-7],很多技术细节都鲜有介绍。在组网技术、网络管理等课程中有关 RIP 的实验主要是配置 RIP^[8-11],对加深学生理解 RIP 与路由协议工作原理的作用不大。本文设计的 RIP 原理实验基于协议分析的方法,通过观察 RIP 报文的传递与 V-D 报文的具体内容,直观展现 RIP 的工作原理与工作过程,使学生可以深入理解 RIP 与路由协议的工作原理,更好地体会其存在的无穷计算问题,领悟水平分割与毒化路由的设计想法,并通过实验提高其分析问题和解决问题的能力。

收稿日期: 2014-05-29

基金项目: 中央高校基本科研专项基金(DC12010106); 大连民族学院教育教学改革项目

作者简介: 刘向东(1967-),男,山东莱州人,博士,教授,研究方向: 计算机网络及信息安全。E-mail: liuxd@dlnu.edu.cn

1 RIP 协议原理

1.1 矢量-距离算法

RIP 基于 D-V 基本思想是: 路由器刚启动时仅知道自己直连的网段。每个路由器周期性地向外广播自己的 V-D 报文, 主要内容是由若干 (V, D) 序偶组成的序偶表; 序偶中的“向量”V 标识路由器可到达的信宿, “距离”D 指出该路由器去往信宿 V 的距离, 按需转发的路由器的个数计。其他路由器收到某路由器的 (V, D) 报文后, 据此按照最短路径原则对各自的路由表进行刷新。

路由表更新的原则如下:

(1) 如果 (V, D) 报文通告的是一个新的信宿, 即原来自己的路由表中没有到信宿 V 的路由, 路由器须增加相应新的到信宿 V 的表目到自己的路由表, 其“距离”为 $D + 1$, 下一跳为发送该 (V, D) 报文的路由器;

(2) 如果 (V, D) 报文通告的不是一个新的信宿, 但其去往该信宿的距离较自己现在的好, 即比自己去往该信宿的距离减 1 还小, 路由器须更新该信宿表目, 其“距离”为 $D + 1$, 下一跳为发送该 (V, D) 报文的路由器;

(3) 如果 (V, D) 报文通告的既不是一个新的信宿, 其去往该信宿的距离也不比自己现在的好, 但却是自己原来对应表项中的下一跳路由器, 即自己去往该信宿的路由是从该路由器学习来的, 路由器也须更新该信宿表目, 其“距离”为 $D + 1$, 下一跳仍为发送该 (V, D) 报文的路由器;

(4) 其他情形不进行路由表更新。

1.2 RIP 报文的格式

RIP 报文封装在 UDP 报文中, 使用 UDP 的 520 号周知端口^[12]。受 UDP 报文的长度的限制, RIP 报文不能超过 512B。RIP 有 2 个版本, RIP v1 和 RIP v2 的报文格式稍有不同。不包含认证项的 RIP v2 报文格式如图 1 所示^[13-14]。而 RIP v1 的报文格式与 RIP v2 很类似, 只是图中黄色字段必须为全 0。

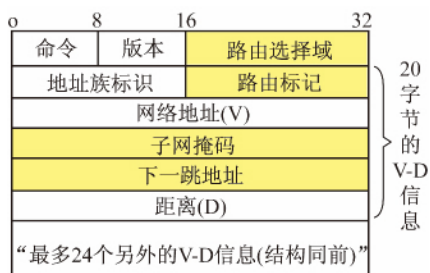


图1 RIP v2 报文格式

在 RIP 报文中, 命令字段的正式值有 1 和 2, 分别标识一个请求报文和一个响应报文。版本字段的值的

范围是从 1 到 2, 分别标识 RIP v1 和 RIP v2。路由选择域指明与该报文相关的路由选择守护进程的标识符。在 UNIX 系统中, 该字段是一个进程的标识符。一台机器通过使用路由选择域, 可以同时运行多个 RIP。但现在的标准建议不用, 所以总是为全 0。后面是 1 ~ 25 个可变数目的 20B 的 V-D 信息。每个 V-D 信息包含:

地址族标识字段, 对于 IP 地址, 该字段的值为 2。

路由标记 (Routing tag) 为外部路由标记, 是为了支持外部网关协议而设计的。它携带着一个自治系统号, 是表示路由是保留还是重播的属性。它提供一种从外部路由中分离内部路由的方法, 用于传播从外部路由器协议获得的路由信息。

网络地址和子网掩码字段, 标识目的网络的 IP 地址与掩码。

下一跳地址, 如果该字段为 0, 则表明分组应当发送到正在发送该 RIP 报文的路由器, 否则, 该字段包含一个 IP 地址, 指明应将分组发往何处。

距离字段, 标识到达目的网络的跳数。

从报文中我们可以看出, RIP v1 是有类路由协议, 不支持无类域间路由 CIDR 和变长子网掩码 VLSM, 因为它的 V-D 信息没有包含所必须的子网信息 - 子网掩码。RIP v2 是无类路由协议, 支持无类域间路由和变长子网掩码, 这也是 RIP v2 对 RIP v1 有意义的改进。

1.3 RIP 协议存在的问题和解决的方法

RIP 使用 D-V 算法。D-V 算法的优点是简单、易于实现, 但是存在一个问题: 当网络出现故障时, 要经过比较长的时间才能将此信息传送到所有的路由器^[13,14]。因为某路由器的路径变化像波动一样从相邻路由器传播出去, 其过程非常缓慢。且 D-V 算法路径刷新过程中, 可能出现路径不一致和寻径回路等问题, 即所谓的“慢收敛” (Slow convergence) 与“计数到无穷” (Count to infinity) 问题。所以, RIP 不适应路径剧烈变化的或大型的网间网环境。

为防止寻径回路的长期存在, RIP 规定, 长度为 16 的路径为无限长路径, 即不存在路径。同时, 引入水平分割 (Split horizon)、毒性逆转 (Poison Reverse) 和触发更新 (Triggered update) 等技术减少出现寻径回路的可能性。水平分割的原理是: 当路由器从某个接口发送 RIP 报文时, 其中不能包含从该接口获得的路径信息, 这样就能消除相邻路由器间的环路。毒性逆转法是水平分割的加强版, 它在路由器从某个接口发送 RIP 报文时, 将从该接口获得的路径信息的距离置为 16, 即不可达。为了加强水平分割与毒性逆转的效果, 可以同时使用触发更新技术: 一旦检测到路径崩溃, 立即广播 RIP 路径刷新报文, 而不必等待下一个广播周期, 以

使新的路由信息尽快传送到所有路由器上。

2 实验

2.1 实验名称

RIP 协议分析。

2.2 实验目的

在路由器上配置启用 RIP 协议,并利用协议分析软件捕获 RIP 报文,了解 RIP 的工作过程。同时,改变网络的连接状态,观察理解 RIP 的慢收敛现象,体会水平分割与触发更新新技术的作用。

2.3 实验设备

实验采用华为 AR2200 系列路由器 4 台,在 2 号槽位配 1 块 8FE1GE 接口卡。实验另需 Hub 5 台 4 台主机,均安装开源协议分析软件 WireShark。

2.4 实验拓扑

实验网络拓扑如图 2 所示。各路由器接口间连接

与 IP 地址的分配如图中标注。

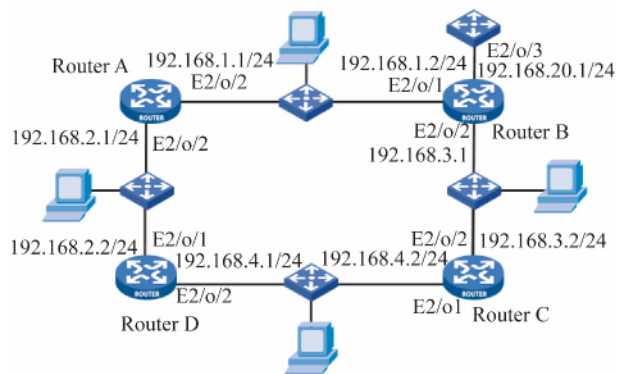


图 2 实验网络拓扑图

2.5 实验过程与参考配置

(1) 不启动路由协议时网络的连通状况。连接好相应设备后,我们首先在路由器上配置各接口 IP 地址。以 Router A 为例,在其上配置:

```
< Huawei > system-view
[ Huawei ] interface Ethernet2/0/1
[ Huawei-Ethernet2/0/1 ] ip address 192.168.1.1 24
[ Huawei-Ethernet2/0/1 ] quit
[ Huawei ] interface Ethernet2/0/2
[ Huawei-Ethernet2/0/2 ] ip address 192.168.2.1 24
[ Huawei-Ethernet2/0/2 ] quit
```

在路由器 B、C 和 D 上也进行类似配置。配置完成后,在各个路由器上,通过 display ip routing-table 命令观察各个路由器的路由表。由于还没有运行路由协议,每个路由器路由表中只有直连的路由表项,所以这 4 个路由器间还不会完全联通。可以通过 ping 命令测试路由器间的联通性验证这一结果。

(2) 启动 RIP 后网络的连通状况。接下来我们分别在 4 个路由器上启动 RIP 协议,其中 Router A 的配置命令为:

```
[ Huawei ] rip #在系统视图下配置,设置 RIP 协议
[ Huawei-rip-1 ] network 192.168.1.0 #设置启用 RIP 协议的网络
[ Huawei-rip-1 ] network 192.168.2.0
[ Huawei-rip-1 ] rip version 2 #设置使用 RIP v2
```

再观察各个路由器的路由表,并测试路由器间的联通性。此时,每个路由器的路由表中不仅直连的路由表项,还有通过 RIP 学到的路由,并且具有到达图中每个网络地址的路由,整个网络是连通的。

在每个主机上开始抓包,并进行协议分析。可以观察到路由器间周期性组播的 RIP v2 报文,检查 RIP 报文,对比各路由器的路由表,可以验证 RIP 报文中传

#切换到系统视图

#进入以太网 Ethernet2/0/1 接口视图

#设置以太网 Ethernet2/0/1 的 IP 地址

#退出接口模式

#进入以太网 Ethernet2/0/2 接口视图

#设置以太网 Ethernet2/0/2 的 IP 地址

#退出接口模式

递的 V-D 信息。

(3) 理解水平分割与触发更新的工作方式。华为路由器 RIP 启动后默认就启用水平分割与触发更新。可以在接口状态通过命令 undo rip split-horizon 禁用该接口启动水平分割功能。在路由器各接口禁用水平分割后,再次观察 RIP 报文中的 V-D 信息。与没禁用水平分割时的 V-D 信息对比,可以看到禁用水平分割后,V-D 信息包含全部路由表项,而启用水平分割功能后,V-D 信息包含的只是不是从该接口学下的那部分路由表项。

然后,通过改变网络连接状况,比如,down 掉 Router B 的 Ethernet2/0/2 接口,通过分析捕获的 RIP 报文观察触发更新的工作方式。触发更新发出的 RIP 报文只含引发触发的路由变化的 V-D 信息,在我们的例子中就是只含一条关于 192.168.20.0/24 的路由信息,跳数为 16。而周期性的路由更新报文包含整个路由表,或经水平分割过滤过的整个路由表。

(4) 观察、理解收敛到无穷现象。保存 4 个路由器的配置,并在主机上启动协议分析软件进行捕包。然后重新启动各个路由器,让它们重新交换路由信息。这样,就可以捕获路由器进行路由信息交换的所有 RIP 报文。通过对 RIP 报文的分析,对照各个路由器的路由表,就可以了解 RIP 协议工作的全过程。

继续禁用路由器的水平分割功能,并 down 掉 Router B 的 Ethernet2/0/2 接口。在各个主机上经过一段时间的捕获 RIP 报文,然后终止。这些 RIP 报文就可以反映 RIP 的工作过程,以及收敛到无穷的过程与现象。为便于协议分析,首先利用 WireShark 的数据合并功能,将 4 个主机上抓取的报文按时间合并到一个 cap 文件中^[15]。下面是我们分析该文件关于 192.168.20.0/24 的 V-D 信息的部分结果。见表 1。我们只列出了前面的一部分,可以请学生根据抓包文件补全该表,并运用协议运行原理,分析理解表中各项间的关系与合理性。

表 1 4 个路由器间关于 192.168.20.0/24 的交互的 V-D 信息(黄色条目为触发更新)

发送路由器	距离	接收路由器	距离变化[习得该路由的路由器]
Router B	16	Router C	2->16
Router B	16	Router A	2->16
Router A	16	Router B	16
Router A	16	Router D	3[Router A, Router C]->3[Router C]
Router D	3	Router C	16->4[Router D]
Router C	4	Router B	16->5[Router C]
Router C	4	Router D	3->5[Router C]
Router A	16	Router B	5[Router C]
Router A	16	Router D	5[Router C]
Router D	5	Router A	16->6[Router C]
Router B	5	Router A	6[Router D]->6[Router B, Router D]
Router B	5	Router C	4[Router D]
Router D	5	Router A	6[Router B, Router D]
Router D	5	Router C	4->6[Router D]
Router A	6	Router D	6[Router C]
Router A	6	Router B	5[Router C]
Router B	5	Router A	6[Router B, Router D]
Router C	6	Router D	5->7[Router C]

3 结 语

路由协议是计算机网络、组网技术、网络管理等网

络工程专业系列课程的教学重点内容,也是学生难以深入理解的知识点之一。利用协议分析的方法,通过跟踪路由器间路由信息的交互、分析传递的 V-D 报文的具体内容,对比路由表的变化,明了、直观地展现了 RIP 工作原理和工作工程,既加深了学生对 RIP 及其存在的无穷计算问题与水平分割、毒化路由技术的理解,又很好地培养了学生分析问题、解决问题、以及综合应用知识的能力,教学效果良好。

参考文献(References):

- [1] Douglas E Comer. 用 TCP/IP 进行网际互联第一卷:原理、协议与结构[M]. 林瑶译,谢希仁校. 4 版. 北京:电子工业出版社, 2006.
- [2] Jeff Doyle, Jennifer Carroll. TCP/IP 路由技术(第一卷)[M]. 2 版. 葛建立译. 北京:人民邮电工业出版社, 2011.
- [3] Jeff Doyle, Jennifer Carroll. TCP/IP 路由技术(第二卷)[M]. 夏俊杰译. 北京:人民邮电工业出版社, 2011.
- [4] 吴功宜,吴英. 计算机网络[M]. 北京:清华大学出版社, 2004.
- [5] 谢希仁. 计算机网络[M]. 5 版. 北京:电子工业出版社, 2007.
- [6] Andrew S Tanenbaum. 计算机网络[M]. 5 版. 严伟译. 北京:清华大学出版社, 2012.
- [7] Forouzan B A. TCP/IP 协议族[M]. 4 版. 王海译,谢希仁校. 北京:清华大学出版社, 2011.
- [8] 田增国,刘晶晶,张召贤. 组网技术与网络管理[M]. 2 版. 北京:清华大学出版社, 2009.
- [9] 黄中砥,张召贤,周飞菲. 组网技术与网络管理[M]. 北京:清华大学出版社, 2006.
- [10] 惠玥,张媛,唐海. IP 静态路由实验的研究[J]. 实验室研究与探索, 2010, 29(11): 61-64.
- [11] 傅伟,高海侠,熊平. RIP 路由协议实验的设计与实现[J]. 实验技术与管理, 2012, 29(5): 127-129.
- [12] Hedrick C. Routing Information Protocol[EB/OL]. IETF RFC1058 (1988), <http://www.rfceditor.org>.
- [13] Malkin G. RIP Version 2 Protocol Analysis[EB/OL]. IETF RFC1721(1994), <http://www.rfceditor.org>.
- [14] Malkin G. RIP Version 2[EB/OL]. IETF RFC2453(1998), <http://www.rfceditor.org>.
- [15] Angela Orebaugh, Gilbert Ramirez, Jay Beale. Wireshark & Ethereal Network Protocol Analyzer Toolkit[M]. Burlington: Syngress Press, 2006: 87-89.

• 名人名言 •

伟大的科学家在实验室里的生活,是对物体和对周围一切的执着地斗争。

——居里夫人