基于域内路由协议 RIP 的防环机制仿真实验

孙光懿[1],姚洪祥[2]
(1. 天津音乐学院 网络安全和信息化办公室,天津 300171; 2. 国网电商科技有限公司,天津 300022)

摘 要: RIP 协议属于内部网关路由协议,有 RIPv1、RIPv2 两个版本,通常用于小型自治系统内交换路由信息。本文在对 RIP 报文格式、产生路由环路的原因以及防环机制进行深入研究的基础上,利用 EVE-NG 网络模拟器设计了计数无穷大、水平分割、毒性逆转等防环机制仿真实验。通过分析 debug ip rip 命令输出的路由更新信息并对照路由表的变化,直观地展现了上述防环机制的工作过程,同时验证了其有效性。本文研究结果可为读者在实际网络中部署 RIP 协议提供重要参考。

关键词: RIP; 计数无穷大; 水平分割; 毒性逆转
中图分类号: TP393.18 **文献标识码:** A **文章编号:** 1005-8036(2020) 04-0053-07

域内路由协议 RIP(Routing Information Protocol) 起源于上世纪 80 年代,由美国加州大学伯克利分校开发,主要用于在小型自治系统内交换路由信息。其早期版本 RIPv1[1-2] 为有类路由协议,它具有使用广播地址 255.255.255.255 发送路由更新(不携带子网掩码信息) 、不支持 VLSM(Variable Length Subnetwark Masr) 和 CIDR (Classless Inter-Domain Routing) ,可在主类边界路由器中自动执行路由汇总且无法人工关闭等特点。随着互联网技术的不断发展,RIPv1 已被其后续版本 RIPv2 所替代。RIPv2 为无类路由协议,相比 RIPv1 来说功能有了大幅扩展: 其一,它使用组播地址 224.0.0.9 发送路由更新(该路由更新允许携带子网掩码信息,并且只发送给网络中使用该路由协议的路由器) ,这样以来不仅有效节省了网络带宽,还提高了路由更新的效率; 其二,支持 VLSM 和 CIDR,即使出现同一主类网络下的子网掩码长度不同的情况,也不会丢失子网; 其三,允许网络管理者手动关闭主类边界路由器中自动路由汇总功能; 其四,报文中增加了路由标记字段,允许传递自治系统编号、路由起点等相关信息; 其五,报文中增加了下一跳字段,可有效防止出现 RIPv1 中存在的额外跳问题; 其六,支持 MD5(Message-Digest Algorithm) 认证,网络安全性有了大幅提高。需要读者明确的是: 在实际的网络工程中,受其跳数(16 跳即为不可达路径) 和慢收敛的影响,域内路由协议 RIP 通常只在中小型网络中部署使用。

1 域内路由协议 RIP 的报文格式

域内路由协议 RIP 使用用户数据报协议 UDP(User Datagram Protocol) 来封装路由信息[3-5],端口号为 520。受用户数据报协议报文长度限制的影响,RIP 报文长度不能超过 512 字节(一条 RIP 报文最多可包括 25 条路由信息。如果需要传递的路由信息超过 25 条,则需要拆分后再传递) 。根据 RIP 协议规定,相关 RIP 报文的交换也只能在两台邻居路由器之间进行,并且所交换的报文主要有以下两种类型: 其一,请求(request) 报文。该报文主要用来向邻居 RIP 路由器请求路由信息。其二,响应(response) 报

收稿日期: 2020-07-28
作者简介: 孙光懿(1979-) ,男(汉族) ,天津人,天津音乐学院工程师,主要研究方向: 计算机网络。

文。该报文主要用来向邻居 RIP 路由器通告本地路由信息。当路由器首次加入 RIP 网络时,通常会首先发送 request 报文,请求邻居 RIP 路由器的路由并进入循环等待状态(等待邻居 RIP 路由器的 response 报文的到来)。邻居 RIP 路由器在收到 request 报文后,会根据自身路由表生成 response 报文,予以应答。路由器在收到该响应报文后,会依据矢量-距离算法更新自己的路由表。需要读者注意的是:RIPv2 与 RIPv1 的报文格式相类似,均是由首部和路由信息所构成。只是 RIPv2 在路由信息中新增了路由标记、子网掩码、下一跳三个字段。

2 RIP 路由环路

2.1 环路原因

域内路由协议 RIP 产生路由环路主要基于以下两点原因[6-8]:其一,由于 RIP 采用距离-矢量算法,因此 RIP 路由器自身无法掌握网络的全局情况,只能依靠相邻 RIP 路由器来获取网络可达信息。其二,RIP 存在的慢收敛问题,会造成网络中的 RIP 路由器无法在同一时间内完成对路由表的更新。举例说明:路由器 A 已将目标网络 C 标记为不可达(对应目标网络 C 路由表项的跳数被修改为 16),正准备将此路由更新以每隔 30 s 一次的频率向网络中的其他 RIP 路由器进行广播时,路由器 A 收到了路由器 B 的路由更新报文,而该路由更新报文中包含着去往目标网络 C 的路由信息(对应目标网络 C 路由表项的跳数为 3)。此时,路由器 A 就会错误地认为存在一条通过路由器 B 达到目标网络 C 的路由,从而对自身路由表进行更新(对应目标网络 C 路由表项的跳数由原来的 16 被修改为 4)。路由器 A 在完成路由表更新后,会将该条路由信息发送给路由器 B,路由器 B 收到路由器 A 的路由更新报文后,除了对自身路由表进行更新外(对应目标网络 C 路由表项的跳数由原来的 4 被修改为 5),还会再将该路由信息发送给路由器 A,至此路由环路形成。

2.2 防环机制

域内路由协议 RIP 在诞生之初,开发者就注意到了其容易产生路由环路问题,因此设计了以下四种防环机制[9-11]:其一,计数无穷大。其工作原理为:路由条目的最大跳数被定义为 16 跳,当其跳数达到 16 跳时,则认为该路由条目不可达。其二,水平分割。其工作原理为:RIP 路由器接口不会把从某接口学习到的路由信息,再从该接口以广播或组播的方式发送给网络中的其他 RIP 路由器。需要读者注意的是:水平分割是 RIP 避免产生路由环路最核心的方法。其三,毒性逆转。其工作原理为:RIP 路由器从某些接口学习到的路由信息,会从该接口以广播或组播的方式再发送回去(跳数增加到 16 跳)。其四,触发更新。其工作原理为:当网络拓扑发生改变,RIP 路由器无需等待 30 s 的路由更新周期,可立即将路由更新发送给邻居 RIP 路由器。该防环机制可使故障路由信息快速的传播到整个网络,从而提高网络收敛速度。

3 仿真实验

3.1 网络拓扑构建及基本配置

为完成本次仿真实验,我们通过 GNS3 思科网络模拟器(Version 2.2.8),搭建了一个由三台思科 3760 路由器 R1、R2、R3 所构成的小型网络,该网络共有四个不同的网段(192.168.70.0/24 - 192.168.73.0/24)。其中,在路由器 R1 上建有回环接口 loopback1(192.168.73.1/24)。三台路由器之间均运行 RIP 路由协议(RIPv2)并相互连接。网络拓扑如图 3 所示。路由器间接口互联及 IP 地址分配情况如图 1 所示。路由器 R2 的核心配置如下(R1、R3 的相关配置与其类似,故省略):

(1) 路由器 R2 配置

```
R2(config)#router rip
```

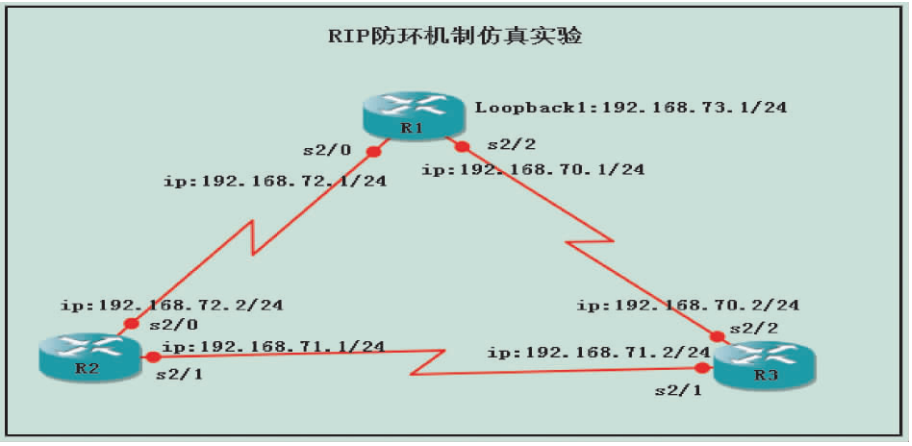

图 1　网络拓扑

Fig.1　Network topology

R2(config-router) #version 2

R2(config-router) #network 192.167.71.0

R2(config-router) #network 192.167.72.0

查看路由器 R2 的路由表,如图 2 所示。我们不难发现: RIP 路由协议已配置成功,各网段间实现了互联互通。其路由表中不仅存在两条路由代码为“C”的直连路由(运行 RIP 路由协议前即生成) ,而且还存在两条路由代码为“R”,下一跳地址为 192.168.72.1 的 RIP 路由(显而易见,上述两条 RIP 路由来自路由器 R1) 。

```
R2#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, 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, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.72.0/24 is directly connected, Serial2/0
R    192.168.73.0/24 [120/1] via 192.168.72.1, 00:00:28, Serial2/0
R    192.168.70.0/24 [120/1] via 192.168.72.1, 00:00:28, Serial2/0
C    192.168.71.0/24 is directly connected, Serial2/1
```

图 2　路由器 R2 的路由表

Fig.2　Routing table of router R2

3.2　计数无穷大

为能更清楚地向读者展现 RIP 计数无穷大[12](默认为开启状态) 的工作过程与防环效果,我们使用 passive-interface 命令将路由器 R1 的 S2/0 接口设置为被动接口(可以接收 RIP 路由更新,但无法向外发送 RIP 路由更新) ,4 m 后再次查看路由器 R2 的路由表,如图 3 所示。我们不难发现: 两条路由代码为“R”的 RIP 路由,其目标网络未发生改变,但下一跳地址变为了 192.168.71.2。这充分说明上述两条 RIP 路由来自路由器 R3。相关具体配置命令如下。

(1) 路由器 R1 配置

R1(config-router) #passive-interface s2/0

我们将路由器 R1 的 S2/2 接口也设置为被动接口,且关闭 Loopback1(192.168.73.1/24) 接口。路由器 R1 丢失了 Loopback1 接口网络,本应会产生一个 RIP 路由更新发送给路由器 R2、R3,但由于路由器 R1 与 R2、R3 互联的两个接口均被设置为被动接口,因此该 RIP 路由更新无法送达到路由器 R2、R3。而路由器 R3 虽未收到路由器 R1 的 RIP 路由更新信息,但仍可向路由器 R2 以每隔 30s 的频率发送 RIP 路由更新,向其通告 Loopback1 接口网络以 2 跳距离可达。同理路由器 R2 向路由器 R1 通告 Loopback1 接口网络以 3 跳距离可达。

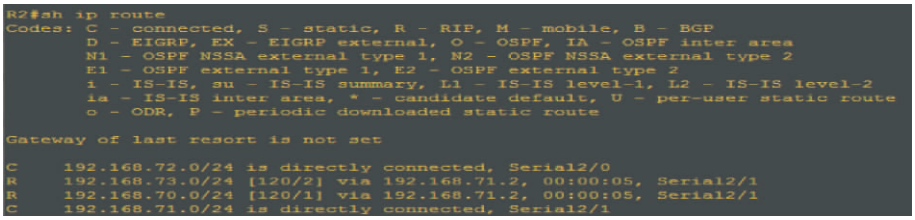

图3 路由器R1的路由表

Fig.3 Routing table of router R1

在路由器R1的路由表中,存在一条目标地址为192.168.73.0/24,下一跳地址为192.168.72.2的RIP路由(路由器R1认为存在一条通过路由器R2到达Loopback1接口网络的新路径),此时再恢复S2/2接口为非被动接口。同时使用debug ip rip命令查看路由器R2、R3发送和接收的RIP路由更新信息。

(2)路由器R2、R3发送和接收的RIP路由更新信息如下:

R3#

* Mar 1 00:08:29.571: RIP: sending v2 update to 224.0.0.9 via Serial2/1 (192.168.71.2)

* Mar 1 00:08:29.579: 192.168.73.0/24 via 0.0.0.0, metric 2, tag 0

//路由器R3使用组播地址224.0.0.9向路由器R2发送RIP路由更新,向其通告Loopback1接口网络以2跳距离可达。

R2#

* Mar 1 00:03:32.007: RIP: sending v2 update to 224.0.0.9 via Serial2/0 (192.168.72.2)

* Mar 1 00:03:32.019: 192.168.73.0/24 via 0.0.0.0, metric 3, tag 0

//路由器R2使用组播地址224.0.0.9向路由器R1发送RIP路由更新,向其通告Loopback1接口网络以3跳距离可达。

R3#

* Mar 1 00:08:40.707: RIP: received v2 update from 192.168.70.1 on Serial2/2

* Mar 1 00:08:40.715: 192.168.73.0/24 via 0.0.0.0 in 4 hops

//将路由器R1的S2/2接口恢复为非被动接口后,路由器R3收到了来自路由器R1的RIP路由更新,向其通告Loopback1接口网络以4跳距离可达。至此,Loopback1接口网络在拓扑上出现R1-R3-R2-R1的路由环路。

R3#

* Mar 1 00:09:05.435: RIP: received v2 update from 192.168.70.1 on Serial2/2

* Mar 1 00:09:05.439: 192.168.73.0/24 via 0.0.0.0 in 16 hops (inaccessible)

//该路由环路持续循环,直到路由器R3收到了来自路由器R1的RIP路由更新,向其通告去往Loopback1接口网络的距离为16跳。

R3#

* Mar 1 00:09:07.443: RIP: sending v2 flash update to 224.0.0.9 via Serial2/2 (192.168.70.2)

* Mar 1 00:09:07.447: 192.168.73.0/24 via 0.0.0.0, metric 16, tag 0

//而后路由器R3向邻居路由器R1发送RIP路由更新,向其通告去往Loopback1接口网络不可达的信息。

仔细分析上述信息我们不难发现:其一,只要路由器R3收到去往Loopback1接口网络为16跳距离的路由更新,就将其标记为不可达(inaccessible),并向邻居路由器发送此条路由更新。这足以充分说明RIP防环机制计数无穷大在发挥作用。其二,计数无穷大防环机制虽可有效解决RIP网络中的路由环

路,但也限制了 RIP 网络的整体规模。

3.3　水平分割

为能更清楚地向读者展现 RIP 防环机制水平分割[13](路由器接口下默认为开启状态)的工作过程与防环效果,首先,需要我们重启路由器 R1、R2、R3,以使它们能够重新交换路由信息;其次,我们使用 shutdown 命令将路由器 R1 的 S2/2 接口关闭;最后,我们分别查看路由器 R2、R3 的路由表,如图 4、图 5 所示。

```
R2#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, 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, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.72.0/24 is directly connected, Serial2/0
R    192.168.73.0/24 [120/1] via 192.168.72.1, 00:00:01, Serial2/0
C    192.168.71.0/24 is directly connected, Serial2/1
```

图 4　路由器 R2 的路由表

Fig.4　Routing table of router R2

```
R3#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, 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, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

R    192.168.72.0/24 [120/1] via 192.168.71.1, 00:00:14, Serial2/1
R    192.168.73.0/24 [120/2] via 192.168.71.1, 00:00:14, Serial2/1
C    192.168.71.0/24 is directly connected, Serial2/1
```

图 5　路由器 R3 的路由表

Fig.5　Routing table of router R3

从图 4、图 5 中我们不难发现: 其一,在路由器 R2 的路由表中存在一条去往 Loopback1 接口网络(192.168.73.0/24)的 RIP 路由,其下一跳地址为 192.168.72.1。显而易见,该条 RIP 路由是学自路由器 R1。其二,在路由器 R3 的路由表中同样存在一条去往 Loopback1 接口网络(192.168.73.0/24)的 RIP 路由,其下一跳地址为 192.168.71.1。显而易见,该条 RIP 路由是学自路由器 R2。

我们以路由器 R2 为例,使用 debug ip rip 命令查看其发送和接收的 RIP 路由更新信息。具体如下所示:

R2#

* Mar　1 00:07:46.475: RIP: received v2 update from 192.168.72.1 on Serial2/0

* Mar　1 00:07:46.483:　　192.168.73.0/24 via 0.0.0.0 in 1 hops

//路由器 R2 通过 s2/0 接口收到来自路由器 R1 的 RIP 路由更新,去往 Loopback1 接口网络以 1 跳距离可达。

R2#

* Mar　1 00:08:42.723: RIP: sending v2 flash update to 224.0.0.9 via Serial2/0 (192.168.72.2)

……

* Mar　1 00:08:42.731: 192.168.71.0/24 via 0.0.0.0, metric 1, tag 0

//路由器 R2 使用组播地址 224.0.0.9,通过 s2/0 接口向路由器 R1 发送 RIP 路由更新,只向其通

告去往目标网络 192.168.71.0/24 以 1 跳距离可达。

R2#

* Mar 1 00:08:42.723: RIP: sending v2 flash update to 224.0.0.9 via Serial2/1 (192.168.71.1)

……

* Mar 1 00:07:46.483: 192.168.73.0/24 via 0.0.0.0 in 2 hops

//路由器 R2 使用组播地址 224.0.0.9,通过 s2/1 接口向路由器 R3 发送 RIP 路由更新,向其通告去往 Loopback1 接口网络以 2 跳距离可达。

仔细分析上述 debug 信息,我们不难发现:其一,路由器 R2 从 s2/0 接口学习到了去往 Loopback1 接口网络的路由条目,但再从该接口向路由器 R1 发送 RIP 路由更新时,并不包括 Loopback1 接口网络。其二,路由器 R2 从 s2/1 接口向路由器 R3 发送 RIP 路由更新时,却包括了 Loopback1 接口网络。这足以充分说明 RIP 防环机制中的水平分割在发挥作用。

3.4 毒性逆转

毒性逆转[14]防环机制,读者可将其看做一种改进后的水平分割。如果 RIP 路由器收到的路由信息是经该机制处理过的,那么就会立即将该条路由从路由表中删除,从而有助于加快网络的收敛速度。但该防环机制也存在浪费链路带宽、使路由表增大的不足。

为能更清楚地向读者展现 RIP 毒性逆转防环机制的工作过程,首先,我们重启路由器 R1、R2、R3,以使它们能够重新交换路由信息;其次,我们使用 shutdown 命令将路由器 R1 的 S2/2 接口关闭;第三,在确保每台路由器均学习到了全网路由后,我们再使用 shutdown 命令将路由器 R1 的 Loopback1 接口关闭;第四,我们以路由器 R1 为例,使用 debug ip rip 命令查看其发送和接收的 RIP 路由更新信息:

(一)路由器 R1 发送和接收的 RIP 路由更新信息

R1#

* Mar 1 00:17:07.115: RIP: received v2 update from 192.168.72.2 on Serial2/0

* Mar 1 00:17:07.119: 192.168.73.0/24 via 0.0.0.0 in 16 hops (inaccessible)

//R1 通过 S2/0 接口收到来自 R2 的 RIP 路由更新,去往 Loopback1 接口网络不可达。

R1#

* Mar 1 00:17:19.483: RIP: sending v2 update to 224.0.0.9 via Serial2/0 (192.168.72.1)

* Mar 1 00:17:19.487: 192.168.73.0/24 via 0.0.0.0, metric 16, tag 0

//R1 通过 S2/0 接口向 R2 发送 RIP 路由更新,将去往 Loopback1 接口网络标记为 16 跳。

仔细分析上述 debug 信息,我们不难发现:当路由器 R1 从 S2/0 接口学习到 Loopback1 接口网络的路由后,会将该条路由再从 S2/0 接口发送回去,但是该条路由已被毒化(被标记为 16 跳)。这足以充分说明 RIP 毒性逆转防环机制在发挥作用。

4 讨 论

RIP 作为一种经典路由协议,具有配置简单、易于部署管理、占用网络带宽小等特点,但也存在易产生路由环路的不足。本文利用 EVE-NG 网络模拟器设计了 RIP 防环机制仿真实验,分析了计数无穷大、水平分割、毒性逆转等防环机制的实现原理并给出了具体实验方法,可以使读者更直观的观察上述防环机制的工作过程与防环效果。此次仿真实验不仅有助于读者对 RIP 防环机制的进一步理解,而且还有助于读者熟练掌握 RIP 协议的配置方法。

参考文献:

[1] SIVASUBRAMANIAN B.CCNP SWITCH 学习指南[M].北京: 人民邮电出版社,2011.
[2] 冯昊,黄治虎,伍技祥.交换机/路由器配置与管理[M].北京: 清华大学出版社,2010.
[3] 张钢,黄小波.思科虚拟实验平台的构建[J].实验室研究与探索,2010,(08):216-218.
[4] 桑世庆,卢晓慧.交换机/路由器配置与管理[M].北京: 人民邮电出版社, 2010.
[5] 李旺,陈荣,肖兰,等.NAT 在不同环境下企业网中的应用分析[J].铜仁学院学报,2018,20(06):104-107.
[6] 张前进, 齐美彬, 李莉.基于应用层负载均衡策略的分析与研究[J].计算机工程与应用, 2007, 43(32):138-142.
[7] 李永.NAT 仿真实验设计与实现[J].实验技术与管理,2018,35(04):132-135.
[8] 杨礼.ACL 和 NAT 技术在局域网中的应用与实践[J].喀什大学学报,2018,39(03):108-111.
[9] 仇宇.校园网多链路接入及其负载均衡的设计与实现[J].绵阳师范学院学报,2009,25(05):130-134.
[10] 孙光懿.基于策略路由和 NAT 的多出口校园网仿真实验设计[J].西北民族大学学报(自然科学版),2017,38(02):14-20.
[11] 杨文彬.NAT 网络地址翻译技术在高校网络管理中的应用[J].山西大同大学学报(自然科学版),2017,33(02):6-8,11.
[12] 蒙元胜. 基于 UDP/TCP 协议的 NAT 穿越方案研究[D].广州: 中山大学,2014.
[13] 王东.智能 DNS 和 NAT 技术在多出口高校校园网中的应用[J].重庆科技学院学报(自然科学版),2012,14(03):151-152,176.
[14] 吕景涛. 非对称 NAT 穿透模型研究[D].北京: 北京邮电大学,2013.
[15] 孙光懿,贾英霞.基于 GNS3 的多自治系统路由仿真[J].实验室研究与探索,2019,38(04):123-128,142.
[16] 陈利,王冠.基于 ENSP 的 GRE VPN 结合 NAT 的研究与实现[J].喀什大学学报,2019,40(06):68-74.

Simulation Experiment of Anti-routing Loop Based on RIP

SUN Guangyi[1], YAO Hongxiang[2]

(1.*Office of Network Security and Information, Tianjin Conservatory of Music, Tianjin* 300171, *China*;
2.*State Grid-Commerce Technology Co.Ltd.*, *Tianjin* 300022, *China*)

Abstract: RIP is an internal gateway routing protocol, which has two versions, RIPv1 and RIPv2. It is often used to exchange routing information in a small autonomous system. Based on the in-depth study of RIP message format, the cause of routing loop and anti loop mechanism, the simulation experiments of anti loop mechanism such as infinite count, horizontal segmentation, toxicity reversal are designed and implemented by EVE-NG network simulator. Combined with the analysis of debug IP rip command and rip routing table, the working process and effectiveness of the above-mentioned anti ring mechanism are verified. It can provide important reference for readers to deploy RIP protocol in actual network.

Key words: RIP; count infinity; horizontal division; toxicity reversal

[责任编辑: 王向华]