**路由协议分析**

# 1.RIP分析

RIP有2个版本，有V1、V2,不指定版本是有个默认版本

**默认版本的特点（其实根RIPv1差不多，就是能够接收RIPv1、2的路由）：**

自动汇总，不能手工关闭

唯一有类路由协议

广播更新

无认证

R1：

router rip

 network 172.16.0.0

 network 192.167.1.0

 network 192.168.1.0

R2：

router rip

 network 192.168.1.0

 network 192.168.2.0

 network 192.168.3.0

R2#show ip protocols

　Default version control: send version 1, receive any version

    Interface             Send  Recv  Triggered RIP  Key-chain

    Ethernet0/0            1     1 2

    Loopback0             1     1 2     //默认接收版本1、2,发送版本1

Loopback2             1     1 2　//发送为RIPv1,不携带子网掩码

**RIPv1的特性：**

自动汇总，不能手工关闭

唯一有类路由协议

广播更新

无认证

router rip

version 1

show ip protocols

  Default version control: send version 1, receive version 1

    Interface             Send  Recv  Triggered RIP  Key-chain

    Ethernet0/0           1    1

    Loopback0             1     1  //默认只收发RIPv1

    Loopback2             1     1

R    172.16.0.0/16 [120/1] via 192.168.1.1, 00:00:14, Ethernet0/0　//自动汇总，有类路由协议

     192.168.1.0/30 is subnetted, 1 subnets

C       192.168.1.0 is directly connected, Ethernet0/0

R    192.167.1.0/24 [120/1] via 192.168.1.1, 00:00:14, Ethernet0/0

C    192.168.2.0/24 is directly connected, Loopback0

C    192.168.3.0/24 is directly connected, Loopback2

**RIPv2的特性：**

自动汇总，可以关闭，可以手工汇总

无类路由协议（携带子网掩码）

组播更新（目标地址224.0.0.9）

可以认证（明文、MD5）

router rip

version 2

show ip protocols

Default version control: send version 2, receive version 2

    Interface             Send  Recv  Triggered RIP  Key-chain

    Ethernet0/0           2     2

    Loopback0             2     2  //默认只收发RIPv2

    Loopback2             2     2

show ip route

     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks

R       172.16.0.0/16 [120/1] via 192.168.1.1, 00:02:06, Ethernet0/0**自动汇总**

R       172.16.1.0/24 [120/1] via 192.168.1.1, 00:00:13, Ethernet0/0 **无类路由**

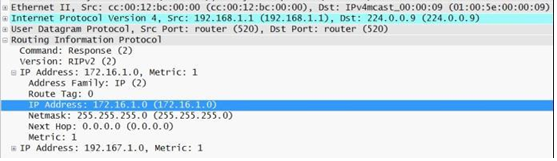
     192.168.1.0/30 is subnetted, 1 subnets

C       192.168.1.0 is directly connected, Ethernet0/0

R    192.167.1.0/24 [120/1] via 192.168.1.1, 00:00:13, Ethernet0/0

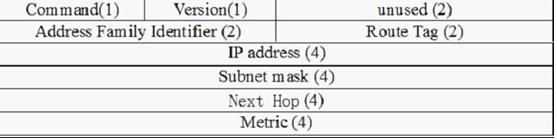
C    192.168.2.0/24 is directly connected, Loopback0

C    192.168.3.0/24 is directly connected, Loopback2



可以从这看出RIPv2的路由是带子网掩码的！同时是组播更新的，目标地址为224.0.0.9！使用UDP协议，端口号为520.

**RIP Version2的格式：**



**命令Command：**1.路由信息请求　2.路由信息响应　3、4过时　5.留作Sun微系统公司内部使用

**版本Version:**版本1、版本2

**Unused：**未使用，设置全为0

**地址标识Address Family Identifier：**指示路由项中的地址种类，对于IPV4总是设置为2；当请求全部路由信息时，设置为0.

**Route Tag：**外部路由标记，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(EGP)获得的路由信息。

**Ip Address：**路由条目的IPV4地址，可以是网络地址，子网地址或主机路由。

**Subnet mask：**子网掩码，应用于IP地址产生非主机部分地址，为0时表示不包括子网掩码部分，使得RIP能够适应更多的环境。

**Next Hop：**下一跳，可以对使用多路由协议的网络环境下的路由进行优化；如果是0.0.0.0的话，表示通告路由器的地址是最优的下一跳地址。

**Metric：**是一个1-16之间的跳数。

关闭自动汇总

router rip

no auto-summary

     172.16.0.0/24 is subnetted, 1 subnets

R       172.16.1.0 [120/1] via 192.168.1.1, 00:00:14, Ethernet0/0**没汇总的路由了**

     192.168.1.0/30 is subnetted, 1 subnets

C       192.168.1.0 is directly connected, Ethernet0/0

R    192.167.1.0/24 [120/1] via 192.168.1.1, 00:00:14, Ethernet0/0

C    192.168.2.0/24 is directly connected, Loopback0

手工汇总

interface Loopback2

 ip summary-address rip 172.16.0.0 255.255.192.0

R1(config-if)#do show ip rip da

172.16.0.0/16    auto-summary

172.16.0.0/18    int-summary　刚刚手工汇总的

明文认证（简单字符认证）

RT2（config）：

key chain tang　　　　　　//密钥管理串（只具本地意义）

 key 5　　　　　　　　　　//密钥ID

 key-string cisco　　　　//密钥字符为cisco

 key 10　　　　　　　　　//密钥ID，可建多个密钥

  key-string cisco2　　　　//密钥字符为cisco2　（只需配一个就行，这里我是用来验证的）

int e0/0

ip rip authentication mode text  　//使用明文进行认证（默认方式）

ip rip authentication key-chain tang　//认证使用的密钥串

RT1（config）：

key chain tang

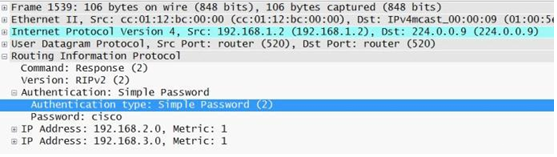
 key 5

  key-string cisco

int e0/0

ip rip authentication mode text  　//使用明文进行认证

ip rip authentication key-chain tang　//认证使用的密钥串



认证原则：KeyChain里可以有多个KeyID和密钥。只发送最小KeyID的密钥

明文：发送时不带KeyID，接收方和KeyChain里所有密钥匹配，成功则通过认证。

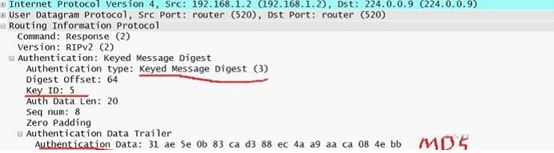
MD5：发送时携带KeyID，接收方寻找相同的KeyID，如果有，只进行一次匹配决定是否成功。如果无，向下查找下一个KeyID进行匹配，决定是否成功。

MD5认证配置

int e0/0

ip rip authentication mode md5

ip rip authentication key-chain tang



其它配置一样注意两边的KeyID需一致。

对方发来的密钥只要在本地有，就能通过认证，如果只有一边认证通过那也只有一边能学习到路由，另一边因不匹配密钥而丢弃！

**RIP的共同特性：**

使用UDP传输协议，端口号为520,最大跳数为15跳，16跳为不可达；基于Bellman-Ford算法，基于距离矢量路由协议，管理距离为120，以跳数作为度量值。

定义了2种消息类型：

request message(请求消息)：用来向邻居请求一个update更新

response message(应答消息)：包含路由条目的更新消息

注意：一个消息中最大可以包含25个路由条目，当AFI(地址族标识)为0时，表示对整个路由表的请求。该值通常为2。在认证时只有24个了，AFI为全1(0xffff)。

**工作原理：**

1.发现路由：首先运行RIP进程，发现自己的路由信息（收集直连网段信息）

2.通告路由：将自己知道的路由信息通告给其它邻居（request、respose）

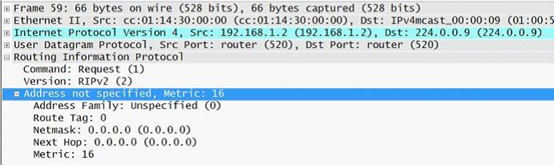
3.计算路由：基于距离矢量算法，计算最优路由添加到全局路由表（跳数）

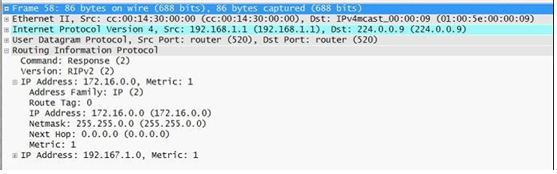
4.路由收敛：当网络拓扑发生变化时，能重新计算出最优路由（触发更新）

首先R1、R2运行RIP，向外发送request message，收到request message，给出响应response message报文。通过收到的路由运行距离矢量算法，计算出最佳路由添加到全局路由表中。









R2(config-router)#do show ip protocols

Routing Protocol is "rip"

  Sending updates every 30 seconds, next due in 25 seconds

  Invalid after 180 seconds, hold down 180, flushed after 240

Update(路由更新计时器)：30秒，每隔30s发送update更新报文

Invalid(无效计时器)：180秒（超时将条目hop置为Possibly down，并发送跳数为16的update）

Flush(刷新计时器)：240秒（超时删除条目）

Holddown(抑制计时器)：180秒（在Invalid超时后开启。另外，当收到一个更坏的跳数的更新后抑制开始）

命令：

router rip

timer basic 30 180 180 240　　　(RIP域内必须一致)

手动修改接口的RIP版本，并且优先router rip下指定的版本

int e0/0

ip rip receive version 1　//指定接口接收RIPv1

ip rip send version 2　　　//指定接口发送RIPv2

Default version control: send version 1, receive any version

    Interface             Send  Recv  Triggered RIP  Key-chain

    Ethernet0/0           2     1

手工指定单播更新

router rip

neighbor 192.168.1.1 //指定邻居地址，单播更新

**防环机制：**

定义最大跳数：每一跳增加1，到16跳认为不可达。

水平分割：从某接口学习到的路由不会再从该接口发送回去。(可以打开或关闭[no]ip split-horizon)

路由毒化：路由器主动把路由表中发生故障的路由项以度量值最大16跳的形式，通告给邻居。

毒性逆转：从某接口学习到的路由再从该接口发送回去但跳数已经被增加到了16跳。

抑制定时器：当某网络消失时，并不立即删除该条目而是等待定时器（240秒）才删除，为了网络可能的恢复。

触发更新：网络拓扑变化时，立即通知直连邻居而不再等待更新周期（30秒）。

修改管理距离：

(config-router)#distance 管理距离值(1-255)

只能改变路由器自身上的RIP路由的AD值。

配置被动接口：

(config-router)#passive-interface interface e0/0  //阻止单个接口发送路由更新

当很多接口需配置成被动接口时：

(config-router)#passive-interface default  //把所有接口配置成被动接口

(config-router)#no passive-interface interface e0/0//此接口不需要配置成被动接口

**注意：**被动接口命令是停止以广播或组播方式发送更新，但仍然可以接收广播和组播。passive-interface对单播是没有任何作用的。

RIP是距离矢量算法，是根据跳数来进行优先的，当一条链路带宽为2M，另一条链路为64K时，如果它们通告的路由的跳数相等时，RIP会走负载均衡，这是不合理的，为了解决此种状况，我们可以用offer-list进行调整。

如上拓扑，修改192.168.2.0/24此路由的跳数

R2（config）#access-list 10 permit 192.168.2.0

R2（config）#router rip

R2(config-router)#offset-list 10 out 10 e0/0　　//对匹配的路由在E0/0的出方向上修改增加10跳

格式：offset-list　列表号/名　in/out 跳数　进接口/出接口

R1：show ip route

R    192.168.2.0/24 [120/11] via 192.168.1.2, 00:00:01, Ethernet0/0

另外：Router#show ip rip database　可以用来查看RIP路由数据库

**RIP协议**

**RIP简介：**

RIP(Routing Information Protocol 路由信息协议)是一种简单的IGP。RIP是一个国际标准协议，所有的路由器厂商都支持它。RIP是应用层协议工作在UDP的520端口上，所有的RIP数据包的源端口和目的端口的端口号都是520。RIP使用距离矢量算法，当数据包通过一个路由器是一跳。RIP初始化时会从每个参与工作的接口上发送请求报文，该数据包向所有的RIP路由器请求一份对方完整的路由表，该请求以广播或点到点的形式发送到直连路由器。RIP默认支持4条最多6条等开销路径做负载均衡。RIP不适用于路径剧烈变化网络环境中，也不适用于大型的网络环境中。RIP在小型网络中仍在大量使用，现在大型网络多采用OSPF。

**RIP的工作原理：**

RIP协议是V－D算法在局域网上的直接实现，RIP将协议的参加者分为主动机和被动机两种。主动机主动地向外广播路径刷新报文，被动机被动地接受路径刷新报文。一般情况下，网关作主动机，主机作被动机。RIP规定，网关每30秒向外广播一个V－D报文，报文信息来自本地路由表。RIP协议的V－D报文中，其距离以跳数计：与目的网络直接相连的网关规定为一跳，相隔一个网关则为两跳……依次类推。一条路径的距离为该路径（从源发送方到目的发送方）上的网关数。为防止寻径回路的长期存在，RIP规定，长度为16跳的路径为无限长路径，即不存在路径。所以一条有限的路径长度不得超过15。正是这一规定限制了RIP的使用范围，使RIP局限于小型的局域网络中。对于相同开销路径的处理是采用先入为主的原则。在具体的应用中，可能会出现这种情况，去往相同网络有若干条相同距离的路径。在这种情况下，无论哪个网关的路径广播报文先到，就采用谁的路径，直到该路径失败或被新的更短的路径来代替。RIP协议对清除过时路径的处理是采用了两个定时器；超时(路由无效)计时器和垃圾收集(路由刷新)计时器。路由器对表中的每个项目都设置两个计时器，每增加一个新路由条目，就相应的增加两个计时器。当新的路由条目被装入到路由表中时，超时计时器被初始化为0，并开始计数。每当收到包含该路由条目的RIP消息，该条目的超时计时器就被重新设置为0。如果在180秒内没有接收到包含该路由条目的RIP消息，该路由的度量就被设置为16，而启动该路由的垃圾收集计时器。如果在接下来的60秒，仍没有收到该路由的RIP消息，该路由就从路由表中删除。如果在垃圾收集计时器到240秒之前，收到了包含路由的消息，路由条目被装入到路由表中，计时器被清0并重新启动超时计时器。包括RIP在内的V－D算法路径刷新协议，都有一个严重的缺陷，即“慢收敛”（slow convergence）问题，又叫“计数到无穷”(count to infinity)。如果出现环路，直到路径长度达到16，也就是说要经过7番来回（至少30×7秒），路径回路才能被解除，这就是所谓的慢收敛问题。解决的方法有很多种，主要的解决方法有水平分割（split horizon）法和带触发更新的毒性逆转(Posion Reverse with Triggered updates))法。水平分割法的原理是：当网关从某个网络接口发送RIP路径刷新报文时，其中不能包含从该接口获得的路径信息。毒性逆转法的原理是：某路径崩溃后，最早广播此路径的网关将原路径继续保存在若干刷新报文中，但是指明路径为无限长。为了加强毒性逆转的效果，最好同时使用触发更新技术：一旦检测到路径崩溃，立即广播路径刷新报文，而不必等待下一个广播周期。

**RIP的工作过程：**

网关刚启动时，运行V－D算法，对V－D路由表进行初始化，为每一个和它直接相连的实体建一个路由条目，并设置目的IP地址，距离为1（RIP和V－D在这里略有不同），下一站的IP为0，还要为这个表目设置两个定时器（超时计时器和垃圾收集计时器）。每隔30秒就向它相邻的实体广播路由表的内容。相邻的实体收到广播时，就对广播的数据报进行检查。因为广播的内容可能引起路由表的更新，所以这种检查是细致的。当报文传至IP层时，首先检查报文是否来自端口520的UDP数据报，如果不是则丢弃，因为路由器不转发受限广播。否则再看RIP报文的版本号：如果为0，这个报文就被忽略；如果为1，检查必须为0的字段，如果不为0，忽略该报文；如果大于1，RIPv1对必须为0的字段就不检查。然后对源IP地址进行检查，看它是否来自直接相连的邻居，如果不是来自直接邻居，则报文被忽略。如果上面的检查都是有效的，则对广播的内容进行逐项的处理。看它的度量值是否大于15，如果是则忽略该报文（实际上，如果来自相邻网关的广播，这是不可能的）。然后检查地址族的内容，如果不为2，则忽略该报文。如果是更新自己的路由表，并为每个更新后的条目设置两个计时器，初始化值为0。就这样所有的网关都每隔30秒向外广播自己的路由表，相邻的网关和主机收到广播后来更新自己的路由表。直到每个实体的路由表都包含到所有实体的寻径信息。如果某条路由突然断了，或者是其度量大于15，与其直接相邻的网关采用水平分割或触发更新的方法向外广播该信息，其他的实体在两个计时器溢出的情况下将该路由从路由表中删除。如果某个网关发现了一条更好的路径,它也向外广播,与该路由相关的每个实体都要更新自己的路由表的内容。

**RIP的版本：**

RIP有RIPv1和RIPv2两种版本。RIPv1不支持VLSM是有类的路由选择协议，路由通告中不携带子网掩码；使用受限广播地址发送路由更新。RIPv2支持VLSM是无类的路由选择协议，路由通告中携带子网掩码；使用多播地址224.0.0.9发送路由更新。

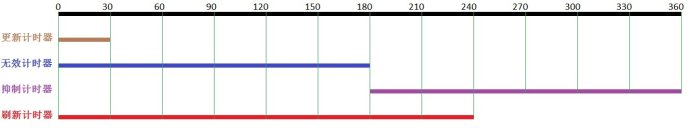
**RIP的消息类型：**

RIP有两种消息类型，request(请求消息)和response(响应消息)。

**request：**RIP的request消息在特殊情况下发送，当路由器需要时它可以提供即时的路由信息。最常见的例子是当路由器第一次加入网络时，通常会发送request消息，以要求获取相邻路由器的最新路由信息。

**response：**当RIP接收到request消息，将处理并发送一个response消息。消息包含自己的整个路由表，或请求要求的条目，正常情况下路由器通常不会发送对路由信息有特殊要求的请求消息。RIP会每30秒发送一个response消息，用于路由表更新。

**RIP计时器：**

**  
路由更新计时器：**默认30秒，用于设置定期路由更新的时间间隔，在这个间隔里路由器发送一个自己完整路由表的拷贝到所有相邻的路由器。为了避免在MA(多路访问)的网络中由于系统时延引起的更新同步，在Cisco中实际更新时间是25.5-30秒之间，即30秒减去一个在4.5秒内的随机值。

**路由无效计时器：**默认180秒，路由器在确定一个路由条目称为无效路由之前所需要等待的时间。路由器在收到这个更新包开始计时，如果在这个期间内没有得到关于某个指定路由的任何更新消息，它将认为这个路由条目已失效，在路由条目中该路由被标志为A.B.C.D is possibly down。当这一情况发生时，这个路由器将会给它所有的邻居发送一个更新消息以通知他们这个路由条目已经无效。

**抑制计时器：**默认180秒，抑制计时器是Cisco私有计时器。路由器如果在相同的接口上收到某个路由条目的距离比原先收到的距离大，那么将启动一个抑制计时器。在抑制计时器的时间内该目的不可达，路由器也不学习该条路由信息，除非是一条更好的路由信息即度量值更小的路由才接受；抑制周期过后，即使是差的路由信息也接受。抑制计时器主要是在RIP协议中用来避免路由抖动保持网络的稳定性，也可以避免路由环路。例如路由器收到了一个不可达报文即16跳的通告时，在接下来的60秒内会显示possibly down，60秒后刷新计时器超时时会删除该路由，但这时抑制计时器才过去了60秒还有120秒的时间，而这120秒就是保持网络稳定用的，即使有一个新的路由也不更新，他会一直等到120秒后再更新。在抑制计时器开始时就开始对外发送毒化的路由即hop=16，收到这个路由的设备毒性逆转再发送回来(打破水平分割原则)，抑制计时器存在的理由就是为了使全网毒化的路由接收一致，防止路由环路。该定时器的原理是引用一个怀疑量，不管是真的还是假的路由消息，路由器先认为是假消息来避免路由抖动。如果在抑制计时器超时后还接收到该消息，那么这个路由器就认为该消息是真的。

**路由刷新计时器：**默认240秒，用于设置某个路由称为无效路由并将它从路由表中删除的时间间隔，在这个路由条目无效之后，并将它从路由表中删除前，路由器会通告它的邻居这个路由即将消亡。如果在刷新时间内没有收到更新报文，那么该目的的路由条目将被刷掉也就是直接删除；如果在刷新时间内收到更新报文，那么该刷新计时器将置0，并重新无效计时。RIP中真正删除路由条目的是刷新计时器超时(无效计时器过后60秒，会删除无效的路由条目)。路由无效计时器的值比无效定时器多了60秒，也就是说无效计时器的值必须要小于路由刷新计时器的值，这就为路由器提供足够的时间在本地路由表更新前通告它的邻居有关这一无效路由条目的情况。

**触发更新计时器：**如果在路由的度量值发生改变时就会产生触发更新。而且触发更新不会引起接收路由器重置它们的更新计时器，因为如果这么做网络拓扑的改变会造成触发更新“风暴”。当一个触发更新传播时，这个计时器被随机的设置为1-5秒之间的数值来避免触发更新风暴，在这个计时器超时前不能发送并发的触发更新。如果启用触发更新(ip rip triggered)则保持时间=0永不超时，即下列配置timers basic 30 180 0 240自动出现(计时器默认配置为timers basic 30 180 180 240)。触发更新只能配置在串口下，启用触发更新的链路两边的路由器都要配置触发更新(因为需要协商，否则有问题)，启用触发更新后路由更新时是增量更新，且更新时只从启用了触发更新的接口发送一次更新，触发更新计时器单位是毫秒，其他计时器单位都是秒。

**不连续子网：**同一主类网络下的若干连续子网被另一主类网络分割开来。

**连续子网:**10.1.0.0/16----R1----10.2.0.0/16----R2----10.3.0.0/16

10.1.0.0/16----R1----10.2.0.0/16----R2----11.1.0.0/16

**不连续子网：**10.1.0.0/16----R1----11.1.0.0/16----R2----10.2.0.0/16

10.1.1.0/24----R1----192.168.1.0/24----R2----192.168.2.0/24----R3----10.1.2.0/24

**metric(跳数)：**RIP仅使用metric来衡量源网络到目的网络的距离。从源到目的地的路径中每经过一个路由器就被赋予一个跳数值，此值通常为1。当路由器收到包含新的或改变的目的网络表项的路由更新信息，就把其metric值加1然后存入路由表，发送者的IP地址就作为下一跳地址。RIP通过对从源到目的地的最大跳数加以限制来防止路由环路，最大metric为15，16为不可达。

**RIP的优点：**对于小型网络，RIP占带宽小，易于配置、管理、实现。

**RIP的缺点：**

1.仅以跳数作为度量值，常常不能计算出最优路径。

2.度量值以16跳为上限，不适合于大的网络。

3.安全性差，接受来自任何设备的路由更新，容易受到恶意的RIP欺骗。(单指RIPv1，RIPv2有密码验证机制)

4.不支持VLSM。(RIP采用子网掩码恢复机制，并不能解决这个问题)

5.收敛慢，RIP采用周期性的更新而不是触发更新。(如抑制计时器也增加了收敛时间)

6.带宽消耗大。RIP需要大量的信息交换：一方面，每个更新报文就每一条路由都包含一个条目，更新报文的大

  小相当于一个路由表(其条目数与网间网络数成正比)，而且其中的许多条目都是与当前路径刷新无关的；另一

  方面，所有网络都参与定期交换信息，要交换的信息量极大。

注意：RIP通告的时候只需要通告主类网络号。

**RIPv1：**

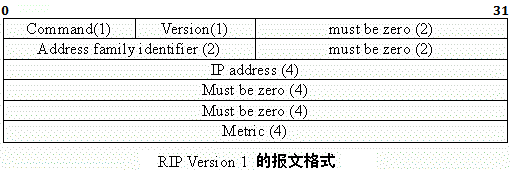
**特性：**

1.路由更新是广播地址255.255.255.255更新

2.在主类边界路由器执行自动汇总，并且该自动汇总无法人工关闭

3.有类路由协议，所有的主机和路由器接口的使用相同的子网掩码(不支持VLSM、不支持不连续子网)

**报文：**



**Command(命令)：**当为1时表示request报文；当为2时表示response报文。请求报文：要求接收方路由器发送其全部或部分路由表。response报文：主动提供周期性路由更新或对请求消息的响应。大的路由表可以由多个response报文来传递信息。

**Version Number(版本号)：**使用的RIP版本。

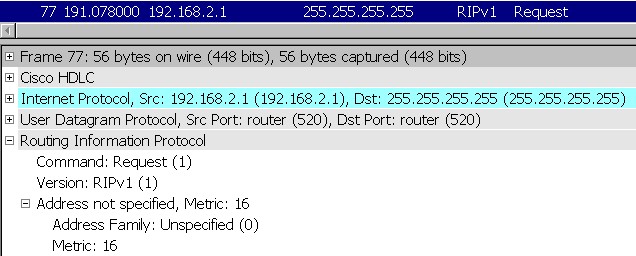
**Zero(0)：**未使用。

**Address Family Identifier(地址簇标志)：**指明使用的地址簇。RIP设计用于携带多种不同协议的路由信息。每个项都有地址标志来表明使用的地址类型，IP的AFI为2，0为没有指定。

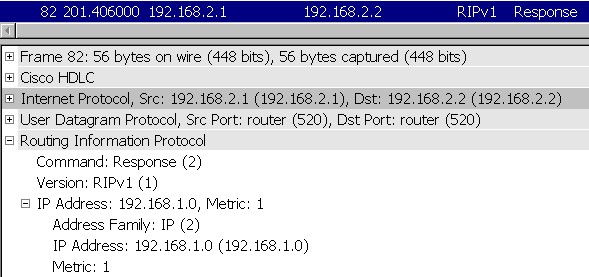
**IP Address(地址)：**目的网络地址(自然网段地址、子网地址、主机地址)。

**Metric(跳数)：**到目的的过程中经过了多少跳数。有效路径的值在1-15跳之间，16跳为不可达路径。

**RIPv1 request报文：**

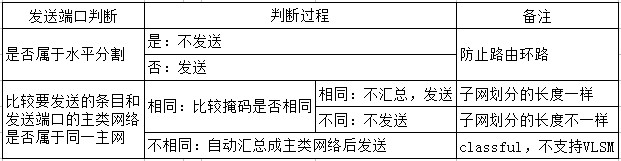


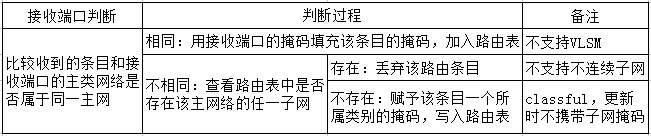
**RIPv1 response报文：**

  
注意：一个IP RIP报文中最多可有25条地址项；如果是RIPv2的验证报文，第一条路由表项作为验证项，所以最多可以有24条路由表项。RIP请求报文中AFI为0，Metric为16。

**RIPv1发送、接收规则：**

**发送规则：**

  
**接收规则：**



注意：若是一条主机路由，则路由器都发送，接收时加上32位掩码。

**RIPv2：**

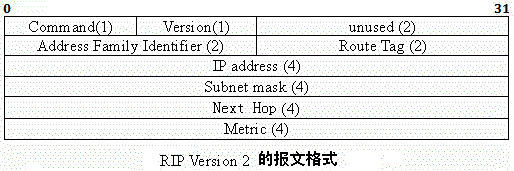
**特性：**

1.路由更新是组播地址224.0.0.9更新(减少网络与系统资源消耗)

2.自动汇总是自动开启的，但可以人工关闭，支持手工汇总。

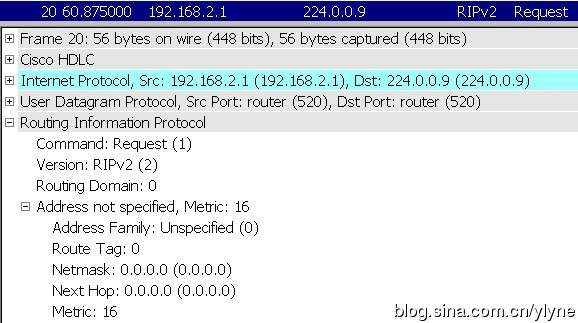
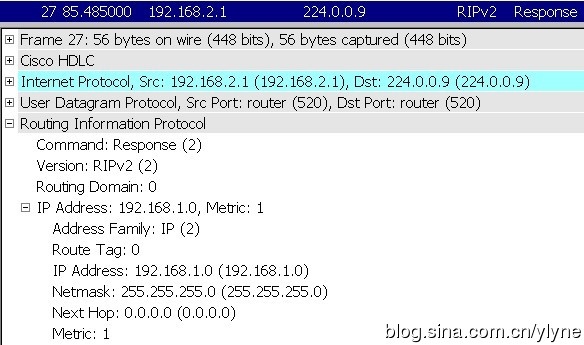
3.属于无类路由协议，支持变长掩码(支持vlsm、支持不连续子网)

**报文：**

  
**Route Tag(路由标记)：**用来支持EGP，它传递自治系统的标号给EGP及BGP(边界网关协议)。在路由策略中可根据路由标记对路由进行灵活的控制。没有路由标记的路由器必须将0作为自己的路由标记对外广播。  
**Subnet Mask(子网掩码)：**包含该条路由项目的子网掩码，支持路由聚合和CIDR。如果此字段为0，则该项不指定子网掩码。

**Next Hop(下一跳)：**指明下一跳的IP地址。在广播网上可以选择到最优下一跳地址。

**RIPv2 request报文：**

**  
RIPv2 response报文：**

说明：启动RIP前在接口模式下已配置了RIP相关命令，则这些配置只有在RIP启动后才生效；RIP只在指定网段的接口上运行，对于不在指定网段上的接口，RIP既不在它上面接收和发送路由，也不将它的接口路由转发出去，因此RIP启动后必须指定其工作网段；R1(config-router)#network 0.0.0.0命令用来在所有接口上能使RIP。

**RIPv2和RIPv2的主要区别：**

1.RIPv1是有类路由协议，更新过程中不携带子网信息，RIPv2是无类路由协议，更新过程中携带子网信息；

2.RIPv1不支持VLSM，RIPv2支持VLSM；

3.RIPv1没有认证功能，RIPv2支持认证，且有明文和MD5两种认证；

4.RIPv1自动汇总不能关闭，且不支持手动汇总，RIPv2可以关闭自动汇总，且支持手动汇总；

5.RIPv1是广播更新，RIPv2是组播更新；

6.RIPv1对路由没有标记功能，RIPv2可以对路由打标记(tag)，用于过滤和作策略；

7.RIPv1发送的updata最多可以携带25条路由条目，RIPv2在有认证的情况下最多只能携带24条路由条目；

8.RIPv1发送的updata包里没有next-hop属性，RIPv2有next-hop属性，可以用于路由更新的重定。

**RIP的防环机制：**

1.计数无穷大：定义最大跳数为15跳，当16跳为不可达；

2.水平分割：从一个接口学习到的路由不会再广播回该接口,减少带宽消耗，防止路由环路，但有时不能解决某

  些拓扑的环路(拓扑本身就是循环结构)；

3.毒性逆转：从一个接口学习的路由会发送回该接口，但是已经被毒化了，跳数设置为16跳，可以消除对方路由

  表中的无用路由信息；

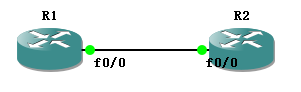
4.触发更新：一旦某条路由的度量值发生了变化，就立即向邻居路由器发布更新报文，而不等到下一刷新周期，

  避免在多个路由器之间形成路由环路的可能，加快了网络的收敛速度但会造成网络上突然的流量激增；

5.抑制计时器：防止路由表频繁跳动，增加了网络的稳定性，但也增加了收敛时间。

说明：以上防环路机制全部默认开启的；RIPv1不支持触发更新，RIPv2支持触发更新。

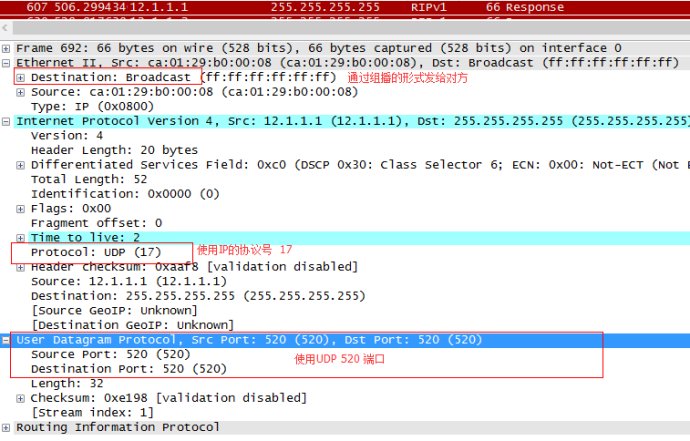
各路由协议封装格式



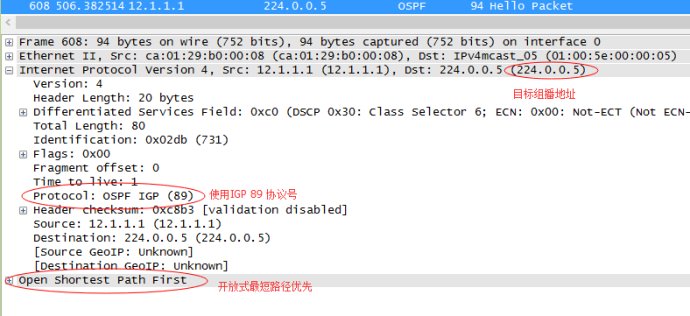
|  |  |  |  |
| --- | --- | --- | --- |
|  | 封装形式 | 协议&协议号&端口 | 组播地址 |
| rip v2 | eth-ip--udp--rip | UDP & 17 & 520 | 224.0.0.9 |
| ospf | eth--ip--ospf | IGP & 89 | 224.0.0.5(建立邻居) |
| eigrp | eth--ip--eigrp | Eigrp88 | 224.0.0.10 |
| bgp | eth--ip--tcp--bgp | TCP & 6 & 179 |  |

RIP数据包封装格式    eth-ip--udp--rip

rip使用的UDP 协议，协议号为17 ，端口号为520

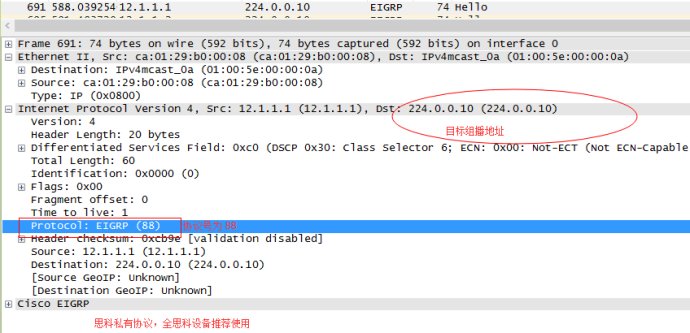


OSPF数据包封装格式：eth--ip--ospf

ospf使用ip的协议号为89，组播地址为224.0.0.5(建立邻居使用)  


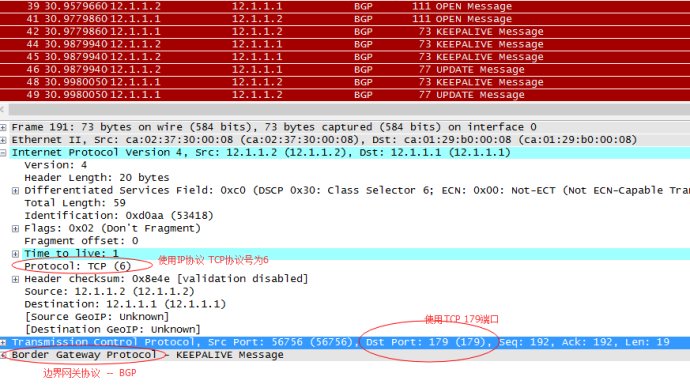
EIGRP数据包封装格式：eth--ip--eigrp

eigrp使用的协议是88，组播地址是224.0.0.10



BGP数据包封装格式：eth--ip--tcp--bgp

使用 tcp 协议，协议号为 6  端口号为179



# 2.[路由协议分析](http://www.cnblogs.com/leftshine/p/5698911.html)

分析所用软件下载：[Wireshark-win32-1.10.2.exe](https://pan.baidu.com/s/1pLH6gUB)

一、分析目的

分析OSPF的包格式

二、分析要求

1. 设计应用以获取ospf报文

2. 分析ospf报文的格式与内容

3. 理解ospf协议的工作过程

三、分析内容

1.设计应用以获取ospf报文

使用Wireshark抓包工具抓取OSPF的Hello报文

计算机会周期性的自动发送hello报文，只需用Wireshark获取即可

2. 分析ospf报文的格式与内容（分析至少2个报文）

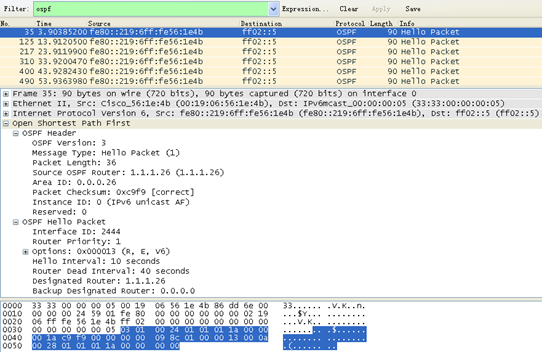
分析见第四部分

3. 理解ospf协议的工作过程

四、分析结果及总结

抓取到的OSPF Hello报文：

030100240101011a0000001ac9f900000000098c01000013000a00280101011a00000000



报文分析：

**公共首部OSPF Header**

版本：03

OSPF Version: 3

类型：01

Message Type: Hello Packet (1)

报文长度：00 24

Packet Length: 36

路由器标识：01 01 01 1a

Source OSPF Router: 1.1.1.26 (1.1.1.26)

区域标识：00 00 00 1a

Area ID: 0.0.0.26

校验和：c9 f9

Packet Checksum: 0xc9f9 [correct]

实例标志号：00

Instance ID: 0 (IPv6 unicast AF)

**Hello报文 OSPF Hello Packet**

接口标志符：00 00 09 8c

Interface ID: 2444

路由器优先级：01

Router Priority: 1

选项：00 00 13

Options: 0x000013 (R, E, V6)

Hello间隔：00 0a

Hello Interval: 10 seconds

路由器死亡间隔：00 28

Router Dead Interval: 40 seconds

指定路由器：01 01 01 1a

Designated Router: 1.1.1.26

后备指定路由器：00 00 00 00

Backup Designated Router: 0.0.0.0

**OSPF协议的工作过程为：**

(1) OSPF路由器接口up，发送Hello包，（NBMA模式时将进入Attempt状态）。

(2) OSPF路由器接口收到Hello包，检查Hello中携带的参数，如果匹配，进入Init状态；并将该Hello包的发送者的Router ID，添加到Hello包（自己将要从该接口发送出去的Hello包）的邻居列表中。

(3) OSPF路由器接口收到邻居列表中含有自己Router ID的Hello包，进入Two-way状态，形成OSPF邻居关系，并把该路由器的Router ID添加到自己的OSPF邻居表中。

(4) 在进入Two-way状态后，广播、非广播网络类型的链路，在DR选举等待时间内进行DR选举。点对点没有这个过程。

(5) 在DR选举完成或跳过DR选举后，建立OSPF邻接关系，进入exstart（准启动）状态；并通过交换DBD交换主从路由器，由主路由器定义DBD序列号，Router ID大的为主路由器。目的是为了解决DBD自身的可靠性。

(6) 主从路由器选举完成后，进入Exchange（交换）状态，通过交换携带lsa头部信息的DBD包描述各自的LSDB。

(7) 进入Loading状态，对链路状态数据库和收到的DBD的LSA头部进行比较，发现自己数据库中没有的LSA就发送LSR，向邻居请求该LSA；邻居收到LSR后，回应LSU；收到邻居发来的LSU，存储这些LSA到自己的链路状态数据库，并发送LSAck确认。

(8) LSA交换完成后，进入FULL状态，同一个区域内所有OSPF路由器都拥有相同链路状态数据库。

(9) 定期发送Hello包，维护邻居关系。

分析过程中发现由于器材关系只能获取到OSPF hello报文，且该hello报文为ipv6的OSPF报文（即OSPF v3）相对于书上的OSPF v2报文有一些区别：如PSPF v3报文头中不包含认证信息、数据包结构不同等，分析其报文格式需要注意。