RIP 路由协议

RIP（Routing Information Protocol ）路由信息协议

RIP 知识点

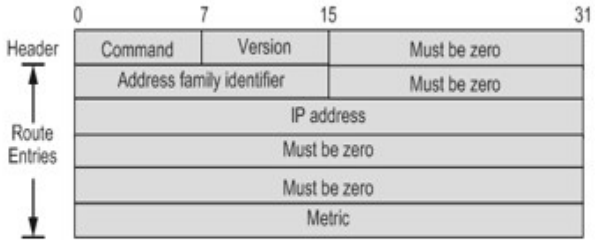
RIP 基本配置，RIP 两种报文 ，RIPv1 与 RIPv2 的区别，配置 RIP 的版本兼容及计时器，RIPv2 next-hop 的作用，RIPv2 接口认证，路由聚合，RIP 抑制接口及单播更新， RIP 不连续子网，RIP 路由附加度量值，RIP 路由引入，下放默认路由，Replay-protect（重放保护），filter-policy

RIP 每个报文只有承载 25 个路由条目

I. RIP是Routing Information Protocol（路由信息协议）的简称。
II. RIP是一种基于距离矢量（Distance-Vector）算法、简单的内部网关协议。
III. RIP主要应用于规模较小的、可靠性要求较低的网络。对于环境复杂的大型网络，一般不使用RIP协议。

RIPv1

RIPv1报文结构



RIPv1特点：

- 有类别路由协议
- 广播更新
- 基于UDP，端口号为520

RIPv1 报文结构

- RIP 每条消息包含两个部分，分别为 Header 和 Route Entries。其中 Header 包含 Command 和 Version。Route Entries 最多包含 25 个路由条目，每个路由条目包含 Address Family Identity、路由可达的 IP 地址和跳数。
- 报文格式各个字段解释如下：

  Command：取值 1 或 2，当取值为 1 时表示该消息为请求消息；当取值为 2 时表示该消息为响应消息。

  Version：当取值为 1 时表示该消息为 RIPv1 消息；当取值为 2 时表示该消息为 RIPv2 消息。

  Address Family Identity：对于 IPv4 协议，该字段取值为 2。当该消息是对整张路由表的请求消息时，该字段取值为 0。

  IP Address：该字段表示路由的目的地址。这一项可以是网络地址、主机地址。

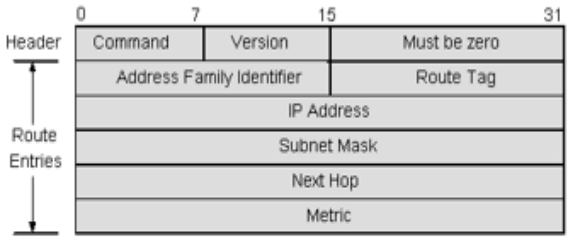
  Metric：该字段是指 RIP 中的跳数。虽然该字段取值范围为 0-2^32，但是在 RIP 中，该字段的取值范围为 1-16。

RIPv1 特点

- RIP 是一个基于 UDP 的路由协议，并且 RIPv1 的数据包不能超过 512 字节（RIP 报文头部占用 4 个字节,而每个路由条目占用 20 个八位组字节。因此,RIP 消息最大为 4+(25*20)=504 个字节,再加上 8 个字节的 UDP 头部,所以 RIP 数据报的大小(不含 IP 包的头部)最大可达 512 个字节。 ）。RIPv1 的协议报文中没有携带掩码信息，所以 RIPv1 在处理数据包时会根据主类网段掩码或者接口地址掩码处理数据包。因此 RIPv1 无法支持路由聚合，也不支持不连续子网。RIPv1 的协议报文中没有验证字段，所以 RIPv1 也不支持验证。

RIPv2

RIPv2 报文结构



RIPv2特点

- 无类别路由协议
- 组播更新，组播地址224.0.0.9
- 基于UDP，端口号为520
- 支持外部路由Tag；支持路由聚合和CIDR；支持指定下一跳；支持认证

问题：为何RIPv2报文没有认证字段？

RIPv2 报文结构

- RIPv2 的报文格式的基本结构和 RIPv1 相同。RIPv2 使用了 RIPv1 中部分未用字段以提供扩展功能。
- 报文格式部分字段解释如下：

Route Tag：用于标记外部路由或者路由引入到 RIPv2 协议中的路由。

Subnet Mask：用来标识使用 IPv4 地址的网络和子网部分。

Next Hop：表示比通告路由器地址更好的下一跳地址。如果该字段为 0.0.0.0，则说明通告路由器地址为最优下一跳地址。

- 当 RIPv2 配置认证时，RIPv2 会对报文第一条 Route Entries 进行修改。具体修改如下：

Address Family Identity 字段改为 0XFFFF。

Route Tag 字段改为 Authentication Type 字段。

IP Address、Subnet Mask、Next Hop 和 Metric 会变为口令字段。

RIPv2 相较 RIPv1 的改进包括如下几点：

- 支持外部路由标记（Route Tag），可以在路由策略中根据 Tag 对路由进行灵活的控制。

实际上不同 RIP 进程间相互引入路由也可以使用 Tag。

- 报文中携带掩码信息，支持路由聚合和 CIDR。
- 支持指定下一跳，在广播网上可以选择到最优下一跳地址。
- 支持以组播方式发送更新报文，只有运行 RIPv2 的设备才能收到协议报文，减少资源消耗。
- 支持对协议报文进行验证，增强安全性。

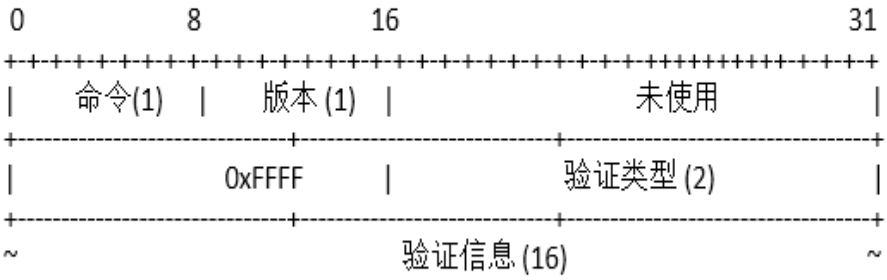
在多于两台设备组建的广播网络环境中，Next Hop 字段会发生变化，从而使路径最优。

MD5 认证实际上是把路由表项和共享密钥进行与运算，然后

路由器将运行运算结果和路由条目发送给对端邻居。

RIPv2

RIPv2 携带验证的报文结构



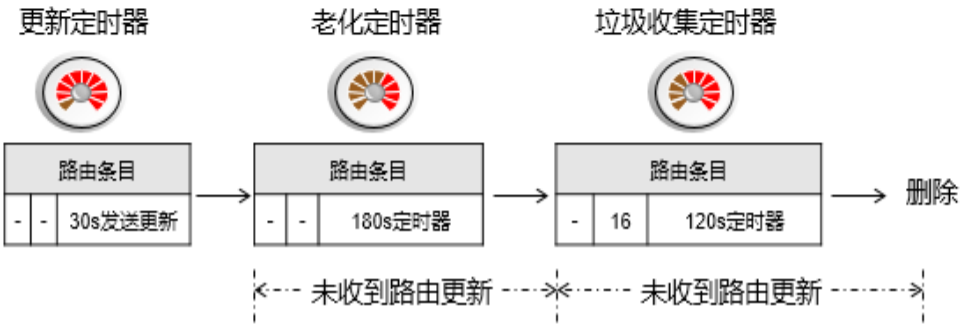
当配置了验证，一个RIP报文最多只能承载24条路由信息

定时器

RIP主要使用三个定时器

- 更新定时器
- 老化定时器
- 垃圾收集定时器

三个定时器之间的关系



RIP 主要使用三个定时器

- 更新定时器：它定时触发更新报文的发送，更新周期默认为 30 秒。
- 老化定时器：RIP 设备如果在老化时间内没有收到邻居发来的路由更新报文，则认为该路由不可达。老化定时器超时后，该路由条目设置为 16。
- 垃圾收集定时器：如果在垃圾收集时间内（默认为更新定时器的 4 倍，即 120 秒），不可达路由没有收到来自同一邻居的更新，则该路由将被从路由表中彻底删除。

三个定时器之间的关系

- RIP 的更新信息发布是由更新定时器控制的，默认为每 30 秒发送一次。
- 每一条路由表项对应两个定时器：老化定时器和垃圾收集定时器。当学到一条路由并添加到路由表中时，老化定时器启动。如果老化定时器超时，设备仍没有收邻居发来的更新报文，则把该路由的度量值置为 16（表示路由不可达），并启动垃圾收集定时器。如果垃圾收集定时器超时，设备仍然没有收到更新报文，则在路由表中删除该条目。

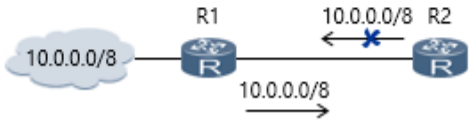
注意事项

- 如果在没有触发更新的前提下，一个路由表项最多需要 300 秒才能被删除（老化时间+垃圾收集时间）。
- 如果存在触发更新，那么一个路由条目最多需要 120 秒才能被删除（即为老化时间）。

水平分割

水平分割

- 水平分割指的是RIP从某个接口学到的路由，不会从该接口再发回给邻居设备。在帧中继和X.25等NBMA网络中，水平分割功能缺省为禁止状态。



水平分割

- RIP 采用水平分割不但减少了带宽消耗，还可以防止路由环路。

实现情况

- 如拓扑所示，R2 从某一接口学习到路由 10.0.0.0/8，不会再通过该接口发送回给 R1。如果没有水平分割，R2 将从 R1 收到的 10.0.0.0/8 的路由在发送会给 R1，那么 R1 会将该路由再次发送给 R2，这样该路由条目 10.0.0.0/8 就会在 R1 和 R2 之间不停的转发直至度量值到达 16。

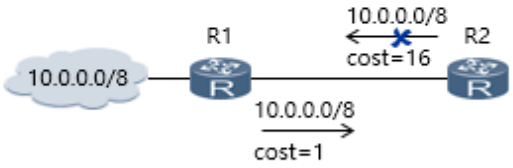
特殊情况

- 在 NMBA 网络中，水平分割缺省是禁用的。

毒性逆转

毒性逆转

- 毒性逆转指的是RIP从某个接口学到路由后，将该路由的开销设置为16（即指明该路由不可达），并从原接口发回邻居设备。



如果同时配置了毒性逆转和水平分割，则只使用毒性逆转功能。

毒性逆转的作用

- 利用毒性逆转，可以清除对方路由表中的无用路由。

实现情况

- 配置毒性逆转后，R2 在接收到从 R1 发来的路由 10.0.0.0/8 后，向 R1 发送一个这条路由不可达的消息（将该路由的开销设置为 16），这样 R1 就不会再利用从 R2 学到的路由 10.0.0.0/8，因此就可以避免路由环路的产生。

现实情况

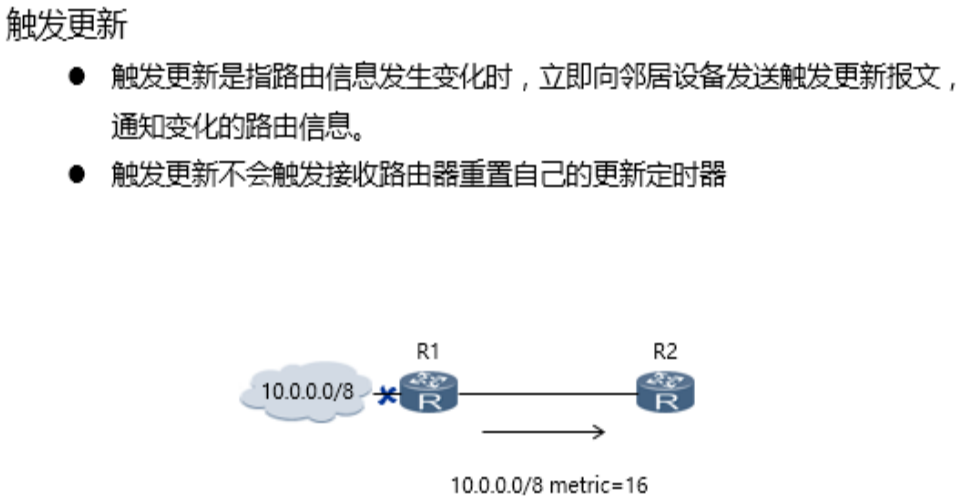
- 缺省情况下不使能毒性逆转。一般情况下，在华为设备中均使能水平分割（除 NBMA 网络外）而禁用毒性逆转。

水平分割和毒性逆转的差别

- 水平分割和毒性逆转都是为了防止 RIP 中的路由环路而设计的，但是水平分割是不将收到路由条目再按“原路返回”来避免环路，而毒性逆转遵循“坏消息比没消息好”的原则，即将路由条目按“原路返回”，但是该路由条目被标记为不可达（度

量值为 16）。

触发更新



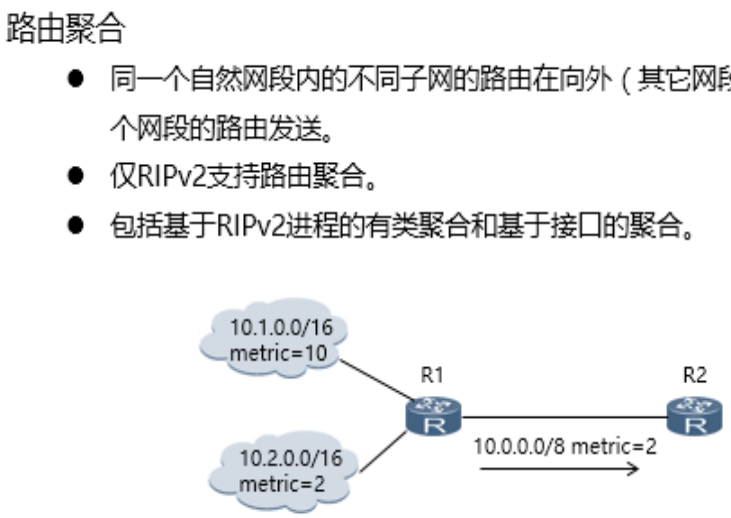
触发更新

- 触发更新缩短了收敛时间，触发更新可以缩短网络收敛时间，在路由表项变化时立即向其他设备广播该信息，而不必等待定时更新。如果没有触发更新，缺省情况下，失效的路由条目会在路由表停留最多 300 秒（老化定时器+垃圾收集定时器）
- 下一跳地址不可达，不会触发触发更新。

实现过程

- 如果 R1 发现网络故障之后，不再等待更新周期到来，就立即发送路由更新信息给路由器 R2，使路由器 B 的路由表及时更新，则可以避免产生上述问题。

路由聚合



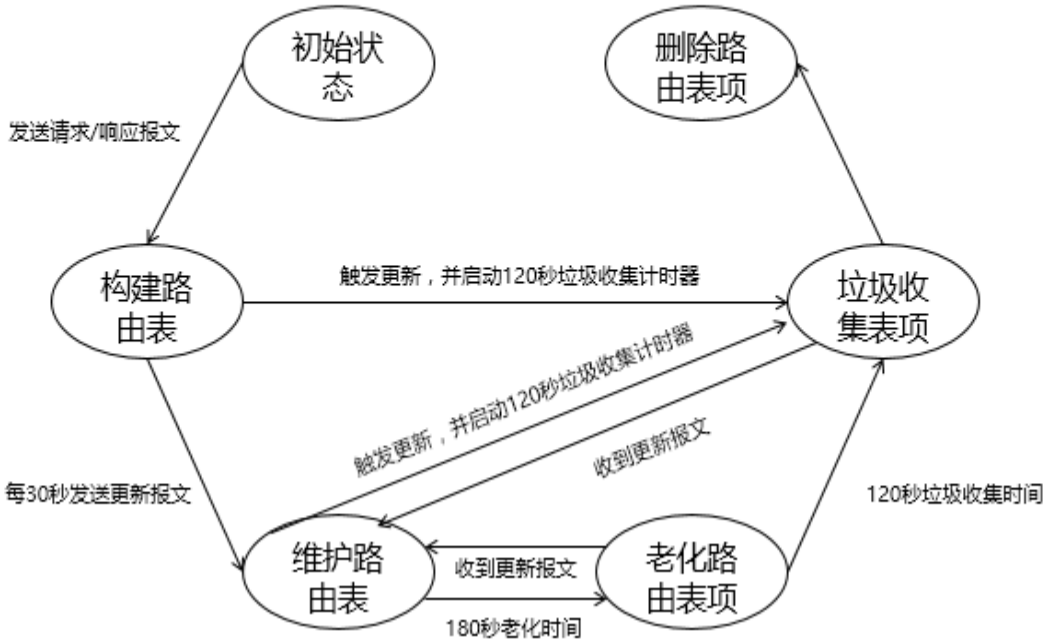
路由聚合

- RIPv2 支持路由聚合，因为 RIPv2 报文携带掩码位，所以支持子网划分。在 RIPv2 中进行路由聚合可提高大型网络的可扩展性和效率，缩减路由表。
- 基于 RIPv2 进程的有类聚合即实现自动聚合。
- 基于接口的聚合即实现手动聚合。
- 如果被聚合路由携带了 Tag，那么路由聚合发生之后，Tag 信息将被清除。

聚合案例

- 对于 10.1.0.0/16（metric=10）和 10.2.0.0/16（metric=2）这两条路由，会聚合成自然网段路由 10.0.0.0/8（metric=2）。

工作过程分析



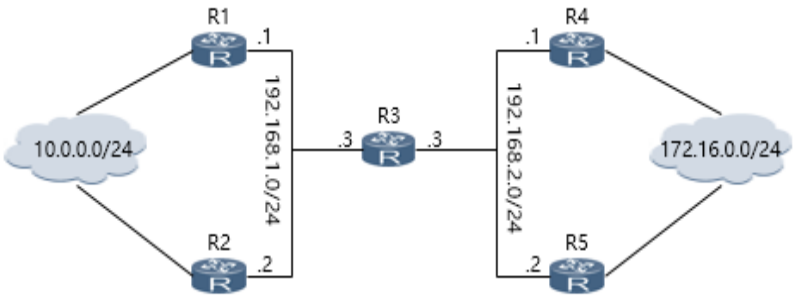
过程分析：

- 初始状态:路由器开启 RIP 进程，宣告相应接口，则设备就会从相关接口发送和接收 RIP 报文。
- 构建路由表：路由器依据收到的 RIP 报文构建自己的路由表项。
- 维护路由表：路由器每个 30 秒发送更新报文以维护自己的路由表项。
- 老化路由表项：路由器为将自己构建的路由表项启动 180 秒的定时器。180 秒内，如果路由器收到更新报文，则重置自己的更新定时器和老化定时器。
- 垃圾收集表项：如果 180 秒过后，路由器没有收到相应路由表项的更新，则启动时长为 120 秒的垃圾收集定时器，同时将该路由表象的度量置位 16。
- 删除路由表项：如果 120 秒之后，路由器仍然没有收到相应路由表象的更新，则路由器将该表相删除。

配置RIP的路由属性

假如你是公司A网络管理员，公司A网络如下图所示。现公司A要求：

- R3优选R2到达网络10.0.0.0/24，需在R1上进行配置；
- R3上到达网络172.16.0.0/24的度量值调整为3，需在R3上操作。




```
[R3]display ip routing-table
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
        10.0.0.0/24 RIP     100  1           D   192.168.1.2     GigabitEthernet0/0/0
                    RIP     100  1           D   192.168.1.1     GigabitEthernet0/0/0
      172.16.0.0/24 RIP     100  1           D   192.168.2.2     GigabitEthernet0/0/1
                    RIP     100  1           D   192.168.2.1     GigabitEthernet0/0/1
```

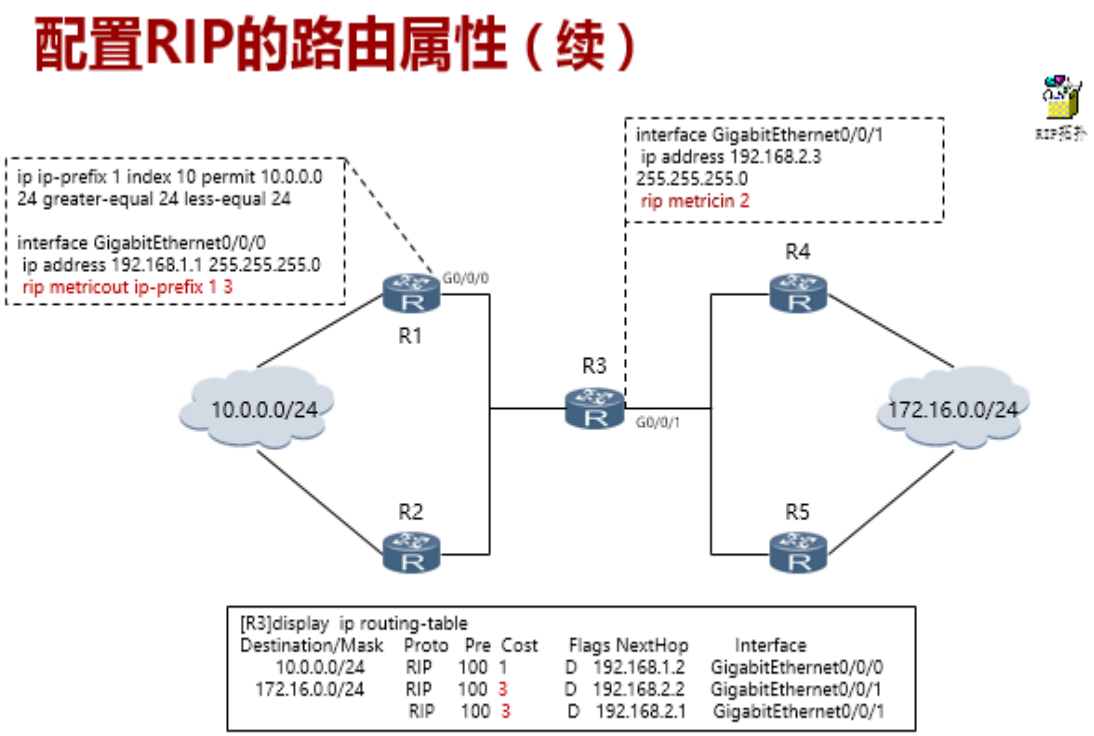
案例描述

- 本案例中，R1、R2 和 R3 所在网段为 192.168.1.0/24；R3、R4 和 R5 所在网段为 192.168.2.0/24。所有路由器均运行 RIPv2，通告互联接口地址。对案例分析，可以得出要想左右 R3 的路由选择，一般情况下，我们可以通过修改度量值来实现。

部分说明

- 注意该路由表项为缩减的路由表项，只是摘取了相关信息。路由表象中的 Flags 字段 R 表示该路由是迭代路由，D 表示该路由下发到 FIB 表。
- 路由的迭代过程就是进行路由替换。在某一台设备上当去往目的地址的 “下一跳”不能直接匹配到该设备的出接口时，可以通过一次或几次路由替换找到转发的出接口，该路由则成为迭代路由。
- FIB 即路由转发表，由路由表生成，可以通过命令 displa

y fib 命令用来查看转发信息表。



运用rip metricin/metricout会影响其他设备的路由选择！

命令含义

- **rip metricin** 用于在接收到路由后，给其增加一个附加度量值，再加入路由表中，使得路由表中的度量值发生变化。运行该命令会影响到本地设备和其他设备的路由选择。
- **rip metricout** 用于自身路由的发布，发布时增加一个附加的度量值，但路由表中的度量值不会发生变化。运行该命令不会影响本地设备的路由选择，但是会影响其他设备的路由选择。

具体用法

- **rip metricin/metricout** 均为接口视图命令。

参数意义

- **rip metricout** { *value* | { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } *value1* }，设置接口在发布路由

时增加的度量值。

value：对发送的路由增加的度量值。取值范围是1～15。缺省值为1。

acl-number：指定基本ACL的编号。取值范围是2000～2999。

acl-name *acl-name*：指定访问控制列表名称。区分大小写。

ip-prefix *ip-prefix-name*：指定IP地址前缀列表的名称。该名称必须唯一。

Value1：对通过ACL或**ip-prefix**方式过滤的路由增加度量值。

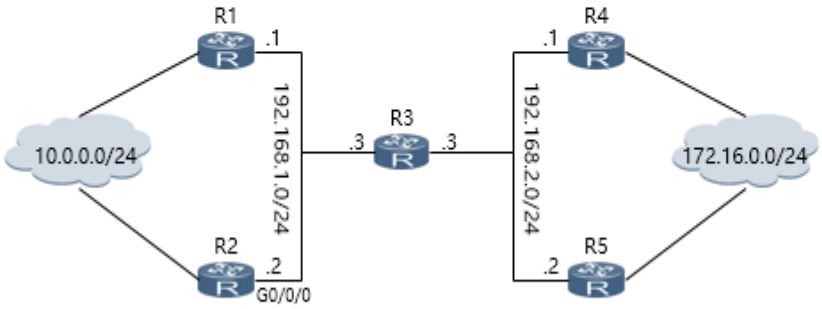
注意事项

- 当用ACL或ip-prefix方式来设置接口发送RIP路由增加的度量值时，指定*value1*为通过过滤策略的RIP路由增加的度量值，没有通过过滤的RIP路由增加的度量值为1。
- 运用rip metricin/metricout会影响其他设备的路由选择。

控制RIP路由信息的发布

下面是公司A的网络，假设公司A邀请你进行网络改造，现公司A对网络的要求如下：

- R4的所有接口只能接收更新，需在R4上进行配置；
- R2的接口G0/0/0不能发送RIP报文，需在R2上操作。

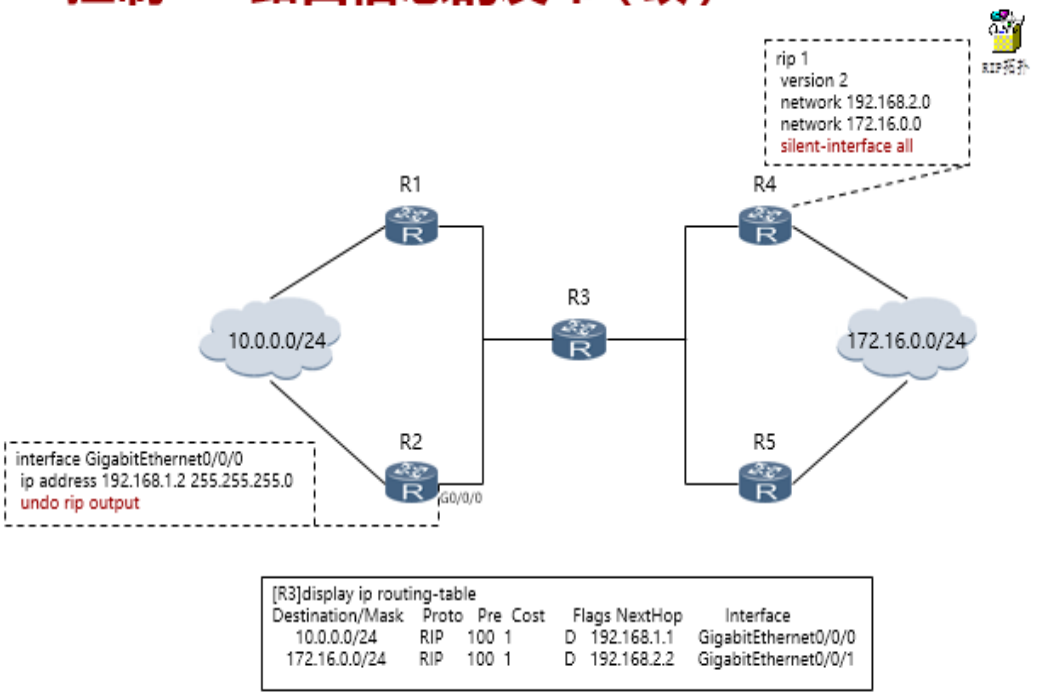



```
[R3]display ip routing-table
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
      10.0.0.0/24   RIP     100  1           D   192.168.1.2     GigabitEthernet0/0/0
                    RIP     100  1           D   192.168.1.1     GigabitEthernet0/0/0
    172.16.0.0/24   RIP     100  1           D   192.168.2.2     GigabitEthernet0/0/1
                    RIP     100  1           D   192.168.2.1     GigabitEthernet0/0/1
```

案例描述

- 该案例拓扑和之前的拓扑一致。为了实现公司 A 的需求，即不发送或者更更新，我们一般情况通过配置抑制接口或 undo rip input/output 来实现。

控制RIP路由信息的发布（续）



命令含义

- **silent-interface** 命令用来抑制接口，使其只接收报文，用来更新自己的路由表，而不发送 RIP 报文。如果一个接口被抑制，该接口所在网段的直连路由仍然可以发布给其它接口。该命令与 **peer** (RIP)命令协同使用，可向指定设备发布路由。
- **undo rip output/input** 命令用来允许接口发送/接收 RIP 报文。

具体用法

- **silent-interface** 为 RIP 视图命令。
- **undo rip output/input** 为接口视图命令。

参数意义

- **silent-interface** { **all** | *interface-type interface-number* }

  all：抑制所有接口。

注意事项

- 当配置所有接口为抑制状态后，不能再激活其中的一个接口，即 silent-interface all 命令的优先级高。本案例中由于 R4 抑制了所有接口，所以 R4 不能激活本身的其他接口。

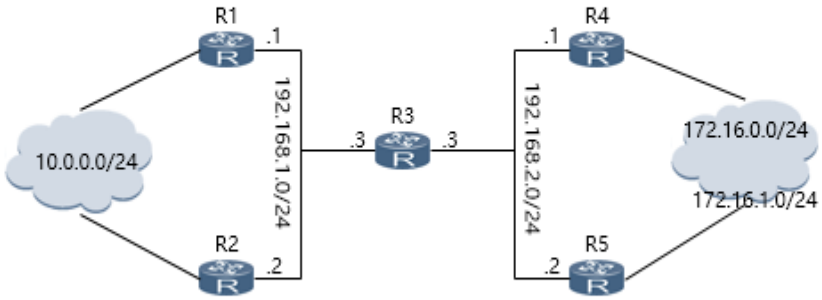
实验现象

- 我们通过查看 R3 的路由表项可以看出，R3 由于不能通过 R4 收到关于网络 172.16.0.0/24 的更新，所以只能选用从 R5 收到的关于网络 172.16.0.0/24 的更新；同时，由于 R3 不能收到 R2 收到关于网络 10.0.0.0/24 的更新，只能选用从 R1 收到关于网络 10.0.0.0/24 的更新。

控制RIP路由信息的接收

公司A网络拓扑如图所示。现公司A对网络具体需求如下：

- R3不能接收R4发送的路由，在R3上进行操作。

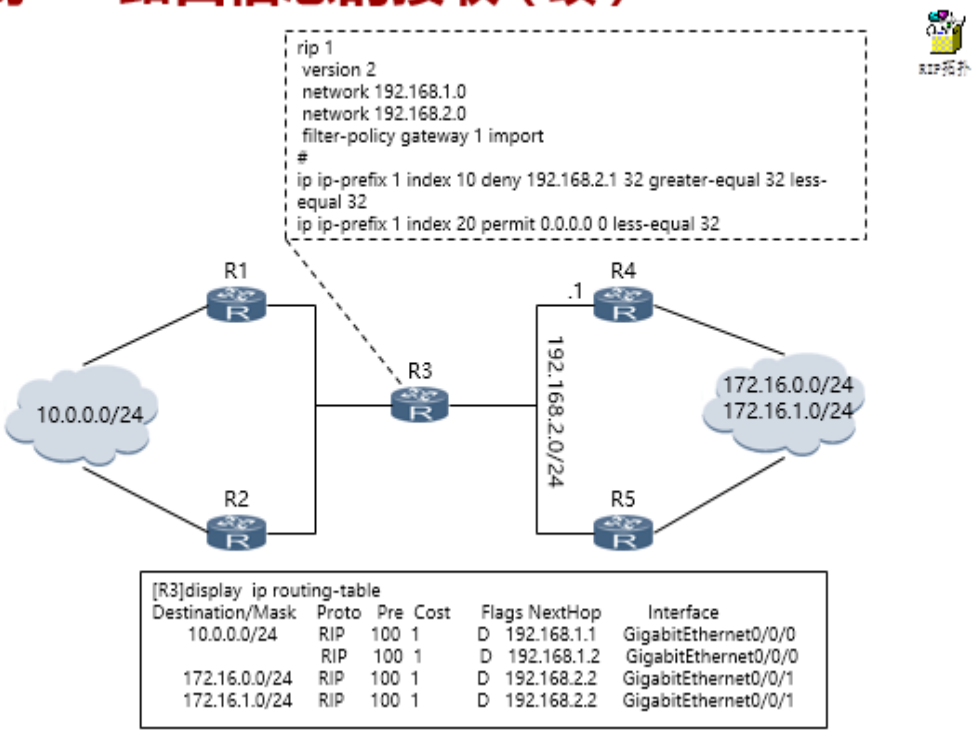



```
[R3]display ip routing-table
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
      10.0.0.0/24   RIP     100  1           D   192.168.1.1     GigabitEthernet0/0/0
                    RIP     100  1           D   192.168.1.2     GigabitEthernet0/0/0
    172.16.0.0/24   RIP     100  1           D   192.168.2.2     GigabitEthernet0/0/1
                    RIP     100  1           D   192.168.2.1     GigabitEthernet0/0/1
    172.16.1.0/24   RIP     100  1           D   192.168.2.2     GigabitEthernet0/0/1
                    RIP     100  1           D   192.168.2.1     GigabitEthernet0/0/1
```

案例描述

- 该案例拓扑和之前的拓扑一致。为了实现公司 A 的需求，即接收特定邻居发送的路由，我们可以考虑命令 **filter-policy gateway**。

控制RIP路由信息的接收（续）



命令含义

- 命令 **filter-policy** { *acl-number* | **acl-name** *acl-name* } **import**，基于 ACL 过滤学到的路由信息。
- 命令 **filter-policy gateway** *ip-prefix-name* **import**，基于目的地址前缀过滤邻居发布的路由信息。

具体用法

- 命令 **filter-policy** { *acl-number* | **acl-name** *acl-name* } **import** 为 RIP 视图命令。
- 命令 **filter-policy gateway** *ip-prefix-name* **import** 为 RIP 视图命令

参数意义

- 命令 **filter-policy** { *acl-number* | **acl-name** *acl-name* } **import**

acl-number：用于过滤路由信息目的地址的基本

ACL 编号。

acl-name *acl-name*：指定访问控制列表名称。区分大小写，开头第一个字符必须是英文字母。

ip-prefix：使用 IP 地址前缀列表过滤路由。

ip-prefix-name：用于过滤路由信息目的地址的地址前缀列表名。

- 命令 **filter-policy gateway** *ip-prefix-name* **import**

gateway：基于发布网关过滤路由。

ip-prefix-name：用于过滤路由信息目的地址的地址前缀列表名。

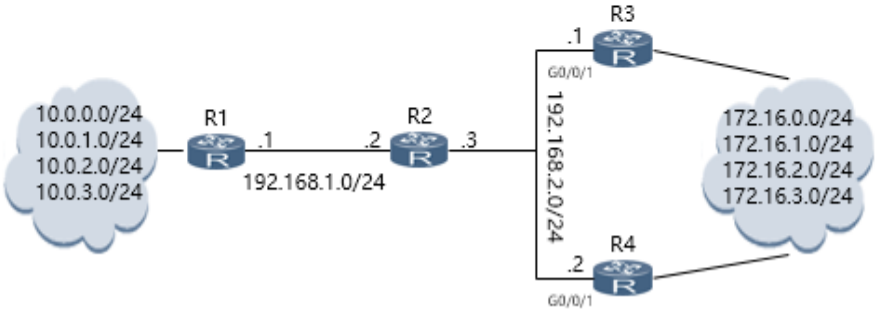
实验现象

- 我们通过命令 filter-policy gateway 来指定邻居过滤。这里我们在 R3 上指定不从 R4 接收路由信息。

配置RIPv2特性

现公司A修改了自己的网络，并提出了一些需求：

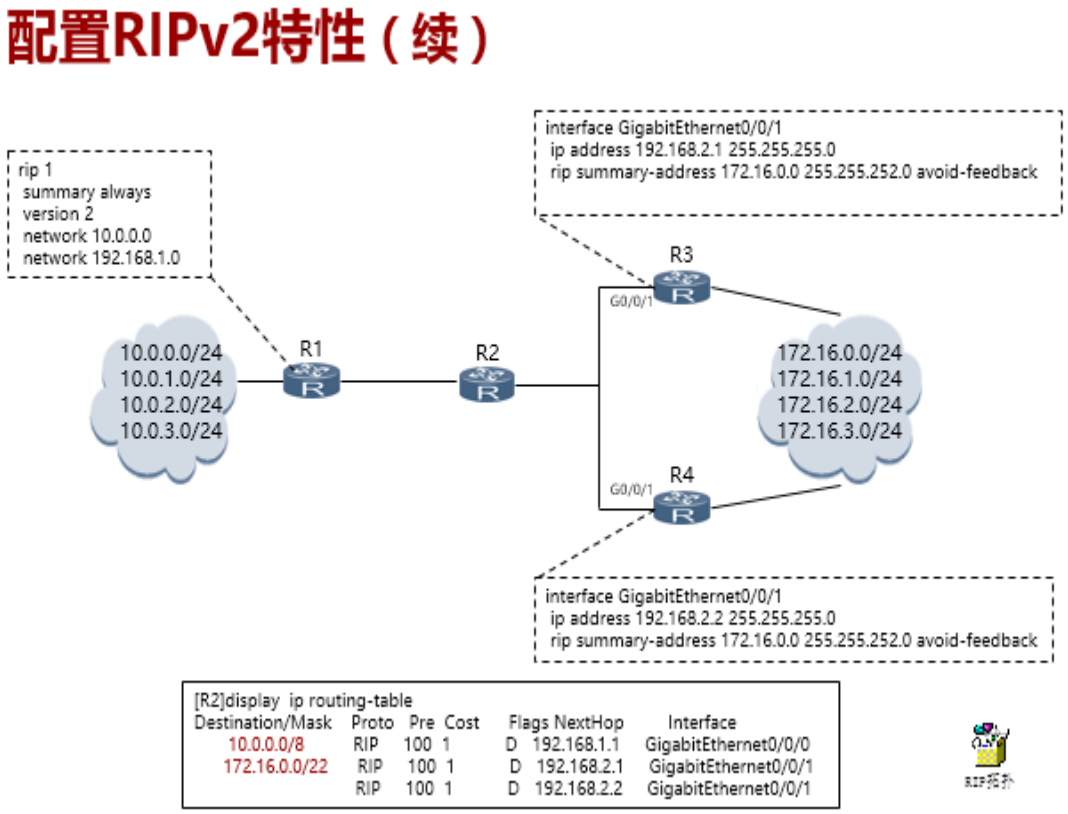
- 对网络10.0.X.0/24的网络进行有类聚合，在R1上操作；
- 对网络172.16.X.0/24的网络进行最优聚合，R3和R4禁止从接口G0/0/1学习到该聚合路由，在R3和R4上操作。



案例描述

- 该案例拓扑和之前的拓扑一致。为减少路由条目，公司

A 决定进行路由聚合配置。RIPv2 聚合分为两类，一类是基于主类网络的自动聚合，一类是手工聚合。我们可以在 R1 采用手工聚合的方法，在 R3 和 R4 上使用自动聚合的方法。



命令含义

- **summary [always]**：在未使能水平分割的基础上使能 RIPv2 自动路由聚合，则不用配置参数 **always**；不论水平分割是否使能，都使能 RIPv2 自动路由聚合，则需要配置参数 **always**。如果配置了水平分割或毒性反转，有类聚合将失效。因此在向自然网段边界外发送聚合路由时，相关视图下的水平分割和毒性反转功能都应关闭。
- **rip summary-address** *ip-address mask* **[avoid-feedback]**：用来设置一个 RIP 路由器发布一个聚合的本地 IP 地址。通过指定 **avoid-feedback** 关键字，本接口将不再学习到和已发布的聚合 IP 地址相同的聚合路由，从而可以起到防止产生路由环路的作用。

具体用法

- 命令 **summary** [**always**] 为 RIP 视图命令。
- **rip summary-address** *ip-address mask* [**avoid-feedback**]接口视图命令。

参数意义

- **summary [always]**

  always：如果不配置 **always** 参数，在配置水平分割或毒性反转的情况下，有类聚合将失效。因此在向自然网段边界外发送聚合路由时，相关视图下的水平分割和毒性反转功能都应关闭。
- **rip summary-address** *ip-address mask* **[avoid-feedback]接口视图命令**

  ip-prefix-name：需要聚合的网络 IP 地址。

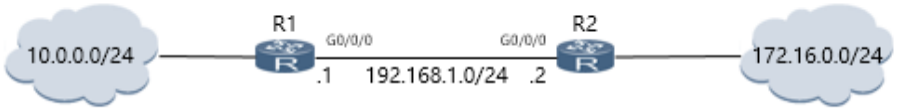
  mask：网络掩码。

  avoid-feedback：禁止从此接口学习到相同的聚合路由。

调整优化RIP网络

现公司A需要对网络进行优化，需求如下：

- 调整Update和Age定时器分别为10秒和60秒，Garbage-collect请自行决定；
- RIP路由信息在接口up/down之后，容易产生信息不同步的情况，请使用相关命令解决该问题。



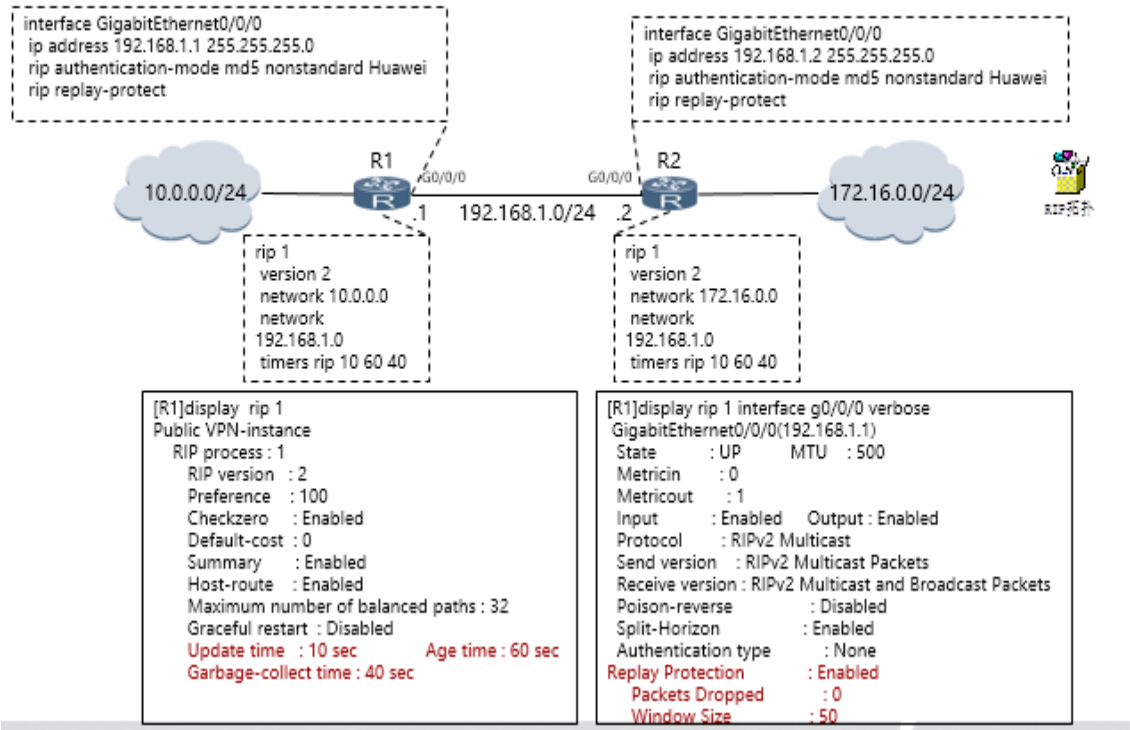

```
[R1]display  rip 1
Public VPN-instance
   RIP process : 1
     RIP version   : 2
     Preference    : 100
     Checkzero     : Enabled
     Default-cost  : 0
     Summary       : Enabled
     Host-route    : Enabled
     Maximum number of balanced paths : 32
     Update time   : 30 sec          Age time : 180 sec
     Garbage-collect time : 120 sec
```

```
[R1]display rip 1 interface g0/0/0 verbose
 GigabitEthernet0/0/0(192.168.1.1)
  State          : UP          MTU    : 500
  Metricin       : 0
  Metricout      : 1
  Input          : Enabled     Output : Enabled
  Protocol       : RIPv2 Multicast
  Send version   : RIPv2 Multicast Packets
  Receive version : RIPv2 Multicast and Broadcast Packets
  Poison-reverse              : Disabled
  Split-Horizon               : Enabled
  Authentication type         : None
  Replay Protection           : Disabled
```

案例描述

- 本案例中，R1 和 R2 通过网段 192.168.1.0/24 进行互联。R1 左侧连接网段 10.0.0.0/24，R2 右侧连接网段 172.16.0.0/24。全网运行基本的 RIPv2，并通过各自所在的网段。仅给出 R1 的 display 信息，且该信息只是截取与本案例相关的信息。

调整优化RIP网络（续）



命令含义：

- 命令 **timers rip** *update age garbage-collect*：命令用来调整定时器。
- 命令 **rip authentication-mode md5 nonstandard** *password-key key-id*，配置 RIP-2 使用 MD5 密文的验证方式，验证报文使用非标准报文格式。**nonstandard** 指定 MD5 密文验证报文使用非标准报文格式（IETF 标准）。
- 命令 **rip replay-protect** [*window-range*]，使能 replay-protect 功能。*window-range* 指定面向连接的收发缓冲区大小，缺省 *window-range* 为 50。

具体用法

- 命令 **timers rip** *update age garbage-collect* 为 RIP 视图命令。
- 命令 **rip authentication-mode md5 nonstandard** *passwo*

rd-key key-id 为接口视图命令

- 命令 **rip replay-protect** [*window-range*]为接口视图命令。

参数意义

- 命令 **timers rip** *update age garbage-collect*

  update：路由更新报文的发送间隔。

  age：路由老化时间。

  garbage-collect：路由被从路由表中删除的时间（标准中定义的 garbage 收集时间）。

注意事

- 如果这三个定时器的值如果配置不当，会引起路由不稳定。它们的配置值关系是：update<age。例如，如果更新时间大于失效时间，那么在更新时间内，如果 RIP 路由发生变化，路由器将无法及时通知邻居。在实际应用中，Garbage-collect 定时器的超时时间并不是固定的，当 Update 定时器设为 30 秒时，Garbage-collect 定时器可能在 90 到 120 秒之间。这是因为：RIP 在将不可达路由从路由表中彻底删除前，将通过发送 4 次定时更新报文对外发布这条路由（发送时权值设为 16），从而使所有邻居了解这条路由已经处于不可达状态。由于路由变为不可达状态并不总是恰好在一个更新周期的开始，因此，Garbage-collect 定时器的实际时长是 Update 定时器的 3～4 倍。
- 假设运行 RIP 的接口状态变为 Down 之前发送的最后的 RIP 报文的 Identification（该字段为 IP 头部中的字段）为 X，该接口状态变为 Up 后，再次发送 RIP 报文的 Identification 会变为 0。如果对方没有收到这个 Identification 为 0 的 RIP 报文，那么后续的 RIP 报文都将被丢弃，直到收到 Identification 为 X＋1 的 RIP 报文。这样就会导致双方的 RIP 路由信息不同步、丢失。通过使能 Replay-protect 功能，可以得到接口 Down 之

前所发送 RIP 报文的 Identification，再次发送 RIP 报文的 Identification 会顺次加一，从而避免了上述情况的发生。

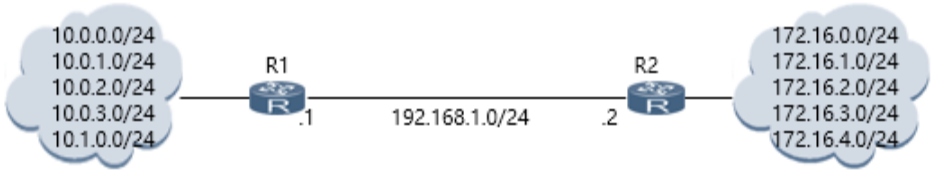
故障排除Tips

在进行故障排除时，需要考虑如下因素

- 确保清晰定义故障；
- 收集所有相关的现象、考虑各种潜在的可能；
- 定义一个计划，并执行它，观察执行的结果；
- 如果问题未解决，收集额外的现象采用其他计划。这时需要注意，你应该消除哪些因为执行计划带来的额外变化；
- 如果问题解决，记录下来你如何解决这个问题的。

RIP故障诊断

全网运行RIPv2之后，用户10.0.0.2发现不能访问服务器172.16.0.2。
你如何分析、解决此故障？



- 确认 ARP 是否正常
- 确认接口是否 up
- 检查接口是否在 RIP 中使能：使用命令 **display current-configuration configuration rip** 可以看到当前使能 RIP 的网段信息，检查接口是否在其中。**network** 命令使能的网络地址，必须是自然网段的地址。
- 检查对方发送版本号和本地接口接收的版本号是否匹配：

缺省情况下，接口只发送 RIPv1 报文，但可以接收 RIPv1 和 RIPv2 报文。当入接口与收到的 RIP 报文使用不同的版本号时，有可能造成 RIP 路由不能被正确的接收。

- 检查在 RIP 中是否配置了策略，过滤掉收到的 RIP 路由：如果被路由策略过滤掉，则需修改路由策略。
- RIP 使用的端口 520 是否被禁用
- 检查接口是否配置了 undo rip input/output 或者 rip metricin 设置度量值多大
- 检查接口是否配置了抑制接口
- 检查路由度量值是否大于 16
- 检查链路两端的接口认证方式是否匹配：如果报文认证失败，则需正确配置

正常工作分析

在故障排除之前，需要考虑正常通信的过程

用户10.0.0.2和用户172.16.0.2相互ping通的过程如下：

- 10.0.0.2主机配置了正确的IP地址、掩码和网关IP地址，
- 10.0.0.2发现目标地址与自己的IP在不同的网段
- 通过ARP获得网关10.0.0.1的MAC地址
- 10.0.0.2封装数据包成数据帧，发送给网关
- 网关R1查找路由，确认下一跳的IP地址，通过ARP查找下一跳的MAC地址
- 由于R1的入接口和出接口未配置访问控制信息，R1转发数据到R2
- R2查找路由表，确认目标网络与自己直连，通过ARP获取目标主机的MAC地址
- 封装数据，发送给目标主机，数据包返程过程略

故障排除流程

由于本次主讲RIP，非RIP部分，假设没有问题

- 检查接口是否在RIP中使能
- 检查对方发送版本号和本地接口接收的版本号是否匹配
- 检查在RIP中是否配置了策略，过滤掉收到的RIP路由：
- RIP使用的端口520是否被禁用
- 检查接口是否配置了undo rip input/output或者rip metricin设置度量值多大
- 检查接口是否配置了抑制接口
- 检查路由度量值是否大于16
- 检查链路两端的接口认证方式是否匹配：如果报文认证失败，则需正确配置

- 检查接口是否在 RIP 中使能：使用命令 **display current-configuration configuration rip** 可以看到当前使能 RIP 的网段信息，检查接口是否在其中。**network** 命令使能的网络地址，必须是自然网段的地址。
- 检查对方发送版本号和本地接口接收的版本号是否匹配：缺省情况下，接口只发送 RIPv1 报文，但可以接收 RIPv1 和 RIPv2 报文。当入接口与收到的 RIP 报文使用不同的版本号时，有可能造成 RIP 路由不能被正确的接收。
- 检查在 RIP 中是否配置了策略，过滤掉收到的 RIP 路由：如果被路由策略过滤掉，则需修改路由策略。
- RIP 使用的端口 520 是否被禁用
- 检查接口是否配置了 **undo rip input/output** 或者 **rip metricin** 设置度量值多大
- 检查接口是否配置了抑制接口
- 检查路由度量值是否大于 16
- 检查链路两端的接口认证方式是否匹配：如果报文认证失败，则需正确配置

案例1

公司B网络部分拓扑如下图所示。需要进行部分改造，且只能对R1进行操作，现提出需求如下：

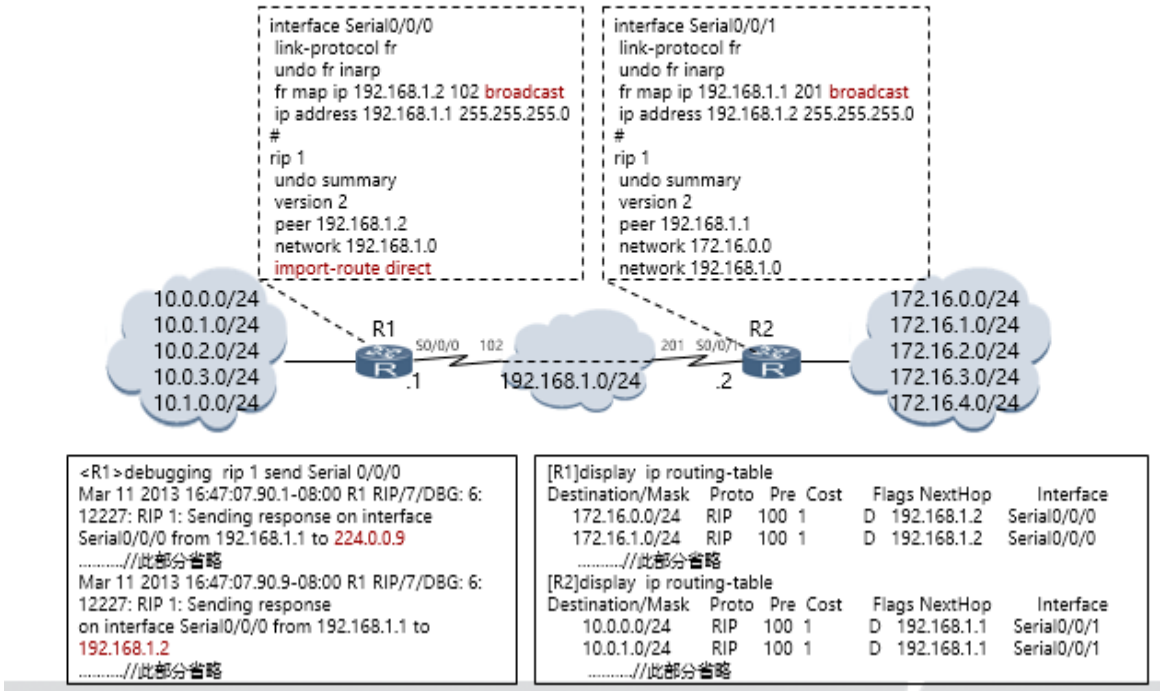
- 不能删除现有配置，可以添加必要配置；
- R1只有接口S0/0/0运行RIP，R1通过单播发送更新报文；
- R1只接收172.16.0.0/24、 172.16.1.0/24、 172.16.2.0/24和172.16.3.0/24这四条路由；
- R1已将网络10.X.X.0/24引入RIP，但是向R2仅发送一条10.0.0.0/16汇总路由，请用最少配置命令,确保该聚合不能再通过接口S0/0/0学到。

案例描述

- 本案例的拓扑中，路由器 R1 通过帧中继网络和 R2 相连。R1 左侧与网络 10.X.X.0/24 相连，R2 右侧与网络 172.16.X.0/24 相连。

案例1—预配

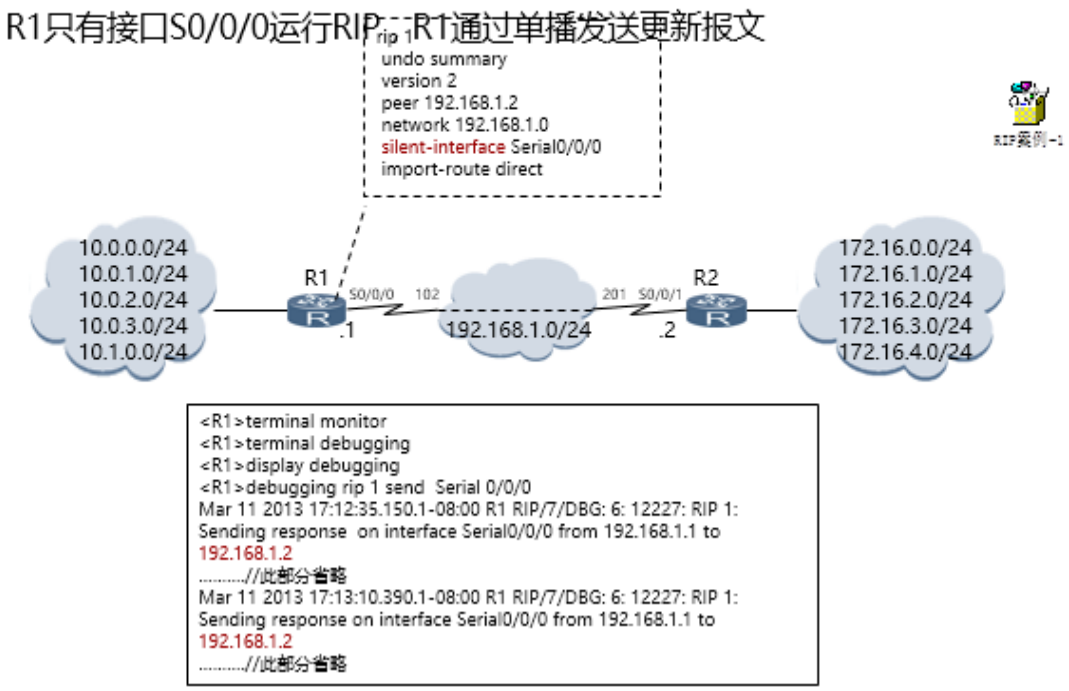
不能删除现有配置，可以添加必要配置



分析过程

- R1 和 R2 上的预配中，帧中继的配置是支持组播的。
- R1 向 R2 发送更新时组播和单播发送更新的，主要是由于 peer 命令即发送组播的更新，又发送单播的更新。
- R1 和 R2 能相互学到对方的路由。

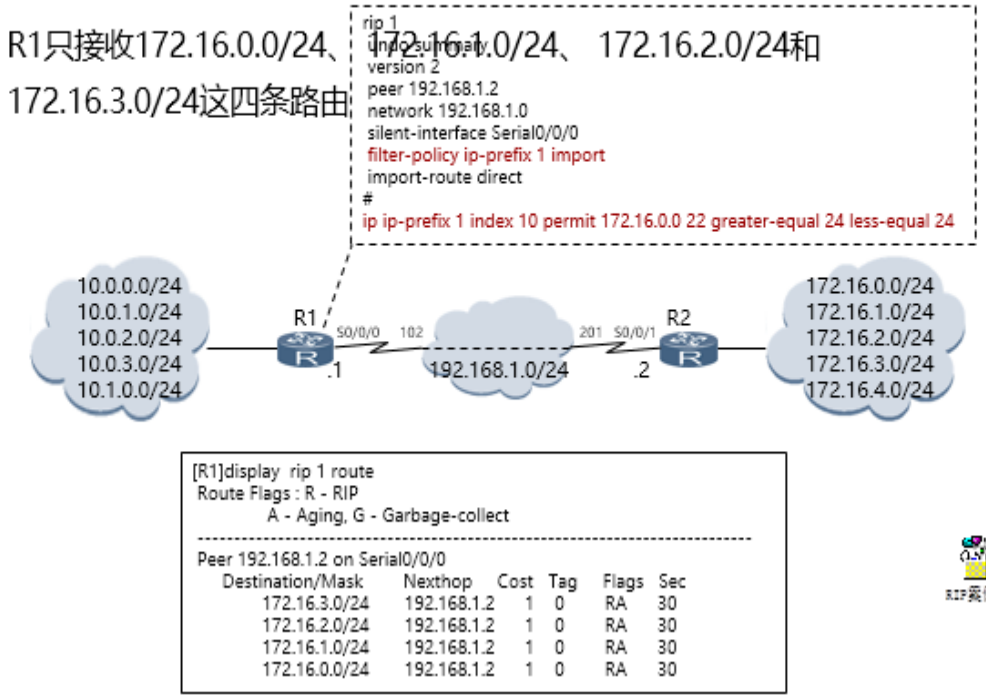
案例1—需求1



结果说明

- 通常情况下，peer 命令会造成对端同时收到同一报文的组播（或广播）和单播两种形式报文。因此建议在配置该命令的同时，将相关接口改为被动（silent）模式。这样，发送的报文只有单播报文。

案例1—需求2



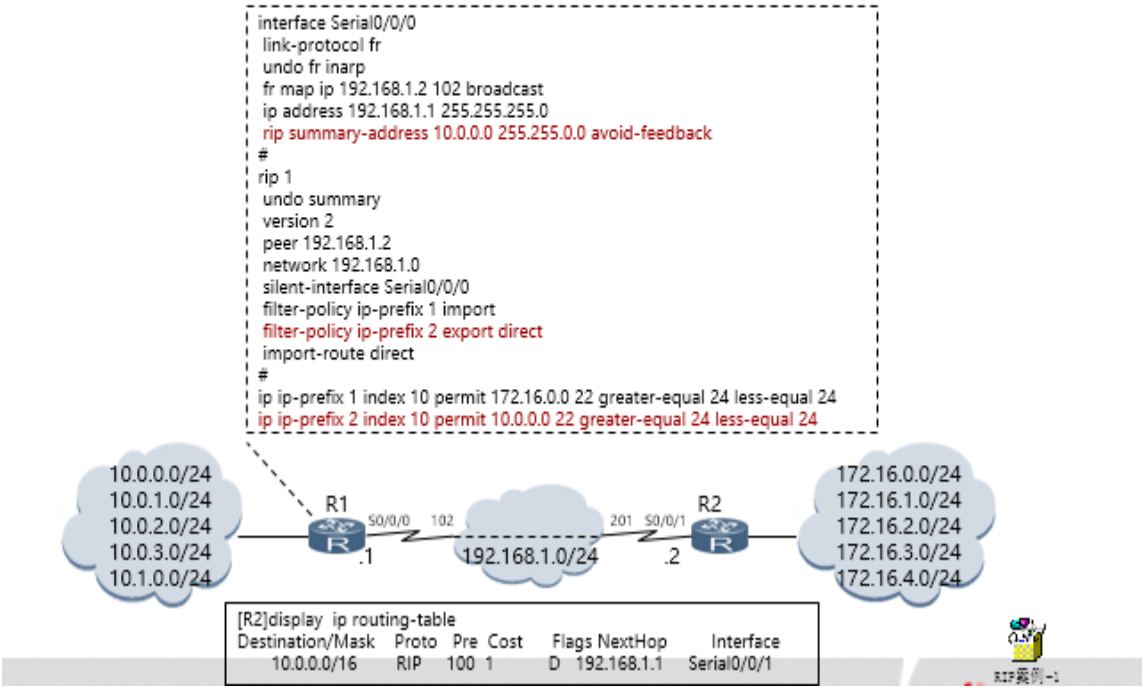

```
[R1]display  rip 1 route
 Route Flags : R - RIP
               A - Aging, G - Garbage-collect
------------------------------------------------------------------------------
Peer 192.168.1.2 on Serial0/0/0
     Destination/Mask    Nexthop      Cost   Tag    Flags  Sec
          172.16.3.0/24  192.168.1.2  1      0      RA     30
          172.16.2.0/24  192.168.1.2  1      0      RA     30
          172.16.1.0/24  192.168.1.2  1      0      RA     30
          172.16.0.0/24  192.168.1.2  1      0      RA     30
```

结果说明

- **display rip route** 命令用来显示所有从其它路由器学来的 RIP 路由信息，以及与每条路由相关的不同定时器的值。其中 Tag 区分内部 RIP 路由和外部路由的标识，Tag=0 表示该 RIP 路由为内部路由，Tag=1 表示该 RIP 路由为外部路由。Flags 为 RA 表示该 RIP 路由条目为激活路由，Flags 为 RG 表示该 RIP 路由条目为非激活路由，并且已经启动了垃圾超时定时器。

案例1—需求3

R1已将网络10.X.X.0/24引入RIP，但是向R2仅发送一条10.0.0.0/16汇总路由，请用最少配置命令,确保该聚合不能再通过接口S0/0/0学到。



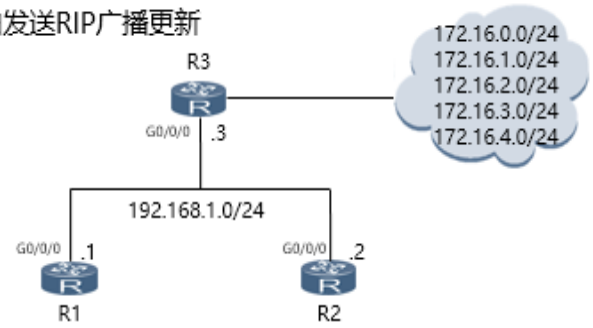
结果说明

- 通过指定 avoid-feedback 关键字，本接口将不再学习到和已发布的聚合 IP 地址相同的聚合路由，从而可以起到防止产生路由环路的作用。
- filter-policy export 命令用来配置全局、协议、接口的出口过滤策略，只有通过过滤的路由才能被加入其路由表中，并通过更新报文发布出去。

案例2

公司C网络运行RIPv2,拓扑如下图所示。现公司C对网络有具体需求，需求如下：

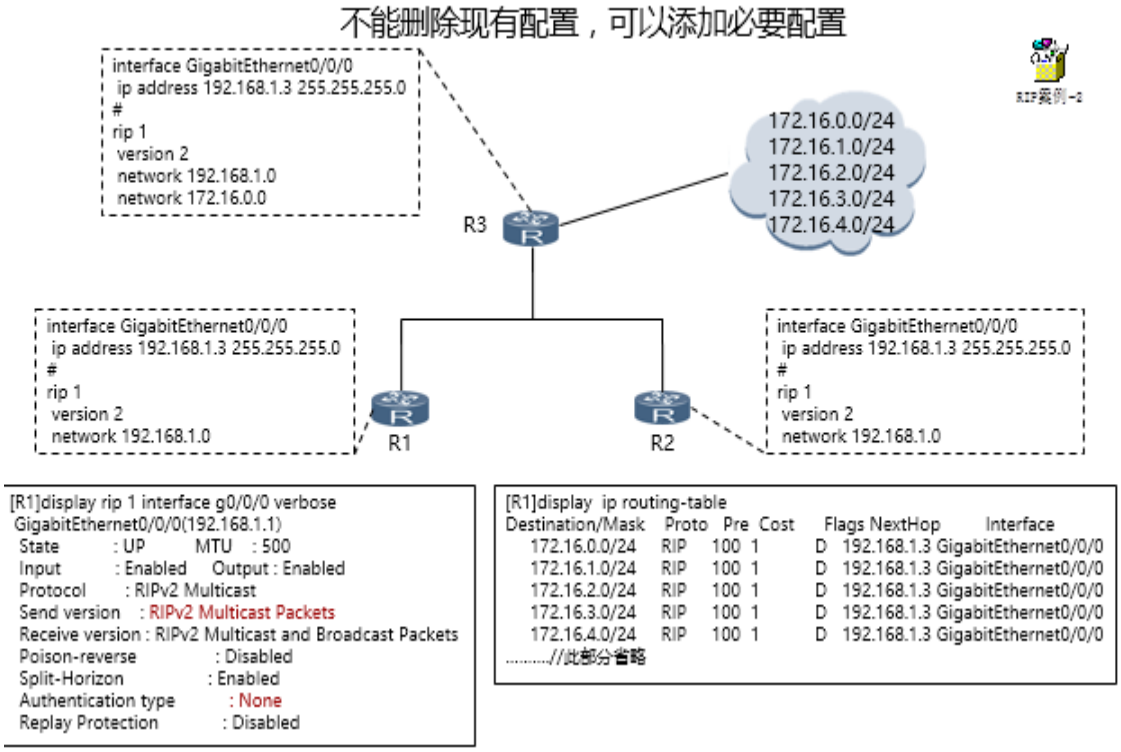
- 不能删除现有配置，可以添加必要配置；
- 要求全网配置较强的华为特有认证模式，密码为Huawei，以保证网络的安全；
- R1只接收172.16.X.0/24网段地址中第24位为1的网络，禁止使用前缀列表，且最少命令；
- 全网路由发送RIP广播更新



案例描述

- 本案例的拓扑中，路由器 R1、R2 和 R3 共享形同的广播域，R3 与网段 172.16.X.0/24 互联，并发布到 RIP 中。

案例2-预配

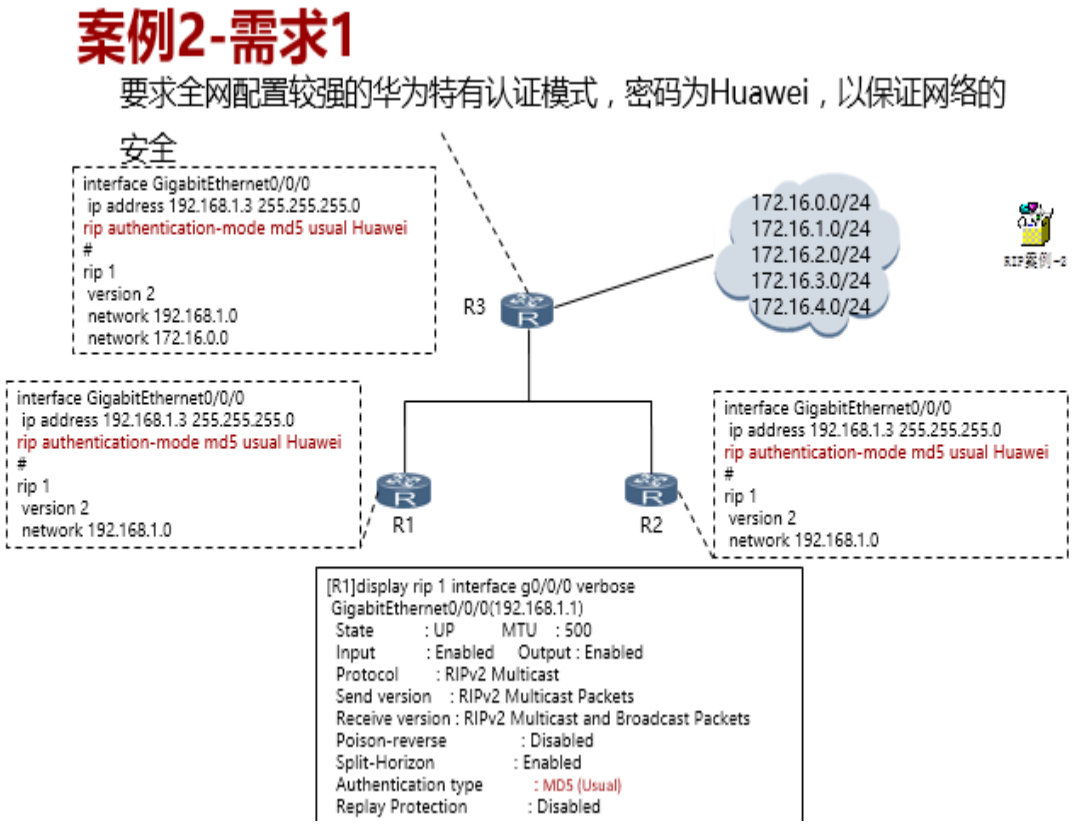



```
[R1]display rip 1 interface g0/0/0 verbose
 GigabitEthernet0/0/0(192.168.1.1)
  State          : UP          MTU    : 500
  Input          : Enabled     Output : Enabled
  Protocol       : RIPv2 Multicast
  Send version   : RIPv2 Multicast Packets
  Receive version : RIPv2 Multicast and Broadcast Packets
  Poison-reverse             : Disabled
  Split-Horizon              : Enabled
  Authentication type        : None
  Replay Protection          : Disabled
```

```
[R1]display  ip routing-table
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
    172.16.0.0/24   RIP     100  1           D   192.168.1.3     GigabitEthernet0/0/0
    172.16.1.0/24   RIP     100  1           D   192.168.1.3     GigabitEthernet0/0/0
    172.16.2.0/24   RIP     100  1           D   192.168.1.3     GigabitEthernet0/0/0
    172.16.3.0/24   RIP     100  1           D   192.168.1.3     GigabitEthernet0/0/0
    172.16.4.0/24   RIP     100  1           D   192.168.1.3     GigabitEthernet0/0/0
.....//此部分省略
```

分析过程

- 关于需求 1 和需求 3，我们这里只是拿 R1 做一个举例。可以看到，路由器是发送组播报文的，并且没有启动认证。
- R1 在没有满足需求 2 之前，是可以收到 172.16.X.0/24 所有网段信息的。



结果说明

- RIP 认证命令只能在接口下进行配置，且 MD5 认证华为设备中即支持标准的 MD5 认证，也支持华为特有的认证模式。
- 通过命令 **display rip** *process-id* **interface** *interface-type* **verbose** 可以看到认证的模式。

参数意义

- **rip authentication-mode** { **simple** *password* | **md5** { **nonstandard** { *password-key1 key-id* | **keychain** *keychain-name* } | **usual** *password-key2* } }

  simple：使用明文验证方式。

  password：明文验证关键字。

  md5：使用 MD5 密文验证方式。

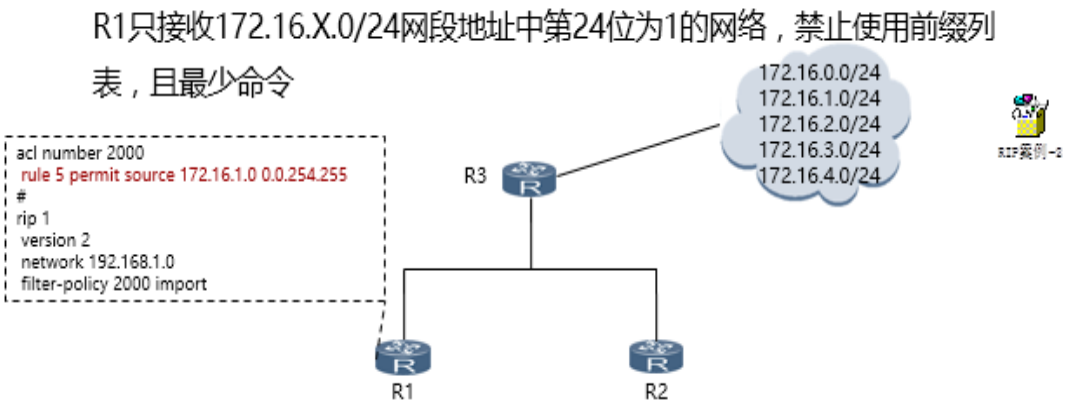
  nonstandard：指定 MD5 密文验证报文使用非标准报文格式（IETF 标准）。

password-key1 : 密文验证关键字。
key-id : MD5 密文验证标识符。
keychain *keychain-name :* Key-Chain 名称。
usual：指定 MD5 密文验证报文使用通用报文格式（私有标准）。
password-key2 : 密文验证关键字。

注意事项

- 每次验证只支持一个验证字。新输入的验证字将覆盖旧验证字。验证字中不允许包含空格。

案例2-需求2



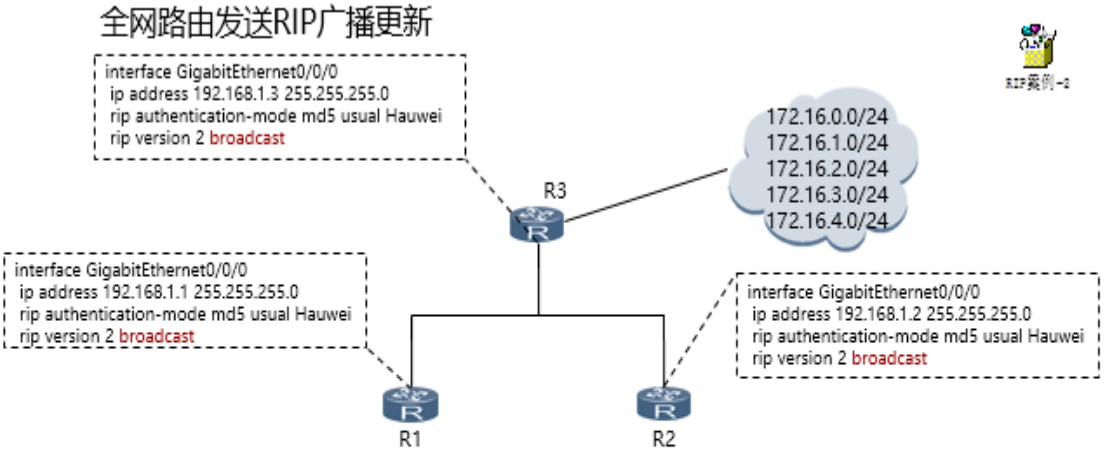

```
[R1]display ip routing-table
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
    172.16.1.0/24   RIP     100  1           D   192.168.1.3     GigabitEthernet0/0/0
    172.16.3.0/24   RIP     100  1           D   192.168.1.3     GigabitEthernet0/0/0
.....//此部分省略
```

结果说明

- 需求要求不能使用前缀列表，则只能使用 ACL。另外需求要求使用最少命令，所以我们不能通过 ACL 一条一条的将需求路由挑出。所以我们采用了案例中给出的解法。

案例2-需求3

全网路由发送RIP广播更新




```
<R1>debugging rip  1 send  GigabitEthernet 0/0/0
Mar 15 2013 10:04:37.820.1-08:00 R1 RIP/7/DBG: 6: 12227: RIP 1: Sending response on interface GigabitEthernet0/0/0
from 192.168.1.1 to 255.255.255.255
Mar 15 2013 10:04:37.820.2-08:00 R1 RIP/7/DBG: 6: 12247: Packet: Version 2, Cmd  response, Length 48
Mar 15 2013 10:04:37.820.3-08:00 R1 RIP/7/DBG: 6: 12407: Authentication-mode - MD5 Digest:
3bf85fbb.6e101fcb.49d5b51e.e5893eb1
Mar 15 2013 10:04:37.820.4-08:00 R1 RIP/7/DBG: 6: 12439: Sequence: 00000edc
Mar 15 2013 10:04:37.820.5-08:00 R1 RIP/7/DBG: 6: 12315: Dest 192.168.1.0/24, Nexthop 0.0.0.0, Cost 16, Tag 0
Mar 15 2013 10:05:09.900.1-08:00 R1 RIP/7/DBG: 6: 12227: RIP 1: Sending response on interface GigabitEthernet0/0/0
from 192.168.1.1 to 255.255.255.255
Mar 15 2013 10:05:09.900.2-08:00 R1 RIP/7/DBG: 6: 12247: Packet: Version 2, Cmd
.....//此部分省略
```

结果说明

- RIPv2 默认情况下组播发送 RIP 更新，通过接口视图命令 **rip version 2 broadcast** 可以修改以广播形式发送更新