三. 路由器ACL列表

**什么是访问列表**

* IP Access-list：IP访问列表或访问控制列表，简称IP ACL
* IP ACL就是对经过网络设备的数据包根据一定的规则进行数据包的过滤。

**设置访问列表的步骤**

* + 第一步，定义规则（哪些数据允许通过，哪些数据不允许通过）
  + 第二步，将规则应用在路由器（或交换机）的接口上

**访问控制列表的分类（区别在规则定义）：**

* + 1、标准访问控制列表
  + 2、扩展访问控制列表
* 标准访问列表
  + 根据数据包源IP地址进行*规则定义*
* 扩展访问列表
  + 根据数据包中源IP、目的IP、源端口、目的端口、协议进行*规则定义*

**访问列表规则的应用**

* 路由器应用访问列表对流经接口的数据包进行控制
  + 1.入栈应用（in）
    - 经某接口进入设备内部的数据包进行安全规则过滤
  + 2.出栈应用（out）
    - 设备从某接口向外发送数据时进行安全规则过滤
* 一个接口在一个方向只能应用一组访问控制列表

**IP ACL的基本准则**

* 一切未被允许的就是禁止的
  + 定义访问控制列表规则时，最终的缺省规则是拒绝所有数据包通过
* 按规则链来进行匹配
  + 使用源地址、目的地址、源端口、目的端口、协议、时间段进行匹配
* 规则匹配原则
  + 从头到尾，至顶向下的匹配方式
  + 匹配成功马上停止
  + 立刻使用该规则的“允许/拒绝……”

**访问列表规则的定义**

* 访问控制列表 ACL 是控制网络访问的基本手段，它可以限制网络流量，提高网络性能。ACL 使用包过滤技术来达到访问控制目的。ACL 分为标准 ACL和扩展 ACL 两种，标准访问控制列表的编号为1~99和1300---1999之间的数字，标准访问控制列表只使用数据包的源地址进行过滤，扩展的 ACL 的编号使用100~199以及 2000----2699 之间的数字。
* 每一个正确的访问列表都至少应该有一条permit语句， 具有严格限制条件的语句应放在访问列表所有语句的最上面， 在靠近源的网络接口上设置扩展 ACL，在靠近目的的网络接口上设置标准的 ACL。
* ACL的基本用途是限制访问网络的用户，保护网络的安全。
* ACL一般只在以下路由器上配置：
* 内部网和外部网的边界路由器
* 两个功能网络交界的路由器
* 限制的内容包括：
* 允许哪些用户访问网络（根据用户的IP地址进行限制）
* 允许用户访问的类型，如允许http和ftp的访问，但拒绝Telnet的访问。（根据用户使用的上层协议进行限制）

-----------------------------------------------------------------------------

**定义规则**：每条ACL语句的形式为：

* Router（config）#access-list 表号 处理方式 条件
* ACL表号用于区分各访问控制列表。
* 处理方式：取值有permit（允许）和deny（拒绝）两种。当数据包与该语句的条件相匹配时，用给定的处理方式进行处理。
* 条件：每条ACL语句只能定义一个条件。

例：

* access-list 1 permit 10.0.0.0 0.255.255.255
* access-list 1 deny 20.0.0.0 0.255.255.255
* 第一句允许源地址为10.\*.\*.\*的数据包通过
* 第二句拒绝源地址为20.\*.\*.\*的数据包通过

**应用ACL**

如果只是定义了ACL，它还不会起任何作用，必须把ACL应用到一个接口上才能起作用。

应用ACL：

***Router（config）#interface 接口号***

***Router（config-if）#ip access-group 表号 [in|out]***

* in:表示数据包进入此接口时使用ACL进行过滤；
* out：表示数据包在离开此接口时使用ACL进行过滤。

**通配符掩码**

* 在ACL语句中，当使用地址作为条件时，它的一般格式为：地址 通配符掩码
* 通配符掩码决定了地址中的哪些位需要精确匹配，哪些位不需要匹配。
* 通配符掩码是一个32位数，采用点分十进制方式书写。匹配时，“0”表示检查位，“1”表示不检查位。
* 如：192.168.1.1 0.0.255.255
* 表示检查前16位，忽略后16位，所以这个条件表示的地址是192.168.\*.\*
* 当条件为所有地址时，如果使用通配符掩码应写为：0.0.0.0 255.255.255.255这时可以用“any”这个条件。
* *Router(config)#access-list 1 permit 0.0.0.0 255.255.255.255*
* *Router(config)#access-list 1 permit any*
* 上面两句话是等价的

host关键字

* 当条件为单一IP地址时，如果使用通配符掩码应写为：IP地址 0.0.0.0，这时可以用“host”关键字
* **Router(config)#access-list 1 permit 200.1.1.5 0.0.0.0**
* **Router(config)#access-list 1 permit host 200.1.1.5**

**ACL语句的增加与删除**

* ACL由一系列访问控制语句组成。
* 当创建一个ACL列表后，**新增加的语句**总是**放到列表最后**。
* 无法删除某一条ACL语句，只能**删除整个ACL列表**。

-------------------------------------------------------------------------

**标准ACL**

* + 使用IP包中的**源IP地址**进行过滤。
  + 在思科的路由器上使用的ACL编号为**1~99**以及**1300~1999**。
* **第一步，定义访问控制列表，命令如下：**

**Router(config)# access-list *access-list-number（通配符掩码）* { permit | deny } source（源地址） [source-wildcard（通配符掩码）] [log（生成日志文件）]**

* **第二步，把标准 ACL应用到一个具体接口：**

**Router(config)# int *interface***

**Router(config-if)# { *protocol* } access-group *access-list-number* {in | out}**

例如

**Router(config)# access-list 1 permit 10.0.0.0 0.255.255.255**

**//允许源地址为10.0.0.0网段的数据通过**

**Router(config)# int s1/1**

**Router(config-if)# ip access-group 1 out**

-------------------------------------------------------------------------------

**扩展ACL**

* + 可以控制**源IP，目的IP，源端口，目的端口**等。
  + 在思科路由器上，扩展ACL的编号为**100~199**以及**2000~2699**。
* **第一步，定义访问控制列表，命令：**

**Router(config)# access-list *access-list-number* { permit | deny } *protocol（指定协议类型） source source-wildcard [operator* operand*]* *destination destination-wildcard* [ *operator* operand] [ established ] [log]**

***operator* ：lt, gt, eq, neq(小于, 大于, 等于, 不等于)**

**operand：一个端口号或应用名称**

**established：**如果数据包使用一个已建立连接，则允许TCP信息通过

**例：Router(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20**

* **第二步，把扩展 ACL应用到一个具体接口：**

**Router(config)# int *interface***

**Router(config-if)# { *protocol* } access-group *access-list-number {in | out}***

例如

**Router(config)# int f0/0**

**Router(config-if)# ip access-group 1 out**

------------------------------------------------------------------------------

**命名ACL的配置**

* **命名ACL——在标准ACL和扩展ACL中，使用名字代替ACL编号。**
* **命名ACL好处：**
  + 字母数字串直观表示特定ACL。
  + 不受99条标准ACL和100条扩展ACL限制。
  + 修改方便，无需删除后再重新配置。
* **第一步，创建一个ACL命名，要求名字字符串要唯一。**

**Router(config)# ip access-list { standard | extended } name**

* **第二步，定义访问控制列表，命令格式：**

**（1）命名的标准ACL：**

**Router(config-sta-nacl)# { permit | deny } source [source-wildcard] [log]**

**（2）命名的扩展ACL：**

**Router(config-sta-nacl)# { permit | deny } protocol source [source-wildcard] [operator operand] destination destination-wildcard [ operator operand] [ established ] [log]**

* **第三步，把 ACL应用到一个具体接口上：**
* **Router(config)# int interface**
* **Router(config-if)# { protocol } access-group name {in | out}**

**命名ACL配置实例**

* **Router(config)# access-list extend server-protect**
* **Router(config-ext-nad)# permit tcp 10.1.0.0 0.0.255.255 host 10.1.2.20 eq www**
* **Router(config)# int f0/0**
* **Router(config)# ip access-group server-protect out**

**删除命名ACL命令**

**（1）删除命名的标准ACL：**

**Router(config-sta-nacl)# no { permit | deny }** **source [source-wildcard] [log]**

**（2）删除命名的拓展ACL：**

**Router(config-sta-nacl)# no { permit | deny } protocol source [source-wildcard] [operator operand] destination destination-wildcard [ operator operand] [ established ] [log]**

**命名ACL注意事项**

* **不能**在任意位置加入新的ACL条目。
* 新增的ACL仍然放在最后一行。
* 必须注意ACL的放置顺序。

-------------------------------------------------------------------------------

**四.RIP协议**

**一.配置路由器的IP地址**

* 要使Cisco路由器在IP网络中正常工作，路由器端口的配置一般要遵循以下规则：
* 一般地，路由器的每个物理网络端口通常要有一个IP地址。
* 相邻路由器的相邻端口IP地址必须在同一IP网段上。
* 同一路由器不同端口的IP地址必须在不同IP网段上。
* 除了相邻路由器的相邻端口外，所有网络中路由器所连接的网段即所有路由器的任何两个非相邻端口都必须不在同一个网段上。

**情形1，配置局域网接口**

* 每个LAN接口都应在一个单独子网上，LAN接口上分配IP地址的最简单方法是使用该接口所在子网地址范围中的第一个IP地址。
* 配置LAN接口的IP地址过程如下：
* 在特权模式下输入config t进入全局配置模式
* 配置具体的LAN接口，输入接口名称：interface *type slot/number*（type端口类型，slot/number插槽号和端口号）
* 输入ip address，提供IP地址和子网掩码 ：ip address *ip address mask*（ip address端口IP地址，mask网络掩码）
* 完成接口配置 ，Ctrl-z

**举例：配置路由器Router1以太网接口0，IP地址为 172.119.16.1，网络掩码255.255.240.0。**

* Router1#configure terminal
* Router1(config)#interface ethernet 0
* Router1(config-if)#ip address 172.119.16.1 255.255.240.0
* Router1(config-if)#no shutdown
* (如果接口已经为激活，此命令可不用)
* Router1(config-if)# Ctrl-Z
* Router1#
* 查看接口配置信息 show ip interface e0

**情形2，配置广域网接口WAN**

* WAN接口的IP地址配置与LAN接口完全一样，如配置串口1，可依下述步骤完成：
* 假设WAN接口IP地址 172.119.32.1，网络掩码为255.255.240.0。
* Router1#config t
* Router1(config)#interface serial 1
* Router1(config-if)#ip address 172.119.32.1 255.255.240.0
* Router1(config-if)#no shutdown
* (如果接口已经为激活，此命令可不用)
* Router1(config-if)# Ctrl-Z退到最前面一级 exit 退到上一级
* Router1(config)#
* Router1#
* 查看接口配置信息 show ip interface s1
* 在广域网端口配置中，两个路由器通过各自串口相连(使用WAN连接协议)。此连接需要配置为单独子网，即A路由器的串口,要从一单独子网中选择一个IP地址，与之相连的B路由器的串口，也应从同一子网中选择一个IP地址，而此子网中其他所有可用的IP地址则浪费掉了。
* 为了克服这种明显的IP地址浪费问题，可以将串口配置为不带IP地址(但仍可路由IP包)。
* ip unnumbered [ interface or virtual interface]。
* 其中interface or virtual interface参数即为指定的实际接口，比如Ethernet 0，或者是一个虚拟接口。

无编号IP地址除了节省地址空间，还可以与其他无编号的IP地址进行通信，而不必担心两个互连的端口是否在同一个子网上。但是它也有如下限制

* 串口使用HDLC，PPP，LAPB，Frame Relay和tunnel interface打包方式。
* 不能使用ping来探测端口是否正常工作，因为它是没有IP地址的。
* 不能用简单网管协议（SNMP）远程监测端口状态。
* 不能通过unnumbered端口远程启动系统。
* 在unnumbered端口上不支持IP安全选项。

---------------------------------------------------------------------------

**信道分类**

**点对点信道：由链路的一端的单个发送方和链路另一端的单个接收方组成。如：点对点协议（PPP），高级数据链路控制（HDLC）**

**广播信道：**局域网是一种典型的广播信道，一个节点发送的数据能够被广播信道上所有的节点接收到.(CSMA/CD)

**配置广域网接口协议**

配置高级数据链路控制（HDLC）协议

* HDLC是一个点对点的WAN协议，也是Cisco路由器默认的广域网协议。
* 默认的情况下，Cisco路由器的HDLC的协议是激活的。即使没有被激活，也只需一个简单的封装命令就可以打开。

**举例：在路由器Router1的串口1上配置HDLC。**

* **Router1#config t**
* **Router1(config)#interface serial 1**
* **Router1(config-if)#encapsulation hdlc**
* **Router1(config-if)#bandwidth 64**
* **Router1(config-if)#Ctrl-Z**
* **Router1#**
* **如果不同厂家的路由器互连，建议使用点对点数据链路层协议（ PPP ）。**

**Router1(config-if)#encapsulation ppp**

**二.配置路由协议**

* 路由器的接口配置了适当的IP地址和子网掩码后，就可以配置路由协议了。
* 依据网络的大小，可以选用各种不同的内部路由协议(内部网络上用于路由的协议)。比如，RIP对于小型网络还是不错的，但仅局限于15跳(从一个路由器到另一路由器称为一跳)，因此用于大型网络显然是个问题。对于大型网络，可以用IGRP或OSPF。

**路由协议 RIP**

* 在内部网关协议IGP ( Interior Gateway Protocol)中，RIP ( Routing information Protocol)是应用较早、使用较普遍的的IGP协议。RIP适用于小型同类网络，是典型的距离向量 (distance-vector) 协议。
* RIP通过广播UDP报文来交换路由信息，每30秒发送一次路由信息更新。RIP是以跳数(hop count)作为尺度来衡量路由距离，跳数是一个包到达目标所必须经过的路由器的数目。

举例：设路由器连接了三个网络202.119.224.0，202.119.225.0，202.119.226.0

在配置路由协议之前激活IP路由，其方法是：在配置提示符下，输入全局命令：ip routing，如果想禁止IP路由，可使用配置命令：no ip routing。

* Router1(config)#router rip
* Router1(config-router)#router rip
* Router1(config-router)#network 202.119.224.0
* Router1(config-router)#network 202.119.225.0
* Router1(config-router)#network 202.119.226.0

查看RIP路由表：show ip route

查看和RIP相关的协议信息：show ip protocol

----------------------------------------------------------------

**路由协议 IGRP**

* IGRP (Interior Gateway Routing Protocol)是一种动态距离向量路由协议，它由Cisco公司20世纪80年代中期设计，使用包括延迟、带宽、可靠性和负载的组合配置进行度量。
* 配置IGRP的方法和配置RIP相似，也必须激活IGRP协议，并指定与路由器相连的主IP网络。

**------------------------------------------------------------------**

**路由进程如何确定路径（补充静态路由配置）**

* 通过配置写好的路由表来传送，这种需要有系统管理员手工配置和配置路由表并制定每条路由线路的方法称为静态路由。静态路由具有较高的安全系数，比较适合娇小型的网络使用。
* 由路由器按指定的协议格式在网上广播和接收路由信息，通过路由器之间不断交换的路由信息动态的更新和确定路由表，并随时向附近的路由器广播，这种方式称为动态路由。它较具灵活性，使用配置简单，成为最主要的路由类型，如RIP、IGRP等
* 在Cisco路由器上可以配置三种路由：静态路由、动态路由和默认路由。
* 一般地，路由器查找路由的顺序为静态路由、动态路由，如果静态路由表和动态路由表中都没有合适的路由，则通过默认路由将数据包传输出去，可以综合使用这三种路由。

**静态路由配置**

* 在全局配置模式下，建立静态路由的命令格式为：

*ip route prefix mask*（address|interface）[distance][tag tag][permanent]

prefix 所要到达的目的网络（目的地子网地址）；

mask 子网掩码；

address 下一跳的IP地址，即相邻路由器的相邻端口地址；

interface 本地网络端口（本地物理端口号）

distance 管理距离（可选）

tag tag值

permanent 指定即使该端口关闭仍然保持该路由

**--------------------------------------------------------------------**

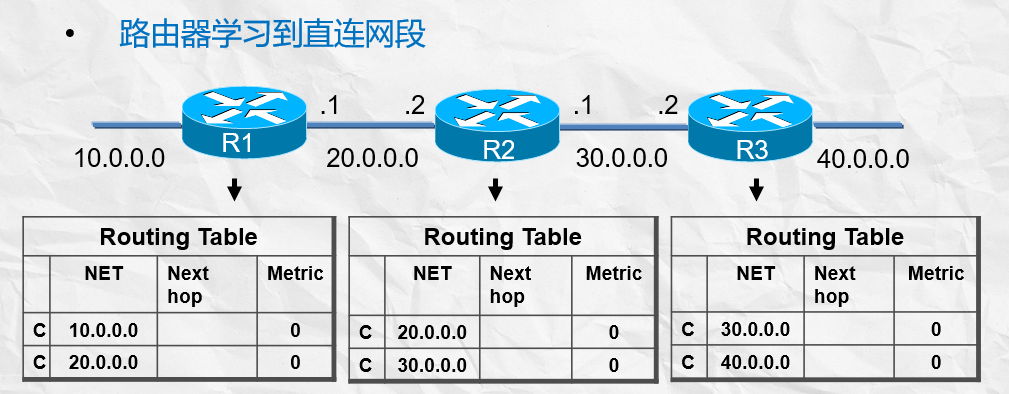
**Show命令**

* Exec命令中，有许多命令都是和检查路由器的各种配置信息及硬件信息相关的。其中最有用的是”show”命令。该命令可以用来查看路由器的所有端口以及有关flash RAM或被路由的协议的统计信息。
* 路由器的状态可以在用户模式和特权模式下用”show”命令来检查。show命令可以显示配置许多路由器的参数以及工作状况。
* show version 显示路由器的硬件配置
* show running-config 显示当前配置
* show startup-config 显示启动配置
* show flash 显示flash中的IOS文件名、flash RAM所使用的空间和空闲的空间。
* show controllers 显示所有的网络模块及其端口
* show interface[type slot／port)显示命令指定的端口，第一行给出端口正确的插槽号、端口编号以及端口及线路的协议状态、工作状态等
* show ip route ：该命令可以查看路由协议所获取的路由信息。其中，以C为标志的网络是和路由器直接相连的，以R为标志的网络是通过RIP获得的路由信息，以I为标志的网络则是通过IGRP获得的。
* show ip protocol ：该命令可以查看相关路由协议的信息。如更新周期、路由信息“挂起”时间，路由信息“作废”时间等
* **debug ip rip：打开RIP协议调试命令**

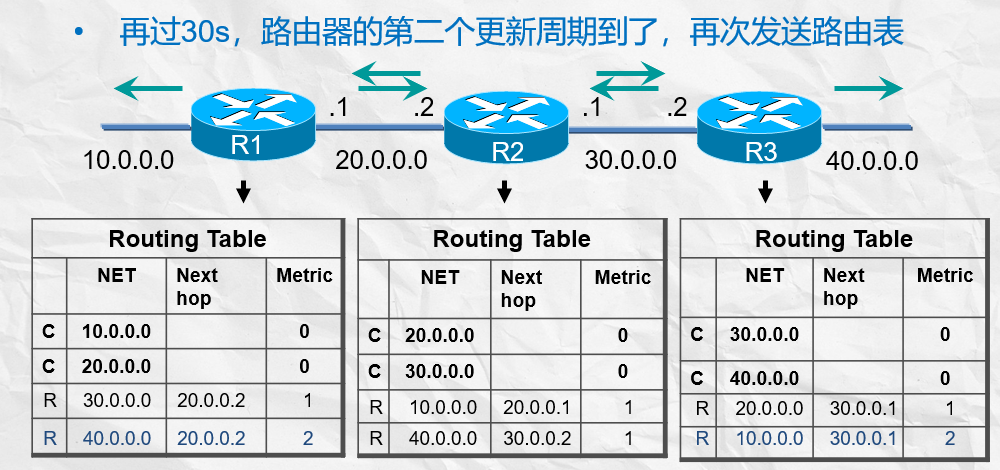
---------------------------------------------------------------------

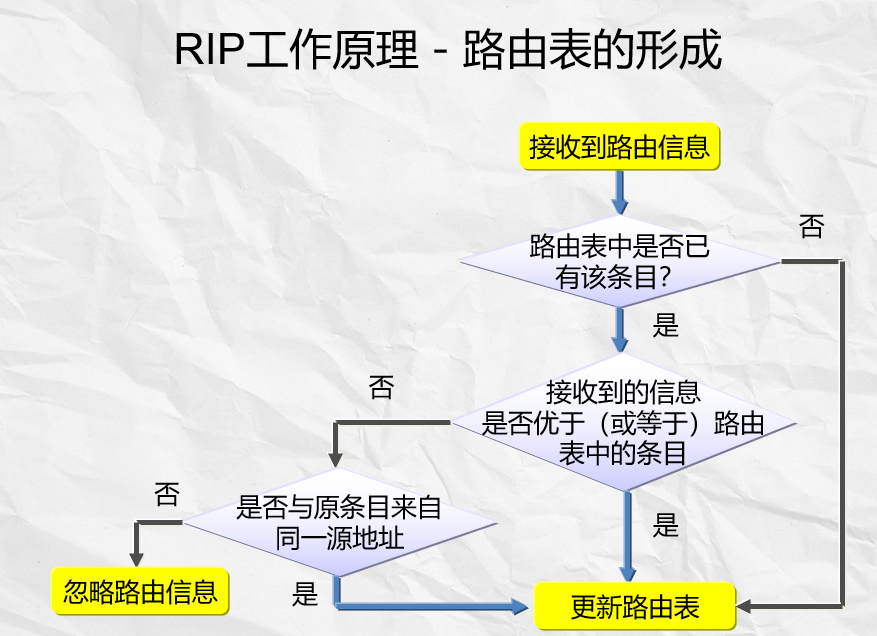
**RIP工作原理**

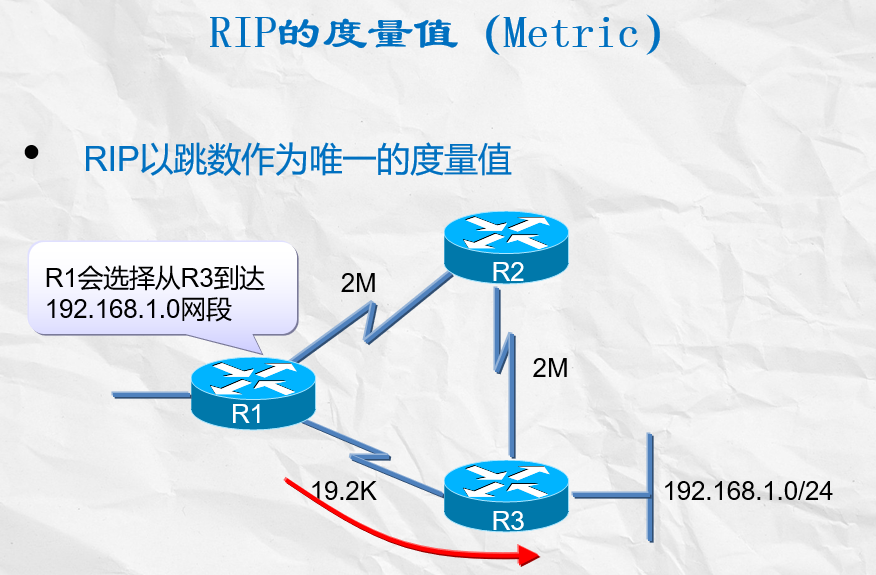
**路由表的形成过程**





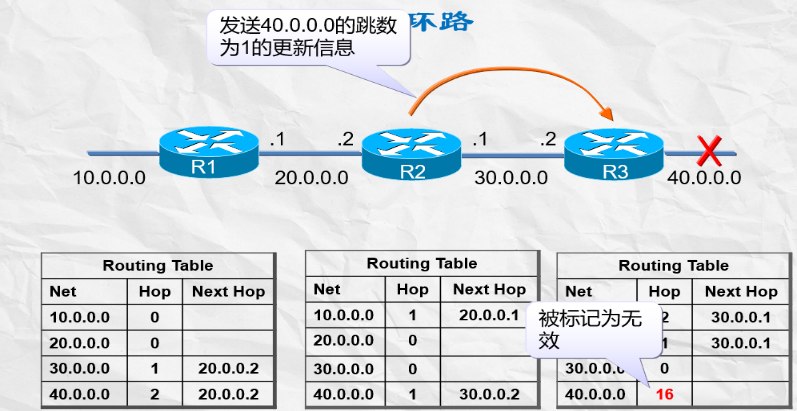


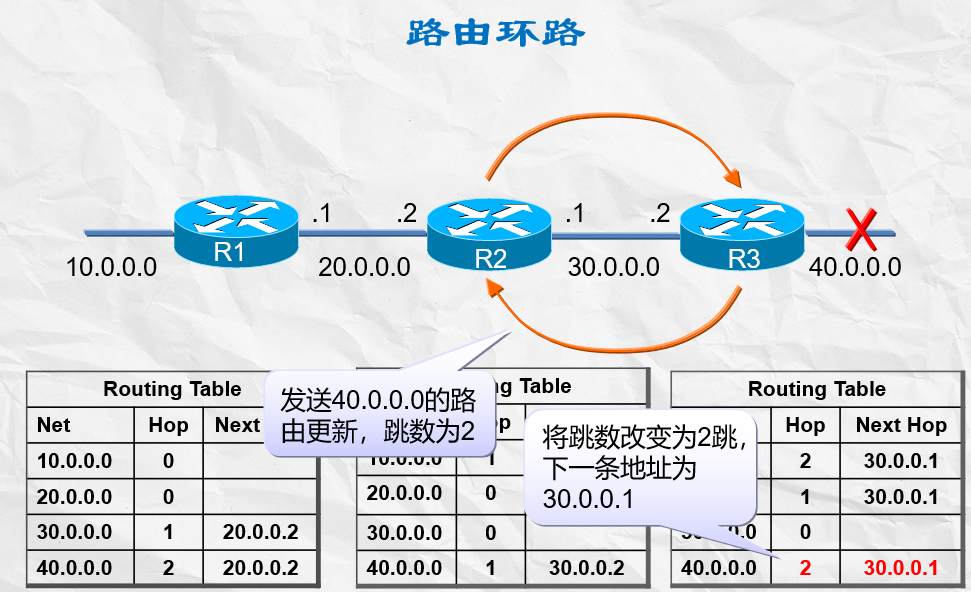


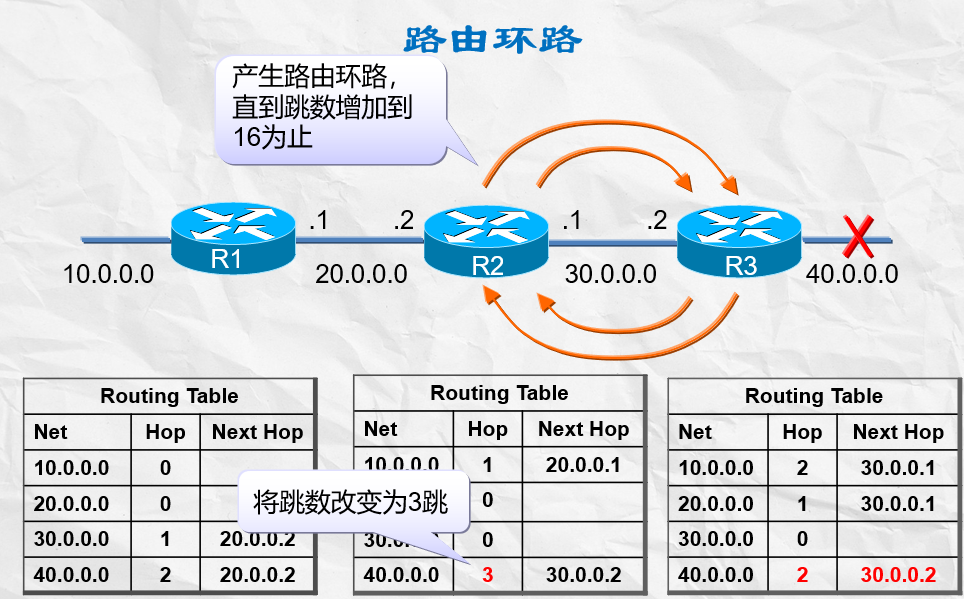


**RIP计时器**

* 更新计时器
  + 路由器每隔30秒从每个启动RIP协议的接口发送出路由更新信息
* 无效计时器
  + 如果一条路由在180s内没有收到更新，这条路由的跳数将记为16
* 刷新计时器
  + 如果这条路由在被记为16跳后，60s内还没有收到更新，则将这条路由从路由表中删除
* 抑制计时器
  + 如果一个目标的距离增加或变为不可达，启动抑制计时器（180s），直到抑制计时器超时，路由器才接收有关于这条路由的更新信息。
  + 作用是防止路由抖动

 **路由环路的产生条件**





**水平分割是一个规则，用来防止路由环路的产生**

* **规则：从一个接口上学习到的路由信息，不再从这个接口发送出去**

**---------------------------------------------------------------------------**

**有类路由与无类路由**

* 根据路由协议,在进行路由信息宣告时,是否包含网络掩码,可以把路由协议分为两种:
  + 一种是有类路由（Classful）协议,它们在宣告路由信息时不携带网络掩码
  + 一种是无类路由（Classless）协议,它们在宣告路由信息时携带网络掩码

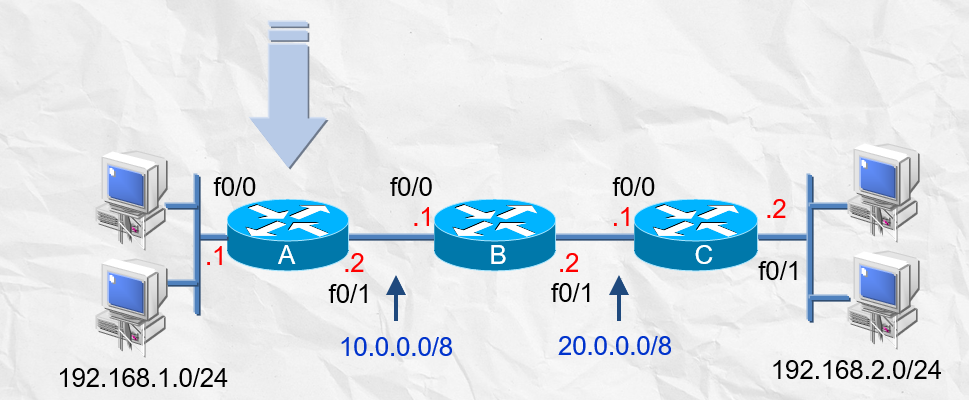
**RIP路由协议的版本**

* RIP v1
  + 发送路由更新时不携带子网掩码，属于有类路由协议
  + 发送路由更新时，目标地址为广播地址:

255.255.255.255

* RIP v2
  + 发送路由更新时携带子网掩码，属于无类路由协议
  + 发送路由更新时，目标地址为组播地址：224.0.0.9

**举例：RIP v1路由协议配置实例**



**RouterA(config)#interface f0/0**

**RouterA(config-if)#ip address 192.168.1.1 255.255.255.0**

**RouterA(config-if)#no shutdown**

**RouterA(config)#interface f0/1**

**RouterA(config-if)#ip address 10.0.0.2 255.0.0.0**

**RouterA(config-if)#no shutdown**

**RouterA(config)#router rip**

**RouterA(config-router)#network 10.0.0.0**

**RouterA(config-router)#network 192.168.1.0**

**RouterB(config)#interface f0/0**

**RouterB(config-if)#ip address 10.0.0.1 255.0.0.0**

**RouterB(config-if)#no shutdown**

**RouterB(config)#interface f0/1**

**RouterB(config-if)#ip address 20.0.0.2 255.0.0.0**

**RouterB(config-if)#no shutdown**

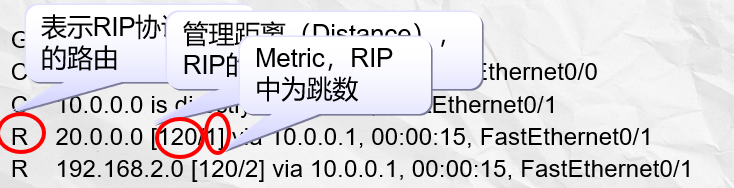
**RouterB(config)#router rip**

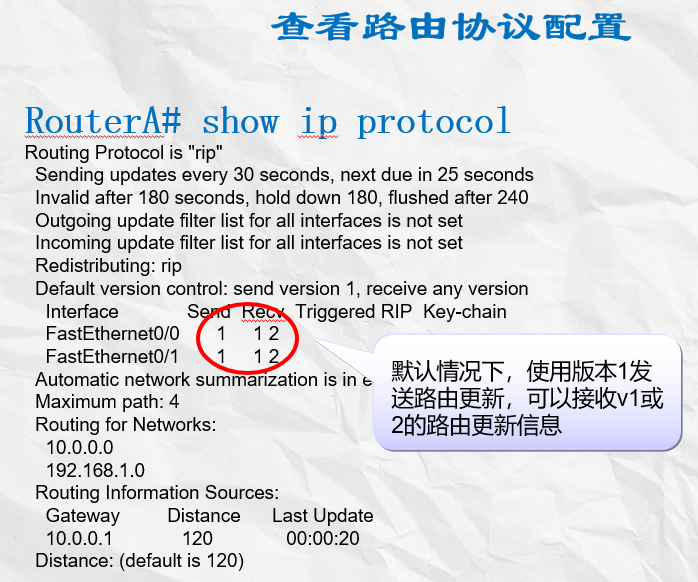
**RouterB(config-router)#network 10.0.0.0**

**RouterB(config-router)#network 20.0.0.0**

**-----------------------------------------------**

**验证配置，查看路由表RouetrA# show ip route**



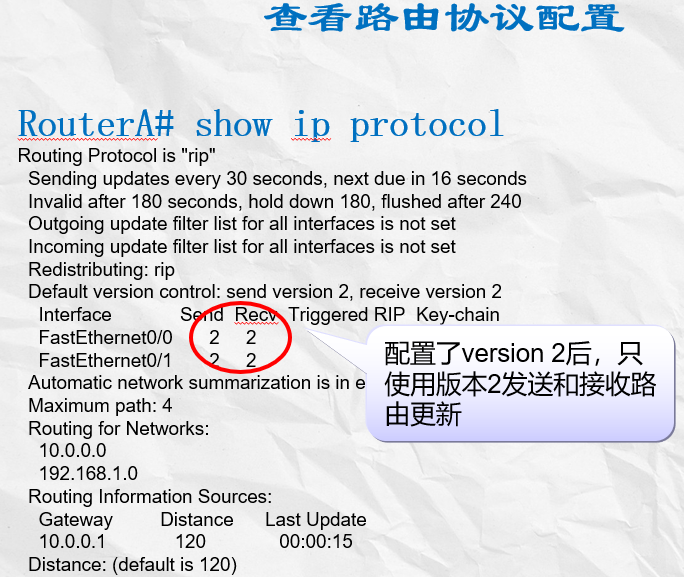
 

**配置RIP协议使用版本2**

**Router(config)# router rip**

**Router(config-router)# version 2**

**Router(config-router)# no auto-summary**

**验证配置**

