第1章　10个路由与交换专题解答

问题

- 多路由协议
  什么时候使用多路由协议
  定义距离向量路由协议
  定义链接状态路由协议
  一个路由器使用多种路由协议
- 过滤
  确定访问表
  支持多种访问表
  创建标准IP访问表
  创建扩展IP访问表
  访问表到接口的链接
  使用有名访问表
  访问表的定位
  访问表的显示和状态
  IPX标准访问表与SAP过滤器的区别
  配置IPX标准访问表
  配置IPX SAP过滤器
  配置AppleTalk访问表
- 路由再分配
  定义路由再分配
  使用路由再分配
  定义管理距离
  管理距离的值
  配置路由再分配
- 毗邻路由器
  确定毗邻路由器的重要性
  距离向量路由协议与链接状态路由协议是如何发现毗邻路由器的
- 内部、系统和外部路由
  定义自治系统
  内部和外部路由协议
  配置路由器使用RIP
  确认RIP是激活的

关闭RIP路由状态更新的显示
确定哪些网络是由RIP路由协议发现的
激活IGRP路由协议
定义增强型IGRP
确定哪些网络是由IGRP路由协议发现的
边界网关协议（BGP）
BGP支持的连接种类
有BGP时的路由再分配
在数据库中显示BGP路径

- 水平分割
  定义水平分割
  路由环的产生
- 度量值
  路由度量值
  IGRP对路由度量值的使用
  修改度量值
  路由选择需要知道的信息
- 与其他厂家设备的兼容
  开放性标准与专利性技术
- 路由数据库
  回顾路由选择表
- 特殊的路由技术
  建立静态路由
  禁止水平分割

本章摘要

每一种路由协议都有一套规则来指示路由器如何以及向哪里发送数据包，使其能到达正确的目的地。这些规则（方法）通过了解路由器接口的连接参数和接口配置情况，计算出一些度量值，然后根据这些度量值选出最优路径，指出数据包发向哪一个接口。一些路由器有多种路由选择协议，包括距离向量路由协议或链接状态路由协议。每一种协议都要根据一些关键信息，如地址，来确定毗邻站点、发现路由、选择路由和保持路由信息。

本章介绍一些广泛使用的路由协议的参数，这些协议有： RIP、OSPF、IGRP和EIGRP。每一节的内容如下：

- 多路由协议　说明距离向量路由协议与链接状态路由协议的区别。
- 过滤　说明如何在网络中使用访问表控制流量。
- 路由再分配　说明路由选择表从一种路由选择协议到另一种路由选择协议的转换。
- 毗邻路由器　说明在寻找路由的过程中如何发现相邻节点。
- 内部、系统和外部路由解释路由协议的分类及其功能。
- 水平分割　说明避免路由环的步骤。

- 度量值 回顾路由协议确定最优路径时使用的方法。
- 与其他厂家设备的兼容 解释开放性路由协议与专利性路由协议的关系。
- 路由数据库 解释路由选择表的使用及其重要性。
- 特殊的路由技术 解释建立静态路由和禁止水平分割。

1.1 多路由协议

1 什么时候使用多路由协议？

当两种不同的路由协议要交换路由信息时，就要用到多路由协议。当然，路由再分配也可以交换路由信息。下列情况不必使用多路由协议：

- 从老版本的内部网关协议（Interior Gateway Protocol，IGP）升级到新版本的IGP。
- 你想使用另一种路由协议但又必须保留原来的协议。
- 你想终止内部路由，以免受到其他没有严格过滤监管功能的路由器的干扰。
- 你在一个由多个厂家的路由器构成的环境下。

2 什么是距离向量路由协议？

距离向量路由协议是为小型网络环境设计的。在大型网络环境下，这类协议在学习路由及保持路由将产生较大的流量，占用过多的带宽。如果在 90秒内没有收到相邻站点发送的路由选择表更新，它才认为相邻站点不可达。每隔 30秒，距离向量路由协议就要向相邻站点发送整个路由选择表，使相邻站点的路由选择表得到更新。这样，它就能从别的站点（直接相连的或其他方式连接的）收集一个网络的列表，以便进行路由选择。距离向量路由协议使用跳数作为度量值，来计算到达目的地要经过的路由器数。

例如，RIP使用Bellman-Ford算法确定最短路径，即只要经过最小的跳数就可到达目的地的线路。最大允许的跳数通常定为15。那些必须经过15个以上的路由器的终端被认为是不可到达的。

距离向量路由协议有如下几种：IP RIP、IPX RIP、AppleTalk RTMP和IGRP。

3 什么是链接状态路由协议？

链接状态路由协议更适合大型网络，但由于它的复杂性，使得路由器需要更多的 CPU资源。它能够在更短的时间内发现已经断了的链路或新连接的路由器，使得协议的会聚时间比距离向量路由协议更短。通常，在 10秒钟之内没有收到邻站的 HELLO报文，它就认为邻站已不可达。一个链接状态路由器向它的邻站发送更新报文，通知它所知道的所有链路。它确定最优路径的度量值是一个数值代价，这个代价的值一般由链路的带宽决定。具有最小代价的链路被认为是最优的。在最短路径优先算法中，最大可能代价的值几乎可以是无限的。如果网络没有发生任何变化，路由器只要周期性地将没有更新的路由选择表进行刷新就可以了（周期的长短可以从30分钟到2个小时）。

链接状态路由协议有如下几种：IP OSPF、IPX NLSP和IS-IS。

4 一个路由器可以既使用距离向量路由协议，又使用链接状态路由协议吗？

可以。每一个接口都可以配置为使用不同的路由协议；但是它们必须能够通过再分配路

由来交换路由信息。（路由的再分配将在本章的后面进行讨论。）

1.2 过滤

1 什么是访问表？

访问表是管理者加入的一系列控制数据包在路由器中输入、输出的规则。它不是由路由器自己产生的。访问表能够允许或禁止数据包进入或输出到目的地。访问表的表项是顺序执行的，即数据包到来时，首先看它是否是受第一条表项约束的，若不是，再顺序向下执行；如果它与第一条表项匹配，无论是被允许还是被禁止，都不必再执行下面表项的检查了。每一个接口的每一种协议只能有一个访问表。

2 支持哪些类型的访问表？

一个访问表可以由它的编号来确定。具体的协议及其对应的访问表编号如下：

- IP标准访问表编号：1～99
- IP扩展访问表编号：100～199
- IPX标准访问表编号：800～899
- IPX扩展访问表编号：1000～1099
- AppleTalk访问表编号：600～699

提示 在Cisco IOS Release 11.2或以上版本中，可以用有名访问表确定编号在1～199的访问表。

3 如何创建IP标准访问表？

一个IP标准访问表的创建可以由如下命令来完成：

```
Access-list access list number{permit | deny}
source [source-mask]
```

在这条命令中：

- access list number：确定这个入口属于哪个访问表。它是从1到99的数字。
- permit | deny：表明这个入口是允许还是阻塞从特定地址来的信息流量。
- source：确定源IP地址。
- source-mask：确定地址中的哪些比特是用来进行匹配的。如果某个比特是“ 1”，表明地址中该位比特不用管，如果是“ 0”的话，表明地址中该位比特将被用来进行匹配。可以使用通配符。

以下是一个路由器配置文件中的访问表例子：

```
Router# show access-lists
Standard IP access list 1
deny 204.59.144.0, wildcard bits 0.0.0.255
permit any
Router#
```

下面是给定一个访问表的名字，使用SHOW IP ACCESS-LIST命令的输出：

```
showcase# show ip access-list Internetfilter
Extended IP access list Internetfilter
permit tcp any 171.69.0.0 0.0.255.255 eq telnet
deny tcp any any
deny udp any 171.69.0.0 0.0.255.255 lt 1024
deny ip any any log
```

4 如何创建IP扩展访问表？

创建IP扩展访问表可以用：

```
Access-list access list number{permit | deny}
protocol source [source-mask] destination
destination-mask [operator operand] [established]
```

在这条命令中：

- access list number：用在100～199中的数字确定访问表。
- permit | deny：表明这个入口是允许还是阻塞特定地址的信息流量。
- protocol：IP、TCP、UDP、ICMP、GRE、IGRP。
- source和destination：确定源和目的IP地址。
- source-mask和destination-mask：确定地址中的哪些比特是用来进行匹配的。如果某个比特是“ 1 ”，表明地址中该位比特可以忽略，如果是“ 0 ”的话，表明地址中该位比特将被用来进行匹配。可以使用通配符。
- operator和operand：It、gt、eq、neq（小于、大于、等于、不等）和端口号。
- established：如果数据包使用一个已经建立的连接（如ACK位有效），则允许TCP流量通过。

注意 一个访问表必须有一个对所有使用访问表的数据包都适用的表项。最后一个隐含的表项用来处理那些前面的表项都不处理的数据包，即它能匹配所有的剩余的数据包。

5 链接访问表和接口使用什么命令？

使用IP ACCESS-GROUP命令将访问表链接到一个接口：

```
ip access-groupaccess-list-number    { in | out }
```

在这个命令中：

- access-list-number：表明要链接的访问表的编号。
- in | out：选择访问表是用于输入还是输出接口，未指明就使用缺省值。

提示 要去除一个访问表，首先键入NO ACCESS-GROUP命令及其相应的参数，然后再键入NO ACCESS-LIST命令及其相应的参数。

6 如何使用有名IP访问表？

你可以使用有名IP访问表从一个特定的访问表中删除一个单独的表项。这使得你能够方便地修改访问表，而不用删除它然后重新配置。在下列情况下可以使用有名访问表：

- 你想使用一个字母数字（alphanumeric）名确认一个访问表。

• 对于一个给定的协议，你有超过99个简单的，超过100个扩展的访问控制表需要配置。

注意 你不能对多个访问表使用相同的名字，不同种类的访问表也不能有相同的名字。

7 为什么访问表的位置很重要？

管理者使用访问表来减少不必要的流量。被禁止的终端不能使用网络资源发送数据包到目的地。标准访问表没有指明目的地的地址，所以应该放在离目的地近的地方。扩展访问表指明了目的地，就应该放在距离数据流的源较近的地方。

8 如何找出已配置的访问表及其状态？

使用SHOW IP INTERFACE命令来显示哪些访问表是激活的。使用 SHOW ACCESS-LISTS命令来显示所有访问表的内容。如果你指明了访问表的名字或编号，你就可以看到这个访问表的具体内容了。

9 IPX标准访问表和SAP过滤器有何区别？

IPX标准访问表能够过滤源和目的地址。 SAP过滤器是为在一个或多个网络上的服务器服务的。IPX标准访问表检查源地址或源和目的地址，可以使用通配符掩码，像 IP的通配符掩码一样。SAP过滤器能够控制获得最近的服务器（GNS）、IPX RIP和NetWare的链路服务协议（NLSP）等产生的流量。

10 如何配置IPX标准访问表？

可以使用如下命令配置IPX标准访问表：

```
Access-list access-list number{ deny | permit }
Protocol source-network [. source-node] [source-node-mask]
[destination-network] [.destination-node]
[destination-node-mask]
```

在这个命令中：

• access-list-number：是一个IPX过滤器列表的编号，从800到899。

• protocol：是协议类型的编号， 0表示任何协议；1表示RIP；4表示SAP；5表示SPX；17表示NCP；20表示IPX NetBIOS。

• source-network：指明源网络编号，用8个十六进制数表示。

• source-node：指明在源网络中的节点编号，是一个 48比特的数字，可以由每4个就用点分开的十六进制数表示。

• destination-network：指明报文的目的网络编号。

• destination-node：指明报文的目的节点号。

用IPX ACCESS-GROUP命令可以将访问表链接到一个接口：

```
ipx access-group access-list-number
```

下面是创建一个名叫sal的扩展访问表的例子，它禁止所有的SPX报文：

```
ipx access-list extended sal
deny spx any all any all log
permit any
```

下面是一个IPX标准访问表的例子：

```
Hostname Router
!
!
ipx routing 00e0.1e68.5c62
!
interface Ethernet0
ip address 192.168.68.1 255.255.255.0
ipx access-group 800
ipx network 100
!
interface Serial0
ip address 172.16.1.1 255.255.255.252
no fair-queue
!
!
access-list 800 deny 1 200
access-list 800 permit FFFFFFFF
```

11 如何配置IPX SAP过滤器？

SAP过滤器可以按以下格式创建：

```
access-list access-list-number    { deny | permit } network
[.node] [network-mask node-mask]
[service-type [server-name]]
```

下一行可以是：

```
ipx input-sap-filteraccess-list-number
```

或：

```
ipx output-sap.-filteraccess-list-number
```

在这个命令中：

- access-list-number：指明一个IPX过滤器的编号，从1000到1099，它是指向一个SAP过滤器。
- network[.node]：指明Novell源内部网络编号和选项节点号（－1表示所有网络）。
- network-mask node-mask：指明网络和节点的掩码。1表示该位不作处理。
- service-type：指明要过滤的SAP服务类型。每一种服务类型用一个十六进制数表示：4代表文件服务器，7代表打印服务器，24代表远端网桥服务器（路由器）。
- server-name：指明提供该项服务的服务器名称。

使用IPX INPUT | OUTPUT-SAP FILTER命令将过滤器与接口进行链接，同时决定在进入SAP表之前，在哪儿SAP报文被过滤，或者在下一次更新时进行过滤。

如下的配置文件显示了一个IPX SAP过滤器：

```
Hostname Router
!
!
ipx routing 00e0.1e68.5c62
!
```

```
interface Ethernet0
ip address 192.168.68.1 255.255.255.0
ipx input-sap-filter 1000
ipx network 100
!
interface Serial0
ip address 172.16.1.1 255.255.255.252
no fair-queue
!
!
access-list 1000 deny 1 200 7
access-list 1000 permit FFFFFFFF
```

下面是创建一个名叫 Merchant的SAP访问表的例子。它使得在 SAP广告中，只允许Merchant被传送：

```
ipx access-list sap Merchant
permit 1234 4 Merchant
```

12 AppleTalk访问表的主要概念是什么？

AppleTalk的访问表能够过滤扩展的网络或电缆范围。你也可以在一个扩展的网络内选择部分电缆范围。使用AppleTalk Ⅰ时，你可以指定一个网络；但在AppleTalk Ⅱ中，你可以指定电缆范围的全部或一部分。访问表可以控制数据报文和使用 RTMP和ZIP的路由更新报文。

13 如何配置AppleTalk访问表？

AppleTalk使用两种格式进行配置。定义一个全电缆范围的过滤器，使用如下命令：

```
access-list number {permit | deny} cable-range cable-range
```

定义一个部分电缆范围的过滤器，使用如下命令：

```
access-list number {permit | deny} within cable range cable-range
```

在这个命令中：

- number：AppleTalk的访问表编号（从600到699）。
- cable-range：指明特定的电缆范围。

可以使用APPLETALK ACCESS-GROUP命令将访问表链接到一个或多个接口：

```
Appletalk access-group access-list-number
```

1.3 路由再分配

1 什么是路由再分配？

路由再分配允许一个寻找路由进程发现的路由可以更新其他进程的路由选择表。例如，RIP的路由选择表可以输入到OSPF或EIGRP的路由选择表中，反向亦可。

提示 你只能在支持相同协议栈的路由协议之间进行路由再分配。例如， IP RIP和OSPF之间可以进行路由再分配是因为它们都支持 TCP/IP协议栈。但是，IPX RIP和

OSPF之间就不能进行路由再分配，因为IPX RIP支持的是IPX/SPX协议栈而OSPF不是。还要注意的一个例外是： EIGRP支持多种路由协议，并且可以用来与 IP、IPX和AppleTalk之间进行路由再分配。

2 什么时候使用路由再分配？

路由再分配通常在那些负责从一个自治系统学习路由，然后向另一个自治系统广播的路由器上进行配置。如果你在使用IGRP或EIGRP，路由再分配通常是自动执行的。

3 什么是管理距离？

管理距离是指一种路由协议的路由可信度。每一种路由协议按可靠性从高到低，依次分配一个信任等级，这个信任等级就叫管理距离。对于两种不同的路由协议到一个目的地的路由信息，路由器首先根据管理距离决定相信哪一个协议。

4 管理距离的值是什么？

表1-1是各种协议的管理距离的值。

表1-1 管理距离缺省值

路由信息源	距离缺省值	路由信息源	距离缺省值
相连接口	0	IS-IS	115
静态路由	1	RIP	120
增强型IGRP汇总路由	5	EGP	140
外部BGP	20	外部增强型IGRP	170
内部增强IGRP	90	内部BGP	200
IGRP	100	未知	255
OSPF	110		

5 如何配置再分配？

在进行路由再分配之前，你必须首先：

1) 决定在哪儿添加新的协议。
2) 确定自治系统边界路由器（ASBR）。
3) 决定哪个协议在核心，哪个在边界。
4) 决定进行路由再分配的方向。

可以使用以下命令再分配路由更新（这个例子是针对 OSPF的）：

```
router(config-router)#redistribute protocol [process-id]
[metric metric-value  ] [metric-type type-value  ] [subnets]
```

在这个命令中：

- protocol：指明路由器要进行路由再分配的源路由协议。主要的值有： bgp、eqp、igrp、isis、ospf、static[ip]、connected和rip。
- process-id：指明OSPF的进程ID。
- metric：是一个可选的参数，用来指明再分配的路由的度量值。缺省的度量值是 0。你应

该使用与目的协议含义一致的度量值。

- metric-type：是一个可选的OSPF参数，指明向OSPF选路域通告缺省度量值的外部链路的类型。它的值为1时，表明类型1外部路由；为2时表明类型2外部路由。类型2是缺省的值。
- subnets：是一个可选的OSPF参数，该参数要求适当地再分配内部子网络。

注意 你只需要使用REDISTRIBUTE和DEFAULT-METRIC命令对那些不能自动执行路由再分配的协议进行路由再分配。

1.4 毗邻路由器

为什么确定毗邻路由器很重要？

在一个小型网络中确定毗邻路由器并不是一个主要问题。因为当一个路由器发生故障时，别的路由器能够在一个可接受的时间内收敛。但在大型网络中，发现一个故障路由器的时延可能很大。知道毗邻路由器可以加速收敛，因为路由器能够更快地知道故障路由器，因为hello报文的间隔比路由器交换信息的间隔时间短。

使用距离向量路由协议的路由器在毗邻路由器没有发送路由更新信息时，才能发现毗邻路由器已不可达，这个时间一般为 10～90秒。而使用链接状态路由协议的路由器没有收到hello报文就可发现毗邻路由器不可达，这个间隔时间一般为 10秒钟。

距离向量路由协议和链接状态路由协议如何发现毗邻路由器？

使用距离向量路由协议的路由器要创建一个路由表（其中包括与它直接相连的网络），同时它会将这个路由表发送到与它直接相连的路由器。毗邻路由器将收到的路由表合并入它自己的路由表，同时它也要将自己的路由表发送到它的毗邻路由器。使用链接状态路由协议的路由器要创建一个链接状态表，包括整个网络目的站的列表。在更新报文中，每个路由器发送它的整个列表。当毗邻路由器收到这个更新报文，它就拷贝其中的内容，同时将信息发向它的邻站。在转发路由表内容时没有必要进行重新计算。

注意 使用IGRP和EIGRP的路由器广播hello报文来发现邻站，同时像OSPF一样交换路由更新信息。EIGRP为每一种网络层协议保存一张邻站表，它包括邻站的地址、在队列中等待发送的报文的数量、从邻站接收或向邻站发送报文需要的平均时间，以及在确定链接断开之前没有从邻站收到任何报文的时间。

1.5 内部、系统和外部路由

什么是自治系统？

一个自治系统就是处于一个管理机构控制之下的路由器和网络群组。它可以是一个路由器直接连接到一个LAN上，同时也连到Internet上；它可以是一个由企业骨干网互连的多个局域网。在一个自治系统中的所有路由器必须相互连接，运行相同的路由协议，同时分配同一个自治系统编号。

自治系统之间的链接使用外部路由协议，例如 BGP。

在网络地址前如果是字母C，表示是与路由器直接相连的网络，即已经用NETWORK命令配置的网络。

10 什么是BGP？

BGP(Border Gateway Protocol)是一种在自治系统之间动态交换路由信息的路由协议。一个自治系统的经典定义是在一个管理机构控制之下的一组路由器，它使用 IGP和普通度量值向其他自治系统转发报文。在 BGP中使用自治系统这个术语是为了强调这样一个事实：一个自治系统的管理对于其他自治系统而言是提供一个统一的内部选路计划，它为那些通过它可以到达的网络提供了一个一致的描述。

11 BGP支持的会话种类？

BGP相邻路由器之间的会话是建立在 TCP协议之上的。TCP协议提供一种可靠的传输机制，支持两种类型的会话：

- 外部BGP（EBGP）：是在属于两个不同的自治系统的路由器之间的会话。这些路由器是毗邻的，共享相同的介质和子网。
- 内部BGP（IBGP）：是在一个自治系统内部的路由器之间的会话。它被用来在自治系统内部协调和同步寻找路由的进程。 BGP路由器可以在自治系统的任何位置，甚至中间可以相隔数个路由器。

注意 “初始的数据流的内容是整个BGP路由表。但以后路由表发生变化时，路由器只传送变化的部分。BGP不需要周期性地更新整个路由表。因此，在连接已建立的期间，一个BGP发送者必须保存有当前所有同级路由器共有的整个BGP路由表。BGP路由器周期性地发送KeepAlive消息来确认连接是激活的。当发生错误或特殊情况时，路由器就发送Notification消息。当一条连接发生错误时，会产生一个notification消息并断开连接。”——来自RFC11654、BGP操作。

12 BGP允许路由再分配吗？

允许。因为BGP主要用来在自治系统之间进行路由选择，所以它必须支持 RIP、OSPF和IGRP的路由选择表的综合，以便将它们的路由表转入一个自治系统。 BGP是一个外部路由协议，因此它的操作与一个内部路由协议不同。在 BGP中，只有当一条路由已经存在于 IP路由表中时，才能用NETWORK命令在BGP路由表中创建一条路由。

13 如何显示在数据库中的所有BGP路由？

要显示数据库中的所有BGP路由，只需在EXEC命令行下输入：

```
show ip bgp paths
```

这个命令的输出可能是：

Address	Hash	Refcount	Metric	Path
0x297A9C	0	2	0	i

(续)

Address	Hash	Refcount	Metric	Path
0x30BF84	1	0	0	702 701 ?
0x2F7BC8	2	235	0	?
0x2FA1D8	3	0	0	702 701 i

在这个输出中：

- Address：存储路径的内部地址。
- Hash：存储路径的散列记录
- Refcount：使用这条路径的路由数。
- Metric：指明这条路径的INTER_AS度量值。
- Path：指明路由的AS_PATH属性，接着是路由的起始码。

1.6 水平分割

1 什么是水平分割？

水平分割是一种避免路由环的出现和加快路由汇聚的技术。由于路由器可能收到它自己发送的路由信息，而这种信息是无用的，水平分割技术不反向通告任何从终端收到的路由更新信息，而只通告那些不会由于计数到无穷而清除的路由。

2 路由环是如何产生的？

由于网络的路由汇聚时间的存在，路由表中新的路由或更改的路由不能够很快在全网中稳定，使得有不一致的路由存在，于是会产生路由环。

1.7 度量值

1 什么是度量值？

度量值代表距离。它们用来在寻找路由时确定最优路由。每一种路由算法在产生路由表时，会为每一条通过网络的路径产生一个数值（度量值），最小的值表示最优路径。

度量值的计算可以只考虑路径的一个特性，但更复杂的度量值是综合了路径的多个特性产生的。一些常用的度量值有：

- 跳步数：报文要通过的路由器输出端口的个数。
- Ticks：数据链路的延时（大约1/18每秒）。
- 代价：可以是一个任意的值，是根据带宽，费用或其他网络管理者定义的计算方法得到的。
- 带宽：数据链路的容量。
- 时延：报文从源端传到目的地的时间长短。
- 负载：网络资源或链路已被使用的部分的大小。
- 可靠性：网络链路的错误比特的比率。
- 最大传输单元（MTU）：在一条路径上所有链接可接受的最大消息长度（单位为字节）。

2 IGRP使用什么类型的路由度量值？这个度量值由什么组成？

IGRP使用多个路由度量值。它包括如下部分：

- 带宽：源到目的之间最小的带宽值。
- 时延：路径中积累的接口延时。
- 可靠性：源到目的之间最差的可能可靠性，基于链路保持的状态。
- 负载：源到目的之间的链路在最坏情况下的负载，用比特每秒表示。
- MTU：路径中最小的MTU值。

3 度量值可以修改或调整吗？

加一个正的偏移量。这个命令的完整结构如下：可以使用 OFFSET-LIST ROUTER子命令为访问表中的网络输入和输出度量值添加一个正的偏移量。

```
offset-list {in|out}offset [access-list]
no offset-list {in|out}offset [access-list]
```

如果参数LIST的值是0，那么OFFSET参数将添加到所有的度量值。如果OFFSET的值是0，那么就没有任何作用。对于 IGRP来说，偏移量的值只加到时延上。这个子命令也适用于 RIP和hello路由协议。

使用带适当参数的NO OFFSET-LIST命令可以清除这个偏移量。

在以下的例子中，一个使用IGRP的路由器在所有输出度量值的时延上加上偏移量 10：

```
offset-list out 10
```

下面是一个将相同的偏移量添加到访问表 121上的例子：

```
offset-list out 10 121
```

4 每个路由器在寻找路由时需要知道哪五部分信息？

所有的路由器需要如下信息为报文寻找路由：

- 目的地址：报文发送的目的主机。
- 邻站的确定：指明谁直接连接到路由器的接口上。
- 路由的发现：发现邻站知道哪些网络。
- 选择路由：通过从邻站学习到的信息，提供最优的（与度量值有关）到达目的地的路径。
- 保持路由信息：路由器保存一张路由表，它存储所知道的所有路由信息。

1.8 与其他厂家设备的兼容

1 Cisco路由器支持的路由协议与其他厂家设备的协议兼容吗？

除了IGRP和EIGRP，Cisco路由器支持的所有路由协议都与其他厂家实现的相同协议兼容。IGRP和EIGRP是Cisco的专利产品。

1.9 路由数据库

1 RIP路由表的表项的信息说明了什么？

RIP路由表的每一个表项都提供了一定的信息，包括最终目的地址、到目的地的下一跳地址和度量值。这个度量值表示到目的终端的距离（跳步数）。其他的信息也可以包括

在路由表中，如与路由相关的各种计时器。一个典型的 RIP路由表如表1-2所示。

表1-2 一个典型的RIP路由表

目 的 地	下 一 跳	距离	计 时 器	标 志
Network A	Router 1	3	11，12，13	X，y
Network B	Router 2	5	11，12，13	X，y
Network C	Router 1	2	11，12，13	X，y

1.10 特殊的路由技术

1 如何创建静态路由？

IP ROUTE全局配置命令是用来建立静态路由的。如果路由器不能动态地创建到达目的地的路由，那么可以使用静态路由。命令的格式如下：

```
ip route network mask {address|interface} [distance]
```

在这个命令中：

- network：是目的网络或子网的Internet地址。
- mask：是网络掩码，用来指示网络和子网地址比特。
- address：指明能到达那个网络的路由器的 Internet地址。
- interface：指明到达那个网络要用到的接口的名字。
- distance：指明一个管理距离。

指向一个接口的静态路由（使用参数 INTERFACE指定）通过RIP和IGRP进行广播，不管这些协议是否执行了 REDISTRIBUTE STATIC命令。这是因为指向一个接口的静态路由在路由表中只是被认为是一个连接，而不管它是不是静态的。然而，如果你定义了一条静态路由，它指向一个不是用NETWORK命令定义的网络地址，那么RIP和IGRP都不会通告这条路由。

在下面的例子中，发向网络131.108.0.0的报文将被转发到路由器131.108.6.6：

```
ip router 131.108.0.0 255.255.0.0 131.108.6.6
```

2 什么时候应该禁止水平分割？

连接到IP广播类型的网络上的路由器，如果使用的是距离向量路由协议，那么可以使用水平分割机制避免路由环。水平分割绝不将从接口收到的路由信息在返回发送到该接口。这样可以优化多个路由器之间的数据流，特别是在有链路断开的时候。然而在非广播的网络中，如帧中继和SMDS，这种机制的效果就不太理想。

NO IP SPLIT-HORIZON接口子命令禁止使用水平分割机制：

```
ip split-horizon
no ip split-horizon
```