任务4

局域网互联配置

4.1 项目导引

新起点网络技术有限公司承接的某城市城域网建设项目，在项目已规划设计完成的情况下进行项目实施，前期已完成了设备选购和网络拓扑硬件搭建，并完成了接入层交换机的配置。接下来要进行的工作就是对各县区局域网络的互联配置，主要是对城域网中核心层和汇聚层路由器的配置以及局域网间的互联配置。

从该城域网的网络拓扑中可以看到，网络设计为核心层、汇聚层和接入层三层组成。其中，核心层有 R1 和 R5 两台路由器，汇聚层包括 R2、R3、R4、R6 四台路由器。路由器 R1、R2、R3、R4、R5 划分为 OSPF(或 EIGRP)路由区域，各路由器上运行 OSPF(或 EIGRP)路由协议；路由器 R1、R5、R6 划分为 RIP 路由区域，各路由器上运行 RIP 路由协议。路由器 R1 和 R5 上同时运行 OSPF(或 EIGRP)、RIP 协议。另外，各接入层 VLAN 间的通信需要经过路由器或三层交换机的转发。

4.2 项目分析

我们对该城域网项目进行了分析，在前面已配置环境的基础上，对局域网互联配置任务进行细化，可将项目分解为以下任务：

(1)OSPF 区域：在路由器 R1、R2、R3、R4、R5 上配置单区域 OSPF 路由协议，所连接各接口参与 OSPF 路由更新。

(2)RIP 区域：在路由器 R1、R5、R6 上配置 RIP 路由协议，所连接各接口参与 RIP 路由更新。

(3)因为 R5 是接入 Internet 的出口，在路由器 R5 上配置默认路由重分布，并在 OSPF 和 RIP 路由区域共同实施。

(4)路由注入：路由器 R1、R5 上同时运行了 OSPF 和 RIP 路由协议，需要在路由器 R1、R5 上配置路由注入，在 OSPF 和 RIP 路由间互相注入。

(5)交换机 S5、S6、S7 上配置默认路由。

(6)在路由器 R1 和交换机 S1 间配置单臂路由。

(7)在交换机 S7 上配置三层交换机实现 Vlan 间路由。

4.3 技术准备

本章主要讲解如何使用路由器进行局域网的互联配置,主要内容包括实现 VLAN 间通信,利用静态路由、动态路由协议实现局域网的互联。

路由器的主要功能是将数据包转发到目的网络,即转发到数据包目的 IP 地址。为此,路由器需要搜索存储在路由表中的路由信息。路由表是保存在路由器的存储器 RAM 中的数据文件,其中存储了与直连网络以及远程网络相关的信息。路由表包含网络与下一跳的关联信息。这些关联告知路由器要以最佳方式到达某一目的地,可以将数据包发送到特定路由器(即在到达最终目的地途中的"下一跳")。下一跳也可以关联到通向最终目的地的送出接口。

网络/送出接口关联还可以表示 IP 数据包的目的网络地址。这种关联发生在与路由器直连的网络。直连网络就是直接连接到路由器某一接口的网络。当路由器接口配置有 IP 地址和子网掩码时,此接口即成为该相连网络的主机。接口的网络地址和子网掩码以及接口类型和编号都将直接输入路由表,用于表示直连网络。路由器若要将数据包转发到某一主机(如 Web 服务器),则该主机所在的网络应该是路由器的直连网络。

远程网络就是间接连接到路由器的网络,也就是非直连网络以外的其他网络。要将远程网络添加到路由表中,可以使用动态路由协议,也可以通过配置静态路由来实现。动态路由是路由器通过动态路由协议自动获知的远程网络路由。静态路由是网络管理员手动配置的网络路由。通过 show ip route 命令可以查看路由表。可以看出,在此路由表中仅有与该路由器直连的网络,分别是 172.16.2.0 和 172.16.3.0。

```
R1#show  ip  route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, 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

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.2.0 is directly connected, Serial0/0/0                    C表示直连路由
C       172.16.3.0 is directly connected, FastEthernet0/0
```

对于路由表中列出的每个网络,都可以看到以下信息:

◆ C:此列中的信息指示路由信息的来源是直连网络、动态路由还是动态路由协议。C 表

示直连路由。

◆ 172.16.2.0/24：这是直连网络或远程网络的网络地址和子网掩码。在本例中，路由表的两个条目 172.16.2.0/24 和 172.16.3.0/24 都是直连网络。

◆ FastEthernet 0/0：路由的出口，表示送出接口和(或)下一跳路由器的 IP 地址。在本例中，FastEthernet0/0 和 Serial0/0/0 都是用于到达目的网络的送出接口。

当路由表包含远程网络的路由条目时，还会包括额外的信息，如路由度量和管理距离等，我们将在后面的内容中学习到。所有配置了 IP 的设备都会有路由表。例如 PC 也有路由表。可以通过 route print 命令显示所配置或获得的网关、相连网络、回环网络、组播网络和广播网络，如图 4-1 所示。

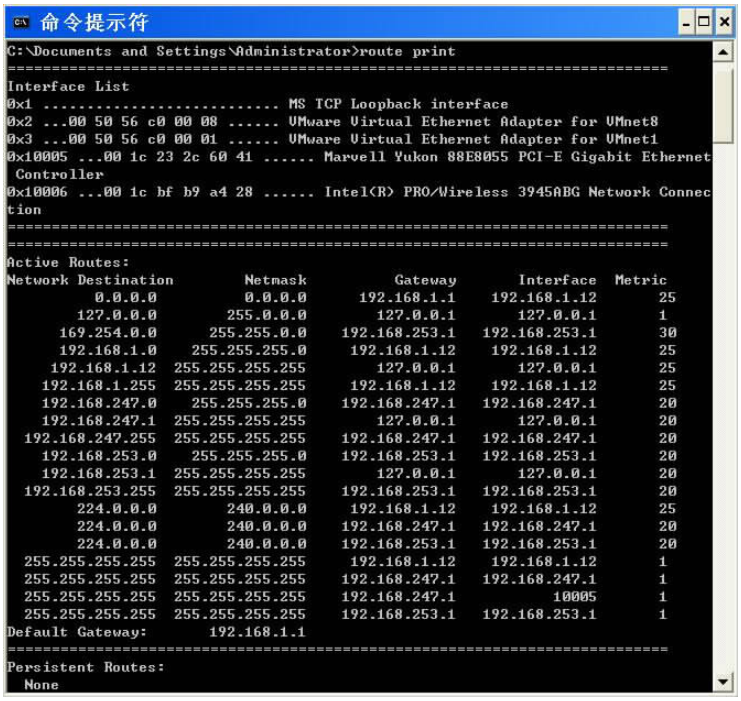


图 4-1　PC 机的 route print 输出

理解路由表的三大原理可以帮助我们理解、配置和排查路由问题。这些原理来自于 Alex Zinin 的著作 Cisco IP Routing。

(1)每台路由器根据其自身路由表中的信息独立作出决策。

(2)一台路由器的路由表中包含某些信息并不表示其他路由器也包含相同的信息。

(3)有关两个网络之间路径的路由信息并不能提供反向路径(即返回路径)的路由信息。

因为各个路由器的路由表中保存的信息不尽相同，所以数据包可以沿网络中的一条路径传送，而有可能会通过另一条路径返回，我们将这种情况称为非对称路由。

4.3.1　知识点 1：VLAN 间通信

1. 单臂路由简介

“单臂路由器”是通过单个物理接口在网络中的多个 VLAN 之间发送流量的路由器配置。如图 4-2 所示。路由器接口被配置为中继链路，并以中继模式连接到交换机端口。子接口是基

于软件的、与同一物理接口相关联的虚拟接口，可分配到各物理接口。这些子接口在路由器的软件中配置，每个子接口配置有自己的 IP 地址、子网掩码和唯一的 VLAN 分配，使单个物理接口可同属于多个逻辑网络。根据各自的 VLAN 分配，子接口被配置到不同的子网，以便在数据帧被标记 VLAN 并从物理接口发送回之前进行逻辑路由。这种方法适用于在网络中有多个 VLAN 但只有少数路由器物理接口的 VLAN 间路由。路由器通过接收中继接口上来自相邻交换机 VLAN 标记流量，以及通过子接口在 VLAN 之间进行内部路由，路由器便可实现 VLAN 间路由。随后，路由器会将发往目的 VLAN 的 VLAN 标记流量从同一物理接口转发出去。

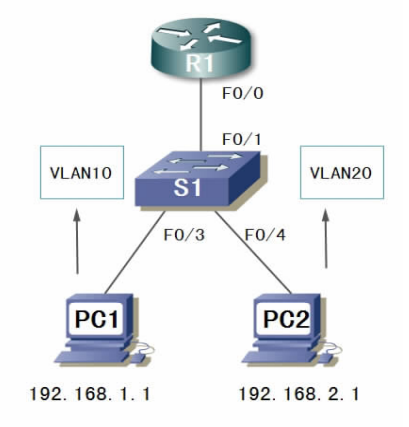


图 4-2 单臂路由

2. 配置单臂路由器 VLAN 间路由

使用单臂路由器模式配置 VLAN 间路由时，路由器的物理接口必须与相邻交换机的中继链路相连接。子接口针对网络上唯一的 VLAN/子网创建。每个子接口都分配有所属子网的 IP 地址，并对与其交互的 VLAN 帧添加 VLAN 标记。这样，路由器可以在流量通过中继链路返回交换机时区分不同子接口的流量。配置路由器子接口与配置物理接口类似，不同之处是需要创建子接口并分配到 VLAN。

下面，以图 4-2 为例讲解单臂路由器 VLAN 间路由的配置。配置路由器之前，首先应配置将与其相连的交换机。

```
S1(config)#VLAN  10
S1(config-VLAN)# exit
S1(config)#VLAN  20
S1(config-VLAN)#exit
S1(config)#interface  f0/1
S1(config)#switchport  mode  trunk
S1(config)# interface  f0/3
S1(config-if)#switchport  access  VLAN  10
S1(config)# interface  f0/4
S1(config-if)#switchport  access  VLAN  20
```

配置路由器如下：

```
R1(config)# interface  f0/0.10
```

```
R1(config-subif)# encapsulation  dot1q  10
R1(config-subif)# ip  address  192.168.1.1  255.255.255.0
R1(config-subif)# interface  f0/0.20
R1(config-subif)#encapsulation  dot1q  20
R1(config-subif)# ip  address  192.168.2.1  255.255.255.0
R1(config-subif)#interface  f0/0
R1(config-if)# no  shutdown
```

子接口编号可配置，但通常设置为 VLAN 的编号。本例中，使用 10 和 20 作为子接口编号，以便记住相关联的 VLAN。将 IP 地址分配给子接口之前，需要使用 encapsulation dot1q VLAN id 命令配置子接口，使之在特定 VLAN 上运行。

只要物理接口通过 no shutdown 命令启用后，配置的所有子接口都会被启用。如果物理接口被禁用，所有子接口都会被禁用。

路由器通过路由表确定所接收流量的发送位置。在路由器特权模式下使用 show ip route 命令查看路由表，从图中可以看到，路由表中有 2 个直连网络，分别是 VLAN10、20 所对应的网络。

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, 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

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0.10
C       172.16.3.0 is directly connected, FastEthernet0/0.20
```

使用中继链路的好处在于节省了路由器和交换机的端口。这样，不仅节约了成本，还降低了配置的复杂性。因此，相对于每个 VLAN 配置一个物理接口的配置设计，配置路由器子接口更适合有许多 VLAN 的网络。物理接口和子接口都可用于执行 VLAN 路由。但两者各有优缺点，主要区别如下：

(1)端口限制。与物理接口相比，子接口方式允许路由器容纳更多的 VLAN。对于有许多 VLAN 的大型环境下的 VLAN 间路由，更适合使用有多个子接口的单个物理接口。

(2)性能比较。由于独立的物理接口无带宽争用现象，与子接口相比，物理接口的性能更好。子接口用于 VLAN 间路由时，被发送的流量会争用单个物理接口的带宽。网络繁忙时，会导致通信瓶颈。为均衡物理接口上的流量负载，可将子接口配置在多个物理接口上，以减轻 VLAN 流量之间竞争带宽的现象。

(3)端口模式不同。要连接物理接口用于 VLAN 间路由，需要将交换机端口配置为接入端

口。而使用子接口则需要将交换机端口配置为中继接口,以接收中继链路上的 VLAN 标记流量。

(4)成本比较。从成本方面来说,使用子接口方式只需要一个路由器物理接口和一个交换机物理接口,比传统的独立物理接口更经济。

(5)复杂性。如果使用子接口进行 VLAN 间路由,由于电缆数量少,交换机上的电缆连接并不混乱。由于 VLAN 在单条链路上进行中继,更易于排查物理连接的故障。但是,使用配有中继端口的子接口会使软件配置更为复杂,不利于排查软件配置故障。在单臂路由器模式下,只使用单个接口来支持所有不同的 VLAN。如果某个 VLAN 路由到其他 VLAN 时出现故障,不能只查看电缆插入的端口是否正确。应查看交换机端口是否被配置为中继,并确保在到达路由器接口之前该 VLAN 不通过任何中继链路过滤。还需检查路由器子接口的配置,是否使用了该 VLAN 所关联子网的正确 VLAN ID 和 IP 地址。

3. 三层交换机实现 VLAN 间路由

利用三层交换机也可以实现 VLAN 间通信问题。实际上,在局域网内部多采用三层交换进行 VLAN 间的通信。三层交换机通常采用硬件来实现路由,其路由数据包的速率是普通路由器的几倍。设置方法也很简单,只需要在三层交换机上创建相应的 VLAN 虚接口,并在接口上配置 IP 地址,PC 的网关指向三层交换机上本 VLAN 的 IP 地址即可。

```
Switch(config)# ip  routing  //三层交换机上启用路由功能
Switch(config)# interface  vlan  10
Switch(config-if)# ip  address 192.168.2.1 255.255.255.0  //配置 VLAN10 的 IP,即 VLAN10 的默认网关
Switch(config)# interface  f0/0
Switch(config-if)# no  switchport //开启物理接口的三层路由功能
```

三层交换机是带有三层路由功能的交换机,也就是这台交换机的端口既有三层路由功能,也有二层交换功能。三层交换机端口默认为二层口,如果需要启用三层功能就需要在此端口输入本命令“no switchport”,这样就可以在该端口配置 IP 地址和路由口一样了,使用命令“switchport”把端口恢复成二层口。

4.3.2 知识点 2:静态路由实现网络互联

1. 直连路由

路由器有多个接口,每个接口必须是不同网络的一员。配置路由器的接口并使用 no shutdown 命令将其激活后,该接口必须收到来自其他设备(路由器、交换机、集线器等)的载波信号,其状态才能视为“up”(开启)。一旦接口为“up”(开启)状态,该接口所在的网络就会作为直连网络而加入路由表。

在路由器上配置静态或动态路由之前,路由器只知道与自己直连的网络。这些网络是在配置静态或动态路由之前唯一显示在路由表中的网络。直连网络对于路由决定起着重要作用。如果路由器没有直连网络,也就不会有静态和动态路由的存在。如果路由器接口未启用 IP 地址和子网掩码,路由器就不能从该接口将数据包发送出去,正如在以太网接口未配置 IP 地址和子网掩码的情况下,PC 也不能将 IP 数据包从该接口发送出去。

(1)获取直连路由

show ip route 命令可显示路由表的内容。路由表是一种数据结构,用于存储从其他源获得的路由信息。路由表的主要用途是为路由器提供通往不同目的网络的路径。

路由表包含一组“已知”网络地址,即那些直接相连、静态配置以及动态获知的地址。

在网络拓扑图 4-3 中,R1 和 R2 只有直连网络的路由。路由表中路由条目中的“C”表示 connected 直连路由。

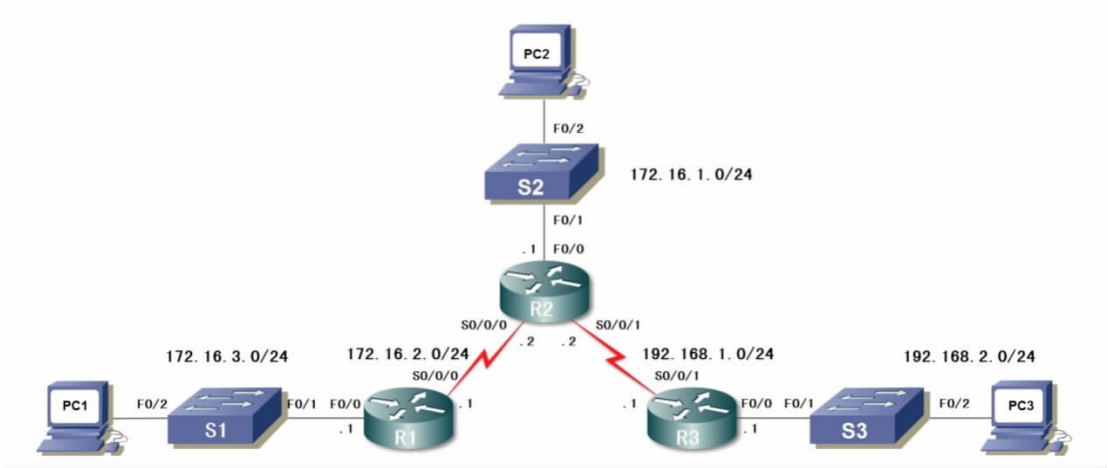


图 4-3　静态路由配置拓扑

```
R1#show  ip  route
 * * * * * *
Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
```

如果一台路由器只配置了接口,并且路由表中只含直连网络、没有其他路由,则只可以到达那些直连网络上的设备。如果路由器只知道与其直连的网络,也就是说,该路由器的路由表中只含有直连路由,那么该路由器就只能与直连网络上的设备通信。

(2)Cisco 发现协议(CDP)

Cisco 发现协议(Cisco Discovery Protocol,CDP)是功能强大的网络监控与故障排除工具,可以使用 CDP 作为信息收集工具,通过它来收集与直连的思科设备有关的信息。CDP 是思科的一款专有工具,它工作在数据链路层。通过它可以了解与直连思科设备有关的协议与地址概要信息。默认情况下,每台思科设备会定期向直连的思科设备发送消息,我们将这种消息称为 CDP 通告。这些通告包含特定的信息,如连接设备的类型、设备所连接的路由器接口、用于进行连接的接口以及设备型号等。

大多数网络设备本身都不是独立工作的。在网络中,思科设备通常都会有其他相邻的思科设备。从其他设备收集到的信息有助于设计网络、排除故障以及调整设备。缺少网络拓扑记录或缺乏详细信息时,您可将 CDP 作为网络发现工具,利用它来构建网络逻辑拓扑结构。

思科设备启动时会默认启动 CDP。CDP 会自动发现运行 CDP 的邻居设备,无论这些设备

运行的是何种协议或协议簇，CDP 会与直连的 CDP 邻居交换硬件和软件设备信息。

(3)通过 CDP 获取网络信息

我们可以通过 show cdp neighbors 和 show cdp neighbors detail 命令查看网络设备的 CDP 邻居信息。以图 4-3 为例，如查看 R2 的 CDP 邻居信息如下，可以看出 R2 的 CDP 邻居有 3 个，分别是 R1、R3、S2。

```
R2 # show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform      Port ID
R1           Ser 0/0/0         160          R        C1841        Ser 0/0/0
R3           Ser 0/0/1         127          R        C1841        Ser 0/0/1
S2           Fas 0/0           144          S        2960          Fas 0/1
```

通过 show cdp neighbors 命令，可以获取 CDP 邻居设备的以下信息：

- Device ID：邻居设备 ID，例如为交换机配置的主机名；
- Local Intrfce：本地接口；
- Holdtme：保持时间(以秒为单位)；
- Capability：邻居设备功能代码。例如，该设备是路由器还是交换机；
- Platform：邻居硬件平台，例如 Cisco 7200 系列路由器；
- Port ID：邻居远程端口 ID。

通过 show cdp neighbors detail 命令也会显示邻居设备的 IP 地址。无论是否能 ping 通邻居，CDP 都会显示邻居的 IP 地址。当两台 Cisco 路由器无法通过共享的数据链路进行路由时，此命令非常有用。show cdp neighbors detail 命令也有助于确定某个 CDP 邻居是否存在 IP 配置错误。

对于网络发现，通常只要知道 CDP 邻居的 IP 地址就能 telnet 到该设备。通过所建立的 Telnet 会话，便可收集与邻居直连的 Cisco 设备有关的信息。按照这种方式，您可以 telnet 遍整个网络，并据此构建逻辑拓扑。

CDP 的使用会给网络带来安全风险。例如，CDP 会给邻居设备发送 CDP 通告，通过在网络中捕获这些数据包，来了解网络信息。如果需要对整台设备彻底禁用 CDP，可以在全局模式下使用 no cdp run 命令。如果要使用 CDP 但需要针对特定接口停止 CDP 通告，可以在该接口模式下使用 no cdp enable 命令。

2. 配置静态路由

通过配置静态路由或启用动态路由协议，可以将远程网络添加至路由表。当 IOS 获知远程网络及用于到达远程网络的接口时，只要送出接口为 up 状态，它就会将该路由添加到路由表中。

静态路由包括远程网络的网络地址和子网掩码，以及下一跳路由器或送出接口的 IP 地址。直连路由在路由表中以代码 C 表示，而静态路由在路由表中以代码 S 表示(S 即 Static)。

在以下情况中应使用静态路由：

- 网络中仅包含几台路由器。在这种情况下，如果使用动态路由协议可能会增加额外的管理负担，没有任何实际好处。

◆ 网络仅通过单个 ISP 接入 Internet。因为该 ISP 就是唯一的 Internet 出口点，网络只能通过一条路径到达其他目的地，所以不需要在此链路间使用动态路由协议。

◆ 以集中星型拓扑结构配置的大型网络。集中星型拓扑结构由一个中心点和多个分散点组成，其中每个分散点到中心点只有一条连接，所以不需要使用动态路由。

通常，大多数路由表中同时含有静态路由和动态路由。但是，前提是路由表必须首先包含用于访问远程网络的直连网络，然后才能使用任何静态或动态路由。

(1)静态路由配置命令

静态路由可以在全局模式下使用 ip route 命令进行配置。路由器可通过两种方式获知远程网络：

◆ 手动配置，通过配置的静态路由获知。

◆ 自动获取，通过动态路由协议获知。

使用 ip route 命令配置静态路由的语法是：

```
Router(config)# ip route network-address subnet-mask {ip-address | exit-interface }
```

下面，我们对各参数进行详细解释：

◆ network-address：要加入路由表的远程网络的目的网络地址。

◆ subnet-mask：要加入路由表的远程网络的子网掩码。此子网掩码可以为一组总结网络的掩码，后面会进行相关内容的学习。

◆ ip-address：一般指下一跳路由器上与本路由器直连的接口 IP 地址。

◆ exit-interface：将数据包转发到目的网络时使用的送出接口。

其中，参数{ip-address | exit-interface }可以使用一个或两个。

(2)配置带下一跳 IP 地址的静态路由

以图 4-3 为例学习带下一跳 IP 地址的静态路由配置。首先，需要配置所有网络设备的基本接口信息，如表 4-1 所示。

表 4-1　　**网络设备基本信息**

设备名称	接口	IP 地址	子网掩码	网关
R1	F0/0	172.16.3.1	255.255.255.0	
	S0/0/0	172.16.2.1	255.255.255.0	
R2	F0/0	172.16.1.1	255.255.255.0	
	S0/0/0	172.16.2.2	255.255.255.0	
	S0/0/1	192.168.1.2	255.255.255.0	
R3	F0/0	192.168.2.1	255.255.255.0	
	S0/0/1	192.168.1.1	255.255.255.0	
PC1		172.16.3.2	255.255.255.0	172.16.3.1
PC2		172.16.1.2	255.255.255.0	172.16.1.1
PC3		192.168.2.2	255.255.255.0	192.168.2.1

首先在各路由器特权模式下启用 debug ip routing，使 IOS 在新路由添加到路由表中时显示相关消息。因为三台路由器只配置了基本接口信息，因此路由器的路由表中只含有直连网络

的路由信息，例如 R1 的路由表如下：

```
R1#show ip route
     * * * * * *
     Gateway of last resort is not set

          172.16.0.0/24 is subnetted, 2 subnets
     C       172.16.2.0 is directly connected, Serial0/0/0
     C       172.16.3.0 is directly connected, FastEthernet0/0
```

debug ip routing 的输出表明该路由已添加至路由表。在 R1 上输入 show ip route 命令查看新路由表，可以看出我们新添加的静态路由已加入路由表。

```
R1# show ip route
     * * * * * *
     Gateway of last resort is not set

          172.16.0.0/24 is subnetted, 3 subnets
     S       172.16.1.0 [1/0] via 172.16.2.2                    S 表示静态路由
     C       172.16.2.0 is directly connected, Serial0/0/0
     C       172.16.3.0 is directly connected, FastEthernet0/0
     S    192.168.1.0/24 [1/0] via 172.16.2.2
     S    192.168.2.0/24 [1/0] via 172.16.2.2
```

下面对路由表的输出进行分析：

◆ S：路由表中表示静态路由的代码。

◆ 172.16.1.0：该路由的目的网络地址。

◆ /24：该路由的子网掩码；该掩码显示在上一行(即父路由)中。

◆ [1/0]：该静态路由的管理距离和度量。

◆ via 172.16.2.2：下一跳路由器的 IP 地址，即 R2 上 Serial 0/0/0 接口的 IP 地址。目的 IP 地址前 24 位与 172.16.1.0 前 24 位匹配的所有数据包都将使用此路由转发数据包。

除了 show ip route 命令外，也可以使用 show running-config 命令来验证静态路由配置。配置完成后，最好将配置保存到 NVRAM，以免配置丢失。

```
R1#copy running-config startup-config
```

(3)将下一跳 IP 解析到送出接口。

在路由器转发任何数据包之前，路由表过程必须确定用于转发数据包的送出接口，我们将此过程称为路由解析。下面，我们将以 R1 的路由表为例来学习这一过程。

```
S    192.168.2.0/24 [1/0] via172.16.2.2
```

R1 的路由表中有到达远程网络 192.168.2.0/24 的静态路由，该路由会将所有数据包转发至下一跳 IP 地址 172.16.2.2。查找路由只是查询过程的第一步。R1 必须确定如何到达下一跳 IP 地址 172.16.2.2。它将进行第二次搜索，以查找与 172.16.2.2 匹配的路由。在本例中，IP 地址 172.16.2.2 与下面这条直连路由相匹配。

```
C       172.16.2.0 is directly connected,Serial0/0/0
```

172.16.2.0 路由是一个直连网络，送出接口为 Serial 0/0/0。此次查找告知路由表过程数

据包将从此接口转发出去。因此，将任何数据包转发到 192.168.2.0/24 网络实际上经过了两次路由表查找过程。如果路由器在转发数据包前需要执行多次路由表查找，那么它的查找过程就是一种递归查找。对于只具有下一跳 IP 地址而且没有指定送出接口的每一条路由，都必须使用路由表中有送出接口的另一条路由来解析下一跳 IP 地址。通常，这些路由将解析为路由表中直连网络的路由，因为这些条目始终包含送出接口。

(4)配置带送出接口的静态路由

以图 4-3 为例，也可以使用另外一种方法来配置这些静态路由。前面我们已经介绍过，如果使用带下一跳 IP 地址的静态路由，那么需要再进行一次路由表查找才能将下一跳 IP 地址解析到送出接口。而大多数静态路由都可以配置送出接口，这使得路由表可以在一次搜索中解析出送出接口，而不用进行两次搜索节省路由查找时间。

使用 show ip route 命令检查 R1 路由表的变化。我们看到路由表中的这些条目不再使用下一跳 IP 地址，而是直接指向送出接口。此送出接口与该静态路由使用下一跳 IP 地址时最终解析出的送出接口相同。那么当路由表过程发现数据包与该静态路由匹配时，它查找一次便能将路由解析到送出接口。

(5)修改静态路由

如果出现以下情况时，我们需要对以前配置的静态路由进行修改：

◆ 目的网络不再存在，此时应删除相应的静态路由。

◆ 拓扑发生变化，所以中间地址或送出接口必须相应进行修改。

对已配置静态路由的修改方法是：必须将现有静态路由删除，然后重新配置。

要删除静态路由，只需在用于添加静态路由的 ip route 命令前添加 no 即可。如想要静态路由 R1(config)#ip route 192.168.2.0 255.255.255.0 172.16.2.2，可以使用 no ip route 命令删除这条静态路由 R1(config)#no ip route 192.168.2.0 255.255.255.0 172.16.2.2。

(6)检验静态路由配置

无论对静态路由或网络的其他方面进行了何种修改，都需要进行检查，以确保更改生效而且最终结果与预期的一致。可以使用 show ip route 和 show running-config 命令检验。

```
R1#show ip route
     * * * * * *
     Gateway of last resort is not set

          172.16.0.0/24 is subnetted, 3 subnets
     S       172.16.1.0 is directly connected, Serial0/0/0
     C       172.16.2.0 is directly connected, Serial0/0/0
     C       172.16.3.0 is directly connected, FastEthernet0/0
     S    192.168.1.0/24 is directly connected, Serial0/0/0
     S    192.168.2.0/24 is directly connected, Serial0/0/0
R1#show running-config
     * * * * * *
     !
     ip classless
     ip route 172.16.1.0 255.255.255.0 Serial0/0/0
```

```
ip route 192.168.1.0 255.255.255.0 Serial0/0/0
ip route 192.168.2.0 255.255.255.0 Serial0/0/0
!
line con 0
line vty 0 4
login
!
end
```

(7)两种静态路由配置的不同应用

带送出接口的静态路由可提高路由表的查找效率,使用送出接口而不是下一跳 IP 地址配置的静态路由是大多数串行点对点网络的理想选择。使用如 HDLC 和 PPP 之类协议的点对点网络在数据包转发过程中不使用下一跳 IP 地址。路由后的 IP 数据包被封装成目的地址为第 2 层广播地址的 HDLC 第 2 层帧。这种类型的点对点串行链路类似于管道。管道只有两个端点,从一端进入的数据只有一个目的地,即管道的另一端。在前面的配置例子中,任何通过 R1 的 Serial 0/0/0 接口发送的数据包都只能到达一个目的地:R2 的 Serial 0/0/0 接口。R2 的串行接口 IP 地址恰好为 172.16.2.2。

但有时送出接口是以太网络。假设 R1 和 R2 之间的网络链路为以太网链路,并且 R1 的 FastEthernet 0/1 接口连接到该网络,如图 4-4 所示。我们可以使用以下命令设置一条 R1 到 192.168.1.0/24网络的静态路由:

```
R1(config)# ip route 192.168.1.0 255.255.255.0 172.16.2.2
```

我们知道,IP 数据包必须封装成带以太网目的 MAC 地址的以太网帧。如果数据包应该发送到下一跳路由器,则目的 MAC 地址将是下一跳路由器的以太网接口地址。在此情况下,以太网目的 MAC 地址必须与下一跳 IP 地址 172.16.2.2 匹配。R1 会在自己的 FastEthernet 0/1 ARP 表中查找 172.16.2.2,并据此获得相应的 MAC 地址。如果该条目不在 ARP 表中,R1 会通过 FastEthernet 0/1 接口发出一个 ARP 请求。第 2 层广播请求 IP 地址为 172.16.2.2 的设备告知其 MAC 地址。因为 R2 的 FastEthernet 0/1 接口的 IP 地址为 172.16.2.2,所以它会发送包含该接口 MAC 地址的 ARP 应答。R1 收到该 ARP 应答,随后将 IP 地址 172.16.2.2 及其关联的 MAC 地址添加到自身的 ARP 表中。接着,R1 使用 ARP 表中找到的目的 MAC 地址将 IP 数据包封装成以太网帧。封装有数据包的以太网帧随后从 FastEthernet 0/1 接口发送到路由器 R2。

现在我们将把静态路由配置为使用以太网送出接口,而不是下一跳 IP 地址。使用以下命令将 192.168.1.0/24 的静态路由更改为使用送出接口:

```
R1(config)# ip route 192.168.1.0 255.255.255.0 fastethernet 0/1
```

以太网络和点对点串行网络之间的区别在于,点对点网络只有一台其他设备位于网络中,即链路另一端的路由器。而对于以太网络,可能会有许多不同的设备共享相同的多路访问网络,包括主机甚至多台路由器。如果仅仅在静态路由中指定以太网送出接口,路由器就没有充足的信息来决定哪台设备是下一跳设备。在本例中,R1 知道数据包需要封装成以太网帧并从 FastEthernet 0/1 接口发送出去。但是,R1 不知道下一跳的 IP 地址,因此它无法决定该以太网帧的目的 MAC 地址。根据拓扑结构和其他路由器上的配置,该静态路由或许能正常工作,

也或许不能。因此建议当送出接口是以太网络时，不要在静态路由中仅使用送出接口。

我们可以在以太网中配置这样一条静态路由，使它不必通过递归查找获得下一跳 IP 地址，即通过在静态路由中同时包含送出接口和下一跳 IP 地址来实现。

```
R1(config)# ip route 192.168.1.0 255.255.255.0 fastethernet 0/1 172.16.2.2
```

该路由的路由表条目应该是：

```
S   192.168.1.0/24 [1/0] via 172.16.2.2 FastEthernet0/1
```

路由表过程仅需要执行一次查找就可以同时获得送出接口和下一跳 IP 地址。

对于串行点对点网络和以太网出站网络来说，在静态路由中使用送出接口都比较有利。路由表过程只需要执行一次查找就可以找到送出接口，不必为了解析下一跳地址再次进行查找。对于使用出站点对点串行网络的静态路由，最好只配置送出接口。对于点对点串行接口，数据包传送程序从不使用路由表中的下一跳地址，因此不需要配置该地址。对于使用出站以太网络的静态路由，最好同时使用下一跳地址和送出接口来配置。如图 4-4 所示。

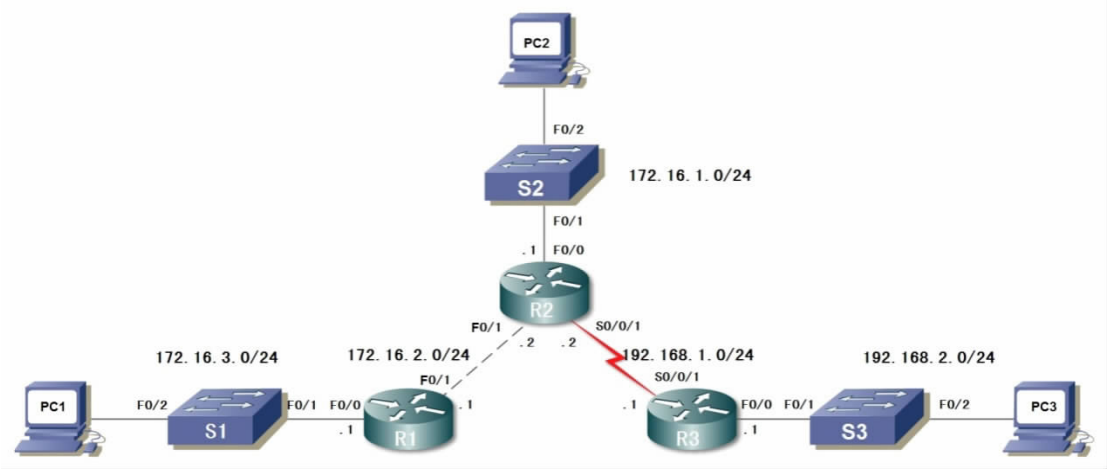


图 4-4　两种静态路由的对比

3. 静态路由总结和默认静态路由

(1)配置总结静态路由

较小的路由表可以使路由表查找过程更加有效率，因为需要搜索的路由条数更少。如果可以使用一条静态路由代替多条静态路由，则可减小路由表。在许多实际应用中，一条静态路由可用于代表数十、数百、甚至数千条路由。我们可以使用一个网络地址代表多个子网。例如，192.168.1.0/24、192.168.2.0/24、192.168.3.0/24、192.168.4.0/24、192.168.5.0/24 …… 192.168.255.0/24 所有这些网络都可以用一个网络地址代表：192.168.0.0/16。

多条静态路由可以总结成一条静态路由，称为路由总结。但前提是同时满足以下条件：

- 目的网络可以总结成一个网络地址；
- 这些静态路由都使用相同的送出接口或下一跳 IP 地址。

我们仍然以图 4-3 为例，R3 有三条静态路由。所有三条路由都通过相同的 Serial0/0/1 接口转发通信。R3 上的这三条静态路由分别是：

```
ip route 172.16.1.0 255.255.255.0 Serial0/0/1
ip route 172.16.2.0 255.255.255.0 Serial0/0/1
ip route 172.16.3.0 255.255.255.0 Serial0/0/1
```

可以看出，这三条静态路由满足路由总结的两个前提条件，因此可以将这些路由总结成一条静态路由。172.16.1.0/24、172.16.2.0/24 和 172.16.3.0/24 可以总结成 172.16.0.0/22 网络。因为所有三条路由使用相同的送出接口，而且它们可以总结成一个 172.16.0.0 255.255.252.0 网络，所以我们可以创建一条总结路由。

以下为创建总结路由 172.16.1.0/22 的过程，如图 4-5 所示。

①以二进制格式写出想要总结的网络地址。

②找出用于总结的子网掩码，从最左侧的位开始。

③从左向右，找出所有连续匹配的位。

④当发现有位不匹配时，立即停止。当前所在的位即为总结边界。

⑤计算从最左侧开始的匹配位数，本例中为 22。该数字即为总结路由的子网掩码，本例中为 /22 或 255.255.252.0。

⑥找出用于总结的网络地址，方法是复制匹配的 22 位并在其后用 0 补足 32 位。

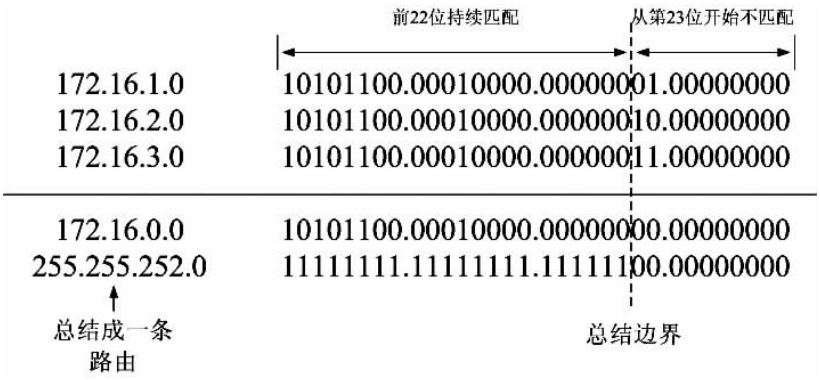


图 4-5 路由总结示意图

通过上述步骤，我们便可将 R3 上的三条静态路由总结成一条静态路由，该路由使用总结网络地址 172.16.0.0 255.255.252.0：ip route 172.16.0.0 255.255.252.0 Serial0/0/1。

要使用总结路由，我们必须首先删除当前的三条静态路由，然后配置总结静态路由：

```
R3(config)# ip route 172.16.0.0 255.255.252.0 serial0/0/1
```

通过这条总结路由，数据包的目的 IP 地址仅需要与 172.16.0.0 网络地址最左侧的 22 位匹配。而目的 IP 地址属于 172.16.1.0/24、172.16.2.0/24 或 172.16.3.0/24 网络的所有数据包都与这条总结路由匹配。

(2)配置默认静态路由

数据包的目的 IP 地址可能会与路由表中的多条路由匹配。例如，假设路由表中有以下两条静态路由：

```
192.168.0.0/24 is subnetted, 3 subnets
S   192.168.1.0 is directly connected, Serial0/0/0
S   192.168.0.0/16 is directly connected, Serial0/0/1
```

考虑目的 IP 地址为 192.168.1.10 的数据包。该 IP 地址同时与这两条路由匹配。路由表查找过程将使用最精确匹配。因为 192.168.1.0/24 路由有 24 位匹配，而 192.168.0.0/16

路由仅有 16 位匹配，所以将使用有 24 位匹配的静态路由，即最长匹配。随后，数据包被封装成第 2 层帧并通过 Serial 0/0/0 接口发送出去。路由条目中的子网掩码决定数据包的目的 IP 地址必须有多少位匹配才能使用这条路由。

注：此过程对于路由表中的所有路由（包括静态路由、通过路由协议获知的路由以及直连网络）均相同。

默认静态路由是与所有数据包都匹配的路由。出现以下情况时，便会用到默认静态路由：

路由表中没有其他路由与数据包的目的 IP 地址匹配。也就是说，路由表中不存在更为精确的匹配。在公司网络中，连接到 ISP 网络的边缘路由器上往往会配置默认静态路由。如果一台路由器仅有另外一台路由器与之相连，该路由器即称为末节路由器。

配置默认静态路由的语法：

```
Router(config)# ip route 0.0.0.0 0.0.0.0 [exit-interface | ip-address ]
```

其中，0.0.0.0 0.0.0.0 网络地址和掩码也称为“全零”路由。

我们仍然以图 4-3 为例，路由器 R1 上有三条静态路由，通过这些路由可以到达拓扑中的远程网络。并且这三条静态路由的送出接口都是 Serial 0/0/0，并且转发数据包的下一跳路由器都是 R2。通过前面的学习，我们知道 R1 上的三条静态路由分别是：

```
ip route 172.16.1.0 255.255.255.0 serial 0/0/0
ip route 192.168.1.0 255.255.255.0 serial 0/0/0
ip route 192.168.2.0 255.255.255.0 serial 0/0/0
```

在本例中，路由器 R1 上我们可以用一条默认静态路由来取代所有静态路由。首先，删除这三条静态路由，然后配置一条有相同送出接口 Serial 0/0/0 的默认静态路由：

```
R1(config)# ip route 0.0.0.0 0.0.0.0 serial 0/0/0
```

下面，在 R1 的特权模式下输入 show ip route 命令查看当前路由表：

```
R1# show ip route
     * * * * * *
     Gateway of last resort is 0.0.0.0 to network 0.0.0.0

          172.16.0.0/24 is subnetted, 2 subnets
     C       172.16.2.0 is directly connected, Serial0/0/0
     C       172.16.3.0 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 is directly connected, Serial0/0/0                    *(星号)表示默认路由
```

从上面的代码我们可以看到，* 星号表明该静态路由是一条默认路由，S * 表示这是一条默认静态路由。

我们知道，路由表中的子网掩码决定着数据包的目的 IP 地址与路由表中的路由之间必须有多少位匹配。/0 掩码表示只需要有零位匹配（即无需匹配）。只要不存在更加精确的匹配，则默认静态路由将与所有数据包匹配。

在路由器的路由配置中，默认路由是常用配置。这样，路由器便不需要存储通往 Internet 中所有网络的路由，而可以存储一条默认路由来代表不在路由表中的任何网络。

4.3.3　知识点 3：用 RIP 实现网络互联

前面我们学习了使用静态路由配置网络互联，下面学习使用动态路由协议进行网络互联的

配置。在大型网络中通常采用动态路由协议，与仅使用静态路由相比，可以减少管理和运行方面的成本。一般情况下，网络会同时使用动态路由协议和静态路由。在大多数网络中，通常只使用一种动态路由协议，但是也存在网络的不同部分使用不同路由协议的情况。

1. 动态路由协议

(1)动态路由协议介绍

动态路由协议是用于路由器之间交换路由信息的协议。通过动态路由协议，路由器可以动态共享有关远程网络的信息，并自动将信息添加到各自的路由表中。路由协议可以确定到达各个网络的最佳路径，然后将路径添加到路由表中。使用动态路由协议的一个主要的好处是，只要网络拓扑结构发生了变化，路由器就会相互交换路由信息。通过这种信息交换，路由器不仅能够自动获知新增加的网络，还可以在当前网络连接失败时找出备用路径。路由协议由一组处理进程、算法和消息组成，用于交换路由信息，并将其选择的最佳路径添加到路由表中。路由协议的功能包括：

- 发现远程网络；
- 维护最新路由信息；
- 选择通往目的网络的最佳路径；
- 当前路径无法使用时找出新的最佳路径。

网络发现是路由协议的一项功能，通过该功能路由器能够与使用相同路由协议的其他路由器共享网络信息。动态路由协议使路由器能够自动地从其他路由器获知远程网络，这样便无需在每台路由器上配置指向这些远程网络的静态路由。这些网络以及到达每个网络的最佳路径将添加到路由器的路由表中，并被标记为通过特定动态路由协议获知的网络。在初次网络发现后，动态路由协议将更新并维护其路由表中的网络。动态路由协议不仅会确定通往各个网络的最佳路径，同时还会在初始路径不可用或者拓扑结构发生变化时确定新的最佳路径。因此，动态路由协议比静态路由更具优势。如果使用动态路由协议，则路由器无需网络管理员的参与，即可自动与其他路由器共享路由信息并对拓扑结构的变化作出反应。

与静态路由相比，动态路由协议需要的管理开销较少。但是运行动态路由协议需要占用一部分路由器资源，包括 CPU 时间和网络链路带宽，如表 4-2 所示。动态路由确实在很多方面优于静态路由，不过，现今的网络仍会用到静态路由。而实际上，网络通常是将静态路由和动态路由结合使用。

表 4-2　　动态路由与静态路由的比较

比较内容	静态路由	动态路由
配置的复杂性	网络规模越大越复杂	通常不受网络规模限制
管理员所需知识	不需要额外的专业知识	需要掌握高级的知识和技能
拓扑结构变化	需要管理员参与	自动根据拓扑结构变化进行调整
可扩展性	适合简单的网络拓扑结构	适合各类拓扑结构的网络
安全性	更安全	存在安全隐患
资源使用情况	不需要额外的资源	占用 CPU、内存和链路带宽
可预测性	总是通过同一路径到达网络	根据当前网络拓扑结构确定路径

(2)动态路由协议的分类(表 4-3)

表 4-3　　动态路由协议的分类

	动态路由协议				
	内部网关协议				外部网关协议
	距离矢量路由协议		链路状态路由协议		路径矢量
有类	RIP	IGRP			EGP
无类	RIPv2	EIGRP	OSPFv2	IS-IS	BGPv4
IPv6	RIPng	EIGRP(IPv6)	OSPFv3	IS-IS(IPv6)	BGPv4(IPv6)

用于 IP 的动态路由协议有很多种,如表 4-3。路由 IP 数据包时常用的动态路由协议有:

◆ RIP(Routing Information Protocol,路由信息协议);

◆ IGRP(Interior Gateway Protocol,内部网关路由协议);

◆ EIGRP(Enhanced Interior Gateway Routing Protocol,增强型内部网关路由协议);

◆ OSPF(Open Shortest Path First,开放最短路径优先);

◆ IS-IS(Intermediate System to Intermediate System Routing Protocol,中间系统到中间系统);

◆ BGP(Border Gateway Protocol,边界网关协议)。

其中,IGRP 和 EIGRP 是 Cisco 专有的路由协议,IGRP 是早期的路由协议,已经被 EIGRP 所取代。在大多数情况下路由器的路由表中同时包含静态路由和动态路由。

①内部网关协议和外部网关协议

AS(自治系统)也称为路由域,是指一个共同管理区域内的一组路由器。例如公司的内部网络和 Internet 服务提供商的网络。由于 Internet 基于自治系统,因此既需要使用内部路由协议,也需要使用外部路由协议。这两类协议就是 IGP(内部网关协议),用于在自治系统内部路由,同时也用于在独立网络内部路由;EGP(外部网关协议),用于在自治系统之间路由。内部网关协议 (IGP) 又可以划分为距离矢量路由协议和链路状态路由协议。

②距离矢量路由协议和链路状态路由协议

距离矢量是指以距离和方向构成的矢量来通告路由信息。距离按跳数等度量来定义,方向则是下一跳的路由器或送出接口。距离矢量协议通常使用贝尔曼-福特 (Bellman-Ford) 算法来确定最佳路径。某些距离矢量协议会定期向所有邻近的路由器发送完整的路由表。在大型网络中,这些路由更新的数据量会愈趋庞大,因而会在链路中产生大规模的通信流量。路由器唯一了解的远程网络信息就是到该网络的距离(即度量)以及可通过哪条路径或哪个接口到达该网络。距离矢量路由协议并不了解确切的完整网络拓扑图。距离矢量协议适用于以下情形:

◆ 网络结构简单、扁平,不需要特殊的分层设计。

◆ 管理员没有足够的知识来配置链路状态协议和排查故障。

◆ 特定类型的网络拓扑结构,如集中星形 (Hub-and-Spoke) 网络。

◆ 无需关注网络最差情况下的收敛时间。

与距离矢量路由协议的运行过程不同,配置了链路状态路由协议的路由器可以获取所有其他路由器的信息来创建网络的完整拓扑结构。链路状态路由器使用链路状态信息来创建拓扑图,并在拓扑结构中选择到达所有目的网络的最佳路径。链路状态路由协议不采用定期更新机

制，在网络完成收敛之后，只在网络拓扑结构发生变化时才发送链路状态更新信息。链路状态协议适用于以下情形：

- 网络进行了分层设计，大型网络通常如此。
- 管理员对于网络中采用的链路状态路由协议非常熟悉。
- 网络对收敛速度的要求极高。

③有类路由协议和无类路由协议

有类路由协议在路由信息更新过程中不发送子网掩码信息，如 RIPv1。路由协议的路由信息更新中不包括子网掩码，子网掩码根据网络地址的第一组二进制八位数来确定。由于有类协议不包括子网掩码，因此并不适用于所有的网络环境。如果网络使用多个子网掩码划分子网，那么就不能使用有类路由协议。也就是说，有类路由协议不支持 VLSM（可变长子网掩码）。有类路由协议包括 RIPv1 和 IGRP。

在无类路由协议的路由信息更新中，同时包括网络地址和子网掩码。如今的网络已不再按照类来分配地址，子网掩码也就无法根据网络地址的第一个二进制八位数来确定。如今的大部分网络都需要使用无类路由协议，因为无类路由协议支持 VLSM、非连续网络，如图 4-6 所示。无类路由协议包括 RIPv2、EIGRP、OSPF、IS-IS 和 BGP 等。

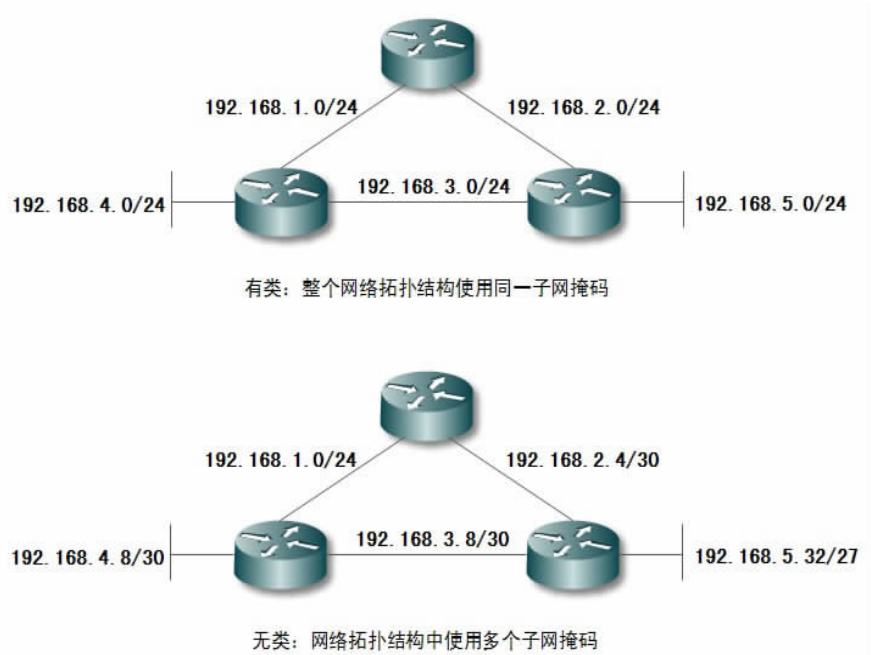


图 4-6　有类网络与无类网络的比较

④收敛

收敛是指所有路由器的路由表达到一致的过程。当所有路由器都获取到完整而准确的网络信息时，网络即完成收敛。收敛时间是指路由器共享网络信息、计算最佳路径并更新路由表所花费的时间。网络在完成收敛后才可以正常运行，因此，大部分网络都需要在很短的时间内完成收敛。收敛过程既具协作性，又具独立性。路由器之间既需要共享路由信息，各个路由器也必须独立计算拓扑结构变化对各自路由过程所产生的影响。由于路由器独立更新网络信息以与拓扑结构保持一致，所以，路由器通过收敛来达成一致状态。收敛的有关属性包括路由信

息的传播速度以及最佳路径的计算方法。可以根据收敛速度来评估路由协议。收敛速度越快，路由协议的性能就越好。通常，RIP 和 IGRP 收敛较慢，而 EIGRP 和 OSPF 收敛较快。

我们可以根据以下特征来比较不同动态路由协议的性能：

◆ 收敛时间：收敛时间是指网络拓扑结构中的路由器共享路由信息并使各台路由器掌握的网络情况达到一致所需的时间。收敛速度越快，协议的性能越好。在发生了改变的网络中，收敛速度缓慢会导致不一致的路由表无法及时得到更新，从而可能造成路由环路。

◆ 可扩展性：可扩展性表示根据一个网络所部署的路由协议，该网络能达到的规模。网络规模越大，路由协议需要具备的可扩展性越强。

◆ 无类（使用 VLSM）或有类：无类路由协议在更新中会提供子网掩码。此功能支持使用可变长子网掩码（VLSM），总结路由的效果也更好。有类路由协议不包含子网掩码且不支持 VLSM。

◆ 资源使用率：资源使用率包括路由协议的要求（如内存空间）、CPU 利用率和链路带宽利用率。资源要求越高，对硬件的要求越高，如此才能对路由协议工作和数据包转发过程提供有力支持。

◆ 实现和维护：实现和维护体现了对于所部署的路由协议，网络管理员实现和维护网络时必须要具备的知识级别。

（3）度量

要选择最佳路径，路由协议必须能够评估和区分所有可用的路径。度量是指路由协议用来分配到达远程网络的路由开销的值。有多条路径通往同一远程网络时，路由协议使用度量来确定最佳的路径。每一种路由协议都有自己的度量。例如，RIP 使用跳数，EIGRP 使用带宽和延迟，Cisco 版本的 OSPF 使用的是带宽。跳数是指数据包到达目的网络必须通过的路由器的数量，是最简单的度量方式。不同的路由协议使用不同的度量，一种路由协议使用的度量可能会与另一种路由协议存在差异。由于使用的度量不同，两种不同的路由协议对于同一目的网络可能会选择不同的路径。比如，RIP 会选择跳数最少的路径，而 OSPF 则会选择带宽最高的路径。IP 路由协议中使用的度量参数有：

◆ 跳数：一种简单的度量，计算的是数据包所必须经过的路由器数量。

◆ 带宽：通过优先考虑最高带宽的路径来做出选择。

◆ 负载：考虑特定链路的通信量使用率。

◆ 延迟：考虑数据包经过某个路径所花费的时间。

◆ 可靠性：通过接口错误计数或以往的链路故障次数来估计出现链路故障的可能性。

◆ 开销：由 IOS 或网络管理员确定的值，表示优先选择某个路由。开销既可以表示一个度量，也可以表示多个度量的组合，还可以表示路由策略。

各路由协议的度量如下：

◆ RIP：跳数——选择跳数最少的路由作为最佳路径。

◆ IGRP 和 EIGRP：带宽、延迟、可靠性和负载——通过这些参数计算综合度量值，选择综合度量值最小的路由作为最佳路径。默认情况下，仅使用带宽和延迟。

◆ IS-IS 和 OSPF：开销——选择开销最低的路由作为最佳路径。Cisco 采用的 OSPF 使用的是带宽。

路由协议根据度量值最低的路由来选择最佳路径。如果通往同一目的网络的多条路由具有相同的度量值，那么路由器会在这些开销相同的路径之间进行“负载均衡”，数据分组会使用所有路由开销相同的路径转发出去。要查看负载均衡是否起作用，可检查路由表。如果路由表中有多个路由条目与同一目的网络关联，则负载均衡正在起作用。

```
Router# show ip route
    * * * * * *
    Gateway of last resort is not set

R     172.16.0.0/14 [120/1] via 172.30.2.2, 00:00:12, FastEthernet0/0        度量值为 1
      172.30.0.0/24 is subnetted, 3 subnets
C        172.30.1.0 is directly connected, FastEthernet0/1
C        172.30.2.0 is directly connected, FastEthernet0/0
R        172.30.3.0 [120/1] via 172.30.2.2, 00:00:12, FastEthernet0/0
S     172.32.0.0/13 is directly connected, Null0
      192.168.4.0/30 is subnetted, 1 subnets
R        192.168.4.8 [120/1] via 172.30.2.2, 00:00:12, FastEthernet0/0
```

(4)管理距离

路由器通过静态路由和动态路由协议来了解与其直连的邻近网络以及远程网络的信息。实际上，路由器可能会通过多个来源获知通往同一网络的路由。那么路由器应该选择在路由表中添加哪条路由呢？由于不同的路由协议使用不同的度量(例如，RIP 使用跳数，而 OSPF 使用带宽)，因此，不能通过比较度量值来确定最佳路径。

管理距离（Administrative Distance，AD）定义路由来源的优先级别。对于每个路由来源(包括动态路由协议、静态路由、直连网络)，使用管理距离值按从高到低的优选顺序来排定优先级。如果从多个不同的路由来源获取到同一目的网络的路由信息，Cisco 路由器会使用 AD 功能来选择最佳路径。管理距离是从 0 到 255 的整数值。值越低表示路由来源的优先级别越高。管理距离值为 0 表示优先级别最高。只有直连网络的管理距离为 0，而且这个值不能更改。静态路由和动态路由协议的管理距离是可以修改的。管理距离值为 255 表示路由器不信任该路由来源，并且不会将其添加到路由表中。不同的路由协议有不同的默认 AD 值，如表 4-4 所示。

表 4-4　　默认管理距离

路由来源	管理距离 AD
直连路由	0
静态路由	1
EIGRP 总结路由	5
外部 BGP	20
内部 EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
外部 EIGRP	170
内部 BGP	200

可以通过 show ip route 命令查看路由条目的 AD 值：

```
R1# show ip route
     * * * * * *
     Gateway of last resort is 0.0.0.0 to network 0.0.0.0

          10.0.0.0/32 is subnetted, 1 subnets
     C       10.1.1.1 is directly connected, Loopback0
          172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
     C       172.16.1.16/28 is directly connected, FastEthernet0/0
     O       172.16.1.32/29 [110/65] via 192.168.10.6, 00:00:11, Serial0/0/1      AD是110
          172.30.0.0/30 is subnetted, 1 subnets
     C       172.30.1.0 is directly connected, Loopback1
          192.168.10.0/30 is subnetted, 3 subnets
     C       192.168.10.0 is directly connected, Serial0/0/0
     C       192.168.10.4 is directly connected, Serial0/0/1
     O       192.168.10.8 [110/128] via 192.168.10.6, 00:00:11, Serial0/0/1
     S*    0.0.0.0/0 is directly connected, Loopback1
```

2. 距离矢量路由协议

(1)距离矢量路由协议简介

距离矢量意味着用距离和方向矢量通告路由。距离使用诸如跳数这样的度量确定，而方向则是下一跳路由器或送出接口。使用距离矢量路由协议的路由器并不了解到达目的网络的整条路径。路由器只知道应该往哪个方向或使用哪个接口转发数据包，以及自身与目的网络之间的距离，如图 4-7 所示。

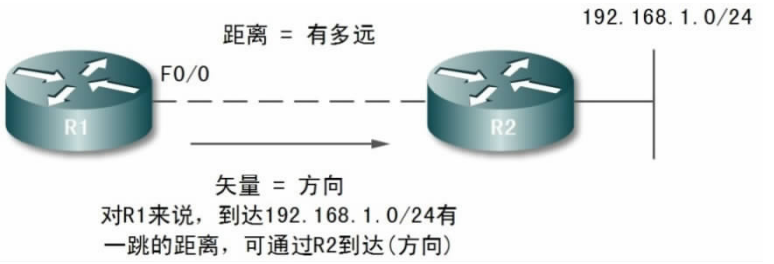


图 4-7　距离矢量示意图

距离矢量路由协议有一些共同特征，如表 4-5 所示。

◆ 按照一定的时间间隔发送定期更新(RIP 的间隔为 30 秒，IGRP 的间隔为 90 秒)。即使拓扑结构数天都未发生变化，定期更新仍然会不断地发送到所有邻居那里。邻居是指使用同一链路并配置了相同路由协议的其他路由器。广播更新均发送到 255.255.255.255。配置了相同路由协议的相邻路由器将处理此类更新。一些距离矢量路由协议使用组播地址而不是广播地址。

◆ 定期向所有邻居发送整个路由表更新。接收这些更新的邻居必须处理整个更新，从中找出有用的信息，并丢弃其余的无用信息。某些距离矢量路由协议(如 EIGRP)不会定期发送路由表更新。

表 4-5　　各路由协议性能比较

比较内容	距离矢量路由协议				链路状态路由协议	
	RIPv1	RIPv2	IGRP	EIGRP	OSPF	IS-IS
收敛速度	慢	慢	慢	快	快	快
可扩展性-网络规模	小	小	小	大	大	大
VLSM	不	支持	不	支持	支持	支持
资源使用率	低	低	低	中	高	高
实施和维护	简单	简单	简单	复杂	复杂	复杂

(2)网络发现

当路由器冷启动或通电开机时,它完全不了解网络拓扑结构。它甚至不知道在其链路的另一端是否存在其他设备。路由器唯一了解的信息来自自身 NVRAM 中存储的配置文件中的信息。当路由器成功启动后,它将应用所保存的配置。如果正确配置了 IP 地址,则路由器将首先发现与其自身直连的网络,如图 4-8 所示。

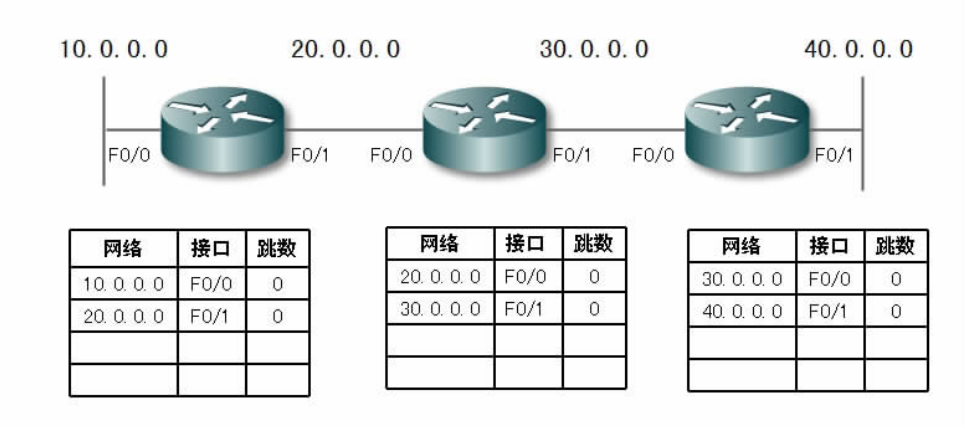


图 4-8　网络发现——冷启动

配置路由协议后,路由器就会开始交换路由更新。一开始,这些更新仅包含有关其直连网络的信息。收到更新后,路由器会检查更新,从中找出新信息。任何当前路由表中没有的路由都将被添加到路由表中,如图 4-9 所示。

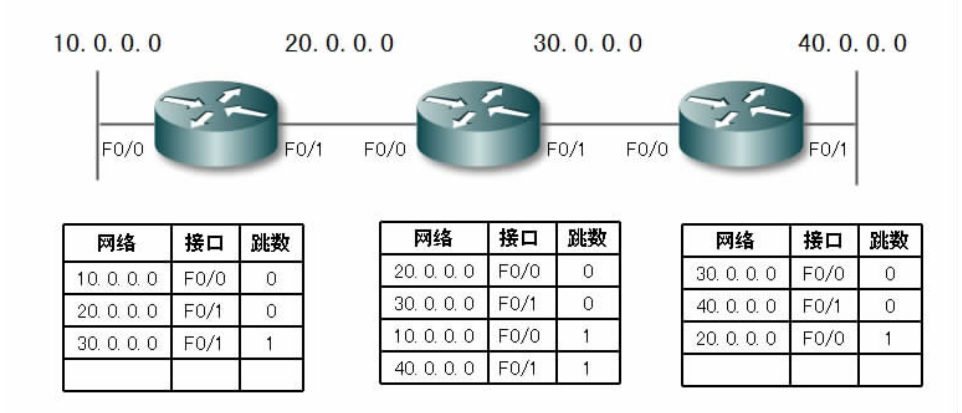
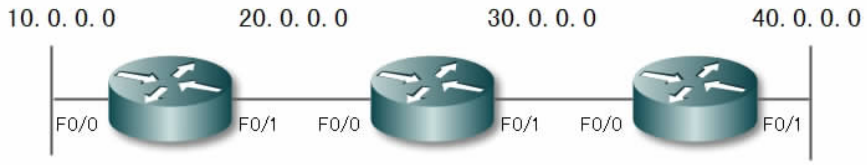


图 4-9　网络发现——第一次路由更新

此时，路由器已经获知与其直连的网络，以及与其邻居相连的网络。接着路由器开始交换下一轮的定期更新，并继续收敛。每台路由器再次检查更新并从中找出新信息，如图 4-10 所示。



网络	接口	跳数
10. 0. 0. 0	F0/0	0
20. 0. 0. 0	F0/1	0
30. 0. 0. 0	F0/1	1
40. 0. 0. 0	F0/1	2

网络	接口	跳数
20. 0. 0. 0	F0/0	0
30. 0. 0. 0	F0/1	0
10. 0. 0. 0	F0/0	1
40. 0. 0. 0	F0/1	1

网络	接口	跳数
30. 0. 0. 0	F0/0	0
40. 0. 0. 0	F0/1	0
20. 0. 0. 0	F0/0	1
10. 0. 0. 0	F0/0	2

图 4-10　网络发现——第二次路由更新

网络收敛所需的时间与网络的规模成直接比例。我们可以根据路由协议传播此类信息的速度(收敛速度)来比较路由协议的性能。达到收敛的速度包含两个方面，即路由器在路由更新中向其邻居传播拓扑结构变化的速度，和使用收集到的新路由信息计算最佳路径路由的速度。网络在达到收敛前无法完全正常工作，因此，网络管理员更喜欢使用收敛时间较短的路由协议。

(3)路由表维护

①定期更新

许多距离矢量协议采用定期更新与其邻居交换路由信息，并在路由表中维护最新的路由信息。RIP 和 IGRP 均属于此类协议。定期更新是指路由器以预定义的时间间隔向邻居发送完整的路由表。对于 RIP，无论拓扑结构是否发生变化，这些更新都将每隔 30 秒钟(更新)以广播的形式 (255. 255. 255. 255) 发送出去。每次收到更新后，路由表中路由信息的定期更新时间都会刷新。通过这种方法便可在拓扑结构发生改变时维护路由表中的信息。拓扑结构发生变化的原因有多种，包括：

◆ 链路故障。

◆ 增加新链路。

◆ 路由器故障。

◆ 链路参数改变。

除更新计时器外，IOS 还针对 RIP 设置了另外三种计时器：

◆ 无效计时器。如果 180 秒(默认值)后还未收到可刷新现有路由的更新，则将该路由的度量设置为 16，从而将其标记为无效路由。在清除计时器超时以前，该路由仍将保留在路由表中。

◆ 清除计时器。默认情况下，清除计时器设置为 240 秒，比无效计时器长 60 秒。当清除计时器超时后，该路由将从路由表中删除。

◆ 抑制计时器。该计时器用于稳定路由信息，并有助于在拓扑结构根据新信息收敛的过程中防止路由环路。在某条路由被标记为不可达后，它处于抑制状态的时间必须足够长，以便拓扑结构中所有路由器能在此期间获知该不可达网络。默认情况下，抑制计时器设置为 180 秒。

计时器的值可以通过两条命令来检验：show ip route 和 show ip protocols。

②限定更新

与其他距离矢量路由协议不同，EIGRP 不发送定期更新，而是在路径改变或路由的度量改变时发送限定更新。当出现新路由或现有路由需要删除时，EIGRP 只会发送有关该网络的信息，而不是整个路由表。该信息只会发往确实需要此信息的那些路由器。EIGRP 使用的更新具有以下特点：

◆ 不定期，因为此类信息不是按固定时间间隔发送。

◆ 仅当拓扑结构中发生影响路由信息的改变时才发送相关部分的更新。

◆ 限定范围，这表示部分更新的传播受到自动限制，只有需要该更新信息的路由器才会收到更新。

③触发更新

当拓扑结构发生改变时，为了加速收敛，RIP 将使用触发更新。触发更新是一种路由表更新方式，此类更新会在路由发生改变后立即发送出去。触发更新不需要等待更新计时器超时。检测到拓扑结构变化的路由器会立即向相邻路由器发送更新消息。接收到这一消息的路由器将依次生成触发更新，以通知邻居拓扑结构发生了改变。当发生以下情况之一时，就会发出触发更新：接口状态改变（开启或关闭）；某条路由进入（或退出）“不可达”状态；路由表中增加了一条路由。

如果能够保证更新能立即到达每台路由器，那么仅使用触发更新就已足够。然而，触发更新存在两个问题：

◆ 包含更新信息的数据包可能在网络的某些链路上丢失或损坏。

◆ 触发更新并不能在瞬间完成。尚未收到触发更新的路由器有可能在错误的时间发送常规定期更新，从而导致错误的路由重新插入已经收到触发更新的邻居的路由表中。

（4）路由环路

路由环路是指数据包在一系列路由器之间不断传输却始终无法到达其预期目的网络的一种现象。当两台或多台路由器的路由信息中存在错误地指向不可达目的网络的有效路径时，就可能发生路由环路。造成环路的可能原因有：静态路由配置错误；路由重分布配置错误（重分布表示将来自一种路由协议的路由信息转给另一种路由协议的过程）；发生了改变的网络中收敛速度缓慢，不一致的路由表未能得到更新；错误配置或添加了丢弃的路由。

距离矢量路由协议的工作方式比较简单，其简单性导致它容易存在诸如路由环路之类的缺陷。在链路状态路由协议中，路由环路较为少见。路由环路会对网络造成严重影响，导致网络性能降低，不仅会耗尽带宽，而且会耗尽路由器资源，导致网络缓慢甚至瘫痪。路由环路一般是由距离矢量路由协议引发的，目前有多种机制可以消除路由环路。这些机制包括：

◆ 定义最大度量以防止计数至无穷大。

◆ 抑制计时器。

◆ 水平分割。

◆ 路由毒化或毒性反转。

◆ 触发更新。

①计数至无穷大

当不正确的路由更新无休止地增加不再可达的网络的度量值时，就会出现“计数至无穷大”。为了防止度量无限增大，可以通过设置最大度量值来界定“无穷大”。例如，RIP 将无穷大定义为 16 跳，大于等于此值的路由即为“不可达”。一旦路由器计数达到该“无穷大”值，该路由就会被标记为不可达。

②使用抑制计时器预防路由环路

假设现在存在一个不稳定的网络，在很短的时间内，接口被重置为 up，然后是 down，接着再重置为 up，该路由将发生摆动，使用触发更新时，路由器可能会反应过快，从而在不知情的情况下造成路由环路。此外，路由器在不稳定期间发送的定期更新也可能导致路由环路，抑制计时器可以防止在上述情况中出现路由环路，抑制计时器还有助于防止计数至无穷大情况的出现。

抑制计时器可用来防止定期更新消息错误地恢复某条可能已经发生故障的路由。抑制计时器指示路由器将那些可能会影响路由的更改保持一段特定的时间。如果确定某条路由为 down(不可用)或 possibly down(可能不可用)，则在规定的时间段内，任何包含相同状态或更差状态的有关该路由的信息都将被忽略。这表示路由器将在一段足够长的时间内将路由标记为 unreachable(不可达)，以便路由更新能够传递带有最新信息的路由表。

抑制计时器通过以下方式工作：

a. 路由器从邻居处接收到更新，该更新表明以前可以访问的网络现在已不可访问。

b. 路由器将该网络标记为 possibly down 并启动抑制计时器。

c. 如果在抑制期间从任何相邻路由器接收到含有更小度量的有关该网络的更新，则恢复该网络并删除抑制计时器。

d. 如果在抑制期间从相邻路由器收到的更新包含的度量与之前相同或更大，则该更新将被忽略。如此一来，更改信息便可以继续在网络中传播一段时间。

e. 路由器仍然会转发目的网络被标记为 possibly down 的数据包。通过这种方式，路由器便能克服连接断续所带来的问题。如果目的网络确实不可达，但路由器又转发了数据包，黑洞路由就会建立起来并持续到抑制计时器超时。

③水平分割

防止由于距离矢量路由协议收敛缓慢而导致路由环路的另一种方法是水平分割。水平分割规则规定，路由器不能使用接收更新的同一接口来通告同一网络。

④路由毒化或毒性反转

路由毒化是距离矢量路由协议用来防止路由环路的一种方法。路由毒化用于在发往其他路由器的路由更新中将路由标记为不可达。标记“不可达”的方法是将度量设置为最大值。对于 RIP，毒化路由的度量为 16。

毒性反转可以与水平分割技术结合使用。这种方法称为带毒性反转的水平分割。“带毒性反转的水平分割”规则规定，从特定接口向外发送更新时，将通过该接口获知的所有网络标示为

不可达。毒性反转非常特殊，它会使路由器忽略水平分割规则的要求。水平分割功能是默认启用的功能。然而，并非所有 IOS 实现都默认启用了带毒性反转的水平分割。

⑤IP 和 TTL

TTL(生存时间)是 IP 报头中的 8 位字段，它限制了数据包在被丢弃之前能够在网络中传输的跳数。设置 TTL 字段的目的是防止无法投递的数据包无休止地在网络中来回传输。数据包的源设备会对 8 位的 TTL 字段设置一个值。在到达目的地的过程中，每经过一台路由器，TTL 的值就会减 1。如果在到达目的地之前 TTL 字段的值减为零，则路由器将丢弃该数据包并向该 IP 数据包的源地址发送 Internet 控制消息协议（ICMP）错误消息。

3. RIPv1

(1)RIPv1 有类距离矢量路由协议

RIP 是最早的距离矢量路由协议。尽管 RIP 缺少许多更为高级的路由协议所具备的复杂功能，但其简单性和使用的广泛性使其具有很强的生命力。学习 RIP 协议有助于我们了解和进一步学习其他高级路由协议。RIP 不是“即将被淘汰”的协议。实际上，现在已经出现了一种支持 IPv6 的 RIP，称为 RIPng(ng 是 next generation 的缩写，意为“下一代”)。

RIP 的第一个版本通常被称为 RIPv1，以便与 RIPv2 相区别。然而，两个版本都具有许多相同的功能。RIP 主要有以下特征：

- RIP 是一种距离矢量路由协议。
- RIP 使用跳数作为路径选择的唯一度量。
- 将跳数超过 15 的路由通告为不可达。
- 每 30 秒广播一次消息。

RIP 消息的数据部分封装在 UDP 数据段内，其源端口号和目的端口号都被设为 520，如图 4-11、图 4-12 所示。在消息从所有配置了 RIP 的接口发送出去之前，IP 报头和数据链路报头会加入广播地址作为目的地址。

图 4-11　RIPv1 报头

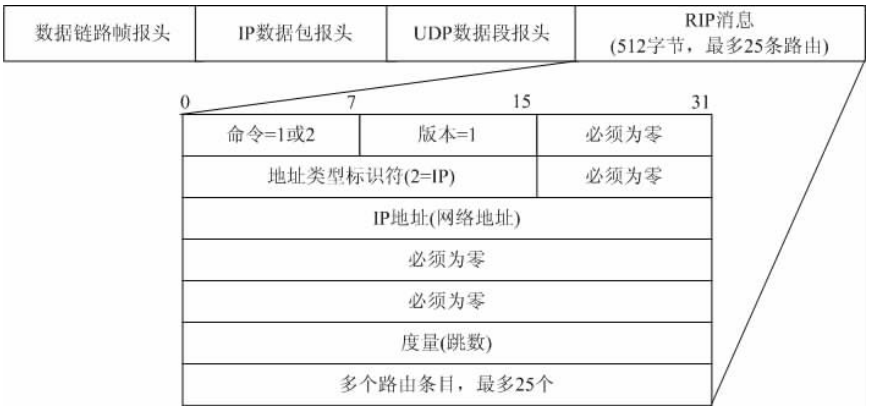


图 4-12　RIPv1 消息格式

RIP 报头长度为四个字节，这四个字节被划分为三个字段。命令字段指定了消息类型。版本字段设置为 1，表示为 RIPv1。第三个字段被标记为必须为零，“必须为零”字段用于为协议将来的扩展预留空间。消息的路由条目部分包含三个字段，其内容分别是：地址类型标识符（设置为 2 代表 IP 地址，但在路由器请求完整的路由表时设置为 0）、IP 地址以及度量。路由条目部分代表一个目的路由及与其关联的度量。一个 RIP 更新最多可包含 25 个路由条目。数据报最大可以是 512 个字节，不包括 IP 或 UDP 报头。

RIP 使用请求消息和响应消息两种类型的消息（在“命令”字段中指定），如表 4-6 所示。每个配置了 RIP 的接口在启动时都会发送请求消息，要求所有 RIP 邻居发送完整的路由表。启用 RIP 的邻居随后传回响应消息。当请求方路由器收到响应时，它将评估每个路由条目。如果路由条目是新的，接收方路由器便将该路由添加到路由表中。如果该路由已经包含在路由表中，则当新条目比现有条目跳数少时，新条目将替换现有条目。启动路由器随后从所有启用了 RIP 的接口发出包含其自身路由表的触发更新，以便 RIP 邻居能够获知所有新路由。

表 4-6　　RIPv1 消息字段描述

命令	1 表示请求，2 表示应答
版本	1 表示 RIPv1，2 表示 RIPv2
地址类型标识符	2 表示 IP，如果请求完整的路由表则设置为 0
IP 地址	目的路由的地址，可以是网络、子网或主机地址
度量	1 到 16 之间的跳数。在发出消息前发送方路由器会增加度量

RIP 是有类路由协议，不会在更新中发送子网掩码信息。因此，路由器将使用本地接口配置的子网掩码，或者根据地址类应用默认子网掩码（A 类地址的默认子网掩码是 255.0.0.0，B 类地址的默认子网掩码是 255.255.0.0，C 类地址的默认子网掩码是 255.255.255.0）。受此限制，RIPv1 网络不能为不连续网络，也不能使用 VLSM。

RIP 的默认管理距离为 120。与其他内部网关协议相比，RIP 路由协议的优先级最低。IS-IS、OSPF、IGRP 和 EIGRP 的默认管理距离值都比 RIP 低。可以通过以下两个 show 命令来查看路由协议的管理距离值。

```
R1# show ip route
     * * * * * *
     Gateway of last resort is not set

     C    192.168.1.0/24 is directly connected, FastEthernet0/0
     C    192.168.2.0/24 is directly connected, Serial0/0/0
     R    192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:05, Serial0/0/0        AD为120
     R    192.168.4.0/24 [120/1] via 192.168.2.2, 00:00:05, Serial0/0/0
     R    192.168.5.0/24 [120/2] via 192.168.2.2, 00:00:05, Serial0/0/0
```

(2)RIPv1 基本配置

应在全局配置模式下进行 RIP 配置：

```
Router(config)# router rip
Router(config-router)#
```

该命令并不直接启动 RIP 过程。但通过它用户可以进入该路由协议的配置模式。此时不会发送路由更新。如果要从设备上彻底删除 RIP 路由过程，可以使用 no router rip 。该命令会停止 RIP 过程并清除所有现有的 RIP 配置。

进入 RIP 路由器配置模式后，路由器便按照指示开始运行 RIP。但路由器还需了解应该使用哪个本地接口与其他路由器通信，以及需要向其他路由器通告哪些本地连接的网络。要为网络启用 RIP 路由，在路由器配置模式下使用 network 命令，并输入每个直连网络的有类网络地址。

```
Router(config-router)# network directly-connected-classful-network-address
```

network 命令的作用是在属于某个指定网络的所有接口上启用 RIP，相关接口将开始发送和接收 RIP 更新，并在每 30 秒一次的 RIP 路由更新中向其他路由器通告该指定网络。

现在使用 network 命令配置图 4-13 所有三台路由器的直连网络。

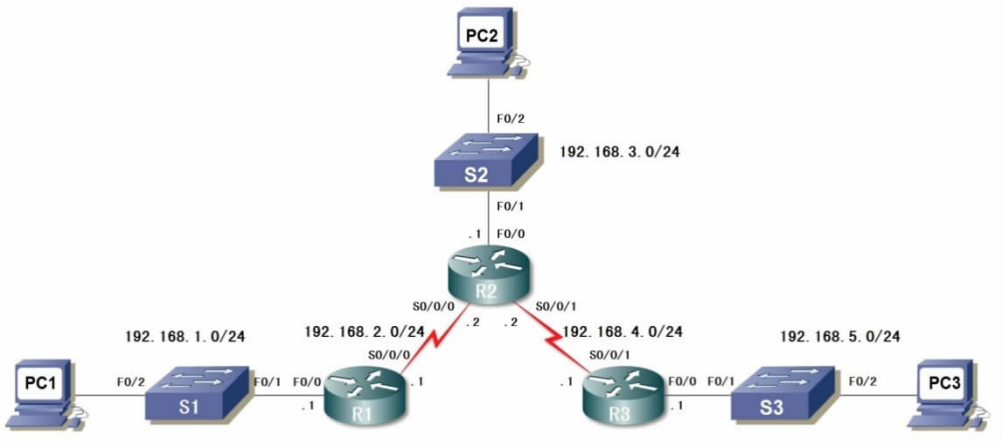


图 4-13　RIP 配置拓扑图

```
R1(config)# router rip
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.2.0
R2(config)# router rip
R2(config-router)# network 192.168.2.0
```

```
R2(config-router)# network 192.168.3.0
R2(config-router)# network 192.168.4.0
R3(config)# router rip
R3(config-router)# network 192.168.4.0
R3(config-router)# network 192.168.5.0
```

如果使用 network 命令进行 RIP 配置时，如果输入了子网地址或接口的 IP 地址而不是有类网络地址，IOS 会自动更正输入，将其变为有类网络地址。但我们建议使用规范的配置命令。

(3)检验 RIP 配置

要检验路由和排除路由故障，可以使用 show ip route 和 show ip protocols。如果使用这两条命令不能找出问题，可以使用 debug ip rip 命令查看详细情况。我们将按照检验路由和排除路由故障时这三条命令的建议使用顺序来分别讨论它们。另外，在配置任何路由时，使用 show ip interface brief 命令确保所有必需的接口都处于“up”和“up”状态。

show ip route 命令检验从 RIP 邻居处接收的路由是否已添加到路由表中，路由条目中的“R ”表示 RIP 路由。show ip route 命令将显示整个路由表，所以在检查收敛情况时，一般首先使用此命令。因为网络收敛需要一定时间，所以当您执行该命令时，路由可能不会立即显示出来。但是，一旦所有路由器上的路由都得到正确配置，则 show ip route 命令将反映出每台路由器都有完整的路由表，其中包含到达拓扑结构中每个网络的路由。

```
R2# show ip route
     * * * * * *
     Gateway of last resort is not set

     R     192.168.1.0/24 [120/1] via 192.168.2.1, 00:00:01, Serial0/0/0
     C     192.168.2.0/24 is directly connected, Serial0/0/0
     C     192.168.3.0/24 is directly connected, FastEthernet0/0
     C     192.168.4.0/24 is directly connected, Serial0/0/1
     R     192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:22, Serial0/0/1
```

现在我们以以上 R2 路由表中第一条 RIP 路由为例来解读路由表中显示的输出。通过检查路由列表中是否存在带 R 代码的路由，我们可快速得知路由器上是否确实运行着 RIP。如果没有配置 RIP，您将不会看到任何 RIP 路由。紧跟在 R 代码后的“192.168.5.0/24”是远程网络地址和子网掩码。“[120/1]”表示 RIP 协议的 AD 值(RIP 为 120)和到该远程网络的距离(1 跳)。“ via 192.168.2.1 ”表示通告路由器的下一跳 IP 地址，“ 00:00:01 ”表示自上次更新以来已经过了多少秒。“ Serial0/0/0 ”表示路由器用来向该远程网络转发数据的送出接口。

```
R2# show ip protocols
     Routing Protocol is "rip"
     Sending updates every 30 seconds, next due in 4 seconds
     Invalid after 180 seconds, hold down 180, flushed after 240
     Outgoing update filter list for all interfaces is not set
     Incoming update filter list for all interfaces is not set
     Redistributing: rip
```

```
Default version control: send version 1, receive any version
  Interface              Send  Recv  Triggered RIP  Key-chain
  FastEthernet0/0        1     2 1
  Serial0/0/1            1     2 1
  Serial0/0/0            1     2 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
    192.168.2.0
    192.168.3.0
    192.168.4.0
Passive Interface(s):
Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.2.1       120           00:00:23
    192.168.4.1       120           00:00:22
Distance: (default is 120)
```

如果路由表中缺少某个网络，可以使用 show ip protocols 命令来检查路由配置。show ip protocols 命令会显示路由器当前配置的路由协议。其输出可用于检验大多数 RIP 参数，包括是否已配置 RIP 路由，发送和接收 RIP 更新的接口是否正确，路由器通告的网络是否正确，RIP 邻居是否发送了更新等信息。此命令对于检验其他路由协议的工作情况也非常有用。

大多数 RIP 配置错误都涉及 network 语句配置错误、缺少 network 语句配置，或在有类环境中配置了不连续的子网。对于这种情况，可使用一个很有效的命令 debug ip rip 找出 RIP 更新中存在的问题，该命令将在发送和接收 RIP 路由更新时显示这些更新信息。因为更新是定期发送的，所以您需要等到下一轮更新开始才能看到命令输出。

从 R2 的 debug ip rip 命令输出中可以看到，尽管 R2 FastEthernet0/0 接口连接的 LAN 上并没有 RIP 设备，R2 仍然会从该接口每 30 秒发送一次更新。在 LAN 上发送不需要的更新会在以下三个方面对网络造成影响：

◆ 带宽浪费在传输不必要的更新上。因为 RIP 更新是广播，所以交换机将向所有端口转发更新。

◆ LAN 上的所有设备都必须逐层处理更新，直到传输层后接收设备才会丢弃更新。

◆ 在广播网络上通告更新会带来严重的风险。RIP 更新可能会被数据包嗅探软件中途截取。

我们可以在路由器配置模式下配置 passive-interface 命令来阻止路由更新通过某个路由器接口传输，但仍然允许向其他路由器通告该网络。所有的路由协议都支持 passive-interface 命令。

```
Router(config-router)# passive-interface interface-type interface-number
```

例如，我们使用 passive-interface 命令配置 R2 的 FastEthernet0/0 接口，因为该 LAN 没有 RIP 邻居，然后使用 show ip protocols 命令检验被动接口。通过下面的代码与前面 R2 上得 show ip protocols 做比较，可以看到，在 Interface 中看不到 FastEthernet0/0 接口，此接口显示

在 Passive Interface(s)下。

```
R2# show ip protocols
    Routing Protocol is "rip"
    Sending updates every 30 seconds, next due in 4 seconds
    Invalid after 180 seconds, hold down 180, flushed after 240
    Outgoing update filter list for all interfaces is not set
    Incoming update filter list for all interfaces is not set
    Redistributing: rip
    Default version control: send version 1, receive any version
      Interface              Send  Recv  Triggered RIP  Key-chain
      Serial0/0/1            1     2 1
      Serial0/0/0            1     2 1
    Automatic network summarization is in effect
    Maximum path: 4
    Routing for Networks:
        192.168.2.0
        192.168.3.0
        192.168.4.0
    Passive Interface(s):
        FastEthernet0/0
    Routing Information Sources:
        Gateway         Distance      Last Update
        192.168.2.1         120       00:00:05
        192.168.4.1         120       00:00:16
    Distance: (default is 120)
```

(4)自动总结(图 4-14)

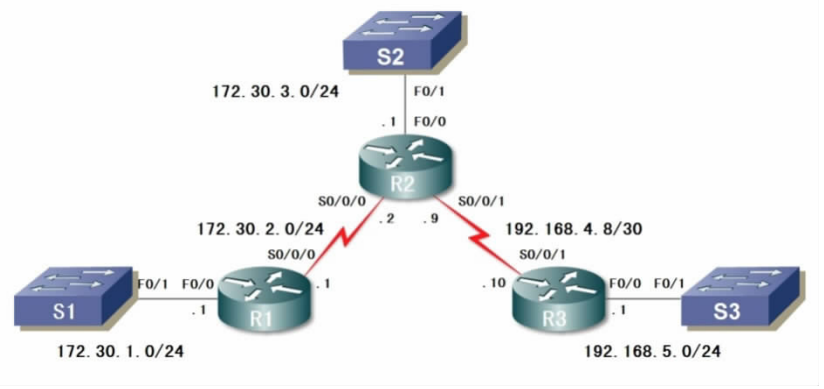


图 4-14　RIP 自动总结

RIP 是一种有类路由协议,它能够在主要的网络边界间自动总结有类网络。对于更新中的路由条目而言,如果发往的主网与其所属的主网不同,则路由条目中的网络地址将总结为有类网络地址(或称主网地址)。在图 4-14 中因为边界路由器 R2 总结从一个主网到另一个主网的 RIP 子网,所以当从 R2 的 Serial 0/0/1 接口发送更新时,有关 172.30.1.0、172.30.2.0 和

172.30.3.0 网络的更新将自动总结到 172.30.0.0(三个子网均属于同一个 B 类网络)。通常 RIPv1 更新会遵循以下两条规则:

◆ 如果某条路由更新及其接收接口属于相同的主网,则在路由更新中对该网络应用该接口的子网掩码。

◆ 如果某条路由更新及其接收接口属于不同的主网,则在路由更新中对该网络应用网络的有类子网掩码。

因为 R2 的 172.30.0.0 更新是从属于不同有类网络 (192.168.4.0) 的接口(Serial0/0/1)发出的,所以 RIP 只发送一个代表整个有类网络的更新,而不是为每个不同的子网各发送一个更新。自动总结可以使发送和接收的路由更新较小,从而使路由更新占用较少的带宽,加快路由表的查找过程。默认情况下,RIPv1 在主网边界上自动总结。

尽管自动总结会带来一些好处,但是有些情况下的自动总结会给网络带来不利影响。有类路由协议的路由更新中不包含子网掩码,而网络在主网边界间自动总结,因此接收路由器无法确定路由的掩码,这是因为接收接口的掩码可能与划分了子网的路由不同。如图 4-15 所示,子网 172.30.1.0/24 和 172.30.2.0/24 同属于同一个有类网络 172.30.0.0/16,但它们被另一个主网 192.168.0.0/16 分隔开,因此便生成了不连续网络。

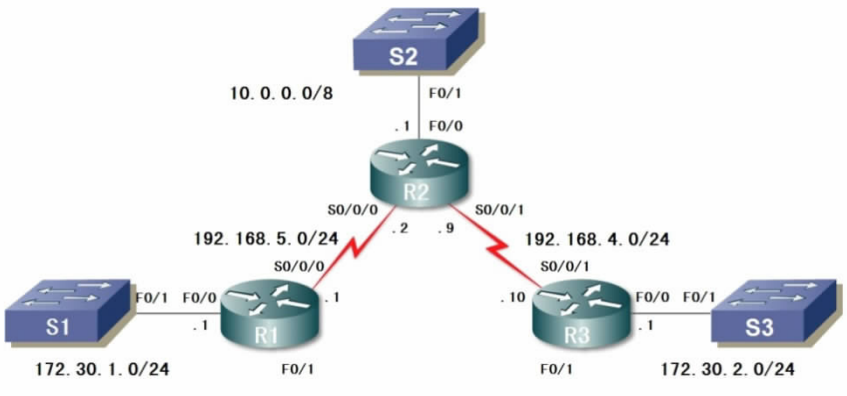


图 4-15 不连续网络图

对网络配置了正确的 RIPv1 后,网络仍然无法确定不连续拓扑结构中的所有网络。原因是对于不属于待通告路由所在网络的接口,路由器只能从该接口发出主网地址通告,就是说,R1 和 R3 会将主网地址 172.30.0.0(即总结路由)通告给 R2,因此在 R2 上会有两条通往 172.30.0.0/16 的等价路由。通过这个例子,我们知道,RIPv1 是不支持不连续网络的。

(5)在 RIPv1 中传播默认路由

RIP 是第一个动态路由协议,在早期的客户与 ISP 之间以及不同 ISP 之间使用非常广泛。但在现在的网络中,客户不需要与 ISP 交换路由更新。连接到 ISP 的客户路由器不需要 Internet 上所有路由的完整列表。相反,这些路由器上都有一条默认路由,可在客户路由器没有通往目的地的路由时,将所有流量发送到 ISP 路由器。而 ISP 则会配置一条指向客户路由器的静态路由,用于路由目的地为客户网络内部地址的流量。在许多路由协议(包括 RIP)中,您可以在路由器配置模式中使用 default-information originate 命令指定该路由器为默认信息的来源,由该路由器在 RIP 更新中传播静态默认路由。

```
Router(config)#router rip
```

```
Router(config-router)#default-information originate
```

4. VLSM 和 CIDR

(1)有类与无类寻址

我们知道,IPv4 将 IP 地址(由 32 位二进制组成)划分为 A、B、C、D、E 五类,其中可用作主机地址的是 A、B、C 三类,它们的地址信息如表 4-7 所示。

表 4-7　　IP 地址的分类

分类	网络号范围	子网掩码	可能的网络数量	每个网络的主机数量
A 类	前 8 位(1～126)	255.0.0.0 或/8	2^7-2	$2^{24}-2$
B 类	前 16 位(128～191)	255.255.0.0 或/16	$2^{14}-2$	$2^{16}-2$
C 类	前 24 位(192～223)	255.255.255.0 或/24	$2^{21}-2$	2^8-2

有类 IP 地址意味着网络地址的子网掩码可由第一组二进制八位数的值来确定,或者更准确地说,掩码由地址的前三个位来确定。像 RIPv1 这样的路由协议只需广播已知路由器的网络地址,而不必在路由更新中包含子网掩码。这是因为,路由器接收路由更新后,只需检查网络地址中第一组二进制八位数的值(或者应用其子网路由接入接口的掩码),就可以确定子网掩码。有类地址的子网掩码直接与网络地址相关。

Internet 呈几何级数的增长,但 Internet 路由表的扩展性却有限。另外,32 位的 IPv4 地址空间也存在最终耗尽的危险。1993 年,IETF 引入了“无类域间路由”这一概念,即 CIDR (RFC 1517)。CIDR 允许更灵活地使用 IPv4 地址空间,允许前缀聚合,这样就减小了路由表。CIDR 可以根据具体的需要而不是按照地址类,使用 VLSM(可变长子网掩码)为子网分配 IP 地址,如可通过任意前缀长度(/8、/9、/10 依次递增等等)更加有效地分配地址空间。在这种类型的地址分配中,允许将地址中的任何位作为地址中网络部分和主机部分的分界点。网络可以不断地拆分或细化为越来越小的子网。CIDR 支持前缀聚合,可以将多条路由信息总结为单条路由信息,有助于减小 Internet 路由表,这类路由就是所谓的“超网路由”,超网使用小于类掩码短的掩码来总结多个网络地址。

有类路由协议不能发送超网路由信息,因为接收这些路由信息的路由器会对路由表中的网络地址使用默认的有类子网掩码。那么如果网络地址的子网掩码是不确定的,并非有类网络的子网掩码,广播 VLSM 和超网路由信息就需要使用无类路由协议,无类路由协议的路由信息更新中同时包含网络地址和子网掩码。无类路由协议包括 RIPv2、EIGRP、OSPF、IS-IS 和 BGP 等。这些路由协议的路由信息更新中同时包含网络地址和子网掩码。在子网掩码不再由第一组二进制八位数值来假定或确定的情况下,必须要使用无类路由协议。

(2)VLSM

如果我们从主机地址借用位(如从 /8 变为 /16)来做子网号,那么就可以产生更多的子网。所以在使用 VLSM 和无类路由的情况下,就具有了更多的灵活性,可以创建更多的网络地址,可以使用适合实际需要的掩码。

(3)CIDR

CIDR 路由是使用比路由的有类掩码更小的子网掩码总结而成的路由。路由总结(或路由聚合)是指使用更笼统、相对更短的子网掩码将一组连续地址作为一个地址来传播。CIDR 忽略有类边界的限制,允许使用小于默认有类掩码的掩码进行总结,它有助于减少路由更新中的

条目数量，以及降低本地路由表中的条目数量，还可以帮助减少路由更新所需的带宽用量，加快路由表查询速度。

5. RIPv2

由于 RIPv1 不会在路由更新中发送子网掩码，因此它不支持 VLSM。RIPv1 和其他有类路由协议也无法支持 CIDR 路由，RIPv1 会忽略路由表中的这些超网，不会将它们包含在发往其他路由器的更新中。RFC 1723 中对 RIPv2 进行了定义。与 RIPv1 一样，RIPv2 封装在使用 520 端口的 UDP 数据段中，最多可包含 25 条路由。虽然 RIPv2 与 RIPv1 的基本消息格式相同，但 RIPv2 添加了两项重要扩展，即子网掩码字段和下一跳地址。

默认情况下，配置了 RIP 过程的 Cisco 路由器上会运行 RIPv1。尽管路由器只发送 RIPv1 消息，但它可以同时解释 RIPv1 和 RIPv2 消息。RIPv1 路由器会忽略路由条目中的 RIPv2 字段。使用以下命令可以配置 RIP 为 RIPv2 版本：

```
Router(config)# router rip
Router(config-router)# version 2
```

RIPv2 的其他配置同 RIPv1。在路由器配置模式下使用 version 1 命令和 no version 命令均可恢复为默认的 RIPv1。默认情况下，RIPv2 与 RIPv1 一样都会在主网边界上自动总结，可以在路由器配置模式下使用 no auto-summary 命令禁用自动总结，此命令对 RIPv1 无效。禁用自动总结后，RIPv2 不再在边界路由器上将网络总结为有类地址。

对 RIPv2 进行检验和故障排除的方法有许多，这些方法也可用于对其他路由协议进行检验和故障排除，最好从基础配置开始检查：

- 确保所有链路（接口）已启用而且运行正常。
- 检查布线。
- 检查并确保每个接口均配置了正确的 IP 地址和子网掩码。
- 删除所有不再需要的配置命令，或者已被其他命令所替代的配置命令。

常用的检验命令有：

- show ip route
- show ip interface brief
- show ip protocols
- debug ip rip
- show running-config

（3）进一步了解路由表

理解路由表的结构和查找过程，就相当于拥有了检验网络和排除网络故障的重要工具。排查路由问题时，知道路由表中应该包含哪些路由以及不应该包含哪些路由是一项非常重要的技能。前面已经学习了静态路由和动态路由，在这里通过介绍路由表的结构、路由查找过程和路由行为，以供大家更深入的了解路由表的工作过程。路由表中添加的网络路由来自于多个来源，包括直连网络、静态路由、有类路由协议和无类路由协议。查找过程、有类路由行为和无类路由行为不受路由来源影响。路由表可能会通过 RIPv1 等有类路由协议获取到路由信息，但会使用无类路由行为（no ip classless）来执行查找过程。

①路由表结构

下面的路由表示例包含有直连路由、静态路由、动态路由协议获取的路由。不同路由来源

的路由条目并不影响路由表的结构。

```
Router# show ip route
    * * * 省略部分输出 * * *
    Gateway of last resort is not set
         192.168.0.0/24 is subnetted, 4 subnets
    R       192.168.1.0 [120/1] via 192.168.2.1, 00:00:01, Serial0/0/0
    C       192.168.2.0 is directly connected, Serial0/0/0
    C       192.168.3.0 is directly connected, FastEthernet0/0
    S       192.168.4.0 is directly connected, Serial0/0/1
    C   10.0.0.0/8is directly connected, FastEthernet0/1
```

Cisco IP 路由表并不是一个平面数据库。路由表实际上是一个分层结构，包括若干个层级，在查找路由并转发数据包时，分层结构可加快查找进程。这里我们将路由分为两级讨论，即 1 级路由和 2 级路由。

1 级路由是指子网掩码等于或小于网络地址有类掩码的路由，来源可以是直连网络、静态路由或动态路由协议。如在上面的路由表中的“C　　10.0.0.0/8　is directly connected, FastEthernet0/1”就是 1 级路由。1 级路由可用作：

- 默认路由——是指地址为 0.0.0.0/0 的静态路由。
- 超网路由——是指掩码小于有类掩码的网络地址。
- 网络路由——是指子网掩码等于有类掩码的路由。网络路由也可以是父路由。

最终路由是指包括下一跳 IP 地址和/或送出接口的路由。路由表中的“C　　10.0.0.0/8 is directly connected, FastEthernet0/1”既是一条 1 级路由，也是一条最终路由，因为它包含送出接口 FastEthernet0/1。

在上面的路由表中，包含了父路由和子路由的信息：

```
    192.168.0.0/24 is subnetted, 4 subnets                                  1 级父路由
R       192.168.1.0 [120/1] via 192.168.2.1, 00:00:01, Serial0/0/0          2 级子路由
C       192.168.2.0 is directly connected, Serial0/0/0
C       192.168.3.0 is directly connected, FastEthernet0/0
S       192.168.4.0 is directly connected, Serial0/0/1
```

其中父路由条目中不包含任何下一跳 IP 地址或送出接口信息，此路由称为 1 级父路由。父路由实际上是表示存在 2 级路由的一个标题，2 级路由也称为子路由。只要向路由表中添加一个子网，就会在表中自动创建 1 级父路由。也就是说，只要向路由表中输入一条掩码大于有类掩码的路由，就会在表中生成父路由。在本例中，1 级父路由有 4 条子路由。

2 级路由是指有类网络地址的子网路由。与 1 级路由一样，2 级路由的来源可以是直连网络、静态路由或动态路由协议。注意 Cisco IOS 中的路由表以有类路由方案组织，1 级父路由是子网路由的有类网络地址，即使子网路由的来源是无类路由协议也同样如此。从上面的路由表中可以看到，2 级子路由不包括子网掩码，该子路由的子网掩码是包含在父路由中。2 级子路由也属于最终路由，因为 2 级路由包含下一跳 IP 地址和/或送出接口。另外，必须至少有一条 2 级子路由，1 级父路由才能存在。

无论何时，只要存在属于同一有类网络但具有不同子网掩码的两条或多条子路由，路由表中的显示就会稍有不同，这表明此父网络经过了可变子网划分。

```
Router# show ip route
    * * * 省略部分输出 * * *
    Gateway of last resort is not set
    172.16.0.0/16   is variably subnetted,  3subnets,  2 masks
C       172.16.1.4/30   is directly connected, Serial0/0/0
C       172.16.1.8/30   is directly connected, Serial0/0/1
C       172.16.3.0/24   is directly connected, FastEthernet0/0
```

该例中得父路由包含以下信息：

◆ 172.16.0.0：父路由，它是与所有子路由相关的有类网络地址。

◆ /16：父路由的有类子网掩码。

◆ variably subnetted：表明对子路由进行了可变长子网划分，且此有类网络中有多个掩码。

◆ 3 subnets，2 masks：表示该父路由下面的子网数量和子路由的不同子网掩码数量。

②路由表查找过程

现在介绍路由表的查找过程，帮助理解路由表的工作原理。

首先，路由器会检查 1 级路由（包括网络路由和超网路由），查找与 IP 数据包的目的地址最匹配的路由。如果最佳匹配的路由是 1 级最终路由（有类网络路由、超网路由或默认路由），则会使用该路由转发数据包。如果最佳匹配的路由是 1 级父路由，则继续步骤 2。路由器检查该父路由的子路由（子网路由），以找到最佳匹配的路由。如果在 2 级路由中存在匹配的路由，则会使用该子网转发数据包。

如果所有的 2 级子路由都不符合匹配条件，则要根据路由器当前执行的是有类路由行为还是无类路由行为，如果执行的是有类路由行为，则会终止查找过程并丢弃数据包，如果执行的是无类路由行为，则继续在路由表中搜索 1 级超网路由以寻找匹配条目，要是存在默认路由，也会对其进行搜索。如果此时存在匹配位数相对较少的 1 级超网路由或默认路由，那么路由器会使用该路由转发数据包。如果路由表中没有匹配的路由，则路由器会丢弃数据包。

注意，如果路由条目中仅有下一跳 IP 地址而没有送出接口，那么必须将其解析为具有送出接口的路由。为此会对下一跳 IP 地址执行递归查找，直到将该路由解析为某个送出接口。从路由表中选择路由时，会选择路由表中与数据包的目的 IP 地址从最左侧开始存在最多匹配位数的路由，称为最佳匹配（最长匹配）。通常情况下，最左侧有着最多匹配位数（最长匹配）的路由总是首选路由。当然前提是这几条路由必须达到其子网掩码所指定的最少匹配位数，才会被视为匹配路由。

4.3.4 知识点 4：用 EIGRP 实现网络互联

1. EIGRP 简介

（1）EIGRP 是一种增强型距离矢量路由协议

尽管 EIGRP 被称为增强型距离矢量路由协议，但它仍是一种距离矢量路由协议，它的前身是 IGRP 协议。Cisco 于 1985 年开发出专有的 IGRP，IGRP 的问世解决了 RIPv1 的某些局限性，如使用跳数度量以及网络的最大跳数为 15 跳等。IGRP 和 EIGRP 不使用跳数作为度量，而是使用由带宽、延迟、可靠性和负载组成的综合度量。默认情况下，这两种协议仅使用带宽和延迟。然而，因为 IGRP 是使用贝尔曼-福特（Bellman-Ford）算法和定期更新的一种有类

路由算法，所以其应用在当今的许多网络中都受到了限制。因此，Cisco 使用新算法 DUAL 以及其他功能使 IGRP 得到增强。IGRP 和 EIGRP 的命令相似，甚至在很多情况下相同，这便于从 IGRP 过渡到 EIGRP。Cisco 从 IOS 12.2(13)T 和 12.2(R1s4)S 开始不再支持 IGRP。

现在简单介绍一下传统距离矢量路由协议（例如 RIP 和 IGRP）与增强型距离矢量路由协议 EIGRP 的一些差异：

◆ 传统距离矢量路由协议的特点：

①使用 Bellman-Ford 或 Ford-Fulkerson 算法。

②路由条目会过期，并使用定期更新。

③只跟踪最佳路由，即到达目的网络的最佳路径。

④当目的路由不可用时，路由器必须等待新的路由更新。

⑤抑制计时器降低了收敛速度。

◆ 增强型距离矢量路由协议 EIGRP 的特点：

①使用扩散更新算法 DUAL。

②路由条目不会过期，而且不会使用定期更新。

③在路由表之外还维护一个拓扑表，该拓扑表包含最佳路径和所有无环备用路径，“无环”表示邻居没有通过本路由器到达目的网络的路由。

④当路由不可用时，DUAL 将使用拓扑表中得无环备用路径。

⑤不使用抑制计时器，与传统距离矢量路由协议相比其收敛时间更短。

(2)EIGRP 消息格式

每条 EIGRP 消息都包含该报头，如图 4-16 所示，报头中包括 Opcode（操作码）和 Autonomous System Number（自治系统编号）2 个字段。操作码用于指定 EIGRP 数据包类型：更新、查询、应答、Hello。自治系统（AS）编号用于指定 EIGRP 路由进程。Cisco 路由器可以运行多个 EIGRP 实例，这一点与 RIP 不同。AS 编号用于跟踪不同的 EIGRP 实例。

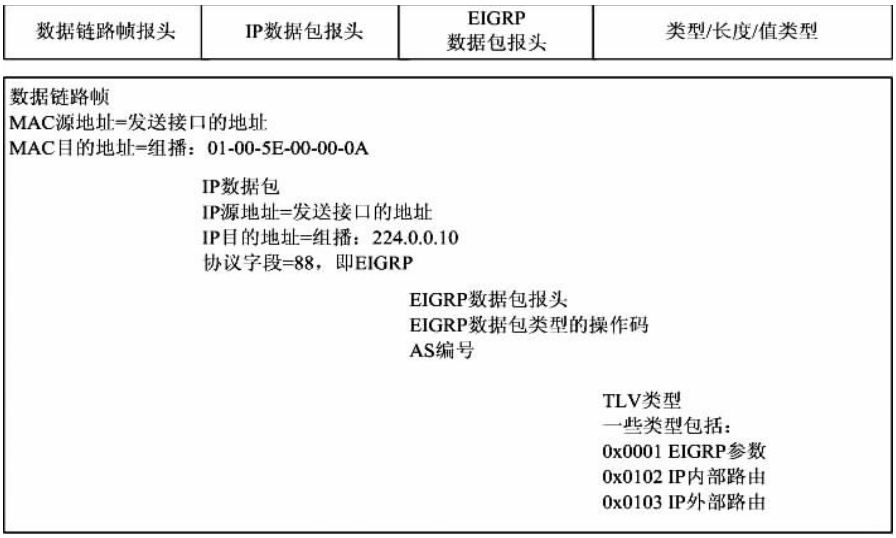


图 4-16　EIGRP 消息格式

EIGRP 参数 TLV 消息包含 EIGRP 用于计算其复合度量的权重，如表 4-8 所示。默认情况下，仅对带宽和延迟计权。它们的权重相等，因此，用于带宽的 K1 字段和用于延迟的 K3 字

段都被设为 1,其他 K 值则被设为零。等待时间(也称保留时间)是收到此消息的 EIGRP 邻居在认为发出通告的路由器发生故障之前应该等待的时长。

表 4-8　　EIGRP 参数 TLV

类型＝0x0001		长度	
K1	K2	K3	K4
K5	保留	等待时间	

(3)PDM 协议相关模块

EIGRP 可以路由多种不同的协议(包括 IP、IPX 和 AppleTalk),通过使用 PDM(协议相关模块)实现。PDM 负责处理与每个网络层协议对应的特定路由任务。

(4)RTP 和 EIGRP 数据包类型

可靠传输协议(RTP)是 EIGRP 用于发送和接收 EIGRP 数据包的协议。EIGRP 被设计为与网络层无关的路由协议,因此它无法使用 UDP 或 TCP 的服务,原因在于 IPX 和 Appletalk 不使用 TCP/IP 协议簇中的协议。RTP 包括 EIGRP 数据包的可靠传输和不可靠传输两种方式,它们分别类似于 TCP 和 UDP,可靠 RTP 需要接收方向发送方返回一个确认,不可靠的 RTP 数据包不需要确认。RTP 能以单播或组播方式发送数据包。

EIGRP 使用五种不同的数据包类型,某些类型会成对使用:

①Hello 数据包用于发现邻居并与所发现的邻居建立邻接关系。EIGRP hello 数据包以组播方式发送,且使用不可靠传输。

②更新数据包用于传播路由信息。与 RIP 不同的是,EIGRP 不发送定期更新,而仅在必要时才发送更新数据包。EIGRP 更新仅包含需要的路由信息,且仅发送给需要该信息的路由器。EIGRP 更新数据包使用可靠传输。当多台路由器需要更新数据包时,通过组播发送;当只有一台路由器需要更新数据包时,则通过单播发送。

③确认(ACK)数据包由 EIGRP 在使用可靠传输时发送。对于 EIGRP 更新、查询和应答数据包,RTP 使用可靠传输。EIGRP 确认数据包始终以不可靠单播方式发送。EIGRP 确认数据包使用不可靠传输。

④查询和应答数据包由 DUAL 在搜索网络以及进行其他任务时使用。查询和应答使用可靠传输。查询可以使用组播或单播,但应答则始终以单播发送。

(5)hello 协议

EIGRP 必须首先发现其邻居,才能在路由器间交换 EIGRP 数据包。EIGRP 邻居是指在直连的共享网络上运行 EIGRP 的其他路由器。EIGRP 使用 Hello 数据包来发现相邻路由器并与之建立邻接关系。在大多数网络中,每 5 秒发送一次 EIGRP Hello 数据包。在多点 NBMA(非广播多路访问)网络上,例如 X.25、帧中继和带有 T1 [1.544 Mbps] 或更慢访问链路的 ATM 接口上,每 60 秒单播一次 Hello 数据包,如表 4-9 所示。EIGRP 路由器假定,只要它还能收到邻居发来的 Hello 数据包,该邻居及其路由就仍然保持活动。

表 4-9　　EIGRP hello 间隔

带宽	链路示例	默认 hello 间隔时间	默认等待时间
1.544Mbps	多点、帧中继	60s	180s
大于 1.544Mbps	T1、以太网	5s	15s

等待时间用于告诉路由器在宣告邻居无法到达前应等待该设备发送下一个 Hello 的最长时间。默认情况下，保留时间是 Hello 间隔时间的三倍，即在大多数网络上为 15 秒，在低速 NBMA 网络上则为 180 秒。等待时间截止后，EIGRP 将宣告该路由发生故障，而 DUAL 则将通过发出查询来寻找新路径。

(6)EIGRP 限定更新

与 RIP 不同的是，EIGRP 不发送定期更新，而仅在路由度量发生变化时才发送更新。EIGRP 更新数据包的方式为部分或限定更新。部分更新是指更新仅包含与路由变化相关的信息。EIGRP 在目的地状态变化时发送这些增量更新，而非发送路由表的全部内容。限定更新是指部分更新仅传播给受变化影响的路由器。部分更新自动“受到限定”，只有需要该信息的路由器才会被更新。EIGRP 仅发送必要的信息且仅向需要该信息的路由器发送，从而将发送 EIGRP 数据包时占用的带宽降到最低。

(7)DUAL 简介

网络中得路由环路即使只是暂时性存在，也会极大地损害网络性能。诸如 RIP 等距离矢量路由协议使用抑制计时器和水平分隔来防止路由环路。尽管 EIGRP 也使用这两种技术，但使用方式有所不同，EIGRP 用于收敛和防止路由环路的主要方式是使用扩散更新算法(DUAL)算法。DUAL 算法用于让路由计算始终能避免路由环路，这使拓扑更改所涉及的所有路由器可以同时得到同步，未受拓扑更改影响的路由器不参与重新计算。此方法使 EIGRP 与其他距离矢量路由协议相比具有更快的收敛时间。

所有路由计算的决策过程由 DUAL 有限状态机完成。通俗地说，有限状态机 (FSM) 是一种行为模型，由有限数量的状态、状态之间的转变以及造成状态转变的事件或操作组成。DUAL 维护一个备用路由列表，其中包含它已确定为无环路由的备用路由。如果路由表中的主路由发生故障，则最佳的备用路由会立即添加到路由表中，加快了收敛速度。

(8)管理距离

内部 EIGRP 路由的默认管理距离为 90，而从外部来源(例如默认路由)导入的 EIGRP 路由的默认管理距离为 170。相比其他的内部网关协议 (IGP)，EIGRP 是 Cisco IOS 最优先选择的协议，因为其管理距离最低。

2. 基本 EIGRP 配置

(1)自治系统和进程 ID

自治系统 (AS) 是由单个实体管理的一组网络，这些网络通过统一的路由策略连接到 Internet。有关创建、选择和注册自治系统的指导原则在 RFC 1930 中规定，AS 编号由互联网编号指派机构 (IANA) 分配，该机构同时也负责分配 IP 地址空间。当地 RIR 负责从其获得的 AS 编号块中为实体分配编号。AS 编号长度为 32 位，可用编号数目增加到超过 40 亿个。需要自治系统编号的通常为 ISP(Internet 服务提供商)、Internet 主干提供商以及连接其他实体的大型机构。这些 ISP 和大型机构使用外部网关路由协议 BGP(边界网关协议)来传播路由信息。BGP 是唯一一个在配置中使用实际自治系统编号的路由协议。使用 IP 网络的绝大多数公司和机构不需要 AS 编号，因为它们都由诸如 ISP 等更高一级的机构来管理，这些公司在自己的网络内部使用 RIP、EIGRP、OSPF 和 IS-IS 等内部网关协议来路由数据包，它们是 ISP 的自治系统内各自独立的诸多网络之一，ISP 负责在自治系统内以及与其他自治系统之间路由

数据包。

EIGRP 和 OSPF 都使用一个进程 ID 来代表各自在路由器上运行的协议实例。

```
Router(config)# router eigrp autonomous-system
```

尽管 EIGRP 将该参数称为“自治系统”编号，它实际上起进程 ID 的作用。此编号与前面谈到的自治系统编号无关，您可以为其分配任何 16 位值。为建立邻接关系，EIGRP 要求使用同一个进程 ID 来配置同一个路由域内的所有路由器。一般来说，在一台路由器上，只会为每个路由协议配置一个进程 ID。RIP 不使用进程 ID，它只支持一个 RIP 实例。EIGRP 和 OSPF 都支持各自路由协议的多个实例，但实际上一般不需要或不推荐实施这种多路由协议的情况。

(2)router eigrp 命令

router eigrp autonomous-system 命令用于启用 EIGRP，该 autonomous-system 参数(进程 ID 号)由网络管理员选择，取值范围在 1 到 65535 之间，该编号很重要，因为此 EIGRP 路由域内的所有路由器都必须使用同一个进程 ID 号。

(3)network 命令

EIGRP 中的 network 命令与其他 IGP 路由协议中的 network 命令功能相同：此路由器上任何符合 network 命令中的网络地址的接口都将被启用，可发送和接收 EIGRP 更新，此网络(或子网)将包括在 EIGRP 路由更新中。

```
Router(config-router)# network network-address
```

network-address 是此接口的有类网络地址。当在 R2 上配置好 EIGRP 后，DUAL 向控制台发送一个通知消息，说明已与另一台 EIGRP 路由器建立了邻接关系，此邻接关系自动建立。默认情况下，当在 network 命令中使用诸如 172.16.0.0 等有类网络地址时，该路由器上属于该有类网络地址的所有接口都将启用 EIGRP。但是如果要配置 EIGRP 以仅通告特定子网，可以使用以下命令：

```
Router(config-router)# network network-address wildcard-mask
```

通配符掩码 (wildcard-mask) 可看作子网掩码的反掩码，如子网掩码 255.255.0.0 的反掩码为 0.0.255.255。如 network 172.16.1.0 0.0.0.255 特指通告 172.16.1.0/24 子网。

(4)修改 EIGRP 度量

EIGRP 在其复合度量中使用带宽、延迟、可靠性和负载来计算通向网络的首选路径，默认使用带宽和延迟。EIGRP 复合度量的计算公式如下：

度量=[k1 * 带宽+(k2 * 带宽)/(256-负载)+k3 * 延迟] * [k5/(可靠性)+k4]

默认 k1=1(带宽)，k2=0(负载)，k3=1(延迟)，k4=0(可靠性)，k5=0(可靠性)。可以使用以下命令更改 k 值：

```
Router(config-router)#metric weights tos k1 k2 k3 k4 k5
```

下面我们介绍 EIGRP 默认使用的两种度量，带宽和延迟。带宽度量 (1544 Kbit) 是一种静态值。EIGRP 和 OSPF 等路由协议使用带宽来计算路由度量，带宽以 Kbit(千比特)为单位显示。大多数串行接口使用默认带宽值 1544 Kbit(即 1.544 Mbps)，这是 T1 连接的带宽。然而，某些串行接口使用不同的默认带宽值。可以使用 show interface 命令来检验带宽。该带宽值可能无法反映出接口的实际物理带宽，如果链路的实际带宽与默认带宽不相等，您就应该修改该带宽值，修改该带宽值不会更改该链路的实际带宽。使用接口命令 bandwidth 修改带宽度量：

```
Router(config-if)# bandwidth kilobits
```

使用接口命令 no bandwidth 恢复为默认值。修改带宽时，必须同时在链路两端进行，才能确保两个方向上的正确路由。

延迟是衡量数据包通过路由所需时间的指标。延迟（DLY）度量是一种静态值，它以接口所连接的链路类型为基础，单位为微秒。延迟不是动态测得的，路由器并不会实际跟踪数据包达到目的地所需的时间。延迟值与带宽值相似，都是一种默认值，可由网络管理员更改，如表 4-10所示。

表 4-10　　传输介质延迟

介质	延迟(单位:微秒)
100M ATM	100
快速以太网	100
FDDI	100
1HSSI	20000
16M 令牌环	630
以太网	1000
T1(串行默认)	20000
512K	20000
DSO	20000
56K	20000

(5)检验 EIGRP

路由器必须与其邻居建立邻接关系，EIGRP 才能发送或接收更新，EIGRP 路由器通过与相邻路由器交换 EIGRP Hello 数据包来建立邻接关系。使用 show ip route 命令来查看路由表：

```
Router# show ip route
    * * * 省略部分输出 * * *
    Gateway of last resort is not set

        10.0.0.0/30 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Loopback1
        172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       172.16.0.0/16 is a summary, 00:01:31, Null0          D 表示 EIGRP 路由
C       172.16.3.0/30 is directly connected, Serial0/0/0
        192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 00:01:31, Null0
D       192.168.10.4/30 [90/2681856] via 192.168.10.10, 00:00:26, Serial0/0/1
C       192.168.10.8/30 isdirectly connected, Serial0/0/1
```

使用 show ip eigrp neighbors 命令来查看邻居表并检验 EIGRP 是否已与其邻居建立邻接关系，并能看到相邻路由器的 IP 地址以及通向该 EIGRP 邻居的接口。

```
Router# show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface     Hold     Uptime   SRTT   RTO   Q   Seq
                                  (sec)           (ms)        Cnt  Num
0   172.16.3.1      Se0/0/0       12     00:03:07  40     1000  0   9
1   192.168.10.10   Se0/0/1       10     00:02:24  40     1000  0   3
```

show ip eigrp neighbor 命令的输出包括：

◆ H 栏：按照发现顺序列出邻居。

◆ Address：该邻居的 IP 地址。

◆ Interface：收到此 Hello 数据包的本地接口。

◆ Hold：当前的保留时间。每次收到 Hello 数据包时，此值即被重置为最大保留时间，然后倒计时，到零为止。如果到达了零，则认为该邻居进入“down”。

◆ Uptime(运行时间)：从该邻居被添加到邻居表以来的时间。

◆ SRTT(平均回程计时器)和 RTO(重传间隔)：由 RTP 用于管理可靠 EIGRP 数据包。

◆ Queue Count(队列数)：通常为 0。如果大于 0，则说明有 EIGRP 数据包等待发送。

◆ Sequence Number(序列号)：用于跟踪更新、查询和应答数据包。

也可使用 show ip protocols 命令来检验 EIGRP 是否已启用。对于不同的路由协议，show ip protocols 命令将显示不同类型的输出。

```
Router# show ip protocols
    Routing Protocol is " eigrp  1 "
      Outgoing update filter list for all interfaces is not set
      Incoming update filter list for all interfaces is not set
      Default networks flagged in outgoing updates
      Default networks accepted from incoming updates
      EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
      EIGRP maximum hopcount 100
      EIGRP maximum metric variance 1
    Redistributing: eigrp 1
      Automatic network summarization is in effect
    Automatic address summarization:
    172.16.0.0/16 for Serial0/0/1
    Summarizing with metric 2169856
        192.168.10.0/24 for Serial0/0/0
          Summarizing with metric 2169856
      Maximum path: 4
      Routing for Networks:
        172.16.0.0
        192.168.10.0
      Routing Information Sources:
        Gateway         Distance      Last Update
        172.16.3.1           90          5860
```

```
        192.168.10.10       90          8893
    Distance: internal 90 external 170
```

3. DUAL

(1)DUAL 概念

下面我们来学习 DUAL 确定最佳无环路径和无环备用路径的方法,DUAL 中最常用的概念包括:

- 后继路由器。
- 可行距离 (FD)。
- 可行后继路由器 (FS)。
- 报告距离 (RD),或称通告距离 (AD)。
- 可行条件,或称可行性条件 (FC)。

这些概念是 DUAL 的环路避免机制的核心。DUAL 算法为 EIGRP 提供最佳无环路径、无环备用路径,并能促进 EIGRP 快速收敛,通过限定更新降低 EIGRP 的带宽使用率。下面我们以图 4-17 的拓扑为例,讲解这几个重要概念。

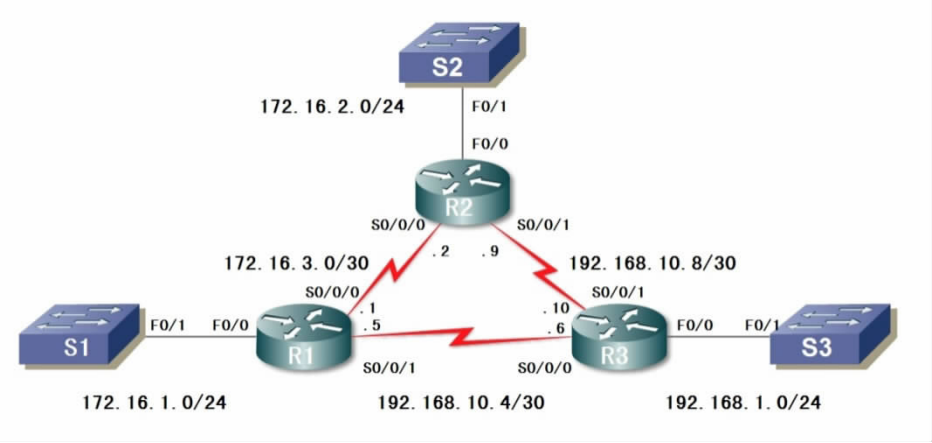


图 4-17　DUAL

(2)后继路由器和可行距离

后继路由器是指用于转发数据包的一台相邻路由器,该路由器是通向目的网络的开销最低的路由。后继路由器的 IP 地址显示在路由表条目中,紧随单词 via。

可行距离 (FD) 是计算出的通向目的网络的最低度量。FD 是路由表条目中所列的度量,就是括号内的第二个数字。与其他路由协议中的情况一样,它也称为路由度量。

```
R2# show ip route
    * * * 省略部分输出 * * *
Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D       172.16.0.0/16 is a summary, 00:06:42, Null0
D       172.16.1.0/24 [90/40514560] via 172.16.3.1, 00:06:47, Serial0/0/0
C       172.16.2.0/24 is directly connected, FastEthernet0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
```

```
D    192.168.1.0/24 [90/3014400] via 192.168.10.10, 00:06:38, Serial0/0/1
                                        此路由的可行距离是 3014400,后继路由器是 192.168.10.10
     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 00:06:42, Null0
D       192.168.10.4/30 [90/3523840] via 192.168.10.10, 00:06:38, Serial0/0/1
C       192.168.10.8/30 isdirectly connected, Serial0/0/1
```

(3)可行后继路由器、可行性条件和报告距离

在拓扑变化时,DUAL 之所以收敛速度快,原因之一就在于它使用通向其他路由器的备用路径,这些路由器称为可行后继路由器,备用路径使得无需重新计算 DUAL。

可行后继路由器(FS)是指一个邻居,它有一条通向后继路由器所连通的同一个目的网络的无环备用路径,并且满足可行性条件。当邻居通向一个网络的报告距离 (RD) 比本地路由器通向同一个目的网络的可行距离短时,即符合了可行性条件 (FC)。报告距离(或称通告距离)即为 EIGRP 邻居通向相同目的网络的可行距离。报告距离是路由器向邻居报告的、有关自身通向该网络的开销的度量。

```
R2# show ip eigrp topology
    IP-EIGRP Topology Table for AS 1
    Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply, r - Reply status

    P 192.168.10.8/30, 1 successors, FD is 3011840
    via Connected, Serial0/0/1
    P 172.16.3.0/30, 1 successors, FD is 40512000
            via Connected, Serial0/0/0
    P 192.168.1.0/24, 1 successors, FD is 3014400
          via 192.168.10.10 (3014400/28160), Serial0/0/1
    via 172.16.3.1 (41026560/2172416), Serial0/0/0
    P 172.16.2.0/24, 1 successors, FD is 28160
            via Connected, FastEthernet0/0
    P 172.16.1.0/24, 1 successors, FD is 40514560
            via 172.16.3.1 (40514560/28160), Serial0/0/0
    P 172.16.0.0/16, 1 successors, FD is 28160
            via Summary (28160/0), Null0
    P 192.168.10.0/24, 1 successors, FD is 3011840
            via Summary (3011840/0), Null0
    P 192.168.10.4/30, 1 successors, FD is 3523840
            via 192.168.10.10 (3523840/2169856), Serial0/0/1
```

对于 R2 的 show ip eigrp topology 命令输出的拓扑表中网络 192.168.1.0/24 的条目的每个部分的详细说明如下:

P 192.168.1.0/24, 1 successors, FD is 3014400

◆ P:该路由处于被动状态。当 DUAL 当前未执行扩散计算来确定通向一个网络的路径时,该路由将处于稳定模式,即被动状态。如果 DUAL 正在重新计算或搜索新路径时,该路径将处于主动状态。对于稳定的路由域来说,该拓扑表中的所有路由都应该处于被动状态。如果该路由"陷入主动状态",DUAL 将显示一个 A 字符。

◆ 192.168.1.0/24:目的网络,也可在路由表中找到。

◆ 1 successors:显示通向此网络的后继路由器数量。如果存在通向此网络的多条等价路径,则会有多台后继路由器。

◆ FD is 3014400:这是可行距离,即通向目的网络的 EIGRP 度量。

via 192.168.10.10 (3014400/28160), Serial0/0/1

◆ via 192.168.10.10:后继路由器(即 R3)的下一跳地址。此地址显示在路由表中。

◆ 3014400:通向 192.168.1.0/24 的可行距离,这是路由表中所示的度量。

◆ 28160:后继路由器通向此网络的报告距离,即 R3 的开销。

◆ Serial0/0/1:通向此网络的出站接口,也显示在路由表中。

via 172.16.3.1 (41026560/2172416), Serial0/0/0,显示了具有可行后继路由器:

◆ via 172.16.3.1:可行后继路由器(即 R1)的下一跳地址。

◆ 41026560:如果 R1 成为新的后继路由器,这将是 R2 通向 192.168.1.0/24 的新的可行距离。

◆ 2172416:可行后继路由器通向该网络的报告距离,即 R1 的度量。此值 (RD) 必须比当前 FD (3014400) 小才能符合可行性条件。

◆ Serial0/0/0:通向可行后继路由器的出站接口。

show ip eigrp topology all-links 命令会显示通向一个网络的所有可能路径,其中包括后继路由器、可行后继路由器,甚至还包括那些不是可行后继路由器的路由。EIGRP 是一种距离矢量路由协议,不具备洞察网络的完整无环拓扑图的能力。DUAL 用于确保邻居具有无环路径的方法是要求邻居满足可行性条件。路由器通过确保邻居的 RD 比自己的 FD 小,即可假定此相邻路由器不是自己已通告的路由的一部分,因此可以始终避免形成路由环路的可能。

4.3.5　知识点 5:用 OSPF 实现网络互联

1. 链路状态路由协议

链路状态路由协议又称为最短路径优先协议,基于 Edsger Dijkstra 的 SPF(最短路径优先)算法。Dijkstra 算法通常称为 SPF(最短路径优先)算法。此算法会累计每条路径从源到目的地的开销。每台路由器都会站在自己的角度计算 SPF 算法并确定开销。链路状态路由协议比距离矢量路由协议复杂得多,但基本功能和配置却很简单。基本的 OSPF 运算可使用 router ospf process-id 命令和一个 network 语句来配置,这一点与 RIP 和 EIGRP 等其他路由协议相似。

(1)链路状态路由协议的工作过程

所有路由器通过下列链路状态通用路由过程来达到收敛:

①每台路由器了解其自身的链路(即与其直连的网络)。这通过检测哪些接口处于工作状态来完成。

对于链路状态路由协议来说,链路是路由器上的一个接口。与距离矢量协议和静态路由一样,链路状态路由协议也需要下列条件才能了解链路:正确配置接口的 IP 地址和子网掩码并将链路设置为 up 状态。还有一点相同的是:必须将接口包括在一条 network 语句中,该接口才能参与链路状态路由过程。

有关各条链路的状态的信息称为链路状态. 如图所示,这些信息包括:

- 接口的 IP 地址和子网掩码。
- 网络类型,例如以太网(广播)链路或串行点对点链路。
- 该链路的开销。
- 该链路上的所有相邻路由器。

②每台路由器负责“问候”直连网络中的相邻路由器。与 EIGRP 路由器相似,链路状态路由器通过直连网络中的其他链路状态路由器互换 Hello 数据包来达到此目的。

与 EIGRP 的 Hello 数据包相似,当两台链路状态路由器获悉它们是邻居时,将形成一种相邻关系。这些小型 Hello 数据包持续在两个相邻的邻居之间互换,以此实现“保持生存”功能来监控邻居的状态。如果路由器不再收到某邻居的 Hello 数据包,则认为该邻居已无法到达,该相邻关系破裂。

③每台路由器创建一个链路状态数据包 (LSP),其中包含与该路由器直连的每条链路的状态。通过记录每个邻居的所有相关信息(包括邻居 ID、链路类型和带宽)来完成。

路由器一旦建立了相邻关系,即可创建链路状态数据包 (LSP),其中包含与该链路相关的链路状态信息。

④每台路由器将 LSP 泛洪到所有邻居,然后邻居将收到的所有 LSP 存储到数据库中。接着,各个邻居将 LSP 泛洪给自己的邻居,直到区域中的所有路由器均收到那些 LSP 为止。每台路由器会在本地数据库中存储邻居发来的 LSP 的副本。

每台路由器将其链路状态信息泛洪到路由区域内的其他所有链路状态路由器。路由器一旦接收到来自相邻路由器的 LSP,立即将该 LSP 从除接收该 LSP 的接口以外的所有接口发出。此过程在整个路由区域内的所有路由器上形成 LSP 的泛洪效应。

路由器接收到 LSP 后,几乎立即将其泛洪出去,不经过中间计算。距离矢量路由协议则不同,该协议必须首先运行贝尔曼-福特 (Bellman-Ford) 算法来处理路由更新,然后 才将它们发送给其他路由器;而链路状态路由协议则在泛洪完成后 再计算 SPF 算法。因此,链路状态路由协议达到收敛状态的速度比距离矢量路由协议快得多。

除链路状态信息外,LSP 中还包含其他信息(例如序列号和过期信息),以帮助管理泛洪过程。每台路由器都采用这些信息来确定是否已从另一台路由器接收过该 LSP 以及 LSP 是否带有链路信息数据库中没有的更新信息。此过程使路由器可在其链路状态数据库中仅保留最新的信息。

⑤每台路由器使用数据库构建一个完整的拓扑图并计算通向每个目的网络的最佳路径。就像拥有了地图一样，路由器现在拥有关于拓扑中所有目的地以及通向各个目的地的路由的详图。SPF 算法用于构建该拓扑图并确定通向每个网络的最佳路径。

每台路由器使用链路状态泛洪过程将自身的 LSP 传播出去后，每台路由器都将拥有来自整个路由区域内所有路由器的 LSP。这些 LSP 存储在链路状态数据库中。现在，路由区域内的每台路由器都可以使用 SPF 算法来构建您之前了解过的 SPF 树。

每台路由器使用来自其他所有路由器的信息独立构建自己的 SPF 树。为确保正确路由，所有路由器上用于创建 SPF 树的链路状态数据库必须相同。

(2)链路状态路由协议的特点

①优点

与距离矢量路由协议相比，链路状态路由协议有几个优点：

◆ 每台路由器自行创建网络拓扑图以确定最短路径，而距离矢量路由协议没有此功能。

◆ 立即泛洪 LSP，实现更快的收敛。使用距离矢量路由协议的路由器需要处理每个路由更新，并且在更新完路由表后才能将更新从路由器接口泛洪出去。

◆ 仅当拓扑发生变化时才发送 LSP，且该 LSP 仅包含与该变化相关的信息。而距离矢量路由协议通常会发送定期更新。

◆ 多区域实施时采用了层次式设计。多个区域形成了层次状的网络结构，这有利于路由聚合(总结)，还便于将路由问题隔离在一个区域内。

②要求

现代链路状态路由协议设计旨在尽量降低对内存、CPU 和带宽的影响，使用并配置多个区域可减小链路状态数据库，划分多个区域还可限制在路由域内泛洪的链路状态信息的数量，并可仅将 LSP 发送给所需的路由器。例如，当拓扑发生变化时，仅处于受影响区域的那些路由器会收到 LSP 并运行 SPF 算法。这有助于将不稳定的链路隔离在路由域中的特定区域内。

与距离矢量路由协议相比，链路状态路由协议通常需要占用更多的内存、CPU 运算量和带宽。对内存的要求源于使用了链路状态数据库和创建 SPF 树的需要。与 Bellman-Ford 等距离矢量算法相比，SPF 算法需要更多的 CPU 时间，因为链路状态路由协议会创建完整的拓扑图。链路状态数据包泛洪会对网络的可用带宽产生负面影响。这只应该出现在路由器初始启动过程中，但在不稳定的网络中也可能导致问题。

2. OSPF 简介

(1)OSPF 消息封装

OSPF 消息的数据部分封装在数据包内。此数据字段可能包含五种 OSPF 数据包类型之一。无论每个 OSPF 数据包的类型如何，都具有 OSPF 数据包报头。OSPF 数据包报头和数据包类型特定的数据被封装到 IP 数据包中。在该 IP 数据包报头中，协议字段被设为 89 以代表 OSPF，目的地址则被设为以下两个组播地址之一：224.0.0.5 或 224.0.0.6。如果 OSPF 数据包被封装在以太网帧内，则目的 MAC 地址也是一个组播地址：01-00-5E-00-00-05 或 01-00-

5E-00-00-06，如图 4-18 所示。

图 4-18　OSPF 数据包报头

(2)OSPF 数据包类型

前面介绍了链路状态数据包（LSP），有五种类型的数据包，每种数据包在 OSPF 路由过程中发挥各自的作用：

◆ Hello：Hello 数据包用于与其他 OSPF 路由器建立和维持相邻关系。

◆ DBD：DBD(数据库说明)数据包包含发送方路由器的链路状态数据库的简略列表，接收方路由器使用本数据包与其本地链路状态数据库对比。

◆ LSR：随后，接收方路由器可以通过发送链路状态请求（LSR）数据包来请求 DBD 中任何条目的有关详细信息。

◆ LSU：链路状态更新（LSU）数据包用于回复 LSR 和通告新信息。LSU 包含七种类型的链路状态通告（LSA）。

◆ LSAck：路由器收到 LSU 后，会发送一个链路状态确认（LSAck）数据包来确认接收到了 LSU。

(3)Hello 协议

表 4-11 为 OSPF 数据包报头和 Hello 数据包。Hello 数据包用于：

表 4-11　　Hello 数据包格式

0　　7	8　　15	16　　23	24　　31
版本	类型＝1	数据包长度	
路由器 ID			
区域 ID			
校验和		身份验证类型	
身份验证			
身份验证			
网络掩码			

（续表）

Hello 间隔	选项	路由器优先级
路由器 Dead 间隔		
指定路由器 DR		
备用指定路由器 BDR		
邻居列表		

◆发现 OSPF 邻居并建立相邻关系。

◆通告两台路由器建立相邻关系所必需统一的参数。

◆在以太网和帧中继网络等多路访问网络中选举指定路由器（DR）和备用指定路由器（BDR）。

表 4-11 中各字段的意义：

◆类型：OSPF 数据包类型：Hello（1）、DD（2）、LS 请求（3）、LS 更新（4）或 LS 确认（5）。

◆路由器 ID：始发路由器的 ID。

◆区域 ID：数据包的始发区域。

◆网络掩码：与发送方接口关联的子网掩码。

◆Hello 间隔：发送方路由器连续两次发送 hello 数据包之间的秒数。

◆路由器优先级：用于 DR/BDR 选举。

◆指定路由器（DR）：DR 的路由器 ID。

◆备用指定路由器（BDR）：BDR 的路由器 ID。

◆邻居列表：列出相邻路由器的 OSPF 路由器 ID。

在 OSPF 路由器可将其链路状态泛洪给其他路由器之前，必须确定在其每个链路上是否存在其他 OSPF 邻居。OSPF Hello 中的信息包括发送方路由器的 OSPF 路由器 ID（路由器 ID 将在后续部分中讨论）。如果通过一个接口收到 OSPF Hello 数据包，即可确认该链路上存在另一台 OSPF 路由器。随后，OSPF 即与该邻居建立相邻关系。两台路由器在建立 OSPF 相邻关系之前，必须统一三个值：Hello 间隔、Dead 间隔和网络类型。

OSPF Hello 间隔表示 OSPF 路由器发送其 Hello 数据包的频度。默认情况下，在多路访问网段和点对点网段中每 10 秒钟发送一次 OSPF Hello 数据包，而在非广播多路访问（NBMA）网段（帧中继、X.25 或 ATM）中则每 30 秒钟发送一次 OSPF Hello 数据包。在多数情况下，OSPF Hello 数据包都会通过组播发送给 ALLSPFRouters 的专用地址 224.0.0.5。由于使用了组播地址，设备的接口如果未启用为接收 OSPF 数据包，则会忽略这些数据包。这样可节省非 OSPF 设备的 CPU 处理时间。

Dead 间隔是路由器在宣告邻居进入 down（不可用）状态之前等待该设备发送 Hello 数据包的时长，单位为秒。Cisco 所用的默认断路间隔为 Hello 间隔的四倍。对于多路访问网段和点对点网段，此时长为 40 秒；而对于 NBMA 网络，则为 120 秒。如果 Dead 间隔已到期，而路由器仍未收到邻居发来的 Hello 数据包，则会从其链路状态数据库中删除该邻居。路由器会将该邻居连接断开的信息通过所有启用了 OSPF 的接口以泛洪的方式发送出去。

为减小多路访问网络中的 OSPF 流量，OSPF 会选举一个指定路由器（DR）和一个备用指

定路由器（BDR）。当多路访问网络中发生变化时，DR 负责使用该变化信息更新其他所有 OSPF 路由器（称为 DROther）。BDR 会监控 DR 的状态，并在当前 DR 发生故障时接替其角色。

（4）OSPF 链路状态更新

链路状态更新（LSU）数据包用于 OSPF 路由更新。一个 LSU 数据包可能包含十种类型的链路状态通告（LSA）。链路状态更新（LSU）和链路状态通告（LSA）之间的差异有时较难分清，有时可以互换使用。一个 LSU 包含一个或多个 LSA，这两个概念中的任何一个都可用于表示由 OSPF 路由器传播的链路状态信息，如表 4-12 所示。

表 4-12　　OSPF 数据包类型

类型	数据包名称	说明
1	Hello	发现邻居并与其建立邻接关系
2	DBD	在路由器间检查数据库同步情况
3	LSR	由一台路由器发往另一台路由器请求特定的链路状态记录
4	LSU	发送所请求的特定链路状态记录
5	LSAck	确认其他数据包类型

（5）OSPF 算法

每台 OSPF 路由器都会维持一个链路状态数据库，其中包含来自其他所有路由器的 LSA。一旦路由器收到所有 LSA 并建立其本地链路状态数据库，OSPF 就会使用 Dijkstra 的最短路径优先（SPF）算法创建一个 SPF 树。然后根据 SPF 树，使用通向每个网络的最佳路径填充 IP 路由表。

（6）管理距离

管理距离（AD）是路由来源的可信度（即优先程度）。OSPF 的默认管理距离为 110。

3. 基本 OSPF 配置

（1）router ospf 命令

OSPF 通过 router ospf process-id 全局配置命令启用：

```
R1(config)# router ospf process-id
```

process-id 是一个介于 1 和 65535 之间的数字，由网络管理员选定。process-id 仅在本地有效，这意味着路由器之间建立相邻关系时无需匹配该值。这一点与 EIGRP 不同。EIGRP 进程 ID 必须匹配，两个 EIGRP 邻居才能建立相邻关系。

（2）network 命

OSPF 中的 network 命令与其他 IGP 路由协议中的 network 命令具有相同的功能：

路由器上任何符合 network 命令中的网络地址的接口都将启用，可发送和接收 OSPF 数据包，此网络（或子网）将被包括在 OSPF 路由更新中。

```
Router(config-router)# network network-address wildcard-mask area area-id
```

◆ network-address 和 wildcard-mask 参数用于指定此 network 命令启用的接口或接口范围，指某特定子网。就像在 EIGRP 中一样，通配符掩码可配置为子网掩码的反码。

◆ area area-id 指 OSPF 区域。OSPF 区域是共享链路状态信息的一组路由器。相同区域

内的所有 OSPF 路由器的链路状态数据库中必须具有相同的链路状态信息，这通过路由器将各自的链路状态泛洪给该区域内的其他所有路由器来实现。OSPF 网络可配置为单区域，也可配置为多区域。将大型 OSPF 网络配置为多区域有很多好处，比如可减小链路状态数据库，还可以将不稳定的网络问题隔离在一个区域之内。如果所有路由器都处于同一个 OSPF 区域，则必须在所有路由器上使用相同的 area-id 来配置 network 命令。尽管可使用任何 area-id，但比较好的做法是在单区域 OSPF 中使用 area-id 0。

```
Router# show ip route
    * * * 省略部分内容 * * *
    Gateway of last resort is 192.168.10.10 to network 0.0.0.0
    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
    C       10.2.2.2/32 is directly connected, Loopback0
    C       10.10.10.0/24 is directly connected, FastEthernet0/0
    172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
    O       172.16.1.16/28 [110/129] via 192.168.10.10, 00:22:50, Serial0/0/1
                                                                    OSPF 路由
    O       172.16.1.32/29 [110/65] via 192.168.10.10, 00:22:50, Serial0/0/1
        192.168.10.0/30 is subnetted, 3 subnets
    C       192.168.10.0 is directly connected, Serial0/0/0
    O       192.168.10.4 [110/128] via 192.168.10.10, 00:22:50, Serial0/0/1
    C       192.168.10.8 is directly connected, Serial0/0/1
    O * E2 0.0.0.0/0 [110/1] via 192.168.10.10, 00:22:50, Serial0/0/1
```

(3)OSPF 路由器 ID

OSPF 路由器 ID（即 router ID)用于唯一标识 OSPF 路由域内的每台路由器。一个路由器 ID 其实就是一个 IP 地址。Cisco 路由器按下列顺序确定路由器 ID：

①使用通过 OSPF router-id 命令配置的 IP 地址。

②如果未配置 router-id，则路由器会选择其所有环回接口的最高 IP 地址。

③如果未配置环回接口，则路由器会选择其所有物理接口的最高活动 IP 地址。

如果 OSPF 路由器未使用 OSPF router-id 命令进行配置，也未配置环回接口，则其 OSPF 路由器 ID 将为其所有接口上的最高活动 IP 地址。该接口并不需要启用 OSPF，就是说不需要将其包括在 OSPF network 命令中。然而，该接口必须是 up 状态。

可用于验证路由器 ID 的一个命令为 show ip protocols。某些 IOS 版本并不象图中所示那样显示路由器 ID。在那些情况下，请使用 show ip ospf 或 show ip ospf interface 命令检验路由器 ID。

```
Router# show ip protocols
    Routing Protocol is "ospf 1"
      Outgoing update filter list for all interfaces is not set
      Incoming update filter list for all interfaces is not set
      Router ID 10.2.2.2                                  本路由器的路由器 ID
      Number of areas in this router is 1. 1 normal 0 stub 0 nssa
      Maximum path: 4
```

```
  Routing for Networks:
    172.16.1.32 0.0.0.7 area 0
    192.168.10.0 0.0.0.3 area 0
    192.168.10.8 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.2.2.2            110         00:00:20
    10.3.3.3            110         00:00:20
    172.30.1.1          110         00:00:21
  Distance: (default is 110)
```

如果未使用 OSPF router-id 命令，但配置了环回接口，则 OSPF 将选择其所有环回接口的最高 IP 地址。环回地址是一种虚拟接口，配置后即自动处于工作状态。使用环回接口的优点在于，不会像物理接口那样发生故障。环回接口无需依赖实际电缆和相邻设备即可处于工作状态。因此，使用环回地址作为路由器 ID 给 OSPF 过程带来了稳定性。用于配置环回接口的命令：

```
Router(config)# interface loopback number
Router(config-if)# ip address ip-address subnet-mask
```

OSPF router-id 命令在 IOS 12.0(T) 中引入，且在用于确定路由器 ID 时优先于环回接口和物理接口 IP 地址。命令语法为：

```
Router(config)# router ospf process-id
Router(config-router)# router-id ip-address
```

路由器 ID 在使用第一个 OSPF network 命令配置 OSPF 时选定。如果配置了 OSPF router-id 命名或环回地址(在 OSPF network 命令之后)，路由器 ID 将来自具有最高活动 IP 地址的接口。路由器 ID 可使用新的环回接口或物理接口 IP 地址修改路由器 ID，但必须通过重新加载路由器或使用下列命令来实现：

```
Router# clear ip ospf process
```

当同一个 OSPF 路由域内的两台路由器具有相同的路由器 ID 时，将无法正常路由。如果两台相邻路由器的路由器 ID 相同，则无法建立相邻关系。因为某些 IOS 版本不支持 router-id 命令，所以我们将使用环回地址的方法分配路由器 ID。通常只有在重新加载路由器后，来自环回接口的 IP 地址才能取代当前 OSPF 路由器 ID。

(4)OSPF 度量

OSPF 度量称为开销。RFC 2328 中有下列描述：“开销与每个路由器接口的输出端关联。系统管理员可配置此开销。开销越低，该接口越可能被用于转发数据流量。”Cisco IOS 使用从路由器到目的网络沿途的传出接口的累积带宽作为开销值。在路由度量中，开销最低的路由是首选路由，表 4-13 为各种接口的默认 OSPF 开销。参考带宽默认为 10^8 bps，即 100 Mbps，这使带宽等于或大于 100 Mbps 的接口具有相同的 OSPF 开销 1。可使用 OSPF 命令 auto-cost reference-bandwidth 修改参考带宽值以适应链路速度更高的网络。如果需要使用此命令，则建议同时用在所有路由器上，以使 OSPF 路由度量保持一致。OSPF 路由的开销为从路由器到目的网络所有链路开销的累计开销值。

表 4-13　　cisco OSPF 开销值

接口类型	10^8/bps＝开销
快速以太网及以上速度	10^8/100000000bps＝1
以太网	10^8/10000000bps＝10
E1	10^8/2048000bps＝48
T1	10^8/1544000bps＝64
128kbps	10^8/128000bps＝781
64kbps	10^8/64000bps＝1562
56kbps	10^8/56000bps＝1785

可使用 show interface 命令查看接口所用的带宽值。在 Cisco 路由器上，许多串行接口的带宽值默认为 T1（1.544 Mbps）。然而某些串行接口可能默认为 128 kbps。具体带宽值应使用 show interface 命令检查。此带宽值实际上并不影响链路速度，而是由某些路由协议用来计算路由度量。在串行接口上，链路的实际速度很可能不同于默认带宽，带宽值必须反映链路的实际速度，路由表才具有准确的最佳路径信息。

```
R2# show interface serial 0/0/1
    Serial0/0/1 is up, line protocol is up (connected)
      Hardware is HD64570
      Internet address is 192.168.10.9/30
      MTU 1500 bytes,BW 1544 Kbit, DLY 20000 usec,                    带宽和延迟
         reliability 255/255, txload 1/255, rxload 1/255
      Encapsulation HDLC, loopback not set, keepalive set (10 sec)
      * * * * * *(省略部分信息)
```

可使用 show ip ospf interface 命令验证路由器上接口 OSPF 开销。

```
Router# show ip ospf interface
    Serial0/0/1 is up, line protocol is up
      Internet address is 192.168.10.9/30, Area 0
      Process ID 1, Router ID 10.2.2.2, Network Type POINT-TO-POINT,Cost: 64
                                                  本路由器的 Serial0/0/1 口链路开销为 64
      Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
      No designated router on this network
      No backup designated router on this network
      Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:07
      Index 1/1, flood queue length 0
      Next 0x0(0)/0x0(0)
      Last flood scan length is 1, maximum is 1
      Last flood scan time is 0 msec, maximum is 0 msec
      Neighbor Count is 1 , Adjacent neighbor count is 1
        Adjacent with neighbor 10.3.3.3
```

```
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.10.2/30, Area 0
  Process ID 1, Router ID 10.2.2.2, Network Type POINT-TO-POINT,Cost: 1562
                                          本路由器的 Serial0/0/0 口链路开销为 1562
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 172.30.1.1
Suppress hello for 0 neighbor(s)
```

如果串行接口的实际工作速率不是默认 T1 速率,则需要手动修改该接口的速率。链路的两端应该配置为相同值。bandwidth 接口命令或 ip ospf cost 接口命令都可用于达到此目的,使 OSPF 在确定最佳路由时使用准确的值。bandwidth 命令用于修改 IOS 在计算 OSPF 开销度量时所用的带宽值。该命令的语法同 EIGRP:

```
Router(config-if)# bandwidth bandwidth-kbps
```

除 bandwidth 命令外,另一种方法是使用 ip ospf cost 命令,该命令可用于直接指定接口开销。例如:

```
R1(config)# interface serial 0/0/0
R1(config-if)# ip ospf cost 1562
```

ip ospf cost 命令适用于使用了多个厂商的设备的环境,在该环境中,非 Cisco 路由器所用的度量并非用于计算 OSPF 开销的带宽值。这两个命令之间的主要差异在于 bandwidth 命令使用开销计算的结果确定链路开销。ip ospf cost 命令则直接将链路开销设置为特定值并免除了计算过程。

(5)验证 OSPF

show ip ospf neighbor 命令可用于验证 OSPF 相邻关系并排除相应的故障。此命令为每个邻居显示下列输出:

```
R2# show ip ospf neighbor
  Neighbor ID     Pri   State           Dead Time         Address         Interface
  172.30.1.1        0   FULL/  -        00:00:33     192.168.10.1       Serial0/0/0
  10.3.3.3          0   FULL/  -        00:00:30     192.168.10.10      Serial0/0/1
```

各参数的意义如下:

- Neighbor ID:该相邻路由器的路由器 ID。
- Pri:该接口的 OSPF 优先级。
- State:该接口的 OSPF 状态。FULL 状态表明该路由器和其邻居具有相同的 OSPF 链

路状态数据库。

◆ Dead Time：路由器在宣告邻居进入 down(不可用)状态之前等待该设备发送 Hello 数据包所剩余的时间。此值在该接口收到 Hello 数据包时重置。

◆ Address：该邻居用于与本路由器直连的接口的 IP 地址。

◆ Interface：本路由器用于与该邻居建立相邻关系的接口。

当排除 OSPF 网络故障时，show ip ospf neighbor 命令可用于验证该路由器是否已与其相邻路由器建立相邻关系。如果未显示相邻路由器的路由器 ID，或未显示 FULL 状态，则表明两台路由器未建立 OSPF 相邻关系。如果两台路由器未建立相邻关系，则不会交换链路状态信息。链路状态数据库不完整可能会导致路由表不准确。在下列情况下，两台路由器不会建立 OSPF 相邻关系：

◆ 子网掩码不匹配，导致该两台路由器分处于不同的网络中。

◆ OSPF Hello 计时器或 Dead 计时器不匹配。

◆ OSPF 网络类型不匹配。

◆ 存在信息缺失或不正确的 OSPF network 命令。

OSPF 故障排除命令还包括 show ip protocols、show ip ospf、show ip ospf interface 等。路由器每次收到有关拓扑的新信息(链路添加、删除或修改)时，必须重新运行 SPF 算法，创建新的 SPF 树，并更新路由表。SPF 算法会占用很多 CPU 资源，且其耗费的计算时间取决于区域大小，区域大小通过路由器数量和链路状态数据库来衡量。

状态在 up 和 down 之间来回变化的网络称为链路不稳。链路不稳会导致区域内的 OSPF 路由器持续重新计算 SPF 算法，从而无法正确收敛。为尽量减轻此问题，路由器在收到一个 LSU 后，会等待 5 秒才运行 SPF 算法。这称为 SPF 计划延时。为防止路由器持续运行 SPF 算法，还存在一个 10 秒的保留时间。路由器运行完一次 SPF 算法后，会等待 10 秒才再次运行该算法。

```
Router# show ip ospf interface
  Serial0/0/1 is up, line protocol is up
    Internet address is 192.168.10.9/30, Area 0
    Process ID 1, Router ID 10.2.2.2, Network Type POINT-TO-POINT,Cost: 64
    Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
    No designated router on this network
    No backup designated router on this network
    Timer intervals configured,Hello 10, Dead 40, Wait 40, Retransmit 5
                                                          hello 和 dead 间隔
      Hello due in 00:00:07
    Index 1/1, flood queue length 0
    Next 0x0(0)/0x0(0)
    Last flood scan length is 1, maximum is 1
    Last flood scan time is 0 msec, maximum is 0 msec
    Neighbor Count is 1 , Adjacent neighbor count is 1
      Adjacent with neighbor 10.3.3.3
  Suppress hello for 0 neighbor(s)
```

OSPF 在不同接口上可能具有不同的 Hello 间隔和 Dead 间隔，但要使 OSPF 路由器建立相邻关系，它们的 OSPF Hello 间隔和断路间隔必须相同。

show ip route 命令可用于检验路由器是否正在通过 OSPF 发送和接收路由。每条路由开头的 O 表示路由来源为 OSPF。与 RIPv2 和 EIGRP 不同的是，OSPF 不会自动在主网络边界总结。

4. OSPF 和多路访问网络

(1)多路访问网络中的挑战

在多路访问网络中，相同的共享介质上连接有两台以上设备。以太网 LAN 就是一种广播多路访问网络，因为该网络中的所有设备会看到所有广播帧，所以它属于广播网络，该网络可能包括许多主机、打印机、路由器和其他设备，所以属于多路访问网络。相比之下，点对点网络中只有两台设备，它们分处网络两端，WAN 链路就属于点对点链路。

OSPF 定义了五种网络类型：点对点、广播多路访问、非广播多路访问（NBMA）、点对多点、虚拟链路。NBMA 和点对多点网络包括帧中继、ATM 和 X.25 网络。多路访问网络中会对 OSPF 的 LSA 进行泛洪，会有大量 LSA 在该网络内的路由器间传输。在多路访问网络中，此泛洪过程中的流量可能变得很大，如果多路访问网络中的每台路由器都需要向其他所有路由器泛洪 LSA 并为收到的所有 LSA 发出确认，网络通信将变得非常混乱。

用于在多路访问网络中管理相邻关系数量和 LSA 泛洪的解决方案是指定路由器（DR）。

在多路访问网络中，OSPF 会选举出一个指定路由器（DR）负责收集和分发 LSA。还会选举出一个备用指定路由器（BDR），以防指定路由器发生故障。其他所有路由器变为 DROther（这就表示该路由器既不是 DR 也不是 BDR）。DROther 仅与网络中的 DR 和 BDR 建立完全的相邻关系。这意味着 DROther 无需向网络中的所有路由器泛洪 LSA，只需使用组播地址 224.0.0.6 将其 LSA 发送给 DR 和 BDR 即可。DR 负责将来自路由器的 LSA 转发给其他所有路由器。DR 使用组播地址 224.0.0.5。最终结果是，多路访问网络中仅有一台路由器负责泛洪所有 LSA。

(2)DR/BDR 选举过程

DR/BDR 选举不会发生在点对点网络中。在多路访问网络中，DR 和 BDR 的选举过程遵循以下条件：

- DR：具有最高 OSPF 接口优先级的路由器。
- BDR：具有第二高 OSPF 接口优先级的路由器。
- 如果 OSPF 接口优先级相等，则取路由器 ID 最高者。

DROther 仅与 DR 和 BDR 建立完全的相邻关系，但也会与该网络中的任何其他 DROthers 建立相邻关系。这意味着多路访问网络中的所有 DROther 路由器仍然会收到其他所有 DROther 路由器发来的 Hello 数据包，通过这种方式，它们可获悉网络中所有路由器的情况。当两台 DROther 路由器形成相邻关系后，其相邻状态显示为 2WAY。相关信息可以通过 show ip ospf neighbor 和 show ip ospf interface 来查看：

```
Router# show ip ospf neighbor
  Neighbor ID     Pri   State           Dead Time       Address         Interface
  172.16.1.3      3     EXSTART/BDR     00:00:37        172.16.1.3      FastEthernet0/0
  172.16.1.2      5     EXSTART/DR      00:00:37        172.16.1.2      FastEthernet0/0
```

```
  172.16.1.4    1      2WAY/DROTHER    00:00:37        172.16.1.4          FastEthernet0/0
  202.112.10.2  0      FULL/  -        00:00:35        202.112.10.2        Serial0/0/0
Router# show ip ospf interface
  FastEthernet0/0 is up, line protocol is up
    Internet address is 172.16.1.1/24, Area 0
    Process ID 1, Router ID 202.112.10.1, Network Type BROADCAST, Cost: 1
    Transmit Delay is 1 sec, State DROTHER, Priority 1
    Designated Router (ID) 172.16.1.2, Interface address 172.16.1.2
    Backup Designated Router (ID) 172.16.1.3, Interface address 172.16.1.3
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:05
    Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
    Last flood scan length is 1, maximum is 1
    Last flood scan time is 0 msec, maximum is 0 msec
    Neighbor Count is3, Adjacent neighbor count is 2
  Adjacent with neighbor 172.16.1.2  (Designated Router)            DR 是 172.16.1.2
  Adjacent with neighbor 172.16.1.3  (Backup Designated Router)    BDR 是 172.16.1.3
  * * * * * *(省略部分信息)
```

通过以上输出可以看出网络中的 DR 和 BDR 信息，及邻居间的状态信息。

当多路访问网络中第一台启用了 OSPF 接口的路由器开始工作时，DR 和 BDR 选举过程随即开始。这可能发生在路由器开机时或配置 OSPF network 命令时，选举过程仅需几秒钟。如果多路访问网络中仍有部分路由器未完成启动过程，则成为 DR 的路由器可能具有较低的路由器 ID，原因可能在于具有较低路由器 ID 的路由器所需的启动时间较短。DR 一旦选出，将保持 DR 地位，直到出现下列条件之一为止：

- DR 发生故障。
- DR 上的 OSPF 进程发生故障。
- DR 上的多路访问接口发生故障。

如果在选出 DR 和 BDR 后有新路由器加入网络，即使新路由器的 OSPF 接口优先级或路由器 ID 比当前 DR 或 BDR 高，也不会成为 DR 或 BDR。如果当前 DR 或 BDR 发生故障，则新路由器可被选举为 BDR。如果当前 DR 发生故障，则 BDR 将成为 DR，新路由器可被选为新的 BDR。当新路由器成为 BDR 后，如果 DR 发生故障，则该新路由器将成为 DR。当前 DR 和 BDR 必须都发生故障，该新路由器才能被选举为 DR 或 BDR。那么如何确保性能稳定的路由器在 DR 和 BDR 选举中获胜呢？解决方案有两种：

- 先启动 DR，再启动 BDR，然后启动其他所有路由器。
- 关闭所有路由器上的接口，然后在 DR 上执行 no shutdown 命令，再在 BDR 上执行该命令，随后在其他所有路由器上执行该命令。

(3)OSPF 接口优先级

由于 DR 成为 LSA 的集散中心,所以它必须具有足够的 CPU 和存储性能才能担此重责。与其依赖路由器 ID 来确定 DR 和 BDR 结果,不如使用 ip ospf priority 接口命令来控制选举。

```
Router(config-if)# ip ospf priority {0 - 255}
```

所有路由器接口的优先级值默认为 1,因此通常由路由器 ID 来确定 DR 和 BDR。但如果将该值从默认值 1 改为更高的值,则具有最高优先级的路由器将成为 DR,具有第二高优先级的路由器将成为 BDR。若该值为 0,则该路由器不具备成为 DR 或 BDR 的资格。因为优先级是特定于具体接口的值,因此可用于更好地控制 OSPF 多路访问网络。它们还可以使一台路由器在一个网络中充当 DR,同时在另一个网络中充当 DROther。简单来说,接口优先级在多路访问的网络中用于强制选举 DR 和 BDR。

4.3.6 知识点 6:不同路由协议的混合使用

如果网络中配置了多种路由协议,需要进行路由重分布。路由重分布是指获取来自某个路由源的路由,然后将这些路由发送到另一个路由源,达到多路由环境下的网络互通。

1. 默认路由重分布

前面我们已经学习了使用 default-information originate 在 RIPv1 中传播默认路由。与 RIP 相似,OSPF 也可以使用 default-information originate 命令来将 0.0.0.0/0 静态默认路由通告给区域内的其他路由器。如果未使用 default-information originate 命令,则不会将默认的"全零"路由传播给 OSPF 区域内的其他路由器。

```
Router(config)#router ospf
Router(config-router)#default-information originate
```

2. 使用 redistribute 命令进行路由注入

路由重分布可以将一种路由协议中的路由条目转换为另一种路由协议的路由条目,达到多路由环境下的网络互通。在路由器上配置多路由协议间的重分布,比如将路由协议 A 重分布到路由协议 B 中,要先进入路由协议 B 的路由模式下,然后再执行 redistribute 命令进行重分布。可以在路由器配置模式下配置 redistribute 命令,例:

◆ 将静态路由注入 OSPF

```
Router(config)#router ospf 1
Router(config-router)# redistribute static
```

◆ 将 OSPF、RIP 注入 EIGRP

```
Router(config)#router eigrp 1
Router(config-router)#redistribute ospf 1                路由重分布只针对 ospf 1 进程
Router(config-router)#redistribute rip subnets
                                  subnets 表示学习 RIP 全部子网,而非只学习有类网络
Router(config-router)# default-metric 30                 指定重分布后的 metric,每个路由器的 metric 值必需一致。
```

4.4　项目实施

下面是教学项目中部分设备有关本章内容的配置情况：

(1)交换机 S7 上通过三层交换机实现 vlan 间路由相关配置：

```
S7# show running-config
Building configuration...

* * * * * *(省略部分信息)
!
hostname S7
!
ip routing
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
no switchport
ip address 10.1.7.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/3
switchport trunk encapsulation dot1q
switchport mode trunk
!
* * * * * *(省略部分信息)
!
interface Vlan13
ip address 192.168.13.254 255.255.255.0
!
interface Vlan14
ip address 192.168.14.254 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet0/2
```

(2)路由器 R1 配置如下，包括单臂路由、OSPF 路由、RIP 路由、路由引入：

```
R1# show running-config
Building configuration...
```

```
Currentconfiguration : 1625 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
!
!
enable password cisco
!
!
no ip domain-lookup
!
!
interface FastEthernet0/0
ip address 10.1.2.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 10.0.4.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet2/0
ip address 10.0.5.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet3/0
no ip address
duplex auto
speed auto
!
interface FastEthernet3/0.10
encapsulation dot1Q 10 native
ip address 192.168.10.254 255.255.255.0
!
interface FastEthernet3/0.11
```

```
encapsulation dot1Q 11
ip address 192.168.11.254 255.255.255.0
!
interface FastEthernet4/0
ip address 10.0.6.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet5/0
no ip address
duplex auto
speed auto
!
interface Serial6/0
ip address 10.0.0.1 255.255.255.252
clock rate 64000
!
router ospf 1
redistribute rip subnets
redistribute static subnets
network 10.0.0.0 0.0.0.3 area 0
network 10.0.4.0 0.0.0.3 area 0
network 10.0.5.0 0.0.0.3 area 0
network 10.0.6.0 0.0.0.3 area 0
network 192.168.10.0 0.0.0.255 area 0
network 192.168.11.0 0.0.0.255 area 0
!
router rip
version 2
redistribute ospf 1
network 10.0.0.0
no auto-summary
!
ip classless
ip route 192.168.12.0 255.255.255.0 FastEthernet4/0
!
!
!
no cdp run
!
!
line con 0
password cisco
login
```

```
!
line aux 0
!
line vty 0 4
password cisco
login
!
!
!
end
```

4.5 技术拓展

1. EIGRP 高级配置

(1)Null0 总结路由

由于 EIGRP 会自动添加 Null0 总结路由,人们在分析包含 EIGRP 路由的路由表时通常会感到困惑。Null0 接口实际上是不通向任何地方的路由,通常称为“比特桶”。所以,默认情况下,EIGRP 使用 Null0 接口来丢弃与父路由匹配但与所有子路由都不匹配的数据包。如果我们使用 ip classless 命令配置无类路由行为,EIGRP 将不会丢弃该数据包,而会继续寻找默认路由或超网路由。然而,EIGRP Null0 总结路由是一条子路由,即使父路由的其他子路由与数据包都不匹配,Null0 总结路由也会与之匹配。即使通过 ip classless 命令使用无类路由行为(使用无类路由行为时,路由查找过程将查找超网路由和默认路由),如果父路由没有匹配的子路由,EIGRP 也将使用 Null0 总结路由并丢弃数据包,因为 Null0 总结路由与父路由传递来的任何数据包都匹配。不管是使用有类还是无类路由行为,都将使用 null0 总结,因此不会使用任何超网路由或默认路由。

只要同时存在下列两种情况,EIGRP 就会自动加入一条 null0 总结路由作为子路由:

- 通过 EIGRP 至少发现了一个子网。
- 启用了自动总结。

EIGRP 在网络边界会自动总结,如果禁用自动总结会删除 Null0 总结路由并允许 EIGRP 在子路由与目的数据包不匹配时寻找超网路由或默认路由。

(2)禁用自动总结

EIGRP 使用默认的 auto-summary 命令在主网络边界自动总结,可使用 no auto-summary 命令禁用自动总结,这时 DUAL 取消所有邻接关系,然后重新建立邻接关系,以充分实现 no auto-summary 命令的效果。所有 EIGRP 邻居将立即发出新一轮更新,这些更新不会被自动总结。禁用自动总结后 EIGRP 不再添加 Null0 总结路由。只要默认的无类路由行为(ip classless)保持有效,则与子网路由不匹配时,将使用超网路由和默认路由。

```
Router(config)# router eigrp 1
Router(config-router)#no auto-summary
```

2. 修改 OSPF 间隔

可能需要更改 OSPF 计时器以使路由器更快地检测到网络故障。这样做会增加流量，但有时要求快速收敛。可使用下列接口命令手动修改 OSPF Hello 间隔和 Dead 间隔：

```
Router(config-if)# ip ospf hello-interval seconds
Router(config-if)# ip ospf dead-interval seconds
```

更改 Hello 间隔之后 Cisco IOS 立即自动将 Dead 间隔修改为 Hello 间隔的四倍。然而，最好是明确修改该计时器，而不要依赖 IOS 的自动功能，因为手动修改可使修改情况记录在配置中。OSPF 要求两台路由器的 Hello 间隔和 Dead 间隔必须相同才能形成相邻关系。这与 EIGRP 不同，两台路由器的 Hello 计时器和抑制计时器无需匹配，即可形成 EIGRP 相邻关系。

4.6　本章小结

通过本章内容我们学习了路由器利用路由表查找数据包转发路径的原理；VLAN 间通信的两种方法：传统独立物理接口的 VLAN 间路由配置、单臂路由器配置 VLAN 间路由；直连路由的添加和删除；静态路由的两种配置方式：带送出接口的静态路由、带下一跳 IP 地址的静态路由；RIP 协议的工作原理与配置：RIPv1 和 RIPv2；OSPF 协议的工作原理与配置、DR/BDR 的选举；EIGRP 协议的工作原理与配置、DUAL 算法。通过本章的学习，能够进行局域网间的互联配置。

4.7　强化练习

1. 对于为防止路由环路而通过毒性反转实现的水平分割方法，哪两项叙述正确？（多选）（　　）

A. 所有 Cisco IOS 都会默认启用此方法

B. 会将一个表示无穷大度量的值分配给路由以将其毒化

C. 将毒化路由更新发回该更新的发送接口

D. 指示路由器将可能会影响路由的更改保持一段特定的时间

E. 限制数据包在被丢弃之前能够在网络中传输的跳数

2. 在两台路由器能够使用 OSPF 形成邻居邻接关系之前必须完成哪两项任务？（多选）（　　）

A. 路由器必须选举出指定路由器

B. 路由器必须在网络类型方面达成一致

C. 路由器必须使用相同的 dead 时间间隔

D. 路由器必须交换链路状态请求

E. 路由器必须交换数据库描述数据包

3. 下列关于链路状态路由协议的陈述，哪两项是正确的？（多选）（　　）

A. 链路状态路由协议了解整个网络的拓扑结构

B. 链路状态路由协议可以使大型网络快速达到收敛

C. 链路状态路由协议的路由更新中不包含子网掩码

D. 链路状态路由协议根据跳数从高到低的顺序来确定最佳路径

E. 链路状态路由协议不适合具有特定层次结构的网络

F. 链路状态路由协议仅向直连的邻居发送整个路由表

4. 路由器通过静态路由和动态路由过程获知网络。它会使用哪条路由来到达网络192.168.168.0？（　　）

A. D 192.168.168.0/24 [90/2195456] via 192.168.200.1，00:00:09，Ethernet0

B. O 192.168.168.0/24 [110/1012] via 192.168.200.1，00:00:22，Ethernet0

C. R 192.168.168.0/24 [120/1] via 192.168.200.1，00:00:17，Ethernet0

D. S 192.168.168.0/24 [1/0] via 192.168.200.1

5. 当存在到达某一目的地的多条有效路由时，路由器采用什么标准来确定将哪些路由加入路由表？（　　）

A. 路由器选择具有最佳度量的路由。具有相同最佳度量的所有路由都会加入路由表

B. 路由器首先选择具有最小管理距离的路由。由此得到的路由再按度量确定优先顺序，具有最佳度量的路由会加入路由表

C. 路由器选择具有最小管理距离的路由。具有相同最小管理距离的所有路由会同时加入路由表

D. 路由器会将所有路由加入路由表，但执行负载均衡时一般使用具有最佳度量的路由

6. 在大型网络中，RIP 使用什么来缩短收敛时间？（　　）

A. 它使用组播而不是广播来发送路由更新

B. 如果路由超过 10 条，它将把更新计时器减少到 15 秒

C. 如果在定期更新间隔期间发生网络变化，它将使用触发更新来通告这些变化

D. 它使用随机 ping 检测路径是否有效，因此能够主动发现断开的网络

7. IP 数据包报头中的 TTL 字段有什么作用？（　　）

A. 在无效计时器超时后从路由表中清除不可达路由

B. 防止定期更新消息错误地恢复可能已经出错的路由

C. 在清除计时器超时后从路由表中删除不可达路由

D. 限制数据包在被丢弃之前能够在网络中传输的时间长度或跳数

E. 用于在发往其他路由器的路由更新中将路由标记为不可达

8. 下列关于 EIGRP 路由操作的描述，哪三项是正确的？（多选）（　　）

A. 一旦发现新邻居，便会向邻居表中加入条目

B. 如果可行后继路由相对于当前后继路由具有更高的通告开销，该可行后继路由即成为主路由

C. 如果在保持时间内未收到 hello 数据包，则 DUAL 必须重新计算拓扑

D. 报告距离是邻居通告的与目的地之间的距离

E. EIGRP 在拓扑表中包含全面的网络拓扑信息，并在每次更新中与邻居路由器交换全部的路由信息

F. EIGRP 会构建一个路由表，其中包含所有所配置路由协议的路由

9. 网络管理员在 Router_A 上配置了一条默认路由，但该路由没有共享给邻接路由器 Router_B 以及该 OSPF 区域中的其他路由器。使用哪条命令可以简单快速地将该默认路由配置到 Router_B 及该 OSPF 区域内的所有其他路由器上？（　　）

A. Router_A(config-router)# ospf redistribute default-route

B. Router_B(config-router)# ospf redistribute default-route

C. Router_A(config-router)# default-information originate

D. Router_B(config-router)# default-information originate

E. Router_A(config-router)# ip ospf update-default

F. Router_B(config-router)# ip ospf update-default

10. 向 OSPF 路由过程配置中添加网络时，需要下列哪几项？（多选）(　　)

A. 网络地址

B. 环回地址

C. 自治系统编号

D. 子网掩码

E. 通配符掩码

F. 区域 ID