目 录

第1章 IP 路由协议概述

1.1 IP 路由和路由表介绍

1.1.1 路由和路由段

在因特网中进行路由选择要使用路由器，路由器根据所收到的报文的目的地址选择一条合适的路由（通过某一网络），将报文传送到下一个路由器，路由中最后的路由器负责将报文送交目的主机。

例如，在图 1-1中，主机 A 到主机 C 共经过了 3 个网络和 2 个路由器，跳数为 3。由此可见，若一节点通过一个网络与另一节点相连接，则此二节点相隔一个路由段，因而在因特网中是相邻的。同理，相邻的路由器是指这两个路由器都连接在同一个网络上。一个路由器到本网络中的某个主机的路由段数算作零。在图中用粗的箭头表示这些路由段。至于每一个路由段又由哪几条物理链路构成，路由器并不关心。

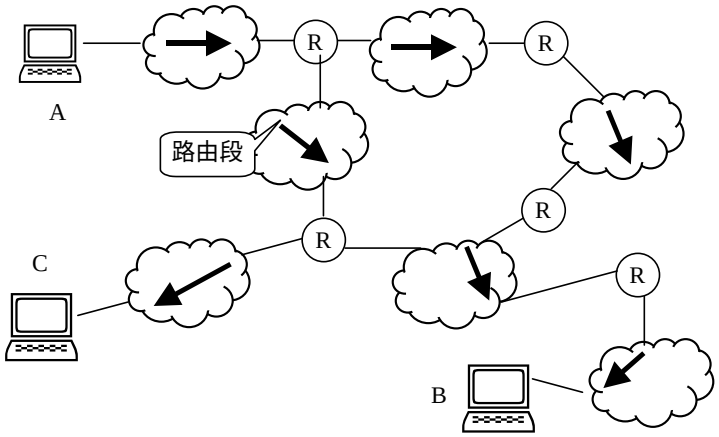


图1-1 路由段的概念

由于网络大小可能相差很大，而每个路由段的实际长度并不相同，因此对不同的网络，可以将其路由段乘以一个加权系数，用加权后的路由段数来衡量通路的长短。

如果把网络中的路由器看成是网络中的节点，把因特网中的一个路由段看成是网络中的一条链路，那么因特网中的路由选择就与简单网络中的路由选择相似了。采用路由段数最小的路由有时也并不一定是最理想的。例如，经过三个高速局域网段的路由可能比经过两个低速广域网段的路由快得多。

1.1.2 通过路由表进行选路

路由器转发分组的关键是路由表。每个路由器中都保存着一张路由表，表中每条路由项都指明分组到某子网或某主机应通过路由器的哪个物理端口发送，然后就可到

达该路径的下一个路由器，或者不再经过别的路由器而传送到直接相连的网络中的目的主机。

路由表中包含了下列关键项：

- 目的地址：用来标识 IP 包的目的地址或目的网络。
- 网络掩码：与目的地址一起来标识目的主机或路由器所在的网段的地址。将目的地址和网络掩码“逻辑与”后可得到目的主机或路由器所在网段的地址。例如：目的地址为 129.102.8.10，掩码为 255.255.0.0 的主机或路由器所在网段的地址为 129.102.0.0。掩码由若干个连续“1”构成，既可以以点分十进制表示，也可以用掩码中连续“1”的个数来表示。
- 输出接口：说明 IP 包将从该路由器哪个接口转发。
- 下一跳 IP 地址：说明 IP 包所经由的下一个路由器。
- 本条路由加入 IP 路由表的优先级：针对同一目的地，可能存在不同下一跳的若干条路由，这些不同的路由可能是由不同的路由协议发现的，也可以是手工配置的静态路由。优先级高（数值小）将成为当前的最优路由。

根据路由的目的地不同，可以划分为：

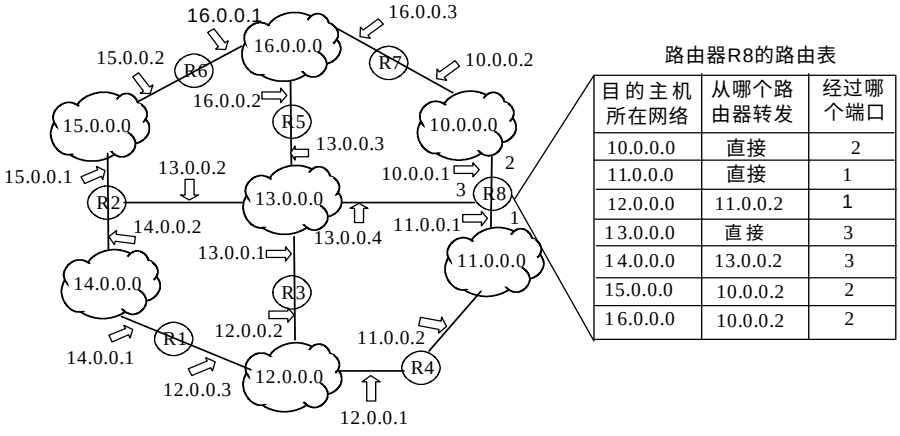
- 子网路由：目的地为子网
- 主机路由：目的地为主机

另外，根据目的地与该路由器是否直接相连，又可分为：

- 直接路由：目的地所在网络与路由器直接相连
- 间接路由：目的地所在网络与路由器不是直接相连

为了不使路由表过于庞大，可以设置一条缺省路由。凡遇到查找路由表失败后的数据包，就选择缺省路由转发。

在图 1-2比较复杂的因特网中，各网络中的数字是该网络的网络地址。路由器 8 与三个网络相连，因此有三个 IP 地址和三个物理端口，其路由表如图所示。



路由器R8的路由表

目的主机所在网络	从哪个路由器转发	经过哪个端口
10.0.0.0	直接	2
11.0.0.0	直接	1
12.0.0.0	11.0.0.2	1
13.0.0.0	直接	3
14.0.0.0	13.0.0.2	3
15.0.0.0	10.0.0.2	2
16.0.0.0	10.0.0.2	2

图1-2 路由表示意图

路由器支持对静态路由的配置，同时支持 RIP、OSPF、IS-IS 和 BGP 等一系列动态路由协议，另外路由器在运行过程中根据接口状态和用户配置，会自动获得一些直接路由。

1.2 路由管理策略

可以使用手工配置到某一特定目的地的静态路由，也可以配置动态路由协议与网络中其它路由器交互，并通过路由算法来发现路由。用户配置的静态路由和由路由协议发现的动态路由在路由器中是统一管理的。静态路由与各路由协议之间发现或者配置的路由也可以在路由协议间共享。

1.2.1 路由协议及其发现路由的优先级

到相同的目的地，不同的路由协议（包括静态路由）可能会发现不同的路由，但并非这些路由都是最优的。事实上，在某一时刻，到某一目的地的当前路由仅能由唯一的路由协议来决定。这样，各路由协议（包括静态路由）都被赋予了一个优先级，这样当存在多个路由信息源时，具有较高优先级的路由协议发现的路由将成为当前路由。各种路由协议及其发现路由的缺省优先级（数值越小表明优先级越高）如表 1-1所示。

其中：0 表示直接连接的路由，255 表示任何来自不可信源端的路由。

表1-1 路由协议及其发现路由的优先级

路由协议或路由种类	相应路由的优先级
DIRECT	0
OSPF	10
IS-IS	15
STATIC	60
RIP	100
OSPF ASE	150
OSPF NSSA	150
IBGP	256
EBGP	256
UNKNOWN	255

除了直连路由（DIRECT）、IBGP 及 EBGP 外，各动态路由协议的优先级都可根据用户需求，手工进行配置。另外，每条静态路由的优先级都可以不相同。

1.2.2 对负载分担与路由备份的支持

1. 负载分担

支持多路由模式，即允许配置多条到同一目的地而且优先级相同的路由。到同一目的地而且优先级相同的路由指的是目的网络和掩码相同，优先级相同，但下一跳地址或者接口不相同。当没有比到此目的地优先级更高的路由时，这几条路由都被系统采纳，在转发报文时，依次通过各条路径发送，从而实现网络的负载分担。路由负载分担只能在同一个路由协议的等价路由（即路由的 cost 代价相等）之间进行，例如不能在所配置的静态路由和 OSPF 路由之间进行。

目前，支持负载分担的路由协议有四种：静态路由、OSPF、BGP 和 IS-IS。

负载分担的实现方式有三种：

- 基于流的负载分担。缺省情况下我们的路由器使能了快速转发功能，此时路由器只能基于流进行负载分担。例如，当前路由器上存在两条等价路由，如果此时只有一个数据流，那么将从一条路由上转发；如果有两个数据流，那么两条路由各转发一个。子接口也支持快转，实现基于流的负载分担。
- 基于报文的负载分担。当关闭了快转功能时，路由器将基于报文进行负载分担，即将待发送报文均匀分配到两条路由上。
- 基于带宽的非平衡负载分担。缺省情况下，路由按接口物理带宽进行负载分担；当用户为接口配置了指定的负载带宽后，路由器将按用户指定的接口带宽进行负载分担，即根据接口间的带宽比例关系，给大带宽接口多发送数据，给小带宽接口少发送数据。

2. 路由备份

支持路由备份，当主路由发生故障时，自动切换到备份路由，提高用户网络的可靠性。为了实现路由的备份，用户可根据实际情况，配置到同一目的地的多条路由，其中一条路由的优先级最高，称为主路由，其余的路由优先级依次递减，称为备份路由。这样，正常情况下，路由器采用主路由发送数据。当线路发生故障时，该路由自动隐藏，路由器会选择余下的优先级最高的备份路由作为数据发送的途径。这样，也就实现了主路由到备份路由的切换。当主路由恢复正常时，路由器恢复相应的路由，并重新选择路由。由于该路由的优先级最高，路由器选择主路由来发送数据。上述过程是备份路由到主路由的自动切换。

1.2.3 路由协议之间的共享

由于各路由协议的算法不同，不同的协议可能会发现不同的路由，因此各路由协议之间存在如何共享各自发现结果的问题。路由器支持将一种路由协议发现的路由引入（import-route）到另一种路由协议中，每种协议都有相应的路由引入机制，具体内容请参见各路由协议的配置指导中引入外部路由部分的描述。

1.3 配置基于带宽的非平衡负载分担

一般情况下负载分担是采用负荷均担的方式，即把数据包均匀的发送给不同的接口；例如有两个相互负载分担的接口，3Mbps 的数据流就会被平均发送给每个接口（即各 1.5Mbps），这样就会导致大带宽接口的利用率不高，而小带宽的接口不断丢弃数据包的情况。为了有效利用大带宽接口的传输能力，需要 IP 层向相互负载分担的接口发送数据时能根据接口间的带宽比例关系，给大带宽接口多发送数据，给小带宽接口少发送数据，即实现基于等价路由各接口带宽的非平衡负载分担。当系统支持该特性后，缺省情况下按接口物理带宽进行负载分担；当用户配置了指定带宽时，按用户的指定带宽进行负载分担。

1.3.1 配置基于带宽的非平衡负载分担

请在接口视图下进行下面配置。

表1-2 配置基于接口带宽的非平衡负载分担

操作	命令
配置接口的负载带宽	**loadbandwidth** *bandwidth*
恢复接口的负载带宽缺省值	**undo loadbandwidth**

当指定参数为 0 时关闭当前接口的路由功能，该接口将不会被选择，但不对物理接口的其它状态产生任何影响。负载带宽缺省值为该接口的物理带宽。

1.3.2 基于带宽的负载分担的显示与调试

请在所有视图下进行下面配置。

表1-3 基于带宽的非平衡负载分担的显示与调试

操作	命令
显示基于接口带宽的非平衡负载分担的统计结果	**display loadsharing ip address** *ip-address mask*

1.3.3 基于带宽的非平衡负载均衡配置举例

1. 组网需求

假设 Route A 上已经存在到目的网络地址 10.2.1.0 /24 的三条等价路由，分别是：

```
[Router A] display fib
Destination/Mask   Nexthop         Flag TimeStamp     Interface
10.2.1.0/24        10.1.1.2         GSU  t[0]           Ethernet0/0/0
```

```
10.2.1.0/24        10.1.2.2         GSU  t[0]           Atm1/0/0
10.2.1.0/24        10.1.3.2         GSU  t[0]           Serial2/0/0
```

使用 **display loadsharing ip address** 命令观察目前的带宽比例关系：

```
[Router A]display loadsharing ip address 10.2.1.0 24
There are/is totally 3 route entry(s) to the same destination network.
Nexthop       Packet(s)   Bandwidth[KB]    Flow(s)    Interface
10.1.1.2      763851      100000       0           Ethernet0/0/0
10.1.2.2      1193501     155000       0           Atm1/0/0
10.1.3.2      15914       2048         0           Serial2/0/0
BandWidth:48:75:1
  Packets:47:74:1
    Flows:0:0:0
```

此时三个接口按缺省带宽进行负载分担。

在路由器 A 上配置基于带宽的负载分担后再观察负载分担的情况。

2. 组网图

图1-3 基于带宽的非平衡负载均衡配置举例组网图

3. 配置步骤

(1) 配置 Router A

配置三个接口的负载分担带宽。

```
[Router A] interface ethernet 0/0/0
[Router A-Ethernet0/0/0] loadbandwidth 200
[Router A-Ethernet0/0/0] quit
[Router A] interface Atm 1/0/0
[Router A-Atm 1/0/0] loadbandwidth 100
[Router A-Atm 1/0/0] quit
[Router A] interface serial 2/0/0
[Router A-serial 2/0/0] loadbandwidth 300
[Router A-serial 2/0/0] quit
```

显示三个接口的负载分担比例。

```
[Router A]display loadsharing ip ad 10.2.1.0 24
There are/is totally 3 route entry(s) to the same destination network.
Nexthop       Packet(s)    Bandwidth[KB] Flow(s)     Interface
```

```
10.1.2.2        142824      100             0             Atm1/0/0
10.1.1.2        285648      200             0             Ethernet0/0/0
10.1.3.2        428472      300             0             Serial2/0/0

BandWidth:1:2:3
  Packets:1:2:3
    Flows:0:0:0
```

显示结果表明此时报文按用户指定带宽进行负载分担。

第2章 静态路由配置

📖 说明：

本章中有关 VPN 实例的具体参数解释，请参见本手册的“ MPLS ”模块。

2.1 静态路由简介

2.1.1 静态路由

静态路由是一种特殊的路由，它由管理员手工配置而成。通过静态路由的配置可建立一个互通的网络，但这种配置缺点在于：当一个网络故障发生后，静态路由不会自动发生改变，必须有管理员的介入。

在组网结构比较简单的网络中，只需配置静态路由就可以使路由器正常工作，仔细设置和使用静态路由可以改进网络的性能，并可为重要的应用保证带宽。

静态路由还有如下的属性：

- 可达路由，正常的路由都属于这种情况，即 IP 报文按照目的地标示的路由被送往下一跳，这是静态路由的一般用法。
- 目的地不可达的路由，当到某一目的地的静态路由具有“ **reject** ”属性时，任何去往该目的地的 IP 报文都将被丢弃，并且通知源主机目的地不可达。
- 目的地为黑洞的路由，当到某一目的地的静态路由具有“ **blackhole** ”属性时，任何去往该目的地的 IP 报文都将被丢弃，并且不通知源主机。

其中“ **reject** ”和“ **blackhole** ”属性一般用来控制本路由器可达目的地的范围，辅助网络故障的诊断。

2.1.2 缺省路由

缺省路由是一种特殊的路由，可以通过静态路由配置，某些动态路由协议也可以生成缺省路由，如 OSPF 和 IS-IS。

简单地说，缺省路由就是在没有找到匹配的路由时才使用的路由。即只有当没有合适的路由时，缺省路由才被使用。在路由表中，缺省路由以到网络 0.0.0.0（掩码为 0.0.0.0）的路由形式出现。可通过命令 **display ip routing-table** 的输出看它是否被设置。如果报文的目的地址不能与任何路由相匹配，那么系统将使用缺省路由转发该报文。如果没有缺省路由且报文的目的地不在路由表中，那么该报文被丢弃，同时，向源端返回一个 ICMP 报文报告该目的地址或网络不可达。

2.2 静态路由配置

静态路由的配置包括：

- 配置静态路由
- 配置缺省路由
- 配置静态路由优先级
- 删除静态路由

2.2.1 配置静态路由

请在系统视图下进行下列配置。

表2-1 配置静态路由

操作	命令
增加一条静态路由	**ip route-static** *ip-address* { *mask* | *mask-length* } [*interface-type interface-number*] [*nexthop-address*] [**preference** *value*] [**reject** | **blackhole**] **ip route-static vpn-instance** { *vpn-instance-name1 vpn-instance-name2 … ip-address* } { *mask* | *mask-length* } [*interface-type interface-number* [*nexthop-address*] **| vpn-instance** *vpn-nexthop-name nexthop-address* | *nexthop-address* [**public**]] [**preference** *preference-value*] [**reject** | **blackhole**] [**tag** *tag-value*] [**description** *string*]
删除一条静态路由	**undo ip route-static** *ip-address* {*mask* | *mask-length* } [*interfacce-name*] [*nexthop-address*] [**preference** *value*] **undo ip route-static vpn-instance** { *vpn-instance-name1 vpn-instance-name2 … ip-address* } { *mask* | *mask-length* } [*interface-type interface-number* | **vpn-instance** *vpn-nexthop-name nexthop-address* | *nexthop-address* [**public**]] [**preference** *preference-value*]

其中各参数的解释如下：

(1) VPN 实例的名字

(2) IP 地址和掩码

IP 地址为点分十进制格式，由于要求掩码 32 位中‘1’必须是连续的，因此掩码可以用点分十进制表示，也可用掩码长度（即掩码中‘1’的位数）表示。

(3) 发送接口或下一跳地址

在配置静态路由时，可指定发送接口 *interface-type interface-number*，也可指定下一跳地址 *nexthop-address*，是指定发送接口还是指定下一跳地址要视具体情况而定。

实际上，所有的路由项都必须明确下一跳地址。在发送报文时，首先根据报文的目的地址寻找路由表中与之匹配的路由。只有路由指定了下一跳地址，链路层才能通过下一跳 IP 地址找到对应的链路层地址，然后按照该地址将报文转发。

在以下几种情况下可以指定发送接口：

- 对于点到点接口，指定发送接口即隐含指定了下一跳地址，这时认为与该接口相连的对端接口地址就是路由的下一跳地址。如 Serial 封装 PPP 协议，通过 PPP 协商获取对端的 IP 地址，这时可以不用指定下一跳地址，只需指定发送接口即可。
- 对于 NBMA 接口（如 ATM 接口），支持点到多点，这时除了配置 IP 路由外，还需在链路层建立二次路由，即 IP 地址到链路层地址的映射。这种情况下应配置下一跳 IP 地址。
- 在配置静态路由时，建议不要指定为以太网接口或 Virtual-template 接口作发送接口。因为以太网接口是广播类型的接口，而 Virtual-template 接口下可以关联多个虚拟访问接口（Virtual Access Interface），这都会导致出现多个下一跳，无法唯一确定下一跳。在某些特殊应用中，如果必须指定广播接口（如以太网接口）、VT 接口或 NBMA 接口做为发送接口，应同时指定通过该接口发送时对应的下一跳地址。

(4) 优先级

对优先级 **preference** 的不同配置，可以灵活应用路由管理策略。

(5) 其它参数

属性 **reject** 和 **blackhole** 分别指明不可达路由和黑洞路由。**public** 指公网。**tag 指**静态路由 **tag** 值，用于路由策略。**description** 为静态路由描述信息，提供给用户使用。

2.2.2 配置缺省路由

请在系统视图下进行下列配置。

表2-2 配置缺省路由

操作	命令
配置缺省路由	**ip route-static** 0.0.0.0 { 0.0.0.0 | 0 } {*interface-type interface-number* | *nexthop-address* } [**preference** *value*] [**tag** *tag-value*] [**description** *string*] **ip route-static vpn-instance** *vpn-instance-name* 0.0.0.0 { 0.0.0.0 | 0 } {*interface-type interface-number* | *nexthop-address* } [**preference** *value*] [**tag** *tag-value*] [**description** *string*]
删除缺省路由	**undo ip route-static** 0.0.0.0 { 0.0.0.0 | 0 } {*interface-type interface-number* | *nexthop-address*} [**preference** *value*] **undo ip route-static vpn-instance** *vpn-instance-name* 0.0.0.0 { 0.0.0.0 | 0 } {*interface-type interface-number* | *nexthop-address* } [**preference** *value*]

命令中各参数意义与静态路由相同。

2.2.3 删除全部静态路由

请在系统视图下进行下列配置。

表2-3 删除全部静态路由

操作	命令
删除全部静态路由	**delete static-routes all**

使用此命令可以删除配置的全部静态路由，包括缺省路由。

2.3 路由表的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后静态路由信息，用户可以通过查看显示信息验证配置的效果。

表2-4 路由表的显示和调试

操作	命令
查看路由表摘要信息	**display ip routing-table**
查看路由表详细信息	**display ip routing-table verbose**
查看指定目的地址的路由	**display ip routing-table** *ip-address* [*mask*] [**longer-match**] [**verbose**]
查看指定目的地址范围内的路由	**display ip routing-table** *ip-address1 mask1 ip-address2 mask2* [**verbose**]
查看通过指定标准访问控制列表过滤的路由	**display ip routing-table acl** *acl-number* [**verbose**]
查看通过指定前缀列表过滤的路由	**display ip routing-table ip-prefix** *ip-prefix-number* [**verbose**]
查看指定协议发现的路由	**display ip routing-table protocol** *protocol* [**inactive** | **verbose**| **vpn-instance** *vpn-instance-name*]
查看树形式路由表	**display ip routing-table radix**
查看路由表的统计信息	**display ip routing-table [vpn-instance** *vpn-instance-name* **] statistics**
查看私网路由表摘要信息	**display ip routing-table vpn-instance** *vpn-instance-name* [*ip-address*]
查看私网路由表详细信息	**display ip routing-table vpn-instance** *vpn-instance-name* [*ip-address*] **verbose**
清除路由表信息。	**reset ip routing-table** [**vpn-instance** *vpn-instance-name*] **statistics protocol** *protocol-type*

2.4 静态路由典型配置举例

1. 组网需求

如下图所示，要求配置静态路由，使任意两台主机或路由器之间都能互通。

2. 组网图

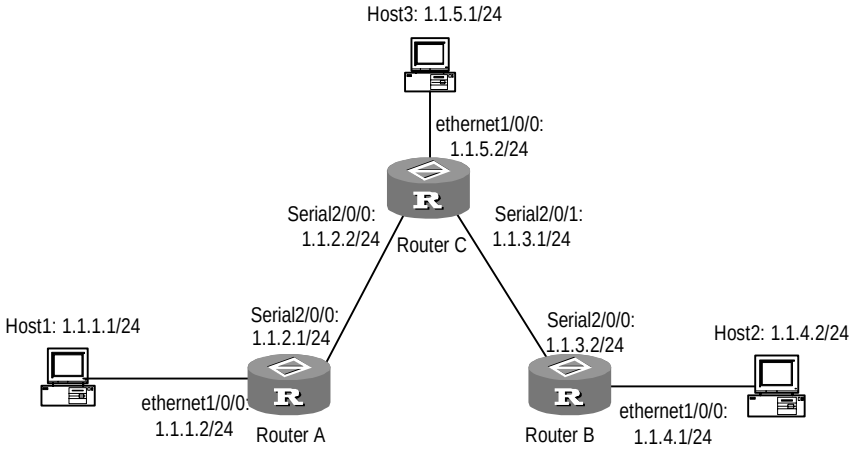


图2-1 静态路由配置举例组网图

3. 配置步骤

配置路由器 Router A 静态路由：

```
[Router A] ip route-static 1.1.3.0 255.255.255.0 1.1.2.2
[Router A] ip route-static 1.1.4.0 255.255.255.0 1.1.2.2
[Router A] ip route-static 1.1.5.0 255.255.255.0 1.1.2.2
```

或只配缺省路由：

```
[Router A] ip route-static 0.0.0.0 0.0.0.0 1.1.2.2
```

配置路由器 Router B 静态路由：

```
[Router B] ip route-static 1.1.2.0 255.255.255.0 1.1.3.1
[Router B] ip route-static 1.1.5.0 255.255.255.0 1.1.3.1
[Router B] ip route-static 1.1.1.0 255.255.255.0 1.1.3.1
```

或只配缺省路由：

```
[Router B] ip route-static 0.0.0.0 0.0.0.0 1.1.3.1
```

配置路由器 RouterC 静态路由：

```
[Router C] ip route-static 1.1.1.0 255.255.255.0 1.1.2.1
[Router C] ip route-static 1.1.4.0 255.255.255.0 1.1.3.2
```

主机 Host1 上配缺省网关为 1.1.1.2

主机 Host 2 上配缺省网关为 1.1.4.1

主机 Host 3 上配缺省网关为 1.1.5.2

至此图 2-1中所有主机或路由器之间能两两互通。

2.5 静态路由配置的故障诊断与排除

故障之一：路由器没有配置动态路由协议，接口的物理状态和链路层协议状态均已处于 UP，但 IP 报文不能正常转发。

故障排除：

- 用 **display ip routing-table protocol static** 命令查看是否正确配置相应静态路由。
- 用 **display ip routing-table** 命令查看该静态路由是否已经生效。
- 查看是否在 NBMA 接口上未指定下一跳地址或指定的下一跳地址不正确。并查看 NBMA 接口的链路层二次路由表是否配置正确。

第3章 RIP 配置

📖 说明：

本章中有关 VPN 实例的具体参数解释，请参见本手册的“ MPLS ”模块，这里没有列出。

3.1 RIP 简介

RIP 是 Routing Information Protocol（路由信息协议）的简称。它是一种较为简单的内部网关协议（Interior Gateway Protocol，IGP），主要用于规模较小的网络中。

由于 RIP 的实现较为简单，协议本身的开销对网络的性能影响比较小，并且在配置和维护管理方面也比 OSPF 或 IS-IS 容易，因此在实际组网中仍有广泛的应用。

3.1.1 RIP 的工作机制

1. RIP 的基本概念

RIP 是一种基于距离矢量（Distance-Vector）算法的协议，它通过 UDP 报文进行路由信息的交换。

RIP 使用跳数（Hop Count）来衡量到达目的网络的距离，称为路由权（Routing Cost）。在 RIP 中，路由器到与它直接相连网络的跳数为 0，通过一个路由器可达的网络的跳数为 1，其余依此类推。为限制收敛时间，RIP 规定 cost 取值 0～15 之间的整数，大于或等于 16 的跳数被定义为无穷大，即目的网络或主机不可达。

为提高性能，防止产生路由环，RIP 支持水平分割（Split Horizon），即不从某接口发送从该接口学到的路由。RIP 还可引入其它路由协议所得到的路由。

2. RIP 的路由数据库

每个运行 RIP 的路由器管理一个路由数据库，该路由数据库包含了到网络所有可达目的网络的路由项，这些路由项包含下列信息：

- 目的地址：指主机或网络的地址。
- 下一跳地址：指为到达目的地，本路由器要经过的下一个路由器地址。
- 接口：指转发报文的接口。
- 路由权值：指本路由器到达目的地的跳数，是一个 0～15 之间的整数。
- 路由时间：从路由项最后一次被修改到现在所经过的时间，路由项每次被修改时，路由时间重置为 0。

- 路由标记：区分路由为内部路由协议的路由还是引入外部路由协议的路由的标记。

3. RIP 使用的定时器

在 RFC1058 中规定，RIP 受三个定时器的控制，分别是 Period update、Timeout 和 Garbage-Collection：

- Period update 定时触发，向所有邻居发送全部 RIP 路由；
- RIP 路由如果在 Timeout 时间内没有被更新（收到邻居发来的路由刷新报文），则认为该路由不可达；
- 如果在 Garbage-Collection 时间内，不可达路由没有收到来自同一邻居的更新，则该路由被从路由表中删除。

3.1.2 RIP 的版本

RIP 有两个版本：RIP-1 和 RIP-2。

RIP-1 是有类别路由协议（Classful Routing Protocol），它只支持以广播方式发布协议报文。RIP-1 的协议报文中没有携带掩码信息，它只能识别 A、B、C 类这样的自然网段的路由，因此 RIP-1 无法支持路由聚合，也不支持不连续子网（Discontiguous Subnet）。

RIP-2 是一种无分类路由协议（Classless Routing Protocol），与 RIP-1 相比，它有以下优势：

- 支持外部路由标记（Route Tag），可以在路由策略中根据 Tag 对路由进行灵活的控制。
- 报文中携带掩码信息，支持路由聚合和 CIDR（Classless Inter-Domain Routing）。
- 支持指定下一跳，在广播网上可以选择到最优下一跳地址。
- 支持组播路由发送更新报文，减少资源消耗。
- 支持对协议报文进行验证，并提供明文验证和 MD5 验证两种方式，增强安全性。

📖 说明：

RIP-2 有两种报文传送方式：广播方式和组播方式，缺省将采用组播方式发送报文，使用的组播地址为 224.0.0.9。当接口运行 RIP-2 广播方式时，也可接收 RIP-1 的报文。

3.1.3 RIP 的启动和运行过程

RIP V1 启动和运行的整个过程可描述如下：

- 某路由器刚启动 RIP 时，以广播的形式向相邻路由器发送请求报文，运行 RIP 协议的相邻路由器的 RIP 收到请求报文后，响应该请求，回送包含本地路由表信息的响应报文。
- 路由器收到响应报文后，更新本地路由表，同时向相邻路由器发送触发更新报文，广播路由更新信息。运行 RIP 协议的相邻路由器收到触发更新报文后，又向其各自的相邻路由器发送触发更新报文。在一连串的触发更新广播后，各路由器都能得到并保持最新的路由信息。
- 同时，RIP 每隔 Period update 的时间向相邻路由器广播本地路由表，运行 RIP 协议的相邻路由器在收到报文后，对本地路由进行维护，选择一条最佳路由，再向其各自相邻网络广播更新信息，使更新的路由最终能达到全局有效。同时，RIP 采用超时机制对过时的路由进行超时处理，以保证路由的实时性和有效性。

RIP V2 的启动和运行过程基本相同，但其更新报文是发送到组播地址 224.0.0.9，而非广播报文。

RIP 正被大多数 IP 路由器厂商广泛使用。它可用于大多数校园网及结构较简单的连续性强的地区性网络。对于更复杂环境及大型网络，一般不使用 RIP。

3.1.4 VRP 支持的 RIP 特性

在 VRP 目前的实现中，支持以下 RIP 特性：

- 支持 RIP-1 和 RIP-2；
- 支持 RIP 多实例，可以作为 VPN 内部路由协议，在 MPLS VPN 解决方案的 CE-PE 之间运行；
- 支持 RIP 等价路由。
- 支持 RIP 触发更新。
- 在提供 IPX 特性的集中式设备中，还支持 IPX RIP（IPX 及 IPX RIP 的详细介绍，请参考本手册的“ 网络协议 ”部分）。

3.2 RIP 配置

配置 RIP 时，必须先启动 RIP，才能配置其它特性。而配置与接口相关的特性不受 RIP 是否使能的限制。需要注意的是，在关闭 RIP 后，与 RIP 相关的接口参数也同时失效。

(1) 基本的 RIP 配置

对于基本的 RIP 配置，需要进行的操作包括：

- 启动 RIP
- 在指定网段使能 RIP

如果在不支持广播或组播报文的链路上运行 RIP，需要配置 RIP 报文定点传送，以正确建立 RIP 邻居。

对于采用 Frame Relay 子接口等 NBMA 链路组网的情况，为保证路由信息的正确传播，可能还需要禁止水平分割特性。

(2) RIP 路由管理

在对路由信息的发布和接收上，可以对 RIP 进行以下配置：

- 配置附加路由权
- 配置 RIP 的路由引入
- 配置 RIP 的路由过滤
- 禁止 RIP 接收主机路由
- 配置 RIP 的路由聚合
- 配置 RIP 非直连邻居的路由交互
- 配置 RIP 在接口间实现负载分担功能

(3) RIP 协议本身的参数配置

- 配置 RIP 优先级
- 配置 RIP 定时器
- 配置 RIP 的零域检查
- 配置接口的 RIP 版本

(4) 安全性考虑

为提高 RIP 在交换路由信息时的安全性，或控制 RIP 报文的扩散范围，可以选择以下配置：

- 配置 RIP 报文认证
- 配置接口的工作状态

(5) RIP 对 MPLS VPN 的支持

- 配置 RIP 多实例

3.2.1 启动 RIP

启动 RIP 后，将进入 RIP 视图。

请在系统视图下进行下列配置。

表3-1 启动 RIP

操作	命令
启动 RIP，进入 RIP 视图	**rip**
停止 RIP 协议的运行	**undo rip**

缺省情况下，不运行 RIP。

RIP 的大部分特性都需要在 RIP 视图下配置，接口视图下也有部分 RIP 相关属性的配置。如果启动 RIP 前先在接口视图下进行了 RIP 相关的配置，这些配置只有在 RIP 启动后才会生效。需要注意的是，在执行 **undo rip** 命令关闭 RIP 后，接口上与 RIP 相关的配置也将被删除。

3.2.2 在指定网段使能 RIP

为了灵活地控制 RIP 工作，可以指定某些接口，将其所在的相应网段配置成 RIP 网络，使这些接口可收发 RIP 报文。

请在 RIP 视图下进行下列配置。

表3-2 在指定网段使能 RIP

操作	命令
在指定的网络接口上应用 RIP	**network** *network-address*
在指定的网络接口上取消应用 RIP	**undo network** *network-address*

RIP 只在指定网段上的接口运行；对于不在指定网段上的接口，RIP 既不在它上面接收和发送路由，也不将它的接口路由转发出去。因此，RIP 启动后必须指定其工作网段。*network-address* 为使能或不使能的网络的地址，也可配置为各个接口 IP 网络的地址。

当对某一地址使用命令 **network** 时，效果是使能该地址的网段的接口。例如：**network** 129.102.1.1，用 **display current-configuration** 和 **display rip** 命令看到的均是 **network** 129.102.0.0。

对于 RIP v1，路由协议在发布路由信息时有如下情况需要注意：

- 如果当前路由的目的地址和发送接口的地址不在同一主网（指自然网段），那么对于超网路由则不发送给邻居；对于子网路由则按自然网段聚合后发送给邻居。
- 如果当前的路由的目的地址和发送接口地址在同一主网，那么如果路由的目的地址的掩码和接口掩码不相等，就不发送给邻居；否则直接发送给邻居。

缺省情况下，任何网段都未使能 RIP。

3.2.3 配置水平分割

水平分割是指不从本接口发送从该接口学到的路由。它可以在一定程度上避免产生路由环。但在某些特殊情况下，却需要禁止水平分割，以保证路由的正确传播。禁止水平分割对点到点链路不起作用，但对以太网来说是可行的。

请在接口视图下进行下列配置。

表3-3 配置水平分割

操作	命令
启动水平分割	**rip split-horizon**
禁止水平分割	**undo rip split-horizon**

缺省情况下，接口允许水平分割。

3.2.4 配置附加路由权

附加路由权是对 RIP 路由添加的输入或输出路由权值，附加路由权并不直接改变路由表中的路由权值，而是在接收或发送路由时增加一个指定的权值。

请在接口视图下进行下列配置。

表3-4 设置附加路由权

操作	命令
设置接口在接收 RIP 报文时给路由附加路由权值	**rip metricin** *value*
禁止接口在接收 RIP 报文时给路由附加路由权值	**undo rip metricin**
设置接口在发送 RIP 报文时给路由附加路由权值	**rip metricout** *value* [**all-route**]
禁止接口在发送 RIP 报文时给路由附加路由权值	**undo rip metricout**

缺省情况下，RIP 在发送报文时给路由增加的附加路由权值为 1；在接收报文时给路由增加的附加路由权值为 0。

3.2.5 配置 RIP 的路由引入

RIP 允许用户将其它路由协议的路由信息引入到 RIP 路由表中，并可以设置引入时使用的缺省路由权。

可引入到 RIP 中的路由类型包括：Direct、Static、OSPF、BGP 和 IS-IS。

请在 RIP 视图下进行下列配置。

表3-5 配置 RIP 的路由引入

操作	命令
引入其它协议的路由	**import-route** *protocol* [**allow-ibgp**] [**cost** *value*] [**route-policy** *route-policy-name*]
取消对其它协议路由的引入	**undo import-route** *protocol*
设定缺省路由权值	**default cost** *value*
恢复缺省路由权值	**undo default cost**

缺省情况下，RIP 不引入其它协议的路由。

当 *protocol* 为 BGP 时，**allow-ibgp** 为可选关键字。**import-route bgp** 表示只引入 EBGP 路由，**import-route bgp allow-ibgp** 表示将 IBGP 路由也引入，该配置危险，请慎用！

如果在引入路由时没有指定路由权，则使用缺省路由权，其缺省值为 1。

3.2.6 配置 RIP 的路由过滤

路由器提供路由过滤功能，通过指定访问控制列表和地址前缀列表，可以配置策略规则，对路由的引入和发布进行过滤。

在引入路由时，还可以指定只接收来自某个邻居的 RIP 报文。

请在 RIP 视图下进行下列配置。

1. 配置 RIP 对接收的路由进行过滤

表3-6 配置 RIP 对接收路由的过滤

操作	命令
对接收的由指定地址发布的路由信息进行过滤	**filter-policy gateway** *ip-prefix-name* **import**
取消对接收的由指定地址发布的路由信息的过滤	**undo filter-policy gateway** *ip-prefix-name* **import**
对接收的全局路由信息进行过滤	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] } **import**
取消对接收的全局路由信息过滤	**undo filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] } **import**
对接收的全局路由信息按路由策略进行过滤	**filter-policy route-policy** *route-policy-name* **import**
取消对接收的全局路由信息按路由策略进行过滤	**undo filter-policy route-policy** *route-policy-name* **import**

2. 配置 RIP 对发布的路由进行过滤

表3-7 配置 RIP 对发布路由的过滤

操作	命令
对其他路由协议发布到 RIP 的路由进行过滤	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name*| **route-policy** *route-policy-name* } **export** [*routing-protocol*]
对发布的路由信息取消过滤	**undo filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **export** [*routing-protocol*]

缺省情况下，RIP 不对接收与发布的任何路由信息进行过滤。

更详细的描述请参见“ IP 路由策略配置 ”的“ 配置路由过滤 ”部分。

3.2.7 禁止 RIP 接收主机路由

在某些特殊情况下，路由器会收到大量来自同一网段的主机路由，这些路由对于路由寻址没有多少作用，却占用了大量网络资源。配置了禁止主机路由功能后，路由器能够拒绝它所收到的主机路由。

请在 RIP 视图下进行下列配置。

表3-8 禁止 RIP 接收主机路由

操作	命令
允许接收主机路由	**host-route**
禁止接收主机路由	**undo host-route**

缺省情况下，路由器接收主机路由。

3.2.8 配置 RIP 的路由聚合

路由聚合是指：同一自然网段内的不同子网的路由在向外（其它网段）发送时聚合成一条自然掩码的路由发送。这一功能主要用于减小路由表的尺寸，进而减少网络上的流量。

路由聚合对 RIP-1 不起作用。RIP-2 支持无类地址域间路由。当需要将所有子网路由广播出去时，可关闭 RIP-2 的路由聚合功能。

请在 RIP 视图下进行下列配置。

表3-9 配置 RIP 路由聚合

操作	命令
启动 RIP-2 的路由聚合功能	**summary**
关闭 RIP-2 的路由聚合功能	**undo summary**

缺省情况下，RIP-2 启用路由聚合功能。

3.2.9 配置 RIP 非直连邻居的路由交互

缺省情况下 RIP 只往直连的网段发送 RIP 报文，在发送单播报文时，会检查目的地址是否是直连地址；在收到 RIP 报文时，会检查报文的源地址，通过报文的源地址来找到入接口。基于这种原理，当两个路由器为 RIP 非直连邻居时，无法实现 RIP 路由信息的交互。

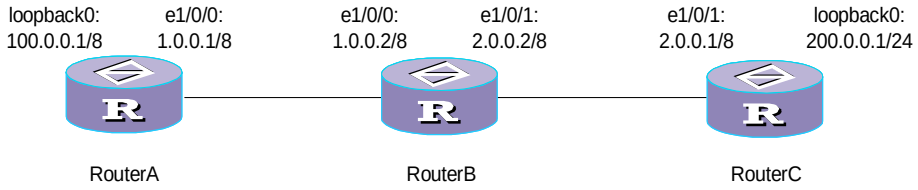


图3-1 RIP 非直连邻居的路由交互应用示意图

如上图所示，当在 RouterA 和 RouterC 为非直连邻居（仅 RouterA 的 1.0.0.0/8，RouterC 的 2.0.0.0/8 网段使能 RIP，RouterB 没有使能 RIP），此时如要实现 RouterA 和 RouterC 上的 RIP 路由交互，需要进行如下配置：

- 配置 RouterA 和 RouterC 互为 RIP peer
- 取消检查收到的 RIP 报文的源地址

此时，路由器在发送单播报文时，就不会检查目的地址是否是直连地址，并会去掉导致 RouterB 不转发报文的标志信息；在收到 RIP 报文时，也不会检查报文的源地址，并能通过报文的源地址和目的地址找到入接口。

1. 配置 RIP 报文定点传送

通常情况下，RIP 使用广播或组播地址发送报文，如果需要在不支持广播报文的链路上运行 RIP，就必须采用定点传送的方式，否则将不能正常地建立 RIP 邻居关系；在运行 RIP 协议的路由器为非直连邻居时，也必须配置 RIP 报文定点传送。

请在 RIP 视图下进行下列配置。

表3-10 配置 RIP 报文定点传送

操作	命令
配置 RIP 报文的定点传送	**peer** *ip-address*
取消 RIP 报文的定点传送	**undo peer** *ip-address*

缺省情况下，RIP 不向任何定点地址发送报文。

需要注意的是：peer 在发送报文时受接口工作状态的限制，接口的工作状态由 **rip work**、**rip output**、**rip input** 和 **network** 等命令进行配置。

2. 配置检查/不检查收到的 RIP 报文的源地址

请在 RIP 视图（或 RIP 的 MBGP 地址族视图）下进行下列配置。

表3-11 配置检查/不检查收到的 RIP 报文的源地址

操作	命令
配置检查 RIP 报文的源地址	**validate-source-address**
取消检查 RIP 报文的源地址	**undo validate-source-address**

该命令对公网 RIP 协议及 MPLS VPN 下的私网 RIP 协议均有效。

缺省情况下，检查 RIP 报文的源地址。

3.2.10 配置 RIP 在接口间实现负载分担功能

当启动了 RIP 接口间的负载分担功能时，可以使流量通过等价路由均衡地在各个接口之间分配。

请在 RIP 视图或 RIP 的 MBGP 地址族视图下进行下列配置。

表3-12 配置 RIP 在接口间实现负载分担功能

操作	命令
配置 RIP 在接口间实现负载分担功能	**traffic-share-across-interface**
关闭 RIP 在接口间的负载分担功能	**undo traffic-share-across-interface**

该命令对公网 RIP 协议及 MPLS VPN 下的私网 RIP 协议均有效。

缺省情况下，关闭 RIP 接口间流量负载分担功能，即仅支持简单的负载分担，并不考虑在接口上均衡分配流量。

3.2.11 配置 RIP 优先级

每一种路由协议都有自己的优先级，协议的优先级将影响路由策略采用哪种路由协议获取的路由作为最优路由。优先级的数值越大，其实际的优先级越低。可以手工设定 RIP 的优先级。

请在 RIP 视图下进行下列配置。

表3-13 设置 RIP 的优先级

操作	命令
设置 RIP 协议的优先级	**preference** *value*
将 RIP 协议的优先级恢复为缺省值	**undo preference**

缺省情况下，RIP 的优先级为 100。

3.2.12 配置 RIP 定时器

在本章开始已经介绍过，RIP 有三个定时器：Period update、Timeout 和 Garbage-collection。改变这几个定时器的值，可以影响 RIP 的收敛速度。

请在 RIP 视图下进行下列配置。

表3-14 配置 RIP 定时器

操作	命令
配置 RIP 定时器的值	**timers** { **update** *update-timer-length* | **timeout** *timeout-timer-length* } *
恢复 RIP 定时器的缺省值	**undo timers** { **update** | **timeout** } *

RIP 定时器的值在更改后立即生效。

缺省情况下，Period update 定时器是 30 秒，Timeout 定时器是 180 秒，Garbage-collection 定时器则是 Period update 定时器的 4 倍，即 120 秒。

在实际应用中，用户可能会发现 Garbage-collection 定时器的超时时间并不固定，当 Period update 定时器设为 30 秒时，Garbage-collection 定时器可能在 90 到 120 秒之间。这是因为：不可达路由在被从路由表中彻底删除前，需要等待 4 个来自同一邻居的更新报文，但路由变为不可达状态并不总是恰好在一个更新周期的开始，因此，Garbage-collection 定时器的实际时长是 Period update 定时器的 3～4 倍。

📖 说明：

在配置 RIP 定时器时需要注意，定时器值的调整应考虑网络的性能，并在所有运行 RIP 的路由器上进行统一配置，以免增加不必要的网络流量或引起网络路由震荡。

3.2.13 配置 RIP 的零域检查

RFC1058 规定，RIP-1 报文中的有些区域必须为零，称之为零域（zero field）。RIP-1 在接收报文时将对零域进行检查，值不为零的 RIP-1 报文将不被处理。由于 RIP-2 的报文没有零域，此项配置对 RIP-2 无效。

请在 RIP 视图下进行下列配置。

表3-15 配置报文的零域检查

操作	命令
设置对 RIP-1 报文进行零域检查	**checkzero**
禁止对 RIP-1 报文进行零域检查	**undo checkzero**

缺省情况下，RIP-1 对报文进行零域检查。

3.2.14 配置接口的 RIP 版本

RIP 有 RIP-1 和 RIP-2 两个版本，可以指定接口所处理的 RIP 报文版本。

RIP-1 的报文传送方式为广播方式。RIP-2 有两种报文传送方式：广播方式和组播方式，缺省将采用组播方式发送报文。RIP-2 中组播地址为 224.0.0.9。组播发送报文的好处是在同一网络中那些没有运行 RIP 的主机可以避免接收 RIP 的广播报文；另外，以组播方式发送报文还可以使运行 RIP-1 的主机避免错误地接收和处理 RIP-2 中带有子网掩码的路由。当接口运行 RIP-2 时，也可接收 RIP-1 的报文。

请在接口视图下进行下列配置。

表3-16 配置接口的 RIP 版本

操作	命令
指定接口的 RIP 版本为 RIP-1	**rip version 1**
指定接口的 RIP 版本为 RIP-2	**rip version 2** [**broadcast** | **multicast**]
将接口运行的 RIP 版本恢复为缺省值	**undo rip version**

缺省情况下，接口接收和发送 RIP-1 报文；指定接口 RIP 版本为 RIP-2 时，缺省使用组播形式传送报文。

3.2.15 配置 RIP 报文认证

RIP-1 不支持报文认证。但当接口运行 RIP-2 时，可以配置报文的认证方式。

RIP-2 支持两种认证方式：明文认证和 MD5 密文认证。MD5 密文认证的报文格式有两种：一种遵循 RFC2453，另一种遵循 RFC2082。

明文认证不能提供安全保障。未加密的认证字随报文一同传送，所以明文认证不能用于安全性要求较高的情况。

请在接口视图下进行下列配置。

表3-17 设置对 RIP 报文认证

操作	命令
对 RIP-2 进行明文认证	**rip authentication-mode simple** *password*
对 RIP-2 进行通用的 MD5 认证	**rip authentication-mode md5 usual** *key-string*
对 RIP-2 进行非标准兼容的 MD5 认证	**rip authentication-mode md5 nonstandard** *key-string key-id*
取消对 RIP-2 的认证	**undo rip authentication-mode**

如果配置 MD5 认证，则必须配置 MD5 的类型，其中 **usual** 类型支持 RFC2453 规定的报文格式，**nonstandard** 类型支持 RFC2082 规定的报文格式。

3.2.16 配置接口的工作状态

在接口视图中可指定 RIP 在接口上的工作状态，如接口上是否运行 RIP，即是否在接口发送和接收 RIP 更新报文；还可单独指定发送（或接收）RIP 更新报文。

请在接口视图下进行下列配置。

表3-18 配置接口的工作状态

操作	命令
指示接口运行 RIP	**rip work**
禁止接口运行 RIP	**undo rip work**
允许接口接收 RIP 更新报文	**rip input**
禁止接口接收 RIP 更新报文	**undo rip input**
允许接口发送 RIP 更新报文	**rip output**
禁止接口发送 RIP 更新报文	**undo rip output**

undo rip work 命令的功能与 **undo network** 命令功能相近，但它们并不完全相同。相同点在于，两命令都使接口不收发 RIP 路由；区别在于：执行了 **undo rip work** 命令的情况下，其它接口对使用该命令的接口的路由仍然转发；而执行 **undo network**，相当于在接口执行 **undo rip work**，而且相应的接口路由不能被 RIP 传播出去，导致到该接口的报文不能被转发。

rip work 从功能上等价于 **rip input** 与 **rip output** 两个命令。

缺省情况下，一个接口既接收 RIP 更新报文，也发送 RIP 更新报文。

3.2.17 配置 RIP 多实例

路由器具有 RIP 多实例功能，能够提供对 MPLS VPN 的支持。

请在 RIP 视图下进行下列配置。

表3-19 配置 RIP 多实例

操作	命令
进入 RIP 的 MBGP 地址族视图	**ipv4-family** [**unicast**] **vpn-instance** *vpn-instance-name*
删除 RIP 的 MBGP 地址族配置	**undo ipv4-family** [**unicast**] **vpn-instance** *vpn-instance-name*

执行 **undo ipv4-family** 命令后，将删除所有在 MBGP 地址族视图下进行的配置。

MBGP 地址族视图用于 BGP/MPLS VPN，相关内容请参见本手册的“ MPLS ”之“ MPLS VPN 配置 ”。

3.3 RIP 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 RIP 的运行情况，用户可以通过查看显示信息验证配置的效果。在用户视图下执行 **debugging** 命令可对 RIP 进行调试。

表3-20 RIP 显示和调试

操作	命令
显示 RIP 的当前运行状态及配置信息	**display rip**
显示 RIP 的接口信息	**display rip interface** [**vpn-instance** *vpn-instance-name*]
显示 RIP 的 MBGP 地址族相关配置	**display rip vpn-instance** *vpn-instance-name*
显示 RIP 路由表	**display rip routing** [**vpn-instance** *vpn-instance-name*]
打开 RIP 的报文调试信息开关	**debugging rip packets** [**interface** *type number*]
关闭 RIP 的报文调试信息开关	**undo debugging rip packets**
打开 RIP 的接收报文情况调试开关	**debugging rip receive**
关闭 RIP 的接收报文情况调试开关	**undo debugging rip receive**
打开 RIP 的发送报文情况调试开关	**debugging rip send**
关闭 RIP 的发送报文情况调试开关	**undo debugging rip send**

3.4 RIP 典型配置举例

3.4.1 配置指定接口的工作状态

1. 组网需求

一个企业的内部网络通过路由器 RouterA 连到 Internet，内部网络的主机直接连接到 RouterB 或 RouterC 上。

要求三个路由器上均运行 RIP。RouterA 只接收从外部网络发来的路由信息，但不对外发布内部网络的路由信息。RouterA、B、C 之间能够交互 RIP 信息，以便于内部主机能够访问 Internet。

2. 组网图

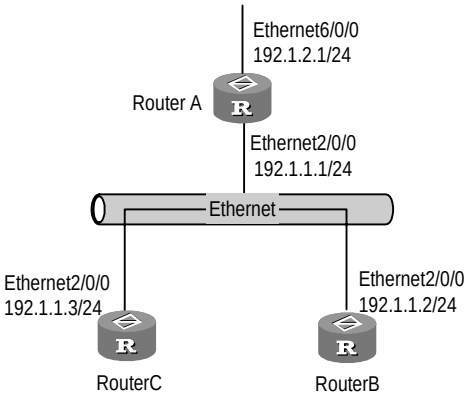


图3-2 配置接口的工作状态

3. 配置步骤

(1) 配置 RouterA

配置接口 Ethernet2/0/0 和 Ethernet6/0/0。

```
[RouterA] interface ethernet 2/0/0
[RouterA-Ethernet2/0/0] ip address 192.1.1.1 255.255.255.0
[RouterA-Ethernet2/0/0] quit
[RouterA] interface ethernet 6/0/0
[RouterA-Ethernet6/0/0] ip address 192.1.2.1 255.255.255.0
```

启动 RIP，并配置在接口 Ethernet2/0/0 和 Ethernet6/0/0 上运行 RIP。

```
[RouterA] rip
[RouterA-rip] network 192.1.1.0
[RouterA-rip] network 192.1.2.0
```

配置接口 Ethernet 6/0/0 只接收 RIP 报文。

```
[RouterA] interface ethernet 6/0/0
[RouterA-Ethernet6/0/0] undo rip output
[RouterA-Ethernet6/0/0] rip input
```

(2) 配置 RouterB

配置接口 Ethernet2/0/0

```
[RouterB] interface Ethernet 2/0/0
[RouterB-Ethernet2/0/0] ip address 192.1.1.2 255.255.255.0
```

启动 RIP，并配置在接口 Ethernet2/0/0 上运行 RIP。

```
[RouterB] rip
[RouterB-rip] network 192.1.1.0
[RouterB-rip] import direct
```

(3) 配置 RouterC

配置接口 Ethernet 2/0/0

```
[RouterC] interface Ethernet 2/0/0
[RouterC-Ethernet2/0/0] ip address 192.1.1.3 255.255.255.0
```

启动 RIP，并配置在接口 Ethernet2/0/0 运行 RIP。

```
[RouterC] rip
[RouterC-rip] network 192.1.1.0
[RouterC-rip] import direct
```

3.4.2 调整 RIP 网络的收敛时间

1. 组网需求

路由器 RouterA、RouterB 和 RouterC 上运行 RIP，要求网络的收敛时间在 30 秒以内。

2. 组网图

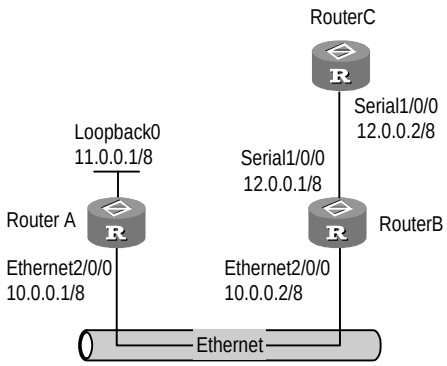


图3-3 RIP 定时器配置组网图

3. 配置步骤

📖 说明：

接口的 IP 地址配置如图 3-3所示，配置步骤中不再赘述。

---

(1) 配置 RouterA：

启动 RIP，并使能 RouterA 的接口 Ethernet2/0/0 和 LoopBack0 运行 RIP。

```
[RouterA] rip
[RouterA-rip] network 10.0.0.0
[RouterA-rip] network 11.0.0.0
[RouterA-rip] timers update 10 timeout 30
```

(2) 配置 RouterB：

启动 RIP，并使能 RouterB 的接口 Ethernet2/0/0 和 Serial1/0/0 运行 RIP。

```
[RouterB] rip
[RouterB-rip] network 10.0.0.0
[RouterB-rip] network 12.0.0.0
[RouterB-rip] timers update 10 timeout 30
```

(3) 配置 RouterC：

启动 RIP，并使能 RouterC 的接口 Serial1/0/0 运行 RIP。

```
[RouterC] rip
[RouterC-rip] network 12.0.0.0
[RouterC-rip] timers update 10 timeout 30
```

配置结束后，在 RouterB 和 RouterC 执行 **display ip routing-table** 命令能看到 11.0.0.0/8 的路由。将 RouterA 的 Ethernet2/0/0 接口 shutdown，30 秒内，可以观察到 RTB 和 RTC 上的路由 11.0.0.0/8 变成不可达。

在调整定时器之前，RouterA 的 Ethernet2/0/0 接口 shutdown 后，RouterB 和 RouterC 需要 180 秒的时间才能感知到路由不可达，可见，调整定时器后，RIP 网络的收敛时间缩短了。

3.4.3 RIP 非直连邻居的路由交互配置举例

1. 组网需求

如下图所示，路由器 B 不支持 RIP 协议。RouterA 在 e1/0/0 口使能 RIP，引入直连路由，并配置指向 2.0.0.0/8 的静态路由；C 上在 e1/0/0 口使能 RIP，引入直连路由，并配置指向 1.0.0.0/8 的静态路由。RouterA 和 RouterC 上配置互为 RIP peer，取消检查收到的 RIP 报文的源地址。最终实现在 RouterA 上获得到 RouterC 的 200.0.0.1/24 RIP 路由，RouterC 上也能获得到 RouterA 的 100.0.0.1/8 RIP 路由。

2. 组网图

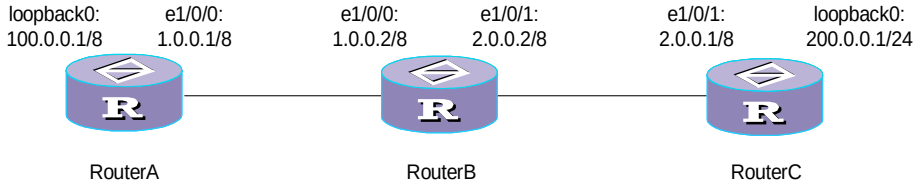


图3-4 RIP 非直连邻居的路由交互配置举例

3. 配置步骤

(1) 配置路由器 A

配置接口 IP 地址。

```
[RouterA] interface Ethernet1/0/0
[RouterA-Ethernet1/0/0] ip address 1.0.0.1 255.0.0.0
[RouterA-Ethernet1/0/0] rip version 2
```

```
[RouterA-Ethernet1/0/0] interface LoopBack0
[RouterA-LoopBack0] ip address 100.0.0.1 255.0.0.0
[RouterA-LoopBack0] quit
```

配置启动 RIP 协议。

```
[RouterA] rip
[RouterA-rip] undo summary
[RouterA-rip] network 1.0.0.0
```

配置启动 RIP peer，并配置不检查 RIP 报文源地址。

```
[RouterA-rip] peer 2.0.0.1
[RouterA-rip] undo validate-source-address
```

配置 RIP 协议引入直连路由。

```
[RouterA-rip] import-route direct
[RouterA-rip] quit
```

配置到 2.0.0.0 网段的静态路由。

```
[RouterA] ip route-static 2.0.0.0 255.0.0.0 1.0.0.2 preference 60
```

(2) 配置路由器 B

配置接口 IP 地址。

```
[RouterB] interface Ethernet1/0/0
[RouterB-Ethernet1/0/0] ip address 1.0.0.2 255.0.0.0
[RouterB-Ethernet1/0/0] interface Ethernet1/0/1
[RouterB-Ethernet1/0/1] ip address 2.0.0.2 255.0.0.0
```

(3) 配置路由器 C

配置接口 IP 地址。

```
[RouterC] interface Ethernet1/0/0
[RouterC-Ethernet1/0/0] ip address 2.0.0.1 255.0.0.0
[RouterC-Ethernet1/0/0] rip version 2
[RouterC-Ethernet1/0/0] interface LoopBack0
[RouterC-LoopBack0] ip address 200.0.0.1 255.255.255.0
```

启动 RIP 协议。

```
[RouterC] rip
[RouterC-rip] undo summary
[RouterC-rip] network 2.0.0.0
```

配置 RIP peer，并配置不检查收到的 RIP 报文。

```
[RouterC-rip] peer 1.0.0.1
[RouterC-rip] undo validate-source-address
```

配置进入直连路由。

```
[RouterC-rip] import-route direct
```

```
[RouterC-rip] quit
```

配置到 1.0.0.0 网段的静态路由器。

```
[RouterC] ip route-static 1.0.0.0 255.0.0.0 2.0.0.2 preference 60
```

RouterA，C 上必须配置到达对端的静态路由，保证路由可达，否则 RIP 报文无法发送给 peer。

另外，若 RouterC 为 PE，则需要配置 RIP 多实例，并在 RIP 的 MBGP 地址族视图下配置取消检查 RIP 接收报文：

配置 vpn-instance。

```
[RouterC] ip vpn-instance in
[RouterC-vpn-in] route-distinguisher 100:1
[RouterC-vpn-in] vpn-target 100:1 export-extcommunity
[RouterC-vpn-in] vpn-target 100:1 import-extcommunity
[RouterC-vpn-in] quit
```

配置 RIP 多实例。

```
[RouterC] rip
[RouterC-rip] ipv4-family vpn-instance in
[RouterC-rip-af-vpn-instance] undo validate-source-address
```

3.5 RIP 故障诊断与排除

故障之一：在物理连接正常的情况下收不到更新报文。

故障排除，可能是下列原因：

相应的接口上 RIP 没有运行（如执行了 **undo rip work** 命令）或该接口未通过 **network** 命令使能。对端路由器上配置的是组播方式（如执行了 **rip version 2 multicast** 命令），但在本地路由器上没有配置组播方式。

故障之二：运行 RIP 的网络发生路由震荡。

故障排除：在各运行 RIP 的路由器上使用 **display rip** 命令查看 RIP 定时器的配置，如果不同路由器的 Period Update 定时器和 Timeout 定时器值不同，重新将全网的定时器配置一致，并确保 Timeout 定时器时间长度大于 Period Update 定时器的时间长度。

第4章 OSPF 配置

4.1 OSPF 简介

4.1.1 OSPF 概述

OSPF 是 Open Shortest Path First（开放最短路由优先协议）的缩写。它是 IETF 组织开发的一个基于链路状态的内部网关协议。目前使用的是版本 2（RFC2328），其特性如下：

- 适应范围——支持各种规模的网络，最多可支持几百台路由器。
- 快速收敛——在网络的拓扑结构发生变化后立即发送更新报文，使这一变化在自治系统中同步。
- 无自环——由于 OSPF 根据收集到的链路状态用最短路径树算法计算路由，从算法本身保证了不会生成自环路由。
- 区域划分——允许自治系统的网络被划分成区域来管理，区域间传送的路由信息被进一步抽象，从而减少了占用的网络带宽。
- 等值路由——支持到同一目的地址的多条等值路由。
- 路由分级——使用 4 类不同的路由，按优先顺序来说分别是：区域内路由、区域间路由、第一类外部路由、第二类外部路由。
- 支持验证——支持基于接口的报文验证以保证路由计算的安全性。
- 组播发送——支持组播地址。

4.1.2 OSPF 的路由计算过程

OSPF 协议的路由计算过程可简单描述如下：

- 每个支持 OSPF 协议的路由器都维护着一份描述整个自治系统拓扑结构的链路状态数据库（Link Sate Database，简称为 LSDB）。每台路由器根据自己周围的网络拓扑结构生成链路状态广播（Link State Advertisement，简称为 LSA），通过相互之间发送协议报文将 LSA 发送给网络中其它路由器。这样每台路由器都收到了其它路由器的 LSA，所有的 LSA 一起组成链路状态数据库。
- 由于 LSA 是对路由器周围网络拓扑结构的描述，那么 LSDB 则是对整个网络的拓扑结构的描述。路由器很容易将 LSDB 转换成一张带权的有向图，这张图

便是对整个网络拓扑结构的真实反映。显然，各个路由器得到的是一张完全相同的图。

- 每台路由器都使用 SPF 算法计算出一棵以自己为根的最短路径树，这棵树给出了到自治系统中各节点的路由，外部路由信息为叶子节点，外部路由可由广播它的路由器进行标记以记录关于自治系统的额外信息。显然，各个路由器各自得到的路由表是不同的。

此外，为使每台路由器能将本地状态信息（如可用接口信息、可达邻居信息等）广播到整个自治系统中，在路由器之间要建立多个邻接关系，这使得任何一台路由器的路由变化都会导致多次传递，既没有必要，也浪费了宝贵的带宽资源。为解决这一问题，OSPF 协议定义了“ 指定路由器 ”（DR），所有路由器都只将信息发送给 DR，由 DR 将网络链路状态广播出去。这样就减少了多址访问网络上各路由器之间邻接关系的数量。

OSPF 协议支持基于接口的报文验证以保证路由计算的安全性；并使用 IP 多播方式发送和接收报文。

4.1.3 OSPF 相关的基本概念

1. Router ID

一台路由器如果要运行 OSPF 协议，必须存在 Router ID。如果没有配置 ID 号，系统会从当前接口的 IP 地址中选出 IP 地址最大的作为 router id。一般建议选择 loopback 接口的 IP 地址作为本机 ID 号，因为该接口永远 UP（除非手工 shutdown）。

2. DR 和 BDR

- DR（Designated Router，指定路由器）

在广播网络或者多点访问网络中，为使每台路由器能将本地状态信息广播到整个自治系统中，在路由器之间要建立多个邻居关系，但这使得任何一台路由器的路由变化都会导致多次传递，浪费了宝贵的带宽资源。为解决这一问题，OSPF 协议定义了 DR，所有路由器都只将信息发送给 DR，由 DR 将网络链路状态广播出去，除 DR/BDR 外的路由器（称为 DR Other）之间将不再建立邻居关系，也不再交换任何路由信息。

哪一台路由器会成为本网段内的 DR 并不是人为指定的，而是由本网段中所有的路由器共同选举出来的。

- BDR（Backup Designated Router，备份指定路由器）

如果 DR 由于某种故障而失效，这时必须重新选举 DR，并与之同步。这需要较长的时间，在这段时间内，路由计算是不正确的。为了能够缩短这个过程，OSPF 提出了 BDR 的概念。BDR 实际上是对 DR 的一个备份，在选举 DR 的同时也选举出 BDR，

BDR 也和本网段内的所有路由器建立邻接关系并交换路由信息。当 DR 失效后，BDR 会立即成为 DR，并重新选举 BDR。

3. 区域（Area）

随着网络规模日益扩大，当一个网络中的 OSPF 路由器数量非常多时，会导致 LSDB 变得很庞大，占用大量存储空间，并消耗很多 CPU 资源来进行 SPF 计算。并且，网络规模增大后，拓扑结构发生变化的概率也会增大，导致大量的 OSPF 协议报文在网络中传递，降低网络的带宽利用率。

OSPF 协议将自治系统划分成多个区域（Area）来解决上述问题。区域在逻辑上将路由器划分为不同的组。不同的区域以区域号（Area ID）标识，其中一个最重要的区域是区域 0，也称为骨干区域（backbone area）。

骨干区域完成非骨干区域之间的路由信息交换，它必须是连续的，对于物理上不连续的区域，需要配置虚连接（virtual links）来保持骨干区域在逻辑上的连续性。

连接骨干区域和非骨干区域的路由器称作区域边界路由器（Area Border Router，简称为 ABR）。

OSPF 中还有一类自治系统边界路由器（Autonomous System Boundary Router，简称为 ASBR），实际上，这里的 AS 并不是严格意义的自治系统，连接 OSPF 路由域（routing domain）和其它路由协议域的路由器都是 ASBR，可以认为 ASBR 是引入 OSPF 外部路由信息的路由器。

4. 路由聚合

AS 被划分成不同的区域，每一个区域通过 OSPF 边界路由器（ABR）相连，区域间可以通过路由汇聚来减少路由信息，减小路由表的规模，提高路由器的运算速度。

ABR 在计算出一个区域的区域内路由之后，查询路由表，将其中每一条 OSPF 路由封装成一条 LSA 发送到区域之外。

例如，图 4-1中，Area 19 内有三条区域内路由 19.1.1.0/24，19.1.2.0/24，19.1.3.0/24，如果此时配置了路由聚合，将三条路由聚合成一条 19.1.0.0/16，在 RTA 上就只生成一条描述聚合后路由的 LSA。

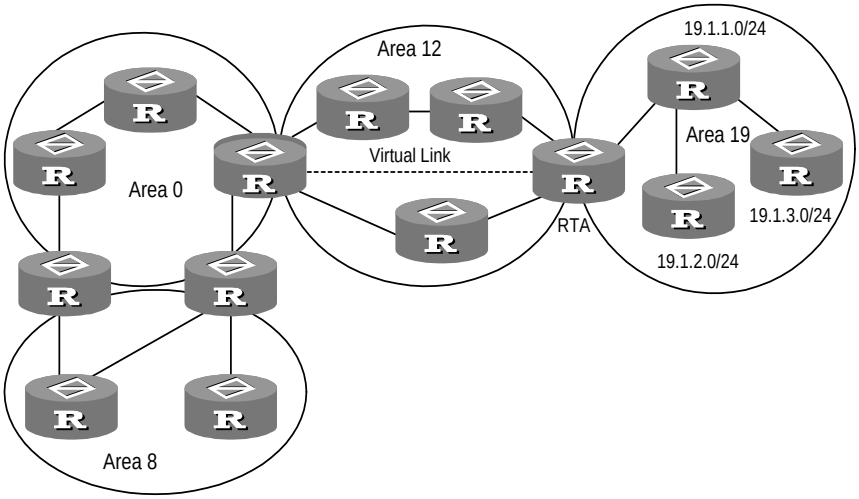


图4-1 区域及路由聚合示意图

4.1.4 OSPF 的协议报文

OSPF 有五种报文类型：

- HELLO 报文（Hello Packet）：

最常用的一种报文，周期性的发送给本路由器的邻居。内容包括一些定时器的数值、DR、BDR 以及自己已知的邻居。

- DD 报文（Database Description Packet）：

两台路由器进行数据库同步时，用 DD 报文来描述自己的 LSDB，内容包括 LSDB 中每一条 LSA 的摘要（摘要是指 LSA 的 HEAD，通过该 HEAD 可以唯一标识一条 LSA）。这样做是为了减少路由器之间传递信息的量，因为 LSA 的 HEAD 只占一条 LSA 的整个数据量的一小部分，根据 HEAD，对端路由器就可以判断出是否已有这条 LSA。

- LSR 报文（Link State Request Packet）：

两台路由器互相交换 DD 报文之后，知道对端的路由器有哪些 LSA 是本地的 LSDB 所缺少的，这时需要发送 LSR 报文向对方请求所需的 LSA。内容包括所需要的 LSA 的摘要。

- LSU 报文（Link State Update Packet）：

用来向对端路由器发送所需要的 LSA，内容是多条 LSA（全部内容）的集合。

- LSAck 报文（Link State Acknowledgment Packet）

用来对接收到的 LSU 报文进行确认。内容是需要确认的 LSA 的 HEAD（一个报文可对多个 LSA 进行确认）。

4.1.5 OSPF 的 LSA 类型

1. 五类基本的 LSA

根据前面几节的介绍可以了解到，链路状态广播报文 LSA 是 OSPF 协议计算和维护路由信息的主要来源。在 RFC2328 中定义了五类 LSA，描述如下：

- Router-LSAs：第一类 LSA（Type-1），由每个路由器生成，描述本路由器的链路状态和花费，只在路由器所处区域内传播。
- Network-LSAs：第二类 LSA（Type-2），由广播网络和 NBMA 网络的 DR 生成，描述本网段的链路状态，只在 DR 所处区域内传播。
- Summary-LSAs：包含第三类 LSA 和第四类 LSA（Type-3，Type-4），由区域边界路由器 ABR 生成，在与该 LSA 相关的区域内传播。每一条 Summary-LSA 描述一条到达本自治系统的、其它区域的某一目的地的路由（即区域间路由：inter-area route）。Type-3 Summary-LSAs 描述去往网络的路由（目的地为网段），Type-4 Summary-LSAs 描述去往自治系统边界路由器 ASBR 的路由。
- AS-external-LSAs：第五类 LSA（Type-5），由自治系统边界路由器 ASBR 生成，描述到达其它 AS 的路由，传播到整个 AS（Stub 区域除外）。AS 的缺省路由也可以用 AS-external-LSAs 来描述。

2. 第七类 LSA

在 RFC1587（OSPF NSSA Option）中增加了一类新的 LSA：NSSA LSAs，也称为 Type-7 LSAs。

根据 RFC1587 的描述，Type-7 LSAs 与 Type-5 LSAs 主要有以下两点区别：

- Type-7 LSAs 在 NSSA 区域（Not-So-Stubby Area）内产生和发布；但 NSSA 区域内不会产生或发布 Type-5 LSAs。
- Type-7 LSAs 只能在一个 NSSA 内发布，当到达区域边界路由器 ABR 时，由 ABR 将 Type-7 LSAs 转换成 Type-5 LSAs 再发布，不直接发布到其它区域或骨干区域。

3. Opaque LSAs

为了使 OSPF 能够支持更多新的业务应用，在 RFC2370（The OSPF Opaque LSA）中定义了用于对 OSPF 进行扩展的 Opaque LSAs。

Opaque LSAs 包含三种类型的 LSA，不同类型的 LSA 扩散范围不同：

- Type-9：扩散范围为 link-local，可以认为只在某一个接口所在的网段扩散，不会发布到本地网段或本地子网以外。

- Type-10：扩散范围为 area-local，即，只在本区域以内扩散。
- Type-11：与 Type-5 LSAs 具有相同的扩散范围，可以在除 STUB 区域和 NSSA 区域之外的整个自治系统内部扩散。

Opaque LSAs 包括一个标准的 20 字节 LSA 头和一个应用信息相关的域，其报文结构如下图所示：

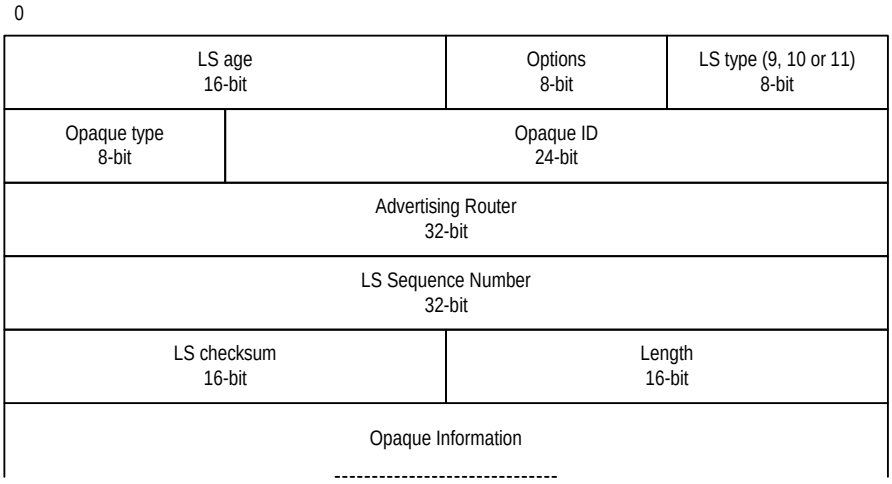


图4-2 Opaque LSAs 结构示意图

其中，Opaque Type 字节用来标识此 LSA 的应用类型，Opaque ID 则对同一应用类型的 LSA 做进一步的区分。

Opaque Information 字段中是 LSA 携带的信息，具体的信息格式可由不同的应用根据自己的需求来定义。

4.1.6 VRP 支持的 OSPF 特性

在 VRP 目前的实现中，支持以下 OSPF 特性：

- 支持 OSPF STUB 区域；
- 支持 OSPF NSSA 区域；
- 支持 OSPF 多进程（Multi-Process），可以在一台路由器上运行多个 OSPF 进程；
- 支持 OSPF 多实例（Multi-VPN-Instance），可以作为 VPN 内部路由协议，在 MPLS VPN 解决方案的 CE-PE 之间运行；
- 支持 MPLS 流量工程（Traffic Engineering，简称 TE），使用 Type-10 的 Opaque LSAs，应用类型（Opaque type）为 1。

OSPF 在 MPLS VPN 中的应用请参考本手册“VPN”部分，OSPF 在 MPLS TE 中的应用请参考本手册“MPLS”部分。

4.2 OSPF 的配置

在各项配置中，必须先启动 OSPF、指定接口与区域号后，才能配置其它的功能特性。

而配置与接口相关的功能特性不受 OSPF 是否使能的限制。需要注意的是，在关闭 OSPF 后，原来与 OSPF 相关的接口参数也同时失效。

(1) 基本的 OSPF 配置

对于基本的 OSPF 配置，需要进行的操作包括：

- 配置 Router ID
- 启动 OSPF
- 进入 OSPF 区域视图
- 在指定网段使能 OSPF

如果 OSPF 的骨干区域不连续，则需要：

- 配置 OSPF 虚连接

根据 OSPF 的网络类型不同，可能还需要进行以下配置：

- 配置 OSPF 网络类型
- 配置邻接点

(2) OSPF 路由的管理

- 配置 OSPF 的路由引入
- 配置 OSPF 的路由过滤
- 配置 OSPF 的路由聚合

(3) OSPF 协议本身的参数配置

- 配置 OSPF 优先级
- 配置 OSPF 定时器
- 配置选举 DR 时的优先级
- 配置接口发送报文的开销
- 配置 OSPF 的 SPF 计算间隔
- 配置发送链路状态更新报文所需时间
- 配置接口发送 DD 报文时是否填 MTU 值
- 配置 OSPF 等值路由的最大个数

(4) 安全性考虑

为提高 OSPF 在交换路由信息时的安全性，或控制 OSPF 报文的扩散范围，可以选择以下配置：

- 配置 OSPF 认证
- 配置接口的工作状态

(5) OSPF 高级特性的配置

- 配置 OSPF 的 STUB 区域
- 配置 OSPF 的 NSSA 区域
- 使能 OSPF 的 Opaque 能力
- 配置 OSPF 与网管系统的配合
- 重启 OSPF

📖 说明：

OSPF 多实例的具体应用和在 MPLS VPN 中的配置，请参考本手册的“ VPN ”部分；OSPF 在 MPLS TE 中的具体应用和配置，请参考本手册的 “ MPLS ” 部分。

4.2.1 配置 Router ID

路由器的 ID 是一个 32 比特无符号整数，采用 IP 地址形式，是一台路由器在自治系统中的唯一标识。路由器的 ID 可以手工配置，如果没有配置 ID 号，系统会从当前接口的 IP 地址中自动选一个作为路由器的 ID 号。手工配置路由器的 ID 时，必须保证自治系统中任意两台路由器的 ID 都不相同。通常的做法是将路由器的 ID 配置为与该路由器某个接口的 IP 地址一致。

请在系统视图下进行下列配置。

表4-1 配置路由器 ID 号

操作	命令
配置路由器的 ID 号	**router id** *router-id*
取消路由器的 ID 号	**undo router id**

为保证 OSPF 运行的稳定性，在进行网络规划时，应确定路由器 ID 的划分并手工配置。

📖 说明：

OSPF 启动后修改的 Router ID，需要重新启动 OSPF 进程之后，Router ID 才能在 OSPF 中生效。

4.2.2 启动 OSPF

OSPF 支持多进程，一台路由器上启动的多个 OSPF 进程之间由不同的进程号区分。OSPF 进程号在启动 OSPF 时进行设置，它只在本地有效，不影响与其它路由器之间的报文交换。

请在系统视图下进行下列配置。

表4-2 启动/关闭 OSPF

操作	命令
启动 OSPF，进入 OSPF 视图	**ospf** [*process-id* [[**router-id** *router-id*] **vpn-instance** *vpn-instance-name*]]
关闭 OSPF 路由协议进程	**undo ospf** [*process-id*]

缺省情况下，不运行 OSPF。

启用 OSPF 时，需要注意：

- 如果在启动 OSPF 时不指定进程号，将使用缺省的进程号 1；关闭 OSPF 时不指定进程号，缺省关闭进程 1。
- 在同一个区域中的进程号必须一致，否则会造成进程之间的隔离。
- 当在一台路由器上运行多个 OSPF 进程时，建议用户使用以上命令中的 **router-id** 为不同进程指定不同的 Router ID。
- 以上命令中的 **vpn-instance** 用于将 OSPF 进程与 VPN 实例进行绑定，用于 MPLS VPN 解决方案，详细介绍请参考本手册的“ VPN ”部分。

4.2.3 进入 OSPF 区域视图

OSPF 协议将自治系统划分成不同的区域（Area），在逻辑上将路由器分为不同的组。在区域视图下可以进行区域相关配置。

请在 OSPF 视图下进行下列配置。

表4-3 进入 OSPF 区域视图

操作	命令
进入 OSPF 区域视图	**area** *area-id*
删除指定的 OSPF 区域	**undo area** *area-id*

区域 ID 可以采用十进制整数或 IP 地址形式输入，但显示时使用 IP 地址形式。

在配置同一区域内的 OSPF 路由器时，应注意：大多数配置数据都应该对区域统一考虑，否则可能会导致相邻路由器之间无法交换信息，甚至导致路由信息的阻塞或者产生路由环。

4.2.4 在指定网段使能 OSPF

在系统视图下使用 **ospf** 命令启动 OSPF 后，还必须指定在哪个网段上应用 OSPF。

请在 OSPF 区域视图下进行下列配置。

表4-4 在指定网段使能 OSPF

操作	命令
指定网段运行 OSPF 协议	**network** *ip-address wildcard-mask*
取消网段运行 OSPF 协议	**undo network** *ip-address wildcard-mask*

一台路由器可能同时属于不同的区域（这样的路由器称作 ABR），但一个网段只能属于一个区域。

4.2.5 配置 OSPF 虚连接

OSPF 协议规定：所有非骨干区域必须与骨干区域保持连通，即 ABR 上至少有一个端口应在区域 0.0.0.0 中。如果一个区域与骨干区域 0.0.0.0 没有直接的物理连接，就必须建立虚连接来保持逻辑上的连通。

虚连接是在两台 ABR 之间，通过一个非骨干区域内部路由的区域而建立的一条逻辑上的连接通道。它的两端必须都是 ABR，并且必须在两端同时配置。虚连接由对端路由器的 Router ID 来标识。为虚连接提供非骨干区域内部路由的区域称为运输区域（Transit Area）。

虚连接在穿过转换区域的路由计算出来后被激活，相当于在两个端点之间形成一个点到点连接，这个连接与物理接口类似，可以配置接口的各参数，如 Hello 报文的发送间隔等。

虚连接的配置是在 Transit 区域进行的。

请在 OSPF 区域视图下进行下列配置。

表4-5 配置 OSPF 虚连接

操作	命令
创建并配置虚连接	**vlink-peer** *router-id* [**hello** *seconds*] [**retransmit** *seconds*] [**trans-delay** *seconds*] [**dead** *seconds*] [**simple** *password* | **md5** *keyid key*]
取消创建的虚连接	**undo vlink-peer** *router-id*

缺省情况下，**hello** 的值为 10 秒；**retransmit** 的值为 5 秒；**trans-delay** 的值为 1 秒；**dead** 的值为 40 秒。

将虚连接看做“逻辑通道”是因为：两个 ABR 之间的 OSPF 路由器只对报文进行透明转发（由于协议报文的目的地址不是这些路由器，所以这些报文对于他们而言

是透明的，只是当作普通的 IP 报文转发），两台 ABR 之间直接传递路由信息。这里的路由信息是指由 ABR 生成的 Type3 LSAs，区域内的路由器同步方式没有因此改变。

4.2.6 配置 OSPF 网络类型

OSPF 以本路由器邻接网络的拓扑结构为基础计算路由。每台路由器将自己邻接的网络拓扑描述出来，传递给所有其它的路由器。

根据链路层协议类型，OSPF 将网络分为四种类型：

- 广播类型：链路层协议是 Ethernet、FDDI。
- 非广播多路访问 Non Broadcast MultiAccess（NBMA）类型：链路层协议是帧中继、ATM、HDLC 或 X.25 时。
- 点到多点 Point-to-Multipoint（p2mp）类型：没有一种链路层协议会被缺省的认为是 Point-to-Multipoint 类型。点到多点必然是由其他网络类型强制更改的。常见的做法是将非全连通的 NBMA 改为点到多点的网络。
- 点到点 Point-to-point（p2p）类型：链路层协议是 PPP 或 LAPB。

NBMA 网络是指非广播、多点可达的网络，典型的有 ATM。可通过配置轮询间隔来指定路由器在与相邻路由器构成邻接关系之前发送轮询 Hello 报文的时间周期。

在没有多址访问能力的广播网上，可将接口配置成 **nbma** 方式。

若在 NBMA 网络中并非所有路由器之间都直接可达时，可将接口配置成 **p2mp** 方式。

若该路由器在 NBMA 网络中只有一个对端，则也可将接口类型改为 **p2p** 方式。

NBMA 与 **p2mp** 之间的区别：

- 在 OSPF 协议中 NBMA 是指那些全连通的、非广播、多点可达网络。而点到多点的网络，则并不需要一定是全连通的。
- 在 NBMA 上需要选举 DR 与 BDR，而在点到多点网络中没有 DR 与 BDR。
- NBMA 是一种缺省的网络类型，例如：如果链路层协议是 ATM，OSPF 会缺省的认为该接口的网络类型是 NBMA（不论该网络是否全连通）。点到多点不是缺省的网络类型，没有哪种链路层协议会被认为是点到多点，点到多点必须是由其它的网络类型强制更改的。最常见的做法是将非全连通的 NBMA 改为点到多点的网络。
- NBMA 用单播发送报文，需要手工配置邻居。点到多点采用多播方式发送报文。

请在接口视图下进行下列配置。

表4-6 配置 OSPF 接口的网络类型

操作	命令
配置接口的网络类型	**ospf network-type** { **broadcast** | **nbma** | **p2mp** | **p2p** }

缺省情况下，OSPF 根据链路层类型类型得出网络类型。如果用户为接口配置了新的网络类型，原接口的网络类型自动取消。

4.2.7 配置邻接点

对于接口类型为 NBMA 的网络，由于无法通过广播 Hello 报文的形式发现相邻路由器，必须手工为其指定相邻路由器的 IP 地址，并说明该相邻路由器是否有选举权。

请在 OSPF 视图下进行下列配置。

表4-7 配置邻接点

操作	命令
配置 NBMA 接口的邻接点	**peer** *ip-address* [**dr-priority** *dr-priority-number*]
取消配置 NBMA 接口的邻接点	**undo peer** *ip-address*

缺省情况下，NBMA 接口的邻接点优先级的取值为 1。

使用 **ospf dr-priority** 命令和使用 **peer** 命令设置的优先级具有不同的用途：

- **ospf dr-priority** 命令设置的优先级用于实际的 DR 选举；
- **peer** 命令设置的优先级用于表示邻居是否具有选举权。如果在配置邻居时将优先级指定为 0，则本地路由器认为该邻居不具备选举权，不向该邻居发送 Hello 报文，这种配置可以减少在 DR 和 BDR 选举过程中网络上的 Hello 报文数量。但如果本地路由器是 DR 或 BDR，它也会向优先级为 0 的邻居发送 Hello 报文，以建立邻接关系。

4.2.8 配置 OSPF 的路由引入

1. 引入其它协议的路由

路由器上各动态路由协议之间可以互相共享路由信息，由于 OSPF 的特性，其它的路由协议发现的路由总被当作自治系统外部的路由信息处理。在接收命令中，可以指定路由的花费类型、花费值和标记以覆盖缺省的路由接收参数（见“ 配置 OSPF 接收外部路由的默认选项 ”的配置部分）。

OSPF 使用 4 类不同的路由，按优先顺序排列如下：

- 区域内路由
- 区域间路由

- 第一类外部路由
- 第二类外部路由

区域内和区域间路由描述自治系统内部的网络结构；外部路由则描述了如何选择到自治系统以外目的地的路由。

第一类外部路由是指接收的是 IGP 路由（例如 RIP，STATIC），由于这类路由的可信程度较高，所以，计算出的外部路由的花费与自治系统内部的路由花费的数量级相同，并且与 OSPF 自身路由的花费具有可比性，即：到第一类外部路由的花费值＝本路由器到相应的 ASBR 的花费值＋ASBR 到该路由目的地址的花费值。

第二类外部路由是指接收的是 EGP 路由，由于这类路由的可信度比较低，所以 OSPF 协议认为，从 ASBR 到自治系统之外的花费远远大于在自治系统之内到达 ASBR 的花费，计算路由花费时主要考虑前者。即，到第二类外部路由的花费值＝ASBR 到该路由目的地址的花费值。如果该值相等，再考虑本路由器到相应的 ASBR 的花费值。

请在 OSPF 视图下进行下列配置。

表4-8 引入其它协议的路由

操作	命令
引入其它协议的路由信息	**import-route** *protocol* [**allow-ibgp]** [**cost** *value*] [**type** { **1** | **2** }] [**tag** *value*] [**route-policy** *route-policy-name*]
取消引入其它协议路由信息	**undo import-route** *protocol*

缺省情况下，OSPF 将不引入其它协议的路由信息。当配置引入其他协议的路由信息时，缺省情况下，cost 为 1，type 为 2，tag 为 1。

当 *protocol* 为 BGP 时，**allow-ibgp** 为可选关键字。**import-route bgp** 表示只引入 EBGP 路由，**import-route bgp allow-ibgp** 表示将 IBGP 路由也引入，该配置危险，请慎用！

可引入的路由包括 direct、static、RIP、IS-IS 与 BGP，也可以引入其它进程的 OSPF 路由。

2. 配置 OSPF 引入外部路由的参数

当 OSPF 将其它路由协议发现的路由信息引入到本自治系统中时，还需要配置一些额外的参数，如引入路由的缺省花费和缺省标记等。路由标记可以用来标识协议相关的信息，如 OSPF 接收 BGP 时用来区分自治系统的编号。

请在 OSPF 视图下进行下列配置。

表4-9 配置 OSPF 引入外部路由的参数

操作	命令
配置 OSPF 引入外部路由的最小时间间隔	**default interval** *seconds*
恢复引入外部路由最小时间间隔的缺省值	**undo default interval**
配置 OSPF 每次引入路由的数量上限	**default limit** *routes*
恢复每次引入外部路由数量上限的缺省值	**undo default limit**
配置 OSPF 在接收外部路由时缺省的花费值	**default cost** *value*
恢复 OSPF 在接收外部路由时花费的缺省值	**undo default cost**
配置 OSPF 在接收外部路由时缺省的标记值	**default tag** *tag*
恢复 OSPF 在接收外部路由时标记的缺省值	**undo default tag**
配置 OSPF 在接收外部路由时缺省的类型	**default type** { **1** | **2** }
恢复 OSPF 接收外部路由类型的缺省值	**undo default type**

缺省情况下，引入外部路由时的 cost 为 1，tag 为 1，路由的类型为 Type 2；引入外部路由的时间间隔为 1 秒；每次可引入的外部路由上限为 1000 条。

4.2.9 在 OSPF 中生成缺省路由

缺省情况下，普通的 OSPF 区域（骨干区域和非骨干区域）中是没有缺省路由的，**import-route** 命令也无法向 OSPF 路由域中引入缺省路由。

命令 **default-route-advertise** 可以在 OSPF 路由域中生成并发布缺省路由，使用这条命令时，需要了解以下几点：

- 在普通 OSPF 区域的 ASBR 或 ABR 上执行 **default-route-advertise** 命令，将生成一条 Type-5 LSA 向 OSPF 路由域内发布缺省路由；
- 在 NSSA 区域的 ASBR 或 ABR 上执行此命令，将生成一条 Type-7 LSA 向 NSSA 区域内发布缺省路由；
- 此命令对于 Stub 区域或完全 stub 区域无效；
- 缺省情况下，对于 ASBR，只有当路由表中已经存在一条缺省路由时，OSPF 才会生成相应的 Type-5 LSA 或 Type-7 LSA；
- 对于 ABR，不论路由表中是否已经存在缺省路由，都会生成 Type-5 LSA 或 Type-7 LSA。
- 发布缺省路由的 Type-5 LSA 或 Type-7 LSA 的扩散范围与普通的 Type-5 LSA 或 Type-7 LSA 相同。

请在 OSPF 视图下进行下列配置。

表4-10 在 OSPF 中生成缺省路由

操作	命令
在 OSPF 中生成缺省路由	**default-route-advertise** [**always**] [**cost** *value*] [**type** *value*] [**route-policy** *route-policy-name*]
取消生成的缺省路由	**undo default-route-advertise** [**always**] [**cost**] [**type**] [**route-policy**]

缺省情况下，OSPF 中没有缺省路由。

如果在生成缺省路由时使用了参数 **always**，则不论路由表中是否存在缺省路由，OSPF 都将生成一条 Type-5 或 Type-7 LSA。这个参数只对 ASBR 有效，应谨慎使用。

由于 OSPF 在进行 SPF 运算时不计算自己生成的 LSA，所以，本路由器上的 OSPF 路由中并不存在缺省路由。为保证路由信息的正确性，应只在那些与外部网络相连的路由器上配置引入缺省路由。

📖 说明：

在 OSPF 路由器上配置 **default-route-advertise** 命令后，这台路由器就成为 ASBR，这一点与在 OSPF 路由器上配置 **import-route** 命令的效果类似。

对于 NSSA 区域的 ABR 或 ASBR，**default-route-advertise** 命令的效果与 **nssa default-route-advertise** 相同。

4.2.10 配置 OSPF 的路由过滤

请在 OSPF 视图下进行下列配置。

1. 对引入的路由进行过滤

OSPF 接收到 LSAs 后，可以根据一定的过滤条件来决定是否将计算后得到的路由信息加入路由表中。

表4-11 配置 OSPF 对引入路由的过滤

操作	命令
配置对引入的全局路由信息进行过滤	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **gateway** *ip-prefix-name* } **import**
取消对引入的全局路由信息进行过滤	**undo filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **gateway** *ip-prefix-name* } **import**

2. 对发布的路由进行过滤

filter-policy export 配置 ASBR 路由器对引入到 OSPF 的外部路由进行过滤，实际上是对向外发布的引入路由的 LSA 进行过滤，该命令只对 ASBR 路由器有效。

表4-12 配置 OSPF 对发布路由的过滤

操作	命令
配置 OSPF 对向外发布的引入路由的 LSA 进行过滤	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*routing-protocol*]
取消 OSPF 对向外发布的引入路由的 LSA 进行过滤	**undo filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*routing-protocol*]

缺省情况下，OSPF 不对引入或发布的路由信息进行过滤。

📖 说明：

filter-policy import 命令只对从邻居收到的本进程 OSPF 路由进行过滤，没有通过过滤的路由将不被加入路由表。该命令只在 ABR 上有效。

filter-policy export 命令只对本机使用 **import-route** 引入的路由起作用。如果仅配置了 **filter-policy export**，而没有配置 **import-route** 命令引入其它外部路由（包括不同进程的 OSPF 路由），**filter-policy export** 不起作用。

如果在 **filter-policy export** 命令中没有指定对哪种类型的路由过滤，则对本机使用 **import-route** 引入的所有类型的路由有效。

4.2.11 配置 OSPF 的路由聚合

1. 配置 OSPF 区域路由聚合

路由聚合是指：具有相同前缀的路由信息，ABR 可以将它们聚合在一起，只发布一条路由到其它区域。一个区域可以配置多条聚合网段，这样 OSPF 可以对多个网段进行聚合。ABR 向其它区域发送路由信息时，以网段为单位生成 Sum_net_Lsa（Type 3 LSA）。如果该区域中存在一些连续的网段，则可以使用 **abr-summary** 命令将这些连续的网段聚合成一个网段。这样 ABR 只发送一条聚合后的 LSA，所有落入本命令指定的聚合网段范围的 LSA 将不再会被单独发送出去，这样可减少其它区域中 LSDB 的规模。

一旦将某一网络的聚合网段加入到区域中，该区域中所有落在这一聚合网段内的 IP 地址的内部路由都不再被独立地广播到别的区域，而只是广播整个聚合网段路由的摘要信息。如果该网段范围用关键字 **not-advertise** 限定，则到这一网段路由的摘要信息将不会被广播出去。这个网段由 IP 地址/掩码说明。

需要注意的是：路由聚合只有在 ABR 上配置才会有效。

请在 OSPF 区域视图下进行下列配置。

表4-13 配置 OSPF 区域路由聚合

操作	命令
配置 OSPF 区域路由聚合	**abr-summary** *ip-address mask* [**advertise** | **not-advertise**]
取消 OSPF 区域路由聚合	**undo abr-summary** *ip-address mask*

缺省情况下，区域边界路由器不对路由聚合。

2. 配置 OSPF 引入路由聚合

OSPF 支持对引入路由进行聚合。

请在 OSPF 视图下进行下列配置。

表4-14 配置 OSPF 引入路由聚合

操作	命令
配置 OSPF 引入路由聚合	**asbr-summary** *ip-address mask* [**not-advertise** | **tag** *value*]
取消 OSPF 引入路由聚合	**undo asbr-summary** *ip-address mask*

缺省情况下，不对引入路由进行聚合。当配置了路由聚合时，缺省情况下通告聚合路由，tag 值为 1。

配置引入路由聚合后，如果本地路由器是自治系统边界路由器 ASBR，将对引入的聚合地址范围内的 Type-5 LSA 进行聚合，当配置了 NSSA 区域时，还要对引入的聚合地址范围内的 Type-7 LSA 进行聚合。

如果本地路由器是区域边界路由器 ABR，且是 NSSA 区域的转换路由器，则对由 Type-7 LSA 转化成的 Type-5 LSA 进行聚合处理，对于不是 NSSA 区域转换路由器的则不进行聚合处理。

4.2.12 配置 OSPF 优先级

由于路由器上可能同时运行多个动态路由协议，就存在各个路由协议之间路由信息共享和选择的问题。系统为每一种路由协议设置一个优先级，在不同协议发现同一条路由时，优先级数值小的路由将被优选。

请在 OSPF 视图下进行下列配置。

表4-15 配置 OSPF 路由的优先级

操作	命令
配置 OSPF 协议在各路由协议之间的优先级	**preference** [**ase**] *preference*
恢复协议缺省优先级	**undo preference** [**ase**]

缺省情况下，OSPF 协议的优先级为 10；引入外部路由协议的优先级为 150。

4.2.13 配置 OSPF 定时器

1. 配置 Hello 报文发送时间间隔

Hello 报文是一种最常用的报文，它周期性地被发送至邻居路由器，用于发现与维持邻居关系、选举 DR 与 BDR。用户可对发送 Hello 报文的时间间隔 hello *seconds* 的值进行设置。

根据 RFC2328 的规定，要保持网络邻居间的 hello 时钟的时间间隔的一致性。需要注意的是，hello 时钟的值与路由收敛速度、网络负荷大小成反比。

请在接口视图下进行下列配置。

表4-16 设置 Hello 报文发送时间间隔

操作	命令
配置接口发送 hello 报文的时间间隔	**ospf timer hello** *seconds*
恢复接口发送 hello 报文时间间隔的缺省值	**undo ospf timer hello**
在 NBMA 接口上配置发送轮询报文的时间间隔	**ospf timer poll** *seconds*
恢复发送轮询报文间隔的缺省值	**undo ospf timer poll**

缺省情况下，**p2p**、**broadcast** 类型接口发送 Hello 报文的时间间隔的值为 10 秒；**p2mp**、**nbma** 类型接口发送 Hello 报文的时间间隔的值为 30 秒。

缺省情况下，发送轮询 Hello 报文的时间间隔为 120 秒。轮询时间间隔 **poll** *seconds* 值至少应为 **Hello** *seconds* 值的 3 倍。

2. 配置相邻路由器间失效时间

在一定时间间隔内，如果路由器未收到对方的 Hello 报文，则认为对端路由器失效，这个时间间隔被称为相邻路由器间的失效时间。

请在接口视图下进行下列配置。

表4-17 设置相邻路由器间失效时间

操作	命令
配置相邻路由器间失效时间	**ospf timer dead** *seconds*
恢复相邻路由器间失效时间的缺省值	**undo ospf timer dead**

缺省情况下，**p2p**、**broadcast** 类型接口相邻路由器间失效时间的值为 40 秒；**p2mp**、**nbma** 类型接口相邻路由器间失效时间的值为 120 秒。

需要注意的是：在用户修改了网络类型后，hello *seconds* 与 dead *seconds* 都将恢复缺省值。

3. 配置邻接路由器重传 LSA 的间隔

当一台路由器向它的邻居发送一条 LSA 后，需要等到对方的确认报文。若在 retransmit 时间内没有收到对方的确认报文，就会向邻居重传这条 LSA。用户可对 retransmit 的值进行设置。

请在接口视图下进行下列配置。

表4-18 设置邻接路由器重传 LSA 的间隔

操作	命令
配置相邻路由器重传 LSA 的时间间隔	**ospf timer retransmit** *interval*
恢复相邻路由器重传 LSA 的时间间隔缺省值	**undo ospf timer retransmit**

缺省情况下，相邻路由器重传 LSA 的时间间隔的值为 5 秒。

interval 的值必须大于一个报文在两台路由器之间传送一个来回的时间。

需要注意的是：相邻路由器重传 LSA 时间间隔的值不要设置得太小，否则将会引起不必要的重传。

4.2.14 配置选举 DR 时的优先级

广播网络或 NBMA 类型的网络需要选举指定路由器 DR（Designated Router）和备份指定路由器 BDR（Backup Designated Router）。

路由器接口的优先级 Priority 将影响接口在选举 DR 时所具有的资格。优先级为 0 的路由器不会被选举为 DR 或 BDR。

DR 由本网段中所有路由器共同选举。Priority 大于 0 的路由器都可作为“候选者”，选票就是 Hello 报文，OSPF 路由器将自己选出的 DR 写入 Hello 报文中，发给网段上的其它路由器。当同一网段的两台路由器都宣布自己是 DR 时，Priority 高的胜出。如果 Priority 相等，则 Router ID 大的胜出。

如果 DR 失效，则网络中的路由器必须重新选举 DR，并与新的 DR 同步，为了缩短这个过程，OSPF 提出了 BDR（Backup Designated Router，备份指定路由器）的概念，与 DR 同时被选举出来。BDR 也与本网段内的所有路由器建立邻接关系并交换路由信息。DR 失效后，BDR 立即成为 DR，由于不需要重新选举，并且邻接关系已经建立，所以这个过程可以很快完成。这时，还需要选举出一个新的 BDR，这时不会影响路由的计算。

需要说明的是：

- 当接口优先级为 0 时，无论什么情况下都不能成为 DR/BDR，这可能造成网络上没有 DR 或 BDR。
- DR 并不一定是网段中 Priority 最大的路由器；同理，BDR 也并不一定就是 Priority 第二大的路由器。若 DR、BDR 已经选择完毕，即使有一台 Priority 值更大的路由器加入，它也不会成为该网段中的 DR。
- DR 是网段中的概念，是针对路由器的接口而言的。某台路由器在一个接口上可能是 DR，在另一个接口上可能是 BDR，或者是 DROther。
- 只有在广播或 NBMA 类型的接口时才会选举 DR，在点到点或点到多点类型的接口上不需要选举 DR。在广播网络或 NBMA 网络上，如果 OSPF 收到的 hello 报文中没有人宣称自己是 DR，则将进入选举过程；如果多个 OSPF 宣称自己是 DR/BDR，也将进入选举过程；如果已经有人宣称自己是 DR/BDR，则新加入者接受已有的 DR/BDR，无论它的优先级是多少；当 DR 失败时，BDR 将变为 DR，再选举出新的 BDR。

请在接口视图下进行下列配置。

表4-19 设置接口在选举 DR 时的优先级

操作	命令
设置接口在选举“指定路由器”时的优先级	**ospf dr-priority** *priority_num*
恢复接口的缺省优先级	**undo ospf dr-priority**

缺省情况下，接口在选举 DR 时的优先级为 1，取值范围为 0～255。

4.2.15 配置接口发送报文的开销

用户可以在不同接口上配置发送报文的开销，从而影响路由的计算。

请在接口视图下进行下列配置。

表4-20 设置接口发送报文的开销

操作	命令
设置接口发送报文的开销	**ospf cost** *value*
将接口发送报文的开销恢复为缺省值	**undo ospf cost**

缺省情况下，OSPF 根据接口的速率自动计算发送报文的开销。

4.2.16 配置 OSPF 的 SPF 计算间隔

当 OSPF 的链路状态数据库 LSDB 发生改变时，需要重新计算最短路径，如果每次改变都立即计算最短路径，将占用大量资源，并会影响路由器的效率，通过调节 SPF（Shortest Path First）的计算间隔时间，可以抑制由于网络频繁变化带来的占用过多资源。

请在 OSPF 视图下进行下列配置。

表4-21 设置 SPF 计算间隔

操作	命令
设置 SPF 计算间隔	**spf-schedule-interval** *seconds*
恢复 SPF 计算间隔	**undo spf-schedule-interval**

缺省情况下，SPF 时间间隔为 5 秒钟。

4.2.17 配置发送链路状态更新报文所需时间

链路状态更新报文（LSU）中链路状态广播（LSA）的老化时间在传送之前要增加 trans-delay 秒。该参数的设置主要考虑到接口上发送报文所需的时间，在低速网络上，该项配置尤为重要。

请在接口视图下进行下列配置。

表4-22 配置发送 LSU 报文所需时间

操作	命令
配置用于发送 LSU 报文的时钟间隔	**ospf trans-delay** *seconds*
恢复发送 LSU 报文的时钟间隔的缺省值	**undo ospf trans-delay**

缺省情况下，发送链路状态更新报文时间的值为 1 秒。

4.2.18 配置接口发送 DD 报文时是否填 MTU 值

运行 OSPF 协议的路由器在进行数据库同步时，使用 DD（Database Description）报文描述自己的 LSDB。

用户可以使用本命令手工设定指定接口在发送时填写 DD 报文中的 MTU 值域，设定的 MTU 值是接口的实际 MTU 值。

请在接口视图下进行下列配置。

表4-23 配置接口发送 DD 报文时是否填 MTU 值

操作	命令
使能接口发送 DD 报文时填 MTU 值	**ospf mtu-enable**
禁止接口发送 DD 报文时填 MTU 值	**undo ospf mtu-enable**

缺省情况下，接口发送 DD 报文时不填 MTU 值，即 DD 报文中的 MTU 值为 0。

4.2.19 配置 OSPF 等值路由的最大个数

请在 OSPF 视图下进行下面配置。

表4-24 配置 OSPF 等值路由的最大个数

操作	命令
配置 OSPF 等值路由的最大个数	**multi-path-number** *number*
恢复 OSPF 等值路由最大个数的缺省值。	**undo multi-path-number**

缺省情况下，OSPF 等值路由最大个数为 3。

4.2.20 配置 OSPF 认证

1. 配置 OSPF 区域支持报文验证

在 OSPF 中，一个区域中所有的路由器的验证类型必须一致（不要求验证、要求明文验证或者要求 MD5 密文验证），但每条链路上的密码可以是不同的。用 **authentication-mode simple** 为该区域的配置明文验证口令；用 **authentication-mode md5** 为该区域配置 MD5 密文验证字口令。

请在 OSPF 区域视图下进行下列配置。

表4-25 配置 OSPF 区域要求报文验证

操作	命令
配置区域要求报文验证	**authentication-mode** { **simple** | **md5** }
配置区域不要求报文验证	**undo authentication-mode**

缺省情况下，区域不要求报文验证。

2. 配置 OSPF 报文的认证

OSPF 支持在相邻路由器之间支持明文验证（simple）或 MD5 密文验证。

请在接口视图下进行下列配置。

表4-26 配置 OSPF 报文的认证

操作	命令
配置接口接收使用报文明文验证字	**ospf authentication-mode simple** *password*
取消接口使用报文明文验证口令	**undo ospf authentication-mode simple**
配置接口使用报文 MD5 密文验证字	**ospf authentication-mode md5** *key_id key*
取消接口使用报文 MD5 密文验证	**undo ospf authentication-mode md5**

缺省情况下，接口未配置任何明文或 MD5 验证字。

4.2.21 配置接口的工作状态

如果要使 OSPF 路由信息不被某一网络中的路由器获得，可禁止在相应接口上发送 OSPF 报文。

不同的进程可以对同一接口禁止发送 OSPF 报文，但 **silent-interface** 命令只对本进程已经使能的 OSPF 接口起作用，不对其它进程的接口起作用。

请在 OSPF 视图下进行下列配置。

表4-27 禁止/允许接口发送 OSPF 报文

操作	命令
禁止接口发送 OSPF 报文	**silient-interface** *interface-type interface-number*
允许接口发送 OSPF 报文	**undo silent-interface** *interface-type interface-number*

缺省情况下，允许所有接口收发 OSPF 报文。

将运行 OSPF 协议的接口指定为 Silent 状态后，该接口的直连路由仍可以发布出去，但接口的 OSPF 呼叫报文将被阻塞，接口上无法建立邻居关系。这样可以增强 OSPF 的组网适应能力，减少系统资源的消耗。

4.2.22 配置 OSPF 的 STUB 区域

Stub 区域是一类特殊的 OSPF 区域，这类区域不接收或扩散 Type-5 的 LSA（AS-external-LSAs），对于产生大量 Type-5 LSA 的网络，这种处理方式能够有效减小 Stub 区域内路由器的 LSDB 尺寸，并缓解 SPF 计算对路由器资源的占用。通常情况下，Stub 区域位于自治系统边界。

为保证 Stub 区域去往自治系统外的报文能被正确转发，Stub 区域的 ABR 将通过 Summary-LSA 向本区域内发布一条缺省路由，并且只在本区域扩散。

🕮 说明：

ABR 通过 Summary-LSA（Type-3 LSA）向区域内发布的缺省路由是区域间缺省路由。

配置 Stub 区域的需要注意下列几点：

- 骨干区域不能配置成 Stub 区域。
- Stub 区域不能用作传输区域，即，虚连接不能穿过 Stub 区域。
- 如果想将一个区域配置成 Stub 区域，则该区域中的所有路由器必须都要配置该属性。
- Stub 区域内不能存在 ASBR，即自治系统外部的路由不能在本区域内传播。

请在 OSPF 区域视图下进行下列配置。

表4-28 配置 OSPF 的 Stub 区域

操作	命令
配置一个区域为 Stub 区域	**stub** [**no-summary**]
取消配置的 Stub 区域	**undo stub**
配置发送到 Stub 区域缺省路由的花费值	**default-cost** *value*
取消发送到 Stub 区域缺省路由的花费值	**undo default-cost**

缺省情况下，不配置 Stub 区域；发送到 Stub 区域缺省路由的花费值为 1。

需要注意的是：参数 **no-summary** 只能在 ABR 上配置，如果在配置 Stub 区域的 ABR 时使用了这一参数，则此 ABR 只向区域内发布一条缺省路由的 Summary-LSA，不生成任何其它 Summary-LSAs。这种既没有 AS-external-LSAs，也没有 Summary-LSAs 的 Stub 区域，又称为完全 stub 区域。

参数 **default-cost** 用于 Stub 区域的 ABR，配置 ABR 发送到 Stub 区域的缺省路由的花费值。

4.2.23 配置 OSPF 的 NSSA 区域

从前一节的描述中我们可以了解到，Stub 区域中没有任何 AS 外部路由信息，通过缺省路由保证到外部目的地的可达性。为了在保持 Stub 区域优点的同时提高组网的灵活性，RFC1587（OSPF NSSA Option）定义了一种新的区域类型：NSSA 区域（Not-So-Stubby Area），这种区域能够以受限方式引入 AS 外部路由。

NSSA 实际是 Stub 区域的扩展，它与 Stub 区域有许多相似之处。配置 NSSA 区域时，也需要注意：

- 骨干区域不能配置成 NSSA 区域；

- NSSA 区域不能用作传输区域，即，虚连接不能穿过 NSSA 区域；
- 如果要将一个区域配置成 NSSA 区域，则该区域中的所有路由器都必须配置此属性；

与 Stub 区域的一个不同是：NSSA 区域内可以存在 ASBR。

NSSA 区域中的 AS 外部路由信息使用一类新的 LSA：Type-7 LSA。Type-7 LSA 与 Type-5 LSA 非常相似，它们的区别在本章“ 4.1.5 OSPF 的 LSA 类型 ”已经介绍过。

下面以图 4-3为例，介绍 AS 外部路由信息在 NSSA 区域的传播情况。图 4-3中，运行 OSPF 进程 100 的自治系统包括 3 个区域：区域 0 是骨干区域，区域 1 是普通的 OSPF 非骨干区域，区域 2 是 NSSA 区域。

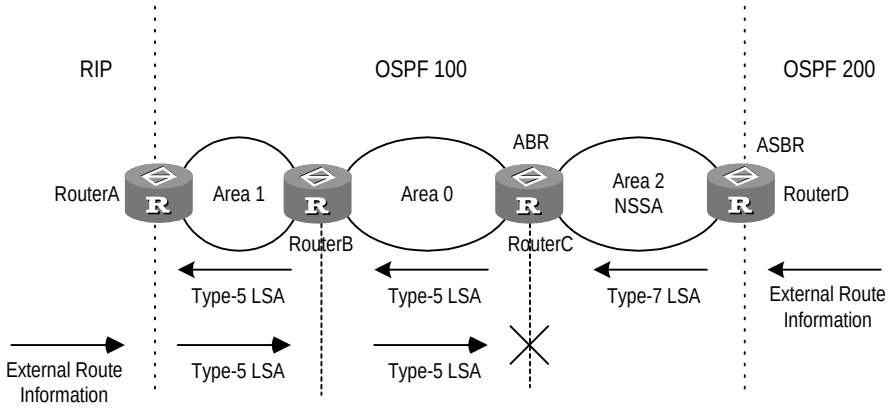


图4-3 NSSA 区域

区域 2 的 NSSA ASBR 引入 AS 外部路由信息（OSPF 进程 200 的路由信息）后，生成 Type-7 LSA 发布到区域 2 内传播，当 Type-7 LSA 到达 NSSA ABR 后，由 ABR 转换成 Type-5 LSA 传播到整个自治系统。区域 1 的 ASBR 引入 AS 外部路由信息（RIP 路由信息）后，产生 Type-5 LSA 在 OSPF 自治系统中传播，但由于区域 2 是 NSSA 区域，所以 RIP 路由信息不会到达区域 2。

请在 OSPF 区域视图下进行下列配置。

表4-29 配置 OSPF 的 NSSA 区域参数

操作	命令
配置一个区域为 NSSA 区域	**nssa** [**default-route-advertise**] [**no-import-route**] [**no-summary**]
取消配置的 NSSA 区域	**undo nssa**
配置发送到 NSSA 区域缺省路由的花费值	**default-cost** *cost*
恢复发送到 NSSA 区域缺省路由的花费缺省值	**undo default-cost**

缺省情况下，不配置 NSSA 区域；发送到 NSSA 区域缺省路由的花费值为 1。

对于 OSPF 自治系统的 ASBR，如果它也是 NSSA 区域的 ABR，通常不需要将同样的外部路由信息以 Type-5 和 Type-7 LSAs 引入两次，这种情况下，可以使用参数 **no-import-route**，禁止将 AS 外部路由以 Type-7 LSA 的方式发布到 NSSA 区域。

由于 NSSA 区域获得的 AS 外部路由信息是受限的，因此，NSSA 区域的 ABR 需要通过 Type-7 LSA 向本区域内发布一条缺省路由，保证去往自治系统外的报文能被正确转发，需要注意的是：NSSA 区域的 ABR 发布的缺省路由信息不会转换成 Type-5 LSA，而 NSSA 区域内的 ASBR 发布的缺省路由信息则可以转换成 Type-5 LSA。

参数 **default-route-advertise** 用来产生发布缺省路由的 Type-7 LSA，这个参数只能用于 NSSA 的 ASBR 或 ABR：

- 在 NSSA 的 ABR 上配置时，不论系统的路由表中是否存在缺省路由 0.0.0.0，都会产生 Type-7 LSA 缺省路由；
- 在 NSSA 的 ASBR 上配置时，只有当路由表中存在缺省路由 0.0.0.0，才会产生 Type-7 LSA 缺省路由。

参数 **no-summary** 的用法与在 Stub 区域的配置相同，只能在 NSSA 区域的 ABR 配置。使用此参数后，NSSA ABR 只通过 Type-3 的 Summary-LSA 向区域内发布一条缺省路由，不再向区域内发布任何其它 Summary-LSAs，这种区域又称为 NSSA 完全 stub 区域。

📖 说明：

参数 **default-route-advertise** 通过生成 Type-7 LSA 向 NSSA 区域内发布的缺省路由是自治系统外部缺省路由；

参数 **no-summary** 通过 Type-3 LSA 向 NSSA 完全 stub 区域发布的缺省路由是区域间缺省路由。

参数 **default-cost** 用于 NSSA 区域的 ABR，配置 ABR 发送到 NSSA 区域的缺省路由的花费值。

4.2.24 使能 OSPF 的 Opaque 能力

要实现 OSPF TE，必须先使能 OSPF 的 Opaque 能力。

请在 OSPF 视图下进行下列配置。

表4-30 使能 OSPF 的 Opaque 能力

操作	命令
使能 OSPF 的 Opaque 能力	**opaque-capability enable**
禁止 OSPF 的 Opaque 能力	**undo opaque-capability**

⚠ 注意：

若某个区域已经使能了 OSPF TE，则“ **undo opaque-capability** ”命令会执行失败。

4.2.25 配置 OSPF 与网管系统的配合

1. 配置 OSPF MIB 绑定

当启动了多个 OSPF 进程时，可以配置 OSPF MIB 对哪个进程进行处理，即绑定在哪个进程。

请在系统视图下进行下列配置。

表4-31 配置 OSPF MIB 绑定

操作	命令
配置 OSPF MIB 绑定	**ospf mib-binding** *process-id*
取消缺省的 OSPF MIB 绑定	**undo ospf mib-binding**

缺省情况下，MIB 绑定在第一个启动的 OSPF 进程上。

2. 配置 OSPF TRAP 功能

可以配置 OSPF 发送多种 SNMP TRAP 报文，并可以通过进程号指定某个 OSPF 进程发送 SNMP TRAP 报文。

请在系统视图下进行下列配置。

表4-32 配置 OSPF TRAP 功能

操作	命令
使能 OSPF 的 TRAP 功能	**snmp-agent trap enable ospf** [*process-id*] [**ifstatechange** | **virifstatechange** | **nbrstatechange** | **virnbrstatechange** | **ifcfgerror** | **virifcfgerror** | **ifauthfail** | **virifauthfail** | **ifrxbadpkt** | **virifrxbadpkt** | **txretransmit** | **viriftxretransmit** | **originatelsa** | **maxagelsa** | **lsdboverflow** | **lsdbapproachoverflow**]
取消 OSPF 的 TRAP 功能	**undo snmp-agent trap enable ospf** [*process-id*] [**ifstatechange** | **virifstatechange** | **nbrstatechange** | **virnbrstatechange** | **ifcfgerror** | **virifcfgerror** | **ifauthfail** | **virifauthfail** | **ifrxbadpkt** | **virifrxbadpkt** | **txretransmit** | **viriftxretransmit** | **originatelsa** | **maxagelsa** | **lsdboverflow** | **lsdbapproachoverflow**]

缺省情况下，OSPF 的 TRAP 功能是禁止的，即，OSPF 进程不发送 TRAP 报文。如果配置时不指定进程号，将对所有 OSPF 进程生效。

关于 SNMP TRAP 的详细配置，请参考本手册的“ 系统管理 ”部分。

4.2.26 重启 OSPF

如果对路由器先执行 **undo ospf**，再执行 **ospf** 来重启 OSPF 进程，路由器上原来的 OSPF 配置会丢失。而使用 **reset ospf all** 命令，可以在不丢失原有 OSPF 配置的前提下重启 OSPF。

请在用户视图下进行下列配置。

表4-33 配置重启 OSPF 进程

操作	命令
重启 OSPF 进程	**reset ospf** [**statistics**] { **all** | *process-id* }

重启路由器的 OSPF 进程，可以立即清除无效的 LSA、使改变的 Router ID 立即生效、或者进行 DR、BDR 的重新选举。

如果不指定 OSPF 进程号，将重启所有 OSPF 进程。

4.3 OSPF 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 OSPF 的运行情况，用户可以通过查看显示信息验证配置的效果。

在用户视图下执行 **debugging** 命令可对 OSPF 进行调试。

表4-34 OSPF 显示和调试

操作	命令
查看 OSPF 路由过程的信息	**display ospf brief**
查看 OSPF 统计信息	**display ospf cumulative**
查看 OSPF 的 LSDB 信息	**display ospf lsdb** [**brief** | **asbr** | **ase** | **network** | **nssa** | **opaque** { **area-local** | **as** | **link-local** } | **router** | **summary**] [*ip-address*] [**originate-router** *ip-address*] [**self-originate**]
查看 OSPF 邻接点信息	**display ospf peer** [**brief**]
查看 OSPF 下一跳信息	**display ospf nexthop**
查看 OSPF 路由表信息	**display ospf routing**
查看 OSPF 虚连接信息	**display ospf vlink**
查看 OSPF 请求列表	**display ospf request-queue**
查看 OSPF 重传列表	**display ospf retrans-queue**
查看 OSPF 到 ABR 及 ASBR 的路由信息	**display ospf abr-asbr**
查看 OSPF 接口信息	**display ospf interface**

操作	命令
查看 OSPF 错误信息	**display ospf error**
查看 OSPF 的调试信息开关状态	**display debugging ospf**
打开该 OSPF 进程下的邻接状态变化的输出开关（OSPF 视图）	**log-peer-change**
关闭该 OSPF 进程下的邻接状态变化的输出开关（OSPF 视图）	**undo log-peer-change**
打开 OSPF 报文调试信息开关	**debugging ospf packet** [**ack** | **dd** | **hello** | **interface** *type num* | **request** | **update**]
关闭 OSPF 报文调试信息开关	**undo debugging ospf packet** [**ack** | **dd** | **hello** **interface** *type num* | **request** | **update**]
打开 OSPF 事件调试信息	**debugging ospf event**
关闭 OSPF 事件调试信息	**undo debugging ospf event**
打开 OSPF LSA 报文调试信息开关	**debugging ospf lsa**
关闭 OSPF LSA 报文调试信息开关	**undo debugging ospf lsa**
打开 OSPF 的 SPF 调试信息开关	**debugging ospf spf**
关闭 OSPF 的 SPF 调试信息开关	**undo debugging ospf spf**

4.4 OSPF 典型配置举例

⚠ 注意：

在配置用例中，只列出了与 OSPF 配置相关的命令。

4.4.1 OSPF 典型配置举例

1. 组网需求

RouterA 与 RouterB 通过串口相连，RouterB 与 RouterC 通过以太网口相连属于；RouterA 属于 area0，RouterC 属于 area1，RouterB 同时属于 area0 和 area1。

2. 组网图

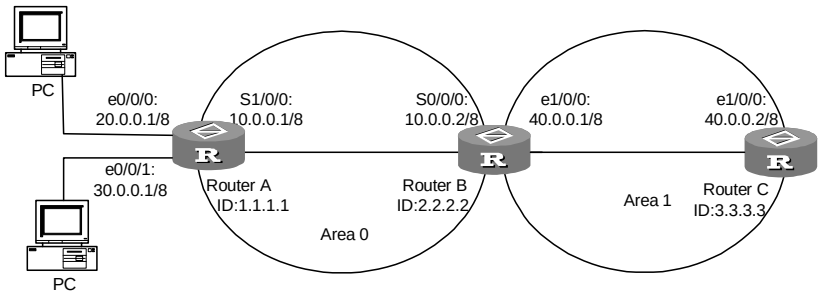


图4-4 OSPF 典型配置举例

3. 配置步骤

(1) 配置 RouterA

```
[RouterA] router id 1.1.1.1
[RouterA] interface serial1/0/0
[RouterA-serial1/0/0] ip address 10.0.0.1 255.0.0.0
[RouterA-serial1/0/0] interface ethernet0/0/0
[RouterA-ethernet 0/0/0] ip address 20.0.0.1 255.0.0.0
[RouterA- ethernet 0/0/0] interface ethernet0/0/1
[RouterA- ethernet 0/0/1] ip address 30.0.0.1 255.0.0.0
[RouterA- ethernet 0/0/1] quit
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 10.0.0.1 0.255.255.255
[RouterA-ospf-1 -area-0.0.0.0] network 20.0.0.1 0.255.255.255
[RouterA-ospf-1 -area-0.0.0.0] network 30.0.0.1 0.255.255.255
```

(2) 配置 RouterB

```
[RouterB] router id 2.2.2.2
[RouterB] internet serial0/0/0
[RouterB-serial0/0/0] ip address 10.0.0.2 255.0.0.0
[RouterB-serial0/0/0] interface ethernet 1/0/0
[RouterB-ethernet 1/0/0] ip address 40.0.0.1 255.0.0.0
[RouterB-ethernet 1/0/0] quit
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 10.0.0.2  0.255.255.255
[RouterB-ospf-1-area-0.0.0.0] area 1
[RouterB-ospf-1-area-0.0.0.1] network 40.0.0.1  0.255.255.255
```

(3) 配置 RouterC

```
[RouterC] router id 3.3.3.3
[RouterC] interface ethernet 1/0/0
```

```
[RouterC-ethernet 1/0/0] ip address 40.0.0.2 255.0.0.0
[RouterC-ethernet 1/0/0] quit
[RouterC] ospf
[RouterC-ospf-1] area 1
[RouterC-ospf-1-area-0.0.0.1] network 40.0.0.2  0.255.255.255
```

在路由器 A 与 C 上执行 **display ip routing-table**，发现二者通过 OSPF 获得了到对方的路由（即都有 20.0.0.0/8，30.0.0.0/8，40.0.0.0/8 网段的路由）。

4.4.2 配置 OSPF 多进程

1. 组网需求

在 Router A 的接口 Ethernet1/0/0 上启动 OSPF 进程 100，接口位于区域 0。

在 Router B 的接口 Ethernet1/0/0 上启动 OSPF 进程 100，接口 Ethernet2/0/0 上启动 OSPF 进程 200，分别处于相应进程的区域 0。

在 Router C 的接口 Ethernet2/0/0 上启动 OSPF 进程 200，处于区域 0。

Router A 和 Router B 之间可以建立邻居关系，Router B 和 Router C 之间可以建立邻居关系。

2. 组网图

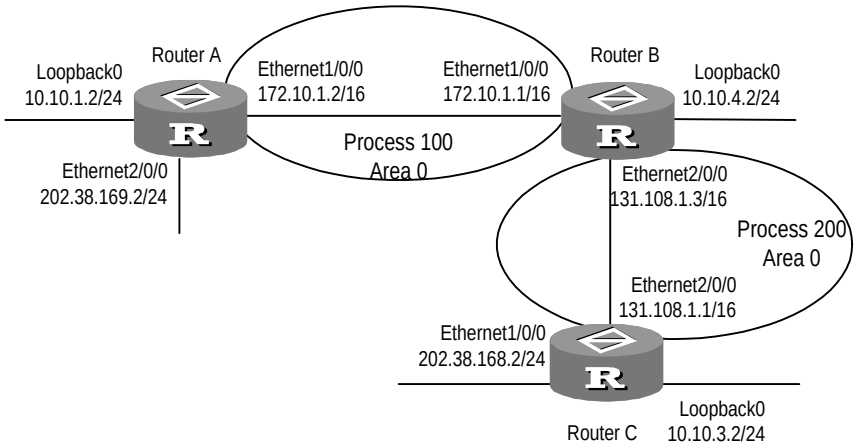


图4-5 OSPF 多进程组网图

3. 配置步骤

(1) 配置 Router A

```
[Router A] interface ethernet 1/0/0
[Router A-Ethernet1/0/0] ip address 172.10.1.2 255.255.0.0
[Router A-Ethernet1/0/0] quit
[Router A] router id 10.10.1.2
[Router A] ospf 100
[Router A-ospf-100] area 0
```

```
[Router A-ospf-100-area-0.0.0.0] network 172.10.0.0 0.0.255.255
```

(2) 配置 Router B

```
[Router B] interface ethernet 1/0/0
[Router B-Ethernet1/0/0] ip address 172.10.1.1 255.255.0.0
[Router B-Ethernet1/0/0] quit
[Router B] interface ethernet 2/0/0
[Router B-Ethernet2/0/0] ip address 131.108.1.3 255.255.0.0
[Router B-Ethernet2/0/0] quit
[Router B] ospf 100 router-id 10.10.2.2
[Router B-ospf-100] area 0
[Router B-ospf-100-area-0.0.0.0] network 172.10.0.0 0.0.255.255
[Router B-ospf-100] quit
[Router B] ospf 200 router-id 10.10.4.2
[Router B-ospf-200] area 0
[Router B-ospf-200-area-0.0.0.0] network 131.108.0.0 0.0.255.255
```

(3) 配置 Router C

```
[Router C] interface ethernet 2/0/0
[Router C-Ethernet2/0/0] ip address 131.108.1.1 255.255.0.0
[Router C-Ethernet2/0/0] quit
[Router C] router id 10.10.3.2
[Router C] ospf 200
[Router C-ospf-200] area 0
[Router C-ospf-200-area-0.0.0.0] network 131.108.0.0 0.0.255.255
```

在 Router B 上使用 **display ospf peer** 命令查看邻居的建立情况，可以看到 Router B 与 Router A 在 OSPF 进程 100 中建立邻居关系，Router B 与 Router C 在 OSPF 进程 200 中建立邻居关系，Router A 和 Router C 不能通过 OSPF 学到对方的路由。

4.4.3 配置 OSPF 优先级的“ DR ”选择

1. 组网需求

在下图中，路由器 A 的优先级为 100，它是网络上的最高优先级，所以路由器 A 被选为 DR；路由器 C 的优先级第二高，被选为 BDR；路由器 B 的优先级为 0，这意味着它将无法成为 DR；路由器 D 没有配置优先级，取缺省值 1。

2. 组网图

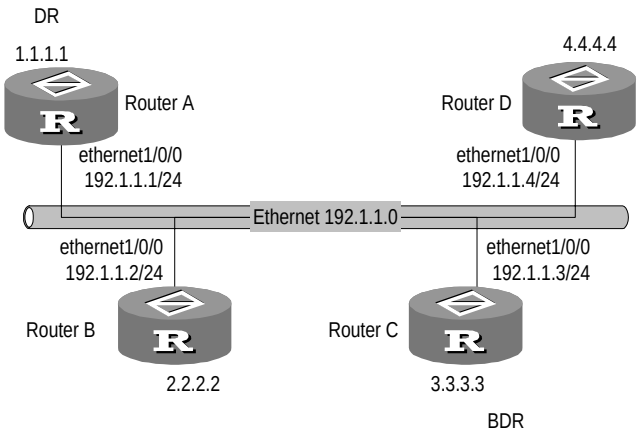


图4-6 配置 OSPF 优先级的“ DR ”选择组网图

3. 配置步骤

配置路由器 A：

```
[Router A] interface ethernet 1/0/0
[Router A-Ethernet1/0/0] ip address 192.1.1.1 255.255.255.0
[Router A-Ethernet1/0/0] ospf dr-priority 100
[Router A-Ethernet1/0/0] quit
[Router A] router id 1.1.1.1
[Router A] ospf
[Router A-ospf-1] area 0
[Router A-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
```

配置路由器 B：

```
[Router B] interface ethernet 1/0/0
[Router B-Ethernet1/0/0] ip address 192.1.1.2 255.255.255.0
[Router B-Ethernet1/0/0] ospf dr-priority 0
[Router B-Ethernet1/0/0] quit
[Router B] router id 2.2.2.2
[Router B] ospf
[Router B-ospf-1] area 0
[Router B-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
```

配置路由器 C：

```
[Router C] interface ethernet 1/0/0
[Router C-Ethernet1/0/0] ip address 192.1.1.3 255.255.255.0
[Router C-Ethernet1/0/0] ospf dr-priority 2
[Router C-Ethernet1/0/0] quit
[Router C] router id 3.3.3.3
[Router C] ospf
```

```
[Router B-ospf-1] area 0
[Router B-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
```

配置路由器 D：

```
[Router D] interface ethernet 1/0/0
[Router D-Ethernet1/0/0] ip address 192.1.1.4 255.255.255.0
[Router D-Ethernet1/0/0] quit
[Router D] router id 4.4.4.4
[Router D] ospf
[Router B-ospf-1] area 0
[Router B-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
```

在路由器 A 上运行 **display ospf peer** 来显示 OSPF 邻居，注意路由器 A 有三个邻居。

每个邻居的状态都是 full，这意味着路由器 A 与它的每个邻居都形成了邻接（路由器 A 和 C 必须与网络中的所有路由器形成邻接，才能分别充当网络的 DR 和 BDR）。路由器 A 是网络中的 DR，而路由器 C 是 BDR。其它所有的邻居都是 DRother（这意味着它们既不是 DR，也不是 BDR）。

将路由器 B 的优先级改为 200：

```
[Router B-Ethernet1/0/0] ospf dr-priority 200
```

在路由器 A 上运行 **display ospf peer** 来显示 OSPF 邻居，注意路由器 B 的优先级变为 200；但它并不是 DR。

只有当现在的 DR 不在网络上了后，DR 才会改变。关掉路由器 A，在路由器 D 上运行 **display ospf peer** 命令可显示邻居，注意本来是 BDR 的路由器 C 成为了 DR，并且路由器 B 现在也是 BDR。

关掉所有的路由器再重新启动，这个操作会带来一个新的 DR/BDR 选择。路由器 B 就被选为 DR（优先级为 200），路由器 A 成为了 BDR（优先级为 100）。

4.4.4 配置 OSPF 虚链路

1. 组网需求

在下图中，区域 2 没有与区域 0 直接相连。区域 1 被用作运输区域（Transit Area）来连接区域 2 和区域 0。路由器 B 和路由器 C 之间配置一条虚链路。

2. 组网图

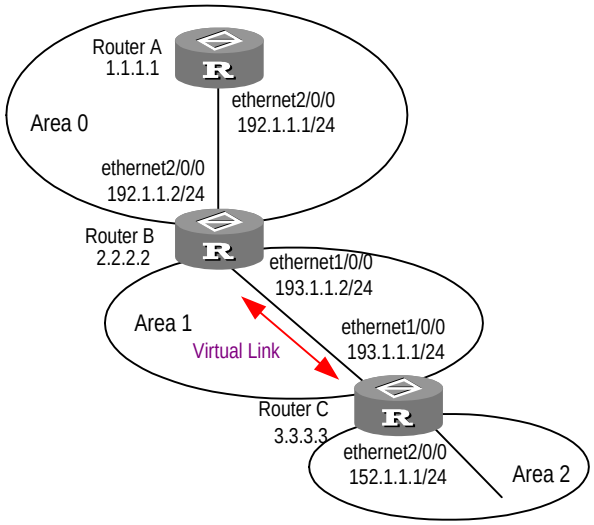


图4-7 配置 OSPF 虚链路的组网图

3. 配置步骤

配置路由器 Router A：

```
[Router A] interface ethernet 2/0/0
[Router A-Ethernet2/0/0] ip address 192.1.1.1 255.255.255.0
[Router A-Ethernet2/0/0] quit
[Router A] router id 1.1.1.1
[Router A] ospf
[Router A-ospf-1] area 0
[Router A-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
```

配置路由器 Router B：

```
[Router B] interface ethernet 2/0/0
[Router B-Ethernet2/0/0] ip address 192.1.1.2 255.255.255.0
[Router B-Ethernet2/0/0] interface ethernet 1/0/0
[Router B-Ethernet1/0/0] ip address 193.1.1.2 255.255.255.0
[Router B-Ethernet1/0/0] quit
[Router B] router id 2.2.2.2
[Router B] ospf
[Router B-ospf-1] area 0
[Router B-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[Router B-ospf-1-area-0.0.0.0] quit
[Router B-ospf-1] area 1
[Router B-ospf-1-area-0.0.0.1] network 193.1.1.0 0.0.0.255
[Router B-ospf-1-area-0.0.0.1] vlink-peer 3.3.3.3
```

配置路由器 Router C：

```
[Router C] interface ethernet 2/0/0
[Router C-Ethernet2/0/0] ip address 152.1.1.1 255.255.255.0
[Router C-Ethernet2/0/0] interface ethernet 1/0/0
[Router C-Ethernet1/0/0] ip address 193.1.1.1 255.255.255.0
[Router C-Ethernet1/0/0] quit
[Router C] router id 3.3.3.3
[Router C] ospf
[Router C-ospf-1] area 1
[Router C-ospf-1-area-0.0.0.1] network 193.1.1.0 0.0.0.255
[Router C-ospf-1-area-0.0.0.1] vlink-peer 2.2.2.2
[Router C-ospf-1-area-0.0.0.1] quit
[Router C-ospf-1] area 2
[Router C –ospf-1-area-0.0.0.2] network 152.1.1.0 0.0.0.255
```

4.4.5 配置 OSPF 邻居认证

1. 组网需求

在下图中，路由器 A 与路由器 B 交换路由更新信息时采用纯文本认证，而在与路由器 C 交换路由更新时使用 MD5 密文认证。

路由器 A 的以太网接口与路由器 B 的以太网接口在 OSPF 区域 0 内。路由器 A 的 Serial 口与路由器 C 的 Serial 口都在区域 1 内，它们都为区域 1 配置了 MD5 认证。

2. 组网图

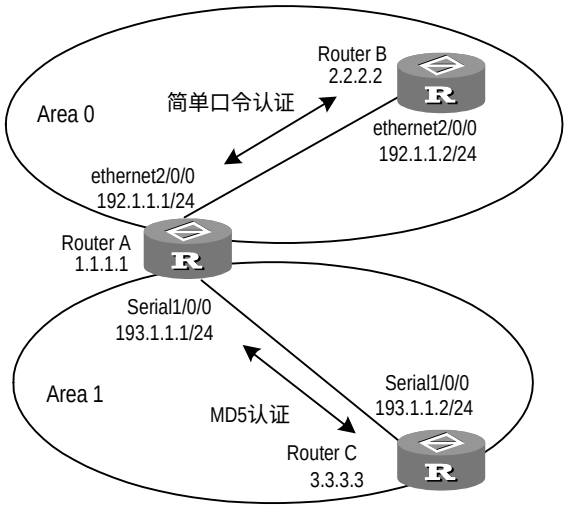


图4-8 配置 OSPF 邻居认证的组网图

3. 配置步骤

配置路由器 Router A：

配置接口 Serial1/0/0 的网段 193.1.1.0 所在的区域 1 支持 MD5 密文验证，验证字标识符为 1，验证字为 password。

配置接口 ethernet 2/0/0 的网段 192.1.1.0 所在的区域 0 支持明文验证，验证字为 password。

```
[Router A] interface ethernet 2/0/0
[Router A-Ethernet2/0/0] ip address 192.1.1.1 255.255.255.0
[Router A-Ethernet2/0/0] ospf authentication-mode simple password
[Router A] interface serial 1/0/0
[Router A-Serial1/0/0] ip address 193.1.1.1 255.255.255.0
[Router A-Serial1/0/0] ospf authentication-mode md5 1 password
[Router A] router id 1.1.1.1
[Router A] ospf
[Router A-ospf-1] area 0
[Router A-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[Router A-ospf-1-area-0.0.0.0] authentication-mode simple
[Router A-ospf-1-area-0.0.0.0] quit
[Router A-ospf-1] area 1
[Router A-ospf-1-area-0.0.0.1] network 193.1.1.0 0.0.0.255
[Router A-ospf-1-area-0.0.0.1] authentication-mode md5
```

配置路由器 Router B：

```
[Router B] interface ethernet 2/0/0
[Router B-Ethernet2/0/0] ip address 192.1.1.2 255.255.255.0
[Router B-Ethernet2/0/0] authentication-mode simple password
[Router B] router id 2.2.2.2
[Router B] ospf
[Router B-ospf-1] area 0
[Router B-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[Router B-ospf-1-area-0.0.0.0] authentication-mode simple
```

配置路由器 Router C：

```
[Router C] interface serial 1/0/0
[Router C-Serial1/0/0] ip address 193.1.1.2 255.255.255.0
[Router C-Serial1/0/0] ospf authentication-mode md5 1 password
[Router C] router id 3.3.3.3
[Router C] ospf
[Router C-ospf-1] area 1
[Router C-ospf-1-area-0.0.0.1] network 193.1.1.0 0.0.0.255
[Router C-ospf-1-area-0.0.0.1] authentication-mode md5
```

4.4.6 配置 OSPF 的 STUB 区

1. 组网需求

RouterA 与 RouterB 通过串口相连，RouterB 与 RouterC 通过以太网口相连属于；RouterA 属于 area0，RouterC 属于 area1，RouterB 同时属于 area0 和 area1。将 area1 配置为 STUB 区。

2. 组网图

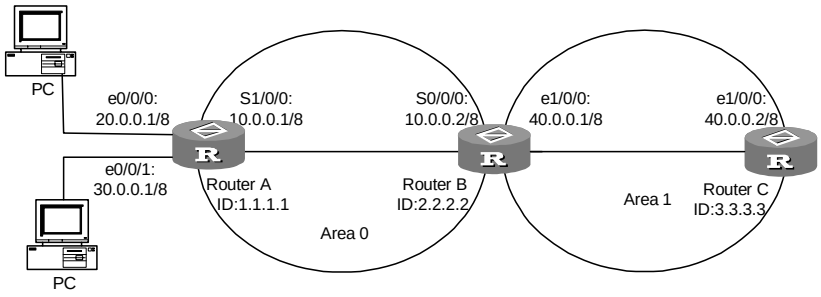


图4-9 配置 OSPF 的 STUB 区

3. 配置步骤

(1) 配置 RouterA

```
[RouterA ] router id 1.1.1.1
[RouterA ] interface serial0/0/0
[RouterA-serial0/0/0] ip address 10.0.0.1 255.0.0.0
[RouterA-serial0/0/0] interface ethernet0/0/0
[RouterA-ethernet 0/0/0] ip address 20.0.0.1 255.0.0.0
[RouterA- ethernet 0/0/0] interface ethernet0/0/1
[RouterA- ethernet 0/0/1] ip address 30.0.0.1 255.0.0.0
[RouterA- ethernet 0/0/1] quit
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 10.0.0.1 0.255.255.255
[RouterA-ospf-1 -area-0.0.0.0] network 20.0.0.1 0.255.255.255
[RouterA-ospf-1 -area-0.0.0.0] network 30.0.0.1 0.255.255.255
```

(2) 配置 RouterB

```
[RouterB] router id 2.2.2.2
[RouterB] interface serial0/0/0
[RouterB-serial0/0/0] ip address 10.0.0.2 255.0.0.0
[RouterB-serial0/0/0] interface ethernet 1/0/0
[RouterB-ethernet 1/0/0] ip address 40.0.0.1 255.0.0.0
[RouterB-ethernet 1/0/0] quit
[RouterB] ospf
[RouterB-ospf-1] area 0
```

```
[RouterB-ospf-1-area-0.0.0.0] network 10.0.0.2  0.255.255.255
[RouterB-ospf-1-area-0.0.0.0] area 1
[RouterB-ospf-1-area-0.0.0.1] network 40.0.0.1  0.255.255.255
[RouterB-ospf-1-area-0.0.0.1] stub
```

(3) 配置 RouterC

```
[RouterC] router id 3.3.3.3
[RouterC] interface ethernet 1/0/0
[RouterC-ethernet 1/0/0] ip address 40.0.0.2 255.0.0.0
[RouterC-ethernet 1/0/0] quit
[RouterC] ospf
[RouterC-ospf-1] area 1
[RouterC-ospf-1-area-0.0.0.1] network 40.0.0.2  0.255.255.255
[RouterC-ospf-1-area-0.0.0.1] stub
```

此时 RouterC 上除了 OSPF 发现的区间路由外，还应有一条缺省路由 0.0.0.0/0。

若将 ABR 路由器 B 上的 **stub** 命令改为 **stub nosummary**，则 area1 变为完全 STUB 区，RouterC 上不在包含任何区间路由，只包含一条默认路由。

4.5 OSPF 故障诊断与排除

故障之一：如果按前述步骤配置了 OSPF，但路由器 OSPF 却不能正常运行。

故障排除：可按如下步骤进行检查。

(1) 局部故障排除：首先检查两台直接相连的路由器之间协议运行是否正常，正常的标志是两台路由器之间 peer 状态机达到 FULL 状态。（注：在广播和 NBMA 网络上，两台接口状态是 DROther 的路由器之间 peer 状态机并不达到 FULL 状态，而是 2 way 状态。DR、BDR 与其它所有路由器之间达到 FULL 状态）

- 使用 display ospf peer 命令查看区域邻居的信息。
- 查看接口上 OSPF 信息可用 display ospf interface 命令。
- 检查物理连接及下层协议是否正常运行。可通过 Ping 命令测试，若从本地路由器 Ping 对端路由器不通，则表明物理连接和下层协议有问题。
- 如果物理连接和下层协议正常，则检查在接口上配置的 OSPF 参数，必须保证与和该接口相邻的路由器的参数一致。区域（Area）号必须相同；网段与掩码也必须一致（点到点与虚连接的网段与掩码可以不同）。
- 检查在同一接口上 dead-interval 值应至少为 hello-interval 值的 4 倍，且与对端的配置保持一致。
- 若网络的类型为 NBMA，则必须手工指定 Peer。使用 **peer ip-address** 命令。
- 若网络类型为广播网或 NBMA，至少有一个接口的 priority 应大于零。

- 如果一个 Area 配置成 stub 区域，则在与这个区域相连的所有路由器中都应将该区域配置成 stub 区域。
- 相邻的两台路由器接口类型必须一致。
- 若配置了两个以上的区域，则至少有一个区域应配成骨干区域（即 Area 号为 0）。
- 应保证骨干区域与所有的区域相连接。
- 虚连接不能穿越 Stub 区域。

(2) 全局故障排除：如果上述步骤无误，但 OSPF 仍不能发现远端路由，则检查如下配置。

- 若一台路由器配置了两个以上的区域，则至少有一个区域应配成骨干区域。

如下图所示：RTA 和 RTD 上只配置了一个区域，RTB（area0，area1）和 RTC（area1，area2）分别配置了两个区域，其中 RTB 中有一个区域为 0，符合要求，但 RTC 中的两个区域都不为 0，则必须在 RTC 与 RTB 之间配置一条虚连接。保证 area 2 与 area 0（骨干区域）相连接。

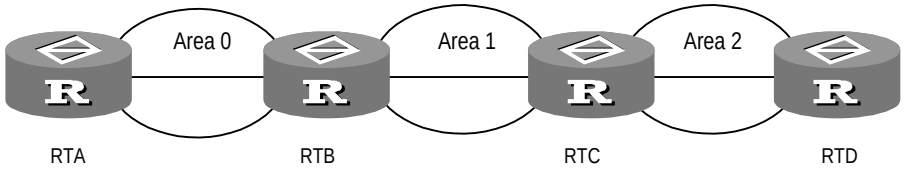


图4-10 OSPF 区域示意图

- 虚连接不能穿越 stub 区域，骨干区域（area 0）也不能配置成 Stub 区域。即如果 RTB 与 RTC 之间配置了一条虚连接，则 area 1 不能配置成 stub 区域，area 0 也不能配置成 stub 区域，上图中只有 area 2 可以配置成 stub 区域。
- 在 Stub 区域内的路由器不能接收外部路由。
- 骨干区域必须保证各个节点的连接。

第5章 集成化 IS-IS 配置

5.1 集成化 IS-IS 简介

IS-IS （ Intermediate System-to-Intermediate System intra-domain routing information exchange protocol，中间系统到中间系统的域内路由信息交换协议）最初是 ISO（the International Organization for Standardization，国际标准化组织）为它的 CLNP（ConnectionLess Network Protocol，无连接网络协议）设计的一种动态路由协议，为了提供对 IP 的路由支持，IETF 在 RFC1195 中对 IS-IS 进行了扩充和修改，使它能够同时应用在 TCP/IP 和 OSI 环境中，称为集成化 IS-IS（Integrated IS-IS 或 Dual IS-IS）。

IS-IS 是一种链路状态协议，使用 SPF（Shortest Path First，最短路径优先）算法，与 OSPF 协议有很多相似之处。IS-IS 属于内部网关协议 IGP（Interior Gateway Protocol），用于自治系统内部。

5.1.1 IS-IS 路由协议的一些概念

1. IS-IS 路由协议的一些术语

- IS（Intermediate System），中间系统。相当于 TCP/IP 中的路由器，是 IS-IS 协议中生成路由和传播路由信息的基本单元。在下文中 IS 和路由器具有相同的含义。
- ES（End System），终端系统。相当于 TCP/IP 中的主机系统。ES 不参与 IS-IS 路由协议的处理，ISO 有专门的 ES-IS 协议定义终端系统与中间系统间的通信。
- RD（Routing Domain），路由域。在一个路由域中一群 IS 通过相同的路由协议来交换路由信息。
- Area，区域，路由域的划分单元。
- LSDB（Link State DataBase），链路状态数据库。所有的网络内连接状态组成了链路状态数据库，在每一个 IS 中都至少有一个 LSDB。IS 使用 SPF 算法，利用 LSDB 来生成自己的路由。
- LSP（Link State Protocol Data Unit），链路状态报文。在 IS-IS 中，每一个 IS 都会生成一个 LSP，此 LSP 包含了本 IS 的所有链路状态信息。每个 IS 收集本区域内所有的 LSP 生成自己的 LSDB。
- NPDU（Network Protocol Data Unit），网络协议数据报文。是 ISO 中的网络层协议报文，相当于 TCP/IP 中的 IP 报文。

- DIS（Designated IS），广播网上的选举中间系统（路由器）。
- NSAP（Network Service Access Point），网络服务接入点，即 ISO 中网络层的地址。用来标识一个抽象的网络层访问服务点，描述 ISO 模型的网络地址结构。

2. IS-IS 路由协议适用的链路类型

IS-IS 可以运行在点到点链路（Point to Point Links），如 PPP、HDLC 等，也可以运行在广播链路（Broadcast Links），如 Ethernet、Token-Ring 等，对于 NBMA（Non-Broadcast Multi-Access）网络，如 ATM，需对其配置子接口，并将子接口类型配置为 P2P 或广播网络。IS-IS 不能在点到多点链路（Point to MultiPoint Links）上运行。

5.1.2 IS-IS 路由协议的两级结构

1. 两级结构

为了支持大规模的路由网络，IS-IS 在路由域内采用两级的分层结构。一个大的路由域被分成一个或多个区域（Areas）。区域内的路由通过 Level-1 路由器管理，区域间的路由通过 Level-2 路由器管理。

2. Level-1 与 Level-2

- Level-1 路由器

Level-1 路由器负责区域内的路由，它只与同一区域的 Level-1 路由器形成邻居关系，维护一个 Level-1 的 LSDB，该 LSDB 包含本区域的路由信息，到区域外的报文转发给最近的 Level-2 路由器。

- Level-2 路由器

Level-2 路由器负责区域间的路由，可以与其它区域的 Level-2 路由器形成邻居关系，维护一个 Level-2 的 LSDB，该 LSDB 包含区域间的路由信息。所有 Level-2 路由器组成路由域的骨干网，负责在不同区域间通信，路由域中的 Level-2 路由器必须是连续的，以保证骨干网的连续性。只有 Level-2 路由器才能直接与路由域外的路由器交换数据报文或路由信息。

- Level-1-2 路由器

同时属于 Level-1 和 Level-2 的路由器称为 Level-1-2 路由器，每个区域至少有一个 Level-1-2 路由器，以将区域连在骨干网上。它维护两个 LSDB，Level-1 的 LSDB 用于区域内路由，Level-2 的 LSDB 用于区域间路由。

下图所示为一个运行 IS-IS 协议的网络，包含路由域 Routing Domain 1 和 Routing Domain 2。Routing Domain 1 包含两个区域：Area 1 和 Area 2，Routing Domain 2 仅包含一个区域：Area 3。在 Routing Domain 1 中，用粗黑线条相连的 3 个 IS 构

成了该路由域的骨干，这 3 个 IS 均是 Level-2 路由器，另外 4 个没有直接用粗黑线条相连的 IS 是 Level-1 路由器。

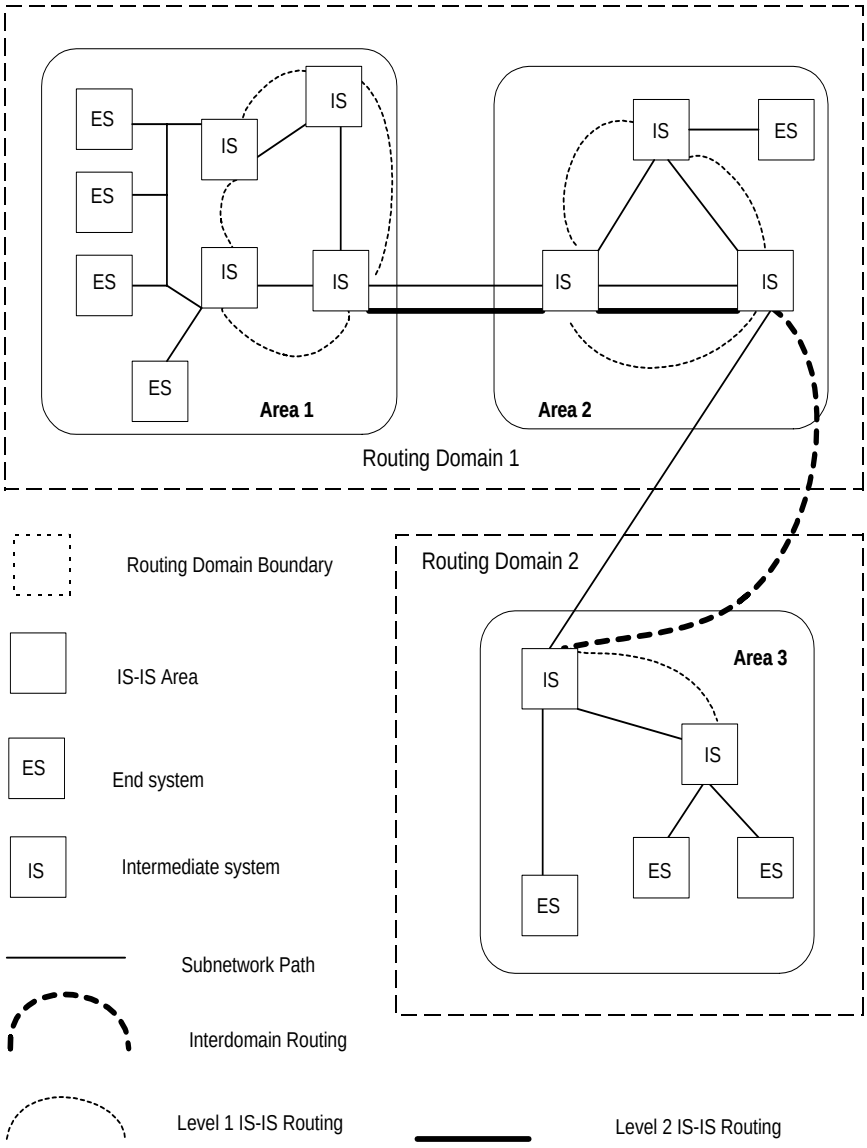


图5-1 IS-IS 拓扑结构图

3. 路由渗透（Routing Leak）

通常情况下，IS-IS 的区域也称为 Level-1 区域，区域内的路由通过 Level-1 的路由器进行管理。所有的 Level-2 路由器构成一个 Level-2 区域。因此，一个 IS-IS 的路由域可以包含多个 Level-1 区域，但只有一个 Level-2 区域。

Level-1 区域必须且只能与 Level-2 区域相连，不同的 Level-1 区域之间并不相连。

Level-1 区域内的路由信息通过 Level-1-2 路由器通报给 Level-2 区域，因此，Level-2 路由器知道整个 IS-IS 路由域的路由信息。但是，在缺省情况下，Level-2 路由器并不将自己知道的其他 Level-1 区域以及 Level-2 区域的路由信息通报给 Level-1 区域。

这样，Level-1 路由器将不了解本区域以外的路由信息，可能导致对本区域之外的目的地址无法选择最佳的路由。

为解决上述问题，IS-IS 提供了路由渗透功能，使 Level-2 路由器可以将已知的其他 Level-1 区域以及 Level-2 区域的路由信息通报给指定的 Level-1 区域。

5.1.3 IS-IS 路由协议的地址结构

1. 地址结构

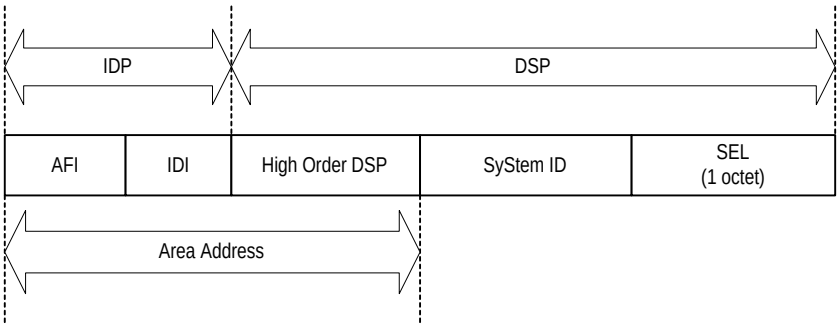


图5-2 IS-IS 协议的地址结构示意图

ISO 采用如上图所示的地址结构，即 NSAP，它由初始域部分（IDP，Initial Domain Part）和域特定部分（DSP，Domain Specific Part）组成。IDP 部分是 ISO 规定的，指定了可分配地址其余部分的责任者和地址使用的格式，DSP 部分由 IDP 中指定的责任者进行分配。IDP 和 DSP 的长度都是可变的，总长最多是 20 个字节。

- 区域地址

IDP 由地址格式标识符（AFI，Authority and Format Indicator）与初始域标识符（IDI，Initial Domain Identifier）组成，AFI 定义了 IDI 的格式。DSP 由多个字节构成。IDP 和 DSP 的 HO-DSP 一起，既能够标识路由域，也能够标识路由域中的区域，因此，〔IDP，HO-DSP〕也被一起称为区域地址（Area Address）。

一般情况下，一台路由器只需要配置一个区域地址，且同一区域中所有节点的区域地址都相同。为支持区域的平滑合并、分割、转换，一台路由器最多可配置 3 个区域地址。

- System ID

System ID 用来在区域内唯一标识终端系统或路由器，它的长度是可选的， System ID 的长度为 48bit（6 字节）。一般使用 Router_ID 与 System ID 进行对应。

假设一台路由器使用接口 Loopback0 的 IP 地址 168.10.1.1 作为 Router_ID，则它在 IS-IS 使用的 System ID 可通过如下方法转换得到：

将 IP 地址 168.10.1.1 的每一部分都扩展为 3 位，不足 3 位的在前面补 0；

将扩展后的地址 168.010.001.001 分为 3 部分，每部分由 4 位数字组成；

重新组合的 1680.1000.1001 就是 System ID。

实际 System ID 的指定可以有不同的方法，但要保证能够唯一标识终端系统或路由器。

- SEL

SEL（NSAP Selector，有时也写成 N-SEL）的作用类似 IP 中的“ 协议标识符 ”，不同的传输协议对应不同的 SEL。在 IP 上 SEL 均为 00。

由于这种地址结构明确地定义了区域，Level-1 路由器很容易识别出发往它所在的区域之外的报文，这些报文是需要转交给 Level-2 路由器的。

Level-1 路由器利用 System ID 进行区域内的路由，如果发现报文的目的地址不属于自己所在的区域，就将报文转发给最近的 Level-2 路由器。

Level-2 路由器根据区域地址（IDP＋HO-DSP）进行区域间的路由。

2. 网络实体名称 NET

网络实体名称 NET（Network Entity Title）指示的是 IS 本身的网络层信息，不包括传输层信息（SEL＝0），可以看作是一类特殊的 NSAP。

通常情况下，一台路由器配置一个 NET 即可，当区域需要重新划分时，例如将多个区域合并，或者将一个区域划分为多个区域，这种情况下配置多个 NET 可以在重新配置时仍然能够保证路由的正确性。由于区域地址最多可配置 3 个，所以 NET 最多也只能配 3 个。

例如，有 NET 名为：47.0001.aaaa.bbbb.cccc.00，其中：

Area=47.0001，System ID=aaaa.bbbb.cccc，SEL=00。

又例如，有 NET 名为：01.1111.2222.4444.00，其中：

Area=01，System ID=1111.2222.4444，SEL=00。

5.1.4 IS-IS 路由协议使用的报文

IS-IS 报文直接封装在数据链路帧中，主要分 3 类：Hello 报文，LSP 和 SNP。

1. Hello 报文

Hello 报文用于建立和维持邻居关系，也称为 IIH（IS-to-IS Hello PDUs），其中，广播局域网中的 Level-1 路由器使用 Level-1 LAN IIH；广播局域网中的 Level-2 路由器使用 Level-2 LAN IIH；非广播网络中则使用 Point-to-Point IIH。

2. LSP

LSP（Link State PDUs），链路状态报文。用来交换链路状态信息。LSP 分为两种：Level-1 LSP 和 Level-2 LSP。Level-2 LSP 由 Level-2 路由器传送，Level-1 LSP 由 Level-1 路由器传送，Level-1-2 路由器则可传送以上两种 LSP。

3. SNP

SNP（Sequence Number PDUs），时序报文，用于确认邻居之间最新接收的 LSP，作用类似于确认（Acknowledge）报文，但更有效。SNP 包括 CSNP（Complete SNP，全时序报文）和 PSNP（Partial SNP，部分时序报文），进一步又分为 Level-1 CSNP、Level-2 CSNP、Level-1 PSNP 和 Level-2 PSNP。

PSNP 只列举最近收到的一个或多个 LSP 的序号，它能够一次对多个 LSP 进行确认，当发现 LSDB 不同步时，也用 PSNP 来请求邻居发送新的 LSP。

CSNP 包括 LSDB 中所有 LSP 的摘要信息，从而可以在相邻路由器间保持 LSDB 的同步。在广播网络上，CSNP 由 DIS 定期发送（缺省的发送周期为 10 秒）；在点到点线路上，CSNP 只在第一次建立邻接关系时发送。

5.2 集成化 IS-IS 配置

使能 IS-IS 是必需的，其它配置则是可选的。

集成化 IS-IS 配置包括：

- 使能 IS-IS
- 配置网络实体名称
- 在指定接口上使能 IS-IS
- 配置 IS-IS 报文中路由权值的类型
- 配置 IS-IS 链路状态路由权
- 配置 IS-IS 协议的定时器
- 配置路由器的优先级
- 配置接口电路类型
- 配置接口的认证密码
- 配置接口的 mesh group
- 配置路由器的类型
- 配置生成缺省路由
- 配置 IS-IS 认证密码
- 配置聚合路由
- 配置过载标志位
- 配置忽略 LSP 的校验和校验错误
- 配置邻接状态输出开关
- 配置 LSP 刷新周期
- 配置 LSP 有效时间
- 配置 SPF 计算间隔

- 配置 SPF 分段计算
- 配置 SPF 主动释放 CPU
- 配置是否允许接口发送报文
- 配置 IS-IS 引入其它协议的路由
- 配置 IS-IS 路由过滤
- 配置 IS-IS 协议的优先级
- 配置 IS-IS 路由渗透
- 清除所有 IS-IS 数据结构
- 清除 IS-IS 特定邻居

5.2.1 使能 IS-IS

创建一个 ISIS 路由进程，并在可能和其他路由器存在关联关系的接口上激活这个路由进程，才可以启动运行 ISIS 协议。

请在系统视图下进行如下配置。

表5-1 使能 IS-IS

操作	命令
使能 IS-IS 路由进程，进入 IS-IS 视图	**isis** [*tag*]
删除 IS-IS 路由进程	**undo isis** [*tag*]

参数 *tag* 是 IS-IS 进程的标识，在目前的版本中仅允许运行一个 IS-IS 进程。

缺省情况下，不使能 IS-IS 路由进程。

5.2.2 配置网络实体名称

网络实体名称 NETs（Network Entity Titles）定义了当前 IS-IS 的区域地址和路由器的系统 ID。

请在 IS-IS 视图下进行下列配置。

表5-2 设置网络实体名称

操作	命令
设置网络实体名称	**network-entity** *net*
删除网络实体名称	**undo network-entity** *net*

参数 *net* 的格式为 X…X.XXXXXXXXXXXX.XX，其中前面的 “ X…X ” 指区域地址，中间的 12 个 “ X ” 用于标识路由器的 System ID。最后的 “ XX ” 必须是 00。

5.2.3 在指定接口上使能 IS-IS

在使能 IS-IS 后，还需要指定 IS-IS 在哪些接口上运行。

请在接口视图下进行下列配置。

表5-3 在指定接口上使能 IS-IS

操作	命令
设置指定接口上使能 IS-IS	**isis enable** [*tag*]
禁止接口上运行的 IS-IS 进程	**undo isis enable** [*tag*]

缺省情况下，接口上不使能 IS-IS 路由进程。

📖 说明：

在目前的实现中，一台路由器最多可以在 255 个接口上使能 IS-IS 路由进程（包括子接口等逻辑接口）。

5.2.4 配置 ISIS 的 Hello 报文是否填充

请在接口视图下进行下面配置。

表5-4 配置 ISIS 的 Hello 报文是否填充

操作	命令
使 ISIS 的 Hello 报文在本身数据长度没有达到接口 MTU 大小时，不填充至接口 MTU 大小	**isis small-hello**
恢复到缺省情况，ISIS 的 Hello 报文在本身数据长度没有达到接口 MTU 大小时，填充至接口 MTU 大小	**undo isis small-hello**

建议 MTU 最大值超过 1500 字节的接口都配置这条命令，如 Tunnel 口、GigabitEthernet 接口。

5.2.5 配置 IS-IS 报文中路由权值的类型

IS-IS 路由协议对于链路路由权值的表示方式有两种：

- 采用 Narrow 方式，路由权值的取值范围为 1～63。
- 采用 Wide 方式，路由权值的取值范围是 1～2^{24}-1，即 1～16777215。

路由器可以选择支持其中一种方式，也可以同时支持这两种方式。

请在 IS-IS 视图下进行下列配置。

表5-5 配置 IS-IS 报文中路由权值的表示方式

操作	命令
设置路由权值的表示方式	**cost-style** { **narrow** | **wide** | **compatible** [**relax-spf-limit**] | **narrow-compatible** [**relax-spf-limit**] | **wide-compatible** }
恢复缺省设置	**undo cost-style**

缺省情况下，IS-IS 只收发采用 Narrow 方式表示路由权值的报文。

5.2.6 配置 IS-IS 链路状态路由权

用户可以配置接口的开销，也就是缺省路由权。当权值类型为 narrow 时，取值范围为 1～63；当权值类型为 wide 时，取值范围为 1～16777215。

请在接口视图下进行下列配置。

表5-6 设置 IS-IS 链路状态路由权

操作	命令
设置接口的路由权	**isis cost** *vlaue* [**level-1** | **level-2**]
恢复接口的路由权缺省值	**undo isis cost** [**level-1** | **level-2**]

如果命令中不指定 level-1 或 level-2，则默认为设置的是 Level-1 的路由权。

缺省情况下，IS-IS 在接口上的路由权值为 10。

5.2.7 配置 IS-IS 协议的定时器

请在接口视图下进行下列配置。

1. 配置 Hello 报文广播间隔

IS-IS 周期性从接口上发送 Hello 报文，路由器通过对 Hello 报文的收发来维护相邻关系。Hello 报文的发送间隔可以通过配置更改。

表5-7 设置 Hello 报文广播间隔

操作	命令
设置接口上 Hello 报文发送间隔	**isis timer hello** *seconds* [**level-1** | **level-2**]
恢复接口上 Hello 报文发送间隔缺省值	**undo isis timer hello** [**level-1** | **level-2**]

广播链路上存在 Level-1 和 Level-2 两种 hello 报文，不同类型的报文可以设置不同的值。但如果链路上不分层，则命令中可以不指定 level-1 或 level-2，所有报文默认设置为 Level-1 和 Level-2 的 Hello 报文广播间隔。在点到点链路上，hello 报文没有 Level-1 和 Level-2 之分，这时也无需设定报文属性了。

缺省情况下，接口上 Hello 报文的发送间隔时间为 10 秒。

2. 配置 CSNP 报文广播间隔

CSNP 报文是指派的中间系统 DIS（Designated IS）在广播型网络上同步链路状态数据库 LSDB 所发送的报文。在广播网络上，CSNP 报文周期性地广播，用户可以设置它的广播间隔。

表5-8 设置 CSNP 报文广播间隔

操作	命令
设置接口上 CSNP 报文发送间隔，时间单位为秒	**isis timer csnp** *seconds* [**level-1** | **level-2**]
恢复接口上 CSNP 报文发送间隔缺省值	**undo isis timer csnp** [**level-1** | **level-2**]

如果命令中不指定 Level-1 或 Level-2，则默认为设置 Level-1 的 CSNP 报文广播间隔。

缺省情况下，接口上 CSNP 报文发送的间隔时间为 10 秒。

3. 配置 LSP 报文发送间隔

链路状态报文 LSP 用来在区域内传播链路状态记录。

表5-9 设置 LSP 报文发送间隔

操作	命令
设置接口上 LSP 报文的发送间隔，单位为毫秒	**isis timer lsp** *time*
恢复接口上 LSP 报文发送间隔的缺省值	**undo isis timer lsp**

缺省情况下，接口上 LSP 报文的发送间隔为 33 毫秒。

4. 配置接口的 LSP 重传间隔

在点到点的链路中，本端发送的 LSP 如果一段时间内没有收到应答，则认为原先发送的 LSP 丢失或被丢弃，为保证发送的可靠性，本端路由器会将原先的 LSP 重新发送一次。

表5-10 设置接口的 LSP 重传间隔

操作	命令
设置 LSP 在点到点链路上的重传间隔	**isis timer retransmit** *seconds*
恢复 LSP 在点到点链路上重传间隔的缺省值	**undo isis timer retransmit**

缺省情况下，接口上 LSP 报文在点到点链路上的重传间隔时间为 5 秒。

5. 配置接口的 Hello 报文失效数目

IS-IS 协议通过 Hello 报文的收发来维护与相邻路由器的邻居关系，当本端路由器在一段时间间隔内收不到对端发送的 Hello 报文时，将认为邻居路由器已经失效，这段等待时间就是 IS-IS 的 Holddown 时间（保持时间）。

在 IS-IS 中，Holddown 时间是通过设置 Hello 报文失效数目来调整的，即，连续没有收到指定数目的 Hello 报文后，认为邻居失效。

表5-11 设置接口的 Hello 报文失效数目

操作	命令
设置 Hello 报文失效数目	**isis timer holding-multiplier** *value* [**level-1** | **level-2**]
恢复缺省设置	**undo isis timer holding-multiplier** [**level-1** | **level-2**]

缺省情况下，Hello 报文失效数目为 3。

如果命令中不指定 Level-1 或 Level-2，则认为是设置 Level-1 和 Level-2 的 Hello 报文失效数目。

5.2.8 配置路由器的优先级

在广播网络中，IS-IS 需要在所有的路由器中选举一个路由器作为 DIS。

当需要在广播网络上的 IS-IS 邻居中挑选 DIS 时，应该分别挑选 1 层和 2 层 DIS。优先级数值越高，被挑中的可能性就越大。当广播网络上优先级最高的路由器有两台或更多，则其中 MAC 地址最大的路由器会被选中。当其相邻的路由器的优先级都是 0 时，则仍然会是其中 MAC 地址最大的路由器会被选中。

Level-1 和 Level-2 的 DIS 是分别选举的，用户可以为不同级别的 DIS 选举设置不同的优先级。

请在接口视图下进行下列配置。

表5-12 设置路由器选举 DIS 的优先级

操作	命令
设置用来选举 DIS 的优先级	**isis dis-priority** *value* [**level-1** | **level-2**]
恢复用来选举 DIS 的优先级缺省值	**undo isis dis-priority** [**level-1** | **level-2**]

缺省情况下，接口上的优先级为 64。如果命令中不指定 level-1 或 level-2，则默认为设置 Level-1 的优先级。

5.2.9 配置接口电路类型

请在接口视图下进行下列配置。

表5-13 设置接口电路类型

操作	命令
设置接口的电路类型	**isis circuit-level** [**level-1** | **level-1-2** | **level-2**]
恢复接口的电路类型缺省值	**undo isis circuit-level**

设置接口的电路类型可以限制接口所能建立的邻接关系，如 level-1 的接口只能建立 Level-1 的邻接关系，level-2 的接口只能建立 Level-2 的邻接关系。对于 Level-1-2 的路由器，将某些接口配置为 Level-2，可以防止将 Level-1 的 Hello 报文发送到 Level-2 骨干上，从而节省带宽。需要注意的是，在点到点链路上，Level-1、Level-2 使用相同的 Hello 报文，这种设置也就没什么意义了。

缺省情况下，接口的电路类型为 **level-1-2**。

5.2.10 配置接口的认证密码

接口上设置的认证密码用在 Hello 报文中，以确认邻居的有效性和正确性。配置时，应保证同一网络所有接口的相同级别的认证密码一致。

请在接口视图下进行下列配置。

表5-14 设置接口的认证密码

操作	命令
设置认证密码	**isis authentication-mode** { **simple** | **md5** } *password* [{ **level-1** | **level-2** } [**ip** | **osi**]]
删除认证密码	**undo isis authentication-mode** { **simple** | **md5** } *password* [{ **level-1** | **level-2** } [**ip** | **osi**]]

缺省情况下，接口上不设置认证密码，不做认证。如果命令中不指定 level-1 或 level-2，则默认为设置 Level-1 的认证密码。

5.2.11 配置接口的 mesh group

在NBMA网络上，路由器的一个接口收到一个新的LSP，会将该LSP扩散（Flooding）到路由器的其它接口，在一个连通程度比较高的，有多条点到点链路的网络中，这种处理方式会造成 LSP 的重复扩散，浪费带宽。

为了避免这种情况的发生，可以将一些接口组成 mesh group，一个组中的接口不把从本组接口扩散来的 LSP 扩散到同组中的其它接口，而只扩散到其它组的接口上。

请在接口视图下进行下列配置。

表5-15 设置接口的 mesh group

操作	命令
设置接口加入 mesh group	**isis mesh-group** [*mesh-group-number* | **mesh-blocked**]
将接口移出 mesh group	**undo isis mesh-group**

缺省情况下，接口正常进行 LSP 的扩散。当对接口设置了 **mesh-blocked** 参数后，接口被阻塞，不再向其它接口扩散 LSP。

至此，接口上的 IS-IS 配置任务就结束了，下面的配置任务主要是用来配置 IS-IS 其它参数。

5.2.12 配置路由器的类型

依据路由器所处的位置不同，可以分为 Level-1（区域内路由器），Level-2（区域间路由器）和 Level-1-2（既是区域内路由器又是区域间路由器）。

请在 IS-IS 视图下进行下列配置。

表5-16 设置路由器的类型

操作	命令
设置路由器的类型	**is-level** { **level-1** | **level-1-2** | **level-2** }
恢复路由器类型的缺省设置	**undo is-level**

缺省情况下，路由器的类型为 **level-1-2**。

5.2.13 配置生成缺省路由

IS-IS 路由域中，Level-1 路由器只有本区域内的 LSDB，只生成本区域内的路由；Level-2 路由器有 IS-IS 路由域内骨干的 LSDB，只生成骨干的路由。区域内的 Level-1 路由器如果要将报文转发到其它区域中，需要将报文先转发到本区域中离它最近的一个 Level-1-2 路由器上，这条路由就是 Level-1 的缺省路由。

请在 IS-IS 视图下进行如下配置。

表5-17 设置生成缺省路由

操作	命令
设置生成缺省路由	**default-route-advertise** [**route-policy** *route-policy-name*]
设置不生成缺省路由	**undo default-route-advertise** [**route-policy** *route-policy-name*]

由该命令产生的缺省路由只被引入到同级别的路由器上。

5.2.14 配置 IS-IS 认证密码

用户可以为 IS-IS 区域或者 IS-IS 路由域配置认证密码。

如果需要区域验证，区域验证密码就会按照设定的方式封装到 1 层（Level-1）的 LSP、CSNP、PSNP 报文。如果同一区域内的其他路由器也启动了区域验证，那么这些路由器的验证方式和密码必须和原有的相符才能正常工作。同样，对于路由域验证的情况，域验证密码也会按照设定的方式封装到 2 层（Level-2）的 LSP、CSNP、PSNP 报文。如果骨干层（Level-2）的其他路由器也需要路由域验证，验证方式和密码必须和原有的相符才行。

请在 IS-IS 视图下进行下列配置。

表5-18 设置 IS-IS 认证密码

操作	命令
设置区域认证密码	**area-authentication-mode** { **simple** | **md5** } *password* [**ip** | **osi**]
删除区域认证密码	**undo area-authentication-mode** { **simple** | **md5** } [**ip** | **osi**]
设置路由域认证密码	**domain-authentication-mode** { **simple** | **md5** } *password* [**ip** | **osi**]
删除路由域认证密码	**undo domain-authentication-mode** { **simple** | **md5** } [**ip** | **osi**]
设置 ISIS 采用与华为兼容的 MD5 算法	**md5-compatible**
用来恢复缺省的 MD5 算法（即标准算法）	**undo md5-compatible**

缺省情况下，系统不设置密码，也不做认证。

5.2.15 配置聚合路由

路由聚合是指将同一网段内多条子网不同的路由聚合成一条路由。这个网段并不限于自然网段，它可以仍然是一个子网网段或者是一个超网网段。当然，被聚合的所有子网路由必须具有相同的下一跳。

使用路由聚合可以使得网络中传播的路由信息量减少，也使得其它路由器的路由表减小。

请在 IS-IS 视图下进行如下配置。

表5-19 设置聚合路由

操作	命令
设置聚合路由	**summary** *ip-address ip-mask* [**level-1** | **level-1-2** | **level-2**]
删除聚合路由	**undo summary** *ip-address ip-mask* [**level-1** | **level-1-2** | **level-2**]

缺省情况下，系统不进行路由聚合。

5.2.16 配置过载标志位

如果 IS-IS 域中的路由器在运行中发生问题，会导致整个区域路由的错误，为避免这种问题的发生，我们可以为此路由器设置过载标志位。

当限定了过载位后，其他路由器就不再将应该由本路由器转发的报文转送过来。

请在 IS-IS 视图下进行如下配置。

表5-20 设置过载标志位

操作	命令
设置过载标志位	**set-overload**
清除过载标志位	**undo set-overload**

缺省情况下，不设置过载标志位。

5.2.17 配置忽略 LSP 的校验和校验错误

当本地 IS-IS 收到 LSP 时，要对它的校验和检验。在缺省状况下，如果发现报文中的校验和与计算出来的校验和不一致，则将此 LSP 丢弃，不作处理；如果通过命令 **ignore-lsp-checksum-error** 设置忽略检验错误，则即使检验出 LSP 的校验和错误，也会将此报文按正常报文处理。

请在 IS-IS 视图下进行下列配置。

表5-21 设置忽略 LSP 的校验和校验错误

操作	命令
设置忽略 LSP 的校验和校验错误	**ignore-lsp-checksum-error**
设置不忽略 LSP 的校验和校验错误	**undo ignore-lsp-checksum-error**

缺省情况下，不忽略 LSP 的校验和校验错误。

5.2.18 配置邻接状态输出开关

当打开邻接状态输出开关后，IS-IS 邻接状态的变化会输出到配置终端上，直至邻接状态输出开关被关闭。

请在 IS-IS 视图下进行如下配置。

表5-22 设置邻接状态输出开关

操作	命令
打开邻接状态输出开关	**log-peer-change**
关闭邻接状态输出开关	**undo log-peer-change**

缺省情况下，关闭邻接状态输出开关。

5.2.19 配置 LSP 刷新周期

为了保证整个区域中的 LSP 能够保持同步，LSP 周期性发送当前全部 LSP。

可以调整发送 LSP 的周期。对于稳定的网络，此周期可以设置得比较长，对于不太稳定的网络，此周期应设置得比较短。

请在 IS-IS 视图下进行下列配置。

表5-23 设置 LSP 刷新周期

操作	命令
设置 LSP 刷新周期	**timer lsp-refresh** *seconds*
恢复 LSP 刷新周期缺省值	**undo timer lsp-refresh**

缺省情况下，LSP 刷新周期为 900 秒，即 15 分钟。

5.2.20 配置 LSP 有效时间

路由器生成系统 LSP 时，会在 LSP 中填写此 LSP 的最大有效时间。当此 LSP 被其它路由器接收后，它的有效时间会随着时间的变化不断减小，如果路由器一直没有收到更新的 LSP，而此 LSP 的有效时间已减少到 0，那么此 LSP 将被从 LSDB 中删除。

LSP 有效时间应大于 LSP 刷新周期。

请在 IS-IS 视图下进行下列配置。

表5-24 设置 LSP 有效时间

操作	命令
设置 LSP 有效时间	**timer lsp-max-age** *seconds*
恢复 LSP 有效时间缺省值	**undo timer lsp-max-age**

缺省情况下，LSP 有效时间为 1200 秒，即 20 分钟。

5.2.21 配置 SPF 计算间隔

当 IS-IS 的链路状态数据库 LSDB 发生改变时，路由器需要重新计算最短路径，如果每次改变都立刻计算最短路径，将占用大量路由器系统资源，影响路由器的效率。设置 SPF 的计算间隔后，当 LSDB 改变时，如果 SPF 的计算间隔定时器未超时，则等待，直到超时后才运行 SPF 算法。

请在 IS-IS 视图下进行下列配置。

表5-25 设置 SPF 计算间隔

操作	命令
设置 SPF 计算间隔	**timer spf** *second* [**level-1** | **level-2**]
恢复 SPF 计算间隔的缺省值	**undo timer spf** [**level-1** | **level-2**]

如果命令中不指定 level-1 或 level-2，则默认为设置 Level-1 的 SPF 计算间隔。

缺省情况下，SPF 计算间隔为 5 秒钟。

5.2.22 配置 SPF 分段计算

当路由表中的路由数目很多时（超过 15 万条），IS-IS 的 SPF 计算可能会长时间占用系统资源，为防止这种情况的发生，可以设置 SPF 的计算分段进行。

请在 IS-IS 视图下进行下列配置。

表5-26 设置 SPF 分段计算

操作	命令
设置 SPF 分段计算	**spf-slice-size** *seconds*
恢复缺省设置	**undo spf-slice-size**

缺省情况下，SPF 的计算不分段，一次运行至结束，参数 *seconds* 取值为 0 也可以达到这种效果。

设置分段计算后，一次运行未处理完的路由，等待 1 秒后继续计算。

通常情况下，建议不要改变缺省设置。当路由数目超过 15 万至 20 万条时，推荐的 *seconds* 取值为 1，即每次 SPF 的计算持续时间为 1 秒。

5.2.23 配置 SPF 主动释放 CPU

为防止 IS-IS 的 SPF 计算长时间占用系统资源，影响控制台的响应速度，可以设置 SPF 每处理一定数量的路由后，自动释放系统 CPU 资源，未处理完的路由等待 1 秒后继续计算。

请在 IS-IS 视图下进行下列配置。

表5-27 设置 SPF 主动释放 CPU

操作	命令
设置 SPF 主动释放 CPU 的间隔	**spf-delay-interval** *number*
恢复缺省设置	**undo spf-delay-interval**

缺省情况下，IS-IS 的 SPF 每处理 5000 条路由主动释放一次 CPU。

5.2.24 配置是否允许接口发送报文

为使 IS-IS 路由信息不被某一网络中的路由器获得，可使用 **silent-interface** 命令来禁止在与此路由器相连的接口上发送 IS-IS 报文。

请在 IS-IS 视图下进行下列配置。

表5-28 禁止/允许接口发送报文

操作	命令
禁止接口发送 IS-IS 报文	**silent-interface** *silent-interface-type silent-interface-number*
允许接口收发 IS-IS 报文	**undo silent-interface** *silent-interface-type silent-interface-number*

缺省情况下，允许接口收发 IS-IS 报文。

silent-interface 只是抑制 IS-IS 报文不在接口上发送，但接口路由仍然会从其它的接口发送。

5.2.25 配置 IS-IS 引入其它协议的路由

对 IS-IS 而言，其它的路由协议发现的路由被当作路由域外部的路由处理。在引入其它协议路由时，可指定引入路由的缺省开销。

在 IS-IS 引入路由时，可以指定将路由引入到 Level-1 级、Level-2 级以及 Level-1-2 级。

请在 IS-IS 视图下进行下列配置。

表5-29 引入其它协议的路由

操作	命令
引入其它协议的路由	**import-route** *protocol* **[allow-ibgp]** [**cost** *value*] [**type** { **external** | **internal** }] [**level-1**] [**level-1-2**] [**level-2**] [**route-policy** *route-policy-name*]
取消引入其它协议路由	**undo import-route** *protocol* [**cost** *value*] [**type** { **external** | **internal** }] [**level-1**] [**level-1-2**] [**level-2**] [**route-policy** *route-policy-name*]

如果命令中不指定引入的级别，则默认为引入路由到 Level-2 的路由表中。

protocol 指定可引入的源路由协议，目前可为 direct、static、rip、bgp、ospf、ospf-ase 和 ospf-nssa。

allow-ibgp：当 *protocol* 为 BGP 时，**allow-ibgp** 为可选关键字。**import-route bgp** 表示只引入 EBGP 路由，**import-route bgp allow-ibgp** 表示将 IBGP 路由也引入，该配置危险，请慎用！

缺省情况下，IS-IS 不引入其它协议的路由信息。

5.2.26 配置 IS-IS 路由过滤

IS-IS 协议可以对接收和发布的路由进行过滤，过滤的标准基于访问控制列表（*acl-number*）。

请在 IS-IS 视图下进行下列配置。

- 配置 IS-IS 对接收路由信息的过滤

表5-30 配置 IS-IS 对接收的路由信息进行过滤

操作	命令
配置对接收的路由信息进行过滤	**filter-policy** *acl-number* **import**
取消对接收的路由信息进行过滤	**undo filter-policy** *acl-number* **import**

- 配置对 IS-IS 发布的路由进行过滤

表5-31 配置 IS-IS 对发布的路由进行过滤

操作	命令
配置 IS-IS 对发布路由的过滤	**filter-policy** *acl-number* **export** *protocol*
取消 IS-IS 对发布路由的过滤	**undo filter-policy** *acl-number* **export** *protocol*

缺省情况下，IS-IS 将不对接收与发布的路由信息进行过滤。

protocol 指定发布路由信息的协议，目前可包括：direct、static、rip、bgp、ospf、ospf-ase 等。

更详细的描述请参见“ IP 路由策略配置 ”的“ 配置路由过滤 ”部分。

5.2.27 配置 IS-IS 协议的优先级

在一台同时运行多种路由协议的路由器上，各个路由协议之间存在路由信息共享和选择的问题。系统为每一种路由协议设置一个优先级，当不同协议都发现了到同一目的地的路由时，优先级高的协议将起作用。

请在 IS-IS 视图下进行下列配置。

表5-32 配置 IS-IS 协议的优先级

操作	命令
配置 IS-IS 协议的优先级	**preference** *value*
恢复 IS-IS 协议优先级的缺省值	**undo preference**

缺省情况下，IS-IS 路由的优先级为 15。

5.2.28 配置 IS-IS 路由渗透

通过 IS-IS 路由渗透功能，Level-2 路由器可以将它所知道的 Level-1 区域路由信息和 Level-2 区域路由信息发布给 Level-1 路由器。

请在 IS-IS 视图下进行下列配置。

表5-33 配置 IS-IS 路由渗透

操作	命令
使能 IS-IS 路由渗透	**import-route isis level-2 into level-1** [**acl** *acl-number*]
禁止 IS-IS 路由渗透	**undo import-route isis level-2 into level-1** [**acl** *acl-number*]

缺省情况下，Level-2 路由器的路由信息不发布到 Level-1 区域中。

5.2.29 清除 IS-IS 数据结构

需要立即刷新某些 LSP 时，请在用户视图下进行如下操作。

表5-34 清除所有 IS-IS 的数据结构

操作	命令
清除 IS-IS 的数据结构	**reset isis all**

5.2.30 清除 IS-IS 特定邻居

需要重新建立与某个特定邻居的连接时，请在用户视图下进行如下操作。

表5-35 清除 IS-IS 的特定邻居

操作	命令
清除 IS-IS 的特定邻居	**reset isis peer** *system-id*

5.3 集成化 IS-IS 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 IS-IS 的运行情况，用户可以通过查看显示信息验证配置的效果。在用户视图下执行 **debugging** 命令可对 IS-IS 进行调试。

通过如下的操作，可以查看 IS-IS 的链路状态数据库，查看 IS-IS 各种报文发送接收情况和 SPF 计算，从而确定 IS-IS 路由维护的情况。

表5-36 集成化 IS-IS 显示和调试

操作	命令
查看 IS-IS 的摘要信息	**display isis brief**
查看 IS-IS 链路状态数据库	**display isis lsdb** [**l1**] [**l2**] [**level-1**] [**level-2**] [**local**] [**verbose**] [*LSPID*]
查看 IS-IS 的 SPF 计算日志	**display isis spf-log**
查看 IS-IS 路由信息	**display isis routing**
查看 IS-IS 邻居信息	**display isis peer** [**verbose**]
查看 mesh group 信息	**display isis mesh-group**
打开 IS-IS 的调试信息开关	**debugging isis** { **adjacency** | **all** | **authentication-error** | **checksum-error** | **circuit-information** | **configuration-error** | **datalink-receiving-packet** | **datalink-sending-packet** | **general-error** | **interface-information** | **memory-allocating** | **receiving-packet-content** | **self-originate-update** | **sending-packet-content** | **snp-packet** | **spf-event** | **spf-summary** | **spf-timer** | **task-error** | **timer** | **update-packet** }
关闭 IS-IS 的调试信息开关	**Undo debugging isis** { **adjacency** | **all** | **authentication-error** | **checksum-error** | **circuit-information** | **configuration-error** | **datalink-receiving-packet** | **datalink-sending-packet** | **general-error** | **interface-information** | **memory-allocating** | **receiving-packet-content** | **self-originate-update** | **sending-packet-content** | **snp-packet** | **spf-event** | **spf-summary** | **spf-timer** | **task-error** | **timer** | **update-packet** }

5.4 集成化 IS-IS 典型配置举例

1. 组网需求

A、B、C 和 D 四台路由器属于同一自治系统。这四台路由器上运行 IS-IS 路由协议，从而实现路由的互通。在网络设计中，A、B、C 和 D 四台路由器属于同一个区域。

2. 组网图

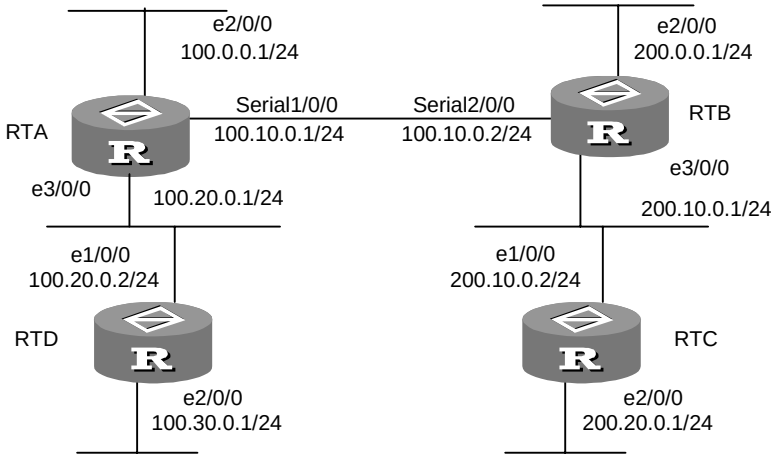


图5-3 IS-IS 配置举例

3. 配置步骤

路由器 RTA 的配置：

```
[RTA] isis
[RTA-isis] network-entity 86.0001.0000.0000.0005.00
[RTA] interface ethernet 2/0/0
[RTA-Ethernet2/0/0] ip address 100.0.0.1 255.255.255.0
[RTA-Ethernet2/0/0] isis enable
[RTA-Ethernet2/0/0] interface serial 1/0/0
[RTA-serial1/0/0] ip address 100.10.0.1 255.255.255.0
[RTA-serial1/0/0] isis enable
[RTA-serial1/0/0] interface ethernet 3/0/0
[RTA-ethernet 3/0/0] ip address 100.20.0.1 255.255.255.0
[RTA-ethernet 3/0/0] isis enable
```

路由器 RTB 的配置：

```
[RTB] isis
[RTB-isis] network-entity 86.0001.0000.0000.0006.00
[RTB] interface ethernet 2/0/0
[RTB-Ethernet2/0/0] ip address 200.0.0.1 255.255.255.0
[RTB-Ethernet2/0/0] isis enable
[RTB-Ethernet2/0/0] interface ethernet 3/0/0
[RTB-ethernet 3/0/0] ip address 200.10.0.1 255.255.255.0
[RTB-ethernet 3/0/0] isis enable
[RTB-ethernet 3/0/0] interface serial 2/0/0
[RTB-serial2/0/0] ip address 100.10.0.2 255.255.255.0
[RTB-serial2/0/0] isis enable
```

路由器 RTC 的配置：

```
[RTC] isis
[RTC-isis] network-entity 86.0001.0000.0000.0007.00
[RTC] interface ethernet 1/0/0
[RTC-Ethernet1/0/0] ip address 200.10.0.2 255.255.255.0
[RTC-Ethernet1/0/0] isis enable
[RTC-Ethernet1/0/0] interface ethernet 2/0/0
[RTC-Ethernet2/0/0] ip address 200.20.0.1 255.255.255.0
[RTC-Ethernet2/0/0] isis enable
```

路由器 RTD 的配置：

```
[RTD] isis
[RTD-isis] network-entity 86.0001.0000.0000.0008.00
[RTD] interface ethernet 1/0/0
[RTD-Ethernet1/0/0] ip address 100.20.0.2 255.255.255.0
[RTD-Ethernet1/0/0] isis enable
[RTD-Ethernet1/0/0] interface ethernet 2/0/0
[RTD-Ethernet2/0/0] ip address 100.30.0.1 255.255.255.0
[RTD-Ethernet2/0/0] isis enable
```

配置完成后，可在各路由器上分别使用 **display isis peer** 命令查看邻居关系的建立情况。

第6章 BGP 配置

📖 说明：

BGP 中有关 VPN 实例及 VPNv4 的具体参数解释及举例，请参见本手册的“ MPLS ”和“ 组播 ”模块。

6.1 BGP 简介

BGP（Border Gateway Protocol）是一种自治系统间的动态路由发现协议。

BGP 协议早期发布的三个版本分别是 BGP-1（请参阅 RFC1105）、BGP-2（请参阅 RFC1163）和 BGP-3（请参阅 RFC1267），当前使用的版本是 BGP-4（请参阅 RFC1771）。BGP-4 适用于分布式结构，并支持无类域间路由 CIDR（Classless Inter-Domain Routing）。利用 BGP 还可以实施用户配置的策略。BGP-4 正迅速成为事实上的 Internet 外部路由协议标准，BGP 协议经常用于 ISP 之间。

BGP 特性描述如下：

- BGP 是一种外部路由协议，与 OSPF、RIP 等内部路由协议不同，其着眼点不在于发现和计算路由，而在于控制路由的传播和选择最好的路由。
- 通过在 BGP 路由中携带 AS 路径信息，可以彻底解决路由循环问题。
- 使用 TCP 作为其传输层协议，提高了协议的可靠性。
- BGP-4 支持无类域间路由 CIDR。这是较 BGP-3 的一个重要改进。CIDR 以一种全新的方法看待 IP 地址，不再区分 A 类网、B 类网及 C 类网。例如一个非法的 C 类网络地址 192.213.0.0（255.255.0.0）采用 CIDR 表示法 192.213.0.0/16 就成为一个合法的超级网络，其中/16 表示子网掩码由从地址左端开始的 16 比特构成。CIDR 的引入简化了路由聚合（Routes Aggregation），路由聚合实际上是合并几个不同路由的过程，这样从通告几条路由变为通告一条路由，减小了路由表规模。
- 路由更新时，BGP 只发送更新的路由，大大减少了 BGP 传播路由所占用的带宽，适用于在 Internet 上传播大量的路由信息。
- 出于管理和安全方面的考虑，每个自治系统都希望能够对进出自治系统的路由进行控制，BGP-4 提供了丰富的路由策略，能够对路由实现灵活的过滤和选择，并且易于扩展以支持网络新的发展。

BGP 系统作为高层协议运行在一个特定的路由器上。系统初启时 BGP 路由器通过发送整个 BGP 路由表与对等体交换路由信息，之后只交换更新消息（update message）。系统在运行过程中，是通过接收和发送 keep-alive 消息来检测相互之间的连接是否正常的。

发送 BGP 消息的路由器称为 BGP 发言人（speaker），它不断的接收或产生新路由信息，并将它广告（advertise）给其它的 BGP 发言人。当 BGP 发言人收到来自其它自治系统的新路由广告时，如果该路由比当前已知路由好、或者当前还没有该接收路由，它就把这个路由广告给自治系统内所有其它的 BGP 发言人。一个 BGP 发言人也将同它交换消息的其它的 BGP 发言人称为对等体（peer），若干相关的对等体可以构成对等体组（group）。

BGP 在路由器上以下列两种方式运行：

- IBGP（Internal BGP）
- EBGP（External BGP）

当 BGP 运行于同一自治系统（AS）内部时，被称为 IBGP；当 BGP 运行于不同自治系统之间时，称为 EBGP。

BGP 协议机的运行是通过消息驱动的，其消息共可分为四类：

- open message
- update message
- notification message
- keep-alive message

open message 是连接建立后发送的第一个消息，它用于建立 BGP 对等体间的连接关系。notification message 是错误通告消息。keep-alive message 是用于检测连接有效性的消息。update message 是 BGP 系统中最重要的信息，用于在对等体之间交换路由信息，它最多由三部分构成：不可达路由(unreachable）、路径属性（path attributes）、网络可达性信息 NLRI（network layer reach/reachable information）。

6.2 BGP 的配置

BGP 的配置包括：

- 启动 BGP
- 指定 BGP 要通告的网络路由
- 配置 BGP 对等体组
- 配置 BGP 定时器
- 配置本地优先级
- 配置自治系统的 MED 值

- 比较来自于不同 AS 邻居的 MED 值
- 配置 BGP 团体属性
- 配置 BGP 路由聚合
- 配置 BGP 协议的优先级
- 配置 BGP 路由反射器
- 配置自治系统联盟属性
- 配置 BGP 路由衰减
- 配置 BGP 与 IGP 的交互
- 配置 BGP 路由过滤
- 定义访问列表、AS 路径列表和 Route-policy
- 配置 BGP 负载分担
- 复位 BGP 连接

6.2.1 启动 BGP

启动 BGP 时应指定本地的自治系统号。启动 BGP 后，本地路由器监听相邻路由器的 BGP 连接请求。要使本地路由器主动向相邻路由器发出 BGP 连接请求，请参照 **peer** 命令的配置。关闭 BGP 时，BGP 将切断所有已经建立的 BGP 连接。

请在系统视图下进行下列配置。

表6-1 启动/关闭 BGP

操作	命令
启动 BGP，进入 BGP 视图	**bgp** *as-number*
关闭 BGP	**undo bgp** [*as-number*]

缺省情况下，系统不运行 BGP。

6.2.2 指定 BGP 要通告的网络路由

请在 BGP 视图下进行下列配置。

表6-2 指定 BGP 发送网络

操作	命令
配置本地 BGP 发送网络	**network** *ip-address* [*address-mask*] [**route-policy** *route-policy-name*]
取消本地 BGP 发送网络	**undo network** *ip-address* [*address-mask*] [**route-policy** *route-policy-name*]

缺省情况下，本地 BGP 不通告任何网络路由。

6.2.3 配置 BGP 对等体组

交换 BGP 报文的 BGP 发言者形成对等体。BGP 对等体不能够脱离对等体组而独立存在，即对等体必须隶属于某一个特定的对等体组。在配置 BGP 对等体时，必须首先配置对等体组，然后再将对等体加入该对等体组中。

当对等体组的配置变化时，每个组员的配置也相应变化。对某些属性可以指定组员的 IP 地址进行配置，从而使指定组员在这些属性上不受对等体组配置的影响。

下列各项配置均在 BGP 视图下进行。

1. 配置对等体组

在配置 BGP 对等体之前，必须首先配置对等体所隶属的对等体组。

表6-3 配置对等体组

操作	命令
创建一个对等体组	**group** *group-name* [**internal** | **external**]
删除指定的对等体组	**undo group** *group-name*

在配置对等体组时需要指定对等体组的类型。internal 类型的对等体组包含的都是 IBGP 对等体；external 类型的对等体都是 EBGP 对等体或者联盟 EBGP 对等体。

配置时，如果不指定对等体组的类型，缺省为 internal。

2. 指定对等体组的自治系统号

可以为类型为 external 的对等体 组指定自治系统号，internal 类型的对等体组无需配置自治系统号。如果为对等体组指定了自治系统号，那么，加入该对等体组的所有对等体都继承了该对等体组的自治系统号。

表6-4 为对等体组指定自治系统号

操作	命令
为对等体组指定自治系统号	**peer** *group-name* **as-number** *as-number*
删除指定的对等体组的自治系统号	**undo group** *group-name* **as-number**

如果对等体组中已经加入了对等体，那么，不能够为该对等体组指定自治系统号；删除对等体组的自治系统号时，会删除对等体组中的所有对等体。

3. 向对等体组中加入组员

BGP 的对等体不能够脱离对等体组而独立存在，在配置对等体的同时必须指定其所属的对等体组，同时可以指定对等体的自治系统号。

表6-5 向对等体组中加入组员

操作	命令
在对等体组中创建一个对等体	**peer** *peer-address* **group** *group-name* [**as-number** *as-number*]
从对等体组中删除一个对等体	**undo peer** *peer-address* **group**

加入对等体组的配置类型为 internal，则命令中不能够指定自治系统号参数。加入的对等体为 IBGP 对等体。

加入对等体组的配置类型为 external，如果对等体没有指定自治系统号，那么对等体加入对等体组的同时必须同时指定该对等体的自治系统号；如果对等体组已经配置了自治系统号，对等体将继承对等体组的自治系统号，无需再为对等体指定。

4. 配置对等体（组）描述信息

为便于了解对等体的特征，可以为 BGP 对等体（组）配置描述信息。

表6-6 配置对等体（组）描述信息

操作	命令
配置对等体（组）描述信息	**peer** { *peer-address* | *group-name* } **description** *description-line*
删除对等体（组）描述信息	**undo peer** { *peer-address* | *group-name* } **description**

缺省情况下 BGP 对等体（组）无描述信息。

5. 配置允许同不直接相连网络上的 EBGP 对等体组建立连接

通常情况下，EBGP 对等体之间必须是物理上直接相连的，如果无法满足，可使用以下命令进行配置。

表6-7 配置允许同不直接相连网络上的 EBGP 对等体组建立连接

操作	命令
配置允许同不直接相连网络上的 EBGP 对等体组建立连接	**peer** *group-name* **ebgp-max-hop** [*ttl*]
配置只允许同直接相连网络上的 EBGP 对等体组建立连接	**undo peer** *group-name* **ebgp-max-hop**

缺省情况下，只允许同直接相连网络上的对等体组建立连接。*ttl* 为最大跳步数，缺省值为 64，范围为 1～255。

6. 配置指定对等体（组）的定时器

使用 **peer timer** 命令可以对指定的 BGP 对等体（组）配置定时器，包括指定 keepalive 报文发送时间间隔和保持定时器，它的优先级高于对所有 BGP 邻居配置定时器使用的 **timer** 命令。

表6-8 配置指定对等体（组）的定时器

操作	命令
配置指定对等体（组）的 keepalive 时间间隔与保持定时器	**peer** { *group-name* | *peer-address* } **timer keep-alive** *keepalive-interval* **hold** *holdtime-interval*
恢复指定对等体（组）的 keepalive 时间间隔与保持定时器的缺省值	**undo peer** { *group-name* | *peer-address* } **timer**

缺省情况下，keepalive 报文的发送时间间隔为 60 秒，保持定时器为 180 秒。

7. 配置对等体组发送路由更新报文的时间间隔

表6-9 配置对等体组发送路由更新报文的时间间隔

操作	命令
配置对等体组发送路由更新报文的时间间隔	**peer** *group-name* **route-update-interval** *seconds*
恢复对等体组发送路由更新报文的缺省时间间隔	**undo peer** *group-name* **route-update-interval**

缺省情况下，IBGP 对等体组发送路由更新报文的时间间隔为 5 秒，EBGP 对等体组发送路由更新报文的时间间隔为 30 秒。

8. 配置把团体属性传给对等体组

表6-10 配置将团体属性传给对等体组

操作	命令
配置将团体属性传给对等体组	**peer** *group-name* **advertise-community**
不将团体属性传给对等体组	**undo peer** *group-name* **advertise-community**

9. 配置对等体组为路由反射器的客户

表6-11 配置对等体组为路由反射器的客户

操作	命令
配置对等体组为路由反射器客户	**peer** *group-name* **reflect-client**
取消对等体组作为路由反射器客户	**undo peer** *group-name* **reflect-client**

只能将配置类型为 internal 的对等体组配置成反射器客户。

缺省情况下，自治系统中的所有 IBGP 必须是全连接的，且邻居间不通告学到的 IBGP 路由，以防止产生路由环。

关于路由反射器，请参考“ 配置 BGP 路由反射器 ”一节的内容。

10. 配置向对等体组发送缺省路由

表6-12 配置向对等体组发送缺省路由

操作	命令
配置向对等体组发送缺省路由	**peer** *group-name* **default-route-advertise**
取消向对等体组发送缺省路由	**undo peer** *group-name* **default-route-advertise**

缺省情况下，本地路由器不向对等体发送缺省路由。使用该命令时，不要求在 BGP 路由表中存在缺省路由，而是无条件地向对等体发送一个下一跳为自身的缺省路由。

11. 配置在发布路由时将自身地址作为下一跳

BGP 路由器向对等体组发布路由时，可使用自身地址作为下一跳。

表6-13 配置在发布路由时将自身地址作为下一跳

操作	命令
配置发布路由时将自身地址作为下一跳	**peer** *group-name* **next-hop-local**
取消发布路由时将自身地址作为下一跳	**undo peer** *group-name* **next-hop-local**

缺省情况下，本地路由器向对等体组发布路由时不把自身地址作为下一跳。

需要说明的是 如果配置了 BGP 负载分担，则不论是否配置了 **peer next-hop-local**，本地路由器向 IBGP 对等体组发布路由时都将把自身地址作为下一跳。

12. 配置传送 BGP 更新报文时不携带私有自治系统号

一般情况下，BGP 在发送 BGP 更新报文时都携带该自治系统号（可能是公有的 AS 号，也可能是私有的 AS 号），为使某些出口路由器在发送更新报文时忽略掉私有 AS 号，可配置发送 BGP 更新报文时不携带私有自治系统号。

表6-14 配置发送 BGP 更新报文时不携带私有自治系统号

操作	命令
配置发送 BGP 更新报文时不携带私有自治系统号	**peer** *group-name* **public-as-only**
配置发送 BGP 更新报文时携带私有自治系统号	**undo peer** *group-name* **public-as-only**

缺省情况下，发送 BGP 更新报文时，携带私有自治系统号。

13. 指定路由更新报文的源接口

为使接口在出现问题时仍能发送更新报文，可配置允许内部 BGP 会话使用任何可与对端建立 TCP 连接的接口，通常指定使用 Loopback 接口。

表6-15 配置指定路由更新报文的源接口

操作	命令
配置指定路由更新报文的源接口	**peer** { *peer-address* | *group-name* } **connect-interface** *interface-type interface-number*
恢复使用最佳路由更新报文的源接口	**undo peer** { *peer-address* | *group-name* } **connect-interface** *interface-type interface-number*

缺省情况下，BGP 使用最佳指定路由更新报文的源接口。

14. 配置激活/去激活对等体（组）

BGP 发言者与被去激活的对等体或对等体组之间不交换路由信息。

表6-16 激活/去激活对等体（组）

操作	命令
激活对等体/对等体组	**peer** { *group-name* | *peer-address* } **enable**
去激活对等体/对等体组	**undo peer** { *group-name* | *peer-address* } **enable**

缺省情况下，对等体或对等体组是激活的。

15. 配置 BGP 的 MD5 认证

BGP 对等体/对等体组之间需要建立并保持 TCP 连接，为提高 BGP 的安全性，可以配置在建立 TCP 连接时进行 MD5 认证，如果认证失败，则不能建立 TCP 连接。BGP 的 MD5 认证功能并不对 BGP 报文进行认证，它只是为 TCP 连接设置一个 MD5 认证密码，由 TCP 完成认证。

表6-17 配置 BGP 的 MD5 认证

操作	命令
配置对等体/对等体组的 MD5 认证	**peer** { *group-name* | *peer-address* } **password** { **cipher** | **simple** } *password*
取消 MD5 认证	**undo peer** { *group-name* | *peer-address* } **password**

缺省情况下，BGP 在建立 TCP 连接时，不进行 MD5 认证。

MD5 认证命令可以在 BGP 视图或 MBGP 的 VPN-instance 地址族视图下配置。当在 BGP 视图下配置时，对 MBGP 的组播扩展和 MBGP 的 VPN 扩展同样有效，因为这三者使用同一条 TCP 连接。

16. 配置禁止 BGP 对等体/对等体组发起或接收 BGP 连接

表6-18 禁止 BGP 对等体/对等体组发起或接收 BGP 连接

操作	命令
禁止 BGP 对等体/对等体组发起或接收 BGP 连接	**peer** { *group-name* | *peer-address* } **shutdown**
恢复缺省设置	**undo peer** {*group-name* | *peer-address* } **shutdown**

缺省情况下，允许对等体/对等体组发起或接收 BGP 连接。

6.2.4 配置 BGP 对等体/对等体组的路由过滤

请在 BGP 视图下进行下面配置。

1. 指定对等体/对等体组的路由策略

对等体组的成员必须与所在的组使用相同的出方向路由更新策略，但入方向的策略可以不同。即，对外发布路由时，一个对等体组遵循的策略是相同的，而在接收路由时，各对等体可以选择自己的策略。

表6-19 指定对等体/对等体组的路由策略

操作	命令
配置 BGP 对从对等体/对等体组接收到的路由应用路由策略	**peer** { *group-name* | *peer-address* } **route-policy** *policy-name* **import**
取消该路由策略	**undo peer** { *group-name* | *peer-address* } **route-policy** *policy-name* **import**
配置 BGP 对向对等体/对等体组发送的路由应用路由策略	**peer** *group-name* **route-policy** *policy-name* **export**
取消该路由策略	**undo peer** *group-name* **route-policy** *policy-name* **export**

缺省情况下，不对接收及发送的路由应用路由策略。

2. 配置对等体/对等体组的基于 IP 访问控制列表的路由过滤策略

表6-20 配置对等体/对等体组的基于 IP 访问控制列表的路由过滤策略

操作	命令
配置 BGP 基于访问控制列表过滤从对等体/对等体组收到的路由	**peer** { *group-name* | *peer-address* } **filter-policy** *acl-number* **import**
取消对接收路由的过滤	**undo peer** { *group-name* | *peer-address* } **filter-policy** *acl-number* **import**
配置 BGP 基于访问控制列表过滤向对等体组发布的路由	**peer** *group-name* **filter-policy** *acl-number* **export**
取消对发布路由的过滤	**undo peer** *group-name* **filter-policy** *acl-number* **export**

缺省情况下，不对接收及发布的路由进行过滤。

3. 配置对等体/对等体组的基于 AS 路径列表的路由过滤策略

表6-21 配置对等体/对等体组的基于 AS 路径列表的过滤策略

操作	命令
配置 BGP 基于 AS 路径列表过滤从对等体/对等体组收到的路由	**peer** { *group-name* | *peer-address* } **as-path-acl** *number* **import**
取消对接收路由的过滤	**undo peer** { *group-name* | *peer-address* } **as-path-acl** *number* **import**
配置 BGP 基于 AS 路径列表过滤向对等体组发布的路由	**peer** *group-name* **as-path-acl** *number* **export**
取消对发布路由的过滤	**undo peer** *group-name* **as-path-acl** *number* **export**

缺省情况下，不对接收及发布的路由进行过滤。

4. 配置对等体/对等体组的基于前缀列表的路由过滤策略

表6-22 配置对等体/对等体组的基于前缀列表的路由过滤策略

操作	命令
配置 BGP 基于地址前缀列表过滤从对等体/对等体组收到的路由	**peer** { *group-name* | *peer-address* } **ip-prefix** *prefixname* { **import** | **export** }
取消对接收路由的过滤	**undo peer** { *group-name* | *peer-address* } **ip-prefix** *prefixname* { **import** | **export** }
配置 BGP 基于地址前缀列表过滤向对等体组发布的路由	**peer** *group-name* **ip-prefix prefixname export**
取消对发布路由的过滤	**undo peer** *group-name* **ip-prefix prefixname export**

缺省情况下，不对接收及发布的路由进行过滤。

6.2.5 取消 IGP 和 IBGP 路由同步

请在 BGP 视图、VPN 实例视图下进行下面配置。

表6-23 配置取消 IGP 和 IBGP 路由同步

操作	命令
配置取消 IGP 和 IBGP 路由同步	**undo synchronization**

6.2.6 配置 BGP 定时器

当对等体间建立了 BGP 连接后，它们定时向对端发送 Keepalive Message，以防止路由器认为 BGP 连接已中断。若路由器在设定的连接保持时间（Holdtime）内未收

到对端的 Keepalive Message 或任何其它类型的报文，则认为此 BGP 连接已经被中断，从而退出此 BGP 连接，并对从此 BGP 连接收到的路由进行相应的处理。因此，发送 Keepalive Message 的间隔时间和 BGP 连接保持时间是 BGP 机制中两个非常重要的参数。

BGP 路由器和它的对等体在建立 BGP 连接时，需要进行协商，协商得到的保持时间为该 BGP 路由器的保持时间、对等体的保持时间中时间较小的那个保持时间。如果保持时间协商结果为 0，则不发送 keepalive Message，且不再检测 Holdtime 是否超时。

请在 BGP 视图下进行下列配置。

表6-24 配置 BGP 定时器

操作	命令
配置 BGP 定时器	**timer keep-alive** *keepalive-interval* **hold** *holdtime-interval*
恢复定时器的缺省值	**undo timer**

合理的最大 keepalive message 发送间隔为 Hold-time 的三分之一，且该发送间隔不能小于 1 秒，因此，如果配置 Holdtime 不为 0，则至少为 3 秒。

缺省情况下，发送 keepalive 的时间间隔为 60 秒；保持定时器时间为 180 秒。

6.2.7 配置本地优先级

可通过配置不同的本地优先级来影响 BGP 的路由选择。当一个运行 BGP 的路由器通过不同的内部对等体（Internal Peer）得到目的地相同、下一跳不同的路由时，将选取本地优先级最高的路由。

请在 BGP 视图下进行下列配置。

表6-25 配置本地优先级

操作	命令
配置本地优先级	**default local-preference** *value*
恢复缺省的本地优先级	**undo default local-preference**

本地优先级只在 IBGP 对等体之间交换 Update 报文时发送，不发送到本自治系统之外。

缺省情况下，本地优先级的值为 100。

6.2.8 配置自治系统的 MED 值

多出口区分 MED（Multi-Exit Descriminators）属性是路由的外部路由权（Cost），它在自治系统之间交换，但进入自治系统的 MED 不会再发送到该自治系统以外。

自治系统使用本地优先级属性来进行出自治系统的路由选择；而 MED 属性用于判断进入自治系统的最佳路由，当一个运行 BGP 的路由器通过不同的外部对等体（External Peer）得到目的地相同、下一跳不同的多条路由时，在其它条件相同的情况下，将选择 MED 值较小者作为自治系统的优选路由。

请在 BGP 视图下进行下列配置。

表6-26 配置系统的 MED 值

操作	命令
配置系统的 MED 值	**default med** *med-value*
恢复系统缺省的 MED 值	**undo default med**

上述配置的路由器只比较来自同一 AS 中的不同 EBGP 对等体的路由的 MED 值，如果要比较来自不同自治系统的对等体的路由的 MED 值，需要使用 **compare-different-as-med** 命令。

缺省情况下，MED 值为 0。

6.2.9 比较来自不同 AS 邻居路径的 MED 值

该命令用于选择最佳路径。在其它条件相同的情况下，MED 较小的路由被优选作为自治系统的外部路由。

请在 BGP 视图下进行下列配置。

表6-27 比较来自不同 AS 邻居路径的 MED 值

操作	命令
比较来自不同 AS 邻居路径的 MED 值	**compare-different-as-med**
禁止比较来自不同 AS 邻居路径的 MED 值	**undo compare-different-as-med**

缺省情况下，不允许比较来自不同 AS 邻居路径的 MED 属性值。

除非能够确认不同的自治系统采用了同样的 IGP 和路由选择方式，否则不要使用该配置。

6.2.10 配置 BGP 团体属性

团体属性是一个可选过渡属性，某些团体属性是公认的，具有全球意义，一般称为标准的团体属性，某些则是用于特殊用途，用户也可以定义扩展的团体属性。

团体属性列表是标识一个团体信息的列表，可分为标准团体访问列表（Standard-community-list）与扩展团体访问列表（Extended-community-list）两种。

此外，一条路由也可以有一个以上的团体属性。在一条路由中多个团体属性的发言者可以按照一个、几个或全部属性行动。路由器在传递路由到其它对等体之前可以选择是否改变团体属性。

请在系统视图下进行下列配置。

表6-28 配置团体属性

操作	命令
配置标准团体列表	**ip community-list** *standard-community-list-number* { **permit** | **deny** } { *aa:nn* | **internet** | **no-export-subconfed** | **no-advertise** | **no-export** }
配置扩展团体列表	**ip community-list** *extended-community-list-number* { **permit** | **deny** } *as-regular-expression*
取消配置的团体列表	**undo ip community-list** { *standard-community-list-number* | *extended-community-list-number* }

缺省情况下，未配置 BGP 团体属性。

标准团体访问列表的取值范围为 1～99，扩展团体访问列表的取值为 100～199。

6.2.11 配置 BGP 路由聚合

BGP 支持 CIDR 路由，支持路由聚合。BGP 路由聚合有两种方式：自动聚合 **summary** 与手动聚合 **aggregate**。自动聚合 **summary** 是对 BGP 引入的 IGP 子网路由进行聚合。配置 **summary** 后，BGP 将不能接收从 IGP 引入的子网路由。手动聚合 **aggregate** 是对 BGP 本地路由进行的聚合。在手动聚合方式下可配置一系列参数。通常情况下，手动聚合的优先级要比自动聚合的优先级高。

请在 BGP 视图下进行下列配置。

表6-29 配置 BGP 路由聚合

操作	命令
配置子网路由自动聚合功能	**summary**
取消子网路由自动聚合功能	**undo summary**
配置本地路由聚合功能	**aggregate** *address mask* [**as-set**] [**detail-suppressed**] [**suppress-policy** *route-policy-name*] [**origin-policy** *route-policy-name*] [**attribute-policy** *route-policy-name*]
取消本地路由聚合功能	**undo aggregate** *address mask* [**as-set**] [**detail-suppressed**] [**suppress-policy** *route-policy-name*] [**origin-policy** *route-policy-name*] **attribute-policy** *route-policy-name*]*policy-name*] [**attribute-policy** *policy-name*]

缺省情况下，BGP 不对子网及本地路由进行聚合。

6.2.12 配置 BGP 协议的优先级

每一种路由协议都有自己的优先级（preference），协议的优先级将最后决定路由策略采用哪种路由协议获取的路由作为最佳路由。优先级的数值越大，其实际的优先级越低。BGP 有三种路由：从外部对等体学到的路由，从内部对等体学到的路由及本地产生的路由。这三种路由的优先级可以是不同的，可以分别针对这三种路由手工设定 BGP 的优先级。

支持为不同的子地址族设置不同的 BGP 优先级，目前支持单播地址族和组播地址族。

请在 BGP 视图或 BGP 组播地址族视图下进行下列配置。

表6-30 设定协议的优先级

操作	命令
设定 BGP 协议的优先级	**preference** *value1 value2 value3*
恢复 BGP 协议优先级的缺省值	**undo preference**

value1 为从 EBGP 邻居收到的路由的优先级，*value2* 为从 IBGP 邻居收到的路由的优先级，*value3* 为本地产生的路由的优先级，取值范围均为 1～256。缺省情况下，*value1*、*value2*、*value3* 的值分别为 256、256、130。

6.2.13 配置 BGP 路由反射器

为保证 IBGP 对等体之间的连通性，IBGP 对等体之间需要建立全闭合网。在某些网络中，IBGP 对等体数目很多，内部 BGP 网络变得非常大，建立全闭合网开销很大。这就要求使用新的对等技术。路由反射器概念的基本思路是：指定一个集中路由器作为内部对话的焦点。多个 BGP 路由器可以与一个中心点对等化，然后多个路由反射器再进行对等化。

路由反射器作为其它路由器的集中点，其它路由器就称为客户机。客户机与路由反射器对等并与其交换选路信息。路由反射器会依次在客户机之间传递（或称反射）信息。

在下图中，Router A 从外部对等体收到一个更新信息并把它传递到 Router C。Router C 被配置成路由反射器，它有两个客户机：Router A 和 Router B。

Router C 把更新信息从客户机 Router A 反射给客户机 Router B。在这种配置下，实际并不需要 Router A 和 Router B 之间的对等对话，因为路由反射器会把 BGP 信息转给 Router B。

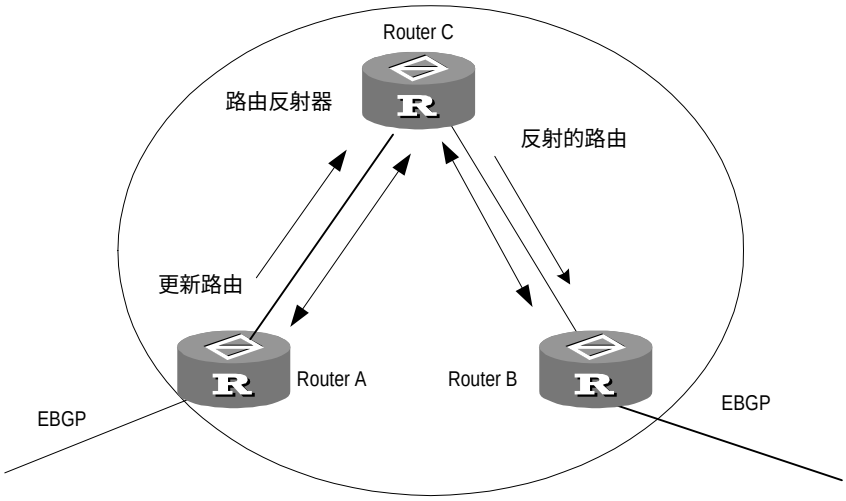


图6-1 路由反射器示意图

反射器是可以完成路由反射功能的路由器。路由反射器的 IBGP 对等体分为两类：客户机和非客户机。一个路由反射器和它的客户机构成一个群（Cluster）。在自治系统中不属于这个群的其它所有对等体就是非客户机。路由反射器的指定和客户机的加入是由命令 **peer reflect-client** 实现的。

非客户机与路由反射器之间，以及非客户机互相之间必须组成闭合网，因为它们遵循 IBGP 闭合网的基本规则。客户机不应与其相关群之外的 IBGP 建立对等。路由反射功能只在路由反射器上完成，所有的客户机和非客户机都是常规的 BGP 对等体，与路由反射器的功能无关。客户机所以被看成是客户机仅仅是因为路由反射器把它们列为客户机。

1. 配置客户到客户的路由反射

请在 BGP 视图下进行下列配置。

表6-31 配置客户到客户的路由反射

操作	命令
允许客户到客户的路由反射	**reflect between-clients**
禁止客户到客户的路由反射	**undo reflect between-clients**

缺省情况下，禁止客户到客户的路由反射。

2. 配置路由反射器

通常一个群中有一个路由反射器，该群由路由反射器的路由器 ID 来识别。

请在 BGP 视图下进行下列配置。

表6-32 配置路由反射器的群 ID

操作	命令
配置路由反射器的群 ID	**reflector cluster-id** { *cluster-id* | *address* }
取消路由反射器的群 ID	**undo reflector cluster-id**

3. 两种在自治系统内部避免循环的措施

随着路由反射器的引入，就有自治系统内产生选路循环的可能性。离开一个群的选路更新报文可能会试图回到这个群中。传统的 AS 路径方法不能探测到 AS 内部的循环，因为选路更新报文尚未离开 AS。BGP 在配置路由反射器时，提供了下述两种在 AS 内部避免循环的措施：

(1) 配置路由反射器的始发者 ID

始发者 ID（Originator_ID）如果配置不当，更新报文回到始发者，始发者会放弃它。

此项参数无须配置，在启动 BGP 时自动发挥作用。

(2) 配置路由反射器的群 ID

6.2.14 配置 BGP 自治系统联盟属性

联盟是处理 AS 内部的 IBGP 网络连接激增的另一种方法，它将一个自治系统划分为若干个子自治系统，每个子自治系统内部的 IBGP 对等体全连接，并同联盟中其它的子自治系统建立连接。

联盟的缺陷是：从非联盟向联盟方案转变时，要求路由器重新进行配置，逻辑拓扑基本上也要改变；而且，若没有手工设置的 BGP 策略，通过联盟的选路有可能选不到最佳的路径。

1. 配置联盟 ID

在不属于联盟的 BGP 发言者看来，属于同一个联盟的多个子自治系统是一个整体，外界不需要了解内部的子自治系统情况，联盟 ID 就是标识联盟这一整体的自治系统号。

请在 BGP 视图下进行下列配置。

表6-33 配置联盟的 ID

操作	命令
配置联盟的 ID	**confederation id** *as-number*
取消联盟的 ID	**undo confederation id**

缺省情况下，未配置联盟的 ID 号。

在配置联盟的 ID 号时，不能够与已经存在的自治系统号相同。

2. 配置属于联盟的子自治系统

请先配置联盟 ID，再配置属于联盟的子自治系统。一个联盟最多可包括 32 个子自治系统。配置属于联盟的子自治系统时使用的 *as-number* 联盟内部有效。

请在 BGP 视图下进行下列配置。

表6-34 配置属于联盟的子自治系统

操作	命令
配置属于联盟的子自治系统	**confederation peer-as** *as-number-1* [*... as-number-n*]
删除属于联盟的子自治系统	**undo confederation peer-as** [*as-number-1*] [*...as-number-n*]

缺省情况下，未配置属于联盟的子自治系统。

配置联盟子自治系统号时，所配置的子自治系统号不能够与没有配置对等体组自治系统号下的某个对等体的自治系统号相同。

3. 配置可同非标准兼容的自治系统联盟属性

如果需要与实现机制不同于 RFC1965 的设备互通，必须对联盟中所有的此类路由器进行配置。

请在 BGP 视图下进行下列配置。

表6-35 配置可同非标准兼容的自治系统联盟属性

操作	命令
配置可同非标准兼容的自治系统联盟属性	**confederation nonstandard**
撤消同非标准兼容的自治系统联盟	**undo confederation nonstandard**

缺省情况下，配置的联盟与 RFC1965 一致。

6.2.15 配置 BGP 路由衰减

路由不稳定性的主要可能原因是以前存在于路由表的一条路由间歇性的消失和重现，这种情况称为摆动（flapping）。摆动发生时，update 报文在网络上反复传播，会占用极大的带宽和路由器的处理时间，应尽力避免这种情况的发生。控制路由不稳定的技术是路由衰减。

衰减把路由分为稳定和不稳定两类，不稳定的路由应该被抑制（不被通告）。路由的历史表现是评估未来稳定性的基础。每当路由发生摆动，就给与惩罚，当惩罚达到一个预定的门限时，路由被抑制。随着时间推移，惩罚值按照幂函数递减，下降到一个门限时，路由解除抑制，被重新通告。

请在 BGP 视图下进行下列配置。

表6-36 配置 BGP 路由衰减

操作	命令
配置 BGP 路由衰减	**dampening** [*half-life-reachable half-life-unreachable reuse suppress ceiling*] [**route-policy** *route-policy-name*]
清除路由摆动衰减信息及解除对已抑制路由的抑制	**reset dampening** [*network-address* [*mask*]]
取消 BGP 路由衰减	**undo dampening**

缺省情况下，未配置 BGP 路由衰减。

需要注意的是：命令中各参数相互依存，若配置了任何一个，那么也必须指定其它参数。

dampening 命令只对从 EBGP 邻居学到的路由进行衰减，对 IBGP 路由不进行衰减。

6.2.16 配置 BGP 与 IGP 的交互

BGP 可以向其它的自治系统发送本自治系统的内部网络的信息。为了达到此目的，可以将本地路由器通过 IGP 路由协议得到的关于本系统内部的网络信息通过 BGP 发送出去。

请在 BGP 视图下进行下列配置。

表6-37 引入 IGP 协议的路由信息

操作	命令
配置 BGP 引入 IGP 协议的路由	**import-route** *protocol* [*process-id*] [**med** *med*] [**route-policy** *route-policy-name*]
取消 BGP 引入 IGP 协议的路由	**undo import-route** *protocol*
将本地的默认路由引入 BGP 中	**default-route imported**
禁止将本地的默认路由引入 BGP 中	**undo default-route imported**

缺省情况下，BGP 将不引入其它协议的路由。

protocol 指定可引入的源路由协议，目前可为 direct、static、rip、isis、ospf、ospf-ase 和 ospf-nssa。

有关引入路由信息的详细描述请参见“ IP 路由策略配置 ”中“ 引入其它协议路由 ”部分。

6.2.17 配置本地 AS 号的重复次数

该命令可配置本地 AS 号的重复次数。

请在 BGP 视图、VPNv4 视图、VPN 实例视图下进行下列配置。

表6-38 配置 as-path 的重复次数

操作	命令
配置本地 AS 号的重复次数	**peer** { *group-name* | *peer-address* } **allow-as-loop** [*number*]
取消配置本地 AS 号的重复次数	**undo peer** { *group-name* | *peer-address* } **allow-as-loop**

缺省情况下，*number* 取值为 3。

6.2.18 定义访问控制列表、AS 路径列表和 Route-policy

访问控制列表（access-control-list）、AS 路径列表和 Route-policy 均可以作为 BGP 过滤的条件。

1. 定义访问控制列表

请参见本手册的“ 安全 ”之“ 防火墙配置 ”部分。

2. 定义 AS 路径列表

BGP 的路由信息包中，包含一自治系统路径域。可以使用 as-path-acl 匹配 BGP 路由信息的自治系统路径域，过滤掉不符合条件的路由信息。对于相同的列表号，用户可以定义多条 as-path-acl，也即一个列表号代表一组 as-path 访问列表。每个 AS 路径列表是用数字来标识的。

请在系统视图下进行下列配置。

表6-39 配置自治系统的正则表达式

操作	命令
配置一个 AS 的正则表达式	**ip as-path-acl** *aspath-acl-number* { **permit** | **deny** } *as-regular-expression*
取消定义的正则表达式	**undo ip as-path-acl** *aspath-acl-number*

缺省情况下，未定义自治系统的正则表达式。

在匹配过程中，AS 访问列表号 *aspath-acl-number* 之间是一种“ 或 ”的关系，即路由信息通过这组列表中的一条就意味着通过由该列表号标识的这组 as-path 列表的过滤。

3. 定义 Route-policy

第一步：定义 Route-policy，请参见“ IP 路由策略配置 ”中的“ 定义 Route-policy ”部分。

第二步 :定义匹配规则，请参见“ IP 路由策略配置 ”中的“ 定义 Route-policy 的 if-match 子句 ”部分。

第三步 :定义赋值规则，请参见“ IP 路由策略配置 ”中的“ 定义 Route-policy 的 apply 子句 ”部分。

6.2.19 配置 BGP 路由过滤

1. 配置 BGP 对接收的路由信息进行过滤

请在 BGP 视图下进行下列配置。

可对 BGP 引入的路由进行过滤，只有满足某些条件的路由才能被 BGP 引入。

表6-40 配置对引入路由的过滤

操作	命令
配置对引入的路由进行过滤	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] } **import**
取消对引入的路由进行过滤	**undo filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] } **import**

更详细描述请参见“ IP 路由策略配置 ”的“ 配置路由过滤 ”部分。

2. 配置 BGP 对发布的路由信息进行过滤

可对 BGP 发布的路由进行过滤，只有满足某些条件的路由才能被 BGP 发布。

请在 BGP 视图下进行下列配置。

表6-41 配置 BGP 对发布路由的过滤

操作	命令
配置对发布的路由进行过滤	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol*]
取消对发布的路由进行过滤	**undo filter-policy** *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol*]

缺省情况下，BGP 不对接收和发布的路由信息进行过滤。

protocol 指定发布路由信息的协议，目前可包括：direct、static、rip、isis、ospf、ospf-ase 和 ospf-nssa。

更详细的描述请参见“ IP 路由策略配置 ”的“ 配置路由过滤 ”部分。

6.2.20 配置 BGP 负载分担

在实现方法上，BGP 的负载分担与 IGP 的负载分担有所不同：

IGP 是通过协议定义的路由算法，对到达同一目的地址的不同路由，根据计算结果，将度量值（metric）在相等的（如 RIP、OSPF）路由进行负载分担，选择的标准很明确（按 metric）。

BGP 本身并没有路由计算的算法，它只是一个选路的路由协议，因此，不能根据一个明确的度量值决定是否对路由进行负载分担，但 BGP 有丰富的选路规则，可以在对路由进行一定的选择后，有条件的进行负载分担，也就是将负载分担加入到 BGP 的选路规则中去。

VRP 支持 BGP 负载分担，当配置了 BGP 负载分担后，BGP 在选择路由时，在最后两条选路规则“优选从 EBGP 学来的路由”和“优选 BGP ID 最低的路由器发布的路由”之间增加一条规则：如果配置了负载分担，并且有多条到达同一 AS 或 AS 联盟的外部路由，则根据配置的路由条数选择多条路由进行负载分担。BGP 负载分担遵循以下规则：

- BGP 只对从 EBGP 学来的路由进行负载分担；
- BGP 只对来自同一 AS，且 med 值相同的路由进行负载分担；
- BGP 只对 AS_PATH 属性和 origin 属性（IGP、EGP、INC）完全相同的路由进行负载分担。

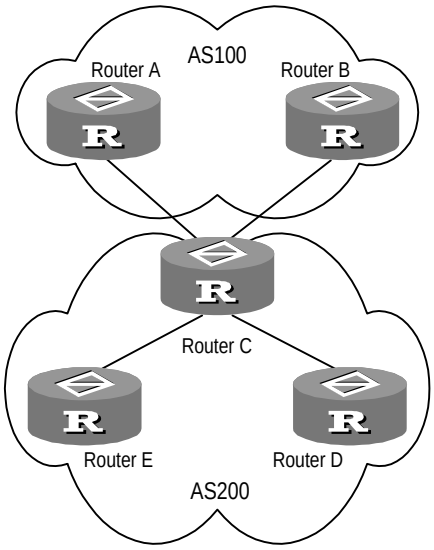


图6-2 BGP 负载分担示意图

在上图中，RouterD 和 RouterE 是 Router C 的 IBGP 对等体。当 RouterA 和 RouterB 同时向 RouterC 通告到达同一目的地的路由时，如果用户在 RouterC 配置了负载分担（如 balance 2），则在满足一定的选路规则后，并且两条路由具有相同的 AS_PATH 属性，RouterC 就将接收的两条路由同时加入到转发表中，实现 BGP 路由的负载分担。RouterC 只向 RouterD 和 RouterE 转发一次该路由，AS_PATH 不变，但

NEXT_HOP 属性改变为 RouterC 的地址，而不是原来的 EBGP 对等体地址。其它的 BGP 过渡属性将按最佳路由的属性传递。

BGP 负载分担特性同样适用于联盟内部的自治系统之间。

请在 BGP 视图下进行下列配置。

表6-42 配置 BGP 负载分担

操作	命令
配置 BGP 负载分担	**balance** *num*
取消 BGP 负载分担	**undo balance**

缺省情况下，BGP 不进行负载分担。

6.2.21 复位 BGP 连接

用户改变 BGP 的策略或协议配置后，必须切断当前 BGP 连接，使新的配置生效。

请在用户视图下进行下列配置。

表6-43 复位 BGP 的连接

操作	命令
复位 BGP 与特定对等体间的连接	**reset bgp** *peer-address* [**vpn-instance** *vpn-instance-name*]
复位所有的 BGP 连接	**reset bgp all** [**vpn-instance** *vpn-instance-name*]
复位指定对等体组中的所有成员的 BGP 连接	**reset bgp group** *group-name* [**vpn-instance** *vpn-instance-name*]

6.3 BGP 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 BGP 的运行情况，用户可以通过查看显示信息验证配置的效果。在用户视图下执行 **debugging** 命令可对 BGP 进行调试。

表6-44 BGP 显示和调试

操作	命令
查看 BGP 路由表中的信息	**display bgp** [**multicast** | **vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }] **routing-table** [*ip-address mask*]
查看 BGP 路由表中的路由统计信息	**display bgp** [**multicast** | **vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }] **routing-table statistic**

操作	命令
查看 BGP 中 AS 路径列表信息	**display ip as-path-acl** *aspath-acl-number*
查看 CIDR 路由	**display bgp** [**multicast** | [**vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }]] **routing-table cidr**
查看指定 BGP 团体的路由信息	**display bgp** [**multicast** | [**vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }]] **routing-table community** [*aa:nn* | **internet** | **no-export-subconfed** | **no-advertise** | **no-export**] [**whole-match**]
查看指定 BGP 团体列表允许的路由	**display bgp** [**multicast** | [**vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }]] **routing-table community-list** *community-list-number* [**whole-match**]
查看 BGP 衰减的路由	**display bgp routing-table dampened**
显示 BGP 对等体通告或者收到的路由信息	**display bgp routing-table peer** *peer-address* { **advertised** | **received** }
显示从 peer 收到的衰减路由信息	**display bgp routing-table peer** *peer-address* **dampened** [**statistic** | *ip-address*]
显示从 peer 收到的匹配正则表达式的路由信息	**display bgp routing-table peer** *peer-address* **regular-expression** *text*
查看与指定 **access-list** 相匹配的路由	**display bgp** [**multicast** | [**vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }]] **routing-table as-path-acl** *aspath-acl-number*
查看路由摆动统计信息	**display bgp routing-table flap-info** [**regular-expression** *as-regular-rexpession* | **as-path-acl** *aspath-acl-number* | *address* [*mask* [**longer-prefix-list**]]]
查看源 AS 不一致的路由	**display bgp** [**multicast**] **routing-table different-origin-as**
查看对等体信息	**display bgp** [**multicast** | [**vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }]] **peer** [[*peer-address*] **verbose**]
查看已经配置的路由信息	**display bgp** [**multicast** | [**vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }]] **network**
查看 AS 路径信息	**display bgp paths** *as-regular-expression*
查看对等体组信息	**display bgp** [**multicast** | [**vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }]] **routing-table group** [*group-name*]
查看匹配 AS 正则表达式的 AS 路径	**display bgp** [**multicast** | [**vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }]] **routing-table regular-expression** *as-regular-expression*
查看配置的 Route-policy 信息	**display route-policy** *route-policy-name*
打开 BGP 邻接状态变化的输出开关（BGP 视图）	**log-peer-change**

操作	命令
关闭 BGP 邻接状态变化的输出开关（BGP 视图）	**undo log-peer-change**
打开/关闭 BGP 所有报文调试信息开关	[**undo**] **debugging bgp all**
打开/关闭 BGP 事件调试信息开关	[**undo**] **debugging bgp event**
打开/关闭 BGP 一般运行信息调试开关	[**undo**] **debugging bgp normal**
打开/关闭 BGP Keepalive 调试信息开关	[**undo**] **debugging bgp keepalive** [**receive** | **send**] [**verbose**]
打开/关闭 MBGP Update 报文调试信息开关	[**undo**] **debugging bgp mp-update** [**receive** | **send**] [**verbose**]
打开/关闭 BGP Open 调试信息开关	[**undo**] **debugging bgp open** [**receive** | **send**] [**verbose**]
打开/关闭 BGP 包调试信息开关	[**undo**] **debugging bgp packet** [**receive** | **send**] [**verbose**]
打开/关闭 BGP 路由更新调试信息开关	[**undo**] **debugging bgp route-refresh** [**receive** | **send**] [**verbose**]
打开/关闭 BGP Update 报文调试信息开关	[**undo**] **debugging bgp update** [**receive** | **send**] [**verbose**]
显示被衰减的路由	**display bgp routing-table dampened**
显示所有路由的摆动统计信息	**display bgp routing-table flap-info**
清除所有路由的摆动统计信息	**reset bgp flap-info**
显示 AS 路径符合正则表达式的路由的摆动统计信息	**display bgp routing-table flap-info regular-expression** *as-regular-expression*
清除 AS 路径符合正则表达式的路由的摆动统计信息	**reset bgp flap-info regular-expression** *as-regular-expression*
显示通过 AS 过滤列表的路由的摆动统计信息	**display bgp routing-table flap-info as-path-acl** *aspath-acl-number*
清除通过 AS 过滤列表的路由的摆动统计信息	**reset bgp flap-info as-path-acl** *aspath-acl-number*
显示指定目的地址的路由的摆动统计信息	**display bgp routing-table flap-info** *network-address mask*
清除指定目的地址的路由的摆动统计信息	**reset bgp** *network-address* **flap-info**
显示比指定地址更具体的路由的摆动统计信息	**display bgp routing-table flap-info** *network-address mask* **longer-match**

6.4 BGP 典型配置举例

6.4.1 配置自治系统联盟属性

⚠ 注意：

配置用例中，只列出了与 BGP 配置相关的命令。

1. 组网需求

下图将自治系统 100 划分为 3 个子自治系统 1001，1002，1003，配置 EBGP、联盟 EBGP 和 IBGP。

2. 组网图

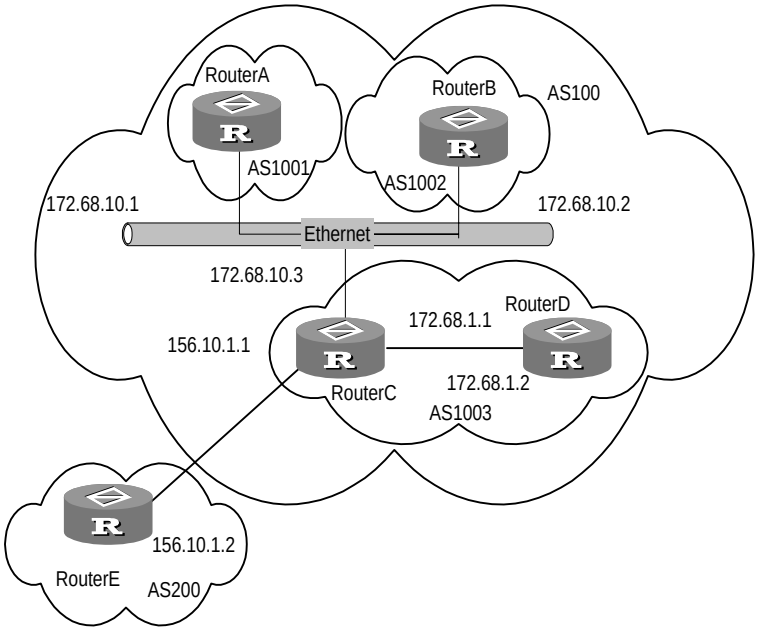


图6-3 配置自治系统联盟组网图

3. 配置步骤

(1) 配置 Router A

配置以太网接口。

```
[Router A] interface Ethernet0/0/0
[Router A-Ethernet0/0/0] ip address 172.68.10.1 255.255.255.0
```

配置 BGP。

```
[Router A] bgp 1001
[Router A-bgp] confederation id 100
```

```
[Router A-bgp] confederation peer-as 1002 1003
[Router A-bgp] undo synchronization
[Router A-bgp] group confed1002 external
[Router A-bgp] peer confed1002 as-number 1002
[Router A-bgp] peer 172.68.10.2 group confed1002
[Router A-bgp] group confed1003 external
[Router A-bgp] peer confed1003 as-number 1003
[Router A-bgp] peer 172.68.10.3 group confed1003
```

(2) 配置 Router B

配置以太网接口。

```
[Router B] interface Ethernet0/0/0
[Router B- Ethernet0/0/0] ip address 172.68.10.2 255.255.255.0
```

配置 BGP。

```
[Router B] bgp 1002
[Router B-bgp] confederation id 100
[Router B-bgp] undo synchronization
[Router B-bgp] confederation peer-as 1001 1003
[Router B-bgp] group confed1001 external
[Router B-bgp] peer confed1001 as-number 1001
[Router B-bgp] peer 172.68.10.1 group confed1001
[Router B-bgp] group confed1003 external
[Router B-bgp] peer confed1003 as-number 1003
[Router B-bgp] peer 172.68.10.3 group confed1003
```

配置 Router C：

配置以太网接口。

```
[Router C] interface Ethernet0/0/0
[Router C-Ethernet0/0/0] ip address 172.68.10.3 255.255.255.0
```

配置 BGP。

```
[Router C] bgp 1003
[Router C-bgp] confederation id 100
[Router B-bgp] undo synchronization
[Router C-bgp] confederation peer-as 1001 1002
[Router C-bgp] group confed1001 external
[Router C-bgp] peer confed1001 as-number 1001
[Router C-bgp] peer 172.68.10.1 group confed1001
[Router C-bgp] group confed1002 external
[Router C-bgp] peer confed1002 as-number 1002
 [Router C-bgp] peer 172.68.10.2 group confed1002
[Router C-bgp] group ebgp200 external
[Router C-bgp] peer 156.10.1.2 group ebgp200 as-number 200
```

```
[Router C-bgp] group ibgp1003 internal
[Router C-bgp] peer 172.68.1.2 group ibgp1003
```

6.4.2 配置 BGP 路由反射器

1. 组网需求

路由器 B 接收了一个经过 EBGP 的更新报文并将之传给路由器 C。路由器 C 被配置为路由反射器，它有两个客户：路由器 B 和路由器 D。 路由器 B 和路由器 D 间不需一个 IBGP 连接，当路由器 C 接收了来自路由器 B 的路由更新时，它将此信息反射给路由器 D，反之亦然。

2. 组网图

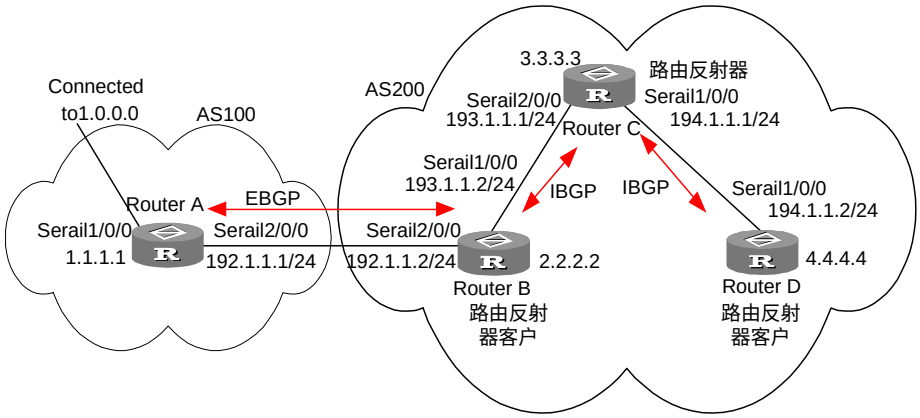


图6-4 配置 BGP 路由反射器组网图

3. 配置步骤

(1) 配置路由器 Router A

```
[Router A] interface serial 2/0/0
[Router A-Serial2/0/0] ip address 192.1.1.1 255.255.255.0
[Router A-Serial2/0/0] interface serial 1/0/0
[Router A-Serial1/0/0] ip address 1.1.1.1 255.0.0.0
[Router A-Serial1/0/0] quit
[Router A] bgp 100
[Router A-bgp] group ex external
[Router A-bgp] peer 192.1.1.2 group ex as-number 200
[Router A-bgp] network 1.0.0.0 255.0.0.0
```

(2) 配置路由器 Router B

```
[Router B] interface serial 2/0/0
[Router B-Serial2/0/0] ip address 192.1.1.2 255.255.255.0
[Router B-Serial2/0/0] interface serial 1/0/0
[Router B-Serial1/0/0] ip address 193.1.1.2 255.255.255.0
[Router B-Serial1/0/0] quit
```

```
[Router B] bgp 200
[Router B-bgp] group ex external
[Router B-bgp] peer 192.1.1.1 group ex as-number 100
[Router B-bgp] peer in next-hop-local
[Router B-bgp] group in internal
[Router B-bgp] peer 193.1.1.1 group in
```

配置路由器 RouterC：

```
[Router C] interface serial 2/0/0
[Router C-Serial2/0/0] ip address 193.1.1.1 255.255.255.0
[Router C-Serial2/0/0] interface serial 1/0/0
[Router C-Serial1/0/0] ip address 194.1.1.1 255.255.255.0
[Router C-Serial1/0/0] quit
[Router C] bgp 200
[Router C-bgp] group rr internal
[Router C-bgp] reflect between-clients
[Router C-bgp] peer rr reflect-client
[Router C-bgp] peer 193.1.1.2 group rr
[Router C-bgp] peer 194.1.1.2 group rr
```

配置路由器 Router D：

```
[Router D] interface serial 1/0/0
[Router D-Serial1/0/0] ip address 194.1.1.2 255.255.255.0
[Router D-Serial1/0/0] quit
[Router D] bgp 200
[Router D-bgp] group in internal
[RouterD-bgp] peer 194.1.1.1 group in
```

在路由器 B 上用命令 **display bgp routing-table**，可以看到路由器 B 已知道网络 1.0.0.0 的存在。

在路由器 D 上用命令 **display bgp routing-table**，可以看到路由器 D 也知道网络 1.0.0.0 的存在。

6.4.3 配置 BGP 负载分担

1. 组网需求

Router C 与 Router A、Router B 建立 EBGP 连接，与 Router D 建立 IBGP 连接。

分别在 Router A、Router B 中引入静态路由 9.0.0.0/8。要求 Router A 和 Router B 实现负载分担。

2. 组网图

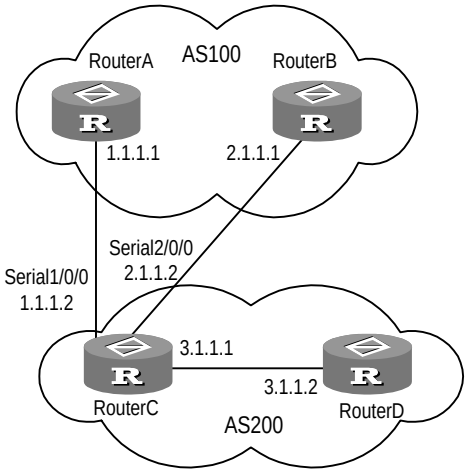


图6-5 BGP 负载分担组网图

3. 配置步骤

(1) 配置 Router A

```
[Router A] router id 11.1.1.1
[Router A] ip route-static 9.0.0.0 255.0.0.0 null0
[Router A] bgp 100
[Router A-bgp] group ex external
[Router A-bgp] peer 1.1.1.2 group ex as-number 200
[Router A-bgp] import-route static
```

(2) 配置 Router B

```
[Router B] router id 12.1.1.1
[Router B] ip route-static 9.0.0.0 255.0.0.0 null0
[Router B] bgp 100
[Router B-bgp] group ex external
[Router B-bgp] peer 2.1.1.2 group ex as-number 200
[Router B-bgp] import-route static
```

(3) 配置 Router C

```
[Router C] bgp 200
[Router C-bgp] group ex external
[Router C-bgp] peer ex as-number 100
[Router C-bgp] peer 1.1.1.1 group ex
[Router C-bgp] peer 2.1.1.1 group ex
[Router C-bgp] group in internal
[Router C-bgp] peer 3.1.1.2 group in
```

(4) 配置 Router D

```
[Router D] bgp 200
[Router D-bgp] group in internal
```

```
[Router D-bgp] peer 3.1.1.1 group in
```

在 Router C 上执行 **display bgp**，可以看到有两条 9.0.0.0/8 有效路由，其中一条是最佳路由。使用 **display ip routing-table** 可以看到，该最佳路由的下一跳为 1.1.1.1。

对 Router C 进行如下配置：

```
[RouterC] bgp 200
[RouterC-bgp] balance 2
```

此时，再在 Router C 上执行 **display ip routing-table**，可以看到路由表显示 BGP 路由 9.0.0.0/8 存在两个下一跳，分别是 1.1.1.1 和 2.1.1.1。

在 Router C 上执行 **display fib**，可以看到转发表中 9.0.0.0/8 的路由项有两个下一跳，分别是 1.1.1.1 和 2.1.1.1。

6.5 BGP 故障诊断与排除

故障之一：邻居关系不能建立（无法进入 Established 状态）。

故障排除：BGP 邻居的建立需要能够使用 179 端口建立 TCP 会话，以及能够正确交换 Open 报文。可按照以下步骤进行检查：

- 检查邻居的 AS 号配置是否正确。
- 检查邻居的 IP 地址是否正确。
- 如果使用 Loopback 接口，检查是否配置了 **connect-interface loopback**。缺省情况下，路由器使用最佳本地接口建立 TCP 连接，而不会用 loopback 接口。
- 如果是物理上非直连的 EBGP 邻居，检查是否配置了 **peer ebgp-max-hop**。
- 使用 ping 命令检查 TCP 连接是否正常，由于一台路由器可能有多个接口能够到达对端，应使用扩展的 **ping -a** *ip-address* 命令指定发送 ping 包的源 IP 地址。
- 如果 Ping 不通，使用 **display ip routing-table** 命令检查路由表中是否存在到邻居的可用路由。
- 如果能 Ping 通，检查是否配置了禁止 TCP 端口 179 的 ACL，如果有，取消对 179 端口的禁止。

6.6 MBGP 简介

6.6.1 MBGP 概述

正如本章开始所介绍的，BGP 作为事实上的外部网关协议，广泛应用于自治系统间的互联。传统的 BGP-4 只能管理 IPv4 的路由信息，对于使用其它网络层协议（如 IPv6 等）的应用，在跨自治系统传播时就会受到一定的限制。

为了提供对多种网络层协议的支持，IETF 对 BGP-4 进行了扩展，形成 MBGP（Multiprotocol Extensions for BGP-4，BGP-4 的多协议扩展），目前的 MBGP 标准是 RFC2858。

MBGP 是向后兼容的，也就是说，支持 BGP 扩展的路由器与不支持 BGP 扩展的路由器可以互通。

6.6.2 MBGP 的扩展属性

BGP-4 使用的报文中，与 IPv4 相关的三条信息都由 Update 报文携带，这三条信息分别是：NLRI（Network Layer Reachability Information，网络层可达性信息）、路径属性中的 Next_Hop（下一跳的 IP 地址）、路径属性中的 Aggregator（该属性中包含形成聚合路由的 BGP 发言者的 IP 地址）。

因特网上实际运行的 BGP 发言者通常都具有一个 IPv4 的地址，因此，BGP-4 只需要将特定网络层协议的信息反映到 NLRI 及路由属性中的 Next_Hop 即可实现对多种网络层协议的支持。

MBGP 中引入了两个新的路径属性：

- MP_REACH_NLRI：Multiprotocol Reachable NLRI，多协议可达 NLRI。用于发布可达路由及下一跳信息。
- MP_UNREACH_NLRI：Multiprotocol Unreachable NLRI，多协议不可达 NLRI。用于撤销不可达路由。

这两种属性都是可选非过渡（optional non-transitive）的，因此，不提供多协议能力的 BGP 发言者将忽略这两个属性的信息，不把它们传递给其它邻居。

6.6.3 路由器的 MBGP 应用

路由器采用地址族（Address Family）来区分不同的网络层协议，关于地址族的一些取值可以参考 RFC1700。

路由器提供多种 MBGP 扩展应用，包括对组播的扩展、对 BGP/MPLS VPN 的扩展等，不同的扩展应用需在各自的地址族视图下进行。

MBGP 在组播中的应用请参考本手册的“组播”之“MBGP 组播扩展配置”部分；在 BGP/MPLS VPN 中的应用请参考本手册的“MPLS”之“MPLS VPN 配置”部分。

6.7 MBGP 配置

MBGP 是对 BGP 的扩展，BGP 的很多概念和配置原理在 MBGP 中也同样适用。

在配置 MBGP 时，首先需要启动 BGP，再进入相应的地址族视图，配置不同的扩展应用的相关参数。

在配置 MBGP 对等体/对等体组时，首先在 BGP 视图下配置对等体或对等体组的 AS 号，再进入相应的地址族视图下激活该应用的对等体/对等体组关系。

BGP 视图下的部分命令在 MBGP 的地址族视图下也存在，但如果在 MBGP 的地址族视图下配置，则这些命令仅对相应的应用有效。

MBGP 地址族视图下的、与特定应用相关的命令不在本章进行介绍，相应的内容可参考本手册的“组播”和“MPLS”。

MBGP 的通用配置包括：

- 配置地址族
- 激活对等体组

6.7.1 配置地址族

在介绍了 MBGP 后，有时用 IPv4 单播地址族视图来指示通常意义上的 BGP 视图。

请在 BGP 视图下进行下列配置。

表6-45 配置地址族

操作	命令
进入 MBGP 的组播地址族视图	**ipv4-family multicast**
删除 MBGP 的组播地址族配置	**undo ipv4-family multicast**
进入 MBGP 的 vpn-instanc 地址族视图	**ipv4-family vpn-instance** *vpn-instance-name*
删除 MBGP 的 vpn-instanc 地址族配置	**undo ipv4-family vpn-instance** *vpn-instance-name*
进入 MBGP 的 VPNv4 地址族视图	**ipv4-family vpnv4** [**unicast**]
删除 MBGP 的 VPNv4 地址族配置	**undo ipv4-family vpnv4** [**unicast**]

执行 **undo** 命令后，将退回到 BGP 视图，并删除相应的 MBGP 扩展应用配置。

6.7.2 激活对等体/对等体组

BGP 发言者之间交换路由信息，必须首先将单播地址族下的某个对等体组激活，然后，再将单播地址族下已经存在的对等体加入到这个激活的对等体组中。

请在地址族视图下进行下列配置。

表6-46 激活对等体/对等体组

操作	命令
激活指定对等体组	**peer** *group-name* **enable**
去掉已激活的指定对等体组	**undo peer** *group-name* **enable**
将对等体加入激活的对等体组中	**peer** *peer-address* **group** *group-name*

操作	命令
将对等体从激活的对等体组中删除	**undo peer** *peer-address*

缺省情况下，只有 BGP 的 IPv4 单播地址族的对等体组才是激活的，其它类型的对等体或对等体组都是没有激活的，不能交换路由信息。

6.8 MBGP 的显示和调试

MBGP 的显示和调试请参考本手册的“ 组播配置 ”和“ MPLS 配置 ”，本章不再赘述。

6.9 MBGP 典型配置举例

MBGP 主要应用于对一些新业务的扩展，其本身的配置与 BGP 很相似，下面的例子与“ BGP 典型配置举例 ”中的例子在组网和配置上都基本一致，主要的不同在于进入 MBGP 的地址族视图，以及激活 MBGP 对等体。

如果需要了解 MBGP 在具体业务中的配置，请请参考本手册的“ 组播 ”和“ MPLS ”。

6.9.1 配置 MBGP 路由反射器

1. 组网需求

路由器 RouterA、RouterB、RouterC 和 RouterD 上都配置 MBGP 的组播扩展应用，RouterA 和 RouterB 是 EBGP 对等体，RouterC 和 RouterB、RouterC 和 RouterD 是 IBGP 对等体。

RouterB 接收了一个来自 RouterA 的 EBGP 更新报文并将之传给 RouterC。RouterC 被配置为路由反射器，它有两个客户：RouterB 和 RouterD。当 RouterC 接收到来自 RouterB 的 EBGP 更新报文时，它将此信息反射给 RouterD，RouterB 和 RouterD 间不需要建立 IBGP 连接，因为 RouterC 将反射信息给 RouterD。

2. 组网图

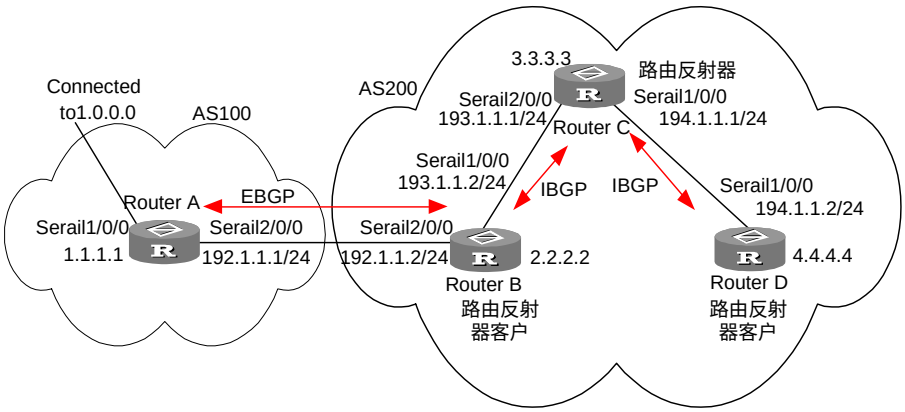


图6-6 配置 MBGP 路由反射器的组网图

3. 配置步骤

(1) 配置 Router A

配置接口。

```
[Router A] interface serial 2/0/0
[Router A-Serial2/0/0] ip address 192.1.1.1 255.255.255.0
[Router A-Serial2/0/0] quit
```

配置 Router A 的 MBGP。

```
[Router A] bgp 100
[Router A-bgp] group ex external
[Router A-bgp] peer 192.1.1.2 group ex as-number 200
[Router A-bgp] ipv4-family multicast
[Router A-bgp-af-mul] peer ex enable
[Router A-bgp-af-mu] peer 192.1.1.2 group ex
[Router A-bgp-af-mu] network 1.0.0.0 255.0.0.0
```

(2) # 配置 Router B

配置接口。

```
[Router B] interface serial 2/0/0
[Router B-Serial2/0/0] ip address 192.1.1.2 255.255.255.0
[Router B-Serial2/0/0] quit
[Router B] interface serial 1/0/0
[Router B-Serial1/0/0] ip address 193.1.1.2 255.255.255.0
[Router B-Serial1/0/0] quit
```

配置 OSPF。

```
[Router B] ospf
[Router B-ospf-1] area 0
[Router B-ospf-1-area-0.0.0.0] network 193.1.1.0 0.0.0.255
```

```
[Router B-ospf-1-area-0.0.0.0] quit
[Router B-ospf-1] quit
```

配置 Router B 的 MBGP。

```
[Router B] bgp 200
[Router B-bgp] group ex external
[Router B-bgp] peer 192.1.1.1 group ex as-number 100
[Router B-bgp] group in internal
[Router B-bgp] peer in next-hop-local
[Router B-bgp] peer 193.1.1.1 group in
[Router B-bgp] import-route ospf
[Router B-bgp] import-route direct
[Router B-bgp] ipv4-family multicast
[Router B-bgp-af-mul] peer in next-hop-local
[Router B-bgp-af-mul] peer ex enable
[Router B-bgp-af-mul] peer in enable
[RouterB-bgp-af-mul] peer 192.1.1.1 group ex
[RouterB-bgp-af-mul] peer 193.1.1.1 group in
```

(3) 配置 Router C。

配置接口。

```
[Router C] interface serial 2/0/0
[Router C-Serial2/0/0] ip address 193.1.1.1 255.255.255.0
[Router C-Serial2/0/0] quit
[Router C] interface serial 1/0/0
[Router C-Serial1/0/0] ip address 194.1.1.1 255.255.255.0
[Router C-Serial1/0/0] quit
```

配置 OSPF。

```
[RouterC] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 193.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

配置 Router C 的 MBGP。

```
[RouterC] bgp 200
[Router C-bgp] group in internal
[Router C-bgp] peer 193.1.1.2 group in
[Router C-bgp] peer 194.1.1.2 group in
[Router C-bgp] peer in reflect-client
[Router C-bgp] ipv4-family multicast
[Router C-bgp-af-mul] peer in enable
```

```
[Router C-bgp-af-mul] peer in reflect-client
[Router C-bgp-af-mul] peer 193.1.1.2 group in
[Router C-bgp-af-mul] peer 194.1.1.2 group in
```

- 配置 Router D

配置接口。

```
[Router D] interface serial 1/0/0
[Route D-Serial1/0/0] ip address 194.1.1.2 255.255.255.0
[Router D-Serial1/0/0] quit
```

配置 OSPF。

```
[Router D] ospf
[Router D-ospf-1] area 0
[Router D-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[Router D-ospf-1-area-0.0.0.0] quit
[Router D-ospf-1] quit
```

配置 Router D 的 MBGP：

```
[RouterD] bgp 200
[RouterD-bgp] group in internal
[RouterD-bgp] peer 194.1.1.1 group in
[RouterD-bgp] ipv4-family multicast
[RouterD-bgp-af-mul] peer in enable
[RouterD-bgp-af-mul] peer 194.1.1.1 group in
```

在 Router B 上用 **display bgp multicast routing-table** 查看 BGP 路由表。注意：Router B 已知道了网络 1.0.0.0 的存在。

在 Router D 上用 **display bgp multicast routing-table** 查看 BGP 路由表。注意：Router D 也知道网络 1.0.0.0 的存在。

第7章 IP 路由策略配置

7.1 IP 路由策略简介

路由器在发布与接收路由信息时，可能需要实施一些策略，以便对路由信息进行过滤，比如只接收或发布一部分满足给定条件的路由信息；一种路由协议（如 RIP）可能需要引入（import）其它的路由协议（如 OSPF）发现的路由信息，从而丰富自己的路由知识；路由器在引入其它路由协议的路由信息时，可能需要只引入一部分满足条件的路由信息，并对所引入的路由信息的某些属性进行设置，以使其满足本协议的要求。

为实现路由策略，首先要定义将要实施路由策略的路由信息的特征，即定义一组匹配规则，可以以路由信息中的不同属性作为匹配依据进行设置，如目的地址、发布路由信息的路由器地址等。匹配规则可以预先设置好，然后再将它们应用于路由的发布、接收和引入等过程的路由策略中。

在路由器中，提供了 Route-policy、acl、as-path、community-list 和 ip-prefix 五种过滤器供路由协议引用。下面对各种过滤器逐个进行介绍。

1. Route-policy

用于匹配给定路由信息的某些属性，并在条件满足后对该路由信息的某些属性进行设置。

一个 Route-policy 可以由多个节点（node）构成，每个节点是进行匹配测试的一个单元，节点间依据顺序号（node-number）进行匹配。每个节点可以由一组 **if-match** 和 **apply** 子句组成。**if-match** 子句定义匹配规则，匹配对象是路由信息的一些属性。同一节点中的不同 **if-match** 子句是“与”的关系，只有满足节点内所有 **if-match** 子句指定的匹配条件，才能通过该节点的匹配测试。**apply** 子句指定动作，也就是在通过节点的匹配测试后所执行的动作——对路由信息的一些属性进行设置。

一个 Route-policy 的不同节点间是“或”的关系，系统依次检查 Route-policy 的各个节点，如果通过了 Route-policy 的某一节点，就意味着通过该 Route-policy 的匹配测试（不进入下一个节点的测试）。

2. 访问控制列表（acl）

访问控制列表分为三类：**advanced**：表示高级访问控制列表；**basic**：表示基本访问控制列表；**interface**：表示基于接口的访问控制列表；。

在对路由信息过滤时，一般使用基本访问列表和高级访问控制列表。若使用基本访问控制列表，在定义访问列表时指定一个源 IP 地址或子网的范围，用于匹配路由信

息的源地址。如使用高级访问列表，则可以使用协议类型、源/目的地址或端口号等多种参数匹配路由信息。

acl 的有关配置请参考本手册安全部分的防火墙配置。

3. 前缀列表（ip-prefix）

前缀列表 ip-prefix 的作用类似于 acl，但比它更为灵活，且更易于为用户理解——ip-prefix 在应用于路由信息的过滤时，其匹配对象为路由信息的目的地址信息域；另外在 ip-prefix 中，用户可以指定 **gateway** 选项，指明只接收某些路由器发布的路由信息。

一个 ip-prefix 由前缀列表名标识。每个前缀列表可以包含多个表项，每个表项可以独立指定一个网络前缀形式的匹配范围，并用一个 index-number 来标识，index-number 指明了在 ip-prefix 中进行匹配检查的顺序。

在匹配的过程中，路由器按升序依次检查由 index-number 标识的各个表项，只要有某一表项满足条件，就意味着通过该 ip-prefix 的过滤（不会进入下一个表项的测试）。

4. 自治系统路径信息访问列表（as-path-acl）

自治系统路径信息访问列表 as-path 仅用于 BGP。BGP 的路由信息包中，包含有一自治系统路径域（在 BGP 交换路由信息的过程中，路由信息经过的自治系统路径会记录在这个域中）。as-path 就是针对自治系统路径域指定匹配条件。

as-path 的定义已经在 BGP 配置中实现，有关的配置请用户参考“ BGP 配置 ”中的“ **ip as-path-acl** ”命令。

5. 团体属性列表（community-list）

团体属性列表 community-list 仅用于 BGP。BGP 的路由信息包中，包含一个 community 属性域，用来标识一个团体。community-list 就是针对团体属性域指定匹配条件。

community-list 的定义已经在 BGP 配置中实现，有关的配置请用户参考 BGP 中的 **ip community-list** 命令。

7.2 IP 路由策略配置

路由策略可以通过两种方式来实现，一是通过过滤列表如 ACL、ip-prefix、as-path-acl、community-list 等，直接实现路由或路由属性的过滤；另一种是通过配置 Route-policy，对满足匹配条件的路由属性进行设置。

本章中的配置包括：

- 定义地址前缀列表

(1) 配置路由过滤

- 定义地址前缀列表或 ACL
- 配置对接收到的路由进行过滤
- 引入其它路由协议发现的路由（仅 OSPF 和 ISIS 路由过滤需要配置）
- 配置对发布的路由（对 OSPF 和 ISIS 指引入路由）进行过滤

(2) 通过 Route-policy 实现路由策略

- 定义 Route-policy
- 定义 Route-policy 的 **if-match** 子句
- 定义 Route-policy 的 **apply** 子句
- 通过 Route-policy 对引入的路由进行过滤

有关 BGP 通过 as-path-acl，community-list 实现的路由过滤，请参见 BGP 部分。

7.2.1 配置路由过滤

1. 定义过滤条件

(1) 定义地址前缀列表

一个 ip-prefix 由前缀列表名标识。每个前缀列表可以包含多个表项，每个表项可以独立指定一个网络前缀形式的匹配范围，并用一个 *index-number* 来标识，*index-number* 指明了在 ip-prefix 中进行匹配检查的顺序。

请在系统视图下进行下列配置。

表7-1 定义地址前缀列表

操作	命令
定义地址前缀列表	**ip ip-prefix** *ip-prefix-name* [**index** *index-number*] { **permit** | **deny** } *network len* [**greater-equal** *greater-equal* | **less-equal** *less-equal*]
取消地址前缀列表	**undo ip ip-prefix** *ip-prefix-name* [**index** *index-number* | **permit** | **deny**]

在匹配的过程中，路由器按升序依次检查由 *index-number* 标识的各个表项，只要有某一表项满足条件，就意味着通过该 ip-prefix 的过滤（不会进入下一个表项的测试）。

需要注意的是：

- 如果定义了一个以上的前缀列表表项，那么至少应该有一个表项的匹配模式是 **permit** 模式。
- **deny** 模式的表项可以先被定义以快速的过滤掉不符合条件的路由信息，但如果所有表项都是 **deny** 模式，则任何路由都不会通过该地址前缀列表的过滤。
- 可以在定义了多条 **deny** 模式的表项后定义一条 **permit** 0.0.0.0/0 **greater-equal** 0 **less-equal** 32 的表项以允许其它所有路由信息通过。

例如，按如下配置可以保证仅过滤掉 10.1.0.0，10.2.0.0，10.3.0.0 三个网段的路由，而其它网段的路由信息可以通过。

```
[Router] ip ip-prefix 1 deny 10.1.0.0 16
[Router] ip ip-prefix 2 deny 10.2.0.0 16
[Router] ip ip-prefix 3 deny 10.3.0.0 16
[Router] ip ip-prefix 4 permit 0.0.0.0/0 greater-equal 0 less-equal 32
```

(2) 定义访问控制列表

请参见安全部分。

2. 配置对接收的路由进行过滤

请在路由协议视图下进行下列配置。

定义一条策略规则，通过对一个 ACL 或地址前缀列表的引用实现在接收路由过程中对不满足条件的路由信息进行过滤。**gateway** 指定只接收来自特定邻居路由器的更新报文。

表7-2 配置对接收路由的过滤

操作	命令
配置对接收的指定地址发布的路由信息进行过滤	**filter-policy gateway** *ip-prefix-name* **import**
取消对接收的指定地址发布的路由信息进行过滤	**undo filter-policy gateway** *ip-prefix-name* **import**
配置对接收的全局路由信息进行过滤	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } [**gateway**] **import**
取消对接收的全局路由信息进行过滤	**undo filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } [**gateway**] **import**

filter-policy import 是对接收到的本路由协议（由所在的协议视图决定）的路由进行过滤，肯定都是邻居发来的，与引入路由没关系。

对于链路状态协议来说，它是在由 LSDB 生成路由表时进行过滤，因为无法对 LSA 进行过滤。

RIP 和 BGP 协议是对邻居发来的路由表直接过滤。

3. 引入其它路由协议发现的路由信息

路由协议可以引入其它路由协议发现的路由来丰富自己的路由知识。在引入其它协议路由信息时，可以通过 Route-policy 来进行路由信息的过滤，实现有选择的引入。进行引入操作的目标路由协议如果不能直接引用原路由协议的路由权值，需要为引入的路由指定一个路由权以满足本协议的要求。

请在路由协议视图下进行下列配置。

表7-3 引入其它协议路由

操作	命令
设置引入其它协议的路由	**import-route** *protocol* [**med** *med* | **cost** *cost*] [**tag** *value*] [**type 1** | **2**]
取消引入其它协议的路由的设置	**undo import-route** *protocol*

缺省情况下，不引入其它协议的路由信息。

📖 说明：

在不同的路由协议视图下，可选的参数也有所区别，具体情况请分别参考手册中相应路由协议的 **import-route** 命令。

4. 配置对发布的路由进行过滤

定义一条有关路由发布的策略规则，通过对一个 ACL 或地址前缀列表的引用实现在路由发布的过程中过滤不满足条件的路由信息，通过指定 *routing-process* 实现仅过滤发布的 *routing-process* 的路由信息。

请在路由协议视图下进行下列配置。

表7-4 配置对发布路由的过滤

操作	命令
配置对协议发布路由的过滤	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*routing-process*]
取消对协议发布路由的过滤	**undo filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*routing-process*]

filter-policy export 对 OSPF 和 ISIS 来说，是对引入的路由进行过滤，要与 **import-route** 命令结合使用，否则失效。它后面有个参数，可以对特定类型的引入路由信息进行过滤。如果没有指定，则对所有引入的路由进行过滤。

对 RIP 和 BGP 来说，即使没有 **import-route** 命令，它也会对路由表过滤，可以看作是对发布的路由进行过滤。

目前，路由策略支持将如下协议发现的路由接收到路由表中：

- direct：本机接口直接相连的网段（或主机）路由。
- static：静态配置的路由。
- rip：RIP 发现的路由。
- ospf：OSPF 协议发现的路由。
- ospf-ase：OSPF 协议发现的外部路由。
- ospf-nssa：OSPF 协议发现的 NSSA 区域路由。

- isis：IS-IS 协议发现的路由。
- bgp：BGP 获得的路由。

缺省情况下，不对接收与发布的路由进行过滤。

7.2.2 通过 Route-policy 实现路由策略

1. 定义 Route-policy

一个 Route-policy 可由多个节点构成，每个节点是进行匹配检查的一个单元，节点间依据顺序号 *sequence-number* 标识检查顺序。

请在系统视图下进行下列配置。

表7-5 定义 Route-policy

操作	命令
进入路由策略视图	**route-policy** *route-policy-name* { **permit** | **deny** } **node** *node-number*
删除指定的 Route-policy	**undo route-policy** *route-policy-name* [**permit** | **deny** | **node** *node-number*]

permit 指定所定义的 Route-policy 节点的匹配模式为允许模式。当路由项满足该节点的所有 **if-match** 子句时，认为通过该节点的过滤，并执行该节点的 **apply** 子句，不进入下一个节点的测试；如路由项不满足该节点的 **if-match** 子句，将进入下一个节点继续测试。

deny 指定所定义的 Route-policy 节点的匹配模式为拒绝模式（此模式下 **apply** 子句不会被执行），当路由项满足该节点的所有 **if-match** 子句时被拒绝通过该节点，不进入下一个节点的测试；如路由项不满足该节点的 **if-match** 子句，将进入下一个节点继续测试。

不同节点间是“或”的关系，即路由器依次检查 Route-policy 的各个节点，通过 Route-policy 的某一节点，就意味着通过该 Route-policy 过滤。

缺省情况下，未定义 Route-policy。

需要注意的是：如果定义了一个以上的 Route-policy 节点，Route-policy 的各个节点中至少应该有一个节点的匹配模式是 permit。当一个 Route-policy 用于路由信息过滤时，如果某路由信息没有通过任一节点，则认为该路由信息没有通过该 Route-policy。当 Route-policy 的所有节点都是 deny 模式时，所有路由信息都不会通过该 Route-policy。

2. 定义 Route-policy 的 if-match 子句

if-match 子句定义匹配准则，也就是路由信息通过当前 Route-policy 所需满足的过滤条件，匹配对象是路由信息的一些属性。

请在路由策略视图下进行下列配置。

表7-6 定义匹配条件

操作	命令
匹配 BGP 路由信息的 AS 路径域	**if-match as-path** *aspath-acl-number*
取消匹配 BGP 路由信息的 AS 路径域	**undo if-match as-path**
匹配 BGP 路由信息的团体属性	**if-match community** { *standard-community-number* [**whole-match**] | *extended-community-number* }
取消匹配 BGP 路由团体属性	**undo if-match community**
匹配路由信息的目的地址	**if-match** { **acl** *acl-number* | **ip-prefix** *ip-prefix-name* }
取消匹配路由信息的目的地址	**undo if-match** { **acl** *acl-number* | **ip-prefix** *ip-prefix-name* }
匹配路由信息下一跳接口	**if-match interface** [*interface-type number*]
取消匹配路由信息下一跳接口	**undo if-match interface**
匹配路由信息的下一跳	**if-match ip next-hop** { **acl** *acl-number* | **ip-prefix** *ip-prefix-name* }
取消匹配路由信息的下一跳	**undo if-match ip next-hop** [**ip-prefix**]
匹配路由信息的路由权值	**if-match cost** *value*
取消匹配路由信息的路由权值	**undo if-match cost**
匹配 OSPF 路由信息的标记域	**if-match tag** *value*
取消匹配 OSPF 路由的标记域	**undo if-match tag**

缺省情况下，不进行任何匹配。

需要注意：

(1) 对于同一个 Route-policy 节点，在匹配的过程中，各个 **if-match** 子句间是“ 与 ”的关系，即路由信息必须同时满足所有 **match** 才算满足节点的匹配，可以执行 **apply** 子句的动作。

(2) 如不指定 **if-match** 子句，则所有路由信息都会通过该节点的过滤。

3. 定义 Route-policy 的 apply 子句

apply 子句指定动作，也就是在满足由 **if-match** 子句指定的过滤条件后所执行的一些配置命令，对路由的一些属性进行修改。

请在路由策略视图下进行下列配置。

表7-7 定义 apply 子句

操作	命令
在 BGP 路由信息的 as-path 系列前加入指定的 AS 号	**apply as-path** *as-number-1* [*as-number-2* [*as-number-3* ...]]
取消在 BGP 路由信息的 as-path 系列前加入指定的 AS 号的设置	**undo apply as-path**
在 BGP 路由信息中设置团体属性	**apply community** { { *aa:nn* | **no-export-subconfed** | **no-advertise** | **no-export** }… [**additive**] | **additive** | **none** }
取消所设置的 BGP 路由信息中的团体属性	**undo apply community**
设置路由信息的下一跳地址	**apply ip-address** [**default**] { **next-hop** *ip-address* [*ip-address*] | **acl** *acl-number* }
取消路由信息的下一跳地址	**undo apply ip-address** [**default**] { **next-hop** *ip-address* [*ip-address*] | **acl** *acl-number* }
设置引入路由到 IS-IS 的级别：level-1、level-2 还是 level-1-2	**apply isis** [**level-1** | **level-2** | **level-1-2**]
取消引入路由到 IS-IS 的级别	**undo apply isis**
设置 BGP 路由信息的本地优先级	**apply local-preference** *localpref*
取消 BGP 路由信息的本地优先级	**undo apply local-preference**
设置路由信息的路由权值	**apply cost** *value*
取消路由信息的路由权值	**undo apply cost**
设置路由信息的路由权类型	**apply cost-type** [**internal** | **external**]
取消路由信息的路由权类型	**undo apply cost-type**
设置 BGP 路由信息的路由源	**apply origin** { **igp** | **egp** *as-number* | **incomplete** }
取消 BGP 路由信息的路由源	**undo apply origin**
设置 OSPF 路由信息的标记域	**apply tag** *value*
取消 OSPF 路由信息的标记域	**undo apply tag**

缺省情况下，不进行任何设置。

请注意：如果满足 Route-policy 中指定的匹配条件，并且在向 EBGP 同伴通告 IGP 路由时通告了 **apply cost-type internal** 配置的 MED 值，那么该值将作为 IGP 路由的 MED 值。用 **apply cost-type internal** 所配置的优先级低于 **apply cost** 命令，高于 **default med** 命令。

4. 应用 Route-policy

请在路由协议视图下进行下列配置。

表7-8 引入其它协议路由

操作	命令
设置引入其它协议的路由	**import-route** *protocol* [**med** *med* | **cost** *cost*] [**tag** *value*] [**type 1** | **2**] **route-policy** *route-policy-name*
取消引入其它协议的路由的设置	**undo import-route** *protocol*

缺省情况下，不引入其它协议的路由信息。

说明：

在不同的路由协议视图下，可选的参数也有所区别，具体情况请分别参考手册中相应路由协议的 **import-route** 命令。

对于 BGP，还可以通过配置对等体组的 Route-policy 策略可以控制从对等体（组）引入的路由或向对等体组通告的路由。对等体组的成员不能配置不同于对等体组的出方向路由更新策略，但可以配置不同的入口策略。

表7-9 配置对等体的 Route-policy 策略

操作	命令
配置对等体的 Route-policy 策略	**peer** *peer-address* **route-policy** *route-policy-name* **import**
取消对等体的 Route-policy 策略	**undo peer** *peer-address* **route-policy** *policy-name* **import**

7.3 IP 路由策略显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 IS-IS 的运行情况，用户可以通过查看显示信息验证配置的效果。

表7-10 路由策略显示和调试

操作	命令
查看 Route-policy	**display route-policy** [*route-policy-name*]
查看 BGP 中 AS 过滤的路径信息	**display ip as-path-acl** [*aspath-acl-number*]
查看地址前缀列表信息	**display ip ip-prefix** [*ip-prefix-name*]

7.4 路由策略典型配置举例

7.4.1 配置引入其它协议的路由信息

1. 组网需求

本例说明了一种 OSPF 协议有选择地引入 RIP 协议路由的情况。

路由器连接了一所大学的校园网和一个地区性网络。校园网使用 RIP 作为其内部路由协议，地区性网络使用 OSPF 路由协议，路由器需要将校园网中的某些路由信息在地区性网络中发布。为实现这一功能，路由器上的 OSPF 协议在引入 RIP 协议路由信息时通过对一个路由策略的引用实现路由过滤的功能。该路由策略由两个节点组成，实现 192.1.0.0/24 和 128.2.0.0/16 的路由信息以不同的路由权值被 OSPF 协议发布。

2. 组网图

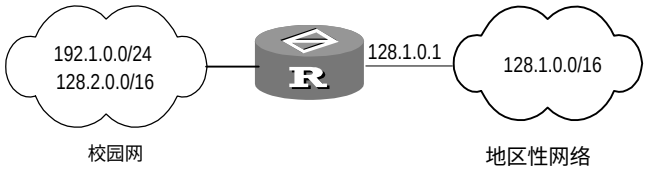


图7-1 配置 OSPF 引入 RIP 协议路由的组网图

3. 配置步骤

定义地址前缀列表。

```
[Router]ip ip-prefix  p1 permit 192.1.1.0 24
[Router]ip ip-prefix  p2 permit 128.2.0.0 16
```

配置路由策略。

```
[Router]route-policy r1 permit node 10
[Router-route-policy] if-match ip-prefix p1
[Router-route-policy] apply cost 120
[Router-route-policy] route-policy r1 permit node 20
[Router-route-policy] if-match ip-prefix p2
[Router-route-policy] apply cost 100
[Router-route-policy] quit
```

配置 OSPF 协议

```
[Router]ospf
[Router-ospf-1] area 0
[Router -ospf-1-area-0.0.0.0] network 128.1.0.0 0.0.0.255
[Router -ospf-1-area-0.0.0.0] quit
[Router-ospf-1] import-route rip route-policy r1
```

```
[Router-ospf-1] quit
[Router]interface ethernet 0/0/0
[Router-Ethernet0/0/0]ip address 128.1.0.1 255.255.255.0
```

7.4.2 配置 RIP 过滤发布的路由信息

1. 组网需求

本例说明了 RIP 协议有选择地发布路由信息的情况。

路由器连接了校园网 A 和校园网 B，它们都使用 RIP 作为内部路由协议，路由器仅将校园网 A 中的 192.1.1.0/24 和 192.1.2.0/24 两个网段的路由发布到校园网 B 中去。为实现这一功能，路由器上的 RIP 协议使用一条 **filter-policy** 命令过滤发布的路由信息，通过对一个地址前缀列表的引用来实现对由路发布路由进行过滤的功能。

2. 组网图

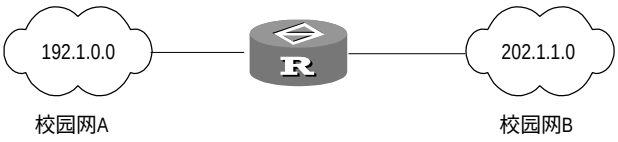


图7-2 配置过滤发布路由信息的组网图

3. 配置步骤

配置地址前缀列表。

```
[Router]ip ip-prefix p1 permit 192.1.1.0 24
[Router]ip ip-prefix p1 permit 192.1.2.0 24
```

配置 RIP 协议。

```
[Router]rip
[Router-rip]network 192.1.0.0
[Router-rip]network 202.1.1.0
[Router-rip]filter-policy ip-prefix p1 export
```

7.4.3 配置 OSPF 过滤接收的路由信息

1. 组网需求

- Router A 与 Router B 通信，链路层封装 PPP，都运行 OSPF 协议。
- 对 Router A 上的 OSPF 路由进程进行配置，引入三条静态路由。
- 通过在 Router B 上配置路由过滤规则，使接收到的三条静态路由部分可见，部分被屏蔽掉——20.0.0.0 和 40.0.0.0 网段的路由是可见的，30.0.0.0 网段的路由则被屏蔽。

2. 组网图

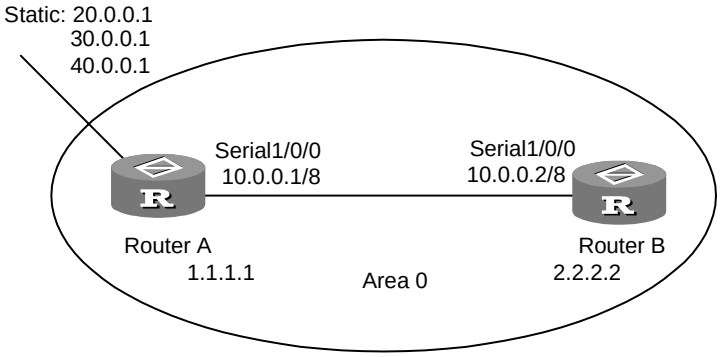


图7-3 过滤接收的路由信息组网图

3. 配置步骤

(1) 配置 Router A

配置接口 Serial1/0/0 的 IP 地址，封装 PPP 协议。

```
[Router A] interface serial 1/0/0
[Router A-Serial1/0/0] ip address 10.0.0.1 255.0.0.0
[Router A-Serial1/0/0] link-protocol ppp
[Router A-Serial1/0/0] quit
```

配置三条静态路由。

```
[Router A] ip route-static 20.0.0.1 32 serial 1/0/0
[Router A] ip route-static 30.0.0.1 32 serial 1/0/0
[Router A] ip route-static 40.0.0.1 32 serial 1/0/0
```

启动 OSPF 协议，指定该接口所属区域号。

```
[Router A] router id 1.1.1.1
[Router A] ospf
[Router A-ospf-1] area 0
[Router A-ospf-1-area-0.0.0.0] network 10.0.0.0 0.0.0.255
```

引入静态路由。

```
[Router A-ospf-1] import-route static
```

(2) 配置 Router B

配置接口 Serial1/0/0 的 IP 地址，封装 PPP 协议。

```
[Router B] interface serial 1/0/0
[Router B-Serial1/0/0] ip address 10.0.0.2 255.0.0.0
[Router B-Serial1/0/0] link-protocol ppp
[Router B-Serial1/0/0] quit
```

配置访问控制列表。

```
[Router B] acl number 2001
```

```
[Router B-acl-basic-2001] rule deny source 30.0.0.0 0.255.255.255
[Router B-acl-basic-2001] rule permit source any
```

启动 OSPF 协议，指定该接口所属区域号。

```
[Router B] router id 2.2.2.2
[Router B] ospf
[Router B-ospf-1] area 0
[Router A-ospf-1-area-0.0.0.0] network 10.0.0.0 0.0.0.255
```

配置 OSPF 对接收的外部路由进行过滤。

```
[Router B-ospf-1] filter-policy 2001 import
```

7.4.4 通过配置 BGP 的 cost 属性来选择路径

1. 组网需求

本例说明怎样通过 BGP 属性的使用来管理路由选择。

所有路由器都配置 BGP，AS200 中的 IGP 使用 OSPF。

路由器 A 在 AS100 中，路由器 B、路由器 C 和路由器 D 在 AS200 中。路由器 A 与路由器 B 和路由器 C 之间运行 EBGP。路由器 B 和路由器 C 与路由器 D 之间运行 IBGP。

2. 组网图

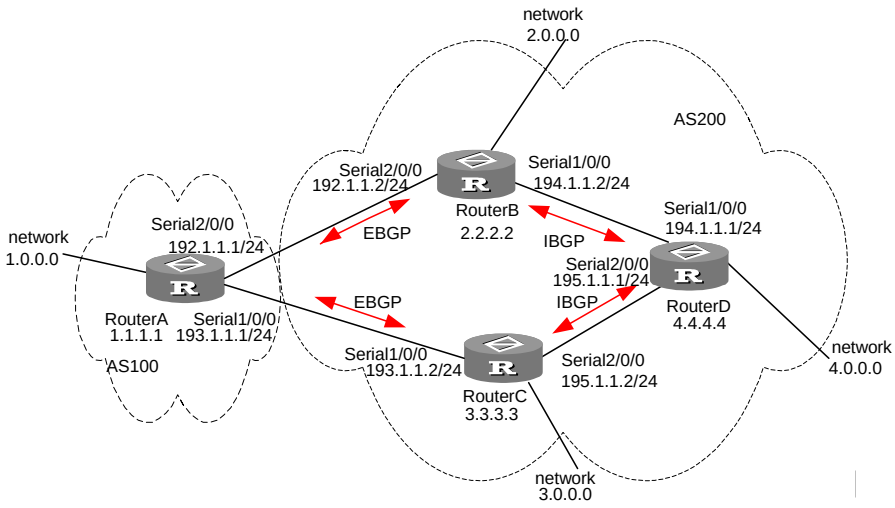


图7-4 配置 BGP 路径选择的组网图

3. 配置步骤

配置路由器 Router A：

```
[Router A] interface serial 2/0/0
[Router A-Serial2/0/0] ip address 192.1.1.1 255.255.255.0
[Router A-Serial2/0/0] interface serial 1/0/0
```

```
[Router A-Serial1/0/0] ip address 193.1.1.1 255.255.255.0
[Router A-Serial1/0/0] quit
[Router A] bgp 100
[Router A-bgp] network 1.0.0.0
[Router A-bgp] group ex192 external
[Router A-bgp] peer 192.1.1.2 group ex192 as-number 200
[Router A-bgp] group ex193 external
[Router A-bgp] peer 193.1.1.2 group ex193 as-number 200
[Router A-bgp] quit
```

配置路由器 A 的 MED 属性

增加访问列表到路由器 A 上，允许网络 1.0.0.0

```
[Router A] acl number 2001
[Router A-acl-basic-2001] rule permit source 1.0.0.0 0.255.255.255
```

定义两个 Route-policy，一个名为 apply_med_50，另一个名为 apply_med_100，第一个 Route-policy 为网络 1.0.0.0 设置的 MED 属性为 50，第二个 Route-policy 设置的 MED 属性为 100。

```
[Router A] route-policy apply_med_50 permit node 10
[Router A-route-policy] if-match acl 2001
[Router A-route-policy] apply cost 50
[Router A-route-policy] quit
[Router A] route-policy apply_med_100 permit node 10
[Router A-route-policy] if-match acl 2001
[Router A-route-policy] apply cost 100
[Router A-route-policy] quit
```

应用 apply_med_50 到邻居 Router C（193.1.1.2）出口路由更新上，应用 apply_med_100 到邻居 Router B（192.1.1.2）的出口路由更新上。

```
[Router A] bgp 100
[Router A-bgp] peer ex193 route-policy apply_med_50 export
[Router A-bgp] peer ex192 route-policy apply_med_100 export
```

配置路由器 Router B：

```
[Router B] interface serial 2/0/0
[Router B-Serial2/0/0] ip address 192.1.1.2 255.255.255.0
[Router B-Serial2/0/0] interface serial 1/0/0
[Router B-Serial1/0/0] ip address 194.1.1.2 255.255.255.0
[Router B-Serial1/0/0] quit
[Router B] ospf
[Router B-ospf-1] import-route bgp
[Router B-ospf-1] area 0
[Router B-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[Router B-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
```

```
[Router B] bgp 200
[Router B-bgp] undo synchronization
[Router B-bgp] group ex external
[Router B-bgp] peer 192.1.1.1 group ex as-number 100
[Router B-bgp] group in internal
[Router B-bgp] peer 194.1.1.1 group in
[Router B-bgp] import-route ospf
```

配置路由器 Router C：

```
[Router C] interface serial 1/0/0
[Router C-Serial1/0/0] ip address 193.1.1.2 255.255.255.0
[Router C-Serial1/0/0] interface serial 2/0/0
[Router C-Serial2/0/0] ip address 195.1.1.2 255.255.255.0
[Router C-Serial2/0/0] quit
[RouterC] ospf
[Router C-ospf-1] import-route bgp
[Router C-ospf-1] area 0
[Router C-ospf-1-area-0.0.0.0] network 193.1.1.0 0.0.0.255
[Router C-ospf-1-area-0.0.0.0] network 195.1.1.0 0.0.0.255
[Router C] bgp 200
[Router C-bgp] group ex external
[Router C-bgp] peer 193.1.1.1 group ex as-number 100
[Router C-bgp] group in internal
[Router C-bgp] peer 195.1.1.1 group in
[Router C-bgp] import-route ospf
```

配置路由器 Router D：

```
[RouterD] interface serial 1/0/0
[RouterD-Serial1/0/0] ip address 194.1.1.1 255.255.255.0
[RouterD-Serial1/0/0] interface serial 2/0/0
[RouterD-Serial2/0/0] ip address 195.1.1.1 255.255.255.0
[RouterD-Serial2/0/0] quit
[RouterD] ospf
[Router D-ospf-1] import-route bgp
[Router D-ospf-1] area 0
[Router D-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[Router D-osp-1f-area-0.0.0.0] network 195.1.1.0 0.0.0.255
[Router D-ospf-1-area-0.0.0.0] network 4.0.0.0 0.255.255.255
[Router D] bgp 200
[Router D-bgp] group in internal
[Router D-bgp] peer 195.1.1.2 group in as-number 200
[Router D-bgp] peer 194.1.1.2 group in as-number 200
[Router D-bgp] import-route ospf
```

为使配置生效，需要使用 **reset bgp all** 命令复位所有的 BGP 邻居。

通过上述配置后，由于路由器 C 学到的路由 1.0.0.0 的 MED 属性比路由器 B 学到的更小，路由器 D 优选来自路由器 C 的路由 1.0.0.0。

如果在配置路由器 A 时，不配置路由器 A 的 MED 属性，而在路由器 C 上配置本地优先级如下：

在路由器 C 上加上访问列表 2001，允许网络 1.0.0.0

```
[Router C] acl number 2001
[Router C-acl-basic-2001] rule permit source 1.0.0.0 0.255.255.255
```

定义名为 localpref 的路由策略，设置匹配 acl 2001 的路由的本地优先级为 200，不匹配的为 100。

```
[Router C] route-policy localpref permit node 10
[Router C-route-policy] if-match acl 2001
[Router C-route-policy] apply local-preference 200
[Router C-route-policy] route-policy localpref permit node 20
[Router C-route-policy] apply local-preference 100
[Router C] quit
```

应用此路由策略到来自 BGP 邻居 193.1.1.1（路由器 A）的路由信息上。

```
[RouterC] bgp 200
[RouterC-bgp] peer 193.1.1.1 route-policy localpref import
```

此时，由于路由器 C 学到的路由 1.0.0.0 的 Local preference 属性值为 200，比路由器 B 学到的路由 1.0.0.0 的 Local preference 属性值（路由器 B 没有配置 Local preference 属性，默认为 100）更大，路由器 D 依然优选来自路由器 C 的路由 1.0.0.0。

7.4.5 基于 BGP next-hop/as-path/origin/ local-preference 属性的路由策略配置举例

1. 组网需求

RouterA 和 RouterB 在 AS300，RouterD 在 AS100，RouterC 在 AS200。配置 RouterA 与 D、RouterB 与 C、RouterC 与 D 均为 EBGP peer。RouterA 与 B 为 IBGP peer；RouterA 与 B 间的 IGP 协议为 RIP。

2. 组网图

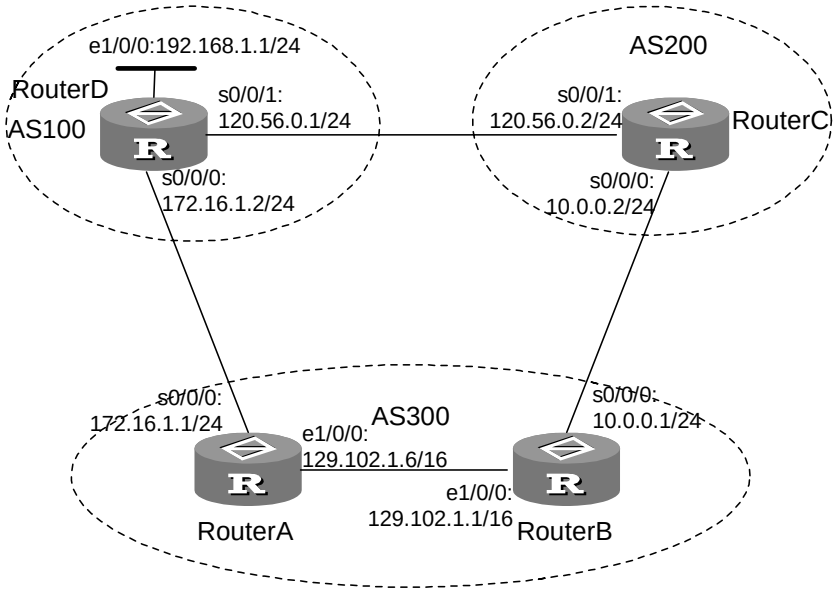


图7-5 基于 BGP next-hop/as-path/origin/ local-preference 属性的路由策略配置举例

3. 配置步骤

(1) 配置 RouterA：

配置接口 IP 地址。

```
[RouterA] interface serial 0/0/0
[RouterA-serial 0/0/0] ip address 172.16.1.1 255.255.255.0
[RouterA-serial 0/0/0] interface ethernet 1/0/0
[RouterA-ethernet 1/0/0] ip address 129.102.1.6 255.255.0.0
[RouterA-ethernet 1/0/0] quit
```

配置 RIP 协议。

```
[RouterA] rip
[RouterA-rip] network 129.102.1.6
[RouterA-rip] quit
```

配置 BGP 内部邻居和外部邻居。

```
[RouterA] bgp 300
[RouterA-bgp] undo synchronization
[RouterA-bgp] import-route rip
[RouterA-bgp] group ex100 external
[RouterA-bgp] peer 172.16.1.2 group ex100 as-number 100
[RouterA-bgp] group in300 internal
[RouterA-bgp] peer 129.102.1.1 group in300
```

(2) 配置 RouterB：

```
[RouterB] interface serial 0/0/0
[RouterB-serial 0/0/0] ip address 10.0.0.1 255.255.255.0
[RouterB-serial 0/0/0] interface ethernet 1/0/0
[RouterB-ethernet 1/0/0] ip address 129.102.1.1 255.255.0.0
[RouterB-ethernet 1/0/0] quit
[RouterB] rip
[RouterB-rip] network 129.102.1.1
[RouterB-rip] quit
[RouterB] bgp 300
[RouterB-bgp ] import-route rip
[RouterB-bgp ] undo synchronization
[RouterB-bgp ] group in300 internal
[RouterB-bgp ] peer 129.102.1.6 group in300
[RouterB-bgp ] group ex200 external
[RouterB-bgp ] peer 10.0.0.2 group ex200 as-number 200
```

(3) 配置 RouterC：

```
[RouterC] interface serial 0/0/0
[RouterC-interface serial 0/0/0] ip address 10.0.0.2 255.255.255.0
[RouterC-interface serial 0/0/0] interface serial 0/0/1
[RouterC-interface serial 0/0/1] ip address 120.56.0.2 255.255.255.0
[RouterC-interface serial 0/0/1] quit
[RouterC] bgp 200
[RouterC-bgp] group ex100 external
[RouterC-bgp] peer 120.56.0.1 group ex100 as-number 100
[RouterC-bgp] group ex300 external
[RouterC-bgp] peer 10.0.0.1 group ex300 as-number 300
```

(4) 配置 RouterD：

```
[RouterD] interface serial 0/0/0
[RouterD-serial 0/0/0] ip address 172.16.1.2 255.255.255.0
[RouterD-serial 0/0/0] interface serial 0/0/1
[RouterD-serial 0/0/1] ip address 120.56.0.1 255.255.255.0
[RouterD-serial 0/0/1] interface ethernet 1/0/0
[RouterD-ethernet 1/0/0] ip address 192.168.1.1 255.255.255.0
[RouterD-ethernet 1/0/0] quit
[RouterD] bgp 100
[RouterD-bgp] network 192.168.1.0
[RouterD-bgp] group ex300 external
[RouterD-bgp] peer 172.16.1.1 group ex300 as-number 300
[RouterD-bgp] group ex200 external
[RouterD-bgp] peer 120.56.0.2 group ex200 as-number 200
[RouterD-bgp] network 192.168.1.0 255.255.255.0
[RouterD-bgp] quit
```

```
[RouterD] quit
```

完成上面配置在 RouterA/B 上执行 **display bgp routing**，可以看到到 192.168.1.0 的路由下一跳为 172.16.1.2，Origin 属性为 igp。

- 如在 RouterD 上增加 as-path

```
[RouterD] bgp 100
[RouterD-bgp] peer ex300 route-policy AS300 export
[RouterD-bgp] quit
[RouterD] route-policy AS300 permit node10
[RouterD- route-policy] if-match acl 2001
[RouterD-route-policy] apply as-path 300
[RouterD- route-policy] quit
[RouterD] acl number 2001 match-order auto
[RouterD-acl-2001] rule permit source any
[RouterD-acl-2001] quit
[RouterD] quit
```

观察到 192.168.1.0 的路由下一跳变为 10.0.0.2，as-path 为 200，100，原来的到 AS300 的路由被过滤掉了。

- 如在 RouterA 上指定下一跳地址

```
[RouterA] bgp 300
[RouterA-bgp] peer ex100 route-policy AS100 export
[RouterA-bgp] quit
[RouterA] route-policy AS100 permit node 10
[RouterA-route-policy] if-match acl 2001
[RouterA-route-policy] apply ip-address 10.0.0.2
[RouterA-route-policy] quit
[RouterA] acl number 3001
[RouterA-acl-3001] rule permit ip destination 192.168.1.0
[RouterA-acl-3001] quit
[RouterA] quit
```

观察到 192.168.1.0 的路由下一跳变为 10.0.0.2。

- 如在 RouterD 上设置 Origin 属性

```
[RouterD] bgp 100
[RouterD-bgp] peer ex300 route-policy AS300 export
[RouterD] quit
[RouterD] route-policy AS300 permit node10
[RouterD-route-policy] if-match acl 2001
[RouterD-route-policy] apply origin Incomplete
[RouterD-route-policy] quit
[RouterD] acl number 2001 match-order auto
[RouterD-acl-2001] rule permit  source 192.168.1.0
```

```
[RouterD-acl-2001] quit
[RouterD] quit
```

此时 Origin 属性变为 Incomplete。

- 如在 RouterB 上配置 local-preference 属性

```
[RouterB] bgp 200
[RouterB-bgp] peer ex200 route-policy AS200 export
[RouterB-bgp] quit
[RouterB] route-policy AS200 permit node10
[RouterB-route-policy] if-match acl 2001
[RouterB-route-policy] apply local-preference 150
[RouterB-route-policy] quit
[RouterB] acl number 2001 match-order auto
[RouterB-acl-2001] rule permit ip destination 192.168.1.0
[RouterB-acl-2001] quit
[RouterB] quit
```

观察到 192.168.1.0 的路由下一跳变为 10.0.0.2。

7.4.6 基于 BGP 团体属性的路由策略配置举例

1. 组网需求

RTA，RTB，RTC 互为 BGP peer，其中 RTB，RTC 向对等体发布带有团体属性的路由信息，RTA 根据团体属性设置该路由不向对等体发布。

2. 组网图

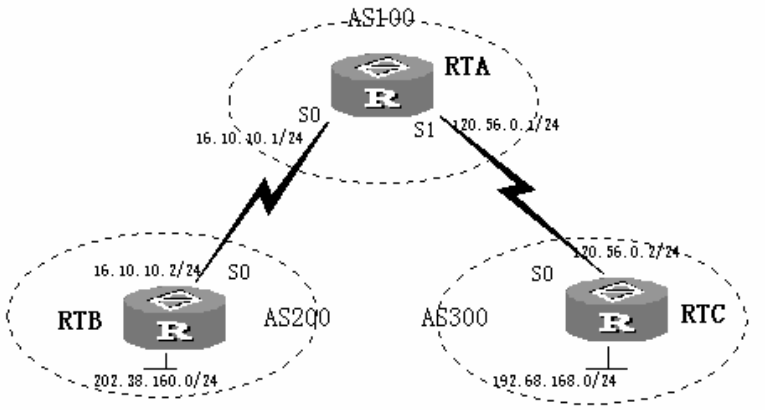


图7-6 基于 BGP 团体属性的路由策略配置举例

3. 配置步骤

(1) 配置 RTA

```
[RouterA] bgp 100
```

配置对等体 ex200，并对收到的路由按照策略 SETNOEXP 进行过滤。

```
[RouterA-bgp] group ex200 external
[RouterA-bgp] peer 16.10.10.2 group ex200 as-number 200
[RouterA-bgp] peer ex200 route-policy SETNOEXP import
```

配置对等体 ex300，并对收到的路由进行过滤。

```
[RouterA-bgp] group ex300 external
[RouterA-bgp] peer 120.56.0.2 group ex300 as-number 300
[RouterA-bgp] peer ex300 route-policy SETNOEXP import
[RouterA-bgp] quit
```

配置团体列表。

```
[RouterA] ip community-list 10 permit 100:200
[RouterA] ip community-list 20 permit 100:300
```

配置针对对等体 ex200 及 ex300 的路由策略。

```
[RouterA] route-policy SETNOEXP permit node 10
[RouterA- route-policy] if-match community 10
[RouterA- route-policy] apply community no-export
[RouterA- route-policy] route-policy SETNOEXP permit node 20
[RouterA- route-policy] if-match community 20
[RouterA- route-policy] apply community no-export
```

(2) 配置 RTB

```
[RTB] bgp 200
```

配置对等体 ex100，并向对等体发布团体属性。

```
[RTB-bgp] group ex100 external
[RTB-bgp] peer 16.10.10.1 group ex100 as-number 100
[RTB-bgp] peer ex100 advertise-community
```

#配置向 ex100 发布路由时的路由策略。

```
[RTB-bgp] peer ex100 route-policy SET_COMM export
[RTB-bgp] quit
```

配置 as-path-acl 包含所有的路由。

```
[RTB] ip as-path-acl 10 permit ^$
[RTB] ip as-path-acl 10 deny .*
```

配置 as100 发布的所有路由团体号为 100:200。

```
[RTB] route-policy SET_COMM permit node 10
[RTB-route-policy] if-match as-path 10
[RTB-route-policy] apply community 100:200
```

(3) 配置 RTC

```
[RTC] bgp 300
```

配置对等体 ex100，并向对等体发布团体属性。

```
[RTC-bgp] group ex100 external
[RTC-bgp] peer 120.56.0.1 group ex100 as-number 100
[RTC-bgp] peer ex100 advertise-community
```

配置向 ex100 发布路由时的路由策略。

```
[RTC-bgp] peer ex100 route-policy SET_COMM export
[RTC-bgp] quit
```

配置 as-path-acl 包含所有的路由。

```
[RTC] ip as-path-acl 10 permit ^$
[RTC] ip as-path-acl 10 deny .*
```

配置 as100 发布的所有路由团体号为 100:300。

```
[RTC] route-policy SET_COMM perm node 10
[RTC- route-policy] if-match as-path 10
[RTC- route-policy] apply community 100:300
```

RTB/RTC 的配置为将向外发布的所有路由的团体属性分别配置为 100:200 和 100:300；RTA 的配置为将从 ex200 及 ex300 收到的路由的团体类型配置为 no-export，即不再向外部对等体发布此路由信息。所以配置的结果是 RTA 上有到 202.38.160.0 和 192.68.168.0 的路由，但 RTB 上没有到 192.68.168.0 的路由，RTC 上也没有到 202.38.160.0 的路由。

7.5 路由策略故障诊断与排错

故障一：路由协议运行正常的情况下无法实现路由信息过滤。

故障排除：检查如下几种错误：

- Route-policy 的各个节点中至少应该有一个节点的匹配模式是 **permit** 模式。当一个 Route-policy 用于路由信息过滤时，如果某路由信息没有通过任一节点的过滤，则认为该路由信息没有通过该 Route-policy 的过滤。当 Route-policy 的所有节点都是 **deny** 模式时，所有路由信息都不会通过该 Route-policy 的过滤。
- 地址前缀列表的各个表项中至少应该有一个表项的匹配模式是 **permit** 模式。**deny** 模式的表项可以先被定义以快速的过滤掉不符合条件的路由信息，但如果所有表项都是 **deny** 模式，则任何路由都不会通过该地址前缀列表的过滤。可以在定义了多条 **deny** 模式的表项后定义一条 permit 0.0.0.0 0 less-equal 32 的表项以允许其它所有路由信息通过（如果不指定 less-equal 32 将只匹配缺省路由）。

第8章 路由容量配置

8.1 路由容量配置简介

8.1.1 概述

在大型组网应用中，路由表中的路由数量往往非常大，尤其是 OSPF 路由和 BGP 路由。路由信息通常是存储在路由器的内存中，当路由表规模不断增大时，路由器的内存使用量也将不断增加。但路由器总的内存大小并不会改变（除非进行硬件升级，而升级也不能保证解决所有问题），当让路由器内存被用完时，路由器就不能正常工作了。

为了解决这种矛盾，路由器提供了一种对路由表规模进行控制的机制，通过监控系统当前空闲内存的大小，决定是否继续向路由表中增加新的路由及是否保持路由协议的连接。

📖 说明：

需要注意的是，通常情况下使用系统的默认值就可以满足要求，不建议用户自行改变配置，以避免配置不当导致的系统的稳定性和可用性降低。

8.1.2 路由器实现的路由容量限制

造成路由表规模过于庞大的，通常是 BGP 路由项和 OSPF 路由项，因此，路由器的路由容量限制只对这两类路由有效，静态路由和其它动态路由协议不受影响。

当路由器的空闲内存大小降低到设定的内存下限时，BGP 和 OSPF 连接将被断开，相应的路由项从路由表中删除，从而释放占用的内存。系统定期检查空闲内存的大小，当发现空闲内存恢复到安全值后，再重新恢复 BGP 和 OSPF 连接。

8.2 路由容量配置

路由容量配置包括：

- 设置/恢复路由器内存的下限与安全值
- 禁止路由器自动恢复断开的路由协议
- 使能路由器自动恢复断开的路由协议

8.2.1 配置路由器内存的下限与安全值

当路由器的空闲内存大小等于或低于下限值时，BGP 和 OSPF 连接将被断开。

当路由器中的空闲内存大小降低到安全值，但还没有到达下限值时，通过 **dispaly memory limit** 命令可以看到路由器进入一种紧急状态（Exigent）。

如果使能了自动恢复功能，当路由器中的空闲内存大小恢复到超过安全值时，断开的 BGP 和 OSPF 连接将重新建立。

请在系统视图下进行下列配置。

表8-1 设置路由器内存的下限与安全值

操作	命令
设置路由器内存的下限与安全值	**memory** { **safety** *safety-value* | **limit** *limit-value* }*
将路由器内存的下限与安全值恢复为缺省值	**undo memory** { **safety** *safety-value* | **limit** *limit-value* }*

safety-value 的缺省值由内存大小决定，对于提供 128Mbytes 内存的路由器，*safety-value* 缺省值为 5Mbytes；对于提供 256Mbytes 内存的路由器，*safety-value* 缺省值为 50Mbytes。

limit-value 的缺省值由内存大小决定，对于提供 128Mbytes 内存的路由器，*limit-value* 缺省值为 3Mbytes；对于提供 256Mbytes 内存的路由器，*limit-value* 缺省值为 40Mbytes。

📖 说明：

请注意，在配置时，*safety-value* 必须大于 *limit-value*。

8.2.2 禁止路由器自动恢复断开的路由协议

如果禁止了自动恢复功能，则即使空闲内存已经超过了安全值，断开的 BGP 和 OSPF 连接也不会恢复，因此，请不要轻易使用该功能。

请在系统视图下进行下列配置。

表8-2 禁止路由器的内存恢复

操作	命令
禁止自动恢复功能	**memory auto-establish disable**

缺省情况下，使能路由器的自动恢复功能。

8.2.3 使能路由器自动恢复断开的路由协议

请在系统视图下进行下列配置。

表8-3 使能路由器的内存恢复

操作	命令
使能路由器的自动恢复功能	**memory auto-establish enable**

缺省情况下，使能路由器的自动恢复功能。

8.3 路由容量显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后的路由容量信息，用户可以通过查看显示信息验证配置的效果。

表8-4 路由容量显示和调试

操作	命令
查看路由容量相关的内存设置和状态信息	**display memory** [**limit**]