

## FRRouting 配置指南

本手册对应的软件版本为： release/5.1.0

文档版本号： V5.1.0

发布时间： 2019.11.30

## 目录

1. FRR CLI .....	6
1.1. 与主 CLI 的功能划分 .....	6
1.2. 命令行模式 .....	7
1.3. 配置保存/清除 .....	8
1.4. 命令格式说明 .....	9
2. 配置 IP 路由 .....	12
2.1. IP 路由概述 .....	12
2.2. 功能详解 .....	12
2.2.1. 路由策略 .....	12
2.2.2. 路由管理 .....	16
2.3. 配置命令 .....	22
2.3.1. 路由策略 .....	22
2.3.2. 路由管理 .....	34
2.4. 配置案例 .....	35
2.5. 显示命令 .....	37
2.5.1. 路由策略 .....	37
2.5.2. 路由管理 .....	43
3. 配置 OSPFv2 .....	49
3.1. 概述 .....	49
3.2. 典型应用 .....	49
3.2.1. 域内互联 .....	49
3.2.2. 域间互联 .....	50
3.3. 功能详解 .....	50
3.3.1. OSPF 协议 .....	51
3.3.2. OSPF 路由管理 .....	55
3.4. 配置命令 .....	59
3.4.1. OSPF 基本功能 .....	59

---

3.4.2.	虚链路 .....	61
3.4.3.	网络类型 .....	63
3.4.4.	路由重分布及缺省路由 .....	64
3.4.5.	Stub, NSSA 区域 .....	66
3.4.6.	路由汇聚及路由过滤 .....	68
3.4.7.	路由代价及管理距离 .....	71
3.4.8.	认证功能 .....	74
3.4.9.	控制参数 .....	75
3.5.	配置案例 .....	79
3.6.	显示命令 .....	83
3.7.	清除命令 .....	97
4.	配置 RIP .....	98
4.1.	概述 .....	98
4.2.	典型应用 .....	98
4.2.1.	RIP 基本应用 .....	98
4.2.2.	RIP 与 BGP 互联 .....	98
4.3.	功能详解 .....	99
4.3.1.	RIP 协议 .....	99
4.3.2.	RIP 路由管理 .....	101
4.4.	配置命令 .....	102
4.4.1.	RIP 基本功能 .....	102
4.4.2.	RIP 报文交互 .....	103
4.4.3.	路由重分布及缺省路由 .....	105
4.4.4.	路由过滤 .....	105
4.4.5.	认证功能 .....	107
4.4.6.	控制参数 .....	108
4.5.	配置案例 .....	110
4.6.	显示命令 .....	112

---

5. 配置 IS-IS.....	114
5.1. 概述.....	114
5.2. 典型应用.....	114
5.2.1. 平面拓扑.....	114
5.2.2. 分层拓扑.....	114
5.3. 功能详解.....	115
5.3.1. IS-IS 协议.....	115
5.3.2. IS-IS 路由管理.....	118
5.4. 配置命令.....	119
5.4.1. 使能 IS-IS.....	119
5.4.2. IS-IS 层次结构.....	120
5.4.3. IS-IS 报文控制.....	121
5.4.4. 路由重分布及缺省路由.....	124
5.4.5. 认证功能.....	125
5.4.6. 控制参数.....	126
5.5. 配置案例.....	128
5.6. 显示命令.....	131
5.7. 清除命令.....	136
6. 配置 BGP.....	138
6.1. 概述.....	138
6.2. 典型应用.....	138
6.2.1. AS 跨域路由通告.....	138
6.2.2. AS 域内路由反射.....	139
6.3. 功能详解.....	139
6.3.1. BGP 基本概念.....	139
6.3.2. BGP 信息交互.....	141
6.3.3. BGP 路径参数.....	144
6.3.4. BGP 路由管理.....	152

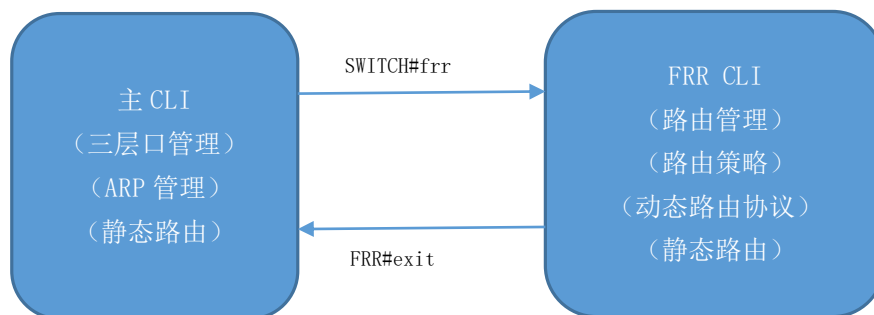
---

6.4. 配置命令 .....	155
6.4.1. 定义对等体 .....	155
6.4.2. 配置对等体 .....	157
6.4.3. 对等体信息交互 .....	160
6.4.4. AS-PATH 列表 .....	162
6.4.5. COMMUNITY 列表 .....	162
6.4.6. 路由策略 .....	163
6.4.7. 路由反射器 .....	165
6.4.8. AS 联盟 .....	165
6.4.9. 注入路由 .....	166
6.4.10. 路由聚合 .....	167
6.4.11. 路由表下发 .....	168
6.4.12. 软复位 .....	168
6.4.13. 路由优选 .....	169
6.4.14. 路由衰减 .....	171
6.4.15. 管理距离 .....	171
6.4.16. 定时器 .....	172
6.5. 配置案例 .....	174
6.5.1. 配置 BGP 对等体 .....	174
6.5.2. 配置路由反射器 .....	185
6.5.3. 配置 AS 联盟 .....	189
6.6. 显示命令 .....	193
6.7. 清除命令 .....	195

## 1. FRR CLI

FRRouting 是一个独立的路由软件包，其 CLI 也是独立的。FRRouting 对设备而言，是可选组件，仅三层设备支持。FRRouting 的 CLI 称为 FRR CLI。

FRR CLI 与设备的主 CLI 之间的关系如下图所示：



当需要配置 FRRouting 时，在主 CLI 的特权模式下，通过命令“frr”进入 FRR CLI 界面，当需要退出 FRR CLI 时，通过特权模式下，输入命令“exit”完成。

FRRouting 对应的网络设备不局限于三层交换机，只要具备三层功能的网络设备使用上都完全一样。下文中的“路由设备”，“三层交换机”，“路由器”等表示的含义均指具备三层功能的网络节点。

### 1.1. 与主 CLI 的功能划分

#### ■ 三层口管理

三层口管理功能指：

- 三层口创建/删除
- IP 地址设置/删除
- shutdown/no shutdown
- mtu 设置。

三层口管理在主 CLI 完成。在 FRR CLI 可以通过如下命令查看相应的三层口设置：

（注意，在 FRR CLI 中，只能用三层口接口名字表示三层口）

对 SVI 而言，三层口接口名字为：“Vlan+vlan\_id”，比如 vlan 100 对应的三层口为“Vlan100”（切记：第一个字母 V 为大写）。

```
FRR# show int Vlan1
Interface Vlan1 is up. line protocol is up
  Link ups:      1      last: 1970/01/01 00:00:33.99
  Link downs:    0      last: (never)
  PTM status: disabled
  vrf: Default-IP-Routing-Table
  index 8 metric 0 mtu 2000 speed 10
  flags: <UP,BROADCAST,RUNNING,MULTICAST>
  Type: Unknown
  HWaddr: 00:aa:bb:09:26:16
  inet 192.168.100.50/24 broadcast 192.168.100.255
  inet6 fe80::2aa:bbff:fe09:2616/64
  Interface Type Other
```

#### ■ ARP 管理

在 FRRouting 中，不涉及 ARP 功能。

#### ■ 路由管理

主 CLI 和 FRR CLI 中均可设置静态路由，**建议对三层设备，使用 FRR CLI 来配置静态路由。**

主 CLI 的 show ip route 命令仅能查看到主 CLI 配置的静态路由以及配置 IP 地址自动生成的直连路由。

FRR CLI 的 show ip route 可以查看到设备的所有路由信息。包括主 CLI 配置 IP 地址自动生成的直连路由，以及主 CLI 配置的静态路由，**主 CLI 配置的静态路由在 FRR CLI 中体现为 kernel 路由，以便与 FRR CLI 配置的静态路由区分。**如下例，主 CLI 和 FRR CLI 均配置前缀为 192.168.40.0/24 的路由。经过 FRRouting 的路由优选，选择了主 CLI 配置的静态路由生效。

```
FRR# show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR,
       > - selected route, * - FIB route

C>* 3.3.3.0/24 is directly connected, Vlan33, 1d18h00m
R   192.168.1.0/24 [120/2] via 192.168.2.1, Vlan2, 1d01h18m
B>* 192.168.1.0/24 [20/0] via 192.168.2.1, Vlan2, 1d18h10m
C>* 192.168.2.0/24 is directly connected, Vlan2, 1d18h11m
S> 192.168.33.0/24 [1/0] via 192.168.1.100 (recursive), 15:01:22
   * via 192.168.2.1, Vlan2, 15:01:22
   * unreachable (blackhole), 15:01:22
   * via 192.168.100.3, Vlan1, 15:01:22
S   192.168.40.0/24 [1/0] via 192.168.1.5, 00:00:02
K>* 192.168.40.0/24 [0/0] via 192.168.100.3, Vlan1, 00:00:44
C>* 192.168.100.0/24 is directly connected, Vlan1, 1d18h11m
```

## 1.2. 命令行模式

FRR CLI 与主 CLI 的命令行模式类似，管理界面分成若干不同的模式，用户当前所处的命令模式决定了可以使用的命令。在命令提示符下输入问号键（?）可以列出每个命令模式支持使用的命令。当用户从主 CLI 切换到 FRR CLI 时，首先处于特权模式。要从 FRR CLI 切换回主 CLI 时，必须处于特权模式或者用户模式。

模式名称	提示符	切换模式	模式描述
用户模式	FRR>	配置 enable 切换到特权模式；配置 exit 退出 FRR CLI，切换回主 CLI。	支持设备信息显示、调试命令行等。
特权模式	FRR#	配置 configure terminal 切换到全局模式；配置 disable 切换到用户模式；配置 exit 退出 FRR CLI，切换回主 CLI。	支持网络测试； 支持功能模块信息查看； 支持配置保存等操作。
全局模式，或者配置模式	FRR(config)#	配置 exit 切换到特权模式；配置 interface 切换到接口模式；配置 router 切换到路由模式；配置 route-map 切换到路由图模式。	支持基于全局的配置命令。
接口模式	FRR(config-if)#	配置 exit 切换到全局模式；配置 end 切换到特权模式。	支持基于接口的配置命令。
路由模式	FRR(config-router)#	配置 exit 切换到全局模式；配置 end 切换到特权模式；针对 bgp 的路由模式，配置 address-family xxx 进入 BGP 的地址簇模式。	不同的路由协议，该模式下的配置命令各不相同。
BGP 的地址簇模式	FRR(config-router-af)#	配置 exit 切换到路由模式，配置 end 切换到特权模式	仅针对 BGP 协议而言。
路由图模式	FRR(config-route-map)#	配置 exit 切换到全局模式，配置 end 切换到特权模式。	配置路由图的某条具体的策略。

### 1.3. 配置保存/清除

由于 FRR CLI 与主 CLI 是分开的，两者的 show running 只能看到各自的配置信息。

#### ■ 配置保存



FRRouting 的配置保存在 FRR CLI 和主 CLI 均可完成（任选一种方式即可）。两边的命令一样，有两种方式实现，两种方式等价：

➤ Write 命令

FRR CLI: `FRR#write`

或者主 CLI: `SWITCH#write`

➤ Copy 命令

FRR CLI: `FRR#copy running-config startup-config`

或者主 CLI: `SWITCH#copy running-config startup-config`

■ 配置清除

FRRouting 的配置清除只能在主 CLI 完成，**配置清除后需要重启设备后生效。**

主 CLI:

`SWITCH#copy empty-config startup-config`

`SWITCH#reload`

## 1.4. 命令格式说明

本文档中的配置命令，关键字使用**加黑**字体。非关键字的参数使用*斜体*表示。

另外，关于配置命令中的特殊符号，说明如下：

■ 尖括号，<>：表示可配置的数值范围

比如：`area area-id virtual-link A.B.C.D message-digest-key <1-255> md5 KEY`  
<1-255>:表示这个位置可以输入的数值范围是：最小为 1，最大为 255。

■ 中括号 []：表示括号内的命令可选。

比如：`no router-id [A.B.C.D]`，表示如下两种情况：

1) `no router-id`

2) `no router-id A.B.C.D`

■ 小括号 (|)：其中“|”用于分隔多个命令，最后一个位置可以为空，为空表示可选，跟中括号的含义一样。

比如上例中的命令也可以写成：`no router-id (A.B.C.D | )`，跟使用中括号完全等价。

小括号中可以使用若干个命令，通过“|”分隔，表示从多个命令中选择 1 个。

(*A* | *B* | *C*)：要么是 A，要么是 B，要么是 C，三种情况。

(*A* | *B* | *C* | )：要么是 A，要么是 B，要么是 C，要么都不选择，四种情况。

例 1: `redistribute (static|connect|kernel|rip|isis|bgp)`，表示可能存在 6 种情况：

1) `redistribute static`

2) `redistribute connect`

3) `redistribute kernel`

4) `redistribute rip`

5) `redistribute isis`

6) `redistribute bgp`

例 2: `ip ospf authentication (message-digest|null|)`, 表示可能存在 3 种情况:

1) `ip ospf authentication`

2) `ip ospf authentication message-digest`

3) `ip ospf authentication null`

■ 大括号 `{|}`: 其中 “|” 用于分隔多个命令。括号中不能以 “|” 结束。

大括号中一般而言, 至少要有两个命令, 表示从两个命令中至少选择一个命令, 并且命令的先后顺序无关。

`{ A | B | C }`: 表示的可能性有: 三个命令选择从 1 个到 3 个的任意排列情况。共有  $3 + 6 + 6 = 15$  种情况。

举例: `distance ospf {intra-area distance | inter-area distance | external distance}`, 表示可能存在 15 种情况。

1) `distance ospf intra-area distance`

2) `distance ospf intra-area distance inter-area distance`

3) `distance ospf intra-area distance external distance`

4) `distance ospf intra-area distance inter-area distance external distance`

5) `distance ospf intra-area distance external distance inter-area distance`

6) `distance ospf inter-area distance`

7) `distance ospf inter-area distance intra-area distance`

8) `distance ospf inter-area distance external distance`

9) `distance ospf inter-area distance intra-area distance external distance`

10) `distance ospf inter-area distance external distance intra-area distance`

11) `distance ospf external distance`

12) `distance ospf external distance intra-area distance`

13) `distance ospf external distance inter-area distance`

14) `distance ospf external distance intra-area distance inter-area distance`

15) **distance ospf external** *distance* **inter-area** *distance* **intra-area** *distance*

如果希望大括号内的内容可选，可以使用括号嵌套，在大括号外面加一个中括号[]，或者带一个“|”的小括号(|)。

这样，上述命令的可能情况就再增加一种，就是大括号内的命令全部不选择。

■ 省略号 “...”：

省略号放在某个命令的后面，表示该命令可以输入 1 到若干次。

举例：**set as-path exclude** *AS\_NUM*... 可以表示如下若干种情况：

1) **set as-path exclude** *AS\_NUM*

2) **set as-path exclude** *AS\_NUM AS\_NUM*

3) **set as-path exclude** *AS\_NUM AS\_NUM AS\_NUM*

4) ...

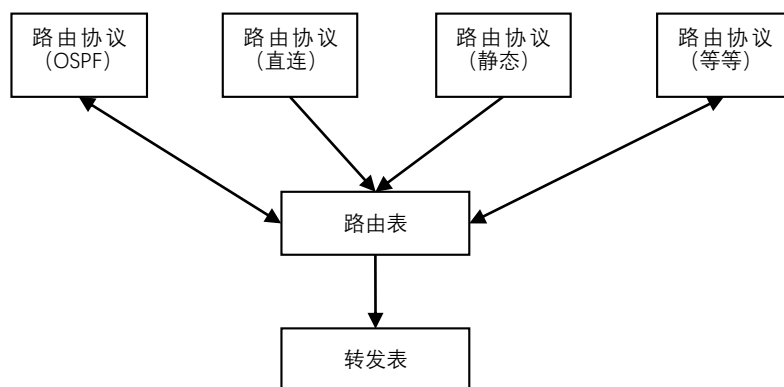
## 2. 配置 IP 路由

### 2.1. IP 路由概述

本章节分为两个部分：路由策略和路由管理。

路由策略包含了路由信息采集的策略集，该策略集作为基础功能为其他路由协议提供服务，在路由协议中使用路由策略，可以过滤路由信息或者修改路由信息。

路由管理负责管理路由表，整合各种路由协议下发的路由，进行优选，并下发给转发表。路由表中保存了各种路由协议发现的路由，根据来源不同，通常分为三类：**直连路由**，**静态路由**和**动态路由**。直连路由和静态路由在本章节路由管理中描述，而动态路由作为单独章节说明。



路由协议发现生成的路由信息下发到路由表管理，生成路由表项，路由表管理会记录所有路由信息以及来源，根据路由过滤，路由优选等确定有效的路由表项，并下发到转发表。IP 报文的三层转发通过查找转发表完成。

对动态路由协议而言，可以配置路由重分布，从路由表管理中将其其他协议的路由信息重新分布到对应的动态路由协议，参与动态路由协议。

### 2.2. 功能详解

#### 2.2.1. 路由策略

路由策略通过过滤列表和路由图进行实现，路由策略的应用灵活广泛。典型应用于路由过滤和路由重分布。

- 路由过滤：在路由协议中引用过滤列表，可以过滤其发送或接收的路由信息。
- 路由重分布：在路由协议中引用路由图，可以过滤路由信息或者修改路由信息。
- 路由管理：在路由管理中对某个路由协议产生的路由引用路由图，可以过滤路由信息或者修改路由信息。

路由图提供了更为丰富的匹配方式和策略行为。路由图也可以进一步引用过滤列表作为匹配。

2.2.1.1. 过滤列表

过滤列表是定义匹配域的一组列表，在进行匹配查找时，根据列表顺序从前到后进行查找。查找到匹配项，则退出当前查找。

过滤列表是路由策略进行过滤的工具，单独配置过滤列表没有任何作用，只有在路由协议中应用这些过滤列表，才能达到由过滤的效果。过滤列表分为两种：

■ 访问控制列表（ACL）：

ACL 可以配置若干个 ACE，每个 ACE 中可以指定 IP 地址和掩码，用于匹配路由信息的目的网段或下一跳地址。

访问控制列表的表项没有序号。因此，配置必须按照先后顺序进行，即新配置的一定放在列表的尾部，不能在列表中间位置插入某个 ACE。

➤ Zebra ACL

Zebra ACL 直接使用 ACL 名称定义一个 ACL。Zebra ACL 的 ACE 提供了 exact-match 选项，当 ACE 配置了 exact-match 选项时，只有路由信息对应的网段 IP 地址和掩码与 ACE 的 IP 地址和掩码完全一致时，才会认为匹配。若未配置 exact-match 选项，只要路由信息的网段包含在 ACE 定义的网段内，即可认为匹配。举例说明：

ACL	目的网段 192.168.3.0/24	目的网段 192.168.3.0/16	下一跳 192.168.3.10
192.168.3.0/16	匹配	匹配	匹配
192.168.3.0/16 exact-match	不匹配	匹配	不匹配
192.168.3.0/24	匹配	不匹配	匹配
192.168.3.10/32	不匹配	不匹配	匹配

上例列举的 192.168.3.0/16 和 192.168.3.0/16 exact-match 两条 ACE，虽然 IP 地址和掩码相同，但是由于选项不同，所以在同一个 ACL 中可以同时存在，作为两条独立的 ACE。

**当对下一跳进行匹配时，类似对一个掩码长度为 32 的网段进行匹配，若 ACE 不包含掩码长度为 32，则无法匹配下一跳。**

➤ 标准 ACL

使用 ACL ID 来定义 ACL，ACL ID 的范围为<1-99>以及<1300-1999>。标准 ACL 可以定义一个网段（通过 ip 地址和掩码），也可以直接定义一个主机（仅 ip 地址，无掩码）。前者可以用于匹配目的网段或者下一跳，或者只可用于匹配下一跳。

➤ 扩展 ACL

使用 ACL ID 来定义 ACL，ACL ID 的范围为<100-199>以及<2000-2699>。扩展 ACL 有更丰富的匹配字段，可以同时定义源 IP 和目的 IP 的匹配规则。但由于路由策略中的

匹配对象是目的网段（前缀）或者下一跳，不涉及源 IP 和目的 IP（只有报文匹配才涉及到源 IP 和目的 IP）。所以扩展 ACL 在路由策略中一般不使用。

■ 地址前缀列表（prefix-list）：

地址前缀列表的作用类似于访问控制列表，每个地址前缀表项可以指定 IP 地址和掩码（以及掩码的长度范围），用于匹配路由信息的目的网段或下一跳地址。

地址前缀列表的每条表项均有一个序号，可以自动生成，也可以进行指定。当自动生成时，新配置的表项自动添加到列表的尾部，序号根据最大序号加 5 得到（第一条表项序号为 5，第二条表项序号为 10，第三条表项序号为 15，依次类推）；当指定序号时，按照序号选择列表中对应的位置进行插入。

地址前缀列表的排序功能可以关闭，关闭后，跟访问控制列表一样，表项加在尾部，没有序号。该功能默认是开启的。

地址前缀列表提供了掩码长度范围配置，通过可选配置参数 `le` 和 `ge` 完成。当既没有配置 `le`，也没有配置 `ge` 时，掩码长度需要精确匹配，与访问控制列表的 `exact-match` 效果类似。

当 `le` 和 `ge` 配置参数至少配置了 1 个的时候，最终的可以匹配的掩码长度范围为`[ge, le]`。（中括号表示包括 `ge` 和 `le`）

✧ `ge`：默认值等于配置的掩码长度（即未配置参数 `ge` 时表示默认），可配置的范围**大于**配置的掩码长度，**小于等于** `le` 的值。

✧ `le`：默认值等于 32（即未配置参数 `le` 时表示默认），可配置的范围**大于等于** `ge` 的值，**小于等于** 32。

下面举例说明：（跟访问控制列表一样，对下一跳匹配时，类似于对掩码长度为 32 的网段进行匹配，因此，若掩码长度不包含 32，则不能匹配。）

Prefix-list	掩码长度说明
192.168.3.0/24	精确匹配 192.168.3.0/24，比如目的网段为 192.168.3.0/25 则不匹配；比如下一跳 192.168.3.10/32 则不匹配。
192.168.3.0/24 le 24	完全等同于 192.168.3.0/24。
192.168.3.0/24 ge 24	不支持配置， <code>ge</code> 必须大于掩码长度 24。
192.168.3.0/24 ge 25	支持的掩码长度范围为 <code>[25, 32]</code> 。目的网段为 192.168.3.0/24 不匹配，目的网段 192.168.3.0/25 和下一跳 192.168.3.10/32 可以匹配。
192.168.3.0/24 ge 32	可以配置，但该 <b>配置无效（无法匹配任何网段或者主机）</b> 。因为该配置仅仅匹配掩码长度 32，即某个主机（192.168.3.0），但由于合法的主机位不能为 0，所以，没有任何主机可以与其匹配。

192.168.3.0/24 le 28	支持的掩码长度范围为[24, 28]。目的网段为 192.168.3.0/24 和 192.168.3.0/25 均可匹配，下一跳 192.168.3.10/32 不匹配。
192.168.3.0/24 le 32	支持的掩码长度范围为[24, 32]。目的网段 192.168.3.0/24, 192.168.3.0/25 和下一跳 192.168.3.10/32 均可匹配。
192.168.3.0/24 ge 25 le 28	支持的掩码长度范围为[24, 32]。目的网段 192.168.3.0/24 和下一跳 192.168.3.10/32 不匹配， 192.168.3.0/24 可以匹配。

过滤列表中的每条表项都有 permit 和 deny 两种行为，过滤列表作用在路由过滤和路由图时，作用不尽相同。当作用于路由过滤时，默认行为是 deny（可以理解为最后有一条匹配所有路由信息的默认表项，其行为是 deny）。**路由信息匹配过滤列表后的行为若为 permit，表示允许协议发送或接收该路由信息；行为若为 deny，表示协议禁止发送或接收该路由信息。**

当作用于路由图时，过滤列表的目的不是过滤，而仅仅是匹配，所以没有默认行为，只用于确定路由信息是否匹配了对应的路由图（若匹配中 deny 的表项，当成是未匹配处理），对路由图处理的行为跟路由图的行为相关（与关联的过滤列表无关）。

2.2.1.2. 路由图

路由图是由一组策略组成的列表。一条策略就是包含了匹配域和行为两个部分（若匹配，则执行行为）。过滤列表只是通过表项的 permit 或者 deny 定义了简单的行为，而路由图的每条策略，除了 permit 或者 deny 外，还定义了丰富的 set 规则。

路由图中的每条策略都有对应的序号（Sequence），序号越小优先级越高。策略按序号顺序依次执行，一旦满足某条策略的匹配条件，就执行该策略对应的处理动作，并退出路由图。如果不能满足任何一条策略的匹配条件，则不做任何处理。

■ 路由图的匹配条件

- 如果包含 0 条 match 规则，则无条件匹配。
- 如果包含 1 条或多条 match 规则，则**必须同时匹配**所有 match 规则，才能满足策略的匹配条件。

路由图的 match 提供了多种匹配规则，具体参见配置命令章节描述，这里说明一下应用过滤列表时的情况。

过滤列表行为	描述
Permit	如果路由信息匹配该过滤列表表项，则认为路由信息 <b>匹配</b> 该匹配条件。
Deny	如果路由信息匹配该过滤列表表项，则认为路由信息 <b>未匹配</b> 该匹配条件。

■ 路由图的跳转

- 跳转到另外一个路由图，在策略中设置 `call` 参数，当匹配该策略，并执行相关行为后，跳转到 `call` 参数所指定的另外一个路由图进行处理。
- 本路由图中跳转：在策略中通过 `on-match` 关键字指定，表示当匹配该策略，并执行相关行为后的退出策略。（默认退出策略就是退出整个路由图）
  - ✧ 参数 `goto number`：退出策略为跳转到 `number` 参数所指定的策略（`number` 表示本路由图中某个策略的序号，若 `number` 表示的策略不存在，则退出整个路由图）。主要用于在一个路由图中执行多种行为的时候，比如，约定 1-100 的策略用于过滤；101-200 的策略用于设置 `metric`；200-300 的策略用于设置 `tag`；三种行为需要同时生效，因此，需要在过滤策略中全部跳转到 101，在设置 `metric` 的策略中全部跳转到 201。
  - ✧ 参数 `next`：退出策略为继续执行下一个策略。与 `goto` 参数所举例子类似，处理多种行为，但是没有按照行为进行策略组的划分，为了保证多种行为同时生效，也不能匹配某个策略后直接退出路由图。该参数主要用于配置策略较少的情况，比如设置 `metric` 策略和设置 `tag` 策略各 1 条，但两种策略对应的匹配域不同，需要两个策略，且同时生效。

## ■ 路由图的行为

路由图的策略有两种工作模式：`permit` 和 `deny`，**当策略的工作模式为 `deny` 时，表示过滤行为，其他的任何行为包括路由图的跳转，都必须使用 `permit` 工作模式。**（因为匹配 `deny` 策略的路由信息将被过滤，执行其他行为不再有意义）

当使用过滤行为时（配置策略的工作模式为 `deny`），其他跳转配置或者 `set` 配置其他行为均没有意义（即使配置了也不产生任何效果）。

路由图定义了多种 `set` 规则，具体参见“配置命令”章节描述。

路由图默认行为为 `deny`（可以理解为最后有一条匹配所有路由信息的默认策略，其行为是 `deny`），比如路由重分布时使用路由图进行过滤，将需要过滤的用 `deny` 的策略匹配后，后面需要加一个 `permit` 的策略（不配置 `match` 表示匹配所有），否则，所有的路由信息都将被过滤。

## 2.2.2. 路由管理

动态路由协议由单独章进行描述，本章节仅描述路由表的构成，优选，路由过滤以及静态路由。

### 2.2.2.1. 路由表

路由管理负责管理路由表，整合各种路由协议下发的路由，进行优选。路由表中根据来源不同，通常分为以下三类：

- 直连路由：链路层协议发现的路由，也称为接口路由。直连路由由三层口配置 IP 地址时自动生成，路由前缀为该三层口直连的网络，因此直连路由均是网络路由。



- 静态路由：网络管理员手工配置的路由，可以是网路路由，主机路由，也可以是缺省路由。
- 动态路由：动态路由协议（比如 RIP，OSPF，IS-IS，BGP）发现的路由。可以是网络路由，主机路由，也可以是缺省路由。

## ■ 表项构成

路由表项由两个部分组成：

- 前缀：由一个 IP 地址及网络掩码(或者掩码长度)来表示，指路由表项所确定的目的网络或者主机（当掩码长度为 32 表示主机）。
- 下一跳：决定了匹配中该路由表项时，对 IP 报文的处理策略。行为表现为如下 4 类：
  - ✧ Blackhole：当 IP 报文匹配该表项时，**静默地**丢弃掉报文。Blackhole 路由主要用于路由汇聚时，汇聚路由的地址范围可能超出路由表中实际的网络范围，如果数据发往汇总范围内不存在的网络，将有可能发生路由环路或者加重路由负担，为阻止这种情况的发生，需要配置一条 Blackhole 路由丢弃这类报文。
  - ✧ Reject：当 IP 报文匹配该表项时，设备会向发送 IP 报文的源端（根据 IP 报文 Source IP 地址）**发送 ICMP unreachable 报文**，并丢弃该报文。Reject 路由可以用于网络测试或者抵挡不安全的网络。
  - ✧ 三层出口：三层出口的方式认为该路由的目的 IP 直接可达（直连路由全部属于此情况），在配置静态路由时，指定三层口而非 IP 地址，也会生成此类路由表项。当 IP 报文匹配该表项时，**直接根据 IP 报文的目的 IP 进行 ARP 查询**，获取链路层封装的目的 MAC 地址。路由表项对应了唯一的三层口，用于发送 IP 报文时选择三层出口。
  - ✧ IP 地址：下一跳由一个 IP 主机地址表示，表示了要到达目的网络或主机，需要先转发到该 IP 地址表明的 IP 网络设备。当 IP 报文匹配该表项时，**根据下一跳中的 IP 地址进行 ARP 查询**，获取链路层封装的目的 MAC 地址。路由表项对应了唯一的三层口，用于发送 IP 报文时选择三层出口。

## ■ 表项查找

对 IP 报文转发，或者本设备直接发送的 IP 报文（比如 ping 远端的某设备），均需要进行路由查找，根据找到的路由表项确定的行为来进行下一步处理。若未匹配任何路由表项，则报文直接丢弃（可以理解为默认行为为 Blackhole）。

IP 报文发送时还需要进行链路层封装，源 MAC 地址使用设备自身的链路层 MAC 地址，目的 MAC 地址通过 ARP 查询得到，ARP 查询分为两个步骤：

- 1， 查询本地 ARP 表，若找到，使用 ARP 中记录的 MAC 地址。若未找到，进入步骤二；

- 2，触发路由打通（发送若干个 ARP 请求报文，默认为 3 个），以生成动态 ARP 表项（存在本地 ARP 表中），若生成了动态 ARP 表项，按照步骤一处理，若路由打通失败，IP 报文被丢弃。

路由表项间可能存在包含关系（根据掩码长度不同），所以，路由查找过程满足 LPM (Longest Prefix Match，最长前缀匹配)。即 IP 报文进行路由查找时，若同时命中多个路由表项，则选择前缀的掩码长度最长的那个路由表项。

■ 路由优选

若来自于不同来源的多个路由表项前缀相同（前缀 IP 地址和掩码完全相同），这多个路由表项表示同个路由信息，但行为可能不同，因此，需要进行优选。

管理距离（administrative distance，缩写为 AD）用于评价路由的可信度，取值范围 0～255（整数）。AD 值越小，则表示此路由更值得信任。到达同一目的地存在多条路由时，路由设备优先选择 AD 值较小的路由。AD 值较大者，成为浮动路由（作为最优路由的备份）。

缺省情况下，每种来源的路由对应一个 AD 值。AD 值为本地概念，修改 AD 值只会影响当前路由器上的路由选择。

路由来源	直连网络	静态路由	EBGP	OSPF	IS-IS	RIP	IBGP	不可达
缺省 AD	0	1	20	110	115	120	200	255

路由管理模块维护的路由表是多个来源路由表项的全集，通过 show ip route 可以查看，但同个路由信息只能选择一个路由表项生效，该生效的路由表项在表项前通过“>”表示。

通过 show ip route A.B.C.D/MASK detail 可以看到该路由的多个来源，以及其中的 distance 信息，选中的路由会标记 best。

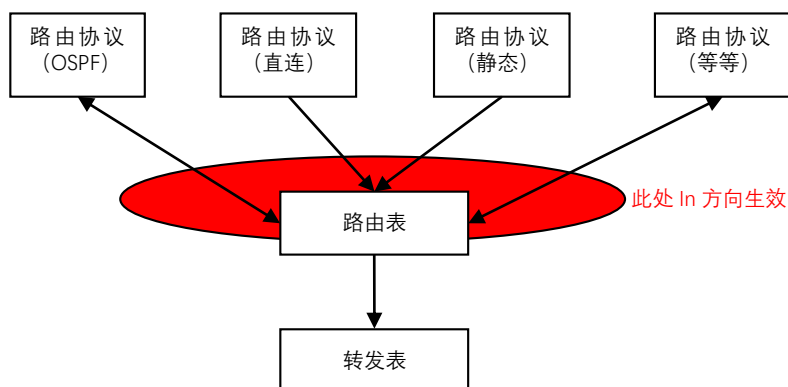
```
Routing entry for 192.100.6.0/24
  Known via "static", distance 1, metric 0
  Last update 00:00:10 ago
    unreachable (ICMP unreachable)

Routing entry for 192.100.6.0/24
  Known via "ospf", distance 110, metric 100
  Last update 04:42:06 ago
    directly connected, Vlan6

Routing entry for 192.100.6.0/24
  Known via "connected", distance 0, metric 0, best
  Last update 04:42:06 ago
    * directly connected, Vlan6
```

■ 路由过滤

路由过滤可以基于路由协议来配置，使用路由图来进行过滤。发生作用处如下图所示：



被过滤的路由信息，依然会生成路由表项，但是不生效，不会下发到转发表，因此，会影响到本地路由转发，同时，往动态路由协议重分布路由的时候，也会忽略掉过滤的路由信息。

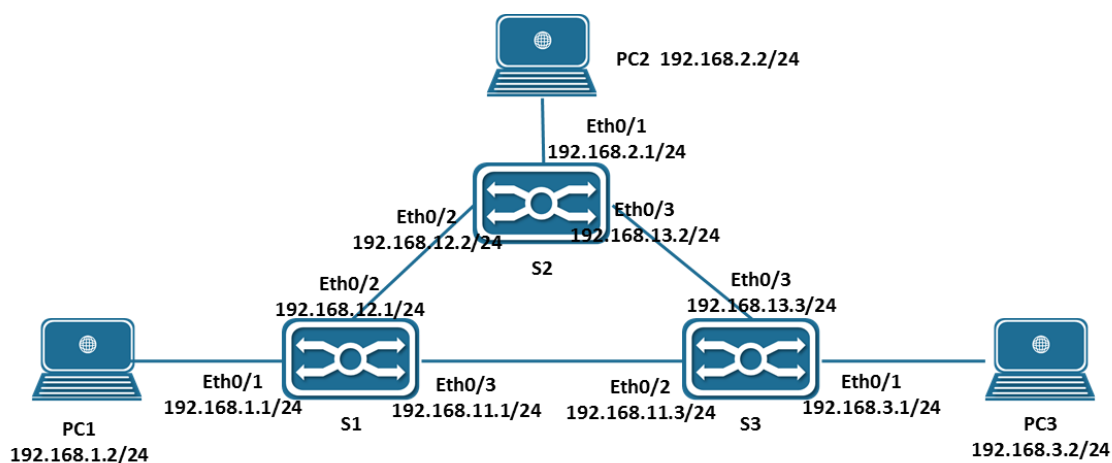
比如配置了静态路由的路由过滤，被过滤的静态路由不生效，若 OSPF 协议开启了重分布静态路由，被过滤掉的静态路由信息也不会分发到 OSPF 协议，通过 `show ip ospf database extern` 可以查看到 Type-5 LSA 的 Database (extern LSA) 没有过滤掉的静态路由信息。

## 2.2.2.2. 静态路由

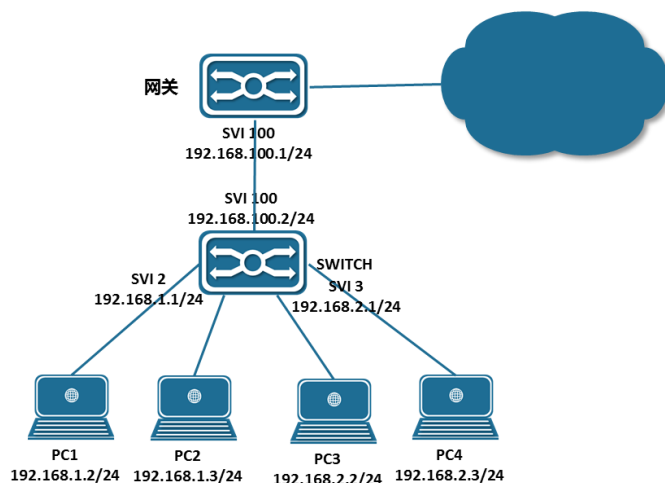
### ■ 使用场景

静态路由主要使用在如下两种场景：

- 组网比较简单的网络：只需要配置静态路由就可以实现网络互通。恰当地设置和使用静态路由可以改善网络的性能，并可为重要的网络应用保证带宽。本章的配置案例一即是此种情况。



- 存在弱三层网关的网络：本章的配置案例二即是此种情况。



该网络中涉及到静态路由的角色有两个：

- ✧ 弱三层网关设备（上图的 SWITCH）：当设备仅具备弱三层能力（不支持动态路由协议），设备可以作为弱三层网关，为开启路由协议的上一级设备节约一些路由资源和 ARP 资源。设备管理的若干个网络中，终端的网关均为该设备，弱三层网关设备只需要配置一条缺省路由（属于静态路由，下一跳为真正的网关设备）即可。对上一级设备，只需要关注该弱三层网关管理了哪些网络即可，不用生成终端对应的 ARP 表项和主机路由，可以节约资源。
- ✧ 下联弱三层网关的上一级设备（上图的网关）：由于该设备与终端间间隔了一个弱三层网关，而弱三层网关又不支持动态路由协议，因此，该设备要获知有弱三层网关下有哪些网络，只能通过静态配置完成，一个网络配置一条静态路由（或者多个网络汇聚为一条），下一跳均为弱三层网关。

## ■ 下一跳配置

静态路由可以支持上一节描述的 4 种下一跳：Blackhole，Reject，三层出口和 IP 地址。可以针对同一个路由前缀配置多条路由表项。然后路由管理模块会进行优选，选择其中一个行为生效。

### ➤ 三层出口

静态路由由配置下一跳直接指定三层出口的方式，需要注意，路由所指定的主机或者网络可能并非在直连网络当中，结合前述的代理 ARP 功能，当本设备与目的设备之间的设备开启了代理 ARP 时，当命中本路由表项时，即可以通过报文的目的 IP 进行 ARP 查询得到链路层 MAC 地址（实际是中间设备的链路层 MAC 地址），从而将报文发往中间设备，中间设备再路由到真正的目的。

### ➤ IP 地址

静态路由配置下一跳为 IP 地址时，三层出口会根据 IP 地址自动获得。需要注意的是，在配置时，下一跳 IP 地址也不要求一定属于直连网络。静态路由配置和生效是两个过程，配置了即可在 `show ip route` 中看到，但该路由表项不一定有生效标志“>”。对静态路由表项而言，生效需要三个条件：

条件 1，若配置了路由管理针对静态路由的路由过滤，该路由未被过滤。

条件 2，该路由的下一跳 IP 地址可达（通过其他路由表项，可以路由到达配置的下一跳 IP）。

条件 3，路由优选过程，该路由表项在相同前缀的所有路由表项中 distance 最小。

若条件 1 或者条件 2 不满足，则该路由表项不参与路由优选过程（因为，选中该路由，实际也不生效）。

当配置的下一跳 IP 地址属于直连网络时，路由一定可达。当配置的下一跳 IP 地址不属于直连网络时，该路由就称为**递归路由**。递归路由在路由表中的下一跳会记录递归查找后的结果（即路由转发时真正的下一跳 IP 地址，该 IP 地址属于直连网络）。

比如：配置 ip route 192.230.3.0/24 133.133.0.5(133.133.0.5 不属于直连网络)。

133.133.0.5 可达时，路由表如下：

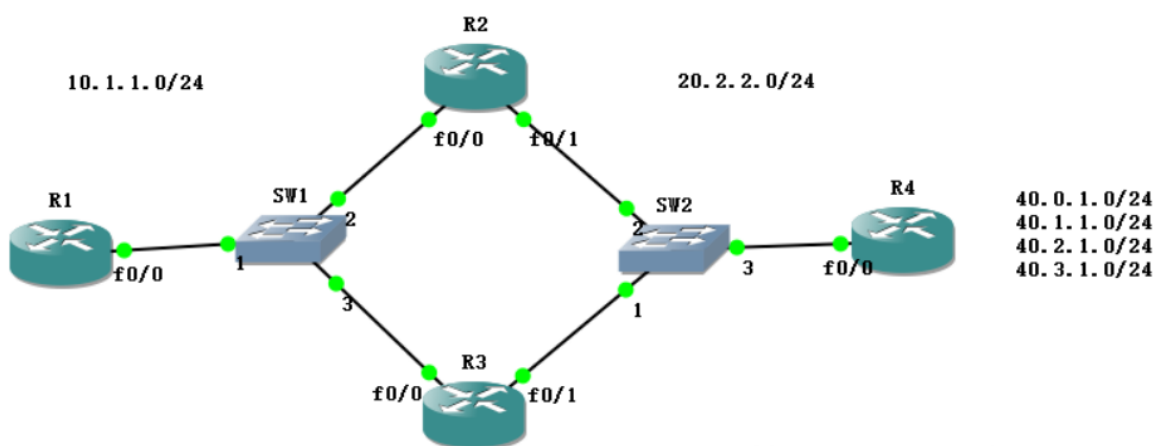
```
S>* 1.1.1.0/24 [1/0] via 192.168.3.11, Vlan1, 00:28:46
S> 192.230.3.0/24 [1/0] via 133.133.0.5 (recursive), 00:00:02
*                               via 192.10.10.100, Vlan100, 00:00:02
```

当 133.133.0.5 路由变为不可达，路由表变为：

```
S 192.230.3.0/24 [1/0] via 133.133.0.5 inactive, 00:03:57
```

（“>”表示该路由表项是有效的。“\*”表示下发到转发表，转发表用于 IP 报文的查找转发）

递归路由在实际使用当中可以简化配置和运维。如下图所示：



网络中只要配置好了 R1→R4 的路由，对 R4 所管理的 4 个网络，在 R1 上就不用管到达 R4 是走 R2 还是 R3，直接配置下一跳为 R4 即可。同样，当网络变动，需要修改配置时，递归路由往往也不用重新配置。如上图，假设在 R1 和 R4 间增加了一个 R5，R1→R4 的路由配置修改下一跳为 R5，但是 40.0.1.0/24 等 4 个网络的路由不用重新配置。

2.3. 配置命令

2.3.1. 路由策略

2.3.1.1. 过滤列表

■ 配置访问控制列表

命令	<p><b>配置 ACE (标准 ACL)：</b></p> <p>A:</p> <pre>FRR(config)#access-list ACL_ID (deny permit) A.B.C.D/M</pre> <p>B:</p> <pre>FRR(config)#access-list ACL_ID (deny permit) host A.B.C.D</pre> <p>C:</p> <pre>FRR(config)#access-list ACL_ID (deny permit) any</pre> <p><b>删除 ACE：</b></p> <pre>FRR(config)#no access-list ACL_ID (deny permit) A.B.C.D/M</pre> <pre>FRR(config)#no access-list ACL_ID (deny permit) host A.B.C.D</pre> <pre>FRR(config)#no access-list ACL_ID (deny permit) any</pre> <p><b>删除 ACL：</b></p> <pre>FRR(config)#no access-list ACL_ID</pre>
描述	<p>在全局模式下进行配置。</p> <p>ACL_ID 为： (&lt;1-99&gt; &lt;1300-1999&gt;)</p> <p>A: 定义一个网段范围。用于匹配时只要包含在网段范围内即可命中。可用于匹配前缀或者下一跳。</p> <p>B: 定义一个主机地址，可以用于匹配下一跳。</p> <p>C: 定义任意地址。可以匹配任何网段或者主机。可以用于匹配前缀或者下一跳。</p> <p>每次配置一条 ACE，放在 ACL 的末尾，不支持插入。</p> <p>ACE 的 KEY (唯一标识) 为： 行为 + 匹配范围。因此，相同的匹配范围，行为不同可以添加为 2 条 ACE。但是 KEY 相同的添加两次会认为重复添加。</p> <p>Deny 或者 permit 两种行为必须 2 选 1。</p> <p>删除配置，可以选择删除某个 ACE，或者删除整个 ACL。删除 ACE 时需要指定 ACE 的 KEY 信息。</p>

命令	<p><b>配置 ACE (zebra ACL)：</b></p> <p>A:</p> <pre>FRR(config)#access-list ACL_NAME (deny permit) A.B.C.D/M</pre> <p>B:</p> <pre>FRR(config)#access-list ACL_NAME (deny permit) A.B.C.D/M exact-math</pre> <p>C:</p> <pre>FRR(config)#access-list ACL_NAME (deny permit) any</pre>
----	--

	<p><b>删除 ACE:</b></p> <pre>FRR(config)#no access-list ACL_NAME (deny permit) A.B.C.D/M</pre> <pre>FRR(config)#no access-list ACL_NAME (deny permit) A.B.C.D/M exact-match</pre> <pre>FRR(config)#no access-list ACL_NAME (deny permit) any</pre> <p><b>删除 ACL:</b></p> <pre>FRR(config)#no access-list ACL_NAME</pre>
描述	<p>在全局模式下进行配置。</p> <p>A: 不带 exact-match 选项, 只要路由信息 (匹配目标是前缀或者下一跳) 包含在 ACE 定义的网络范围内即可。</p> <p>B: 带 exact-match 选项, 表示只有路由信息 (匹配目标是前缀或者下一跳, 下一跳的掩码当成 32) 与 ACE 完全相同才算匹配</p> <p>C: 表示该 ACE 匹配所有的路由信息。</p> <p>每次配置一条 ACE, 放在 ACL 的末尾, 不支持插入。</p> <p>ACE 的 KEY (唯一标识) 为: 行为 + 匹配范围。因此, 相同的匹配范围, 行为不同可以添加为 2 条 ACE。但是 KEY 相同的添加两次会认为重复添加。</p> <p>Deny 或者 permit 两种行为必须 2 选 1。</p> <p>删除配置, 可以选择删除某个 ACE, 或者删除整个 ACL。删除 ACE 时需要指定 ACE 的 KEY 信息。</p>

#### ■ 配置访问控制列表的 remark

命令	<p><b>设置 ACL 的 remark:</b></p> <pre>FRR(config)#access-list (ACL_ID   ACL_NAME) remark COMMENT</pre> <p><b>取消 ACL 的 remark:</b></p> <pre>FRR(config)# no access-list (ACL_ID   ACL_NAME) remark</pre>
描述	<p>在全局模式下进行配置。</p> <p>ACL_ID 用于表示标准 ACL。取值范围为 (&lt;1-199&gt;   &lt;1300-1999&gt;)。</p> <p>ACL_NAME 用于表示 Zebra ACL。</p> <p>该命令为 ACL 设置一个描述信息。ACL 名字不适宜取太长, 可以通过 remark 对其进行描述, 当环境中配置有多个 ACL 的时候, 避免混淆。</p>

#### ■ 配置地址前缀列表

命令	<p><b>配置前缀列表表项</b></p> <p>A:</p> <pre>FRR(config)#ip prefix-list NAME [seq &lt;1-4294967295&gt;] (deny permit)</pre> <pre>A.B.C.D/M [ge &lt;0-32&gt;   le &lt;0-32&gt;]</pre> <p>B:</p> <pre>FRR(config)#ip prefix-list NAME [seq &lt;1-4294967295&gt;] (deny permit) any</pre>
----	---

	<p><b>删除前缀列表表项</b></p> <pre>FRR(config)#no ip prefix-list NAME [seq &lt;1-4294967295&gt;] (deny permit) A.B.C.D/M [ge &lt;0-32&gt;   le &lt;0-32&gt;]</pre> <p><b>删除整个前缀列表:</b></p> <pre>FRR(config)#no ip prefix-list NAME</pre>
描述	<p>在全局模式下进行配置。</p> <p>A:配置一个匹配范围，当没有带 le 和 ge 参数时，需要精确匹配，只有路由信息掩码长度等于配置的掩码长度时才能匹配。当配置至少一个参数时，匹配的掩码范围为 [ge, le]。ge 默认值等于配置的掩码长度，le 默认值等于 32。配置的 ge 和 le 需要满足要求：mask-len &lt; ge &lt;= le &lt;= 32。</p> <p>B: 该表项匹配所有的路由信息。</p> <p>Seq 用于配置表项的序号，用于表项间排序。表项按照序号自小到大排序。可以通过 no routing prefix-list sequence-num 关闭排序功能。</p> <p>表项的 KEY（唯一标识）为：seq-number 或者 行为 + 匹配范围。两种 KEY 均唯一对应一条表项。配置某个已经存在的序号的表项，将对原有表项进行更新操作。</p> <p>Deny 或者 permit 两种行为必须 2 选 1。</p> <p>删除配置，可以选择删除某个表项，或者删除整个地址前缀列表。删除表项时行为 + 匹配范围必选，seq 可选。</p>

#### ■ 配置地址前缀列表的排序功能

命令	<p><b>关闭地址前缀列表排序功能:</b></p> <pre>FRR(config)#no ip prefix-list sequence-num</pre> <p><b>开启地址前缀列表排序功能:</b></p> <pre>FRR(config)#ip prefix-list sequence-num</pre>
描述	<p>在全局模式下进行配置。默认该功能开启。</p> <p>当关闭了排序功能，配置的地址前缀列表表项中的序号会无意义，通过 show run 可以看到，配置信息中自动隐藏了序号信息。当开启排序功能，序号信息又会出现。</p>

#### ■ 配置地址前缀列表的 description

命令	<p><b>设置地址前缀列表的 description:</b></p> <pre>FRR(config)#ip prefix-list NAME description COMMENT</pre> <p><b>取消地址前缀列表的 description:</b></p> <pre>FRR(config)# ip prefix-list NAME description</pre>
描述	<p>在全局模式下进行配置。</p>



	该命令为地址前缀列表设置一个描述信息。当环境中配置有多个地址前缀列表的时候，避免混淆。
--	---

■ 清除地址前缀列表的统计值

命令	<p><b>清除某个地址前缀列表的统计值：</b></p> <pre>FRR#clear ip prefix-list NAME</pre> <p><b>清除全部地址前缀列表的统计值：</b><pre>FRR# clear ip prefix-list</pre></p>
描述	<p>在特权模式下进行清除操作。</p> <p>地址前缀列表模块会对查询命中情况进行统计（通过 show routing prefix-list 相关命令可以看到），该命令用于对统计值清 0。</p>

2.3.1.2. 路由图

■ 创建删除策略

命令	<p><b>创建策略并进入该策略的路由图模式</b></p> <pre>FRR(config)#route-map NAME (deny permit) seq-number(&lt;1-65535&gt;)</pre> <pre>FRR(config-route-map)#</pre> <p><b>删除策略</b></p> <pre>FRR(config)#no route-map NAME (deny permit) seq-number(&lt;1-65535&gt;)</pre> <p><b>删除路由图</b></p> <pre>FRR(config)# no route-map NAME</pre>
描述	<p>如果策略已经存在，route-map 命令仅仅用于进入策略的路由图模式，进入路由图模式后进行的相关配置都是针对该策略的。</p> <p>策略的 KEY（唯一标识）是 seq-number，deny 和 permit 仅仅是设置该策略的行为模式，若某条已存在的策略（比如路由图名为 test，seq-number 为 1）行为模式为 permit，使用 route-map test deny 1 除了进入该策略外，还会将该策略的行为模式修改为 deny。</p> <p>Deny 的策略用于过滤，permit 的策略用于修改路由信息。</p> <p>Seq-number 也表示了该策略在路由图中的优先级关系，策略按照 seq-number 从小到大排列，seq-number 越小，越优先进行匹配处理。</p> <p>可以一次性删除整个路由图，此时会删除该路由图中的所有策略。</p> <p>虽然策略的 KEY 只是 seq-number，但是在删除策略的时候，需要携带行为模式参数，并且会对该参数进行检查，如果行为模式不匹配（比如策略的行为模式为 permit，删除时使用 deny），会删除失败。</p>

■ 配置策略匹配条件

命令	<p><b>匹配路由的三层出口：</b></p> <pre>FRR(config-route-map)#match interface IFNAME</pre> <p><b>取消匹配路由的三层出口：</b><pre>FRR(config-route-map)#no match interface (IFNAME )</pre></p>
描述	<p>路由图模式下进行配置。</p> <p>一条策略只能匹配一个三层出口，当某策略已经配置匹配三层出口的时候，再配置匹配另外一个三层出口，将会覆盖原来的配置。</p> <p>配置了匹配三层出口的的策略，不能匹配任何 Blackhole 路由和 Reject 路由。</p> <p>删除配置时，IFNAME 参数可选。</p>

命令	<p><b>匹配路由的前缀：</b></p> <pre>FRR(config-route-map)#match ip address (ACL_ID ACL_NAME prefix-len &lt;0-32&gt; prefix-list PRELIST_NAME)</pre> <p><b>取消匹配路由的前缀：</b></p> <p><b>取消关联 ACL 配置：</b></p> <pre>FRR(config-route-map)#no match ip address (ACL_ID ACL_NAME )</pre> <p><b>取消关联 prefix-list 配置：</b></p> <pre>FRR(config-route-map)#no match ip address prefix-list (PRELIST_NAME )</pre> <p><b>取消 prefix-len 配置：</b></p> <pre>FRR(config-route-map)#no match ip address prefix-len (&lt;0-32&gt; )</pre>
描述	<p>路由图模式下进行配置。</p> <p>有如下三种匹配方式：</p> <ol style="list-style-type: none"><li>1 关联 ACL 进行匹配 <i>ACL_ID</i> 用于表示标准 ACL。取值范围为(&lt;1-199&gt;   &lt;1300-1999&gt;)。 <i>ACL_NAME</i> 用于表示 Zebra ACL。</li><li>2 关联 prefix-list 进行匹配</li><li>3 按照前缀长度进行匹配</li></ol> <p>每种匹配方式只能配置一个值（比如只能关联一个 ACL）。但可以同时配置多种匹配方式，此时，路由信息的前缀必须同时满足多个匹配条件，才会与策略匹配。</p> <p>取消配置时，变参可选。</p>

命令	<p><b>匹配路由的下一跳：</b></p> <pre>FRR(config-route-map)#match ip next-hop (ACL_ID ACL_NAME prefix-len &lt;0-32&gt; prefix-list PRELIST_NAME)</pre> <p><b>取消匹配路由的下一跳：</b></p> <p><b>取消关联 ACL 配置：</b></p> <pre>FRR(config-route-map)#no match ip next-hop (ACL_ID ACL_NAME )</pre>
----	---

	<p><b>取消关联 prefix-list 配置：</b>  FRR(config-route-map)#no match ip next-hop prefix-list (PRELIST_NAME )</p> <p><b>取消 prefix-len 配置：</b>  FRR(config-route-map)#no match ip next-hop prefix-len (&lt;0-32&gt; )</p>
描述	<p>路由图模式下进行配置。</p> <p>有如下三种匹配方式：</p> <ol style="list-style-type: none"> <li>1 关联路由 ACL 进行匹配  ACL_ID 用于表示标准 ACL。取值范围为(&lt;1-199&gt;   &lt;1300-1999&gt;)。  ACL_NAME 用于表示 Zebra ACL。</li> <li>2 关联 prefix-list 进行匹配</li> <li>3 按照掩码长度进行匹配，由于下一跳的掩码长度固定为 32，所以，该匹配方式对下一跳的结果只有两种： <ol style="list-style-type: none"> <li>1) 配置 32（或者未配置），该匹配方式会匹配所有路由信息的下一跳</li> <li>2) 配置非 32，该匹配方式对所有路由信息的下一跳均不匹配。</li> </ol> </li> </ol> <p>每种匹配方式只能配置一个值（比如只能关联一个 ACL）。但可以同时配置多种匹配方式，此时，路由信息的下一跳必须同时满足多个匹配条件，才会与策略匹配。</p> <p>需要注意的时，下一跳有 4 种行为，只有当下一跳为 IP 地址时，策略的下一跳匹配才有可能匹配，而对其他三类（Blackhole, Reject, 三层出口），配置了下一跳匹配的策略，都无法匹配。</p> <p>取消配置时，变参可选。</p>

命令	<p><b>匹配路由的通告源：</b>  FRR(config-route-map)#match ip route-source (ACL_ID ACL_NAME prefix-list PRELIST_NAME)</p> <p><b>取消匹配路由的通告源：</b></p> <p><b>取消关联 ACL 配置：</b>  FRR(config-route-map)#no match ip route-source (ACL_ID ACL_NAME )</p> <p><b>取消关联 prefix-list 配置：</b>  FRR(config-route-map)#no match ip route-source prefix-list (PRELIST_NAME )</p>
描述	<p>路由图模式下进行配置。</p> <p>路由协议中的每条路由都有一个通告的来源。该来源用一个 IP 地址表示。</p> <p>有如下两种匹配方式：</p> <ol style="list-style-type: none"> <li>1 关联路由 ACL 进行匹配  ACL_ID 用于表示标准 ACL。取值范围为(&lt;1-199&gt;   &lt;1300-1999&gt;)。  ACL_NAME 用于表示 Zebra ACL。</li> <li>2 关联 prefix-list 进行匹配</li> </ol> <p>每种匹配方式只能配置一个值（比如只能关联一个 ACL）。但可以同时配置多种匹配方式，此时，路由信息的通告来源必须同时满足多个匹配条件，才会与策略匹配。</p> <p>取消配置时，变参可选。</p>

命令	<p><b>匹配路由的 metric 值:</b> FRR(config-route-map)#<b>match metric</b> &lt;0-4294967295&gt;</p> <p><b>取消匹配路由的 metric 值:</b> FRR(config-route-map)#<b>no match metric</b> (&lt;0-4294967295&gt; )</p>
描述	<p>路由图模式下进行配置。</p> <p>动态路由协议生成的路由存在 metric 值，用于协议内进行路由计算使用。</p> <p>一个策略只能匹配一个 metric，当需要匹配多个 metric 值时，需要拆分成多个策略完成。</p> <p>取消配置时，变参可选。</p>

命令	<p><b>匹配路由的源协议:</b> FRR(config-route-map)#<b>match source-protocol</b> (connected ospf rip isis bgp static)</p> <p><b>取消匹配路由的源协议:</b> FRR(config-route-map)#<b>no match source-protocol</b> (connected ospf rip isis bgp static )</p>
描述	<p>路由图模式下进行配置。</p> <p>每条路由都有来源，来源即生成路由的对应协议这里进行匹配的就是路由来源。一个策略只能配置一个路由来源，当需要匹配多个路由来源时，需要拆分成多个策略完成。</p> <p>取消配置时，来源参数可选。</p>

命令	<p><b>匹配路由的 Tag:</b> FRR(config-route-map)#<b>match tag</b> &lt;0-4294967295&gt;</p> <p><b>取消匹配路由的 Tag:</b> FRR(config-route-map)#<b>no match tag</b> (&lt;0-4294967295&gt; )</p>
描述	<p>路由图模式下进行配置。</p> <p>动态生成的路由或者静态配置的路由，均可以指定 Tag（比如静态路由，在配置时可以通过 tag 参数指定其 Tag 的值），作为路由的一个分类标记。路由图可以匹配 Tag，从而匹配相应的路由。</p> <p>一个策略只能匹配一个 Tag，当需要匹配多个 Tag 值时，需要拆分成多个策略完成。</p> <p>取消配置时，变参可选。</p>

命令	<p><b>匹配 BGP 路由的 local_preferance:</b> FRR(config-route-map)#<b>match local_preferance</b> &lt;0-4294967295&gt;</p>
----	---

	<b>取消匹配 BGP 路由的 local-preference:</b> FRR(config-route-map)#no match local_preference (<0-4294967295>   )
描述	路由图模式下进行配置。 仅针对 BGP 路由有效。用于匹配 BGP 路由的 local_preference (即 metric)。 取消配置时, 变参可选。

命令	<b>匹配 BGP 路由的 origin code:</b> FRR(config-route-map)#match origin (egp igp incomplete)  <b>取消匹配 BGP 路由的 origin code:</b> FRR(config-route-map)#no match origin (egp igp incomplete )
描述	路由图模式下进行配置。 仅针对 BGP 路由有效。用于匹配 BGP 路由的来源。 egp: 表示来源于远端的 EGP。 igp: 表示来源于本地的 IGP。 incomplete: 表示来源未知。  取消配置时, 参数可选。

命令	<b>匹配 BGP 路由的 AS-PATH 属性:</b> FRR(config-route-map)#match as-path as_path_name  <b>取消匹配 BGP 路由的 AS-PATH 属性:</b> FRR(config-route-map)#no match as-path (as_path_name   )
描述	路由图模式下进行配置。 仅针对 BGP 路由有效。 用于匹配 BGP 路由的 AS-PATH 属性, 该策略关联到 AS-PATH 列表, 由 AS-PATH 列表确定 BGP 路由是否匹配。AS-PATH 列表使用正则表达式, AS-PATH 列表相关配置以及具体匹配规则参见“配置 BGP”章节中关于 AS-PATH 的说明。 取消配置时, 变参可选。

命令	<b>匹配 BGP 路由的 COMMUNITY 属性:</b> FRR(config-route-map)#match community (<1-99>   <100-500>   community_list_name)  <b>取消匹配 BGP 路由的 COMMUNITY 属性:</b>
----	--

	<code>FRR(config-route-map)#no match community (&lt;1-99&gt;   &lt;100-500&gt;   community_list_name   )</code>
描述	<p>路由图模式下进行配置。</p> <p>仅针对 BGP 路由有效。</p> <p>用于匹配 BGP 路由的 COMMUNITY 属性，该策略关联到 COMMUNITY 列表，由 COMMUNITY 列表确定 BGP 路由是否匹配。</p> <p>COMMUNITY 列表可以用 ID 表示，1-99 表示标准表项，100-500 表示扩展表项；也可以使用列表名字表示。</p> <p>COMMUNITY 列表相关配置以及具体匹配规则参见“配置 BGP”章节中关于 COMMUNITY 的说明。</p> <p>取消配置时，变参可选。</p>

#### ■ 配置策略的处理动作

策略的处理动作只有当策略行为模式为 permit 时才有意义。

命令	<p><b>设置 OSPF 外部路由的 metric-type:</b></p> <code>FRR(config-route-map)#set metric-type (type-1 type-2)</code>
	<p><b>取消设置 OSPF 外部路由的 metric-type:</b></p> <code>FRR(config-route-map)#no set metric-type (type-1 type-2 )</code>
描述	<p>路由图模式下进行配置。</p> <p>该命令仅仅针对 OSPF 重分布路由时（对 OSPF 协议来说，是外部路由）设置 metric 类型。</p> <p>Type-1: 外部路由类型 E-1, 计算外部路由时，AS 域内 metric 纳入 OSPF 协议计算。</p> <p>Type-2: 外部路由类型 E-2, 计算外部路由时，AS 域内 metric 忽略。</p> <p>默认是 Type-2。</p> <p>在取消配置时，type 类型可选。</p>

命令	<p><b>设置路由的 metric:</b></p> <code>FRR(config-route-map)#set metric &lt;0-4294967295&gt;</code>
	<p><b>取消设置路由的 metric:</b></p> <code>FRR(config-route-map)#no set metric (&lt;0-4294967295&gt; )</code>
描述	<p>路由图模式下进行配置。</p> <p>此 set 规则用来修改路由的度量值 (metric)。</p> <p>在取消配置时，metric 值可选。</p>

命令	<p><b>设置路由的 Tag:</b></p> <code>FRR(config-route-map)#set tag &lt;0-4294967295&gt;</code>
----	--

	<b>取消设置路由的 tag:</b> FRR(config-route-map)#no set tag (<0-4294967295> )
描述	路由图模式下进行配置。 此 set 规则用来修改路由的标记值 (tag)。 在取消配置时, tag 值可选。

命令	<b>设置 BGP 路由的 AS-PATH 属性:</b> <b>剥除 AS_NUM:</b> A: FRR(config-route-map)#set as-path exclude AS_NUM... <b>添加 AS_NUM:</b> B: FRR(config-route-map)#set as-path prepend (AS_NUM   last-as INSERT_NUM)  <b>取消设置 BGP 路由的 AS-PATH 属性:</b> C: FRR(config-route-map)#no set as-path exclude AS_NUM D: FRR(config-route-map)#no set as-path prepend (AS_NUM  )
描述	路由图模式下进行配置。 AS_NUM : 取值范围为: 1-4294967295。 A: 将 BGP 路由的 AS-PATH 中的对应 AS_NUM 剥除掉。(设置的 AS_NUM 可以有若干个) B: 往 BGP 路由的 AS-PATH 中添加 AS_NUM。可以直接根据配置的 AS_NUM 添加, 也可使用最后一个 AS_NUM 来重复添加。INSERT_NUM 表示重复添加的次数。 在取消配置时, tag 值可选。

命令	<b>设置 BGP 路由自动聚合:</b> FRR(config-route-map)#set atomic-aggregate  <b>取消设置 BGP 路由自动聚合:</b> FRR(config-route-map)#no set atomic-aggregate
描述	路由图模式下进行配置。 用于设置 BGP 路由的 atomic-aggregate 属性

命令	<b>设置 BGP 路由的 COMMUNITY 属性:</b> FRR(config-route-map)#set community (none   COMMUNITY_NUM... [additive])  <b>取消设置 BGP 路由的 COMMUNITY 属性:</b> FRR(config-route-map)#no set community (COMMUNITY_NUM... [additive]   )
----	---

描述	<p>路由图模式下进行配置。</p> <p>用于设置 BGP 路由的 COMMUNITY 属性。</p> <p>none：表示清空 COMMUNITY 属性。</p> <p>additive：表示将设置的若干个 COMMUNITY_NUM 添加到原有的 COMMUNITY 属性上。</p> <p>COMMUNITY_NUM 的可能格式如下：</p> <ol style="list-style-type: none"> <li>1) AA:NN AA 和 NN 的取值范围均为 0-65535。</li> <li>2) 知名团队名称：（local-AS no-advertise no-export internet）</li> </ol>
----	---

命令	<p><b>设置 BGP 路由的 COMMUNITY 属性（删除某些 COMMUNITY_NUM）：</b></p> <pre>FRR(config-route-map)#set comm-list (&lt;1-99&gt;   &lt;100-500&gt;   community_list_name) delete</pre> <p><b>取消设置 BGP 路由的 COMMUNITY 属性：</b></p> <pre>FRR(config-route-map)#no set comm-list (&lt;1-99&gt;   &lt;100-500&gt;   community_list_name   ) delete</pre>
描述	<p>路由图模式下进行配置。</p> <p>根据 COMMUNITY 列表中定义的 COMMUNITY_NUM，从路由的 COMMUNITY 属性中删除。</p> <p>COMMUNITY 列表可以用 ID 表示，1-99 表示标准表项，100-500 表示扩展表项；也可以使用列表名字表示。</p> <p>COMMUNITY 列表相关配置以及具体匹配规则参见“配置 BGP”章节中关于 COMMUNITY 的说明。</p>

命令	<p><b>设置 BGP 路由的 local_preference 属性：</b></p> <pre>FRR(config-route-map)#set local_preference &lt;0-4294967295&gt;</pre> <p><b>取消设置 BGP 路由的 local-preference 属性：</b></p> <pre>FRR(config-route-map)#no set local_preference (&lt;0-4294967295&gt;   )</pre>
描述	<p>路由图模式下进行配置。</p> <p>仅针对 BGP 路由有效。用于设置 BGP 路由的 local_preference（即 metric）。</p>

命令	<p><b>设置 BGP 路由的 originator-id 属性：</b></p> <pre>FRR(config-route-map)#set originator-id IP_ADDR</pre> <p><b>取消设置 BGP 路由的 originator-id 属性：</b></p> <pre>FRR(config-route-map)#no set originator-id (IP_ADDR   )</pre>
描述	<p>路由图模式下进行配置。</p> <p>仅针对 BGP 路由有效。用于设置 BGP 路由的 originator-id 属性，该属性用于记录本 AS 中原始通告该路由的路由设备的 Router ID。</p>



## ■ 配置策略的跳转

策略的跳转只有当策略行为模式为 permit 时才有意义。

命令	<p><b>在路由图内部跳转：</b></p> <p><b>跳转到指定 sn 的策略：</b></p> <pre>FRR(config-route-map)#on-match goto &lt;1-65535&gt;</pre> <p><b>跳转到相邻的下一条策略：</b></p> <pre>FRR(config-route-map)#on-match next</pre> <p><b>取消跳转配置：</b></p> <pre>FRR(config-route-map)#no on-match goto</pre> <pre>FRR(config-route-map)#no on-match next</pre>
描述	<p>路由图模式下进行配置。</p> <p>该配置用于当路由匹配中该策略时的内部跳转策略。默认不跳转，退出路由图，当指定跳转策略时按照指定策略进行跳转。</p> <p>对一条策略只能配置一个内部跳转策略。</p>

命令	<p><b>跨路由图跳转：</b></p> <pre>FRR(config-route-map)#call ROUTEMAP_NAME</pre> <p><b>取消跳转配置：</b></p> <pre>FRR(config-route-map)#no call</pre>
描述	<p>路由图模式下进行配置。</p> <p>该配置用于当路由匹配中该策略时的外部跳转策略。默认不跳转，只处理当前路由图。</p> <p>对一条策略只能配置一个外部跳转策略。</p>

## ■ 配置策略的 description

命令	<p><b>设置策略的 description：</b></p> <pre>FRR(config-route-map)#description COMMENT</pre> <p><b>取消策略的 description：</b></p> <pre>FRR(config)# no description</pre>
描述	<p>路由图模式下进行配置。</p> <p>该命令为路由图策略设置一个描述信息。当环境中配置有多个策略的时候，避免混淆。</p>

## ■ 配置路由图的延迟生效时间

命令	<p><b>设置路由图的 delay-timer</b>  FRR(config)#route-map delay-timer &lt;0-600&gt;</p> <p><b>取消设置路由图的 delay-timer</b>  FRR(config)# no route-map delay-timer (&lt;0-600&gt; )</p>
描述	<p>全局模式下进行配置。</p> <p>路由图配置后，需要事件驱动应用路由图的模块进行更新。该事件驱动有一定的延迟时间。<b>默认为 5S。</b></p> <p>可以通过该命令修改延迟时间。当<b>配置的延迟时间为 0，表示不进行事件驱动。</b>即路由图对后续应用的模块生效，之前已经应用的模块不生效，若需要触发生效，需要取消应用，再重新应用。</p> <p>在取消配置时，延迟时间不进行校验，均可恢复为默认值 5S。</p>

### 2.3.2. 路由管理

#### ■ 配置全局 router-id

命令	<p><b>配置全局 router-id</b>  router-id A.B.C.D</p> <p><b>删除全局 router-id 配置</b>  no router-id [A.B.C.D]</p>
描述	<p>全局模式下进行配置。</p> <p>当路由协议中未设置 router-id 时，会使用全局设置的 router-id。</p>

#### ■ 配置静态路由

命令	<p><b>设置 Blackhole 路由：</b>  FRR(config)# ip route PREFIX blackhole [&lt;1-255&gt; tag &lt;1-4294967295&gt;]</p> <p><b>设置 Reject 路由：</b>  FRR(config)# ip route PREFIX reject [&lt;1-255&gt; tag &lt;1-4294967295&gt;]</p> <p><b>设置三层出口路由：</b>  FRR(config)# ip route PREFIX IFNAME [&lt;1-255&gt; tag &lt;1-4294967295&gt;]</p> <p><b>设置 IP 地址路由：</b>  FRR(config)# ip route PREFIX NH(A.B.C.D) [&lt;1-255&gt; tag &lt;1-4294967295&gt;]</p> <p><b>取消路由配置：</b>  FRR(config)# no ip route PREFIX blackhole [&lt;1-255&gt; tag &lt;1-4294967295&gt;]  FRR(config)# no ip route PREFIX reject [&lt;1-255&gt; tag &lt;1-4294967295&gt;]  FRR(config)# no ip route PREFIX IFNAME [&lt;1-255&gt; tag &lt;1-4294967295&gt;]  FRR(config)# no ip route PREFIX NH(A.B.C.D) [&lt;1-255&gt; tag &lt;1-4294967295&gt;]</p>
描述	<p>全局模式下进行配置。</p> <p>PREFIX 采用 A.B.C.D/M 的格式。</p>

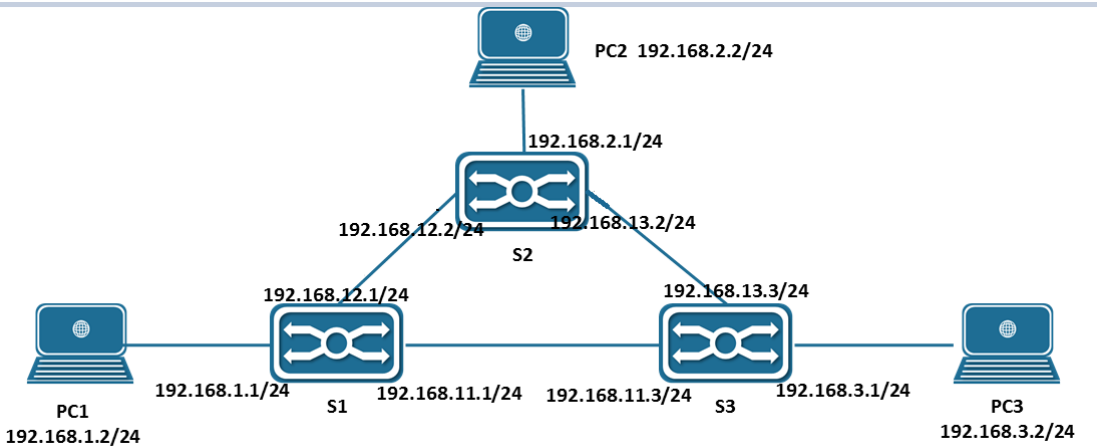
	<p>静态路由的下一跳有 4 种方式：blackhole，reject，三层出口，IP 地址。</p> <p>有两个可选参数，可以配置 0-2 个。</p> <p>&lt;1-255&gt;：指定该路由的 distance 值。</p> <p>tag &lt;1-4294967295&gt;：指定该路由的标记值。</p> <p>当需要修改路由的参数（distance 或者 tag）时，可以再配置一次进行更新。在删除路由时，下一跳的 4 种方式也是必选参数，若前缀匹配，但是下一跳不匹配，将会删除失败。</p>
--	--

■ 应用路由过滤

命令	<p><b>应用路由过滤：</b></p> <pre>FRR(config)# ip protocol (connected static ospf rip isis bgp any) route-map RM_NAME</pre> <p><b>取消路由过滤：</b></p> <pre>FRR(config)# no ip protocol (connected static  ospf rip isis bgp  any) route-map RM_NAME FRR(config)# no ip protocol (connected static  ospf rip isis bgp  any)</pre>
描述	<p>全局模式下进行配置。</p> <p>针对每个路由协议进行路由管理的路由过滤。使用 any 表示所有路由协议都进行路由过滤。</p> <p>取消配置时，两种方式等价。</p>

2.4. 配置案例

■ 案例一：内网三层互联



如上图的网络环境，PC1，PC2 和 PC3 分别通过 S1，S2 和 S3 进行互联。

➤ 配置 PC

PC1，PC2 和 PC3 按照如图所示配置 IP 地址，同时指定网关，比如 PC1 的网关为 192.168.1.1。

### ➤ 配置 S1

- ✧ 配置三层口和 IP 地址：（主 CLI 模式）（假设 gigabitEthernet 0/1 连接 PC1，gigabitEthernet 0/2 连接 S2，gigabitEthernet 0/3 连接 S3）

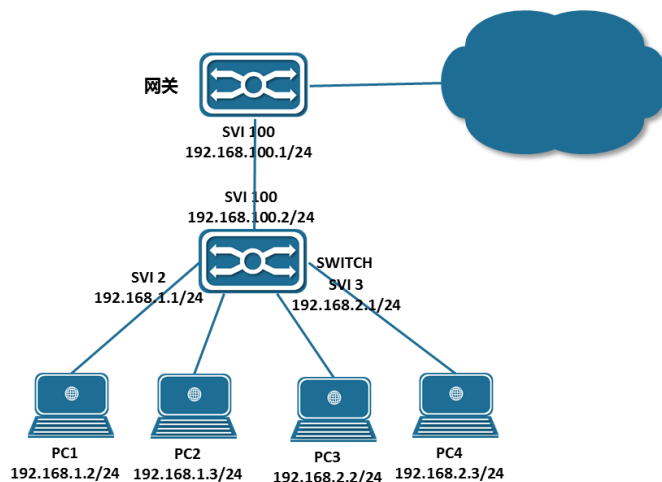
```
SWITCH(config)#vlan 2-4
SWITCH(config)#interface gigabitEthernet 0/1
SWITCH(config-if)#switch access vlan 2
SWITCH(config)#interface gigabitEthernet 0/2
SWITCH(config-if)#switch access vlan 3
SWITCH(config)#interface gigabitEthernet 0/3
SWITCH(config-if)#switch access vlan 4
SWITCH(config)#int Vlan2
SWITCH(config-if)#ip address 192.168.1.1/24
SWITCH(config)#int Vlan3
SWITCH(config-if)#ip address 192.168.12.1/24
SWITCH(config)#int Vlan4
SWITCH(config-if)#ip address 192.168.13.1/24
```

- ✧ 配置静态路由：（FRR CLI 模式）

```
FRR(config)#ip route 192.168.2.0/24 192.168.12.2
FRR(config)#ip route 192.168.3.0/24 192.168.11.3
```

S2 和 S3 类似 S1 的配置。

### ■ 案例二 弱三层网关



Switch 作为弱三层网关，为真正的网关减少 ARP 负担。

### ➤ 配置 PC：

PC1, PC2 和 PC3 按照如图所示配置 IP 地址，同时指定网关，比如 PC1 和 P2 的网关为 192.168.1.1。

### ➤ 配置 SWITCH：

- ✧ 配置三层口和 IP 地址：（假设连接 PC1-PC4 的接口为 gigabitEthernet 0/1-4，上链接口为 gigabitEthernet 0/17）（主 CLI 模式）

```
SWITCH(config)#vlan 2-3,100
SWITCH(config)#interface gigabitEthernet 0/1-2
SWITCH(config-if)#switch access vlan 2
SWITCH(config)#interface gigabitEthernet 0/3-4
SWITCH(config-if)#switch access vlan 3
SWITCH(config)#interface gigabitEthernet 0/17
SWITCH(config-if)#switch access vlan 100
SWITCH(config)#int Vlan2
SWITCH(config-if)#ip address 192.168.1.1/24
SWITCH(config)#int Vlan3
SWITCH(config-if)#ip address 192.168.2.1/24
SWITCH(config)#int Vlan100
SWITCH(config-if)#ip address 192.168.100.2/24
```

✧ 配置静态路由（默认路由）：（FRR CLI 模式）

```
FRR(config)#ip route 0.0.0.0/0 192.168.100.1
```

➤ 配置网关：（三层口配置忽略）

✧ 配置静态路由：

```
FRR(config)#ip route 192.168.1.0/24 192.168.100.2
FRR(config)#ip route 192.168.2.0/24 192.168.100.2
```

## 2.5. 显示命令

### 2.5.1. 路由策略

#### ■ 查看路由 ACL

假设路由 ACL 配置如下：

```
access-list test remark fordod
access-list test permit 133.133.0.0/24
access-list test permit 192.168.3.0/24 exact-match
access-list test deny any
access-list test1 permit 100.100.0.0/16
access-list test1 deny 192.168.2.0/24 exact-match
```

➤ 查看名为 test 的 ACL

```
FRR#show ip access-list test
ZEBRA:
Zebra IP access list test
    permit 133.133.0.0/24
    permit 192.168.3.0/24 exact-match
    deny any
OSPF:
Zebra IP access list test
```

```

    permit 133.133.0.0/24
    permit 192.168.3.0/24 exact-match
deny    any
...

```

➤ 查看所有 ACL

```

FRR#show ip access-list
ZEBRA:
Zebra IP access list test
    permit 133.133.0.0/24
    permit 192.168.3.0/24 exact-match
    deny    any
Zebra IP access list test1
    permit 100.100.0.0/16
    deny    192.168.2.0/24 exact-match
OSPF:
Zebra IP access list test
    permit 133.133.0.0/24
    permit 192.168.3.0/24 exact-match
    deny    any
Zebra IP access list test1
    permit 100.100.0.0/16
deny    192.168.2.0/24 exact-match
...

```

■ 查看地址前缀列表

假设地址前缀列表配置如下：

```

ip prefix-list prelist-in description ospf_filterlist_in
ip prefix-list prelist-in seq 5 permit 192.200.2.0/24
ip prefix-list test seq 5 permit 133.133.0.0/24
ip prefix-list test seq 8 deny any
ip prefix-list test seq 10 permit any

```

➤ 查看地址前缀列表

按照地址前缀列表名称查看：

```

FRR#show ip prefix-list test
ZEBRA: ip prefix-list test: 3 entries
    seq 5 permit 133.133.0.0/24
    seq 8 deny any
    seq 10 permit any
OSPF: ip prefix-list test: 3 entries
    seq 5 permit 133.133.0.0/24
    seq 8 deny any
    seq 10 permit any

```

查看所有地址前缀列表：

```

FRR#show routing prefix-list
ZEBRA: ip prefix-list prelist-in: 1 entries
  Description: ospf_filterlist_in
  seq 5 permit 192.200.2.0/24
ZEBRA: ip prefix-list test: 3 entries
  seq 5 permit 133.133.0.0/24
  seq 8 deny any
  seq 10 permit any
OSPF: ip prefix-list prelist-in: 1 entries
  Description: ospf_filterlist_in
  seq 5 permit 192.200.2.0/24
OSPF: ip prefix-list test: 3 entries
  seq 5 permit 133.133.0.0/24
  seq 8 deny any
  seq 10 permit any

```

➤ 查看地址前缀列表 summary

按照地址前缀列表名称查看:

```

FRR#show ip prefix-list summary test
ZEBRA: ip prefix-list test:
  count: 3, range entries: 0, sequences: 5 - 10
OSPF: ip prefix-list test:
  count: 3, range entries: 0, sequences: 5 - 10
...

```

查看所有地址前缀列表:

```

FRR #show ip prefix-list summary
Prefix-list with the last deletion/insertion: test
ZEBRA: ip prefix-list prelist-in:
  Description: ospf_filterlist_in
  count: 1, range entries: 0, sequences: 5 - 5
ZEBRA: ip prefix-list test:
  count: 3, range entries: 0, sequences: 5 - 10
Prefix-list with the last deletion/insertion: test
OSPF: ip prefix-list prelist-in:
  Description: ospf_filterlist_in
  count: 1, range entries: 0, sequences: 5 - 5
OSPF: ip prefix-list test:
  count: 3, range entries: 0, sequences: 5 - 10
...

```

➤ 查看地址前缀列表 detail

按照地址前缀列表名称查看:

```

FRR#show ip prefix-list detail test

```

```

ZEBRA: ip prefix-list test:
  count: 3, range entries: 0, sequences: 5 - 10
  seq 5 permit 133.133.0.0/24 (hit count: 0, refcount: 0)
  seq 8 deny any (hit count: 0, refcount: 0)
  seq 10 permit any (hit count: 0, refcount: 0)
OSPF: ip prefix-list test:
  count: 3, range entries: 0, sequences: 5 - 10
  seq 5 permit 133.133.0.0/24 (hit count: 0, refcount: 0)
  seq 8 deny any (hit count: 0, refcount: 0)
  seq 10 permit any (hit count: 0, refcount: 0)
...

```

查看所有地址前缀列表:

```

FRR#show ip prefix-list detail
Prefix-list with the last deletion/insertion: test
ZEBRA: ip prefix-list prelist-in:
  Description: ospf_filterlist_in
  count: 1, range entries: 0, sequences: 5 - 5
  seq 5 permit 192.200.2.0/24 (hit count: 0, refcount: 0)
ZEBRA: ip prefix-list test:
  count: 3, range entries: 0, sequences: 5 - 10
  seq 5 permit 133.133.0.0/24 (hit count: 0, refcount: 0)
  seq 8 deny any (hit count: 0, refcount: 0)
  seq 10 permit any (hit count: 0, refcount: 0)
Prefix-list with the last deletion/insertion: test
OSPF: ip prefix-list prelist-in:
  Description: ospf_filterlist_in
  count: 1, range entries: 0, sequences: 5 - 5
  seq 5 permit 192.200.2.0/24 (hit count: 0, refcount: 0)
OSPF: ip prefix-list test:
  count: 3, range entries: 0, sequences: 5 - 10
  seq 5 permit 133.133.0.0/24 (hit count: 0, refcount: 0)
  seq 8 deny any (hit count: 0, refcount: 0)
  seq 10 permit any (hit count: 0, refcount: 0)
...

```

## ■ 查看路由图

假设路由图配置如下:

```

route-map newrm permit 1
  set metric 555
!
route-map rmnew permit 1
  call newrm
  match ip address test

```



```
set metric 333
set metric-type type-1
!
route-map rmnew permit 2
match ip address prefix-list test
set tag 1000
!
route-map rmtest deny 1
match ip address 101
match ip address prefix-list test
```

➤ 按照 route-map 名称进行查看:

```
FRR#show route-map rmnew
ZEBRA:
route-map rmnew, permit, sequence 1
  Match clauses:
    ip address test
  Set clauses:
  Call clause:
    Call newrm
  Action:
    Exit routemap
route-map rmnew, permit, sequence 2
  Match clauses:
    ip address prefix-list test
  Set clauses:
  Call clause:
  Action:
    Exit routemap
OSPF:
route-map rmnew, permit, sequence 1
  Match clauses:
    ip address test
  Set clauses:
    metric-type type-1
    metric 333
  Call clause:
    Call newrm
  Action:
    Exit routemap
route-map rmnew, permit, sequence 2
  Match clauses:
    ip address prefix-list test
```

```
Set clauses:
tag 1000
Call clause:
Action:
Exit routemap
...
➤ 查看所有 route-map
FRR#show route-map
ZEBRA:
route-map newrm, permit, sequence 1
Match clauses:
Set clauses:
Call clause:
Action:
Exit routemap
ZEBRA:
route-map rmnew, permit, sequence 1
Match clauses:
ip address test
Set clauses:
Call clause:
Call newrm
Action:
Exit routemap
route-map rmnew, permit, sequence 2
Match clauses:
ip address prefix-list test
Set clauses:
Call clause:
Action:
Exit routemap
ZEBRA:
route-map rmtest, deny, sequence 1
Match clauses:
ip address 101
ip address prefix-list test
Set clauses:
Call clause:
Action:
Exit routemap
OSPF:
route-map newrm, permit, sequence 1
```

```

Match clauses:
Set clauses:
    metric 555
Call clause:
Action:
    Exit routemap
OSPF:
route-map rmnew, permit, sequence 1
Match clauses:
    ip address test
Set clauses:
    metric-type type-1
    metric 333
Call clause:
    Call newrm
Action:
    Exit routemap
route-map rmnew, permit, sequence 2
Match clauses:
    ip address prefix-list test
Set clauses:
    tag 1000
Call clause:
Action:
    Exit routemap
OSPF:
route-map rmtest, deny, sequence 1
Match clauses:
    ip address 101
    ip address prefix-list test
Set clauses:
Call clause:
Action:
    Exit routemap
...

```

### 2.5.2. 路由管理

#### ■ 查看路由过滤配置

```

FRR#show ip protocol
Protocol      : route-map
-----
system       : none

```

```
kernel      : none
connected   : none
static      : none
rip         : none
ripng       : none
ospf        : rmtest          <== 针对 ospf 的路由表项应用路由图 rmtest
ospf6       : none
isis        : none
bgp         : none
pim         : none
eigrp       : none
nhrrp       : none
hsrls       : none
olsr        : none
table       : none
ldp         : none
vnc         : none
vnc-direct  : none
vnc-rn      : none
bgp-direct  : none
bgp-direct-to-nve-groups : none
babel       : none
sharp       : none
pbr         : none
wildcard    : none
any         : none
```

■ 查看路由表

➤ 查看整体路由表项

> selected route 表示优选的路由，作为路由转发表的候选表项。

\* FIB route 表示路由转发表中的表项。

比如递归路由，就属于 selected route，但是不属于 FIB route，实际的下一跳属于 FIB route，但是不属于 selected route。见下例最后两条表项。

每条表项的最后一个字段表示该路由已经存活的时间。

```
#show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR,
       > - selected route, * - FIB route

S>* 1.1.1.0/24 [1/0] via 192.168.3.11, Vlan1, 3d06h41m
```

```

S>* 33.33.33.0/24 [1/0] unreachable (blackhole), 3d00h52m
O>* 133.133.0.0/24 [110/20] via 192.10.10.100, Vlan100, 3d05h17m
O 192.10.10.0/24 [110/100] is directly connected, Vlan100, 3d05h18m
C>* 192.10.10.0/24 is directly connected, Vlan100, 3d06h41m
O 192.100.3.0/24 [110/100] is directly connected, Vlan3, 3d06h41m
C>* 192.100.3.0/24 is directly connected, Vlan3, 3d06h41m
O 192.100.4.0/24 [110/100] is directly connected, Vlan4, 3d06h41m
C>* 192.100.4.0/24 is directly connected, Vlan4, 3d06h41m
O 192.100.5.0/24 [110/100] is directly connected, Vlan5, 3d06h41m
C>* 192.100.5.0/24 is directly connected, Vlan5, 3d06h41m
O 192.100.6.0/24 [110/100] is directly connected, Vlan6, 3d06h41m
C>* 192.100.6.0/24 is directly connected, Vlan6, 3d06h41m
S 192.100.6.0/24 [1/0] unreachable (ICMP unreachable), 3d06h41m
S>* 192.155.0.0/16 [1/0] via 192.168.3.3, Vlan1, 00:00:30
O 192.168.2.0/24 [110/100] is directly connected, Vlan2, 3d06h41m
C>* 192.168.2.0/24 is directly connected, Vlan2, 3d06h41m
O 192.168.3.0/24 [110/100] is directly connected, Vlan1, 3d06h41m
S 192.168.3.0/24 [1/0] unreachable (blackhole), 3d06h41m
C>* 192.168.3.0/24 is directly connected, Vlan1, 3d06h41m
S>* 192.200.1.0/24 [1/0] via 192.100.3.10, Vlan3, 3d06h41m
S>* 192.200.2.0/24 [1/0] via 192.100.3.10, Vlan3, 3d06h41m
S>* 192.200.3.0/24 [1/0] via 192.100.3.20, Vlan3, 3d06h41m
S>* 192.200.4.0/24 [1/0] via 192.100.3.20, Vlan3, 3d06h41m
S>* 192.210.1.0/24 [1/0] via 192.168.3.1, Vlan1, 3d06h41m
S>* 192.210.2.0/24 [1/0] via 192.168.3.1, Vlan1, 3d06h41m
S>* 192.210.3.0/24 [1/0] via 192.168.3.1, Vlan1, 3d06h41m
S>* 192.210.4.0/24 [1/0] via 192.168.3.1, Vlan1, 3d06h41m
S> 192.230.3.0/24 [1/0] via 133.133.0.5 (recursive), 3d06h41m
* via 192.10.10.100, Vlan100, 3d06h41m

```

➤ 按照协议查看路由表项（比如 OSPF）

```
FRR#show ip route ospf
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
```

```
O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
```

```
T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
```

```
F - PBR,
```

```
> - selected route, * - FIB route
```

```

O>* 133.133.0.0/24 [110/20] via 192.10.10.100, Vlan100, 3d05h19m
O 192.10.10.0/24 [110/100] is directly connected, Vlan100, 3d05h19m
O 192.100.3.0/24 [110/100] is directly connected, Vlan3, 3d06h43m
O 192.100.4.0/24 [110/100] is directly connected, Vlan4, 3d06h43m
O 192.100.5.0/24 [110/100] is directly connected, Vlan5, 3d06h43m

```

```
O 192.100.6.0/24 [110/100] is directly connected, Vlan6, 3d06h43m
O 192.168.2.0/24 [110/100] is directly connected, Vlan2, 3d06h43m
O 192.168.3.0/24 [110/100] is directly connected, Vlan1, 3d06h43m
```

```
FRR#show ip route connected
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
```

```
O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
```

```
T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
```

```
F - PBR,
```

```
> - selected route, * - FIB route
```

```
C>* 192.10.10.0/24 is directly connected, Vlan100, 3d06h48m
```

```
C>* 192.100.3.0/24 is directly connected, Vlan3, 3d06h48m
```

```
C>* 192.100.4.0/24 is directly connected, Vlan4, 3d06h48m
```

```
C>* 192.100.5.0/24 is directly connected, Vlan5, 3d06h48m
```

```
C>* 192.100.6.0/24 is directly connected, Vlan6, 3d06h48m
```

```
C>* 192.168.2.0/24 is directly connected, Vlan2, 3d06h48m
```

```
C>* 192.168.3.0/24 is directly connected, Vlan1, 3d06h48m
```

```
FRR#show ip route static
```

```
2000 Aug 04 23:35:23 OLT OSPF-6: vtysh -c "show ip route static"
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
```

```
O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
```

```
T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
```

```
F - PBR,
```

```
> - selected route, * - FIB route
```

```
S>* 1.1.1.0/24 [1/0] via 192.168.3.11, Vlan1, 3d06h48m
```

```
S>* 33.33.33.0/24 [1/0] unreachable (blackhole), 3d00h59m
```

```
S 192.100.6.0/24 [1/0] unreachable (ICMP unreachable), 3d06h48m
```

```
S>* 192.155.0.0/16 [1/0] via 192.168.3.3, Vlan1, 00:00:30
```

```
S 192.168.3.0/24 [1/0] unreachable (blackhole), 3d06h48m
```

```
S>* 192.200.1.0/24 [1/0] via 192.100.3.10, Vlan3, 3d06h48m
```

```
S>* 192.200.2.0/24 [1/0] via 192.100.3.10, Vlan3, 3d06h48m
```

```
S>* 192.200.3.0/24 [1/0] via 192.100.3.20, Vlan3, 3d06h48m
```

```
S>* 192.200.4.0/24 [1/0] via 192.100.3.20, Vlan3, 3d06h48m
```

```
S>* 192.210.1.0/24 [1/0] via 192.168.3.1, Vlan1, 3d06h48m
```

```
S>* 192.210.2.0/24 [1/0] via 192.168.3.1, Vlan1, 3d06h48m
```

```
S>* 192.210.3.0/24 [1/0] via 192.168.3.1, Vlan1, 3d06h48m
```

```
S>* 192.210.4.0/24 [1/0] via 192.168.3.1, Vlan1, 3d06h48m
```

```
S> 192.230.3.0/24 [1/0] via 133.133.0.5 (recursive), 3d06h48m
```

```
* via 192.10.10.100, Vlan100, 3d06h48m
```

➤ 仅查看超网路由

```
OLT#show ip route supernets-only
```

Codes: K - kernel route, C - connected, S - static, R - RIP,  
O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,  
T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,  
F - PBR,  
> - selected route, \* - FIB route

S>\* 192.155.0.0/16 [1/0] via 192.168.3.3, Vlan1, 00:00:07

➤ 查看路由表的 summary

```
FRR#show ip route summary
```

Route Source	Routes	FIB (vrf Default-IP-Routing-Table)
connected	7	7
static	14	12
ospf	8	1
-----		
Totals	29	20

➤ 查看某条具体的路由细节

```
FRR#show ip route 192.168.3.0/24 detail
```

Routing entry for 192.168.3.0/24

Known via "ospf", distance 110, metric 100

Last update 3d06h53m ago

directly connected, Vlan1

Routing entry for 192.168.3.0/24

Known via "static", distance 1, metric 0

Last update 3d06h54m ago

unreachable (blackhole)

Routing entry for 192.168.3.0/24

Known via "connected", distance 0, metric 0, best

Last update 3d06h54m ago

\* directly connected, Vlan1

➤ 查看给定路由前缀包含的相关路由表项

```
FRR# show ip route 192.168.0.0/16 longer-prefixes
```

Codes: K - kernel route, C - connected, S - static, R - RIP,  
O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,  
T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,  
F - PBR,  
> - selected route, \* - FIB route

O 192.168.2.0/24 [110/100] is directly connected, Vlan2, 3d06h56m

C>\* 192.168.2.0/24 is directly connected, Vlan2, 3d06h56m

```
O 192.168.3.0/24 [110/100] is directly connected, Vlan1, 3d06h55m
S 192.168.3.0/24 [1/0] unreachable (blackhole), 3d06h56m
C>* 192.168.3.0/24 is directly connected, Vlan1, 3d06h56m
```

也可以根据路由协议进行筛选:

```
FRR#show ip route 192.168.3.0/17 longer-prefixes ospf
Codes: K - kernel route, C - connected, S - static, R - RIP,
        O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
        T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
        F - PBR,
        > - selected route, * - FIB route
```

```
O 192.168.2.0/24 [110/100] is directly connected, Vlan2, 3d06h56m
O 192.168.3.0/24 [110/100] is directly connected, Vlan1, 3d06h55m
```



### 3. 配置 OSPFv2

#### 3.1. 概述

OSPF（Open Shortest Path First，开放式最短路径优先协议）是一种内部网关协议（Interior Gateway Protocol，简称 IGP），应用在 AS（Autonomous System，自治系统）内部，使路由设备获得远端网络的路由。

OSPF 具备如下特点：

- 适用范围广：适用于更大规模的网络（最大可支持几百台路由设备）。
- 快速收敛：一旦网络拓扑发生变化，路由设备之间能够快速通告信息，更新路由。
- 无自环：路由设备之间仅同步链路状态信息，每台路由设备独立计算路由，不会形成自环。
- 区域划分：将一个大的路由域划分为多个较小的区域，可以节省系统资源和网络带宽，使路由稳定可靠。
- 路由分类：将路由分为多种类型区别对待，支持灵活的控制策略。
- 支持认证：支持报文认证，保障协议交互过程的安全。
- 组播发送：支持以组播地址发送协议报文，可以避免干扰无关者、节省系统资源。

*注意：OSPF Version 2 应用于 IPv4，OSPF Version 3 应用于 IPv6，协议运行机制和大部分配置都相同。本章节中的 OSPF，若无特殊说明，均指 OSPFv2。*

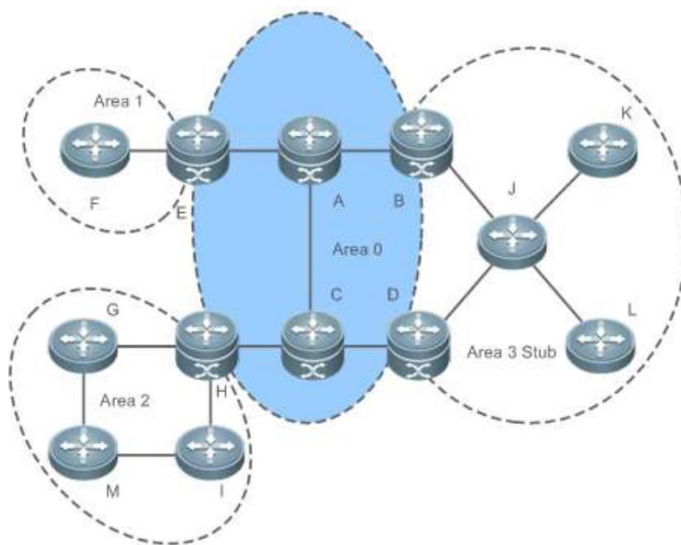
#### 3.2. 典型应用

典型应用	场景描述
域内互联	在 AS 内部运行 OSPF，划分多个区域。
域间互联	多个 AS 互联，在 AS 内部运行 OSPF，在 AS 之间运行 BGP。

##### 3.2.1. 域内互联

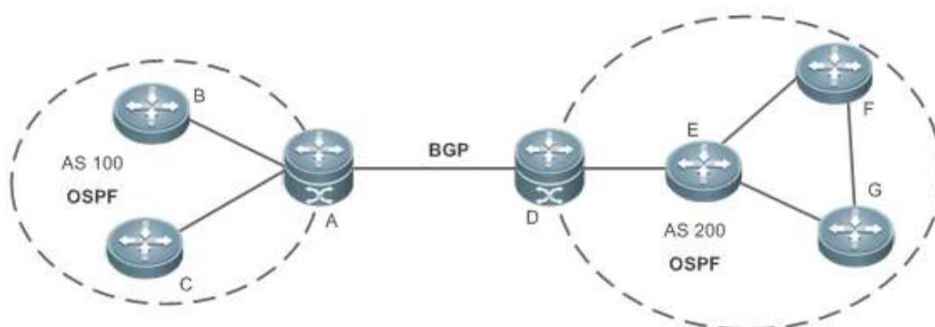
在 AS 内部运行 OSPF，如果路由设备超过 40 台，建议划分多个区域。通常，骨干区域应该采用性能可靠且处理速度较快的高端设备，非骨干区域可以采用性能相对较低的中低端设备。所有非骨干区域都必须与骨干区域相连。建议将位于末梢的非骨干区域设置为 Stub 区域。以下图为例。

- 将该网络划分成 4 个区域，不同区域间的通信都经过骨干区域（即区域 0）。
- Area 3 设置为 Stub 区域。
- 所有路由设备运行 OSPF 协议，实现单播路由。



### 3.2.2. 域间互联

多个 AS 互联，在 AS 内部运行 OSPF，在 AS 之间运行 BGP。通常，OSPF 和 BGP 应该相互学习路由信息。以下图为例，AS 100 和 AS 200 内部都是通过 OSPF 协议来实现单播路由，在两个 AS 之间通过 BGP 协议来实现单播路由。



- AS 100 和 AS 200 内部运行 OSPF 协议，实现单播路由。
- 两个 AS 之间运行 BGP 协议，实现单播路由。
- A 和 D 同时运行 OSPF 协议和 BGP 协议。

### 3.3. 功能详解

OSPF 是一种链接状态路由协议。与距离矢量协议（例如 RIP 或 BGP）不同，在路由设备中，描述了彼此之间的可用路径（即路由），而在链路状态协议中，路由设备则描述了其到其直接相邻路由设备的链路状态。

每个路由设备在称为 LSA 的消息中描述其链路状态信息，然后通过称为泛洪的过程传播到链路状态路由域中的所有其他路由设备。因此，每个路由设备都会为所有链路状态消息建立一个 LSDB（Link-State Database，链路状态数据库）。然后，通过使用 Dijkstra 的 SPF 算法等算法，从每个 LSDB 中的 LSA 集合中，每个路由设备都可以基于一些通用度量来计算到任何其他路由设备的最短路径。

通过以路由设备和链路而不是通过网络的路径来描述网络的连通性，链路状态协议可以比其他协议使用更少的带宽并更快地收敛。当任何单个给定路由设备上的链路更改状态时，链路状态协议仅需要在整个链路状态域中分配一个链路状态消息，以使所有路由设备在通过网络的最佳路径上重新收敛。相反，距离矢量协议可能需要来自一系列不同路由器的一系列不同路径更新消息以进行收敛。

链路状态协议的缺点是，与距离矢量协议相比，计算最佳路径的过程可能相对密集，在距离矢量协议中，除了多个路由之间进行选择以外，几乎不需要进行任何计算。对于现代嵌入式 CPU，即使对于具有数千个节点的网络，此开销几乎可以忽略不计。主要的扩展开销更多地在于随着链路状态区域大小的增加，应对 LSA 更新频率的不断提高，以及管理 LSDB 和所需的泛洪。

**当前系统仅支持一个 OSPF 实例**，该 OSPF 实例对应了一个 OSPF 进程（有且仅有一个进程）。

一个 AS 中的所有路由设备必须相互连接，运行相同的路由协议。因此，AS 也被称为路由域（Routing Domain）。运行 OSPF 的 AS 也被称为 OSPF 路由域，简称 OSPF 域。

### 3.3.1. OSPF 协议

#### ■ Area

OSPF 支持多区域（Area）。将一个 OSPF 域划分为多个区域，有利于缓解大规模网络的计算压力。区域是从逻辑上将路由器划分为不同的组，每个组用区域号（Area ID）来标识。区域的边界是区域边界路由器（Area Border Router，ABR）。一台路由器可以只属于一个区域，也可以属于多个区域（即 ABR）。一个网段（链路）只能属于一个区域，或者说每个运行 OSPF 的接口必须指明属于哪一个区域。

区域 0 为骨干区域（Backbone Area），其他区域为常规区域（Normal Area）。常规区域必须与骨干区域直接相连。每个区域必须通过 ABR 连接到骨干区域。这些 ABR 负责将区域的链路状态路由信息汇总为摘要 LSA（可能以压缩（即聚合）形式），然后将这些摘要引入 ABR 连接到的所有其他区域。

请注意，区域之间仅传递摘要和外部路由。由于区域之间交互的信息只描述路径，而不是任何路由器的链路状态，所以区域之间的路由，是距离向量，而不是链路状态。

#### ■ 路由器

在 OSPF 中定义了几种路由器类型，并为每种类型的路由器赋予不同的职责。

##### ➤ 区域内路由器（Internal Router）

该类路由器的所有接口都属于同一个 OSPF 区域。如下图中的 A、C、F、G、I、M、J、K、L。

##### ➤ 区域边界路由器（Area Border Router，简称 ABR）

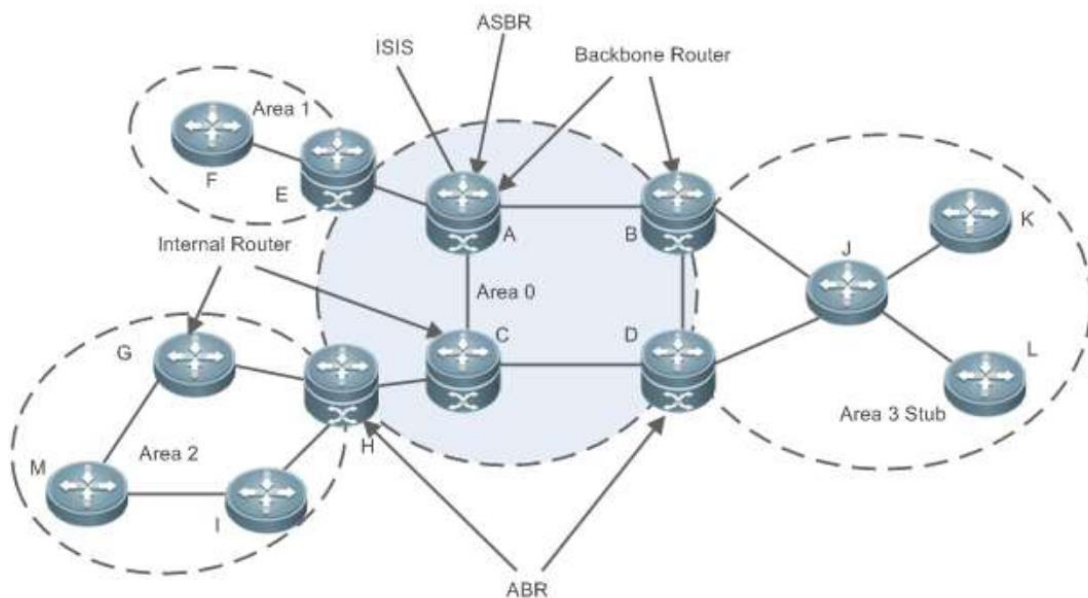
该类路由器用来连接骨干区域和常规区域。ABR 同时属于两个以上的区域，其中一个必须是骨干区域。如下图中的 B、D、E、H。

##### ➤ 骨干路由器（Backbone Router）

该类路由器至少有一个接口属于骨干区域。所有的 ABR 和 Area0 的区域内路由器都是骨干路由器。如下图中的 A、B、C、D、E、H。

➤ 自治系统边界路由器（AS Boundary Router，简称 ASBR）

该类路由器用来与其他 AS 交换路由信息。ASBR 并不一定位于 AS 的边界，它可能是区域内路由器，也可能是 ABR。如下图中的 A。

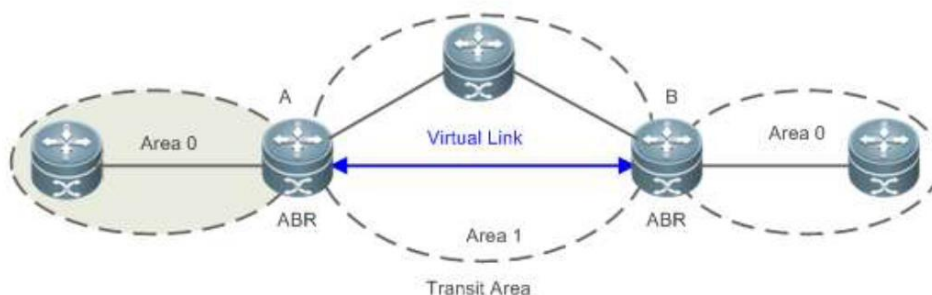


■ 虚链路

OSPF 支持虚链路（Virtual link）。虚链路是一条逻辑链路，**属于骨干区域**，用于解决在物理网络上骨干区域不连续或者骨干区域和常规区域不能直接相连的问题。虚链路只能穿越一个常规区域，该区域被称为“**传输区域**”（Transit Area）。虚链路两端的路由器均为 ABR。

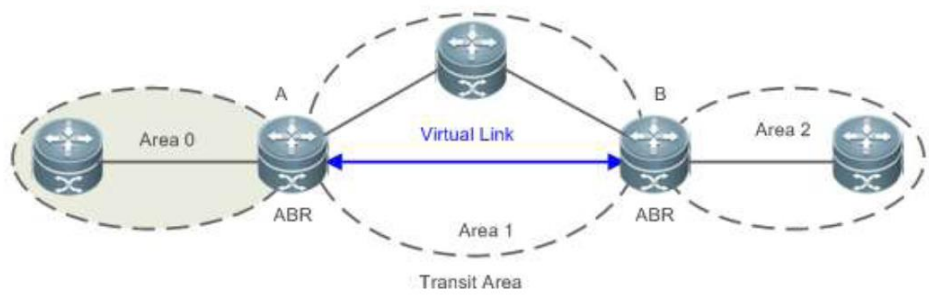
➤ 骨干区域不连续

在 A、B 之间建立虚链路，将 Area0 还接起来；Area1 是传输区域；A、B 是 Area1 的 ABR。



➤ 骨干区域与常规区域不能直接相连

在 A、B 之间建立虚链路，将 Area0 延伸至 B，则 Area0 与 Area2 在 B 上直接相连；Area1 是传输区域；A 是 Area1 的 ABR；B 是 Area1、Area2 的 ABR。



■ LSA

OSPF 以 LSA（Link State Advertisement，链路状态通告）的形式来描述路由信息。

LSA 类型	说明
Router-LSA（Type1）	由每个路由器始发，描述了路由器的链路状态和代价，在始发路由器所在区域内传播。
Network-LSA（Type2）	由 NBMA 类型网络上的 DR 始发，描述本网段的链路状态，在 DR 所在区域内传播。
Network-summary-LSA（Type3）	由 ABR 始发，描述到其它区域的路由，通告给非 Totally STUB、Totally NSSA 区域。
ASBR-summary-LSA（Type4）	由 ABR 始发，描述到 ASBR 的路由，通告给除 ASBR 所在区域外的其他区域。
AS-external-LSA（Type5）	由 ASBR 始发，描述到 AS 外部的路由，通告给非 STUB、NSSA 区域。
NSSA LSA（Type7）	由 ASBR 始发，描述到 AS 外部的路由，仅在 NSSA 区域内传播。

■ 特殊区域

定义这些特殊区域的目的在于减少协议的交互负担，减少路由表的规模。

- Stub 区域：位于骨干末梢的非骨干区域，Stub 区域的特点：
  - ✧ 不能部署 ASBR。
  - ✧ 该区域的 ABR 不发布外部路由（该 OSPF 域的路由还是发布），即发布 Type3 LSA，不发布 Type5 LSA。所有到达 OSPF 域外的报文通过一条指向 ABR 的缺省路由完成。
- Totally Stub 区域：与 Stub 区域的差异在于：

该区域的 ABR 不发布外部路由（Type5 LSA），也不发布 AS 域内其他区域的的路由（Type3 LSA）。所有到达本区域外的报文都通过一条指向 ABR 的缺省路由完成。
- NSSA 区域（Not So Stub Area）：该区域的特点为：

该区域需要部署 ASBR，同时需要保留 Stub 区域的特征。

ASBR 通过 Type7 LSA 将 AS 外部路由在 NSSA 区域内传播，NSSA 的 ABR 收到 Type7 的 LSA 后，转换成 Type 5 的 LSA，然后扩散到整个 AS。

与 Stub 区域一样。该区域的 ABR 不发布其他 Area 的 ASBR 产生的 Type 5 的 LSA。但会发布 Type 3 的 LSA。

显然，本区域的 ASBR 对应的外部路由，在本区域内会扩散学习，但是其他的 OSPF 域外路由，都是通过一条指向 ABR 的缺省路由代替。

- **Totally NSSA 区域：**与 NSSA 区域的差异在于：  
该区域的 ABR 也不发布 AS 域内其他区域的路由（Type3 LSA）。到达本 AS 域内的其他区域的报文都通过一条指向 ABR 的缺省路由完成。

不同区域对 LSA 的传播特点如下表：

区域	Type1, 2	Type3	Type4	Type5	Type7
普通区域	允许	允许	允许	允许	允许
Stub 区域	允许	允许，包括一条缺省路由	不允许	不允许	不允许
Totally Stub 区域	允许	只允许一条缺省路由	不允许	不允许	不允许
NSSA 区域	允许	允许，包括一条缺省路由	允许	不允许	允许
Totally NSSA 区域	允许	只允许一条缺省路由	允许	不允许	允许

#### ■ 网络类型

- **广播（Broadcast）：**自动发现邻居，选举 DR、BDR。DR（或 BDR）与其他所有路由器交换 LSA、建立邻接关系。DR、BDR 之外的路由器之间不交换 LSA、不建立邻接关系。  
Ethernet、FDDI 默认属于此类型。
- **非广播多点访问（Non-broadcast multiple access，简称 NBMA）：**手工配置邻居，选举 DR、BDR。DR（或 BDR）与其他所有路由器交换 LSA、建立邻接关系。DR、BDR 之外的路由器之间不交换 LSA、不建立邻接关系。  
X.25、帧中继、ATM 默认属于此类型。
- **点到点（point-to-point，简称 P2P）：**自动发现邻居，不选举 DR/BDR。链路两端路由器之间交换 LSA、建立邻接关系。  
PPP、HDLC、LAPB 默认属于此类型。
- **点到多点（Point-to-Multipoint，简称 P2MP）：**自动发现邻居，不选举 DR/BDR。任意两台路由器之间都要交换 LSA、建立邻接关系。  
没有任何链路层协议的网络默认为此类型。

#### ■ OSPF 报文

OSPF 使用以下几种类型的协议报文。这些 OSPF 报文被封装在 IP 报文中，以组播或单播方式发送。

报文类型	说明
Hello	周期性发送，用来发现 OSPF 邻居，维持邻接关系。
DD (Database Description)	描述本地LSDB (Link-State Database, 链路状态数据库) 的摘要信息，用于在OSPF邻居之间进行数据库同步。
LSR (Link State Request)	用于向对方请求所需的LSA。另有在OSPF 邻居双方成功交换 DD报文后，才会向对方发出LSR 报文。
LSU (Link State Update)	用于向对方发送其所需要的 LSA。
LSAck (Link State Acknowledgment)	用来对收到的 LSA 进行确认。

■ 协议工作过程

➤ 邻居发现

路由器从所有启动 OSPF 的接口上（或虚链路）发出 Hello 报文。如果两台路由器之间能够交互 Hello 报文，并且能够成功协商 Hello 报文中携带的参数，则它们就成为了邻居（Neighbor）。当互为邻居的路由器在彼此的 Hello 报文中到自己的 Router ID 时，双向通信就建立了。

➤ 完全邻接

邻居路由器之间建立双向通信后，使用 DD、LSR、LSU、LSAck 报文交换 LSA，建立邻接关系。简要过程如下：

- ✧ 路由器产生 LSA，用来描述该设备上的全部链路状态。
- ✧ 邻居之间交换 LSA。当路由器接收到邻居发送的 LSA 时，将拷贝一分到本地 LSDB，然后再传播给其它邻居。
- ✧ 当路由器及其邻居都获得了相同的 LSDB 时，达到完全邻接状态。

➤ 形成路由表

路由器上获得完整的 LSDB 后，将运行 Dijkstra 算法生成一棵从本地到每个目标网络的最短路径树（Shortest Path Tree，简称 SPT）。SPT 中记录了：目标网络、下一跳地址、代价。OSPF 依据 SPT 形成路由表。

如果发生链路代价、网络增删变化，则会引起 LSDB 的更新。设备将再次运行 Dijkstra 算法，生成新的 SPT，并更新路由表。

3.3.2. OSPF 路由管理

■ OSPF 的路由类型

OSPF 的路由简单可以分为，区域内的路由，区域间的路由，AS 域外部路由。

一般而言，区域内的路由不做标识，区域间的路由标识为“IA”。AS 域外部路由根据路由代价的计算方式不同分为两类：“E1”和“E2”。

第一类外部路由 E1：路由代价=本地到 ASBR 的代价+ASBR 到目标网络的代价。

第二类外部路由 E2：路由代价=ASBR 到目标网络的代价。

在 redistribute 的时候通过 metric-type 指定引入的外部路由为哪类。默认为 E1。

```
FRR# show ip ospf route
===== OSPF network routing table =====
N IA 192.168.1.0/24      [20000] area: 0.0.0.0
                        via 192.168.2.1, Vlan2
N   192.168.2.0/24      [10000] area: 0.0.0.0
                        directly attached to Vlan2
N   192.168.100.0/24    [10000] area: 0.0.0.2
                        directly attached to Vlan1

===== OSPF router routing table =====
R   192.168.2.1         [10000] area: 0.0.0.0. ABR, ASBR
                        via 192.168.2.1, Vlan2

===== OSPF external routing table =====
N E2 5.5.5.0/24         [20000/20] tag: 0
                        via 192.168.2.1, Vlan2
N E1 6.6.6.0/24         [20020] tag: 0
                        via 192.168.2.1, Vlan2
```

如上所示：router routing 表项不会生成路由表项，network routing table 中，未标识 IA 的即为区域内的路由。

针对不同的区域，其中路由器存在的路由情况如下表：（区域内的路由都存在，因此下表中只说明区域外的路由）

区域	区域内路由器的路由表中存在那些本区域外的路由
普通区域	IA； E1 或者 E2。
Stub 区域	IA。
NSSA 区域	IA； E1 或者 E2。（仅包含本区域 ASBR 发布的路由）
Totally Stub 区域	IA:仅缺省路由
Totally NSSA 区域	IA:仅缺省路由； E1 或者 E2。（仅包含本区域 ASBR 发布的路由）

■ 路由重分布

路由重分布是指：将设备上存在的“其他路由协议的路由、静态路由、直连路由”引入到 OSPF 域，以 LSA Type 5、7 的方式发送给邻居。路由重分布中若包含缺省路由，具体是否引入 OSPF 域要看其他配置，具体参看下节“缺省路由”说明。

路由重分布常用于 AS 间互联。通过在 ASBR 上配置路由重分布，可以将 AS 外部的路由信息传播到 AS 内部，也可以将 AS 内部的路由信息传播到 AS 外部。

■ 缺省路由

OSPF 缺省路由的生成分为多种情况，具体见下表：

区域类型	产生条件	发布位置	LSA 类型	泛洪范围	说明
普通区域	ASBR: 配置 default-information originate	ASBR	Type5	AS 域	表明 AS 域内无法找到目的 IP 报文全部通过 ASBR 路由。



	且 OSPF 进程中包含缺省路由。				
普通区域	ASBR: 配置 default-information originate always	ASBR	Type5	AS 域	表明 AS 域内无法找到目的 IP 报文全部通过该 ASBR 路由。
Stub 区域	自动生成	ABR	Type3	Stub 区域	对本 Stub 区域, 所有 AS 域的外部路由, 都由指向该 ABR 的缺省路由替代。
NSSA 区域	自动生成	ABR	Type3	NSSA 区域	如果除本 NSSA 区域, AS 域内其他区域还存在 ASBR, 那么通过其他区域到达的外部路由, 都由指向该 ABR 的缺省路由替代。
Totally Stub 区域	自动生成	ABR	Type3	Stub 区域	对本 Stub 区域, 所有 AS 域的外部路由, 以及其他区域的域内路由, 都由指向该 ABR 的缺省路由进行替代。
Totally NSSA 区域	自动生成	ABR	Type3	Totally NSSA 区域	除本 NSSA 区域的区域内路由, 本区域的 ASBR 发布的外部路由以外, 其他的所有路由, 都有指向该 ABR 的缺省路由进行替代。

*注意: NSSA 区域和 Totally NSSA 区域也有 ASBR, 但不建议在该 ASBR 配置生成缺省路由的配置, 因为本区域内 ABR 也会生成缺省路由, 最终不管如何路由优选, 最终总会有路由错误的情况发生。如果外部路由存在缺省路由, 希望重分布到该 AS 域, 那么进行重分布的 ASBR 所在区域, 最好不要配置为 NSSA 区域或者 Totally NSSA 区域。*

## ■ 路由汇聚

路由汇聚是指将具有相同前缀的路由信息汇聚为一条路由, 并将汇聚后的路由 (替代大量琐碎路由) 发布给邻居。路由汇聚有助于减轻协议交互负担、减小路由表的规模。

缺省情况下, 对于区域间的路由信息, ABR 以网段为单位发布 LSA Type 3; 如果其中存在一些连续的网段, 则建议配置路由汇聚。配置路由汇聚时, 汇聚范围有可能超出实际路由的网络范围。如果数据发往汇聚范围内不存在的网络, 将有可能发生路由环路或加重路由器的处理负担。为阻止这种情况的发生, ABR 会自动添加一条 discard 路由到路由表。该路由不会被传播。使用 area xx range 命令, 在 ABR 上汇聚区域间发布的路由 (LSA Type 3)。

## ■ 路由过滤

OSPF 允许在学习、交互、使用路由信息的过程中进行过滤, 以达到安全可控的目的。

通过配置命令, 可以在以下几处进行路由过滤:

- 针对接口: 使用 passive-interface 命令, 设置被动接口。被动接口上不能交互路由信息 (任意 LSA)。
- 针对区域间发布的路由信息:
  - ✧ 使用 filter-list prefix xxx in 或者 import-list 设置从其他区域发布到本区域的过滤条件, 只有满足过滤条件的路由信息才允许发布到本区域 (LSA Type 3)。
  - ✧ 使用 filter-list prefix xxx out 或者 export-list 设置本区域发布到其他区域的过滤条件, 只有满足过滤条件的路由信息才允许发布到其他区域 (LSA Type 3)。
- 针对 AS 域外部的路由信息: 使用 redistribute 命令 route-map 参数或者 distribute-list 命令。只有满足过滤条件的路由信息才能被重分布到 OSPF 进程

(LSA Type 5、7)。另外 redistribute 命令 route-map 参数还可以对重分布到 OSPF 进程的路由进行参数修改。

- 针对缺省路由信息：使用 default-information originate 命令 route-map 参数，可以根据路由图进行过滤或者参数修改。

## ■ 路由代价

如果网络中存在冗余链路或设备，则从本到达目的网络之间可能存在多条路径。OSPF 选择其中总代价最小的路径形成 OSPF 路由。一条路径的总代价等于沿途链路上的代价之和。通过修改沿途链路上的代价，使一条路径的总代价最小，即可使 OSPF 选择此路径形成路由。

- 从接口到直连网段的代价（即接口上的 cost 值）  
缺省值为自动代价。自动代价 = 参考带宽/接口带宽。  
使用 auto-cost reference-bandwidth 命令，可以设置自动代价的参考带宽，缺省值为 100000 (Mbps)。  
使用接口模式下的 bandwidth 命令，可以设置接口对应的带宽，缺省该配置值为 0（当带宽配置值为 0 时，根据接口的速率确定带宽，三层接口速率恒定为 1000）。  
使用接口模式下的 ip ospf cost 命令，可以人为设置接口上的 cost 值。此项配置优先级高于自动代价。
- 从接口到邻居的代价（即从本地到指定邻居的 cost 值）  
等于接口到对应直连网段的代价。
- 从 ABR 到区间汇聚网段的代价（区域间路由汇聚的 cost 值）  
如果兼容 RFC1583，缺省值为被汇总的链路代价的最小值，否则为被汇总的链路代价的最大值。  
使用 compatible rfc1583 命令，设置 OSPF 选路规则兼容 RFC1583。缺省兼容 RFC1583。  
使用 area xx range 命令的 cost 参数，修改区域间路由汇聚的 cost 值。
- 从 ABR 到缺省网段的代价（ABR 自动向 Stub、NSSA 区域发布的缺省路由的 cost 值）  
缺省值为 1。使用 area xx default-cost 命令，可以修改 ABR 自动向 Stub、NSSA 区域发布的缺省路由的 cost 值。
- 从 ASBR 到外部网段的代价（外部路由的 metric 值）  
缺省情况下，重分布 BGP 路由的 metric 为 1，重分布其它路由的 metric 为 20，路由类型为 E2。  
使用 default-metric 命令，可以修改外部路由的 metric 的缺省值。  
使用 redistribute 命令中的 metric、metric-type、route-map 参数，可以修改外部路由的 metric 值、路由类型。

- 从 ASBR 到缺省网段的代价（人为引入的缺省路由的 metric 值）  
缺省情况下，metric 为 1，路由类型为 E2。  
使用 default-information originate 命令的 metric、metric-type、route-map 参数，可以修改人为引入的缺省路由的 metric 值，路由类型。
- 最大代价  
使用 max-metric router-lsa 命令，可以将路由器上发布的所有链路代价均设为最大值。则途经此路由器的任何路径，总代价都会变得很大，几乎不可能成为最短路径。  
*注意：cost 和 metric 都表示路由代价，两者等价。*

■ 管理距离

OSPF 路由的管理距离默认为 110。  
使用 distance 命令，可以设置 OSPF 路由的管理距离值。

■ 认证

认证是为了阻止非法接入网络的路由器和伪造 OSPF 报文的主机参与 OSPF 协议过程。在 OSPF 接口（或虚链路两端）对收到的 OSPF 报文进行认证。如果认证失败，则丢弃报文，邻接关系将不能被建立。  
启动认证功能后，可以避免学到非认证、无效路由，避免通告有效路由到非认证设备。在广播类型网络中，认证还可以避免非认证设备成为指定设备（DR）的可能性，保证了路由系统的稳定性和抗入侵性。

3.4. 配置命令

3.4.1. OSPF 基本功能

■ 进入 OSPF 路由模式

命令	<p><b>进入 OSPF 路由模式（当 OSPF 进程未激活，该命令同时激活 OSPF 进程）</b></p> <pre>FRR(config)#router ospf FRR(config-router)#</pre> <p><b>使 OSPF 进程处于未激活状态</b></p> <pre>FRR(config)#no router ospf</pre>
描述	<p>全局模式下进行配置。</p> <p>OSPF 相关的大部分配置均需要在 OSPF 路由模式下进行。</p> <p>不支持 OSPF 多实例。</p>

■ 配置 OSPF 的 Router ID

命令	<p><b>配置 OSPF 的 Router ID</b></p> <pre>FRR(config-router)#ospf router-id A.B.C.D</pre> <p><b>取消 OSPF 的 Router ID 配置</b></p>
----	---

	<code>FRR(config-router)#no ospf router-id [A.B.C.D]</code>
描述	<p>OSPF 路由模式下进行配置。</p> <p>该配置为可选配置，但建议设置 router-id，避免 router-id 在设备复位后变化。router-id 作为协议交互时的设备 ID。其选择按照如下优先级从高到低：</p> <ol style="list-style-type: none"> <li>1) OSPF 设置的 router-id；</li> <li>2) 全局设置的 router-id；</li> <li>3) 某个三层口的 ip 地址。</li> </ol> <p>当 OSPF 进程激活时，选择好 router-id，即使更高优先级的 router-id 设置，也不会进行切换，如下操作可以触发切换：</p> <ol style="list-style-type: none"> <li>1) no router ospf，再 router ospf，触发 OSPF 进程重新激活。</li> <li>2) 保存配置，重启设备。</li> </ol> <p>因此，当没有显式设置 router-id 的时候，不能保证每次启机 router-id 相同。</p>

■ 启动接口的 OSPF，并指定 area

➤ 基于网段配置

命令	<p><b>配置网段</b></p> <p><code>FRR(config-router)#network A.B.C.D/M area (area-id/A.B.C.D)</code></p> <p><b>取消网段配置</b></p> <p><code>FRR(config-router)#no network A.B.C.D/M area (area-id/A.B.C.D)</code></p>
描述	<p>OSPF 路由模式下进行配置。</p> <p>Area-id 有两种表达方式：</p> <ol style="list-style-type: none"> <li>1) 整数：取值范围为 0-4294967295，骨干 Area 为 0。</li> <li>2) 点分十进制：类似 IP 地址的表达方式，骨干 Area 为 0.0.0.0。</li> </ol> <p>两种表达方式完全等价的。</p> <p>使用该命令，可以通过一条命令将一个或多个接口关联到一个 OSPF 区域。要在一个接口上运行 OSPF，需要将该接口的 IP 地址包括在 network area 定义的 IP 地址范围内。通过该配置，将 IP 地址和掩码长度确定的网络范围所包含的所有接口开启 OSPF，接口开启 OSPF 后，会进行 OSPF 邻居发现，协商，后续的 OSPF 交互；同时，也指定了所属的 Area，只有 Area 相同，路由器才能建立邻居。</p>

➤ 基于接口配置

命令	<p><b>配置网段</b></p> <p><code>FRR(config-if)#ip ospf area (area-id/A.B.C.D) [E.F.G.H]</code></p> <p><b>取消网段配置</b></p> <p><code>FRR(config-if)#no ip ospf area (area-id/A.B.C.D) [E.F.G.H]</code></p>
描述	<p>接口模式下进行配置。</p> <p>与基于网段配置方式作用等价，两者只能选择其中之一，否则配置时会提示冲突。</p>

	<p>[E.F.G.H] 当一个接口存在多个 IP 地址时，也意味着对应多个网段，可以通过 IP 地址区分多个网段，可以基于网段来配置 area。当前系统不支持一个三层接口配置多个 IP 地址，所以，此参数意义不大。</p>
--	--

■ 常见错误

- network 命令配置的网段范围未包含接口 IP 地址。
- 相连接口使能的区域号不一致。
- 多台路由器上配置了相同的 Router ID，导致 Router ID 冲突。
- 多台路由器上配置了相同的接口 IP 地址，导致 OSPF 网络运行错误。

3.4.2. 虚链路

■ 创建虚链路，指定认证方式

命令	<pre>FRR(config-router)#area area-id virtual-link A.B.C.D (authentication (message-digest null ) ) 上述描述说明 4 种情况： A: FRR(config-router)#area area-id virtual-link A.B.C.D B: FRR(config-router)#area area-id virtual-link A.B.C.D authentication C: FRR(config-router)#area area-id virtual-link A.B.C.D authentication message-digest D: FRR(config-router)#area area-id virtual-link A.B.C.D authentication null  反向操作： FRR(config-if)#no area area-id virtual-link A.B.C.D (authentication (message-digest null ) ) 上述描述说明 4 种情况： E: FRR(config-router)#no area area-id virtual-link A.B.C.D F: FRR(config-router)#no area area-id virtual-link A.B.C.D authentication G: FRR(config-router)#no area area-id virtual-link A.B.C.D authentication message-digest H: FRR(config-router)#no area area-id virtual-link A.B.C.D authentication null</pre>
描述	<p>OSPF 路由模式下进行配置。</p> <p>在 OSPF 路由域中，所有的区域都必须与骨干区域相接，如果骨干区域断接，就需要配置虚链路将骨干区域接续起来，否则网络通讯将出现问题。虚链路需要在两个区域边界路由设备（ABR）之间创建，两个 ABR 共同所属的区域成为传输区域。Stub 区域和 NSSA 区域不能作为传输区域。虚链路也可以用于接续其它非骨干区域。</p> <p>虚链路属于 Area0，但是配置虚链路的并非 Area 0。</p> <p>area-id 可以用整数表示或者点分十进制表示。</p> <p>A.B.C.D 虚链路邻居的Router ID。如果不确定Router ID的值，请用show ip ospf neighbor 命令进行确认。</p>

	<p>A: 创建虚链路，未指定认证方式，此时，该虚链路的认证方式根据 area 0 的认证方式确定。具体参见“认证功能”配置。</p> <p>B: 创建虚链路，指定明文方式认证，需要指定明文认证的密钥。</p> <p>C: 创建虚链路，指定 MD5 加密方式认证，需要指定 MD5 加密认证的密钥。</p> <p>D: 创建虚链路，指定该虚链路无需认证。</p> <p>E: 删除虚链路。</p> <p>F/G/H: 删除虚链路的认证方式，即将虚链路设置为未指定认证方式，虚链路配置保留。</p>
--	--

■ 设置虚链路的认证密钥

命令	<p>FRR(config-router)# <b>area</b> <i>area-id</i> <b>virtual-link</b> <i>A.B.C.D</i> (<b>message-digest-key</b> &lt;1-255&gt; <b>md5</b> <i>KEY</i>   <b>authentication-key</b> <i>AUTH_KEY</i>)</p> <p>上述描述说明 2 种情况：</p> <p>A: FRR(config-router)# <b>area</b> <i>area-id</i> <b>virtual-link</b> <i>A.B.C.D</i> <b>message-digest-key</b> &lt;1-255&gt; <b>md5</b> <i>KEY</i></p> <p>B: FRR(config-router)# <b>area</b> <i>area-id</i> <b>virtual-link</b> <i>A.B.C.D</i> <b>authentication-key</b> <i>AUTH_KEY</i></p> <p>反向操作：</p> <p>FRR(config-if)# <b>no</b> <b>area</b> <i>area-id</i> <b>virtual-link</b> <i>A.B.C.D</i> (<b>message-digest-key</b> &lt;1-255&gt; <b>md5</b> <i>KEY</i>   <b>authentication-key</b> <i>AUTH_KEY</i>)</p> <p>上述描述说明 2 种情况：</p> <p>C: FRR(config-router)# <b>no</b> <b>area</b> <i>area-id</i> <b>virtual-link</b> <i>A.B.C.D</i> <b>message-digest-key</b> &lt;1-255&gt; <b>md5</b> <i>KEY</i></p> <p>D: FRR(config-router)# <b>no</b> <b>area</b> <i>area-id</i> <b>virtual-link</b> <i>A.B.C.D</i> <b>authentication-key</b> <i>AUTH_KEY</i></p>
描述	<p>OSPF 路由模式下进行配置。</p> <p><b>area</b> <i>area-id</i> <b>virtual-link</b> <i>A.B.C.D</i> 确定了某条虚链路。</p> <p>A: 配置 MD5 加密认证方式的密钥标识符和密钥。密钥标识符取值范围 1-255。</p> <p>B: 配置明文认证方式的密钥。</p> <p>如果配置认证密钥时，对应虚链路还未创建，会自动创建虚链路，认证方式为未指定（即根据 area 的认证方式来确定）。</p> <p>A 和 B 两种密钥可以同时配置，具体采用哪个，或者都不采用，依赖于虚链路的认证方式来确定。</p> <p>C: 删除 MD5 认证方式的密钥标识符和密钥。</p> <p>D: 删除明文认证方式的密钥。</p>

■ 设置虚链路的 timer

命令	<pre>FRR(config-router)#area area-id virtual-link A.B.C.D { hello-interval &lt;1-65535&gt;   retransmit-interval &lt;1-65535&gt;   transmit-delay &lt;1-65535&gt;   dead-interval &lt;1-65535&gt; }</pre> <p>反向操作:</p> <pre>FRR(config-if)# no area area-id virtual-link A.B.C.D { hello-interval &lt;1-65535&gt;   retransmit-interval &lt;1-65535&gt;   transmit-delay &lt;1-65535&gt;   dead-interval &lt;1-65535&gt; }</pre> <p>四种 timer 可以同时配置 1-4 个, 顺序无关。</p>
描述	<p>OSPF 路由模式下进行配置。</p> <p>area area-id virtual-link A.B.C.D 确定了某条虚链路。</p> <p>hello-interval: OSPF 往虚链路发送 Hello 报文的时间间隔, 以秒为单位, 取值范围: 1-65535, 默认为 10 秒, 该参数必须与邻居保持一致。</p> <p>retransmit-interval: OSPF 链路状态描述 (LSA) 重传时间, 以秒为单位, 取值范围: 1-65535, 默认为 5 秒。</p> <p>transmit-delay: OSPF 链路状态描述 (LSA) 的时延, 以秒为单位, 取值范围: 1-65535, 默认为 1 秒。</p> <p>dead-interval: 定义宣告邻居丢失时间, 以秒为单位, 取值范围: 1-65535, 默认为 40 秒, 该参数必须与邻居保持一致。</p>

#### ■ 常见错误

- 指定虚链路的邻居的 Router ID 错误。
- 与邻居不是属于同个 Area。
- 与邻居端设置的认证方式和密钥不匹配。
- hello-interval 和 dead-interval 与邻居设置不一致。

### 3.4.3. 网络类型

#### ■ 配置接口网络类型

命令	<p><b>配置网络类型</b></p> <pre>FRR(config-if)#ip ospf network (broadcast   non-broadcast   point-to-multipoint [ non-broadcast ]   point-to-point)</pre> <p><b>取消网络类型配置</b></p> <pre>FRR(config-if)#ip ospf network (broadcast   non-broadcast   point-to-multipoint [ non-broadcast ]   point-to-point   )</pre>
描述	<p>接口模式下进行配置。</p> <p>broadcast: 广播类型, 默认类型。</p> <p>non-broadcast: NBMA 类型</p> <p>point-to-multipoint: P2MP 类型</p>

	point-to-point: P2P 类型 以太网对应广播类型，所以一般情况下不需要该配置。
--	--

#### ■ 配置邻居

命令	<p>手工配置邻居</p> <pre>FRR(config-router)#neighbor A.B.C.D [ poll-interval seconds ] [ priority priority ]</pre> <p>取消配置</p> <pre>FRR(config-router)#no neighbor A.B.C.D [ poll-interval seconds ] [ priority priority ]</pre>
描述	<p>OSPF 路由模式下进行配置。</p> <p>只有当对应接口类型为 NBMA 类型时，才需要手工配置邻居，其他类型均是自动发现邻居。</p> <p><b>poll-interval seconds:</b> 邻居轮询时间间隔，以秒为单位，取值范围：1-65535。缺省值为 60。</p> <p><b>priority priority:</b> 邻居的优先权值，取值范围：0-255。缺省值为 0。</p> <p>以太网对应广播类型，所以一般情况下不需要该配置。</p>

#### ■ 配置接口优先级

命令	<p>配置接口优先级</p> <pre>FRR(config-if)#ip ospf priority priority [A.B.C.D]</pre> <p>取消配置</p> <pre>FRR(config-if)#no ip ospf priority [priority] [A.B.C.D]</pre>
描述	<p>接口模式下进行配置。</p> <p><b>priority priority:</b> 接口的优先权值，取值范围：0-255。缺省值为 1。</p> <p>接口的优先权值包含在 OSPF hello 报文中。当 OSPF 广播类型网络发生 DR/BDR（指定路由设备 / 备份指定路由设备）竞选时，高优先权值的路由设备，将成为 DR 或 BDR。如果优先权值一样，路由设备标识符（Router ID）高的路由设备将成为 DR 或 BDR。优先权值为 0 的路由设备，不参与 DR/BDR 竞选。</p> <p>该命令对 OSPF 广播类型和 NBMA 类型有效。</p> <p><i>[A.B.C.D]</i> 当一个接口存在多个 IP 地址时，也意味着对应多个网段，可以通过 IP 地址区分多个网段，可以基于网段来配置 hello 时间。当前系统不支持一个三层接口配置多个 IP 地址，所以，此参数意义不大。</p>

### 3.4.4. 路由重分布及缺省路由

#### ■ 路由重分布

命令	配置路由重分布
----	---------



	<pre>FRR(config-router)#redistribute (static connect kernel rip isis bgp) [metric <i>metric</i>] [metric-type &lt;1-2&gt;] [route-map <i>RM_NAME</i>]</pre> <p><b>取消配置</b></p> <pre>FRR(config-router)#no redistribute (static connect kernel rip isis bgp) [metric <i>metric</i>] [metric-type &lt;1-2&gt;] [route-map <i>RM_NAME</i>]</pre>
描述	<p>OSPF 路由模式下进行配置。</p> <p>通过该命令，将其他源头的路由导入 OSPF 协议，并与 LSA Type5 广播到域内其他 OSPF 路由设备。</p> <p>配置完该命令，设备将会变为 ASBR。</p> <p><b>static:</b> 静态路由</p> <p><b>connect:</b> 直连路由，开启 OSPF 的网段，会自动作为 connect 路由导入 OSPF 协议。</p> <p><b>kernel:</b> 内核路由，如果主 CLI 有配置 CLI，在 FRR CLI 中会作为 kernel 路由。不建议两边同时配置路由。</p> <p><b>rip:</b> RIP 协议的路由</p> <p><b>isis:</b> IS-IS 协议的路由</p> <p><b>bgp:</b> BGP 协议的路由</p> <p><b>metric <i>metric</i>:</b> 可选参数，设置 OSPF external LSA 的 metric，取值范围为 0-16777214。若未指定该参数，BGP 重分布的路由 metric 为 1，其他外部路由 metric 为 20。</p> <p><b>metric-type &lt;1-2&gt;:</b> 可选参数，设置外部路由的类型为 E1 或者 E2，若未指定该参数，外部路由的类型为 E2。</p> <p><b>route-map <i>RM_NAME</i>:</b> 可选参数，关联路由图，对重分布的路由实施过滤或者参数修改。可以修改 metric，metric-type 以及路由的 tag。</p>

#### ■ 导入缺省路由

命令	<p><b>导入缺省路由</b></p> <pre>FRR(config-router)#default-information originate ({ always   metric <i>metric</i>   metric-type &lt;1-2&gt;   route-map <i>RM_NAME</i> } )</pre> <p><b>取消配置</b></p> <pre>FRR(config-router)#no default-information originate ({ always   metric <i>metric</i>   metric-type &lt;1-2&gt;   route-map <i>RM_NAME</i> } )</pre>
描述	<p>OSPF 路由模式下进行配置。</p> <p>执行该命令，设备将会变为 ASBR。ASBR 不会自动产生缺省路由，ASBR 若要产生缺省路由，必须用 default-information originate 配置命令进行配置。</p> <p>如果选择 always 参数，OSPF 路由进程不管是否存在缺省路由，都会向邻居通告一条外部缺省路由。但是本地路由设备不会显示该缺省路由，要确认是否产生缺省路由，可以用 show ip ospf database 观察 OSPF 链路状态数据库，链路标识为 0.0.0.0 的</p>

	<p>外部链路描述了缺省路由。OSPF 的邻居通过执行 <code>show ip route</code> 命令，可以看到是否存在缺省路由。</p> <p><b>metric <i>metric</i>:</b> 可选参数，用于指定外部缺省路由的 <code>metric</code>，取值范围为 0-16777214。若未指定该参数，外部缺省路由的 <code>metric</code> 为 1。</p> <p><b>metric-type (<i>1-2</i>):</b> 可选参数，设置外部缺省路由的类型为 E1 或者 E2，若未指定该参数，外部路由的类型为 E2。</p> <p><b>route-map <i>RM_NAME</i>:</b> 可选参数，关联路由图，对外部缺省路由实施过滤或者参数修改。可以修改 <code>metric</code>，<code>metric-type</code> 以及路由的 <code>tag</code>。</p>
--	---

■ 常见错误

- 多台设备配置了 `default-information originate always`，造成路由环路。
- 在 Stub 区域配置路由重分布，无法引入路由。

3.4.5. Stub, NSSA 区域

■ 配置 Stub 区域

命令	<p><b>配置 Stub 区域</b></p> <pre>FRR(config-router)#area <i>area-id</i> stub [<i>no-summary</i>]</pre> <p><b>取消配置</b><pre>FRR(config-if)#no area <i>area-id</i> stub [<i>no-summary</i>]</pre></p>
描述	<p>OSPF 路由模式下进行配置。</p> <p><code>area-id</code> 可以用整数表示或者点分十进制表示。</p> <p><b>no-summary:</b> 可选参数，携带此参数表示阻止 ABR 往 Stub 区域发送网络摘要链路通告 (LSA Type3)，此时该区域为 Totally Stub 区域。需要注意的是，只有 ABR 才需要配置该参数。</p> <p>OSPF Stub 区域内所有的路由设备都必须执行 <code>area stub</code> 命令。ABR 只向 Stub 区域发送三种链路状态描述 (LSA)：1) Type1，路由设备 LSA；2) Type2，网络 LSA；3) Type3，网络摘要 LSA。从路由表角度看，Stub 区域中的路由设备只能学习到 OSPF 路由域内部的路由，包括由 ABR 产生的内部缺省路由。Stub 区域的路由设备不能学习到 OSPF 路由域外部的路由。</p> <p>如果需要配置 Totally Stub 区域，只需在 ABR 上执行 <code>area stub</code> 命令时，选择 <code>no-summary</code> 关键字。Totally Stub 区域的路由设备只能学习本区域内的路由，以及 ABR 产生的内部缺省路由。</p> <p>在 Stub 区域的 ABR 上配置 <code>area default-cost</code>，可以用于定义内部缺省路由的初始花费（即路由代价）。</p>

■ 配置 NSSA 区域

命令	<p><b>配置 NSSA 区域</b></p> <pre>FRR(config-router)#area <i>area-id</i> nssa [<i>no-summary</i>]</pre> <p><b>取消配置</b></p>
----	--

	<code>FRR(config-if)#no area area-id nssa [no-summary]</code>
描述	<p>OSPF 路由模式下进行配置。</p> <p>area-id 可以用整数表示或者点分十进制表示。</p> <p>no-summary: 可选参数, 携带此参数表示阻止 ABR 往 NSSA 区域发送网络摘要链路通告 (LSA Type3), 此时该区域为 Totally NSSA 区域。需要注意的是, 只有 ABR 才需要配置该参数。</p> <p>OSPF NSSA 区域内所有的路由设备都必须执行 area nssa 命令。ABR 只向 NSSA 区域发送三种链路状态描述 (LSA): 1) Type1, 路由设备 LSA; 2) Type2, 网络 LSA; 3) Type3, 网络摘要 LSA。从路由表角度看, NSSA 区域中的路由设备只能学习到 OSPF 路由域内部的路由 (包括由 ABR 产生的内部缺省路由) 以及本 NSSA 区域内 ASBR 引入的路由。NSSA 区域的路由设备不能学习到其他区域 ASBR 引入的外部路由。</p> <p>如果需要配置 Totally NSSA 区域, 只需在 ABR 上执行 area nssa 命令时, 选择 no-summary 关键字。Totally NSSA 区域相对 NSSA 区域, 区域内的路由设备不能学习到其他区域的路由。</p> <p>在 NSSA 区域的 ABR 上配置 area default-cost, 可以用于定义内部缺省路由的初始花费 (即路由代价)。</p> <p>注意: <code>no area area-id nssa</code> 不仅可以删除 NSSA 区域配置, 也可以删除 NSSA 区域的转换参数配置。</p>

#### ■ 配置 NSSA 区域的转换参数

命令	<p><b>配置 NSSA 区域的转换参数</b></p> <p><code>FRR(config-router)#area area-id nssa (translate-always  translate-candidate  translate-never)</code></p> <p><b>取消配置</b></p> <p><code>FRR(config-if)#no area area-id nssa (translate-always  translate-candidate  translate-never )</code></p>
描述	<p>OSPF 路由模式下进行配置。</p> <p>该配置只需要在 NSSA 区域的 ABR 上配置。</p> <p>area-id 可以用整数表示或者点分十进制表示。</p> <p>如果一个 NSSA 区域有两个 (或者两个以上) ABR, 需要选择一个 ABR 作为 LSA Type7 到 LSA Type5 的转换者。</p> <p>translate-candidate: 缺省值即为 candidate, 选择路由设备标识最大的 ABR 作为转换者。</p> <p>translate-always: 总是希望当前设备作为转换者, 建议一个 NSSA 区域, 只在一台 ABR 上配置 translate-always, 如果存在多台, 依然需要在多台之间进行竞选。</p> <p>translate-never: 当前设备退出转换者的竞选。不能将整个 NSSA 区域的所有 ABR 都配置为 never。</p> <p>注意: <code>no area area-id nssa</code> 不仅可以删除 NSSA 区域配置, 也可以删除 NSSA 区域的转换参数配置。</p>

#### ■ 常见错误

- 对骨干区域, 传输区域设置 Stub, 或者 NSSA。

- 在 Stub 区域中配置路由重分布，将无法加入外部路由。
- 同一区域中的设备，区域类型配置不一致

3.4.6. 路由汇聚及路由过滤

■ 配置区域间路由汇聚

命令	<p><b>配置路由汇聚</b></p> <p>A: FRR(config-router)# <b>area</b> <i>area-id</i> <b>range</b> <i>A.B.C.D/M</i></p> <p>B: FRR(config-router)# <b>area</b> <i>area-id</i> <b>range</b> <i>A.B.C.D/M</i> <b>advertise</b></p> <p>C: FRR(config-router)# <b>area</b> <i>area-id</i> <b>range</b> <i>A.B.C.D/M</i> <b>not-advertise</b></p> <p>D: FRR(config-router)# <b>area</b> <i>area-id</i> <b>range</b> <i>A.B.C.D/M</i> <b>not-advertise cost</b> (0-16777215)</p> <p>E: FRR(config-router)# <b>area</b> <i>area-id</i> <b>range</b> <i>A.B.C.D/M</i> <b>substitute</b> <i>A.B.C.D/M</i></p> <p><b>取消配置</b></p> <p>F: FRR(config-router)# <b>no</b> <b>area</b> <i>area-id</i> <b>range</b> <i>A.B.C.D/M</i></p> <p>G: FRR(config-router)# <b>no</b> <b>area</b> <i>area-id</i> <b>range</b> <i>A.B.C.D/M</i> <b>advertise</b></p> <p>H: FRR(config-router)# <b>no</b> <b>area</b> <i>area-id</i> <b>range</b> <i>A.B.C.D/M</i> <b>not-advertise</b></p> <p>I: FRR(config-router)# <b>no</b> <b>area</b> <i>area-id</i> <b>range</b> <i>A.B.C.D/M</i> <b>not-advertise cost</b> (0-16777215)</p> <p>J: FRR(config-router)# <b>no</b> <b>area</b> <i>area-id</i> <b>range</b> <i>A.B.C.D/M</i> <b>substitute</b> <i>A.B.C.D/M</i></p>
描述	<p>OSPF 路由模式下进行配置。</p> <p>该命令只能在 ABR 上执行有效，用来将一个区域的多个路由汇聚成一条路由，然后通告到其它区域去。路由信息的汇聚行为只发生在区域边界，区域内部路由设备上看到的都是具体的路由信息，但其它区域的设备只能看到一条汇聚路由。并且可以通过设置 advertise 和 not-advertise 选项来决定是否公布整个汇聚范围，起到屏蔽和过滤的作用，<b>缺省是向外公布</b>。可以通过 cost 选项来设置汇聚路由的度量值。</p> <p>可以定义多个区域路由汇聚命令，这样整个 OSPF 路由域的路由将得到简化，特别是网络规模大时，会提高网络转发性能。</p> <p>当配置了多条汇总，并且存在包含关系的时候，路由是根据最长匹配原则确定被汇总的 area range 的。</p> <p>area-id 可以用整数表示或者点分十进制表示。</p> <p>range <i>A.B.C.D/M</i>: 定义了汇聚路由的网段。</p> <p>A/B: 配置路由汇聚，允许向其他区域公布汇聚后的路由，属于汇聚网段内的原有路由不再公布。</p> <p>C: 配置路由汇聚，但不允许向其他区域公布汇聚后的路由，并且属于汇聚网段内的原有路由也不再公布。实际上对该 ABR 发往其他区域的 LSA Type3 起到了过滤的作用。</p> <p>D: 配置路由汇聚（advertise 方式），跟 A/B 一样，同时指定汇聚路由的路由代价。取值范围为 1-16777215。若未设置 cost，如果兼容 RFC1583，缺省值为被汇总的链路代价的最小值，否则为被汇总的链路代价的最大值。</p>

	<p>E: 配置路由汇聚, 但是往其他区域公布时使用一个新的路由, 具体网段信息由参数 <i>substitutue A.B.C.D/M</i> 给出。</p> <p>F/G/H/I/J: 全部等价, 删除路由汇聚。</p>
--	--

配置被动接口

命令	<p><b>配置被动接口</b></p> <p>A: FRR(config-router)# <b>passive-interface</b> <i>IFNAME</i></p> <p>B: FRR(config-router)# <b>passive-interface</b> <i>IFNAME</i> A.B.C.D</p> <p>C: FRR(config-router)# <b>passive-interface</b> default</p> <p><b>取消配置</b></p> <p>FRR(config-router)# <b>no passive-interface</b> (<i>IFNAME</i> (<i>A.B.C.D</i>) default)</p>
描述	<p>OSPF 路由模式下进行配置。</p> <p>为了防止网络中的其他路由设备动的学习到路由设备的路由信息, 可以将本路由设备的指定网络接口设为被动接口或指定网络接口下的 IP 地址为被动地址。被动接口和被动地址不能接受和发送任何 LSA 信息。</p> <p>A: 设置指定网络接口为被动接口;</p> <p>B: 设置指定网络接口下的 IP 地址为被动地址;</p> <p>C: 设置本设备的所有网络接口为被动接口。</p>

配置区域间路由过滤

命令	<p><b>使用地址前缀列表过滤</b></p> <p>FRR(config-router)# <b>area</b> <i>area-id</i> <b>filter-list</b> <i>PL_NAME</i> (in out)</p> <p><b>取消配置</b></p> <p>FRR(config-router)# <b>no area</b> <i>area-id</i> <b>filter-list</b> <i>PL_NAME</i> (in out)</p>
描述	<p>OSPF 路由模式下进行配置。</p> <p>在区域的 ABR 上进行配置才有意义, 对 LSA Type3 进行过滤。</p> <p><i>area-id</i> 可以用整数表示或者点分十进制表示。</p> <p><i>PL_NAME</i>: 关联的地址前缀列表的名字。</p> <p>in: 表示对引入本区域的路由前缀按照关联的 <i>prefix-list</i> 进行过滤。对应表项行为为 permit 的路由允许引入本区域, 对应表项行为为 deny 的路由不允许引入本区域。</p> <p>out: 表示对本区域往其他区域发布的路由前缀按照关联的 <i>prefix-list</i> 进行过滤。对应表项行为为 permit 的路由允许往其他区域发布, 对应表项行为为 deny 的路由不允许往其他区域发布。</p>

命令	使用访问控制列表
----	----------

	<pre>A: FRR(config-router)# area <i>area-id</i> import-list <i>ACL_NAME</i> B: FRR(config-router)# area <i>area-id</i> export-list <i>ACL_NAME</i></pre> <p><b>取消配置</b></p> <pre>C: FRR(config-router)# no area <i>area-id</i> import-list <i>ACL_NAME</i> C: FRR(config-router)# no area <i>area-id</i> export-list <i>ACL_NAME</i></pre>
描述	<p>OSPF 路由模式下进行配置。</p> <p>在区域的 ABR 上进行配置才有意义，对 LSA Type3 进行过滤。</p> <p><i>area-id</i> 可以用整数表示或者点分十进制表示。</p> <p><i>ACL_NAME</i>: 关联的访问控制列表的名字。(只能使用 Zebra ACL，而不能使用标准 ACL)</p> <p>A: 表示对引入本区域的路由前缀按照关联的 ACL 进行过滤。对应表项行为为 permit 的路由允许引入本区域，对应表项行为为 deny 的路由不允许引入本区域。</p> <p>B: 表示对本区域往其他区域发布的路由前缀按照关联的 ACL 进行过滤。对应表项行为为 permit 的路由允许往其他区域发布，对应表项行为为 deny 的路由不允许往其他区域发布。</p>

#### ■ 配置重分布路由过滤

重分布的路由过滤可以直接用 redistribute 命令带 route-map 参数进行过滤，具体参见“路由重分布”章节说明。

也可以用 distribute-list 命令关联访问控制列表进行过滤。

命令	<p><b>重分布路由过滤</b></p> <pre>FRR(config-router)# distribute-list <i>ACL_NAME</i> out (static connect kernel rip isis bgp)</pre> <p><b>取消配置</b></p> <pre>FRR(config-router)# no distribute-list <i>ACL_NAME</i> out (static connect kernel rip isis bgp)</pre>
描述	<p>OSPF 路由模式下进行配置。</p> <p>在 ASBR 上进行配置才有意义，对 LSA Type5 或者 LSA Type7 进行过滤。</p> <p><i>ACL_NAME</i>: 关联的访问控制列表的名字。(只能使用 Zebra ACL，而不能使用标准 ACL)</p> <p>后面的路由协议参数跟 redistribute 配置重分布的路由协议对应，表示对这个/些路由协议引入的路由进行过滤。</p> <p>针对不同的路由协议，可以配置不同的 ACL。对应表项行为为 permit 的路由允许引入本路由域，对应表项行为为 deny 的路由不允许引入本路由域。</p>

#### ■ 注意点

- 在非 ABR 设备上配置 area range，无法进行区间路由汇聚。
- 对 OSPF 而言，若在 ABR 上配置了路由管理的路由过滤（具体参见“路由管理”章节），由于过滤掉的路由本地转发不生效，但是 OSPF 协议还是会将这些路由信息通

过 Type-3 LSA (Summary LSA) 往其他区域通告, 这可能会产生黑洞路由 (即其他区域认为网络可达, 但实际不可达, 因为本设备实际不能转发到对应目的地) 此时可以在 ABR 上通过 `area filter-list out` 或者 `area range` 带 `not-advertise` 选项来避免。

### 3.4.7. 路由代价及管理距离

#### ■ 配置自动代价计算参数

命令	<b>配置参考带宽</b> FRR(config-router)# <b>auto-cost reference-bandwidth</b> <i>ref-bw</i>  <b>取消配置</b> FRR(config-router)# <b>no auto-cost reference-bandwidth</b> ( <i>ref-bw</i>  )
描述	OSPF 路由模式下进行配置。 缺省情况下, OSPF 接口cost 值等于自动代价参考值/接口带宽。 使用auto-cost 命令配置自动代价参考值。使用bandwidth 命令设置接口带宽。  <i>ref-bw</i> : 单位为 Mbps, 取值范围为 1-4294967, 默认值为 100000。

命令	<b>配置接口带宽</b> FRR(config-if)# <b>bandwidth</b> <i>bandwidth</i>  <b>取消配置</b> FRR(config-if)# <b>no bandwidth</b> ( <i>bandwidth</i>  )
描述	接口模式下进行配置。 缺省情况下, OSPF 接口cost 值等于自动代价参考值/接口带宽。 使用auto-cost 命令配置自动代价参考值。使用bandwidth 命令设置接口带宽。  <i>bandwidth</i> : 单位为 Mbps, 取值范围为 1-100000。缺省该配置值为 0 (当带宽配置值为 0 时, 根据接口的速率确定带宽, 三层接口速率恒定为 1000)。

#### ■ 配置接口 cost 值

命令	<b>配置接口 cost</b> FRR(config-if)# <b>ip ospf cost</b> <i>cost</i>  <b>取消配置</b> FRR(config-if)# <b>no ip ospf cost</b> ( <i>cost</i>  )
描述	接口模式下进行配置。 使用该命令配置接口的cost后, 将会覆盖缺省计算的cost值。 虚链路的cost值在配置虚链路章节有相关描述。

	<i>cost</i> : 取值范围为 1-65535。未配置时，接口 <i>cost</i> 根据自动计算得到。
--	---

■ 配置缺省路由的 *cost* 值

命令	<b>配置缺省路由 <i>cost</i> 值</b> FRR(config-router)# <b>area</b> <i>area-id</i> <b>default-cost</b> <i>cost</i>  <b>取消配置</b> FRR(config-router)# <b>no area</b> <i>area-id</i> <b>default-cost</b> <i>cost</i>
描述	OSPF 路由模式下进行配置。 该命令只有在Stub区域或者NSSA区域的ABR上配置才能生效。 Stub区域或者NSSA区域的ABR设备会在本区域内通告一条表示缺省路由的LSA，用户可以通过命令修改通告的缺省路由的LSA的 <i>cost</i> 值。  <i>cost</i> : 取值范围为 0-16777215。缺省值为 1。

■ 配置重分布路由的缺省 *metric* 值

命令	<b>配置重分布路由的缺省 <i>metric</i> 值</b> FRR(config-router)# <b>default-metric</b> <i>metric</i>  <b>取消配置</b> FRR(config-router)# <b>no default-metric</b> <i>metric</i>
描述	OSPF 路由模式下进行配置。 该命令只有在ASBR上配置才能生效。 <i>default-metric</i> 命令必须与 <i>redistribute</i> 命令配合使用，可以修改所有重分布路由的初始化量度值。  <i>metric</i> : 取值范围为 0-16777214。缺省情况下，重分布 BGP 路由的 <i>metric</i> 为 1，重分布其它路由的 <i>metric</i> 为 20。

■ 配置路由汇聚的 *cost* 值

在路由汇聚章节描述了汇聚路由的 *cost* 值的配置方法，如果未配置。缺省值选择依赖于是否兼容 RFC1583，如果兼容 RFC1583，缺省值为被汇总的链路代价的最小值，否则为被汇总的链路代价的最大值。

命令	<b>配置兼容 RFC1583</b> FRR(config-router)# <b>ospf rfc1583compatibility</b>  <b>配置不兼容 RFC1583</b> FRR(config-router)# <b>no ospf rfc1583compatibility</b>
描述	OSPF 路由模式下进行配置。



默认兼容 RFC1583。

## ■ 配置通告最大 metric

命令	<p><b>配置通告最大 metric</b></p> <pre>FRR(config-router)#max-metric router-lsa administrative FRR(config-router)#max-metric router-lsa on-shutdown <i>time</i> FRR(config-router)#max-metric router-lsa on-startup <i>time</i></pre> <p><b>取消配置</b></p> <pre>FRR(config-router)#no max-metric router-lsa administrative FRR(config-router)#no max-metric router-lsa on-shutdown [<i>time</i>] FRR(config-router)#no max-metric router-lsa on-startup [<i>time</i>]</pre>
描述	<p>OSPF 路由模式下进行配置。</p> <p>该命令用于向区域内其他路由设备通知本路由设备的 Router LSA (LSA Type1) 对应的 metric 为最大值。以使得在 OSPF 计算时，途经此路由设备的任何路径，总代价都会变得很大，几乎不可能成为最短路径。</p> <p>该功能用于支持 RFC3137。可以无条件开启此功能或者有条件的支持该功能。</p> <p><b>administrative:</b> 无条件开启此功能，除非手工取消此配置。</p> <p><b>on-shutdown <i>time</i>:</b> 在 OSPF 路由进程关闭前的 <i>time</i> 秒时间内开启此功能，这样可以保证路由器可以从 OSPF 域中正常退出。<i>time</i> 的取值范围为 5-100。</p> <p><b>on-startup <i>time</i>:</b> 在 OSPF 路由进程启动后的 <i>time</i> 秒时间内开启此功能，可以使 OSPF 首先完全收敛，而不会影响其他路由器使用的任何现有路由。<i>time</i> 的取值范围为 5-86400。</p>

## ■ 配置管理距离

命令	<p><b>配置管理距离</b></p> <pre>A: FRR(config-router)#distance <i>distance</i> B: FRR(config-router)#distance ospf {intra-area <i>distance</i>   inter-area <i>distance</i>   external <i>distance</i>}</pre> <p><b>取消配置</b></p> <pre>C: FRR(config-router)#no distance <i>distance</i> D: FRR(config-router)#no distance ospf ({intra-area <i>distance</i>   inter-area <i>distance</i>   external <i>distance</i>}  )</pre>
描述	<p>OSPF 路由模式下进行配置。</p> <p><b>A:</b> 设置所有OSPF路由的管理距离，取值范围：1-255。默认值为110。</p> <p><b>B:</b> 区分设置更详细的OSPF路由的管理距离。</p> <p><b>intra-area <i>distance</i>:</b> 设置区域内路由管理距离，取值范围：1-255。默认等于A对应的管理距离。</p> <p><b>inter-area <i>distance</i>:</b> 设置区域间路由管理距离，取值范围：1-255。默认等于A对应</p>

	<p>的管理距离。</p> <p><code>external distance</code>: 设置外部路由管理距离, 取值范围: 1-255。默认等于 A 对应的管理距离。</p> <p>D: 若 <code>ospf</code> 后没有再带其他关键字, 表示将所有设置的详细 OSPF 路由的管理距离配置全部取消。</p>
--	---

#### ■ 常见错误

- `ip ospf cost` 配置为 0, 路由计算可能会出错, 比如计算出路由环路。

### 3.4.8. 认证功能

#### ■ 配置区域的认证方式

命令	<p><b>配置区域的认证方式</b></p> <pre>FRR(config-router)#area area-id authentication (message-digest )</pre> <p><b>取消配置</b></p> <pre>FRR(config-router)#no area area-id authentication (message-digest )</pre>
描述	<p>OSPF 路由模式下进行配置。</p> <p>区域的认证方式可以支持三种:</p> <ol style="list-style-type: none"> <li>1) 方式 0, 不要求认证, 当没有用该命令启用 OSPF 认证, OSPF 数据包中的认证方式为 0;</li> <li>2) 方式 1, 为明文认证模式, 配置该命令时, 没有使用 <code>message-digest</code> 选项;</li> <li>3) 方式 2, 为 MD5 认证模式, 配置该命令时, 使用 <code>message-digest</code> 选项。</li> </ol> <p>一个 OSPF 区域中所有的路由设备, 必须采用同一种认证方式。如果启用了认证, 还必须在有连接邻居的接口 (或者虚链路, 对应 area 0 的认证方式配置) 配置认证密钥。接口配置命令 <code>ip ospf authentication-key</code> 可以配置明文认证密钥; 接口配置命令 <code>ip ospf message-digest-key</code> 可以配置 MD5 认证密钥。</p> <p>不管普通的三层接口, 还是虚链路, 也可以配置认证方式, 只有未设置认证方式时, 才采用 area 设置的认证方式, 否则以接口配置的认证方式为准。</p> <p>虚链路的认证方式和认证密钥配置参见“虚链路”章节。</p>

#### ■ 配置接口的认证方式

命令	<p><b>配置接口的认证方式</b></p> <pre>FRR(config-if)#ip ospf authentication (message-digest null ) [A.B.C.D]</pre> <p><b>取消配置</b></p> <pre>FRR(config-if)#no ip ospf authentication (message-digest null ) [A.B.C.D]</pre>
描述	<p>接口模式下进行配置。</p> <p>接口的认证方式可以配置如下 4 种情况:</p> <p>未配置: 表示未指定认证方式, 采用所在区域设置认证方式。</p>

	<p>authentication: 采用认证模式。</p> <p>authentication null: 不要求认证。</p> <p>authentication message-digest: 采用 MD5 认证模式。</p> <p>当接口上的认证方式和接口所在的区域的认证方式都设置时，优先采用接口上的认证方式。</p> <p>[A.B.C.D] 当一个接口存在多个 IP 地址时，也意味着对应多个网段，可以通过 IP 地址区分多个网段，可以基于网段来配置认证方式。当前系统不支持一个三层接口配置多个 IP 地址，所以，此参数意义不大。</p>
--	--

■ 配置接口的认证密钥

命令	<p><b>配置接口的认证密钥</b></p> <p>A: FRR(config-if)# ip ospf message-digest-key (1-255) md5 AUTH_KEY [A.B.C.D/M]</p> <p>B: FRR(config-if)# ip ospf authentication-key AUTH_KEY [A.B.C.D]</p> <p><b>取消配置</b></p> <p>C: FRR(config-if)# no ip ospf message-digest-key (1-255) [md5 AUTH_KEY] [A.B.C.D/M]</p> <p>C: FRR(config-if)# no ip ospf authentication-key [AUTH_KEY] [A.B.C.D]</p>
描述	<p>接口模式下进行配置。</p> <p>A: 配置 MD5 加密认证方式的密钥标识符和密钥。密钥标识符取值范围 1-255。</p> <p>B: 配置明文认证方式的密钥。</p> <p>A 和 B 两种密钥可以同时配置，具体采用哪个，或者都不采用，依赖于接口的认证方式来确定。</p> <p>C: 删除 MD5 认证方式的密钥标识符和密钥。</p> <p>D: 删除明文认证方式的密钥。</p> <p>在删除时，AUTH_KEY 是可选参数。</p> <p>[A.B.C.D] 当一个接口存在多个 IP 地址时，也意味着对应多个网段，可以通过 IP 地址区分多个网段，可以基于网段来配置密钥。当前系统不支持一个三层接口配置多个 IP 地址，所以，此参数意义不大。</p>

■ 常见错误

- 设置的认证方式和密钥不匹配。

3.4.9. 控制参数

■ 关闭 MTU 校验

命令	关闭 MTU 校验
----	-----------

	<pre>FRR(config-if)# ip ospf mtu-ignore [A.B.C.D]</pre> <p><b>取消配置</b></p> <pre>FRR(config-if)# no ip ospf mtu-ignore [A.B.C.D]</pre>
描述	<p>接口模式下进行配置。</p> <p>OSPF 在收到数据库描述报文时会校验邻居的接口的 MTU 和自己接口的 MTU 是否相同，如果收到的数据库描述报文中指示的接口的 MTU 大于接收接口的 MTU，那么邻接关系将不能被建立，此时可以通过关闭 MTU 的校验来解决。</p> <p><i>[A.B.C.D]</i> 当一个接口存在多个 IP 地址时，也意味着对应多个网段，可以通过 IP 地址区分多个网段，可以基于网段来关闭 MTU 校验。当前系统不支持一个三层接口配置多个 IP 地址，所以，此参数意义不大。</p>

#### ■ 配置 hello 时间

命令	<p><b>配置 hello 时间</b></p> <pre>FRR(config-if)# ip ospf hello-interval seconds [A.B.C.D]</pre> <p><b>取消配置</b></p> <pre>FRR(config-if)# no ip ospf hello-interval [seconds [A.B.C.D] ]</pre>
描述	<p>接口模式下进行配置。</p> <p>hello 报文时间间隔包含在hello报文中。该时间越短，OSPF检测到拓扑变化的时间也将越快，但是将增加网络流量。同一网段上的所有路由设备的hello报文时间间隔必须一致。如果还想手工修改判断邻居死亡时间，必须<b>保证hello报文时间间隔不能大于邻居死亡时间</b>。</p> <p><i>seconds</i>: 取值范围1-65535，默认10，单位为秒。</p> <p><i>[A.B.C.D]</i> 当一个接口存在多个 IP 地址时，也意味着对应多个网段，可以通过 IP 地址区分多个网段，可以基于网段来配置 hello 时间。当前系统不支持一个三层接口配置多个 IP 地址，所以，此参数意义不大。</p>

#### ■ 配置 dead 时间

命令	<p><b>配置 dead 时间</b></p> <pre>FRR(config-if)# ip ospf dead-interval seconds [A.B.C.D]</pre> <p><b>取消配置</b></p> <pre>FRR(config-if)# no ip ospf hello-interval [seconds [A.B.C.D] ]</pre>
描述	<p>接口模式下进行配置。</p> <p>OSPF的死亡时间包含在Hello 报文内。如果OSPF在死亡时间内，没有收到邻居发送的</p>

	<p>Hello报文，就宣告邻居无效并从邻居表中删除该邻居记录。hello时间和dead时间手工修改时，必须十分谨慎。有两点必须注意：</p> <p>第一点：死亡时间间隔，不能小于hello 报文时间间隔；</p> <p>第二点：同一网段上的所有路由设备的死亡时间间隔必须一致。</p> <p><i>seconds</i>：取值范围1-65535，默认40，单位为秒。</p> <p><i>[A.B.C.D/M]</i> 当一个接口存在多个 IP 地址时，也意味着对应多个网段，可以通过 IP 地址区分多个网段，可以基于网段来配置 dead 时间。当前系统不支持一个三层接口配置多个 IP 地址，所以，此参数意义不大。</p>
--	---

#### ■ 配置 LSU 发送时延

命令	<p><b>配置 LSU 发送延迟</b></p> <pre>FRR(config-if)# ip ospf transmit-delay seconds [A.B.C.D]</pre> <p><b>取消配置</b></p> <pre>FRR(config-if)# no ip ospf transmit-delay [seconds] [A.B.C.D]</pre>
描述	<p>接口模式下进行配置。</p> <p>在传输 LSU 报文之前，该报文中所有 LSAs（链路状态描述）的 Age 字段将增加，增加量根据该接口配置命令 ip ospf transmit-delay 的定义。设置该参数必须考虑到该接口的发送和线路传播时延，对于低速线路，接口的传输延时应该设置得大些。</p> <p>对 Age 达到 3600 的 LSA，将进行重传或请求重传，如果没有得到及时更新，超时的 LSA 将从链路状态数据库中清除。</p> <p><i>seconds</i>：取值范围1-65535，默认1，单位为秒。</p> <p><i>[A.B.C.D/M]</i> 当一个接口存在多个 IP 地址时，也意味着对应多个网段，可以通过 IP 地址区分多个网段，可以基于网段来配置 LSU 发送时延。当前系统不支持一个三层接口配置多个 IP 地址，所以，此参数意义不大。</p>

#### ■ 配置 LSU 重传间隔

命令	<p><b>配置 LSU 重传间隔</b></p> <pre>FRR(config-if)# ip ospf retransmit-interval seconds [A.B.C.D]</pre> <p><b>取消配置</b></p> <pre>FRR(config-if)# no ip ospf retransmit-interval [seconds] [A.B.C.D]</pre>
描述	<p>接口模式下进行配置。</p> <p>当路由设备发送完一个LSU报文，该LSU报文还保留在发送缓冲队列中，如果在ip ospf retransmit-interval命令定义的时间内，没有得到邻居的确认，将重新发送该LSU。</p>

	<p><i>seconds</i>: 取值范围3-65535, 默认5, 单位为秒。</p> <p>[A.B.C.D/M] 当一个接口存在多个 IP 地址时, 也意味着对应多个网段, 可以通过 IP 地址区分多个网段, 可以基于网段来配置 LSU 重传间隔。当前系统不支持一个三层接口配置多个 IP 地址, 所以, 此参数意义不大。</p>
--	--

#### ■ 配置 LSA 重复接收延迟

命令	<p><b>配置 LSA 重复接收延迟</b></p> <pre>FRR(config-router)# timer lsa min-arrival <i>arrival-time</i></pre> <p><b>取消配置</b></p> <pre>FRR(config-router)#no timer lsa min-arrival [<i>arrival-time</i>]</pre>
描述	<p>OSPF 路由模式下进行配置。</p> <p>配置指定时间之内接收到的相同LSA, 认为是重复的LSA, 不做处理。</p> <p><i>Arrival-time</i>: 取值范围0-600000, 默认1000, 单位为毫秒。</p>

#### ■ 配置 LSA 发送间隔

命令	<p><b>配置 LSA 生成时间</b></p> <pre>FRR(config-router)# timer throttle lsa all <i>time</i></pre> <p><b>取消配置</b></p> <pre>FRR(config-router)#no timer throttle lsa all [<i>time</i>]</pre>
描述	<p>OSPF 路由模式下进行配置。</p> <p>配置LSA在两次发送之间的最小间隔。对链路发化时收敛性要求较高时, 可以配置为较小值。若希望减少CPU消耗, 可以把几个值适当调高。</p> <p><i>time</i>: 取值范围0-5000, 默认5000, 单位为毫秒。</p>

#### ■ 配置 SPF 计算延迟

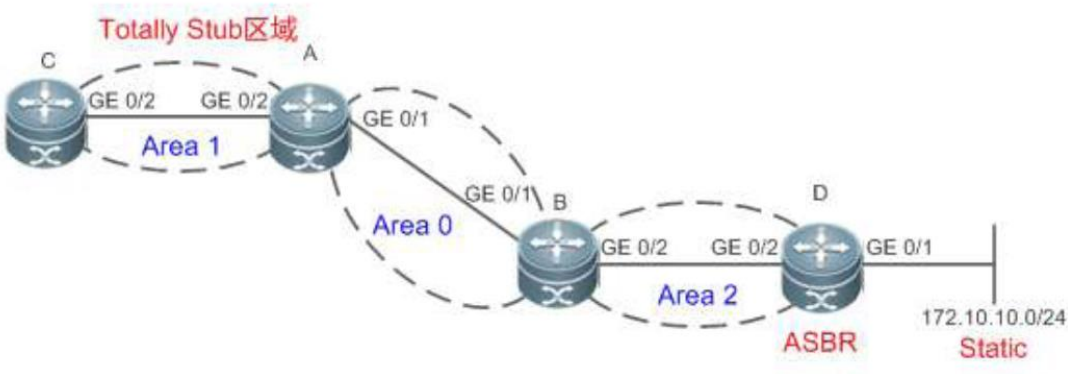
命令	<p><b>配置 LSA 生成时间</b></p> <pre>FRR(config-router)# timer throttle spf <i>spf-delay spf-holdtime spf-max-waittime</i></pre> <p><b>取消配置</b></p> <pre>FRR(config-router)#no timer throttle spf [<i>spf-delay spf-holdtime spf-max-waittime</i>]</pre>
描述	<p>OSPF 路由模式下进行配置。</p>

	<p>spf-delay：定义 SPF 计算的等待时间，以毫秒为单位，取值范围：1-600000。缺省为 0。OSPF 路由进程接收到拓扑变化，触发的 SPF 计算至少要在 spf-delay 时间间隔后执行。</p> <p>spf-holdtime：定义两次 SPF 运算之间的最小时间间隔，以毫秒为单位，取值范围：1-600000。缺省为 50。</p> <p>spf-max-waittime：定义两次 SPF 运算之间的最大时间间隔，以毫秒为单位，取值范围：1-600000。缺省为 5000。</p> <p>spf-delay 表示从拓扑发生发化到 SPF 开始计算，至少需要延迟的时间。第一次触发 SPF 计算到第二次触发 SPF 计算的最小时间间隔为 spf-holdtime，此后，连续触发 SPF 计算的时间间隔至少为上一次时间间隔的两倍，当时间间隔达到 spf-max-waittime 之后，将不再增加。如果两次 SPF 计算的时间间隔已经超过了要求的最小值，那么 SPF 计算时间间隔将重新从 spf-holdtime 开始计算。</p> <p>spf-delay 和 spf-holdtime 可以设置小些以加快拓扑的收敛；spf-max-waittime 可以设置大些以减少 SPF 计算，可以根据实际网络拓扑稳定性采取灵活设置。</p> <ol style="list-style-type: none"><li>1. spf-holdtime 的值不能小于 spf-delay，否则 spf-holdtime 的值将被自动设置为与 spf-delay 相等；</li><li>2. spf-max-waittime 的值不能小于 spf-holdtime，否则 spf-max-waittime 的值将被自动设置为与 spf-holdtime 相等；</li></ol>
--	---

■ 常见错误

- 配置的 dead 时间小于 hello 时间。

3.5. 配置案例



各接口所属的 VLAN 和 SVI 的 IP 地址如下所示：（所有路由设备以交换机为例）

- A : GE 0/1 VLAN10 192.168.1.1/24  
GE 0/2 VLAN20 192.168.2.1/24
- B : GE 0/1 VLAN10 192.168.1.2/24  
GE 0/2 VLAN30 192.168.3.1/24
- C : GE 0/2 VLAN20 192.168.2.2/24
- D : GE0/1 VLAN40 192.168.6.1/24

GEO/2 VLAN30 192.168.3.2/24

## ■ 配置路由设备 A

- 主 CLI：配置接口 VLAN，配置对应 SVI 的 IP 地址。

```
SWITCH(config)#vlan 10,20
SWITCH(config)#interface gi 0/1
SWITCH(config-if)#switch access vlan 10
SWITCH(config-if)#exit
SWITCH(config)#interface gi 0/2
SWITCH(config-if)#switch access vlan 20
SWITCH(config-if)#exit
SWITCH(config)#int Vlan10
SWITCH(config-if)#ip address 192.168.1.1/24
SWITCH(config-if)#exit
SWITCH(config)#int Vlan20
SWITCH(config-if)#ip address 192.168.2.1/24
```

- FRR CLI：

- ✧ 启动 OSPF，配置 Router ID。
- ✧ 启动网段的 OSPF，并指定对应 Area。
- ✧ 配置 Area1 为 Totally Stub 区域。

```
FRR#configure terminal
FRR(config)#router ospf
FRR(config-router)#ospf router-id 192.168.1.1
FRR(config-router)#network 192.168.1.0/24 area 0
FRR(config-router)#network 192.168.2.0/24 area 1
FRR(config-router)#area 1 stub no-summary
```

## ■ 配置路由设备 B

- 主 CLI：配置接口 VLAN，配置对应 SVI 的 IP 地址。（省略）

- FRR CLI：

- ✧ 启动 OSPF，配置 Router ID。
- ✧ 启动网段的 OSPF，并指定对应 Area。
- ✧ 配置 Area2 为 NSSA 区域。

```
FRR#configure terminal
FRR(config)#router ospf
FRR(config-router)#ospf router-id 192.168.1.2
FRR(config-router)#network 192.168.1.0/24 area 0
FRR(config-router)#network 192.168.3.0/24 area 2
FRR(config-router)#area 2 nssa
```

## ■ 配置路由设备 C

- 主 CLI：配置接口 VLAN，配置对应 SVI 的 IP 地址。



➤ FRR CLI:

- ✧ 启动 OSPF，配置 Router ID。
- ✧ 启动网段的 OSPF，并指定对应 Area。
- ✧ 配置 Area1 为 Totally Stub 区域。

```
FRR#configure terminal
FRR(config)#router ospf
FRR(config-router)#ospf router-id 192.168.2.2
FRR(config-router)#network 192.168.2.0/24 area 1
FRR(config-router)#area 1 stub no-summary
```

■ 配置路由设备 D

➤ 主 CLI：配置接口 VLAN，配置对应 SVI 的 IP 地址。

➤ FRR CLI:

- ✧ 启动 OSPF，配置 Router ID。
- ✧ 启动网段的 OSPF，并指定对应 Area。
- ✧ 配置 Area2 为 NSSA 区域。
- ✧ 配置到达 172.10.10.0/24 的静态路由。
- ✧ 重分布静态路由（变为 Area2 的 ASBR）。

```
FRR#configure terminal
FRR(config)#ip route 172.10.10.0/24 192.168.6.2
FRR(config)#router ospf
FRR(config-router)#ospf router-id 192.168.3.2
FRR(config-router)#network 192.168.3.0/24 area 2
FRR(config-router)#area 2 nssa
FRR(config-router)#redistribute static
```

■ 配置效果

➤ 路由设备 A：（学习到 192.168.3.0/24 和 172.10.10.0/24）

```
FRR#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.1.2	1	Full/DR	37.041s	192.168.1.2	Vlan10
192.168.2.2	1	Full/BDR	36.031s	192.168.2.2	Vlan20

```
FRR#show ip route ospf
```

Codes: K - kernel route, C - connected, S - static, R - RIP,

O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,

T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,

F - PBR,

> - selected route, \* - FIB route

```
O 192.168.1.0/24 [110/100] is directly connected, Vlan10, 01w1d17h
```

```
O 192.168.2.0/24 [110/100] is directly connected, Vlan20, 4d20h26m
```

```
O>* 192.168.3.0/24 [110/200] via 192.168.1.2, Vlan10, 3h09m
```

```
O>* 172.10.10.0/24 [110/20] via 192.168.1.2, Vlan10, 3h09m
```

- 路由设备 B: (学习到 192.168.3.0/24 和 172.10.10.0/24)

```
FRR#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.1.1	1	Full/BDR	37.041s	192.168.1.1	Vlan10
192.168.3.2	1	Full/BDR	38.031s	192.168.3.2	Vlan30

```
FRR#show ip route ospf
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
```

```
O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
```

```
T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
```

```
F - PBR,
```

```
> - selected route, * - FIB route
```

```
O 192.168.1.0/24 [110/100] is directly connected, Vlan10, 01w1d17h
```

```
O 192.168.3.0/24 [110/100] is directly connected, Vlan30, 4d20h26m
```

```
O>* 192.168.2.0/24 [110/200] via 192.168.1.1, Vlan10, 3h09m
```

```
O>* 172.10.10.0/24 [110/20] via 192.168.3.2, Vlan10, 3h09m
```

- 路由设备 C: (只有一条默认路由指向 ABR)

```
FRR#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.1.1	1	Full/DR	37.041s	192.168.2.1	Vlan20

```
FRR# show ip route ospf
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
```

```
O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
```

```
T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
```

```
F - PBR,
```

```
> - selected route, * - FIB route
```

```
O 192.168.2.0/24 [110/100] is directly connected, Vlan20, 4d20h26m
```

```
O>* 0.0.0.0/0 [110/1] via 192.168.2.1, Vlan20, 3h09m
```

- 路由设备 D: (学习到 192.168.1.0/24 和 192.168.2.0/24, 同时也存在一条默认路由指向 ABR)

```
FRR#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.1.2	1	Full/DR	34.041s	192.168.3.1	Vlan30

```
FRR#show ip route ospf
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
```

```
O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
```

```
T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
```

```
F - PBR,
```

```
> - selected route, * - FIB route
```

```

O>* 0.0.0.0/0 [110/1] via 192.168.3.1, Vlan30, 3h09m
O 192.168.6.0/24 [110/100] is directly connected, Vlan40, 4d20h26m
O>* 192.168.1.0/24 [110/20] via 192.168.3.1, Vlan30, 3h09m
O>* 192.168.2.0/24 [110/20] via 192.168.3.1, Vlan30, 3h09m

```

### 3.6. 显示命令

#### ■ 查看路由表信息

参见 2.5.2 “路由管理” 章节说明。

#### ■ 查看 OSPF 邻居

```
FRR# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.2.1	1	Full/DR	34.146s	192.168.2.1	Vlan2

```
FRR# show ip ospf neighbor Vlan2
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.2.1	1	Full/DR	33.736s	192.168.2.1	Vlan2

```
FRR# show ip ospf neighbor all
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.2.1	1	Full/DR	35.766s	192.168.2.1	Vlan2

```
FRR# show ip ospf neighbor detail
```

```

Neighbor 192.168.2.1, interface address 192.168.2.1
  In the area 0.0.0.0 via interface Vlan2
  Neighbor priority is 1, State is Full, 5 state changes
  Most recent state change statistics:
    Progressive change 1d22h15m ago
  DR is 192.168.2.1, BDR is 192.168.2.2
  Options 2 *| -| -| -| -| E| -
  Dead timer due in 38.545s
  Database Summary List 0
  Link State Request List 0
  Link State Retransmission List 0
  Thread Inactivity Timer on
  Thread Database Description Retransmission off
  Thread Link State Request Retransmission on
  Thread Link State Update Retransmission on

```

#### ■ 查看 OSPF 路由表

```
FRR# show ip ospf route
```

```
===== OSPF network routing table =====
```

```

N IA 192.168.1.0/24      [10001] area: 0.0.0.0
                        via 192.168.2.1, Vlan2
N   192.168.2.0/24      [1] area: 0.0.0.0
                        directly attached to Vlan2
N   192.168.100.0/24     [1000] area: 0.0.0.2
                        directly attached to Vlan1

```

```

===== OSPF router routing table =====

```

```

R   192.168.2.1          [1] area: 0.0.0.0, ABR, ASBR
                        via 192.168.2.1, Vlan2

```

```

===== OSPF external routing table =====

```

```

N E2 5.5.5.0/24          [10001/20] tag: 0
                        via 192.168.2.1, Vlan2
N E1 6.6.6.0/24          [10021] tag: 0
                        via 192.168.2.1, Vlan2

```

- 查看边界路由器，ABR 或者 ASBR

```

FRR# show ip ospf border-routers

```

```

===== OSPF router routing table =====

```

```

R   192.168.2.1          [1] area: 0.0.0.0, ABR, ASBR
                        via 192.168.2.1, Vlan2

```

- 查看 OSPF 接口信息

```

FRR# show ip ospf interface

```

```

Vlan1 is up

```

```

  ifindex 8, MTU 1500 bytes, BW 10 Mbit <UP, BROADCAST, RUNNING, MULTICAST>

```

```

  Internet Address 192.168.100.50/24, Broadcast 192.168.100.255, Area 0.0.0.2

```

```

[N

```

```

SSA]

```

```

  MTU mismatch detection: enabled

```

```

  Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1000

```

```

  Transmit Delay is 1 sec, State DR, Priority 1

```

```

  No backup designated router on this network

```

```

  Multicast group memberships: OSPFAllRouters OSPFDesignatedRouters

```

```

  Timer intervals configured, Hello 10s, Dead 40s, Wait 40s, Retransmit 5

```

```

    Hello due in 3.485s

```

```

  Neighbor Count is 0, Adjacent neighbor count is 0

```

```

Vlan2 is up

```

```

  ifindex 9, MTU 1500 bytes, BW 1000 Mbit <UP, BROADCAST, RUNNING, MULTICAST>

```

```

  Internet Address 192.168.2.2/24, Broadcast 192.168.2.255, Area 0.0.0.0

```

```

  MTU mismatch detection: enabled

```

```

  Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1

```

```

  Transmit Delay is 1 sec, State Backup, Priority 1

```

```
Backup Designated Router (ID) 3.3.3.3, Interface Address 192.168.2.2
Multicast group memberships: OSPFAllRouters OSPFDesignatedRouters
Timer intervals configured, Hello 10s, Dead 40s, Wait 40s, Retransmit 5
  Hello due in 3.485s
Neighbor Count is 1, Adjacent neighbor count is 1
```

```
FRR# show ip ospf interface Vlan2
Vlan2 is up
  ifindex 9, MTU 1500 bytes, BW 1000 Mbit <UP, BROADCAST, RUNNING, MULTICAST>
  Internet Address 192.168.2.2/24, Broadcast 192.168.2.255, Area 0.0.0.0
  MTU mismatch detection: enabled
  Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State Backup, Priority 1
  Backup Designated Router (ID) 3.3.3.3, Interface Address 192.168.2.2
  Multicast group memberships: OSPFAllRouters OSPFDesignatedRouters
  Timer intervals configured, Hello 10s, Dead 40s, Wait 40s, Retransmit 5
    Hello due in 6.655s
  Neighbor Count is 1, Adjacent neighbor count is 1
```

■ 查看 OSPF 数据库（整体）

```
FRR# show ip ospf database
```

OSPF Router with ID (3.3.3.3)

Router Link States (Area 0.0.0.0)

Link ID	ADV Router	Age	Seq#	CkSum	Link count
3.3.3.3	3.3.3.3	836	0x80000114	0xd574	1
192.168.2.1	192.168.2.1	588	0x8000010a	0x77e6	1

Net Link States (Area 0.0.0.0)

Link ID	ADV Router	Age	Seq#	CkSum
192.168.2.1	192.168.2.1	248	0x800000f3	0xe62f

Summary Link States (Area 0.0.0.0)

Link ID	ADV Router	Age	Seq#	CkSum	Route
192.168.1.0	192.168.2.1	958	0x800000fe	0x93bd	192.168.1.0/24
192.168.100.0	3.3.3.3	1446	0x80000102	0x3e57	192.168.100.0/24

Router Link States (Area 0.0.0.2 [NSSA])

Link ID	ADV Router	Age	Seq#	CkSum	Link count
3.3.3.3	3.3.3.3	1376	0x800000d5	0x9013	1

Summary Link States (Area 0.0.0.2 [NSSA])

Link ID	ADV Router	Age	Seq#	CkSum	Route
0.0.0.0	3.3.3.3	1536	0x800000d2	0x95ea	0.0.0.0/0

NSSA-external Link States (Area 0.0.0.2 [NSSA])

Link ID	ADV Router	Age	Seq#	CkSum	Route
0.0.0.0	3.3.3.3	766	0x800000fe	0x7a4b	E2 0.0.0.0/0 [0x0]
192.168.1.0	3.3.3.3	246	0x80000102	0xcb0c	E2 192.168.1.0/24 [0x0]
192.168.33.0	3.3.3.3	416	0x800000d6	0x6be4	E2 192.168.33.0/24 [0x0]
192.168.58.0	3.3.3.3	536	0x80000102	0x71c8	E2 192.168.58.0/24 [0x0]

AS External Link States

Link ID	ADV Router	Age	Seq#	CkSum	Route
0.0.0.0	3.3.3.3	766	0x800000fe	0x9631	E2 0.0.0.0/0 [0x0]
5.5.5.0	192.168.2.1	168	0x800001c5	0x05a9	E2 5.5.5.0/24 [0x0]
6.6.6.0	192.168.2.1	528	0x800001c5	0x5dce	E1 6.6.6.0/24 [0x0]
192.168.1.0	3.3.3.3	246	0x80000102	0xe7f1	E2 192.168.1.0/24 [0x0]
192.168.33.0	3.3.3.3	416	0x800000d6	0x87ca	E2 192.168.33.0/24 [0x0]
192.168.58.0	3.3.3.3	536	0x80000102	0x8dae	E2 192.168.58.0/24 [0x0]

■ 查看 OSPF 数据库（asbr-summary）

FRR# show ip ospf database asbr-summary

OSPF Router with ID (192.168.2.1)

ASBR-Summary Link States (Area 0.0.0.0)

ASBR-Summary Link States (Area 0.0.0.1)

LS age: 358

Options: 0x2 : \*|---|E|

LS Flags: 0x3

LS Type: summary-LSA

Link State ID: 3.3.3.3 (AS Boundary Router address)

Advertising Router: 192.168.2.1

LS Seq Number: 80000062

Checksum: 0xf05a

Length: 28

Network Mask: /0

TOS: 0 Metric: 10000

ASBR-Summary Link States (Area 0.0.0.2 [NSSA])

■ 查看 OSPF 数据库 (external)

FRR# show ip ospf database external

OSPF Router with ID (192.168.2.1)

AS External Link States

LS age: 1221

Options: 0x2 : \*|---|---|E|---

LS Flags: 0x6

LS Type: AS-external-LSA

Link State ID: 0.0.0.0 (External Network Number)

Advertising Router: 3.3.3.3

LS Seq Number: 800000fe

Checksum: 0x9631

Length: 36

Network Mask: /0

Metric Type: 2 (Larger than any link state path)

TOS: 0

Metric: 1

Forward Address: 0.0.0.0

External Route Tag: 0

LS age: 621

Options: 0x2 : \*|---|---|E|---

LS Flags: 0xb

LS Type: AS-external-LSA

Link State ID: 5.5.5.0 (External Network Number)

Advertising Router: 192.168.2.1

LS Seq Number: 800001c5

Checksum: 0x05a9

Length: 36

Network Mask: /24

Metric Type: 2 (Larger than any link state path)

TOS: 0

Metric: 20

Forward Address: 192.168.1.100

External Route Tag: 0

LS age: 981

Options: 0x2 : \*|---|E|

LS Flags: 0xb

LS Type: AS-external-LSA

Link State ID: 6.6.6.0 (External Network Number)

Advertising Router: 192.168.2.1

LS Seq Number: 800001c5

Checksum: 0x5dce

Length: 36

Network Mask: /24

Metric Type: 1

TOS: 0

Metric: 20

Forward Address: 192.168.1.100

External Route Tag: 0

LS age: 701

Options: 0x2 : \*|---|E|

LS Flags: 0x6

LS Type: AS-external-LSA

Link State ID: 192.168.1.0 (External Network Number)

Advertising Router: 3.3.3.3

LS Seq Number: 80000102

Checksum: 0xe7f1

Length: 36

Network Mask: /24

Metric Type: 2 (Larger than any link state path)

TOS: 0

Metric: 20

Forward Address: 192.168.2.1

External Route Tag: 0

LS age: 871

Options: 0x2 : \*|---|E|



```
LS Flags: 0x6
```

```
LS Type: AS-external-LSA
```

```
Link State ID: 192.168.33.0 (External Network Number)
```

```
Advertising Router: 3.3.3.3
```

```
LS Seq Number: 800000d6
```

```
Checksum: 0x87ca
```

```
Length: 36
```

```
Network Mask: /24
```

```
Metric Type: 2 (Larger than any link state path)
```

```
TOS: 0
```

```
Metric: 20
```

```
Forward Address: 0.0.0.0
```

```
External Route Tag: 0
```

```
LS age: 991
```

```
Options: 0x2 : *|---|E|---
```

```
LS Flags: 0x6
```

```
LS Type: AS-external-LSA
```

```
Link State ID: 192.168.58.0 (External Network Number)
```

```
Advertising Router: 3.3.3.3
```

```
LS Seq Number: 80000102
```

```
Checksum: 0x8dae
```

```
Length: 36
```

```
Network Mask: /24
```

```
Metric Type: 2 (Larger than any link state path)
```

```
TOS: 0
```

```
Metric: 20
```

```
Forward Address: 192.168.100.3
```

```
External Route Tag: 0
```

#### ■ 查看 OSPF 数据库 (network)

```
FRR# show ip ospf database network
```

```
OSPF Router with ID (192.168.2.1)
```

```
Net Link States (Area 0.0.0.0)
```

```
LS age: 775
```

```
Options: 0x2 : *|---|E|---
```

```
LS Flags: 0x3
```

```
LS Type: network-LSA
```

Link State ID: 192.168.2.1 (address of Designated Router)

Advertising Router: 192.168.2.1

LS Seq Number: 800000f3

Checksum: 0xe62f

Length: 32

Network Mask: /24

Attached Router: 192.168.2.1

Attached Router: 3.3.3.3

Net Link States (Area 0.0.0.1)

Net Link States (Area 0.0.0.2 [NSSA])

#### ■ 查看 OSPF 数据库 (nssa-external)

FRR# show ip ospf database nssa-external

OSPF Router with ID (192.168.2.1)

NSSA-external Link States (Area 0.0.0.0)

NSSA-external Link States (Area 0.0.0.1)

NSSA-external Link States (Area 0.0.0.2 [NSSA])

LS age: 777

Options: 0x2 : \*| - | - | - | - | E | -

LS Flags: 0xb

LS Type: NSSA-LSA

Link State ID: 5.5.5.0 (External Network Number for NSSA)

Advertising Router: 192.168.2.1

LS Seq Number: 800001c5

Checksum: 0xe8c3

Length: 36

Network Mask: /24

Metric Type: 2 (Larger than any link state path)

TOS: 0

Metric: 20

NSSA: Forward Address: 192.168.1.100

External Route Tag: 0

LS age: 1137

```
Options: 0x2 : *|---|E|
```

```
LS Flags: 0xb
```

```
LS Type: NSSA-LSA
```

```
Link State ID: 6.6.6.0 (External Network Number for NSSA)
```

```
Advertising Router: 192.168.2.1
```

```
LS Seq Number: 800001c5
```

```
Checksum: 0x41e8
```

```
Length: 36
```

```
Network Mask: /24
```

```
Metric Type: 1
```

```
TOS: 0
```

```
Metric: 20
```

```
NSSA: Forward Address: 192.168.1.100
```

```
External Route Tag: 0
```

#### ■ 查看 OSPF 数据库 (router)

```
FRR# show ip ospf database router
```

```
OSPF Router with ID (192.168.2.1)
```

```
Router Link States (Area 0.0.0.0)
```

```
LS age: 1489
```

```
Options: 0x2 : *|---|E|
```

```
LS Flags: 0x6
```

```
Flags: 0x3 : ABR ASBR
```

```
LS Type: router-LSA
```

```
Link State ID: 3.3.3.3
```

```
Advertising Router: 3.3.3.3
```

```
LS Seq Number: 80000114
```

```
Checksum: 0xd574
```

```
Length: 36
```

```
Number of Links: 1
```

```
Link connected to: a Transit Network
```

```
(Link ID) Designated Router address: 192.168.2.1
```

```
(Link Data) Router Interface address: 192.168.2.2
```

```
Number of TOS metrics: 0
```

```
TOS 0 Metric: 1
```

```
LS age: 1239
```

Options: 0x2 : \*|---|E|

LS Flags: 0x3

Flags: 0x3 : ABR ASBR

LS Type: router-LSA

Link State ID: 192.168.2.1

Advertising Router: 192.168.2.1

LS Seq Number: 8000010a

Checksum: 0x77e6

Length: 36

Number of Links: 1

Link connected to: a Transit Network

(Link ID) Designated Router address: 192.168.2.1

(Link Data) Router Interface address: 192.168.2.1

Number of TOS metrics: 0

TOS 0 Metric: 10000

#### Router Link States (Area 0.0.0.1)

LS age: 1449

Options: 0x2 : \*|---|E|

LS Flags: 0x3

Flags: 0x3 : ABR ASBR

LS Type: router-LSA

Link State ID: 192.168.2.1

Advertising Router: 192.168.2.1

LS Seq Number: 800001c9

Checksum: 0x9b70

Length: 36

Number of Links: 1

Link connected to: Stub Network

(Link ID) Net: 192.168.1.0

(Link Data) Network Mask: 255.255.255.0

Number of TOS metrics: 0

TOS 0 Metric: 10000

#### Router Link States (Area 0.0.0.2 [NSSA])

LS age: 329

```
Options: 0x8 : *|---|N/P|---|
```

```
LS Flags: 0x3
```

```
Flags: 0x13 : ABR ASBR
```

```
LS Type: router-LSA
```

```
Link State ID: 192.168.2.1
```

```
Advertising Router: 192.168.2.1
```

```
LS Seq Number: 800000c2
```

```
Checksum: 0xe8c6
```

```
Length: 24
```

```
Number of Links: 0
```

#### ■ 查看 OSPF 数据库 (summary)

```
FRR# show ip ospf database summary
```

```
OSPF Router with ID (192.168.2.1)
```

```
Summary Link States (Area 0.0.0.0)
```

```
LS age: 1728
```

```
Options: 0x2 : *|---|---|E|
```

```
LS Flags: 0x3
```

```
LS Type: summary-LSA
```

```
Link State ID: 192.168.1.0 (summary Network Number)
```

```
Advertising Router: 192.168.2.1
```

```
LS Seq Number: 800000fe
```

```
Checksum: 0x93bd
```

```
Length: 28
```

```
Network Mask: /24
```

```
TOS: 0 Metric: 10000
```

```
LS age: 498
```

```
Options: 0x2 : *|---|---|E|
```

```
LS Flags: 0x6
```

```
LS Type: summary-LSA
```

```
Link State ID: 192.168.100.0 (summary Network Number)
```

```
Advertising Router: 3.3.3.3
```

```
LS Seq Number: 80000103
```

```
Checksum: 0x3c58
```

```
Length: 28
```

```
Network Mask: /24
```

TOS: 0 Metric: 1000

#### Summary Link States (Area 0.0.0.1)

LS age: 508

Options: 0x2 : \*|---|E|

LS Flags: 0x3

LS Type: summary-LSA

Link State ID: 192.168.2.0 (summary Network Number)

Advertising Router: 192.168.2.1

LS Seq Number: 800000fe

Checksum: 0x88c7

Length: 28

Network Mask: /24

TOS: 0 Metric: 10000

LS age: 1158

Options: 0x2 : \*|---|E|

LS Flags: 0x3

LS Type: summary-LSA

Link State ID: 192.168.100.0 (summary Network Number)

Advertising Router: 192.168.2.1

LS Seq Number: 80000062

Checksum: 0xbbe2

Length: 28

Network Mask: /24

TOS: 0 Metric: 11000

#### Summary Link States (Area 0.0.0.2 [NSSA])

LS age: 568

Options: 0x0 : \*|---|

LS Flags: 0x3

LS Type: summary-LSA

Link State ID: 0.0.0.0 (summary Network Number)

Advertising Router: 192.168.2.1

LS Seq Number: 800000c2

Checksum: 0xef40

Length: 28

Network Mask: /0

TOS: 0 Metric: 1

LS age: 568

Options: 0x0 : \*|---|---|---|

LS Flags: 0x3

LS Type: summary-LSA

Link State ID: 192.168.1.0 (summary Network Number)

Advertising Router: 192.168.2.1

LS Seq Number: 800000c2

Checksum: 0x2a65

Length: 28

Network Mask: /24

TOS: 0 Metric: 10000

LS age: 478

Options: 0x0 : \*|---|---|---|

LS Flags: 0x3

LS Type: summary-LSA

Link State ID: 192.168.2.0 (summary Network Number)

Advertising Router: 192.168.2.1

LS Seq Number: 800000c2

Checksum: 0x1f6f

Length: 28

Network Mask: /24

TOS: 0 Metric: 10000

LS age: 1308

Options: 0x0 : \*|---|---|---|

LS Flags: 0x3

LS Type: summary-LSA

Link State ID: 192.168.100.0 (summary Network Number)

Advertising Router: 192.168.2.1

LS Seq Number: 80000062

Checksum: 0xd9c6

Length: 28

Network Mask: /24

TOS: 0 Metric: 11000

- 查看 OSPF 数据库 (self-originate)

```
FRR# show ip ospf database self-originate
```

```
OSPF Router with ID (192.168.2.1)
```

```
Router Link States (Area 0.0.0.0)
```

Link ID	ADV Router	Age	Seq#	CkSum	Link count
192.168.2.1	192.168.2.1	1535	0x8000010a	0x77e6	1

```
Net Link States (Area 0.0.0.0)
```

Link ID	ADV Router	Age	Seq#	CkSum
192.168.2.1	192.168.2.1	1195	0x800000f3	0xe62f

```
Summary Link States (Area 0.0.0.0)
```

Link ID	ADV Router	Age	Seq#	CkSum	Route
192.168.1.0	192.168.2.1	175	0x800000ff	0x91be	192.168.1.0/24

```
Router Link States (Area 0.0.0.1)
```

Link ID	ADV Router	Age	Seq#	CkSum	Link count
192.168.2.1	192.168.2.1	45	0x800001ca	0x9971	1

```
Summary Link States (Area 0.0.0.1)
```

Link ID	ADV Router	Age	Seq#	CkSum	Route
192.168.2.0	192.168.2.1	685	0x800000fe	0x88c7	192.168.2.0/24
192.168.100.0	192.168.2.1	1335	0x80000062	0xbbe2	192.168.100.0/24

```
ASBR-Summary Link States (Area 0.0.0.1)
```

Link ID	ADV Router	Age	Seq#	CkSum
3.3.3.3	192.168.2.1	1215	0x80000062	0xf05a

```
Router Link States (Area 0.0.0.2 [NSSA])
```

Link ID	ADV Router	Age	Seq#	CkSum	Link count
192.168.2.1	192.168.2.1	625	0x800000c2	0xe8c6	0

```
Summary Link States (Area 0.0.0.2 [NSSA])
```



Link ID	ADV Router	Age	Seq#	CkSum	Route
0.0.0.0	192.168.2.1	745	0x800000c2	0xef40	0.0.0.0/0
192.168.1.0	192.168.2.1	745	0x800000c2	0x2a65	192.168.1.0/24
192.168.2.0	192.168.2.1	655	0x800000c2	0x1f6f	192.168.2.0/24
192.168.100.0	192.168.2.1	1485	0x80000062	0xd9c6	192.168.100.0/24

NSSA-external Link States (Area 0.0.0.2 [NSSA])

Link ID	ADV Router	Age	Seq#	CkSum	Route
5.5.5.0	192.168.2.1	1115	0x800001c5	0xe8c3	E2 5.5.5.0/24 [0x0]
6.6.6.0	192.168.2.1	1475	0x800001c5	0x41e8	E1 6.6.6.0/24 [0x0]

AS External Link States

Link ID	ADV Router	Age	Seq#	CkSum	Route
5.5.5.0	192.168.2.1	1115	0x800001c5	0x05a9	E2 5.5.5.0/24 [0x0]
6.6.6.0	192.168.2.1	1475	0x800001c5	0x5dce	E1 6.6.6.0/24 [0x0]

3.7. 清除命令

- 清除全部 OSPF 信息
 

```
clear ip ospf
```
- 基于接口清除 OSPF 信息
 

```
clear ip ospf interface IF_NAME
```

## 4. 配置 RIP

### 4.1. 概述

RIP（Routing Information Protocol，路由信息协议）是一种单播路由协议，应用于 IPv4 网络。运行 RIP 的路由器之间通过交换路由信息，获得到达远端网络的路由。

RIP 属于 IGP（Interior Gateway Protocol，内部网关协议），只能在 AS 内运行，适用于规模较小的网络（不大于 16 跳）。

*RIP 有两个版本，RFC1058 定义了 RIPv1，RFC2453 定义了 RIPv2。*

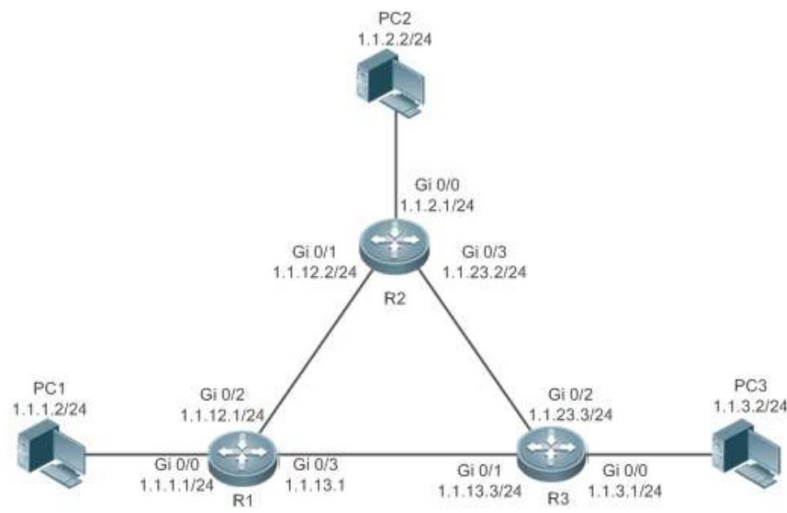
### 4.2. 典型应用

典型应用	场景描述
RIP 基本应用	在一个小型网络中，通过 RIP 自动维护路由信息。
RIP 与 BGP 互联	多个 AS 互联，在 AS 内部运行 RIP，在 AS 之间运行 BGP。

#### 4.2.1. RIP 基本应用

在组网结构比较简单的网络中，可以通过配置 RIP 实现网络互通，相比 OSPF 等 IGP 协议 RIP 的配置更为简单，相比静态路由 RIP 能够动态适应网络结构变化，更容易维护。

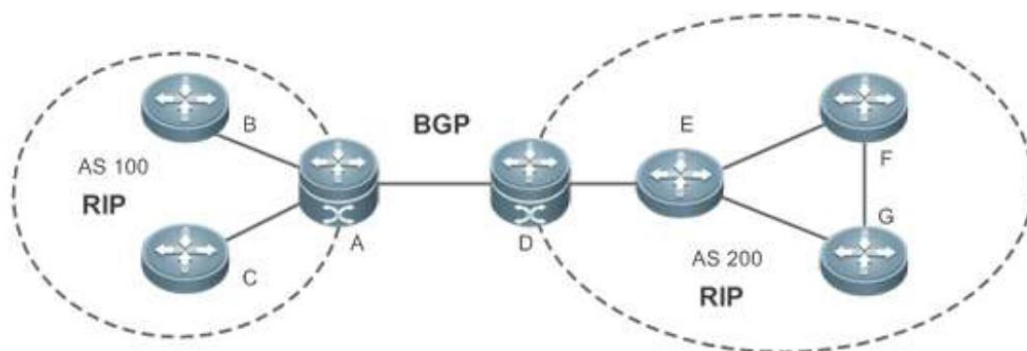
以下图为例，为了使得 PC1，PC2，PC3 互通，可以在 R1，R2，R3 上配置 RIP 路由。



#### 4.2.2. RIP 与 BGP 互联

多个 AS 互联，在 AS 内部运行 RIP，在 AS 之间运行 BGP。通常，RIP 与 BGP 应该相互学习路由信息。

以下图为例，AS100 和 AS200 内部都是通过 RIP 协议来实现单播路由，在两个 AS 之间通过 BGP 协议来实现单播路由。（A，D 上需要同时运行 RIP 协议和 BGP 协议）。



### 4.3. 功能详解

RIP (路由信息协议) 是一种广泛部署的内部网关协议。RIP 是 Xerox Labs 在 1970 年代开发的，是 XNS 路由协议的一部分。RIP 是一种距离矢量协议，基于 Bellman-Ford 算法。作为距离矢量协议，RIP 路由设备定期向其邻居发送更新，从而允许收敛到已知拓扑。在每次更新中，到任何给定网络的距离都将广播到其相邻路由设备。

#### 4.3.1. RIP 协议

##### ■ RIPv1和RIPv2

RIPv1 以广播方式发送 RIPv1 报文，广播地址 255.255.255.255，UDP 端口号 520。RIPv1 不能识别子网掩码，仅支持有类别路由。

RIPv2 以组播方式发送 RIPv2 报文，组播地址 224.0.0.9，UDP 端口号 520。RIPv2 能够识别子网掩码，支持无类别路由、路由汇聚、超网路由。RIPv2 支持认证，提供明文认证和 MD5 加密认证两种方式。

缺省情况下，接口接收 RIPv1 和 RIPv2 报文，以组播方式发送 RIPv2 报文。

- RIP 路由模式下使用 `version` 命令，定义所有接口上接收和发送的 RIP 报文的版本号。
- 接口模式下使用 `ip rip send version` 命令，在接口上定义发送的 RIP 报文的版本号。
- 接口模式下使用 `ip rip receive version` 命令，在接口上定义接收的 RIP 报文的版本号。
- 接口模式下使用 `ip rip receive version none` 命令，禁止接口接收 RIP 报文。
- RIP 路由模式下使用 `passive-interface` 命令，禁止接口以广播或组播的方式发送 RIP 报文。
- 接口模式下使用 `ip rip v2-broadcast` 命令，在接口上以广播方式发送 RIPv2 报文。
- RIP 路由模式下使用 `neighbor` 命令指定邻居，以单播方式向指定的邻居路由设备发送 RIP 报文。

##### ■ 路由算法

RIP 是一种基于距离矢量 (Distance-Vector) 算法的协议，运用矢量叠加的方法来计算路由信息。

**注意：***metric 在各种路由协议中含义不同，RIP 的 metric 不能等同于 OSPF 的 metric。OSPF 的 metric 表示路由代价，等同于 cost。而 RIP 的 metric 表示的是距离（及跳数）。*

##### ➤ 距离矢量算法

RIP 是一种基于距离矢量算法的协议。“距离矢量”就是将一条路由信息看作一个由目的网络和距离 (metric) 组成的矢量。路由设备从邻居处获得一条路由信息，并在

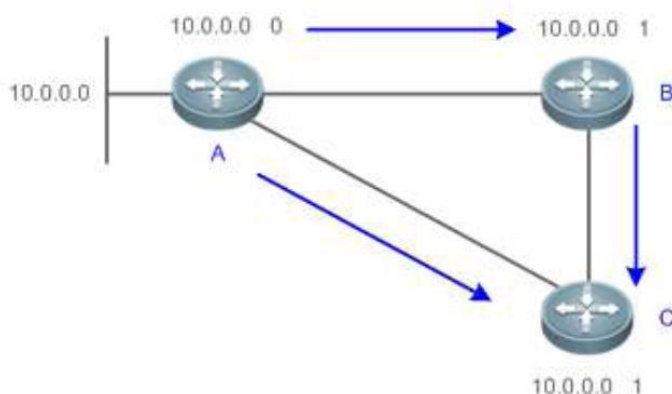
这条路由信息上叠加从自己到这个邻居的距离矢量，从而形成自己的路由信息。

RIP使用跳数（Hop Count）来衡量到达目的网络的距离（metric）。缺省情况下，路由设备与它直接相连网络的跳数为0，通过一个路由设备可达的网络的跳数为1，其余依此类推。也就是说，metric等于从本网络到达目的网络间的路由设备数量。为限制收敛时间，RIP规定metric取0~15之间的整数，大于或者等于16表示目的网络或主机不可达。由于这个限制，使得RIP不可能在大型网络中得到应用。

#### ➤ 选择最优路由

RIP选择最优路由的原则：如果路由器获得了多条到达同一目的网络的路由信息，优先选用metric值较小的路由信息。

如下图所示，A连接网络10.0.0.0。C从A处获得路由信息（10.0.0.0，0），从B处获得路由信息（10.0.0.0，1），则C会选用来自A的路由信息，并在此基础上叠加1到metric，得到自己的路由信息（10.0.0.0，1），下一跳指向A。



### ■ 交换路由信息

#### ➤ 初始化

路由设备启动RIP后，会向相邻路由设备发送请求报文（Request message），请求全部路由信息（即路由表）。邻居收到请求报文后，回送包含本地路由表的响应报文（Response message）。路由设备收到响应报文后，更新本地路由表，同时向相邻路由设备发送更新报文（Update message），通告路由更新信息。相邻路由设备收到更新报文后，更新本地路由表，并向其它相邻路由设备发送更新报文。在一还串的更新通告后，各路由设备都能获得并保持最新的路由信息。

#### ➤ 定时更新

缺省情况下，RIP启用定时更新。相邻路由设备之间每隔30秒（update timer）进行完全的路由信息交换（即将整个路由表发送给给邻居）。1份更新报文只能包含25条路由，发送整个路由表可能需要大量更新报文。通过设置更新报文间的发送间隔，可以避免路由信息丢失。

对于每条非本地路由，如果180秒内（invalid timer）得不到刷新，则metric值改为16（不可达）；如果随后的120秒（flush timer）得不到刷新，则从路由表中删除。

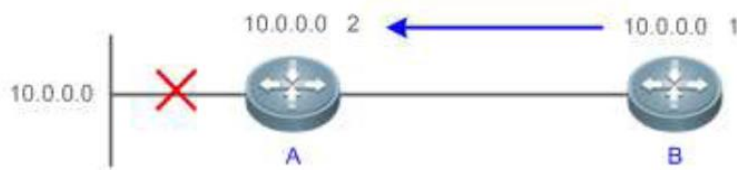
### ■ 避免环路

由于距离矢量算法的固有缺陷，RIP会发生路由环路。

如下图所示，A连接网络10.0.0.0，每隔30秒发送一次Update报文。因此B每30秒会收到从A发送来的到10.0.0.0的路由。如果A到10.0.0.0的连接中断，到10.0.0.0的路由就会从A的路由表中消失，下次A发出的Update报文将不再包含此路由。

因为B没有收到关于10.0.0.0的Update报文，在180秒内认为到10.0.0.0的路由有效，并使

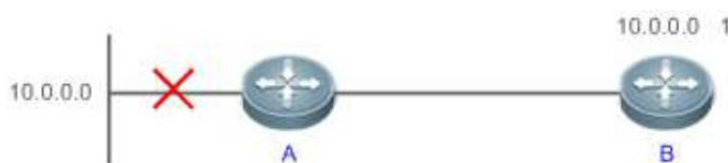
用Update报文将此路由发送给A。因为A上不存在到10.0.0.0的路由，因此将从B学到的路由加入路由表。于是，B认为通过A能够到达网络10.0.0.0，A认为通过B能够到达网络10.0.0.0，形成路由环路。



#### ➤ 水平分隔

水平分割可以防止路由环路。在接口上启动水平分割功能后，从该接口接收到的路由，不会从该接口发送出去。

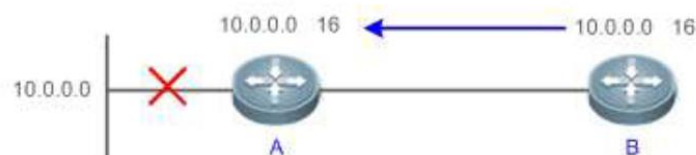
如下图所示，在B上，与A相连的接口上启动水平分割后，B不会再把到10.0.0.0的路由发回给A，180秒后B会知道10.0.0.0不可达。



#### ➤ 毒性逆转

毒性逆转也可以防止路由环路。相比水平分割，毒性逆转更加可靠，但会带来更多的协议报文，增加网络负担。在接口上启动毒性逆转后，从该接口接收到的路由，会再从该接口发送出去，但metric会被改为16（即不可达）。

如下图所示，在B上，与A相连的接口上启动毒性逆转后，B从A学习到路由10.0.0.0之后，就将该路由的metric设置为16，定时发回A。当该路由失效后，B向A通告度量值为16的10.0.0.0路由，这将加快该路由信息的清除。



### 4.3.2. RIP 路由管理

#### ■ 路由重分布

对于RIP来说，其他类型的路由（比如直连路由、静态路由、其他路由协议的路由）为外部路由。

RIP路由模式下使用redistribute 命令，可以将外部路由（**不包括缺省路由**）重分布到RIP，并通告给邻居。

使用redistribute命令带route-map参数，可以对引入的外部路由进行过滤或者修改参数信息。带metric参数可以对引入的外部路由修改metric值。

#### ■ 缺省路由

在路由表中，目的网络为0.0.0.0/0 的路由为缺省路由。可以从邻居学到缺省路由，也可以向邻居发送缺省路由。

RIP路由模式下使用default-information originate 命令，向所有接口向邻居通告缺省路由。

■ 路由过滤

可以通过设置过滤规则，限制相邻设备间交换的路由信息。只有被过滤规则允许的路由信息，才能被发送或接收。

- RIP路由模式下使用`distribute-list xxx out`命令，设置过滤规则，限制设备发出的路由信息。
- RIP路由模式下使用`distribute-list xxx in`命令，设置过滤规则，限制设备接收的路由信息。
- RIP路由模式下使用`passive-interface` 命令，设置被动接口。被动接口上不能交互路由信息。

■ metric 和 distance

对于设备主动发现的RIP路由，缺省metric值等于从本地到目的网络的跳数。对于人为配置的RIP路由（缺省路由、重分布路由），缺省metric值为1。

- RIP路由模式下使用`offset-list xxx in` 命令，可以增加收到的RIP 路由的metric值。
- RIP路由模式下使用`offset-list xxx out` 命令，可以增加发出的RIP 路由的metric值。
- RIP路由模式下使用`default-metric`命令，可以修改重分布路由的缺省metric值。
- RIP路由模式下使用`redistribute`命令带metric参数，可以在重分布路由时修改其metric值。

缺省情况下，RIP 路由的distance值为120。

RIP路由模式下使用`distance`命令，可以修改RIP路由的distance值。

■ 认证

RIPv1不支持认证，RIPv2支持认证。

在接口上启动认证功能后，如果认证失败，则相邻设备间无法交换路由信息。认证功能用来阻止非法设备接入RIP 路由域。

支持两种认证方式：明文认证和MD5加密认证。

## 4.4. 配置命令

### 4.4.1. RIP 基本功能

■ 进入 RIP 路由模式

命令	<p><b>进入 RIP 路由模式（当 RIP 进程未激活，该命令同时激活 RIP 进程）</b></p> <pre>FRR(config)#router rip FRR(config-router)#</pre> <p><b>使 RIP 进程处于未激活状态</b><pre>FRR(config)#no router rip</pre></p>
描述	<p>全局模式下进行配置。</p> <p>RIP 相关的大部分配置均需要在 RIP 路由模式下进行。</p>

■ 关联本地网络

命令	<b>关联本地网络</b>
----	---------------

	<p>FRR(config-router)#<b>network</b> (A.B.C.D/M   IFNAME)</p> <p><b>取消关联</b></p> <p>FRR(config-router)#<b>no network</b> (A.B.C.D/M   IFNAME)</p>
描述	<p>RIP 路由模式下进行配置。</p> <p>网段可以用三层接口来表示，该三层接口对应的网段被关联。也可以用网段的 IP 地址和掩码长度来表示。</p> <p>只有被 network 覆盖的接口才能运行 RIP，才能被 RIP 学到直连路由，才能交互 RIP 报文。配置 network 0.0.0.0/0，即可覆盖所有接口。</p>

#### ■ 配置防环策略

命令	<p><b>启动防环策略</b></p> <p>FRR(config-if)#<b>ip rip split-horizon</b> [ poisoned-reverse ]</p> <p><b>关闭防环策略</b></p> <p>FRR(config-if)#<b>no ip rip split-horizon</b> [ poisoned-reverse ]</p>
描述	<p>接口模式下进行配置。</p> <p>默认情况下，所有接口开启水平分割。</p> <p>ip rip split-horizon: 开启水平分割（关闭毒性逆转），对应默认情况。</p> <p>ip rip split-horizon poisoned-reverse: 开启毒性逆转（关闭水平分割）。</p> <p>no ip rip split-horizon 或者 no ip rip split-horizon poisoned-reverse: 关闭水平分割和毒性逆转，即关闭防环策略。</p>

### 4.4.2. RIP 报文交互

#### ■ 全局定义 RIP 版本

命令	<p><b>定义 RIP 版本</b></p> <p>FRR(config-router)#<b>version</b> &lt;1-2&gt;</p> <p><b>取消配置</b></p> <p>FRR(config-router)#<b>no version</b> (&lt;1-2&gt;   )</p>
描述	<p>RIP 路由模式下进行配置。</p> <p>1 对应 RIPv1，2 对应 RIPv2。</p> <p>此命令对整机生效，定义所有接口上发送和接收的 RIP 报文的版本号。</p> <p>缺省情况下，可同时接收 RIPv1 和 RIPv2，只发送 RIPv2。</p>

#### ■ 接口定义 RIP 版本

命令	<p><b>定义发送 RIP 版本</b></p> <p>FRR(config-if)#<b>ip rip send version</b> {1   2}</p> <p><b>取消配置</b></p>
----	---

	<b>FRR(config-if)#no ip rip send version</b>
描述	<p>接口模式下进行配置。</p> <p>1 对应RIPv1, 2 对应RIPv2。</p> <p>缺省情况下, 发送的RIP版本取决于全局定义RIP版本的配置。该命令的配置结果, 可以覆盖全局定义RIP版本的配置。该命令只影响本接口发送RIP报文的行为, 可以允许该接口同时发送RIPv1和RIPv2的数据 (同时指定1和2)。</p>

命令	<p><b>定义接收 RIP 版本</b></p> <p>FRR(config-if)#<b>ip rip receive version {1   2}</b></p> <p><b>取消配置</b></p> <p>FRR(config-if)#<b>no ip rip receive version</b></p>
描述	<p>接口模式下进行配置。</p> <p>1 对应RIPv1, 2 对应RIPv2。</p> <p>缺省情况下, 接收的RIP版本取决于全局定义RIP版本的配置。该命令的配置结果, 可以覆盖全局定义RIP版本的配置。该命令只影响本接口接收RIP报文的行为, 可以允许该接口同时接收RIPv1和RIPv2的数据 (同时指定1和2)。</p>

#### ■ 接口单播发送路由更新报文

命令	<p><b>配置 neighbor</b></p> <p>FRR(config-router)#<b>neighbor A.B.C.D</b></p> <p><b>取消配置</b></p> <p>FRR(config-router)#<b>no neighbor A.B.C.D</b></p>
描述	<p>RIP 路由模式下进行配置。</p> <p>手工指定邻居后, 对邻居采用单播报文发送路由更新报文。</p> <p>一般可以先配置命令passive-interface 将相应接口设置为被动接口, 然后只定义某些邻居可以接收到路由信息。该命令不会影响RIP信息报文的接收。</p>

#### ■ 接口广播发送 RIPv2 报文

命令	<p><b>配置广播发送 RIPv2</b></p> <p>FRR(config-if)#<b>ip rip v2-broadcast</b></p> <p><b>取消配置</b></p> <p>FRR(config-if)#<b>no ip rip v2-broadcast</b></p>
描述	<p>接口模式下进行配置。</p> <p>缺省情况下, RIPv2报文采用组播报文发送, 如果配置本命令, 在本接口使用广播方式来发送RIPv2报文。但本命令不控制发送RIP报文的版本, 如果本接口只发送RIPv1报</p>



	文，那么本命令配置不取任何作用。
--	------------------

4.4.3. 路由重分布及缺省路由

■ 路由重分布

命令	<p><b>配置路由重分布</b></p> <pre>FRR(config-router)#redistribute (static connect kernel ospf isis bgp) [metric <i>metric</i>] [route-map <i>RM_NAME</i>]</pre> <p><b>取消配置</b><pre>FRR(config-router)#no redistribute (static connect kernel ospf isis bgp) [metric <i>metric</i>] [route-map <i>RM_NAME</i>]</pre></p>
描述	<p>RIP 路由模式下进行配置。</p> <p>通过该命令，将其他源头的路由导入 RIP 协议，并将这些外部路由通告给 RIP 邻居。</p> <p><b>static:</b> 静态路由。</p> <p><b>connect:</b> 直连路由，开启 OSPF 的网段，会自动作为 connect 路由导入 OSPF 协议。</p> <p><b>kernel:</b> 内核路由，如果主 CLI 有配置 CLI，在 FRR CLI 中会作为 kernel 路由。不建议两边同时配置路由。</p> <p><b>ospf:</b> OSPF 协议的路由</p> <p><b>isis:</b> IS-IS 协议的路由</p> <p><b>bgp:</b> BGP 协议的路由</p> <p><b>metric <i>metric</i>:</b> 可选参数，设置外部路由的 metric，取值范围为 0-16。若未指定该参数，metric 为 1。</p> <p><b>route-map <i>RM_NAME</i>:</b> 可选参数，关联路由图，对重分布的路由实施过滤或者参数修改。可以修改 metric 以及路由的 tag。</p>

■ 向邻居通告缺省路由

命令	<p><b>向邻居通告缺省路由</b></p> <pre>FRR(config-router)#default-information originate</pre> <p><b>取消配置</b><pre>FRR(config-router)#no default-information originate</pre></p>
描述	<p>RIP 路由模式下进行配置。</p> <p>路由设备的路由表中即使存在缺省路由，RIP 默认也不会向外通告缺省路由。需要向邻居通告缺省路由，需要使用 default-information originate 命令。该命令只会向邻居通告缺省路由，但不会存在于本地路由表中。</p>

4.4.4. 路由过滤

■ 配置被动接口

命令	<p><b>配置被动接口</b></p> <p>FRR(config-router)#<b>passive-interface</b> (<i>IFNAME</i>   <b>default</b>)</p> <p><b>取消配置</b></p> <p>FRR(config-router)#<b>no passive-interface</b> (<i>IFNAME</i>   <b>default</b>)</p>
描述	<p>RIP 路由模式下进行配置。</p> <p>default 表示所有接口。</p> <p>如果要在某个 RIP 接口抑制更新报文，则需要设置被动接口。可以使用被动接口设置 RIP 由域的边界。被动接口所在网段属于 RIP 路由域，但被动接口上不能发送和接收 RIP 报文。RIP 路由域内的需要交互 RIP 路由的接口不能设置为被动接口。</p> <p>用被动接口来控制 RIP 路由域边界的时候，先配置 passive-interface default，将所有接口设置为被动接口。再配置 no passive-interface IFNAME 取消与域内路由设备互联的接口。</p>

■ 使用访问控制列表设置过滤规则

命令	<p><b>访问控制列表过滤</b></p> <p>FRR(config-router)#<b>distribute-list</b> <i>ACL_NAME</i> (in   out)</p> <p><b>取消配置</b></p> <p>FRR(config-router)#<b>no distribute-list</b> <i>ACL_NAME</i> (in   out)</p>
描述	<p>RIP 路由模式下进行配置。</p> <p><i>ACL_NAME</i>: 关联的访问控制列表的名字。(只能使用 Zebra ACL，而不能使用标准 ACL)</p> <p>in: 表示对收到 RIP 路由信息按照关联的 ACL 进行过滤。对应表项行为为 permit 的路由信息允许，对应表项行为为 deny 的路由信息禁止。</p> <p>out: 表示对发送 RIP 路由信息按照关联的 ACL 进行过滤。对应表项行为为 permit 的路由信息允许，对应表项行为为 deny 的路由信息禁止。</p>

■ 使用地址前缀列表设置过滤规则

命令	<p><b>地址前缀列表过滤</b></p> <p>FRR(config-router)#<b>distribute-list prefix</b> <i>PL_NAME</i> (in   out)</p> <p><b>取消配置</b></p> <p>FRR(config-router)#<b>no distribute-list prefix</b> <i>PL_NAME</i> (in   out)</p>
描述	<p>RIP 路由模式下进行配置。</p> <p><i>PF_NAME</i>: 关联的 prefix-list 的名字。</p> <p>in: 表示对收到 RIP 路由信息按照关联的 prefix-list 进行过滤。对应表项行为为 permit 的路由信息允许，对应表项行为为 deny 的路由信息禁止。</p>

	out：表示对发送 RIP 路由信息按照关联的 prefix-list 进行过滤。对应表项行为为 permit 的路由信息允许，对应表项行为为 deny 的路由信息禁止。
--	---

4.4.5. 认证功能

■ 配置接口的认证方式

命令	<p><b>配置认证方式</b></p> <p>FRR(config-if)#ip rip authentication mode (md5   text)</p> <p><b>取消配置</b></p> <p>FRR(config-if)#no ip rip authentication mode (md5   text   )</p>
描述	<p>接口模式下进行配置。</p> <p>接口的认证方式可以配置如下 3 种情况：</p> <p>未配置：表示不需要认证。</p> <p>md5：采用 MD5 认证模式。</p> <p>text：采用明文认证。</p>

■ 配置接口的认证密钥

命令	<p><b>配置接口的明文认证密钥</b></p> <p>FRR(config-if)#ip rip authentication string <i>AUTH_KEY</i></p> <p><b>取消配置</b></p> <p>FRR(config-if)#no ip rip authentication string (<i>AUTH_KEY</i>   )</p>
描述	<p>接口模式下进行配置。</p> <p>当该接口采用明文认证方式时，采用本命令设置的认证密钥进行认证。</p> <p>在删除时，<i>AUTH_KEY</i> 是可选参数。</p>

命令	<p><b>配置接口的 MD5 认证密钥</b></p> <p>FRR(config-if)#ip rip authentication key-chain <i>KEY_CHAIN_NAME</i></p> <p><b>取消配置</b></p> <p>FRR(config-if)#no ip rip authentication key-chain <i>KEY_CHAIN_NAME</i></p>
描述	<p>接口模式下进行配置。</p> <p>当该接口采用 MD5 认证方式时，采用本命令设置的认证密钥进行认证。</p> <p>在删除时，<i>KEY_CHAIN_NAME</i> 是可选参数。</p>

	<p><i>KEY_CHAIN_NAME</i> 不是 MD5 认证的密钥，而是所关联的 key-chain 的名字。key chain 是一个 key 的链（可以配置多个 key）。下面举例说明：</p> <pre>! key chain test   key 1     key-string dkakdfjkdfj !</pre> <pre>interface Vlan1   ip rip authentication mode md5   ip rip authentication key-chain test</pre>
--	---

4.4.6. 控制参数

■ 配置重分布路由的缺省 metric

命令	<p><b>配置重分布路由的缺省 metric 值</b></p> <p>FRR(config-router)#<b>default-metric</b> <i>metric</i></p> <p><b>取消配置</b></p> <p>FRR(config-router)#<b>no default-metric</b> <i>metric</i></p>
描述	<p>RIP 路由模式下进行配置。</p> <p><b>default-metric</b> 命令必须与 <b>redistribute</b> 命令配合使用，可以修改所有重分布路由的初始化 metric 值。</p> <p><i>metric</i>: 缺省的量度值，有效值为 1 到 16。如果 metric 值大于等于 16，则认为不可达。若配置，metric 为 1。</p>

■ 增加路由的 metric

命令	<p><b>增加路由的 metric</b></p> <p>FRR(config-router)#<b>offset-list</b> <i>ACL_NAME</i> { <b>in</b>   <b>out</b> } <i>offset_metric</i> [ <i>IFNAME</i> ]</p> <p><b>取消配置</b></p> <p>FRR(config-router)#<b>no offset-list</b> <i>ACL_NAME</i> { <b>in</b>   <b>out</b> } <i>offset_metric</i> [ <i>IFNAME</i> ]</p>
描述	<p>RIP 路由模式下进行配置。</p> <p>增加接收或发送的 RIP 路由的 metric 值，若指定接口则对应特定接口，若未指定则对应所有接口。</p> <p><i>ACL_NAME</i>: 关联的 ACL 的名字。（只能使用 Zebra ACL，而不能使用标准 ACL）</p> <p><i>offset_metric</i>: 相对路由原来的 metric 值增加的值。对接收的 RIP 路由，如果没有本配置命令，也会增加 1（表明经过了自己这台路由设备），如果配置了本命令且命中 <b>permit</b> 表项，则不会再额外增加 1。</p> <p><i>IFNAME</i>: 可选参数，对应的接口名字。</p> <p><b>in</b>: 表明对接收的 RIP 路由修改 metric 值。</p>

	<p>out: 表明对发送的 RIP 路由修改 metric 值。</p> <p>查询对应 ACL，对应表项行为为 permit 的路由增加 metric，对应表项行为为 deny 的路由不变动。</p>
--	--

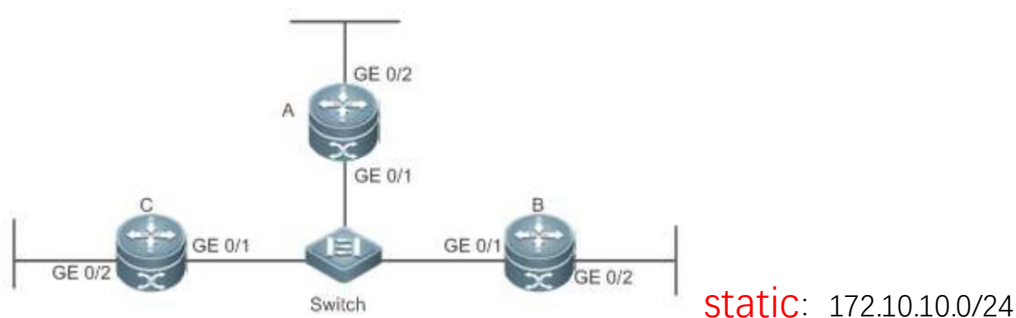
#### ■ 修改路由的 distance

命令	<p><b>配置 distance</b></p> <p>FRR(config-router)# <b>distance</b> <i>distance</i></p> <p><b>取消配置</b></p> <p>FRR(config-router)# <b>no distance</b> <i>distance</i></p>
描述	<p>RIP 路由模式下进行配置。</p> <p>设置所有RIP路由的管理距离，取值范围：1-255。默认值为120。</p>

#### ■ 修改时间参数

命令	<p><b>修改时间参数</b></p> <p>FRR(config-router)# <b>timers basic</b> <i>update_time invalid_time flush_time</i></p> <p><b>取消配置</b></p> <p>FRR(config-router)# <b>no timers basic</b> [<i>update_time invalid_time flush_time</i>]</p>
描述	<p>RIP 路由模式下进行配置。</p> <p><i>update_time</i>: 路由更新时间，以秒计。定义了设备发送路由更新报文的周期，每接收到更新报文，<i>invalid_time</i>和<i>flush_time</i>时钟就复位。缺省每隔30秒发送一次路由更新报文。</p> <p><i>invalid_time</i>: 路由无效时间，以秒计，从最近一次有效更新报文开始计时。定义了路由表中路由因没有更新而变为无效的时间。路由无效时间至少应该为路由更新时间的三倍，如果在路由无效时间内没有接收到任何更新报文，相应的路由将变为无效，进入invalid状态；<i>invalid_time</i>时间内接收到路由更新报文，时钟会复位。缺省时间为180秒。</p> <p><i>flush_time</i>: 路由清除时间，以秒计，从RIP路由进入invalid状态开始计时。<i>flush_time</i>时间到期，处于invalid状态路由将被清除出路由表。缺省时间为120秒。</p>

## 4.5. 配置案例



各接口所属的 VLAN 和 SVI 的 IP 地址如下所示：（所有路由设备以交换机为例）

A : GE 0/1 VLAN10 192.168.1.1/24

GE 0/2 VLAN20 192.168.2.1/24

B : GE 0/1 VLAN10 192.168.1.2/24

GE 0/2 VLAN20 192.168.3.1/24

C : GE 0/1 VLAN10 192.168.1.3/24

GE 0/2 VLAN20 192.168.4.1/24

图中 switch 为 2 层交换设备。

### ■ 配置路由设备 A

- 主 CLI：配置接口 VLAN，配置对应 SVI 的 IP 地址。

```
SWITCH(config)#vlan 10,20
SWITCH(config)#interface gi 0/1
SWITCH(config-if)#switch access vlan 10
SWITCH(config-if)#exit
SWITCH(config)#interface gi 0/2
SWITCH(config-if)#switch access vlan 20
SWITCH(config-if)#exit
SWITCH(config)#int Vlan10
SWITCH(config-if)#ip address 192.168.1.1/24
SWITCH(config-if)#exit
SWITCH(config)#int Vlan20
SWITCH(config-if)#ip address 192.168.2.1/24
```

- FRR CLI：

- ✧ 启动 RIP。
- ✧ 关联本地网络（所有网段）。
- ✧ 配置 RIP 域边界（通过 passive-interface 完成）。

```
FRR#configure terminal
FRR(config)#router rip
FRR(config-router)#network 0.0.0.0/0
FRR(config-router)#passive-interface default
FRR(config-router)#no passive-interface Vlan10
```

#### ■ 配置路由设备 B

- 主 CLI：配置接口 VLAN，配置对应 SVI 的 IP 地址。（省略）
- FRR CLI：
  - ✧ 启动 RIP。
  - ✧ 关联本地网络（所有网段）。
  - ✧ 配置 RIP 域边界（通过 passive-interface 完成）。
  - ✧ 配置到达 172.10.10.0/24 的静态路由。
  - ✧ 重分布静态路由。

```
FRR#configure terminal
FRR(config)#ip route 172.10.10.0/24 192.168.4.2
FRR(config)#router rip
FRR(config-router)#network 0.0.0.0/0
FRR(config-router)#passive-interface default
FRR(config-router)#no passive-interface Vlan10
FRR(config-router)#redistribute static
```

#### ■ 配置路由设备 C

- 主 CLI：配置接口 VLAN，配置对应 SVI 的 IP 地址。（省略）
- FRR CLI（将采用一种新的配置方法，实际跟路由设备 A 的配置等效）
  - ✧ 启动 RIP。
  - ✧ 关联 192.168.1.0/24 网段。
  - ✧ 重分布直连路由。

```
FRR#configure terminal
FRR(config)#router rip
FRR(config-router)#network 192.168.1.0/24
FRR(config-router)#redistribute connect
```

#### ■ 配置效果

- 路由设备 A：（学习到 192.168.3.0/24，192.168.4.0/24 和 172.10.10.0/24）

```
FRR#show ip route rip
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR,
       > - selected route, * - FIB route
```

```
R>* 192.168.3.0/24 [120/2] via 192.168.1.2, Vlan10, 00:45:56
R>* 192.168.4.0/24 [120/2] via 192.168.1.3, Vlan10, 01:03:44
R>* 172.10.10.0/24 [120/2] via 192.168.1.2, Vlan10, 00:45:56
```

➤ 路由设备 B: (学习到 192.168.2.0/24, 192.168.4.0/24)

```
FRR#show ip route rip
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR,
       > - selected route, * - FIB route
```

```
R>* 192.168.2.0/24 [120/2] via 192.168.1.1, Vlan10, 00:42:13
R>* 192.168.4.0/24 [120/2] via 192.168.1.3, Vlan10, 01:03:44
```

➤ 路由设备 C: (学习到 192.168.2.0/24, 192.168.3.0/24 和 172.10.10.0/24)

```
FRR#show ip route rip
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR,
       > - selected route, * - FIB route
```

```
R>* 192.168.2.0/24 [120/2] via 192.168.1.1, Vlan10, 00:42:13
R>* 192.168.3.0/24 [120/2] via 192.168.1.2, Vlan10, 00:45:56
R>* 172.10.10.0/24 [120/2] via 192.168.1.2, Vlan10, 00:45:56
```

#### 4.6. 显示命令

■ 查看路由表信息

参见 2.5.2 “路由管理” 章节说明。

■ 查看 RIP 路由表

```
FRR# show ip rip
Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP
Sub-codes:
       (n) - normal, (s) - static, (d) - default, (r) - redistribute,
       (i) - interface
```

Network	Next Hop	Metric From	Tag Time
R(n) 5.5.5.0/24	192.168.2.1	8 192.168.2.1	0 02:37
S(r) 80.0.0.0/8	192.168.100.50	1 self	0
S(r) 80.1.1.0/24	192.168.100.50	1 self	0
R(n) 192.168.1.0/24	192.168.2.1	6 192.168.2.1	0 02:37



```
C(i) 192.168.2.0/24    0.0.0.0          1 self          0
C(r) 192.168.100.0/24 0.0.0.0          1 self          0
```

■ 查看 RIP 状态

```
FRR# show ip rip status
```

```
Routing Protocol is "rip"
```

```
  Sending updates every 30 seconds with +/-50%, next due in 18 seconds
```

```
  Timeout after 180 seconds, garbage collect after 120 seconds
```

```
  Outgoing update filter list for all interface is not set
```

```
  Incoming update filter list for all interface is not set
```

```
  Default redistribution metric is 1
```

```
  Redistributing: connected static
```

```
  Default version control: send version 2, receive any version
```

```
    Interface      Send  Recv   Key-chain
```

```
    Vlan2           1 2   1 2
```

```
  Routing for Networks:
```

```
    192.168.2.0/24
```

```
  Routing Information Sources:
```

```
    Gateway          BadPackets BadRoutes  Distance Last Update
```

```
    192.168.2.1             0          0        120    00:00:20
```

```
  Distance: (default is 120)
```

## 5. 配置 IS-IS

### 5.1. 概述

IS-IS（Intermediate System-to-Intermediate System，中间系统到中间系统）是一种路由选择协议，适用于 IP 和 ISO CLNS 的双环境网络，是一种可扩展的、健壮的、易使用的 IGP（Interior Gateway Protocol，内部网关协议）协议。

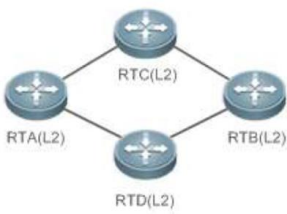
IS-IS 作为链路状态协议，具有链路状态协议的共通性。它通过发送 Hello 包来发现和维护邻居关系，通过向邻居发送协议数据报 LSP（Link State PDU，链路状态协议数据单元），来通告自身的链路状态。IS-IS 支持 2 层路由（Level-1 和 Level-2 路由）方案，同一层次中的所有设备有相同的 LSDB，LSDB 中存储着同一层次的所有设备产生的 LSP，从而同一层次的所有设备都知道自己所在层次的网络拓扑结构，每台设备使用 Dijkstra 最短路径优先（SPF）算法优化路由计算，路径选择并实现快速收敛。

### 5.2. 典型应用

典型应用	场景描述
平面拓扑	规模比较小的网络；大型网络建设初期，核心设备组成一个区域即采用平面拓扑。
分层拓扑	大型网络；链路经常震荡的网络。

#### 5.2.1. 平面拓扑

所有的设备不分区域，都在一个区域内，即为平面拓扑。

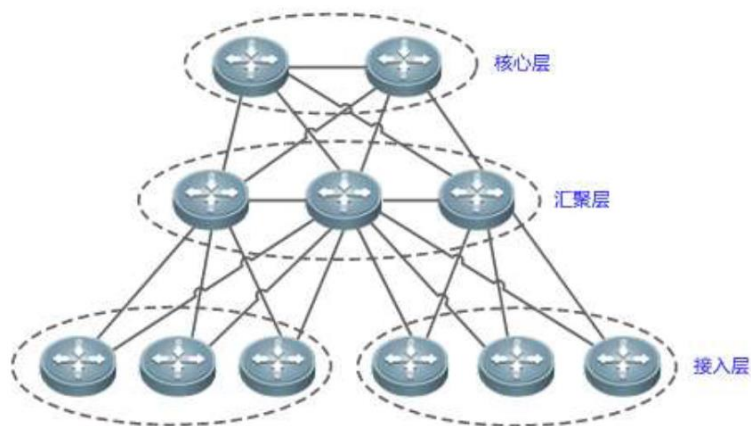


为了将来好扩展并减少设备负担，可以将设备设置为 Level-2。

#### 5.2.2. 分层拓扑

分层拓扑将网络分为核心层、汇聚层、接入层。

- 网络拓扑设计需要从核心层开始。所以核心层设备必须是连续相连的。
- 核心层的设备配置为 Level-2 设备。
- 汇聚层的设备配置为 Level-1-2 设备。
- 接入层的设备配置为 Level-1 设备。



### 5.3. 功能详解

IS-IS 是 ISO10589, RFC1195, RFC5308 描述的 IGP 路由协议。作为链路状态协议，与 RIP 这样的距离矢量协议相比，IS-IS 可以像 OSPF 一样提供可扩展的网络支持和更快的收敛时间。IS-IS 被广泛应用于 ISP 和运营商骨干网等大型网络。

#### 5.3.1. IS-IS 协议

##### ■ 术语

- **ES:** End system  
指非路由设备，比如主机。
- **IS:** Intermediate system  
指路由设备，是 IS-IS 协议中发送传播路由信息和生成路由的基本单元。
- **ES-IS:** End System to Intermediate System Routing Exchange Protocol  
端系统到中间系统，是 OSI 的 ES 和 IS 用来通信以动态发现第二层邻接关系的协议。
- **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，一个路由域可以划分为多个区域。
- **DIS:** Designated Intermedia System  
指定中间系统，类似 OSPF 的 DR，由它向 LAN 其他设备扩散 LSP；与 OSPF 不同的是，DIS 与其他设备建立邻居关系外其他设备之间也还建立着邻居关系。
- **CSNP:** complete serial number PDU  
完整序列号分组，在广播网上由 DIS 每十秒发送以同步链路状态。
- **PSNP:** partial sequence number PDU  
部分序列号分组，在点到点链路上发送用以确认 LSP，在广播网上的 PSNP，用来请求 LSP。
- **CLNP:** Connection Less Network Protocol

无连接网络协议，是网络层传输数据和错误消息的 OSI 协议，类似 IP 协议。

➤ **CLNS:** Connectionless Network Service

无连接网络服务是不可靠服务，不要求在传输数据前建立连接。

➤ **Hello**

该报文用于建立和维护邻居关系。

➤ **LSP:** Link-State PDU

链路状态 PDU，描述链路状态，类似 OSPF 的 LSA，不包含 TCP/IP 协议的信息。对不同类型路由有不同的 LSP，如 L1 LSP 和 L2 LSP。

➤ **NSEL:** Network-Selector

网络选择器有时也称 SEL，指定到哪一个网络层协议服务，类似 IP 协议上层服务的 TCP/UDP 端口，在 IS-IS 中常设 SEL 为 00 表示设备。

➤ **NSAP:** Network Service Access Point

网络服务访问点，是 CLNS 完整地址，包含 OSI 地址和高层进程，OSI 地址包含区域 ID、系统 ID 和 SEL，当 SEL 为 00 时即为 NET 网络实体，类似 IP 地址加协议号。

➤ **SNPA:** Subnetwork Point of Attachment

子网服务点，提供物理连接和网络层服务。它类似于 IP 中的 MAC 地址。

➤ **L1 路由设备**

指区域内路由设备，只接收其区域内的相关信息。要到达其他区域时，需要在 L1 路由设备保存一条到最近 L2 路由设备的默认路由。

➤ **L2 路由设备**

指区域与区域之间的骨干路由设备。L1 路由设备不能和 L2 路由设备直接相连。

➤ **L1/L2 路由设备**

用于连接 L1 路由设备和 L2 路由设备的边界路由设备，它包含有两个数据库即 L1 的和 L2 的。它类似 OSPF 中的 ABR。

➤ **Pseudonode**

伪节点，广播子网 LAN 的标识符，伪节点使得广播介质就像是一个虚拟设备，而每台路由设备就像是它的接口，由 DIS 管理路由设备和伪节点的关系。

➤ **NET 网络实体**

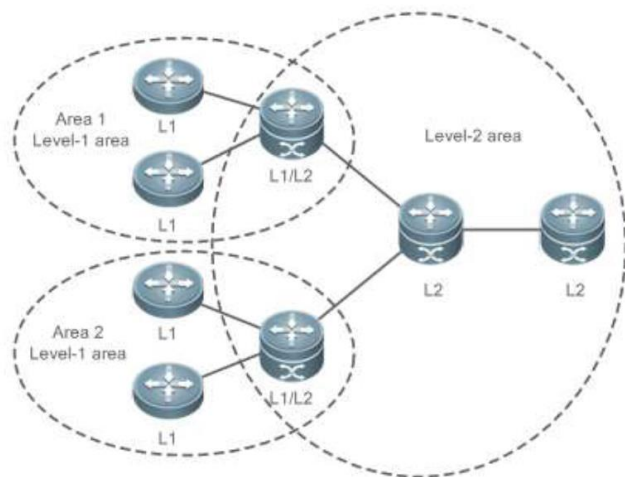
OSI 地址的一部分，描述了区域和系统 ID，但没定义 NSEL。

➤ **Circuit**

电路，在 IS-IS 中表示接口。NSAP 和 NET 代表整个设备，而电路代表接口。对于广播型网络比如 LAN 中，通常是结合 System ID 组成 7 字节长的电路 ID，比如 1921.6800.0001.01。

■ 层次结构

区域内的所有设备知道整个区域的网络拓扑结构，负责区域内的数据交换。Level-1-2 设备是不同区域的边界设备，提供区域连接。各个区域的边界设备组成骨干网，也属于 Level-2 层。Level-2 负责区域间的数据交换。Level-1 设备仅关心本区域拓扑结构，包括本区域所有节点和到达这些节点的下一跳设备。Level-1 设备通过 Level-2 设备访问其他区域，并且转发在区域外的目的网络的数据包到最近的 Level-2 设备。



可以基于 IS-IS 实例和端口配置 Level 类型。缺省情况的 Level 类型为 Level-1-2。

- 在接口模式使用 `isis circuit-type` 命令，可以改变接口的 Level 值。如果设置了 Level-1 或者 Level-2-only 的 `circuit-type`，则 IS-IS 只发送相应 Level 的 PDU。
- 在 IS-IS 路由模式使用 `is-type` 命令，指定 IS-IS 实例所运行的 Level。改变 `is-type` 将启动或者停止某 Level 的路由。缺省情况下，即新建一个 IS-IS 实例时，如果当前系统中不存在运行于 Level-2 的 IS-IS 实例（包括 Level-1-2），则新建实例的 `is-type` 为 Level-1-2 类型。如果已经存在运行于 Level-2 的 IS-IS 实例（包括 Level-1-2），则新建实例的 `is-type` 为 Level-1 类型。

#### ■ 地址编码方式

IS-IS 协议地址称为 NET，可分为三个部份：区域地址，System ID，NSAP 标识。总长度为 8-20 字节。



- 区域地址（区域 ID，Area ID）标识属于路由域中的哪个区域。长度为 1-13 字节。
- System ID（SysID）在自治系统中唯一。
- NSAP 标识（NSEL）为网络选择器，有时也称 SEL，在 IS-IS 中常设 SEL 为 00 表示设备。

缺省情况下，IS-IS 实例未设置 NET 地址。使用 `net` 命令设置 IS-IS 实例的 NET(Network Entry Title, 网络实体名称)地址。使用此命令为 IS-IS 设置它的 Area ID 和 System ID。

#### ■ 报文类型

IS-IS 三种报文类型：

##### ➤ 链路状态报文 LSP

用来在区域中传播链路状态记录。分为两种：Level 1 Link State PDU 和 Level 2 Link State PDU。LSP 只会泛洪到自己所属层次。

##### ➤ IS-IS Hello 报文 (IIH PDU)

用于维护邻接。Hello 包发送组播 MAC 地址，用来发现确定其它系统是否运行 IS-IS。

##### ➤ 序列号报文 SNP (包括 CSNP 和 PSNP)

CSNP 完全序列号报文用于 LSDB (链路状态数据库) 同步。在广播网中 DIS 默认每 10 秒发送一次 CSNP 报文，在点对点网络中 CSNP 报文只在邻居关系建立后发送一次。

PSNP 部份序列号报文同样用于 LSDB 同步。

#### ■ DIS 选举

DIS 将多重访问链路模拟成伪结点，负责生成伪节点的 LSP，伪节点和本网络中的所有设备建立联系，并且不允许它们之间直接联系。广播网络和 NBMA 网络 (非广播多点访问 Non-broadcast multiple access, 简称 NBMA) 在外部被看成一个伪节点，网络中的非 DIS 会向 DIS 报告自己的链路状态信息，而 DIS 则代表整个网络中所有的 IS 报告链路状态信息。选举 DIS 的原因与 OSPF 中选举 DR 的原因一样，其目的是为了减少不必要的邻接关系和路由信息的交换。

#### ■ IS-IS 邻居

两个路由设备能成功建立邻居关系的条件是：

- 两边接口地址在同一个网段。
- 两边接口 Level 匹配。
- 两边互相认证通过。
- 两边支持的协议一致。

### 5.3.2. IS-IS 路由管理

#### ■ 路由重分布

对于 IS-IS 来说，其他类型的路由 (比如直连路由、静态路由、其他路由协议的路由) 为外部路由。IS-IS 路由模式下使用 `redistribute` 命令，可以将外部路由 (**不包括缺省路由**) 重分布到 IS-IS，并通告给邻居。

使用 `redistribute` 命令带 `route-map` 参数，可以对引入的外部路由进行过滤或者修改参数信息。带 `metric` 参数可以对引入的外部路由修改 `metric` 值。

#### ■ 缺省路由

L1路由设备会生成缺省路由指向最近的L2路由设备。但L2路由设备不会自动生成缺省路由，在L2路由设备上，IS-IS路由模式下使用default-information originate 命令，在IS-IS路由域生成缺省路由，并通告到邻居（设备本身并不添加到路由表）。

■ metric 和 distance

metric值放在IP 可达信息的TLV中，它在SPF计算时被应用。越大的Metric值表示此接口的选路消耗越大，SPF计算其路径越长。

metric有三种style，不同的style取值范围不同。

- narrow：这是TLV的旧样式，对应取值范围0-63。
- transition：同时兼容TLV旧样式和TLV新样式，由于要支持旧样式，取值范围也是0-63。
- wide：这是TLV的新样式，对应取值范围0-16777215。

一个IS-IS实例刚建立的时候，metric-style为wide。但通过no操作时，是恢复到narrow。（metric-style通过IS-IS路由模式的metric-style命令设置）。

接口的metric值默认为10，通过接口模式下的isis metric命令可以修改metric值。

对于人为配置的IS-IS路由（缺省路由、重分布路由），缺省metric值为0。通过redistribute命令或者default-metric命令时带metric参数，可以修改引入IS-IS路由域路由的metric值。

IS-IS路由的distance值为115。不支持修改。

■ 认证

IS-IS 认证功能分为接口认证，区域认证和路由域认证。

接口认证在建立维护邻接关系中起作用。如果两台IS-IS设备配置了不同的接口认证密码，就无法建立邻居关系，这样可以避免未经授权或认证的IS-IS设备加入到需要认证的IS-IS 网络中。接口认证的密码被封装在Hello报文中进行发送。

区域认证和路由域认证用于验证LSP、CSNP、PSNP报文，以避免未经授权或认证的路由信息被注入到IS-IS设备的链路状态数据库当中。在发送时，其认证密码被封装在相应的LSP、CSNP、PSNP 报文中进行发送。

支持两种认证方式：明文认证和MD5加密认证。

5.4. 配置命令

5.4.1. 使能 IS-IS

■ 进入 IS-IS 路由模式

命令	<p><b>进入 IS-IS 路由模式，启动 IS-IS 路由实例（当 IS-IS 进程未激活，该命令同时激活 RIP 进程）</b></p> <pre>FRR(config)#router is-is tag FRR(config-router)#</pre> <p><b>关闭 IS-IS 路由实例</b><pre>FRR(config)#no router is-is tag</pre></p>
----	---

描述	<p>全局模式下进行配置。</p> <p>至少配置了一个 NET 地址之后，IS-IS 实例将运行起来。</p> <p><i>tag</i> 表示实例名称。当前系统只支持一个 IS-IS 实例，但是也必须通过 <i>tag</i> 指定实例名称。</p>
----	---

#### ■ 设置本地的 NET 地址

命令	<p><b>设置 NET 地址</b></p> <p>FRR(config-router)#<b>net</b> <i>net-address</i></p> <p><b>取消设置</b></p> <p>FRR(config-router)#<b>no net</b> <i>net-address</i></p>
描述	<p>IS-IS 路由模式下进行配置。</p> <p><i>net-address</i> 格式: <i>AREA_ID.YYYY.YYYY.YYYY.00</i>, <i>YYY.YYYY.YYYY</i> 为 System ID (6 个字节), <i>00</i> 对应 NSAP 标识 (NSEL), 为 <i>00</i> 表示设备。</p> <p><i>AREA_ID</i> 是变长的, 长度范围 1-13 字节。</p> <p>1 个字节时, 格式为: <i>XX</i></p> <p>13 个字节时, 格式为: <i>XX.XXXX.XXXX.XXXX.XXXX.XXXX.XXXX</i></p> <p>如果设置多个 NET 地址, System ID 必须相同。</p>

#### ■ 接口使能 IS-IS

命令	<p><b>设置接口使能</b></p> <p>FRR(config-if)#<b>ip router isis</b> <i>tag</i></p> <p><b>取消设置</b></p> <p>FRR(config-if)#<b>no ip router isis</b> <i>tag</i></p>
描述	<p>接口模式下进行配置。</p> <p><i>tag</i> 表示 IS-IS 实例名称。</p> <p>设置这条命令将此接口参与 IS-IS IPv4 路由协议。</p>

### 5.4.2. IS-IS 层次结构

#### ■ 配置 IS-IS 实例层次

命令	<p><b>配置 IS-IS 实例层次</b></p> <p>FRR(config-router)#<b>is-type</b> (<i>level-1</i>   <i>level-1-2</i>   <i>level-2-only</i>)</p> <p><b>取消配置</b></p> <p>FRR(config-router)#<b>no is-type</b> (<i>level-1</i>   <i>level-1-2</i>   <i>level-2-only</i>)</p>
描述	<p>IS-IS 路由模式下进行配置。</p> <p><i>level-1</i>: 指定 IS-IS 实例仅运行于 Level-1 层。</p> <p><i>level-1-2</i>: 指定 IS-IS 实例同时运行于 Level-1 和 Level-2 层。</p>



	<p>level-2-only: 指定 IS-IS 实例仅运行于 Level-2 层。</p> <p>改变 is-type 将启运或停止某 Level 的路由。</p>
--	--

#### ■ 配置接口电路类型

命令	<p><b>配置接口电路类型</b></p> <pre>FRR(config-if)#isis circuit-type (level-1   level-1-2   level-2-only)</pre> <p><b>取消配置</b></p> <pre>FRR(config-if)#no isis circuit-type (level-1   level-1-2   level-2-only)</pre>
描述	<p>接口模式下进行配置。</p> <p>level-1: 形成 Level-1 邻居。</p> <p>level-2-only: 形成 Level-2 邻居。</p> <p>level-1-2: 形成 Level-1-2 邻居。</p> <p>如果设置了 Level-1 或 Level-2-only 的 circuit-type, 则 IS-IS 只发送相应 Level 的 PDU。如果 is-type 被配置为 Level-1 或 Level-2-only, IS-IS 实例只会处理该 Level 下的事务, 也就是说对于该接口, 只会发送 is-type 与 circuit-type 相重合的 Level PDU。</p>

### 5.4.3. IS-IS 报文控制

#### ■ 配置接口 hello-interval

命令	<p><b>配置接口 hello-interval</b></p> <pre>FRR(config-if)#isis hello-interval interval (level-1   level-2  )</pre> <p><b>取消配置</b></p> <pre>FRR(config-if)#no isis hello-interval [interval (level-1   level-2  )]</pre>
描述	<p>接口模式下进行配置。</p> <p>interval: 发送 Hello 报文的间隔时间, 单位为秒, 取值范围 1-600, 缺省值 3。</p> <p>level-1: 应用于 Level-1 hello 报文。</p> <p>level-2: 应用于 Level-2 hello 报文。</p> <p>设置这条命令来改变 Hello 报文发送的间隔时间。</p> <p>默认情况下 IS-IS 接口的 Hello holdtime 的乘数 (即 hello-multiplier) 为 10, Hello 报文中的 holdtime 值等于该乘数与 hello-interval 的乘积, 即默认的 Hello holdtime 为 30 秒。若 hello-multiplier 配置为 4, 同时设置 isis hello-interval 5, 则 Hello holdtime 为 20 秒。</p> <p>未指定 level 表示两个 level 一起设置。</p>

#### ■ 配置接口 hello-multiplier

命令	<p><b>配置接口 hello-multiplier</b></p> <pre>FRR(config-if)#isis hello-multiplier multiplier-num (level-1   level-2  )</pre>
----	--

	<p><b>取消配置</b></p> <p>FRR(config-if)#no isis hello-multiplier [<i>multiplier-num</i> (level-1   level-2  )]</p>
描述	<p>接口模式下进行配置。</p> <p><i>multiplier-num</i>: 乘数值, 取值范围 2-100, 缺省值 10。</p> <p>level-1: 应用于 Level-1 hello 报文。</p> <p>level-2: 应用于 Level-2 hello 报文。</p> <p>Hello 报文中的 holdtime 值由 hello-interval 值乘以该乘数。</p> <p>未指定 level 表示两个 level 一起设置。</p>

■ 配置 LSP 间隔时间最小值

命令	<p><b>配置 LSP 间隔时间最小值</b></p> <p>FRR(config-router)#lsp-gen-interval (level-1   level-2  ) <i>interval</i></p> <p><b>取消配置</b></p> <p>FRR(config-router)#no lsp-gen-interval [(level-1   level-2  ) <i>interval</i>]</p>
描述	<p>IS-IS 路由模式下进行配置。</p> <p><i>interval</i>: 间隔值, 单位为秒, 取值范围 1-120, 缺省值 30。</p> <p>level-1: 应用于 Level-1 LSP 报文。</p> <p>level-2: 应用于 Level-2 LSP 报文。</p> <p>该参数表示新版本 LSP 生成时间与旧版本 LSP 生成时间的最小间隔。</p> <p>未指定 level 表示两个 level 一起设置。</p>

■ 配置 LSP 刷新闻隔

命令	<p><b>配置 LSP 刷新闻隔</b></p> <p>FRR(config-router)#lsp-refresh-interval (level-1   level-2  ) <i>interval</i></p> <p><b>取消配置</b></p> <p>FRR(config-router)#no lsp-refresh-interval [(level-1   level-2  ) <i>interval</i>]</p>
描述	<p>IS-IS 路由模式下进行配置。</p> <p><i>interval</i>: LSP 刷新闻隔值, 单位为秒, 取值范围 1-65235, 缺省值 900。</p> <p>level-1: 应用于 Level-1 LSP 报文。</p> <p>level-2: 应用于 Level-2 LSP 报文。</p> <p>为了保证各个网络节点都可以维护最新的LSP, 会周期性的将当前LSP全部重发一次, 此周期即LSP刷新闻隔。通过这样的机制, 可以使整个区域中的LSP能够保持最新同步。</p> <p>lsp-refresh-interval 必须小于 max-lsp-lifetime (LSP 有效时间)。</p> <p>未指定 level 表示两个 level 一起设置。</p>

## ■ 配置 LSP 有效时间

命令	<b>配置 LSP 有效时间</b> FRR(config-router)# <b>max-lsp-lifetime</b> (level-1   level-2  ) <i>value</i>  <b>取消配置</b> FRR(config-router)# <b>no max-lsp-lifetime</b> [(level-1   level-2  ) <i>value</i> ]
描述	<p>IS-IS 路由模式下进行配置。</p> <p><i>value</i>: LSP 生存时间的最大值。单位为秒，取值范围 1-65535，缺省值 1200。</p> <p>level-1: 应用于 Level-1 LSP 报文。</p> <p>level-2: 应用于 Level-2 LSP 报文。</p> <p>在LSP中有一个域值为LSP的有效时间，当设备生成系统的LSP时，会在此域中填写此LSP的最大有效时间。当此LSP被其它设备接收后，会随着时间的变化不断的减小，如果收到一个新的LSP，则旧的LSP会被替换掉，如果一直没有收到更新的LSP，而此LSP的有效时间减少到0后，还会在链路状态库中保存60秒，如果在60秒内还没收到更新的LSP，那么此LSP则会从LSDB中被删除。通过这样的机制可以使整个区域中的LSP能够保持最新同步。</p> <p>max-lsp-lifetime 必须大于 lsp-refresh-interval。</p>

## ■ 配置 LSP 报文大小

命令	<b>配置 LSP 报文大小</b> FRR(config-router)# <b>lsp-mtu</b> <i>MTU</i>  <b>取消配置</b> FRR(config-router)# <b>no lsp-mtu</b> [ <i>MTU</i> ]
描述	<p>IS-IS 路由模式下进行配置。</p> <p><i>MTU</i>: LSP 报文的最大字节数，取值范围为 128-4352，缺省值 1497。</p> <p>生成的 LSP 报文会收到 LSP MTU 的限制，通过该命令可以完成 LSP MTU 的修改。</p>

## ■ 配置接口 CSNP 间隔

命令	<b>配置接口 CSNP 间隔</b> FRR(config-if)# <b>isis csnp-interval</b> <i>interval</i> (level-1   level-2  )  <b>取消配置</b> FRR(config-if)# <b>no isis csnp-interval</b> [ <i>interval</i> (level-1   level-2  )]
描述	<p>接口模式下进行配置。</p> <p><i>interval</i>: CSNP 报文发送的间隔时间，以秒为单位，取值范围 1-600，缺省值 10。</p> <p>level-1: 应用于 Level-1 CSNP 报文。</p> <p>level-2: 应用于 Level-2 CSNP 报文。</p>

CSNP 报文是 DIS 在广播型网络上用来同步链路状态数据库而需要发送的报文，是一种周期性广播的报文。设置这条命令来改变 CSNP 报文发送的间隔时间。

#### ■ 配置接口 PSNP 间隔

命令	<p><b>配置接口 PSNP 间隔</b></p> <pre>FRR(config-if)# isis psnp-interval interval (level-1   level-2  )</pre> <p><b>取消配置</b></p> <pre>FRR(config-if)#no isis psnp-interval [interval (level-1   level-2  )]</pre>
描述	<p>接口模式下进行配置。</p> <p><i>interval</i>: PSNP 报文发送的间隔时间，以秒为单位，取值范围 1-120，缺省值 2。</p> <p>level-1: 应用于 Level-1 PSNP 报文。</p> <p>level-2: 应用于 Level-2 PSNP 报文。</p> <p>PSNP 报文在点到点链路上发送用以确认 LSP，在广播网上的 PSNP，用来请求 LSP。</p>

### 5.4.4. 路由重分布及缺省路由

#### ■ 路由重分布

命令	<p><b>配置路由重分布</b></p> <pre>FRR(config-router)#redistribute ipv4 (static connect kernel ospf rip bgp) (level-1   level-2) (metric metric   route-map RM_NAME   )</pre> <p><b>取消配置</b></p> <pre>FRR(config-router)#no redistribute ipv4 (static connect kernel ospf rip bgp)</pre>
描述	<p>IS-IS 路由模式下进行配置。</p> <p>通过该命令，将其他源头的路由导入 IS-IS 协议，并将这些外部路由通告给 IS-IS 邻居，路由信息将被放置到 LSP 的 IP External Reachability Information TLV 中。</p> <p>static: 静态路由。</p> <p>connect: 直连路由，开启 OSPF 的网段，会自动作为 connect 路由导入 OSPF 协议。</p> <p>kernel: 内核路由，如果主 CLI 有配置 CLI，在 FRR CLI 中会作为 kernel 路由。不建议两边同时配置路由。</p> <p>ospf: OSPF 协议的路由</p> <p>rip: RIP 协议的路由</p> <p>bgp: BGP 协议的路由</p> <p><b>metric metric</b>: 可选参数，设置外部路由的 metric，取值范围跟实例的 metric-style 有关，narrow 或者 transition 对应取值范围 0-63，wide 对应取值范围 0-16777215。若未指定该参数，metric 为 0。</p> <p><b>route-map RM_NAME</b>: 可选参数，关联路由图，对重分布的路由实施过滤或者参数修改。可以修改 metric 以及路由的 tag。</p>

## ■ 缺省路由

命令	<p><b>导入缺省路由</b></p> <pre>FRR(config-router)#default-information originate ipv4 (level-1   level-2) [always] (metric <i>metric</i>   route-map <i>RM_NAME</i>   )</pre> <p><b>取消配置</b></p> <pre>FRR(config-router)#no default-information originate ipv4 (level-1   level-2)</pre>
描述	<p>IS-IS 路由模式下进行配置。</p> <p>如果选择 <code>always</code> 参数，IS-IS 实例不管是否存在缺省路由，都会向邻居通告一条外部缺省路由。但是本地路由设备不会显示该缺省路由，要确认是否产生缺省路由，可以用 <code>show isis database detail</code> 观察 IS-IS 链路状态数据库。IS-IS 的邻居通过执行 <code>show ip route</code> 命令，可以看到是否存在缺省路由。</p> <p><b>metric <i>metric</i>:</b> 可选参数，用于指定外部缺省路由的 <code>metric</code>，取值范围跟实例的 <code>metric-style</code> 有关，<code>narrow</code> 或者 <code>transition</code> 对应取值范围 0-63，<code>wide</code> 对应取值范围 0-16777215。若未指定该参数，外部缺省路由的 <code>metric</code> 为 0。</p> <p><b>route-map <i>RM_NAME</i>:</b> 可选参数，关联路由图，对外部缺省路由实施过滤或者参数修改。可以修改 <code>metric</code> 以及路由的 <code>tag</code>。</p>

## 5.4.5. 认证功能

### ■ 接口认证

命令	<p><b>配置接口认证</b></p> <pre>FRR(config-if)#isis password (clear   md5) <i>AUTH_KEY</i></pre> <p><b>取消配置</b></p> <pre>FRR(config-if)#no isis password [ (clear   md5) <i>AUTH_KEY</i> ]</pre>
描述	<p>接口模式下进行配置。</p> <p>IS-IS 的认证模式与密钥配置相结合，当配置明文密钥时，认证模式切换到明文认证，配置 MD5 密钥时，认证模式切换到 MD5 认证。且两种密钥配置时非此即彼，不能同时存在。</p> <p>当删除配置时，表示接口认证关闭（无需认证）。删除时 <code>AUTH_KEY</code> 是可选参数。</p>

### ■ 区域认证

命令	<p><b>配置区域认证</b></p> <pre>FRR(config-router)#area-password (clear   md5) <i>AUTH_KEY</i></pre> <p><b>取消配置</b></p>
----	---

	FRR(config-router)#no area-password [ (clear   md5) AUTH_KEY ]
描述	<p>IS-IS 路由模式下进行配置。</p> <p>IS-IS 的认证模式与密钥配置相结合，当配置明文密钥时，认证模式切换到明文认证，配置 MD5 密钥时，认证模式切换到 MD5 认证。且两种密钥配置时非此即彼，不能同时存在。</p> <p>当删除配置时，表示区域认证关闭（无需认证）。删除时 AUTH_KEY 是可选参数。</p>

#### ■ 路由域认证

命令	<p><b>配置路由域认证</b></p> <p>FRR(config-router)#domain-password (clear   md5) AUTH_KEY</p> <p><b>取消配置</b></p> <p>FRR(config-router)#no domain-password [ (clear   md5) AUTH_KEY ]</p>
描述	<p>IS-IS 路由模式下进行配置。</p> <p>IS-IS 的认证模式与密钥配置相结合，当配置明文密钥时，认证模式切换到明文认证，配置 MD5 密钥时，认证模式切换到 MD5 认证。且两种密钥配置时非此即彼，不能同时存在。</p> <p>当删除配置时，表示路由域认证关闭（无需认证）。删除时 AUTH_KEY 是可选参数。</p>

### 5.4.6. 控制参数

#### ■ 配置实例的 metric-style

命令	<p><b>配置实例的 metric-style</b></p> <p>FRR(config-router)#metric-style ( narrow   transition   wide )</p> <p><b>取消配置</b></p> <p>FRR(config-router)#no metric-style</p>
描述	<p>IS-IS 路由模式下进行配置。</p> <p>metric有三种style，不同的style取值范围不同。</p> <p>narrow：这是TLV的旧样式，对应取值范围0-63。</p> <p>transition：同时兼容TLV旧样式和TLV新样式，由于要支持旧样式，取值范围也是0-63。</p> <p>wide：这是TLV的新样式，对应取值范围0-16777215。</p> <p>一个IS-IS实例刚建立的时候，metric-style为wide。但通过no操作时，是恢复到narrow。</p>

#### ■ 配置接口的 metric

命令	<b>配置接口的 metric</b> FRR(config-if)#isis metric <i>METRIC</i> (level-1   level-2   )  <b>取消配置</b> FRR(config-if)#no isis metric [ <i>METRIC</i> (level-1   level-2   )]
描述	接口模式下进行配置。  <i>METRIC</i> : 取值范围跟对应实例的 metric-style 有关。narrow 或者 transition 对应取值范围 0-63, wide 对应取值范围 0-16777215。默认值 10。  level-1: 表示应用于 Level-1 的路由。 level-2: 表示应用于 Level-2 的路由。 未选择 level: 表示同时应用于 Level-1 和 Level-2 的路由。

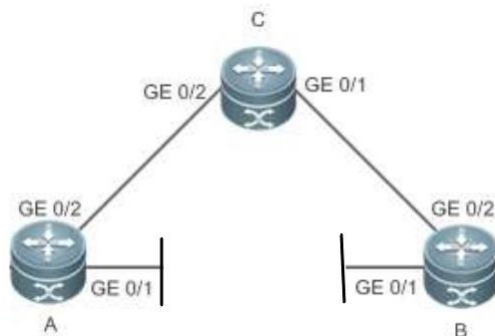
## ■ 配置设备优先级

命令	<b>配置设备优先级</b> FRR(config-if)#isis priority <i>PRIORITY</i> (level-1   level-2   )  <b>取消配置</b> FRR(config-if)#no isis priority [ <i>PRIORITY</i> (level-1   level-2   )]
描述	接口模式下进行配置。  配置此命令改变广播网络的Hello包中Priority value。低的Priority value比高的Priority value在DIS选举中优选度更低。  <i>PRIORITY</i> : 取值范围 0-127, 缺省值 64。  level-1: 表示优先级仅应用于 Level-1 的 DIS 选举。 level-2: 表示优先级仅应用于 Level-2 的 DIS 选举。 未选择 level: 表示优先级同时应用于 Level-1 和 Level-2 的 DIS 选举。

## ■ 配置被动接口

命令	<b>配置被动接口</b> FRR(config-if)#isis passive-interface  <b>取消配置</b> FRR(config-if)#no isis passive-interface
描述	接口模式下进行配置。  被动接口不参不 IS-IS 报文收发, 即不在被动接口上建立 IS-IS 邻居, 但该接口对应的 IP 地址将通过其他接口泛洪出去。

## 5.5. 配置案例



各接口所属的 VLAN 和 SVI 的 IP 地址如下所示：（所有路由设备以交换机为例）

A : GE 0/1 VLAN10 192.168.1.1/24

GE 0/2 VLAN20 192.168.2.1/24

B : GE 0/1 VLAN40 192.168.4.1/24

GE 0/2 VLAN30 192.168.3.1/24

C : GE 0/1 VLAN30 192.168.3.2/24

GE 0/2 VLAN20 192.168.2.2/24

A 和 B 为 Level-1，C 为 Level-2。

A-C 划分区域 00.0001，B-C 划分区域 00.0002。

A 的系统 ID 为 0000.0000.0001。

B 的系统 ID 为 0000.0000.0002。

C 的系统 ID 为 0000.0000.0003。

### ■ 配置路由设备 A

- 主 CLI：配置接口 VLAN，配置对应 SVI 的 IP 地址。

```

SWITCH(config)#vlan 10,20
SWITCH(config)#interface gi 0/1
SWITCH(config-if)#switch access vlan 10
SWITCH(config-if)#exit
SWITCH(config)#interface gi 0/2
SWITCH(config-if)#switch access vlan 20
SWITCH(config-if)#exit
SWITCH(config)#int Vlan10
SWITCH(config-if)#ip address 192.168.1.1/24
SWITCH(config-if)#exit
  
```



```
SWITCH(config)#int Vlan20
```

```
SWITCH(config-if)#ip address 192.168.2.1/24
```

➤ FRR CLI:

- ✧ 启动 IS-IS 实例 test。
- ✧ 设置实例 test 的 net。
- ✧ 设置 test 实例运行在 Level-1。
- ✧ 配置属于 test 实例的接口 Vlan20。
- ✧ 重分布直连路由。

```
FRR#configure terminal
```

```
FRR(config)#router isis test
```

```
FRR(config-router)#net 00.0001.0000.0000.0001.00
```

```
FRR(config-router)#is-type level-1
```

```
FRR(config-router)#redistribute ipv4 connected level-1 metric 44
```

```
FRR(config-router)#exit
```

```
FRR(config)#int Vlan20
```

```
FRR(config-if)#ip router isis test
```

■ 配置路由设备 B

➤ 主 CLI: 配置接口 VLAN, 配置对应 SVI 的 IP 地址。(省略)

➤ FRR CLI:

- ✧ 启动 IS-IS 实例 test。
- ✧ 设置实例 test 的 net。
- ✧ 设置 test 实例运行在 Level-1。
- ✧ 配置属于 test 实例的接口 Vlan30。
- ✧ 重分布直连路由。

```
FRR#configure terminal
```

```
FRR(config)#router isis test
```

```
FRR(config-router)#net 00.0002.0000.0000.0002.00
```

```
FRR(config-router)#is-type level-1
```

```
FRR(config-router)#redistribute ipv4 connected level-1 metric 33
```

```
FRR(config-router)#exit
```

```
FRR(config)#int Vlan30
```

```
FRR(config-if)#ip router isis test
```

■ 配置路由设备 C

➤ 主 CLI: 配置接口 VLAN, 配置对应 SVI 的 IP 地址。(省略)

➤ FRR CLI:

- ✧ 启动 IS-IS 实例 test。
- ✧ 设置实例 test 的两个 net。
- ✧ 设置 test 实例运行在 Level-1-2。

✧ 配置属于 test 实例的接口 Vlan20 和 Vlan30。

```
FRR#configure terminal
FRR(config)#router isis test
FRR(config-router)#net 00.0001.0000.0000.0003.00
FRR(config-router)#net 00.0002.0000.0000.0003.00
FRR(config-router)#is-type level-1-2
FRR(config-router)#exit
FRR(config)#int Vlan20
FRR(config-if)#ip router isis test
FRR(config-if)#int Vlan30
FRR(config-if)#ip router isis test
```

## ■ 配置效果

- 路由设备 A: (学习到 192.168.3.0/24, 192.168.4.0/24)

```
FRR#show ip route isis
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR,
       > - selected route, * - FIB route
```

```
I>* 192.168.3.0/24 [115/20] via 192.168.2.2, Vlan20, 00:45:03
```

```
I>* 192.168.4.0/24 [115/53] via 192.168.2.2, Vlan20, 00:45:29
```

- 路由设备 B: (学习到 192.168.1.0/24, 192.168.2.0/24)

```
FRR#show ip route isis
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR,
       > - selected route, * - FIB route
```

```
I>* 192.168.1.0/24 [115/64] via 192.168.3.2, Vlan30, 00:45:27
```

```
I>* 192.168.2.0/24 [115/20] via 192.168.3.2, Vlan30, 00:45:05
```

- 路由设备 C: (学习到 192.168.1.0/24, 192.168.4.0/24)

```
FRR#show ip route isis
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR,
       > - selected route, * - FIB route
```

```
I>* 192.168.1.0/24 [120/54] via 192.168.2.1, Vlan20, 00:45:05
```

```
I>* 192.168.4.0/24 [120/43] via 192.168.3.1, Vlan30, 00:45:03
```

## 5.6. 显示命令

### ■ 查看路由表信息

参见 2.5.2 “路由管理” 章节说明。

### ■ 查看 IS-IS 邻居

```
FRR# show isis neighbor
```

```
Area 1:
```

System Id	Interface	L	State	Holdtime	SNPA
SWITCH	Vlan2	1	Up	30	0022.3300.0710
SWITCH	Vlan2	2	Up	30	0022.3300.0710

```
FRR# show isis neighbor 0000.0000.0001
```

```
Area 1:
```

```
SWITCH
```

```
Interface: Vlan2, Level: 1, State: Up, Expires in 29s
```

```
Adjacency flaps: 1, Last: 1d19h39m19s ago
```

```
Circuit type: L1L2, Speaks: IPv4
```

```
SNPA: 0022.3300.0710, LAN id: 0000.0000.0002.09
```

```
LAN Priority: 64, is not DIS, DIS flaps: 1, Last: 1d19h39m18s ago
```

```
Area Address(es):
```

```
00.0000
```

```
IPv4 Address(es):
```

```
192.168.2.1
```

```
SWITCH
```

```
Interface: Vlan2, Level: 2, State: Up, Expires in 29s
```

```
Adjacency flaps: 1, Last: 1d19h39m19s ago
```

```
Circuit type: L1L2, Speaks: IPv4
```

```
SNPA: 0022.3300.0710, LAN id: 0000.0000.0002.09
```

```
LAN Priority: 64, is not DIS, DIS flaps: 1, Last: 1d19h39m18s ago
```

```
Area Address(es):
```

```
00.0000
```

```
IPv4 Address(es):
```

```
192.168.2.1
```

```
FRR# show isis neighbor detail
```

```
Area 1:
```

```
SWITCH
```

```
Interface: Vlan2, Level: 1, State: Up, Expires in 30s
```

```
Adjacency flaps: 1, Last: 1d19h39m26s ago
```

```
Circuit type: L1L2, Speaks: IPv4
```

```
SNPA: 0022.3300.0710, LAN id: 0000.0000.0002.09
LAN Priority: 64, is not DIS, DIS flaps: 1, Last: 1d19h39m25s ago
Area Address(es):
    00.0000
IPv4 Address(es):
    192.168.2.1
```

```
SWITCH
Interface: Vlan2, Level: 2, State: Up, Expires in 30s
Adjacency flaps: 1, Last: 1d19h39m26s ago
Circuit type: L1L2, Speaks: IPv4
SNPA: 0022.3300.0710, LAN id: 0000.0000.0002.09
LAN Priority: 64, is not DIS, DIS flaps: 1, Last: 1d19h39m25s ago
Area Address(es):
    00.0000
IPv4 Address(es):
    192.168.2.1
```

■ 查看 IS-IS 接口信息

```
FRR# show isis interface
Area 1:
  Interface  CircId  State  Type  Level
  Vlan2      0x9    Up     lan   L1L2
FRR# show isis interface Vlan2
Area 1:
  Interface: Vlan2, State: Up, Active, Circuit Id: 0x9
  Type: lan, Level: L1L2, SNPA: 00aa.bb09.2616
  Level-1 Information:
    Metric: 10, Active neighbors: 1
    Hello interval: 3, Holddown count: 10 (pad)
    CNRP interval: 10, PSNP interval: 2
    LAN Priority: 64, is DIS
  Level-2 Information:
    Metric: 10, Active neighbors: 1
    Hello interval: 3, Holddown count: 10 (pad)
    CNRP interval: 10, PSNP interval: 2
    LAN Priority: 64, is DIS
  IP Prefix(es):
    192.168.2.2/24
  IPv6 Link-Locals:
    fe80::2aa:bbff:fe09:2616/64
```

```
FRR# show isis interface detail
```

Area 1:

Interface: Vlan2, State: Up, Active, Circuit Id: 0x9

Type: lan, Level: L1L2, SNPA: 00aa.bb09.2616

Level-1 Information:

Metric: 10, Active neighbors: 1

Hello interval: 3, Holddown count: 10 (pad)

CNSP interval: 10, PSNP interval: 2

LAN Priority: 64, is DIS

Level-2 Information:

Metric: 10, Active neighbors: 1

Hello interval: 3, Holddown count: 10 (pad)

CNSP interval: 10, PSNP interval: 2

LAN Priority: 64, is DIS

IP Prefix(es):

192.168.2.2/24

IPv6 Link-Locals:

fe80::2aa:bbff:fe09:2616/64

#### ■ 查看 IS-IS 概述信息

FRR# show isis summary

Process Id : 1

System Id : 0000.0000.0002

Up time : 2d22h55m ago

Number of areas : 1

Area 1:

Net: 00.0000.0000.0000.0002.00

Level-1:

SPF:

minimum interval : 1

IPv4 route computation:

last run elapsed : 00:04:10 ago

last run duration : 231 usec

run count : 667

IPv6 route computation:

last run elapsed : 3d17h51m ago

last run duration : 0 usec

run count : 0

Level-2:

SPF:

minimum interval : 1

IPv4 route computation:

last run elapsed : 00:04:23 ago

last run duration : 215 usec

```
run count      : 663
IPv6 route computation:
last run elapsed : 3d17h51m ago
last run duration : 0 usec
run count      : 0
```

■ 查看 IS-IS 数据库

```
FRR# show isis database
```

```
Area 1:
```

```
IS-IS Level-1 link-state database:
```

LSP ID		PduLen	SeqNumber	Chksum	Holdtime	ATT/P/OL
SWITCH.00-00		84	0x000000b9	0xd053	806	0/0/0
OLT.00-00	*	92	0x00000115	0x2a84	1016	0/0/0
OLT.09-00	*	51	0x000000b7	0xd636	887	0/0/0

```
3 LSPs
```

```
IS-IS Level-2 link-state database:
```

LSP ID		PduLen	SeqNumber	Chksum	Holdtime	ATT/P/OL
SWITCH. 00-00		79	0x000000b8	0x92b6	769	0/0/0
OLT. 00-00	*	76	0x00000113	0x5b51	935	0/0/0
OLT. 09-00	*	51	0x000000b7	0xd832	984	0/0/0

```
3 LSPs
```

```
FRR# show isis database SWITCH.00-00
```

```
Area 1:
```

```
IS-IS Level-1 link-state database:
```

LSP ID	PduLen	SeqNumber	Chksum	Holdtime	ATT/P/OL
SWITCH.00-00	84	0x000000b9	0xd053	803	0/0/0

```
IS-IS Level-2 link-state database:
```

LSP ID	PduLen	SeqNumber	Chksum	Holdtime	ATT/P/OL
SWITCH.00-00	79	0x000000b8	0x92b6	766	0/0/0

```
FRR# show isis database
```

```
<cr>
```

```
WORD    LSP ID
```

```
detail  Detailed information
```

```
FRR# show isis database detail
```

```
<cr>
```

```
WORD    LSP ID
```

```
FRR# show isis database detail
```

```
Area 1:
```

```
IS-IS Level-1 link-state database:
```

LSP ID	PduLen	SeqNumber	Chksum	Holdtime	ATT/P/OL
SWITCH.00-00	84	0x000000b9	0xd053	788	0/0/0

Protocols Supported: IPv4  
Area Address: 00.0000  
Hostname: SWITCH  
TE Router ID: 192.168.2.1  
Extended Reachability: 0000.0000.0002.09 (Metric: 10)  
IPv4 Interface Address: 192.168.2.1  
Extended IP Reachability: 192.168.2.0/24 (Metric: 10)  
Extended IP Reachability: 0.0.0.0/0 (Metric: 33)

OLT.00-00                   \*       92    0x00000115   0x2a84       998    0/0/0

Protocols Supported: IPv4  
Area Address: 00.0000  
Hostname: OLT  
TE Router ID: 192.168.100.50  
Extended Reachability: 0000.0000.0002.09 (Metric: 10)  
IPv4 Interface Address: 192.168.100.50  
Extended IP Reachability: 192.168.2.0/24 (Metric: 10)  
Extended IP Reachability: 192.168.2.0/24 (Metric: 66)  
Extended IP Reachability: 192.168.100.0/24 (Metric: 66)

OLT.09-00                   \*       51    0x000000b7   0xd636       869    0/0/0

Extended Reachability: 0000.0000.0002.00 (Metric: 0)  
Extended Reachability: 0000.0000.0001.00 (Metric: 0)

3 LSPs

IS-IS Level-2 link-state database:

LSP ID	PduLen	SeqNumber	Chksum	Holdtime	ATT/P/OL
SWITCH.00-00	79	0x000000b8	0x92b6	751	0/0/0

Protocols Supported: IPv4  
Area Address: 00.0000  
Hostname: SWITCH  
TE Router ID: 192.168.2.1  
Extended Reachability: 0000.0000.0002.09 (Metric: 10)  
IPv4 Interface Address: 192.168.2.1  
Extended IP Reachability: 192.168.2.0/24 (Metric: 10)

OLT.00-00                   \*       76    0x00000113   0x5b51       917    0/0/0

Protocols Supported: IPv4  
Area Address: 00.0000  
Hostname: OLT  
TE Router ID: 192.168.100.50

```
Extended Reachability: 0000.0000.0002.09 (Metric: 10)
```

```
IPv4 Interface Address: 192.168.100.50
```

```
Extended IP Reachability: 192.168.2.0/24 (Metric: 10)
```

```
OLT.09-00      *      51    0x000000b7  0xd832    966    0/0/0
```

```
Extended Reachability: 0000.0000.0002.00 (Metric: 0)
```

```
Extended Reachability: 0000.0000.0001.00 (Metric: 0)
```

```
3 LSPs
```

```
FRR# show isis database detail SWITCH.00-00
```

```
Area 1:
```

```
IS-IS Level-1 link-state database:
```

LSP ID	PduLen	SeqNumber	Chksum	Holdtime	ATT/P/OL
SWITCH.00-00	84	0x000000b9	0xd053	780	0/0/0

```
Protocols Supported: IPv4
```

```
Area Address: 00.0000
```

```
Hostname: SWITCH
```

```
TE Router ID: 192.168.2.1
```

```
Extended Reachability: 0000.0000.0002.09 (Metric: 10)
```

```
IPv4 Interface Address: 192.168.2.1
```

```
Extended IP Reachability: 192.168.2.0/24 (Metric: 10)
```

```
Extended IP Reachability: 0.0.0.0/0 (Metric: 33)
```

```
IS-IS Level-2 link-state database:
```

LSP ID	PduLen	SeqNumber	Chksum	Holdtime	ATT/P/OL
SWITCH.00-00	79	0x000000b8	0x92b6	743	0/0/0

```
Protocols Supported: IPv4
```

```
Area Address: 00.0000
```

```
Hostname: SWITCH
```

```
TE Router ID: 192.168.2.1
```

```
Extended Reachability: 0000.0000.0002.09 (Metric: 10)
```

```
IPv4 Interface Address: 192.168.2.1
```

```
Extended IP Reachability: 192.168.2.0/24 (Metric: 10)
```

## 5.7. 清除命令

### ■ 清除全部 IS-IS 邻居

```
clear isis neighbor
```

### ■ 基于 System ID 清除 IS-IS 邻居

```
clear isis neighbor SYS_ID
```





## 6. 配置 BGP

### 6.1. 概述

BGP (Border Gateway Protocol, 边界网关协议) 是一种不同 AS (Autonomous Systems, 自治系统) 的路由设备之间进行通信的外部网关协议 (Exterior Gateway Protocol, EGP), 其主要功能是在不同的 AS 之间交换网络可达信息, 并通过协议自身机制来消除路由环路。

BGP 使用 TCP 协议作为传输协议, 通过 TCP 协议的可靠传输机制保证 BGP 的传输可靠性。运行 BGP 协议的 Router (路由设备) 称为 BGP Speaker, 建立了 BGP 会话连接 (BGP Session) 的 BGP Speakers 之间被称作 BGP 对等体 (BGP Peers)。

BGP Speaker 之间建立对等体的模式有两种: IBGP (Internal BGP) 和 EBGP (External BGP)。

- IBGP 是指在相同 AS 内建立的 BGP 连接, 完成路由信息在本 AS 内的过渡。
- EBGP 是指在不同 AS 之间建立的 BGP 连接, 完成不同 AS 之间路由信息的交换。

### 6.2. 典型应用

典型应用	场景描述
AS 跨域路由通告	通过 BGP 协议实现跨 AS 域之间的路由通告。
AS 域内路由反射	在 AS 域搭建路由反射拓扑, 减少 BGP 连接数量。

#### 6.2.1. AS 跨域路由通告

在 AS 域之间, 通过 BGP 协议实现路由通告与维护。

以下图为例, R1 为 AS 65536 的网络边缘设备。R2、R3 为 AS 65537 的网络边缘设备。R4 为 AS 65538 的网络边缘设备。通过 BGP 协议将 AS 65536 的路由, 经过 AS 65537 后传递到 AS 65538。

- R1 与 R2 间建立 EBGP 邻居关系, 实现跨 AS 域路由通告。
- R2 与 R3 之间建立 IBGP 邻居关系, 实现 AS 域内路由通告。
- Internet 网络内部运行 OSPF 路由协议, 实现 R2 与 R3 之间网络可达。
- R3 与 R4 之间建立 EBGP 邻居关系, 实现跨 AS 域路由通告。

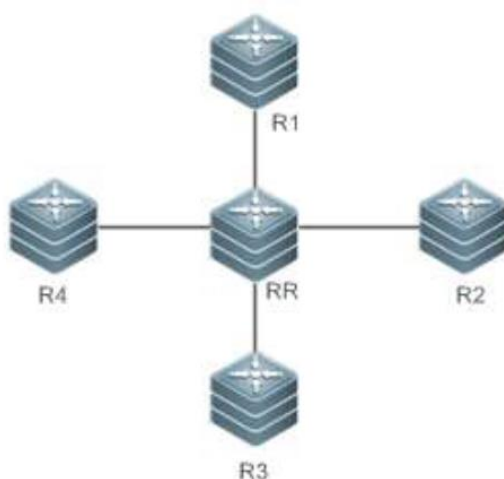


## 6.2.2. AS 域内路由反射

按 BGP 路由通告原则,缺省情况下 IBGP 邻居学习到的路由不会再通告给下一个 IBGP 邻居。因此在同一 AS 域内部,要求运行 BGP 协议的设备必须实现全连接(即 Full-Mesh)。当 AS 内部的 BGP 设备较多时,实现全连接会给网络部署带来较大困难,此时可以通过路由反射解决问题。

以下图为例,通过部署路由反射解决 R1~R4 及 RR 之间的 BGP 全连接问题。

- R1~R4 分别与 RR 建立 IBGP 邻居。
- RR 配置 R1~R4 为路由反射客户端。



## 6.3. 功能详解

BGP 的最新版本为 4。BGP-4 作为外部网关协议,是域间路由协议的事实标准。BGP-4 在 RFC 1771 提出,在 RFC 4271 更新。并在 RFC 2858 中向 BGP-4 添加了多协议支持。

一个 AS (Autonomous Systems, 自治系统) 是由一个或多个网络运营商运行的一个或多个 IP 前缀的连接组,它们具有相同且清晰的路由策略。每个 AS 都有一个与其关联的标识号,称为 ASN。ASN 由两个字节表示,范围从 1 到 65535。AS 号 64512 到 65535 被定义为专用 AS 号。专用 AS 号码不得在全球 Internet 上发布。ASN 是 BGP 的基本要素之一。

BGP 是一种距离矢量路由协议,利用 AS-Path 框架为 BGP 提供距离矢量度量和环路检测。

### 6.3.1. BGP 基本概念

- BGP 邻居 (BGP 对等体)

BGP 邻居由用户手动配置指定,建立连接关系的模式有两种: IBGP (Internal BGP) 和 EBG (External BGP)。通过 BGP Peer 所在的 AS 和本 BGP Speaker 所在的 AS 来判断 BGP Speakers 之间建立的是哪种连接模式。通常,建立 EBG 连接的 BGP Speakers 之间在物理上直接相连,而建立 IBGP 连接的 BGP Speakers 可以在 AS 内的任何地方。

BGP Speaker 会主动向用户指定的 BGP 对等体发起 TCP 连接请求，TCP 连接成功后将交互 BGP 协议报文协商连接参数，协商一致后 BGP 邻居关系就成功建立。

➤ 建立 TCP 连接

BGP Speaker 会主动向邻居发起 TCP 连接请求，目的 IP 就是用户指定的对等体 IP 地址，端口号固定为 179。BGP Speaker 同时会侦听本地 TCP 连接的 179 端口号，以接收来自对等体的连接请求。

➤ 协商各项协议参数

TCP 连接建立成功后，BGP Speaker 会互相交互 OPEN 报文，协商 BGP 连接参数。协商的参数主要包括：

- ✧ Version: BGP 协议版本号，目前仅支持 Version 4。
- ✧ 邻居 AS 号：确定邻居的 AS 号是否与本地指定的一致，不一致将拒绝建立连接。
- ✧ Holdtime: 协商 BGP 连接超时的时间间隔，缺省值为 180 秒。
- ✧ 邻居能力：协商邻居支持的各种扩展能力，如地址族、路由动态刷新等。

➤ 维持邻居关系

BGP Speaker 之间周期性地发送 Keepalive 消息。如果 Holdtime 超时还没有收到该 BGP 邻居发出的新的 Keepalive 报文，则认为该邻居不可达，将断开邻居 TCP 连接，并尝试重新开启。BGP 发送 Keepalive 的时间间隔为协商后的 Holdtime 的三分之一，缺省为 60 秒。

■ 对等体组

对等组用于通过为对等组的所有成员生成相同的更新信息来帮助改善扩展性。请注意，这意味着对等体组的成员生成的路由将被发送回该原始对等体，且其原始发件人标识符属性设置为指示原始对等体。未与特定对等体组关联的所有对等体均被视为属于默认对等体组，并将共享更新。

■ 路由反射器

根据 BGP 路由通告原则，要求一个 AS 内的所有 BGP Speaker 将建立全连接关系 (BGP Speaker 两两建立邻接关系)。当 AS 内的 BGP Speaker 数量过多，将增加 BGP Speaker 的资源开销，同时也给网络管理员增加了配置任务的工作量和复杂度，降低了网络的扩张性能。路由反射器是一种减少自治系统内 IBGP 对等体连接数量的方法（另外一种方法是 AS 联盟）。

将一台 BGP Speaker 设置为路由反射器，其将本自治系统内的 IBGP 对等体分为两类：客户端和非客户端。在 AS 内实现路由反射器，其规则如下：

- 配置路由反射器，并指定其客户端，路由反射器和其客户端形成一个群。路由反射器和客户端之间将建立连接关系。一个群内路由反射器的客户端不应该同群外的其他 BGP Speakers 建立连接关系。

- 在 AS 内，非客户端的 IBGP 对等体之间建立完全连接关系，这里的非客户端的 IBGP 对等体包括以下几种情况：
  - ✧ 一个群内的多个路由反射器之间；
  - ✧ 群内的路由反射器和群外不参与路由反射器功能的 BGP Speaker (通常这些 BGP Speaker 不支持路由反射器功能)；
  - ✧ 群内的路由反射器和其他群的路由反射器之间。

路由反射器接收到一条路由的处理规则如下：

- 从 EBGp Speaker 接收到的路由更新，将发送给所有的客户端和非客户端；
- 从客户端接收到的路由更新，将发送到其他客户端和所有非客户端；
- 从 IBGP 非客户端接收到的路由更新，将发送给其所有客户端。

通常一个群只配置一个路由反射器，在这种情况下，可以使用路由反射器的 Router ID 标识这个群。为了增加冗余，用户可以在一个群内设置多个路由反射器，在这种情况下，用户必须配置群 ID，以便一个路由反射器可以识别来自于群内其他路由反射器的路由更新。通常群内的路由反射器的客户端之间并不需要建立连接关系，路由反射器将反射客户端之间的路由。但是，如果所有客户端之间都已经建立了连接关系，可以取消路由反射器反射客户端路由的功能。

## ■ AS 联盟

AS 联盟是另一种减少自治系统内 IBGP 对等体连接数量的方法。

将一个自治系统划分为多个子自治系统，并通过设置一个统一的联盟 ID (即联盟 AS 号) 将这些子自治系统组成一个联盟。对联盟外部来说，整个联盟仍然认为是一个 AS，且只有联盟的 AS 号对外可见。在联盟内部，子自治系统内部的 BGP Speakers 之间仍然建立完全 IBGP 对等体连接，子自治系统间的 BGP Speaker 之间建立 EBGp 连接。虽然在子自治系统的 BGP Speakers 之间建立的是 EBGp 还接，但交换信息时，对于 NEXT\_HOP、MED 以及 LOCAL\_PREF 等路径属性信息仍然保持不变。

### 6.3.2. BGP 信息交互

#### ■ 向 BGP 注入本地 AS 的网络信息

BGP 不能自动发现/学习可达网络，必须将本地 AS 的可达网络信息注入 BGP。而后，BGP 才能将这些信息发布给邻居。

有两种基本方式实现向 BGP 注入本地 AS 的网络信息。

- 手动静态配置：将指定范围内的可达网络信息注入 BGP。（配置路由聚合也可注入 BGP 路由）
 

路由成功注入到 BGP 的前提条件是，在核心路由表中存在这样一条路由，该路由可以是 IGP、直连路由或者静态路由。
- 配置路由重分布：将 IGP 协议的可达网络信息重分布以注入 BGP。IGP 协议可以是 OSPF，RIP 或者 IS-IS。

## ■ BGP 对等体间的路由交互

BGP 具有强大的路由管理功能，可以通过配置 BGP 对等体的路由交互策略，控制从该对等体接收的和向该对等体通告的路由。

### ➤ 设置对等体通告缺省路由

缺省情况下，BGP 协议不通告缺省路由。通过 `neighbor xxx default-originate` 命令向指定对等体通告缺省路由。

### ➤ 设置对等体 Next-Hop-Self

缺省情况下，BGP 向 IBGP 邻居通告路由时不改变路由下一跳，向 EBGP 邻居通告路由时下一跳设置为本 BGP Speaker。使用 `neighbor xxx next-hop-self` 命令配置朝指定 BGP 对等体分发路由时将路由信息的下一跳设置为本 BGP speaker。（主要针对 IBGP 邻居）。

### ➤ 设置对等体 Remove-Private-AS

缺省情况下，BGP 向对等体通告路由信息时不删除 AS-PATH 属性中的私有 AS。使用 `neighbor xxx remove-private-as` 命令配置朝 EBGP 对等体分发路由信息时删除 AS 路径属性中记录的私有 AS 号。该命令无法针对 IBGP 邻居配置。

### ➤ 设置对等体 Send-Community

缺省情况下，BGP 向对等体通告路由信息时不发送团体属性。使用 `neighbor xxx send-community` 命令配置允许朝指定 BGP 对等体发送团体属性。

### ➤ 设置对等体 Maximum-Prefix

缺省情况下，BGP 未限制从对等体接收的路由信息条目。使用 `neighbor xxx maximum-prefix` 命令限制从指定 BGP 对等体接收的路由信息的条目。

### ➤ 配置 BGP 邻居路由过滤

缺省情况下，BGP 邻居未开启任何过滤策略，将接收邻居通告的所有合法路由信息。BGP 支持多种方式配置邻居的路由过滤策略：

- ✧ `neighbor xxx distribute-list (acl_id|acl_name) (in|out)` 通过 ACL 实现邻居入方向/出方向的路由过滤。
- ✧ `neighbor xxx filter-list as_path_name (in|out)` 通过 AS-PATH 列表实现邻居入方向/出方向的路由过滤。
- ✧ `neighbor xxx prefix-list pl_name (in|out)` 通过地址前缀列表实现邻居入方向/出方向的路由过滤。
- ✧ `neighbor xxx route-map rm_name (in|out)` 通过 route-map 实现邻居入方向/出方向的路由过滤。
- ✧ `neighbor xxx unsuppress-map rm_name (in|out)` 配置朝指定对等体分发路由信息时，选择性的公告先前被 `aggregate-address` 命令抑制的路由信息（关联 route-map）。

## ■ 从 BGP 获取其他 AS 的网络信息

通过将 BGP 交换来的其他 AS 的路由信息下发到设备的路由表，使当前路由设备能够转发发往其他 AS 的报文。通过将 BGP 交换来的其他 AS 的路由信息注入到 IGP 中，本地 AS 的所有路由设备能够转发发往其他 AS 的报文。

### ➤ 核心路由表下发

缺省情况下，允许下发所有路由，而且不改变下发路由的路由属性。BGP 可以使用 table-map 来控制下发到核心路由表的路由信息（table-map 关联到 route-map）。如果匹配路由，则修改路由信息的属性，并下发路由；如果不匹配路由，或者匹配到 deny 表项，则不修改路由信息的属性，仍然下发路由。

### ➤ 注入 IGP

缺省情况下，IGP 协议未重分步 BGP 路由。使用 redistribute 命令将 BGP 路由重分布到 IGP（RIP\OSPF\ISIS）。

## ■ 软复位

只要路由策略(包括 neighbor distribute-list、neighbor route-map、neighbor prefix-list 和 neighbor filter-list)发生改变，必须提供有效的方法使得新的路由策略能够实施。传统的方法是先关闭再重新建立 BGP 连接。通过配置 BGP 的软复位，在不关闭 BGP 会话连接的情况下，就可使新的路由策略得以实施。

将影响输入路由信息的路由策略称为“输入路由策略”（如 In-route-map、In-dist-list 等），将影响输出路由信息的路由策略称为“输出路由策略”（如 Out-route-map、Out-dist-list 等）。

### ➤ 当输出路由策略发生发化时，BGP 软复位会将本 BGP Speaker 的所有路由信息重新向邻居通告。

通过命令 `clear ip bgp xxx [soft] out` 会触发本 BGP Speaker 将所有路由信息重新向邻居通告。

### ➤ 输入路由策略发生发化，其操作将比输出路由策略变化更复杂。这是因为输出路由策略是实施在本 BGP Speaker 的路由信息表上。而输入路由策略是实施在从 BGP Peer 接收来的路由信息上，出于节约内存考虑，本地 BGP Speaker 并不保留原始的从 BGP Peer 接收来的路由信息。如果确实修改了输入路由策略，并且邻居设备支持路由创新功能，可通过配置软复位向邻居发送路由刷新请求，邻居设备接收到请求后会重新通告所有路由信息；或者配置为指定的每个 BGP 对等体在本 BGP Speaker 上保存一份原始的路由信息，为随后修改输入路由策略提供原始路由信息依据。

通过命令 `neighbor xxx soft-reconfiguration inbound` 会保存对应邻居的原始路由信息（即未经过滤的）。

通过命令 `clear ip bgp xxx [soft] in` 可以触发输入路由策略发生变化时的路由更新：

- ✧ 对配置了 `neighbor soft-reconfiguration inbound` 的邻居，不再请求重新通告，根据本地保存的原始路由信息进行路由更新。
- ✧ 对未配置 `neighbor soft-reconfiguration inbound` 的邻居，向其发送路由刷新请求，由邻居设备重新通告所有路由信息。

*“路由刷新功能”支持在不保存原始路由信息的条件下，修改路由策略并能得到实施。本设备支持“路由刷新功能”。通过 `show ip bgp neighbors` 命令可以判断 BGP 的对等体是否支持路由刷新性能。如果支持，在输入路由策略发生变化时就无需执行 `neighbor soft-reconfiguration inbound` 命令。*

### 6.3.3. BGP 路径参数

#### ■ ASN

每个 AS 都有一个与其关联的标识号，称为 ASN（AS Number）。

正式的自治系统编号由互联网地址分派机构（IANA, Internet Assigned Numbers Authority）（该机构也负责分配互联网 IP 地址）成批地分配给各个区域互联网注册管理机构（RIR）。各地区的 RIR 则进一步再从 IANA 分配到的整批 ASN 里为一个实体分配一个 ASN。希望获得 ASN 的实体必须按其所属的地区中心规定的程序进行申请，在申请得到批准后会分配到一个 ASN。

到 2007 年为止，自治系统编号都是 16 位长的整数，这最多能被分配给 65536 个自治系统。自治系统编号被分成两个范围。第一个范围是公开的 ASN，从 1 到 64511，它们可在互联网上使用；第二个范围是被称为私有编号的从 64512 到 65535 的那些（专用 AS 号），它们仅能在一个组织自己的网络内使用，不得在全球 Internet 上发布。

从 2007 年初开始，各 RIR 已开始分配 32 位长度的 ASN。32 位的 ASN 除了直接用一个 10 进制数表示外，有时也通过如下形式来表示：<高 16 位数值的 10 进制形式>.<低 16 位数值 10 进制形式>。本设备的 ASN 支持 32 位长度。

ASN 是 BGP 的基本要素之一。在启动 BGP 进程时，通过 ASN 指定基于那个 ASN 来启动 BGP 进程（`router bgp ASN`）。BGP 协议与邻居建立连接时根据 ASN 是否相同来判断是 IBGP 还是 EBGP。

#### ■ 正则表达式

正则表达式是按照一定的模版来匹配字符串的公式。使用它来评估文本数据并返回一个真值或假值，也就是表达式能不能正确的描述该数据。在 BGP 路由的 AS-PATH 属性匹配时使用了正则表达式。

- 在 AS-PATH 列表中，列表表项使用正则表达式，AS-PATH 列表对 BGP 路由的 AS-PATH 属性进行匹配时，只要 AS-PATH 属性包含正则表达式定义的特征，即匹配中。
- 在 `show ip bgp regexp xxx` 时使用正则表达式，显示 AS-PATH 属性匹配指定正则表达式的 BGP 路由信息。

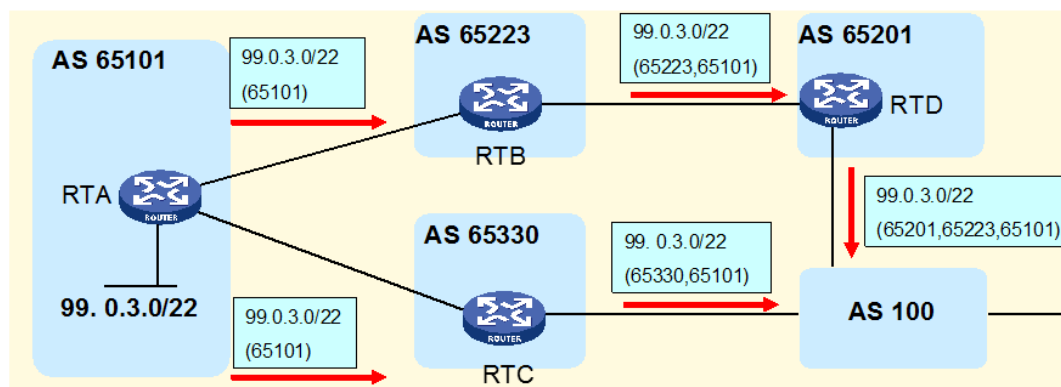
对扩展的 COMMUNITY 列表，也支持正则表达式。



字符	符号	含义
句号	.	匹配任意单字符
星号	*	匹配字符串中的零个或者任意序列， <b>不能放在最前面。</b>
加号	+	匹配字符串中的一个或者任意序列， <b>不能放在最前面。</b>
加字号	^	匹配字符串的开始
美元号	\$	匹配字符串的结束
下划线	_	匹配逗号，括号，字符串的开始和结束，空格
方括号	[]	匹配一定范围中的单个字符

#### ■ AS-PATH 属性

AS 路径（AS-PATH）属性为公认必遵属性，该属性域指示出该路由更新信息经过了哪些 AS 路径，AS\_PATH 属性按一定次序记录了某条路由从本地到目的地址所要经过的所有 ASN。当 BGP 将一条路由通告到其他 AS 时，便会把本地 ASN 添加在 AS-PATH 列表的最前面。收到此路由的 BGP 路由器根据 AS-PATH 属性就可以知道去目的地址所要经过的 AS。离本地 AS 最近的相邻 ASN 排在前面，其他 ASN 按顺序依次排列。



如上图所示，括号中的即为路由的 AS-PATH 属性。

AS-PATH 属性有三个作用：

- 保证 AS 之间无路由环路：通常情况下，BGP 不会接受 AS-PATH 中已包含本地 ASN 的路由，从而避免了形成路由环路的可能。如果 BGP 路由信息发布者从 EBG 对等体收到一条路由，它的 AS-PATH 包含发布者自己的 ASN，就说明这条路由曾经从本 AS 发出过，将其丢弃，同时不再进行转发。基于上述机制，AS-PATH 属性可以避免 AS 之间的路由环路的出现。
- 路由过滤：通过 AS-PATH 列表的正则表达式，对某个邻居（BGP 对等体）接收到或者发送到某个邻居的路由的 AS-PATH 属性进行匹配，若匹配中根据 AS-PATH 列表定义的行为处理，要么放行，要么过滤掉。具体参见下节“AS-PATH 列表”描述。

- 路由选择：如果到达同一个目的，接收到多条路由信息，其 AS-PATH 反应了到达目的需要经过的所有 AS，AS-PATH 中记录的 AS 的个数成为 AS 路径长度，AS 路径长度可以作为路由选择的其中一个因素。具体路由选择策略参见“路由的优先选择”描述。

AS-PATH 属性中支持 4 种类型的 AS 段（AS 集合）：

- AS-SET：无序 AS 集合，当使用路由聚合时，通过 as-set 参数指定，确定是否生成 AS-SET 段。在路由聚合时，若使用 summary-only 参数，则只发布聚合后的路由，汇聚前的原始路由则不发布。若未指定 as-set 参数，在接收到聚合路由的 BGP 对等体，将无法获知完整的 AS-PATH 属性，路径信息丢失（只保留进行路由聚合的设备所在的 AS 信息）。如果路由聚合时，指定 as-set 参数，对聚合的路由，AS-PATH 属性中会生成 AS-SET 段，将聚合前的所有路由的 AS-PATH 属性无序的组成一个新的 AS 集合。保证路径信息的完整性。（完整性可以用于防止环路，路由过滤）
- AS-SEQUENCE：有序 AS 集合。将路由发送给 IBGP 对等体时，AS-PATH 属性不进行修改（因为 AS 未变化），若发送给 EBGP 对等体时，操作如下：
  - ✧ 如果 AS\_PATH 的第一个路径段的类型为 AS\_SEQUENCE，则本地系统会将其自己的 ASN 作为序列的最后一个元素（由于是反序，实际上是最前面）。
  - ✧ 如果 AS\_PATH 的第一个路径段的类型为 AS\_SET，则本地系统会将 AS\_SEQUENCE 类型的新路径段添加到 AS\_PATH 中，包括该段中自己的 ASN。
  - ✧ 如果 AS\_PATH 为空，则本地系统将创建类型为 AS\_SEQUENCE 的路径段，将其自己的 AS 放入该段，然后将该段放入 AS\_PATH。
- AS-CONFED-SET：本地联盟中的无序 AS 集合，类似 AS-SET，差别只在于该 AS 段在本地联盟内部生成和使用。若向联盟外，则删除本联盟内部的 AS-CONFED-SET 和 AS-CONFED-SEQUENCE 段，只使用 AS-SEQUENCE，带有联盟的 ASN。
- AS-CONFED-SEQUENCE：本地联盟中的有序 AS 集合，类似 AS-SEQUENCE，差别只在于该 AS 段在本地联盟内部生成和使用。若向联盟外，则删除本联盟内部的 AS-CONFED-SET 和 AS-CONFED-SEQUENCE 段，只使用 AS-SEQUENCE，带有联盟的 ASN。

## ■ AS-PATH 列表

AS-PATH 列表表项使用正则表达式。BGP 路由的 AS-PATH 属性是一串字符串，判断 AS-PATH 属性是否匹配 AS-PATH 列表的表项时，即是字符串匹配操作。

AS-PATH 列表的表项顺序按照配置的先后顺序依次排列。匹配某 BGP 路由的 AS-PATH 属性时，表项按照先后顺序进行。匹配后的结果分为三种情况：匹配 deny 表项，匹配 permit 表项，未匹配。

- 在对邻居路由进行过滤时（neighbor xxx filter-list），匹配 deny 表项和未匹配的路由都将被过滤掉。匹配 permit 表项的路由被放行。因此，如果希望过滤掉某些路由的情况，在配置了过滤特征的 deny 表项后，最后应该配置一条 permit 所有的表项（特征为：.\*）。

```
ip as-path test deny _200$
```

```
ip as-path test permit .*
```

如上创建的 AS-PATH 列表 test 在应用到路由过滤时，表示过滤掉所有 AS 200 始发的路由。

- route-map 中使用 AS-PATH 列表设置 match 规则时，目的只是借助 AS-PATH 的匹配功能，因此，结果只看匹配中还是未匹配中，匹配 deny 表项当成是未匹配处理。匹配 permit 表项当成是匹配中处理。具体的处理行为依赖于 route-map 的模式和处理策略。因此，在 route-map 中应用 AS-PATH 列表时，AS-PATH 列表的 deny 表项主要用于跳过某些特定的子集，不希望进行处理。如下所示：

```
ip as-path test deny _200$
```

```
ip as-path test permit 200$
```

当该 AS-PATH 列表 test 应用于 route-map，然后 route-map 用于 BGP 路由过滤（neighbor xxx route-map）时。表示除了 AS 200 始发的路由，其他经过 AS 200 的路由全部被过滤掉。

## ■ COMMUNITY 属性

COMMUNITY 属性(团体属性)是能实施路由策略（路由过滤，优先选择等）的一种方式。定义团体属性的作用是为了方便实施基于团体的路由策略，从而简化在 BGP Speaker 上控制路由信息分发的配置。每个目的地可以属于多个团体，自治系统管理员可以定义一个目的地属于哪些团体。

团体属性是一个可选的传递属性，因此本地策略可以在不同的 AS 中传播。团体属性是一组团体值，每个团体值由 32 位表示。团体值用如下格式表示：

AS:VAL，AS 是高 16 位数值的 10 进制形式，可用于表示 ASN。VAL 是低 16 位数值的 10 进制形式，表示策略值。因此，AS 和 VAL 的取值范围均为 0-65535。比如 AS 7565 希望传递自己的本地策略值 80 给邻居，则可以使用团体值 7565:80。

有很多知名团体。下面介绍最常见的 4 个。

- Internet：表示 Internet 团体，所有的路由都属于该团体。团体值为 0。
- no-export：表示本路由不发布给 EBGp 对等体。团体值为 0xFFFFF01（65535:65281）。
- no-advertise：表示本路由不发布给任何一个 BGP 对等体。团体值为 0xFFFFF02（65535:65282）。
- local-as：表示本路由不发往 AS 外部，当配置联盟时，本路由不发布给其它的自治系统或者子自治系统。团体值为 0xFFFFF03（65535:65283）。

BGP 针对每一条路由最多支持 32 个团体值。在收到路由时，将会忽略重复的团体值，并按照数字大小对团体值进行重新排序。

BGP Speaker 可以在接收、发布或者重分发路由时，设置、添加或者修改团体属性值。在进行路由聚合时，聚合后的路由将包含所有被聚合的路由的团体值。

通过 `neighbor xxx send-community` 配置允许向指定 BGP 对等体发送团体属性，缺省未配置，不发送团体属性。

➤ 团体属性匹配：

根据 COMMUNITY 列表进行匹配，参见下节描述。COMMUNITY 列表通过 `route-map` 进行应用。通过 `match community-list`，使 `route-map` 通过 COMMUNITY 列表对路由的 COMMUNITY 属性进行匹配。

➤ 团体属性修改

通过 `route-map` 的 `set community` 和 `set community-list` 对团体属性进行设置和修改。

## ■ COMMUNITY 列表

COMMUNITY 列表是用户自定义的 COMMUNITY 属性列表。每个表项中可以包含若干个 COMMUNITY 值。COMMUNITY 值采用 `AS:VAL` 的格式表示。COMMUNITY 列表用于匹配 BGP 路由的 COMMUNITY 属性。只要 BGP 路由的 COMMUNITY 属性包含 COMMUNITY 列表的某个表项设置的 COMMUNITY 值，则认为匹配成功。

COMMUNITY 列表分为标准和扩展两种。标准的只能使用 COMMUNITY 值的显式值。而扩展的可以支持正则表达式。

COMMUNITY 列表标识方法有两种。ID 和 NAME。

➤ ID: 1-99 表示标准列表，100-500 表示扩展列表。

➤ NAME: 在配置列表时，若使用 NAME，则必须通过 “standard” 或者 “expanded” 关键字标识该列表是标准列表，还是扩展列表。

列表的表项行为分为 `permit` 和 `deny`。列表可以用于 `route-map` 进行匹配或者 COMMUNITY 属性设置。

➤ Route-map 匹配：结果只看匹配中还是未匹配中，匹配 `deny` 表项当成是未匹配处理。匹配 `permit` 表项当成是匹配中处理。具体的处理行为依赖于 `route-map` 的模式和处理策略。因此，在 `route-map` 中应用 COMMUNITY 列表时，列表的 `deny` 表项主要用于跳过某些特定的子集，不希望进行处理。如下所示：

```
ip community-list expanded test deny 8765:100
ip community-list expanded test permit 8765:*
```

当该 COMMUNITY 列表 `test` 应用于 `route-map`，然后 `route-map` 用于 BGP 路由过滤（`neighbor xxx route-map`）时。表示除了携带 8765:100 团体值的路由，其他携带有 ASN 为 8765 的团体值的路由全部过滤掉。

➤ Route-map 设置：根据 COMMUNITY 列表的匹配情况进行 COMMUNITY 属性值的删除。此时只能使用标准的 COMMUNITY 列表。

## ■ MED 属性

多出口比较器 MED (Multi-Exit Discriminators) 属性是一个可选非传递属性。自治系统使用本地优先级属性 (Local Preference) 来进行出自治系统路由的选择；而 MED 属性用于判断进入该自治系统的最佳路由，当一个运行 BGP 的自治系统得到目的地址相同、下一跳不同的多条路由时，在其它条件相同的情况下，MED 值较小的路由将被优先选作进入该自治系统的外部路由。在缺省情况下，自治系统的 MED 值为 0。BGP 的 MED 属性即对应 BGP 的 `metric` 参数，设置 `metric` 参数即修改 MED 属性值。通过 `route-map` 进行 `set metric METRIC` 即可设置对应路由的 MED 属性。

MED 属性用于路由选择时，有如下一些控制参数：

### ➤ `bgp bestpath med confed`

默认情况下，对联盟而言，只比较子 AS 内部各 EBGp 邻居路由的 MED 属性。通过 `bgp` 允许来自 `bestpath med confed` 允许联盟内部其他子 AS 的对等体的路由的 MED 值能进行比较

### ➤ `bgp bestpath med missing-as-worst`

将未设置 MED 属性的路由的优先级设置为最低，默认未设置此功能。

### ➤ `bgp always-compare-med`

一般情况下，只比较来自同一 AS 中各 EBGp 邻居路由的 MED 属性，不比较来自不同 AS 的 MED 值。若非得要比的话，可以通过 BGP 路由模式下的 `bgp always-compare-med` 命令来实现。不同自治系统的 MED 值定义不尽相同。因此，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命令。

### ➤ `bgp deterministic-med`

通过 BGP 路由模式下的 `bgp deterministic-med` 命令可以使得来自于同一个 AS 的同一个目的的多条不同路由优先进行 MED 属性比较。即同属于一个 AS 的路由优胜者再跟其他 AS 的同个目的的不同路由进行 MED 属性比较（在 `bgp always-compare-med` 开启的情况下）。

下面举例说明下 `bgp always-compare-med` 和 `bgp deterministic-med` 功能的效果。

网络 10.0.0.0/8 的以下路由：

entry1: AS (PATH) 500, med 150, external, rid 172.16.13.1

entry2: AS (PATH) 100, med 200, external, rid 1.1.1.1

entry3: AS (PATH) 500, med 100, internal, rid 172.16.8.4

BGP 路由收到的顺序是 entry3、entry2 和 entry1。（entry3 是 BGP 表中最旧的条目，entry1 是最新的条目。）

当 BGP 收到多个通往特定目标的路由时，它会按收到路由的相反顺序列出它们（从最新到最旧）。然后，BGP 按以下顺序成对比较路由：从最新的条目开始，并向最旧的条目移

动（从列表顶部开始，向下移动）。例如，将 entry1 与 entry2 进行比较。随后，将这两个中的较好者与 entry3 进行比较，依此类推。

➤ 两个命令都禁用

首先将 entry1 与 entry2 进行比较。因为 entry2 的路由器 ID 较小，所以它被选为这两个中的较好者。由于路径是来自不同的邻居自治系统，因此不检查 MED。下一步，将 entry2 与 entry3 进行比较。因为 entry2 是外部路径，所以它被选为最佳路径。

➤ bgp deterministic-med 禁用, bgp always-compare-med 启用

将 entry1 与 entry2 进行比较。这些条目来自不同的邻居自治系统，但由于启用了 bgp always-compare-med 命令，因此在比较中使用了 MED。在这两个条目中，entry1 的 MED 较小，因此它是较好者。下一步，将 entry1 与 entry3 进行比较。由于条目现在来自同一个自治系统，因此将再次检查 MED。entry3 被选为最佳路径。

➤ bgp deterministic-med 启用, bgp always-compare-med 禁用

当启用 bgp deterministic-med 命令时，来自同一个自治系统的路由将被分组到一起，然后比较每一组的最佳条目。BGP 表如下所示：

entry1: AS (PATH) 100, med 200, external, rid 1.1.1.1

entry2: AS (PATH) 500, med 100, internal, rid 172.16.8.4

entry3: AS (PATH) 500, med 150, external, rid 172.16.13.1

有一个 AS 100 组，还有一个 AS 500 组。比较每一组的最佳条目。entry1 是其组中的最佳条目，因为它是来自 AS 100 的唯一路由。entry2 是 AS 500 的最佳条目，因为它的 MED 最小。下一步，将 entry1 与 entry2 进行比较。因为这两个条目不是来自同一个邻居自治系统，所以比较中不考虑 MED。外部 BGP 路由要优于内部 BGP 路由，这使 entry1 成为最佳路由。

➤ 两个命令都启用

分组情况与上述第 3 种相同，但最后一次比较，在 entry2 与 entry1 之间，由于启用了 bgp always-compare-med 命令，因此最后一次比较时考虑了 MED。entry2 被选为最佳路径。

## ■ LOCAL\_PREF 属性

BGP Speaker 将从 EBGPeers 接收到的路由发送给 IBGP Peers 时添加本地优先级属性（LOCAL\_PREF）。BGP 使用 LOCAL\_PREF 作为从 IBGP Peers 学习到的路由进行优先级比较的依据之一，LOCAL\_PREF 值越大优先级越高。用户也可以通过 route-map 的 set local-preference 命令修改指定路由的本地优先级属性。

## ■ Origin 属性

BGP 路由的 Origin 属性记录了路由的来源类型。该属性作为路由进行优先级比较的依据之一，属性值越低，优先级越高。按照属性值由低到高（优先级由高到低）分为如下三类：

- IGP: 这里的 IGP 不是指真正的 IGP 协议（比如 OSPF），而是相对于来源于其他 BGP Speaker 而言的。当使用 network 配置的路由或者 aggregate-address 命令生成的路由，则为 IGP 类型。标识为 “i”。
- EGP: 从其他 BGP Speaker 学习到的路由，为 EGP 类型。标识为 “e”。
- Incomplete: 当使用 redistribute 命令重分布的其他路由协议（OSPF, RIP, IS-IS, Static, Connect）的路由，类型为 Incomplete。标识为 “?”

Origin 属性的标识在 show ip bgp 中每条路由的末尾会有显示。

## ■ 路由的优先选择

如下路由优选参数从上往下优先级从高到低。

- 本地优先级检查
 

优先选择 LOCAL\_PREF 属性值越大的路由。
- 本地路由检查
 

优先选择本 BGP speaker 生成的路由。主要有如下这些：

  - ✧ 静态路由（由 network 配置的路由）
  - ✧ 聚合路由（由 aggregate-address 命令配置生成的路由）
  - ✧ 重分布路由（由 redistribute 命令重分布的其他路由协议（OSPF, RIP, ISIS, Static, Connect）的路由）。
- AS-PATH 长度检查
 

优先选择 AS-PATH 长度最短的路由。如下命令可以对该检查进行相应控制：

  - ✧ bgp bestpath as-path confed: 在进行 AS-PATH 长度比较时，AS-CONFED-SETH 和 AS-CONFED-SEQUENCED 段的长度也纳入比较。缺省不纳入比较。
  - ✧ bgp bestpath as-path ignore: 允许 BGP 进行优先选择时不考虑比较 AS-PATH 长度，缺省会比较 AS-PATH 长度。
  - ✧ bgp bestpath as-path multipath-relax: 允许具有相同 AS-PATH 长度的不同路由做负载分担（由于本设备暂不支持 ECMP/WCMP，所以该配置不能配置），缺省情况下 AS-PATH 长度相同会继续比较其他属性。
- Origin 属性检查
 

优先选择 IGP，其次选择 EGP，其次选择 Incomplete。
- MED 检查
 

优先选择 MED 值最小的路由。MED 检查默认只检查同个 AS 的路由，即如果从同一 AS 接收到多条带有 MED 的路由，则首选 MED 值最低的路由。MED 检查有如下控制参数：

  - ✧ bgp bestpath med confed: 允许联盟内部不同子 AS 的路由的进行 MED 检查。
  - ✧ bgp bestpath med missing-as-worst: 未设置 MED 属性的路由，优先级最低。
  - ✧ bgp always-compare-med: 允许来自不同 AS 的路由也进行 MED 检查。
  - ✧ bgp deterministic-med: 优先比较来自于同个 AS 的路由。

✧ 关于 MED 检查控制参数更详细的描述，参见上文“MED 属性”相关描述。

➤ 外部检查

EBGP 路由优先级高于 IBGP 路由和 AS 联盟内的路由，IBGP 路由和 AS 联盟内的路由的优先级同样高。

➤ IGP metric(cost) 检查

针对 IGP 类型的路由，优先选择 metric 值更小的路由。

➤ 已经选择的外部检查

如果从 EBGP 对等体收到两条路由，则首选已选择的路由。该检查可以防止某些情况的振荡。

➤ 路由器 ID 检查

默认不进行 Router ID 检查，通过 `bgp bestpath compare-routerid` 开启 Router ID 检查，优先选择具有最低 Router ID 的路由。如果路由通过 IBGP 反射且具 ORIGINATOR ID 属性，则使用 ORIGINATOR ID 进行比较，否则使用从其接收路由的对等体的 Route ID 进行比较。

➤ 群列表长度检查

这里的群指路由反射器和它的客户端组成的集群。而群列表指路由所选择的 IBGP 反射路径。所以群列表长度实际上是一个路径长度。

优先选择群列表长度最短的路由。

➤ 邻居检查

优先选择邻居（对等体）地址大的路由。该检查必定可以决出胜负。

### 6.3.4. BGP 路由管理

#### ■ 路由聚合

BGP 支持 CIDR，所以允许创建聚合表项，将一条或者多条精细的 BGP 路由，聚合成一条网络掩码长度较短的 BGP 路由。以减小 BGP 路由表的大小。只有当聚合范围内存在有效的路由时，才将 BGP 聚合表项添加到 BGP 路由表中。

➤ `as-set` 参数：保留聚合地址范围内路由的 AS-PATH 信息，缺省情况下 BGP 不保留 AS-PATH 信息。

➤ `summary-only` 参数：缺省情况下路由聚合后，既会向邻居通告聚合后的路由，也会通告聚合范围内的路由。配置该参数，表示只通告聚合后的路由。

#### ■ 路由衰减

路由在被认为有效和无效之间来回变化时，称为路由振荡。路由振荡常引起不稳定的路由在网络中传播，从而导致网络的不稳定性。BGP 路由衰减是一种减少路由振荡的方法，通过监控来自 EBGP Peer 的路由信息来减少可能的路由振荡。

BGP 的路由衰减使用如下术语：

➤ 路由振荡：Route Flap，路由在有效和无效之间来回变化。



- 惩罚值: Penalty, 每一次路由振荡, 启动路由衰减的 BGP Speaker 为该路由增加一次惩罚值, 该值累计直到超过抑制上限。
- 抑制上限: Suppress Limit, 当路由的惩罚值超过该值时, 路由被抑制。默认为 2000, 取值范围为 1-20000。可修改。
- 半衰期: Half-life-time, 惩罚值减为一半的所经过的时间。默认为 15, 单位为分钟, 取值范围为 1-45。可修改。
- 重新启用值: Reuse Limit, 当路由的惩罚值低于该值时, 路由抑制解除。默认为 750, 取值范围为 1-20000。可修改。
- 最大抑制时间: Max-suppress-time, 路由能被抑制的最长时间。默认为  $4 * \text{Half-life-time}$ 。单位为分钟, 取值范围为 1-255。可修改。

对每一次路由振荡, BGP Speaker 对该路由进行一次惩罚(累加到惩罚值中), 当惩罚值达到抑制上限, 路由将被抑制。在半衰期到达时, 惩罚值减为一半, 当惩罚值减到重新启用值时, 路由重新被激活。路由被抑制的最长时限为最大抑制时间。

路由衰减默认关闭, 若要启动, 需要基于 BGP Speaker 全局开启。

#### ■ MD5 认证

在 EBGp 和 IBGP 邻居之间, 可以通过 MD5 进行加密认证。

通过 `neighbor xxx password key-string` 命令设置邻居间的加密密码。

特别需要注意的是, 邻居两端配置的密码必须完全相同, 否则无法通信。

#### ■ Local AS

BGP 的 Local AS 功能用于针对某个特定对等体配置不同于 BGP 真实 AS (router bgp AS) 的本地 AS, 类似于在对等体设备之间虚拟一个新的 AS, 使得当本地 BGP 真实 AS 发生变化时, 不需要改变对等体设备的 BGP 配置, 即可实现 BGP 连接的建立。该功能主要用于大型网络的 AS 迁移, 合并, 可以保证不影响其他互联 AS 中设备的配置。

BGP 协议中本地设备与对等体建立 BGP 连接时会将本地的 AS 号通过 Open 消息通告给对等体设备, 对等体设备会检查连接对端通告的 BGP AS 是否与本地配置的对等体 AS (Remote AS) 相同, 若不相同则会拒绝该 BGP 连接。默认情况下 BGP 连接中的本地 AS 为 BGP 的真实 AS, 而通过为该对等体配置 Local AS, 使得本地设备在与对等体建立 BGP 连接时会使用配置的 Local AS 来替代真实 AS, 建立 BGP 连接。

BGP Local AS 功能只适用于 EBGp 对等体, 即不能对 IBGP 对等体、联盟 EBGp 对等体配置 Local AS。此外, BGP Local AS 功能还存在如下限制:

- 配置的 Local AS 不能与对等体的 Remote AS 相同。
- Local AS 不能单独针对对等体组中的某个成员配置。
- 配置的 Local AS 不能与本地 BGP 真实 AS 相同。
- 若设备为某个联盟 AS 中的成员, 则 Local AS 不应与联盟 AS 号相同。

#### ■ 管理距离

管理距离用于评价各种路由来源的可信度。管理距离越小，则路由越优。（这里的路由优先指的是本地路由表针对各种不同路由协议来源的路由进行优选）。

管理距离表示一个路由信息源的可信度，其范围是从 1~255，管理距离的值越大，其可信度越低。BGP 对所学习到的路由信息的不同来源设定不同的管理距离，分为 External-distance、Internal-distance 和 Local-distance 三类：

- External-distance：从 EBGPeers 学习到路由的管理距离。默认管理距离为 20。
- Internal-distance：从 IBGP Peers 学习到路由的管理距离。默认管理距离为 200。
- Local-distance：后门路由的管理距离。默认管理距离为 200。

如果希望 IGP 的某一条路由优选，而不要使用 EBGPeers 的这一条路由信息，可以将这条路由设置为后门路由。缺省情况下，从建立 EBGPeers 连接的 BGP Speaker 学习到的路由的管理距离为 20。network xxx backdoor 将这些网络信息的管理距离设置为 200，从而使得从 IGP 学习到的相同的网络信息拥有更高的优先级。从 IGP 学习到的这些网络被认为是后门网络，并不公告出去。

不推荐改变 BGP 的管理距离。如果确实存在需要，请注意：

- External-distance 应当比其他 IGP 路由协议 (OSPF, RIP, ISIS, Static 等) 的管理距离更低；
- Internal-distance 和 Local-distance 应当比其他 IGP 路由协议的管理距离更高。

## ■ 定时器

用户可以手动配置 BGP 协议内部的各种定时器，以灵活应对不同网络环境下的邻居保活和路由管理需求。

### ➤ BGP 邻居保活定时器

BGP 使用 Keepalive 定时器来维持和对等体的有效连接，使用 Holdtime 定时器来判断对等体是否有效。缺省情况下，Keepalive 定时器的值为 60 秒，Holdtime 定时器的值为 180 秒。当 BGP Speakers 之间建立 BGP 连接时，双方将对 Holdtime 进行协商，值更小的 Holdtime 将被选择，而 Keepalive 定时器值的将选择协商后的 Holdtime 的 1/3 和配置的 Keepalive 的值的较小者。

邻居保活定时器可以基于全局（针对所有 BGP 对等体）配置，也可以基于某个指定的 BGP 对等体配置。

### ➤ 邻居重连定时器

为降低 BGP 频繁尝试与连接失败的邻居进行重连对网络带宽的影响，BGP Speaker 检测到与邻居建立连接失败之后，将在 connect-retry 定时器到期之后再尝试进行重连。缺省情况下，connect-retry 定时器的值为 15s。

### ➤ 路由通告定时器

为减少路由更新报文对网络带宽的影响，BGP Speaker 在检测到网络拓扑发生变化后，并不立即将路由更新通告给邻居。而是采用定时更新的机制，将所有发生变化的路由信息一起通告给邻居设备。

## 6.4. 配置命令

### 6.4.1. 定义对等体

#### ■ 进入 BGP 路由模式

命令	<p><b>进入 BGP 路由模式，启动 BGP 路由实例（当 BGP 进程未激活，该命令同时激活 BGP 进程）</b></p> <pre>FRR(config)#router bgp [ASN] FRR(config-router)#</pre> <p><b>使 BGP 进程处于未激活状态</b></p> <pre>FRR(config)#no router bgp [ASN]</pre>
描述	<p>全局模式下进行配置。</p> <p>ASN 表示自治系统号。<b>当前系统不支持多实例。</b></p> <p>当 BGP 进程未激活时，ASN 参数是必选的。当 BGP 进程已经激活时，ASN 参数可选。</p>

#### ■ 配置 BGP 的 Router ID

命令	<p><b>配置 BGP 的 Router ID</b></p> <pre>FRR(config-router)#bgp router-id A.B.C.D</pre> <p><b>取消 BGP 的 Router ID 配置</b></p> <pre>FRR(config-router)#no bgp router-id [A.B.C.D]</pre>
描述	<p>BGP 路由模式下进行配置。</p> <p>该配置为可选配置，但建议设置 router-id，避免 router-id 在设备复位后变化。router-id 作为协议交互时的设备 ID。其选择按照如下优先级从高到低：</p> <ol style="list-style-type: none"> <li>1) BGP 设置的 router-id；</li> <li>2) 全局设置的 router-id；</li> <li>3) 某个三层口的 ip 地址。</li> </ol> <p>当 BGP 进程激活时，选择好 router-id，即使更高优先级的 router-id 设置，也不会进行切换，如下操作可以触发切换：</p> <ol style="list-style-type: none"> <li>4) no router bgp，再 router bgp ASN，触发 BGP 进程重新激活。</li> <li>5) 保存配置，重启设备。</li> </ol> <p>因此，当没有显式设置 router-id 的时候，不能保证每次启机 router-id 相同。</p>

#### ■ 创建 BGP 邻居

命令	<p><b>配置 BGP 邻居</b></p> <pre>FRR(config-router)#neighbor PEER remote-as (ASN internal external)</pre>
----	---

	<b>删除 BGP 邻居</b> FRR(config-router)#no neighbor <i>PEER</i> remote-as ( <i>ASN</i>  internal external)
描述	<p>BGP 路由模式下, 或者 BGP 的 IPV4 单播地址簇模式下进行配置。</p> <p>PEER 表示对等体。可以是 IP 地址, 或者是对等体组的名称。</p> <p>ASN: 远端对等体的 ASN, 范围为 1~4294967295。如果配置的值与远端对等体 ASN 不同, 则连接请求会被拒绝。使用此种方式建立的对等体属于 IBGP 还是 EBGP 自动判断。对等体 ASN 与本地 ASN 相同则为 IBGP 对等体, 如果不同则为 EBGP 对等体。</p> <p>internal: 如果远端对等体的 ASN 与本地的 ASN 不同, 则连接请求会被拒绝, 否则建立 IBGP 邻居。</p> <p>External: 如果远端对等体的 ASN 与本地的 ASN 相同, 则连接请求会被拒绝, 否则建立 EBGP 邻居。</p>

#### ■ 配置 BGP 邻居的源接口

命令	<b>配置 BGP 邻居的源接口</b> FRR(config-router)#neighbor <i>PEER</i> update-source <i>SOURCE</i>  <b>删除 BGP 邻居的源接口配置</b> FRR(config-router)#no neighbor <i>PEER</i> update-source ( <i>SOURCE</i>   )
描述	<p>BGP 路由模式下进行配置。</p> <p>PEER 表示对等体。可以是 IP 地址或者对等体组的名称。</p> <p>SOURCE 可以是本地有效的 IP 地址或者三层接口名称。</p> <p>源接口表示与邻居建立连接是通过这个接口完成的。如果未配置源接口, 会根据邻居 IP 地址查询路由得到源接口。</p>

#### ■ 定义对等体组

命令	<b>创建对等体组</b> FRR(config-router)#neighbor <i>PEER_GROUP_NAME</i> peer-group  <b>删除对等体组</b> FRR(config-router)#no neighbor <i>PEER_GROUP_NAME</i> peer-group
描述	<p>BGP 路由模式下进行配置。</p> <p>PEER_GROUP_NAME 指定对等体组的名字。对等体组名不超过 32 个字符。</p> <p>如果多个 BGP 对等体可以运用相同的更新策略, 那么可以为这些对等体设置在一个对等体组中, 从而提供了配置上的简化和运行上的高效。</p>

命令	<b>绑定对等体到对等体组</b>
----	-------------------

	<pre>FRR(config-router)#neighbor PEER_ADDR peer-group PEER_GROUP_NAME</pre> <p><b>删除绑定</b></p> <pre>FRR(config-router)#no neighbor PEER_ADDR peer-group (PEER_GROUP_NAME  )</pre>
描述	<p>BGP 路由模式下进行配置。</p> <p>PEER 表示对等体地址。只能是 IP 地址。</p> <p>PEER_GROUP_NAME 表示对等体组的名字。</p> <p>对等体组的成员能够继承对等体的所有配置。允许对等体组的每个成员单独配置从而取代对等体组的统一配置，但这些单独配置的信息不包含那些影响输出更新的配置信息。</p>

#### 6.4.2. 配置对等体

##### ■ 关闭对等体连接

命令	<p><b>关闭对等体连接</b></p> <pre>FRR(config-router)#neighbor PEER shutdown</pre> <p><b>撤销关闭</b></p> <pre>FRR(config-router)#no neighbor PEER shutdown</pre>
描述	<p>BGP 路由模式下进行配置。</p> <p>PEER 表示对等体，可以是 IP 地址或者对等体组的名称。</p> <p>使用本命令将关闭指定的对等体(组)建立的有效连接，并删除所有关联的路由信息。但本命令仍然保留该指定对等体(组)的配置信息。</p> <p>该命令与 no neighbor PEER remote-as ASN 区别在于后者会完全删除指定对等体的配置信息。</p>

##### ■ 设置对等体描述

命令	<p><b>设置对等体描述</b></p> <pre>FRR(config-router)#neighbor PEER description WORD</pre> <p><b>取消对等体描述设置</b></p> <pre>FRR(config-router)#no neighbor PEER description (WORD  )</pre>
描述	<p>BGP 路由模式下进行配置。</p> <p>PEER 表示对等体，可以是 IP 地址或者对等体组的名称。</p> <p>WORD 用来描述该对等体(组)的文本。最多 80 个字符。</p> <p>该命令用来为对等体(组)添加描述性字符。可以很好的帮助用户记忆该对等体(组)的特点和特性。</p>

##### ■ 设置 Local AS

命令	<p><b>设置 Local AS</b></p> <pre>FRR(config-router)#neighbor PEER local-as ASN [ no-prepend [ replace-as [ dual-as ] ] ]</pre> <p><b>取消 Local AS 设置</b></p> <pre>FRR(config-router)#no neighbor PEER local-as [ ASN [ no-prepend [ replace-as [ dual-as ] ] ] ]</pre>
描述	<p>BGP 路由模式下进行配置。</p> <p>PEER 表示对等体，可以是 IP 地址或者对等体组的名称。</p> <p>ASN 表示设定的本地的 AS 号，范围为 1~4294967295。</p> <p>no-prepend: 从对等体接收到的路由信息中的 AS-PATH 不会附加 Local AS，默认情况下无该选项。</p> <p>replace-as: 向对等体发送的路由信息中的 AS-PATH 将使用 Local AS 来替换 BGP 实际 AS，默认情况下无该选项。</p> <p>dual-as: 使得对等体支持使用 BGP 实际 AS 或 Local AS 与设备建立 BGP 连接，默认情况下无该选项。</p> <p>如果用户指定了 BGP 对等体组，那么对等体组的所有成员都将继承该命令的设置。如果为对等体的某个成员设置该命令，其将覆盖基于对等体组的设置。</p>

#### ■ 设置 AS Override

命令	<p><b>设置 AS Override</b></p> <pre>FRR(config-router-af)#neighbor PEER as-override</pre> <p><b>取消 AS Override 设置</b></p> <pre>FRR(config-router-af)#no neighbor PEER as-override</pre>
描述	<p>BGP 的 IPV4 单播地址簇模式下进行配置。</p> <p>PEER 表示对等体，可以是 IP 地址或者对等体组的名称。</p> <p>正常情况下，BGP 协议不会接收具有和本自治域相同 AS 号的路由信息，使用该命令可以覆盖掉 AS 号，使得 BGP 协议可以接收从相同 AS 号传来的路由信息。</p>

#### ■ 激活对等体

命令	<p><b>在当前的地址簇模式下激活对等体或对等体组</b></p> <pre>FRR(config-router-af)#neighbor PEER active</pre> <p><b>在当前的地址簇模式下关闭对等体或对等体组的能力</b></p> <pre>FRR(config-router-af)#no neighbor PEER active</pre>
描述	<p>BGP 的 IPV4 单播地址簇模式下进行配置。</p> <p>PEER 表示对等体，可以是 IP 地址或者对等体组的名称。</p>

	对于 ipv4 单播的地址簇这个命令是默认打开的。
--	---------------------------

■ 设置对等体 Passive 模式

命令	<p><b>设置对等体 Passive 模式</b></p> <p>FRR(config-router)#neighbor <i>PEER</i> passive</p> <p><b>取消设置。</b></p> <p>FRR(config-router)#no neighbor <i>PEER</i> passive</p>
描述	<p>BGP 路由模式下进行配置。</p> <p>PEER 表示对等体，可以是 IP 地址或者对等体组的名称。</p> <p>设置为 passive 模式后，BGP Speaker 不向对应的 BGP 对等体发送 Open 消息。</p>

■ 设置 EBGp 对等体多跳

命令	<p><b>设置 EBGp 对等体多跳</b></p> <p>FRR(config-router)#neighbor <i>PEER</i> ebgp-multihop (<i>HOPS</i>   )</p> <p><b>取消设置</b></p> <p>FRR(config-router)#no neighbor <i>PEER</i> ebgp-multihop (<i>HOPS</i>   )</p>
描述	<p>BGP 的 IPV4 单播地址簇模式下进行配置。</p> <p>PEER 表示 EBGp 对等体，可以是 IP 地址或者对等体组的名称。</p> <p>默认情况下，EBGP 邻居必须是在直连网络的。如果非直连的，需要通过此命令设置允许的最大跳数。</p> <p>HOPS：取值范围为 1-255，默认为 1。若未配置该参数，HOPS 为 255。</p>

■ 设置 MD5 认证

命令	<p><b>设置 MD5 认证的密码</b></p> <p>FRR(config-router)#neighbor <i>PEER</i> password <i>KEY</i></p> <p><b>取消设置 MD5 认证的密码</b></p> <p>FRR(config-router)#no neighbor <i>PEER</i> password <i>KEY</i></p>
描述	<p>BGP 路由模式下进行配置。</p> <p>PEER 表示对等体，可以是 IP 地址或者对等体组的名称。</p> <p>使用 TCP MD5 认证的密码，范围：最多 80 个字符。BGP 邻居两端都必须设置相同的密码。</p> <p>如果用户指定了 BGP 对等体组，那么对等体组的所有成员都将继承该命令的设置。如果为对等体的某个成员设置该命令，其将覆盖基于对等体组的设置。</p>

6.4.3. 对等体信息交互

■ 设置对等体通告缺省路由

命令	<p><b>设置对等体通告缺省路由</b></p> <pre>FRR(config-router-af)#neighbor PEER default-originate (route-map RM_NAME   )</pre> <p><b>取消设置</b><pre>FRR(config-router-af)#no neighbor PEER default-originate (route-map RM_NAME   )</pre></p>
描述	<p>BGP 的 IPV4 单播地址簇模式下进行配置。</p> <p>PEER 表示对等体，可以是 IP 地址或者对等体组的名称。</p> <p>该命令要求本地通过重分步存在缺省路由，才能够向邻居发送缺省路由。</p> <p>如果用户指定了 BGP 对等体组，那么对等体组的所有成员都将继承该命令的设置。如果为对等体的某个成员设置该命令，其将覆盖基于对等体组的设置。</p> <p><b>route-map RM_NAME:</b> 可选参数，关联路由图，对外部缺省路由实施过滤或者参数修改。比如设置 MED，AS-PATH， COMMUNITY 属性等。</p>

■ 设置对等体 Next-Hop-Self

命令	<p><b>设置对等体 Next-Hop-Self</b></p> <pre>FRR(config-router-af)#neighbor PEER next-hop-self (force )</pre> <p><b>取消设置</b><pre>FRR(config-router-af)#no neighbor PEER next-hop-self (force )</pre></p>
描述	<p>BGP 的 IPV4 单播地址簇模式下进行配置。</p> <p>PEER 表示对等体，可以是 IP 地址或者对等体组的名称。</p> <p>没有打开该功能。向 EBGp 对等体通告路由时，下一跳设置为本 BGP Speaker，向 IBGP 对等体通告路由时不修改下一跳。开启该功能后，向 IBGP 对等体通告路由时下一跳也设置为本 BGP Speaker。</p> <p>如果用户指定了 BGP 对等体组，那么对等体组的所有成员都将继承该命令的设置。如果为对等体的某个成员设置该命令，其将覆盖基于对等体组的设置。</p> <p><b>force:</b> 可选参数，针对路由反射器，表示对客户端通告路由时下一跳也设置为本路由反射器。</p>

■ 设置对等体 Remove-Private-AS

命令	<p><b>设置对等体 Remove-Private-AS</b></p> <pre>FRR(config-router-af)#neighbor PEER remove-private-AS</pre>
----	--



	<b>取消设置</b> FRR(config-router-af)#no neighbor <i>PEER</i> remove-private-AS
描述	<p>BGP 的 IPV4 单播地址簇模式下进行配置。</p> <p>PEER 表示对等体，可以是 IP 地址或者对等体组的名称。</p> <p>本命令只对 EBGp 对等体有效。私有 AS 号的范围：64512~65535。默认情况下，BGP 向 EBGp 对等体通告路由信息时不删除 AS-PATH 属性中的私有 AS。该命令用于控制删除私有 AS。特殊情况下：如果 AS 路径包含的私有 AS 号就是将要发送的 EBGp 对等体的 AS 号，将不会删除该 AS 号。</p>

#### ■ 设置对等体 Send-Community

命令	<b>设置对等体 Send-Community</b> FRR(config-router-af)#neighbor <i>PEER</i> send-community
	<b>取消设置</b> FRR(config-router-af)#no neighbor <i>PEER</i> send-community
描述	<p>BGP 的 IPV4 单播地址簇模式下进行配置。</p> <p>PEER 表示对等体，可以是 IP 地址或者对等体组的名称。</p> <p>使用该命令可以允许将团体的指定的属性传输给固定的邻居或一组邻居。</p>

#### ■ 设置对等体 Maximum-Prefix

命令	<b>设置对等体 Maximum-Prefix</b> FRR(config-router-af)#neighbor <i>PEER</i> max-prefix <i>NUM</i> [ <i>threshold</i> ] (restart <i>interval</i>   warning-only   )
	<b>取消设置</b> FRR(config-router-af)#no neighbor <i>PEER</i> max-prefix [ <i>NUM</i> [ <i>threshold</i> ] (restart <i>interval</i>   warning-only   ) ]
描述	<p>BGP 的 IPV4 单播地址簇模式下进行配置。</p> <p>PEER 表示对等体，可以是 IP 地址或者对等体组的名称。</p> <p>NUM 表示允许的前缀数目，范围为 1-4294967295。默认不限制。</p> <p>设置该功能后，超过数目限制的前缀将不再学习。</p> <p>threshold: 可选参数，指定开始产生警告时，前缀数目和最大数目的百分比的值。取值范围1-100，单位百分比，缺省为75。</p> <p>restart: 可选参数，前缀数目达到限制时，重启BGP连接。interval表示等待一定时间后重启。单位为分钟。取值范围1-65535。</p> <p>warning-only: 可选参数，表示超过数目限制时仅仅告警，而不禁止学习。</p>

## 6.4.4. AS-PATH 列表

命令	<p>添加 AS-PATH 列表表项</p> <pre>FRR(config)#ip as-path access-list <i>as_path_name</i> (permit   deny) <i>regular-expression</i></pre> <p>删除 AS-PATH 列表表项</p> <pre>FRR(config)#no ip as-path access-list <i>as_path_name</i> (permit   deny) <i>regular-expression</i></pre> <p>删除 AS-PATH 列表</p> <pre>FRR(config)#no ip as-path access-list <i>as_path_name</i></pre>
描述	<p>全局模式下进行配置。</p> <p><i>as_path_name</i>: AS-PATH 列表名称。AS-PATH 被 BGP 路由过滤或者路由图应用时，使用该名称标识 AS-PATH 列表。</p> <p>permit 和 deny 两种行为必须二选一。用于路由过滤时，deny 表示过滤，permit 表示允许。用于路由图时，permit 表示匹配中，deny 表示未匹配中。</p> <p><i>regular-expression</i>: 正则表达式。</p>

## 6.4.5. COMMUNITY 列表

命令	<p>添加 COMMUNITY 列表标准表项</p> <pre>FRR(config)#ip community-list (&lt;1-99&gt;   standard <i>NAME</i>) (permit   deny) <i>COMMUNITY_NUM...</i></pre> <p>添加 COMMUNITY 列表扩展表项:</p> <pre>FRR(config)#ip community-list (&lt;100-500&gt;   expanded <i>NAME</i>) (permit   deny) <i>COMMUNITY_NUM...</i></pre> <p>删除 COMMUNITY 列表标准表项:</p> <pre>FRR(config)#no ip community-list (&lt;1-99&gt;   standard <i>NAME</i>) (permit   deny) <i>COMMUNITY_NUM...</i></pre> <p>删除 COMMUNITY 列表扩展表项:</p> <pre>FRR(config)#no ip community-list (&lt;100-500&gt;   expanded <i>NAME</i>) (permit   deny) <i>COMMUNITY_NUM...</i></pre>
描述	<p>全局模式下进行配置。</p> <p>COMMUNITY 列表可以用 ID 表示，1-99 表示标准表项，100-500 表示扩展表项；也可以使用列表名字表示。</p>

	<p>COMMUNITY 列表可以用来路由图匹配或者路由图设置（COMMUNITY 属性删除），用于 COMMUNITY 属性删除时只能使用标准列表。</p> <p>permit 和 deny 两种行为必须二选一。permit 表示匹配中，deny 表示未匹配中。</p> <p>COMMUNITY_NUM 的可能格式如下：</p> <ol style="list-style-type: none"><li>1) AA:NN    AA 和 NN 的取值范围均为 0-65535。</li><li>2) 知名团队名称：（local-AS no-advertise no-export internet）</li></ol> <p>一条表项可以配置若干个 COMMUNITY_NUM。</p>
--	--

6.4.6. 路由策略

■ distribute-list

命令	<p><b>应用 ACL 路由过滤</b></p> <p>FRR(config-router-af)#neighbor <i>PEER</i> distribute-list (<i>acl_id</i>   <i>acl_name</i>) (in   out)</p> <p><b>取消应用 ACL</b></p> <p>FRR(config-router-af)#no neighbor <i>PEER</i> distribute-list (<i>acl_id</i>   <i>acl_name</i>) (in   out)</p>
描述	<p>BGP 的 IPV4 单播地址簇模式下进行配置。</p> <p>PEER 表示对等体，可以是 IP 地址或者对等体组的名称。</p> <p>标准 ACL 使用 <i>acl_id</i> 标识。范围为 1-99 和 1300-1999。</p> <p>Zebra ACL 使用 <i>acl_name</i> 标识。</p> <p>in: ACL 应用于接收到的路由信息。</p> <p>out: ACL 应用于分发出去的路由信息。</p> <p>对应表项行为为permit的路由表示允许，对应表项行为为deny的路由表示禁止。</p> <p>如果用户指定了BGP对等体组，那么对等体组的所有成员都可以继承该命令的设置。如果为对等体的某个成员设置neighbor distribute-list，将覆盖基于对等体组的设置。</p>

■ filter-list

命令	<p><b>应用 AS-PATH 列表路由过滤</b></p> <p>FRR(config-router-af)#neighbor <i>PEER</i> filter-list <i>as_path_name</i> (in   out)</p> <p><b>取消应用 AS-PATH 列表</b></p> <p>FRR(config-router-af)#no neighbor <i>PEER</i> filter-list <i>as_path_name</i> (in   out)</p>
----	--

描述	<p>BGP 的 IPV4 单播地址簇模式下进行配置。</p> <p>PEER 表示对等体，可以是 IP 地址或者对等体组的名称。</p> <p>as_path_name 标识应用的 AS-PATH 列表。</p> <p>in: ACL 应用于接收到的路由信息。</p> <p>out: ACL 应用于分发出去的路由信息。</p> <p>对应表项行为为permit的路由表示允许，对应表项行为为deny的路由表示禁止。</p> <p>如果用户指定了BGP对等体组，那么对等体组的所有成员都可以继承该命令的设置。如果为对等体的某个成员设置neighbor filter-list，将覆盖基于对等体组的设置。</p>
----	--

■ prefix-list

命令	<p><b>应用 prefix-list 路由过滤</b></p> <p>FRR(config-router-af)#neighbor <i>PEER</i> prefix-list <i>pl_name</i> (in   out)</p> <p><b>取消应用 prefix-list</b></p> <p>FRR(config-router-af)#no neighbor <i>PEER</i> prefix-list <i>pl_name</i> (in   out)</p>
描述	<p>BGP 的 IPV4 单播地址簇模式下进行配置。</p> <p>PEER 表示对等体，可以是 IP 地址或者对等体组的名称。</p> <p>pl_name 标识应用的 prefix-list。</p> <p>in: ACL 应用于接收到的路由信息。</p> <p>out: ACL 应用于分发出去的路由信息。</p> <p>对应表项行为为permit的路由表示允许，对应表项行为为deny的路由表示禁止。</p> <p>如果用户指定了BGP对等体组，那么对等体组的所有成员都可以继承该命令的设置。如果为对等体的某个成员设置neighbor prefix-list，将覆盖基于对等体组的设置。</p>

■ route-map

命令	<p><b>应用 route-map 路由过滤或参数修改</b></p> <p>FRR(config-router-af)#neighbor <i>PEER</i> route-map <i>rm_name</i> (in   out)</p> <p><b>取消应用 route-map</b></p> <p>FRR(config-router-af)#no neighbor <i>PEER</i> route-map <i>rm_name</i> (in   out)</p>
描述	<p>BGP 的 IPV4 单播地址簇模式下进行配置。</p> <p>PEER 表示对等体，可以是 IP 地址或者对等体组的名称。</p> <p>rm_name 标识应用的 route-map。</p> <p>in: ACL 应用于接收到的路由信息。</p>

	<p>out: ACL 应用于分发出去的路由信息。</p> <p>若route-map的模式为permit, 匹配route-map的路由将进行路由信息修改。可以设置MED属性 (metric), COMMUNITY属性, AS-PATH属性等等 (具体参见“路由图”的行为设置)。</p> <p>若route-map的模式为deny, 匹配route-map的路由将进行过滤。</p> <p>如果用户指定了BGP对等体组, 那么对等体组的所有成员都可以继承该命令的设置。如果为对等体的某个成员设置neighbor route-map, 将覆盖基于对等体组的设置。</p>
--	--

#### ■ unsuppress-map

命令	<p><b>应用 unsuppress-map 控制聚合路由的原始路由的公告</b></p> <pre>FRR(config-router-af)#neighbor PEER unsuppress-map rm_name</pre> <p><b>取消应用 unsuppress-map</b></p> <pre>FRR(config-router-af)#no neighbor PEER unsuppress-map rm_name</pre>
描述	<p>BGP 的 IPV4 单播地址簇模式下进行配置。</p> <p>PEER 表示对等体, 可以是 IP 地址或者对等体组的名称。</p> <p>rm_name 标识应用的 route-map。</p> <p>该命令仅用于 out 方向, 应用于控制聚合路由的原始路由。该命令可以将由于 aggregate-address 命令抑制的路由选择性的公告出去。</p> <p>如果用户指定了BGP对等体组, 那么对等体组的所有成员都可以继承该命令的设置。如果为对等体的某个成员设置neighbor unsuppress-map, 将覆盖基于对等体组的设置。</p>

### 6.4.7. 路由反射器

命令	<p><b>配置反射客户端</b></p> <pre>FRR(config-router-af)#neighbor PEER route-reflector-client</pre> <p><b>取消配置</b></p> <pre>FRR(config-router-af)#no neighbor PEER route-reflector-client</pre>
描述	<p>BGP 的 IPV4 单播地址簇模式下进行配置。</p> <p>PEER 表示对等体, 可以是 IP 地址或者对等体组的名称。</p> <p>只要配置一个BGP对等体为反射客户端, 本BGP Speaker即成为路由反射器, 当最后一个反射客户端取消, 本BGP Speaker不再作为路由反射器。</p>

### 6.4.8. AS 联盟

#### ■ 配置联盟的 ASN

命令	<b>配置 AS 联盟 ASN</b>
----	---------------------

	FRR(config-router)# <b>bgp confederation identifier</b> <i>ASN</i>  <b>取消配置</b> FRR(config-router)# <b>no bgp confederation identifier</b> ( <i>ASN</i>  )
描述	BGP 路由模式下进行配置。 ASN 标识联盟的 AS 号，对外部而言，只看到这个联盟 ASN。但在联盟内部，各个子 AS 有各自的 ASN。且子 AS 间也是运行 EBGP。ASN 取值范围 1-4294967295。

#### ■ 配置联盟成员

命令	<b>配置 AS 联盟成员</b> FRR(config-router)# <b>bgp confederation peers</b> <i>ASN...</i>  <b>取消配置</b> FRR(config-router)# <b>no bgp confederation peers</b> <i>ASN...</i>
描述	BGP 路由模式下进行配置。 ASN 标识联盟成员（子 AS）的 AS 号，这些子 AS 一般而言，只在联盟内部使用。ASN 取值范围 1-4294967295。 该命令可以配置若干个联盟成员（至少要配置 1 个）。

### 6.4.9. 注入路由

#### ■ 静态配置

命令	<b>静态配置注入路由</b> FRR(config-router)# <b>network</b> <i>A.B.C.D/M</i> [{ <b>backdoor</b>   <b>route-map</b> <i>rm_name</i> }] <b>或者</b> FRR(config-router-af)# <b>network</b> <i>A.B.C.D/M</i> [{ <b>backdoor</b>   <b>route-map</b> <i>rm_name</i> }]  <b>取消配置</b> FRR(config-router)# <b>no network</b> <i>A.B.C.D/M</i> [{ <b>backdoor</b>   <b>route-map</b> <i>rm_name</i> }] <b>或者</b> FRR(config-router-af)# <b>no network</b> <i>A.B.C.D/M</i> [{ <b>backdoor</b>   <b>route-map</b> <i>rm_name</i> }]
描述	BGP 路由模式，或者 BGP 的 IPV4 单播地址簇模式下进行配置。  该命令可以注入路由的前提的核心路由表中存在相同的 IGP 路由（比如 OSPF，IS-IS，RIP，静态，直连）。通过此命令注入的 BGP 路由类型为“IGP”。

	<p>backdoor: 添加 backdoor 参数后, 该命令的目的不是注入路由, 而是将从 EBGp 学习到的路由的管理距离增大 (默认为 20, 配置 backdoor 之后为 200, 类型本来为 “EGP”, 配置 backdoor 之后为 “IGP”)。从而使得选中 IGP 的路由。</p> <p>route-map: 通过关联 route-map 对路由进行过滤或者路由参数修改。</p>
--	---

#### ■ 路由重分布

命令	<p><b>路由重分布</b></p> <pre>FRR(config-router-af)#redistribute (static connect kernel ospf rip isis) (metric metric   route-map rm_name   )</pre> <p><b>取消路由重分布</b></p> <pre>FRR(config-router-af)#no redistribute (static connect kernel ospf rip isis) (metric metric   route-map rm_name   )</pre>
描述	<p>BGP 的 IPV4 单播地址簇模式下进行配置。</p> <p>通过该命令, 将 IGP 的路由导入 BGP 协议。</p> <p>static: 静态路由。</p> <p>connect: 直连路由, 开启 OSPF 的网段, 会自动作为 connect 路由导入 OSPF 协议。</p> <p>kernel: 内核路由, 如果主 CLI 有配置 CLI, 在 FRR CLI 中会作为 kernel 路由。不建议两边同时配置路由。</p> <p>ospf: OSPF 协议的路由</p> <p>rip: RIP 协议的路由</p> <p>isis: IS-IS 协议的路由</p> <p><b>metric metric:</b> 可选参数, 设置重分布路由的 metric, 取值范围 0-4294967295。默认是 0。</p> <p><b>route-map rm_name:</b> 可选参数, 关联路由图, 对重分布的路由实施过滤或者参数修改。</p> <p>通过此命令注入的 BGP 路由类型为 “incomplete”。</p>

#### 6.4.10. 路由聚合

命令	<p><b>路由聚合</b></p> <pre>FRR(config-router)#aggregate-address A.B.C.D/M [{ as-set   summary-only}] 或者 FRR(config-router-af)#aggregate-address A.B.C.D/M [{ as-set   summary- only}]</pre> <p><b>取消路由聚合</b></p> <pre>FRR(config-router)#no aggregate-address A.B.C.D/M [{ as-set   summary-</pre>
----	---

	<code>only}}]</code> <b>或者</b> <code>FRR(config-router-af)#no aggregate-address A.B.C.D/M [{ as-set   summary-only}]</code>
描述	<p>BGP 路由模式，或者 BGP 的 IPv4 单播地址簇模式下进行配置。</p> <p>只有当聚合范围内存在有效的路由时，才将 BGP 聚合表项添加到 BGP 路由表中。</p> <p><code>as-set</code> 参数：保留聚合地址范围内路由的 AS-PATH 信息，缺省情况下 BGP 不保留 AS-PATH 信息。</p> <p><code>summary-only</code> 参数：缺省情况下路由聚合后，既会向邻居通告聚合后的路由，也会通告聚合范围内的路由。配置该参数，表示只通告聚合后的路由。</p>

#### 6.4.11. 路由表下发

命令	<p><b>应用table-map</b></p> <code>FRR(config-router)#table-map rm_map</code> <b>或者</b> <code>FRR(config-router-af)# table-map rm_map</code>  <p><b>取消应用table-map</b></p> <code>FRR(config-router)#no table-map rm_map</code> <b>或者</b> <code>FRR(config-router-af)#no table-map rm_map</code>
描述	<p>BGP 路由模式，或者 BGP 的 IPv4 单播地址簇模式下进行配置。</p> <p>缺省情况下，允许下发所有路由，而且不改变下发路由的路由属性。BGP 可以使用 <code>table-map</code> 来控制下发到核心路由表的路由信息（<code>table-map</code> 关联到 <code>permit</code> 模式的 <code>route-map</code>）。如果匹配路由，则修改路由信息的属性，并下发路由；如果不匹配路由，或者匹配到 <code>deny</code> 表项，则不修改路由信息的属性，仍然下发路由。</p>

#### 6.4.12. 软复位

##### ■ 保存邻居的原始路由信息

命令	<p><b>保存邻居原始路由信息</b></p> <code>FRR(config-router-af)# neighbor PEER soft-reconfiguration inbound</code>  <p><b>取消保存</b></p> <code>FRR(config-router-af)#no neighbor PEER soft-reconfiguration inbound</code>
描述	<p>BGP 的 IPv4 单播地址簇模式下进行配置。</p> <p><code>PEER</code> 表示对等体，可以是 IP 地址或者对等体组的名称。</p>



	<p>缺省情况下，不保存原始路由信息（比如经过路由过滤后，只保存未被过滤的路由）。</p> <p>通过此命令，可以保存相应邻居的发出的所有原始路由信息。</p>
--	--

#### ■ 软复位

命令	<p><b>软复位</b></p> <p>A: FRR#clear ip bgp PEER [soft] (in   out)</p> <p>B: FRR#clear ip bgp PEER soft</p>
描述	<p>特权模式下执行该命令。</p> <p>该命令只对应一个操作，无相关配置保留。</p> <p>PEER 表示对等体，可以是 IP 地址或者对等体组的名称。</p> <p>in: 若没有保存邻居的原始路由信息，则向邻居发送通告请求。邻居若支持“路由刷新功能”，会将所有路由重新通告一遍。若已经保存邻居的原始路由信息，则直接从本地刷新即可。若本 BGP Speaker 的输入路由策略发生变化，需要使用此命令进行即时更新。</p> <p>out: 若本 BGP Speaker 的输出路由策略发生变化，需要使用此命令触发重新往对应邻居的路由通告。</p> <p>B 表示同时软复位 in 和 out 两个方向。</p>

### 6.4.13. 路由优选

#### ■ AS-PATH 长度检查控制

命令	<p><b>配置AS-PATH长度检查控制</b></p> <p>FRR(config-router)#bgp bestpath as-path (confed   ignore)</p> <p><b>取消配置</b></p> <p>FRR(config-router)#no bgp bestpath as-path (confed   ignore)</p>
描述	<p>BGP 路由模式下进行配置。</p> <p>confed: 在进行 AS-PATH 长度比较时，AS-CONFED-SETH 和 AS-CONFED-SEQUENCED 段的长度也纳入比较。缺省不纳入比较。</p> <p>bgp bestpath as-path ignore: 允许 BGP 进行优先选择时不考虑比较 AS-PATH 长度，缺省会比较 AS-PATH 长度。</p>

#### ■ MED 检查控制

命令	<p><b>配置MED bestpath选项</b></p> <p>FRR(config-router)#bgp bestpath med (confed   missing-as-worst)</p> <p><b>取消配置</b></p> <p>FRR(config-router)#no bgp bestpath med (confed   missing-as-worst)</p>
----	--

描述	<p>BGP 路由模式下进行配置。</p> <p>confed: 默认情况下, 联盟内部不进行 MED 检查, 开启后允许联盟内部不同子 AS 的路由的进行 MED 检查。</p> <p>missing-as-worst: 未设置 MED 属性的路由, 优先级最低, 默认情况下, 未设置 MED 属性的路由不参与 MED 检查。</p>
----	---

命令	<p><b>配置比较不同AS的MED</b></p> <p>FRR(config-router)#bgp always-compare-med</p> <p><b>取消配置</b></p> <p>FRR(config-router)#no bgp always-compare-med</p>
描述	<p>BGP 路由模式下进行配置。</p> <p>一般情况下, 只比较来自同一 AS 中各 EBGp 邻居路由的 MED 属性, 不比较来自不同 AS 的 MED 值。由于不同自治系统的 MED 值定义不尽相同。因此, 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命令。</p>

命令	<p><b>配置优先比较同个AS的MED</b></p> <p>FRR(config-router)#bgp deterministic-med</p> <p><b>取消配置</b></p> <p>FRR(config-router)#no bgp deterministic-med</p>
描述	<p>BGP 路由模式下进行配置。</p> <p>该命令可以使得来自于同一个 AS 的同个目的的多条不同路由优先进行 MED 属性比较。即同属于一个 AS 的路由优胜者再跟其他 AS 的同个目的的不同路由进行 MED 属性比较（在 bgp always-compare-med 开启的情况下）。</p>

#### ■ Router ID 检查开关

命令	<p><b>配置比较Router ID</b></p> <p>FRR(config-router)#bgp bestpath compare-routerid</p> <p><b>取消配置</b></p> <p>FRR(config-router)#no bgp bestpath compare-routerid</p>
描述	<p>BGP 路由模式下进行配置。</p>

	默认 Router ID 检查未开启，通过此命令开启 Router ID 检查。
--	--

6.4.14. 路由衰减

■ 配置路由衰减

命令	<p><b>启动路由衰减</b></p> <p>FRR(config-router)#<b>bgp dampening</b></p> <p><b>或者</b></p> <p>FRR(config-router-af)#<b>bgp dampening</b></p> <p><b>配置路由衰减参数</b></p> <p>FRR(config-router)#<b>bgp dampening</b> <i>half-life-time reuse suppress max-suppress-time</i></p> <p><b>或者</b></p> <p>FRR(config-router-af)#<b>bgp dampening</b> <i>half-life-time reuse suppress max-suppress-time</i></p> <p><b>关闭路由衰减</b></p> <p>FRR(config-router)#<b>no bgp dampening</b> (<i>half-life-time reuse suppress max-suppress-time  </i> )</p> <p><b>或者</b></p> <p>FRR(config-router-af)#<b>no bgp dampening</b> (<i>half-life-time reuse suppress max-suppress-time  </i> )</p>
描述	<p>BGP 路由模式，或者 BGP 的 IPV4 单播地址簇模式下进行配置。</p> <p>默认未开启路由衰减功能，此命令用于开启此功能, 可选的进行参数修改。</p> <p>参数说明如下：</p> <p>half-life-time：半衰期，惩罚值减为一半的所经过的时间。默认为 15，单位为分钟，取值范围为 1-45。</p> <p>reuse：重新启用值，当路由的惩罚值低于该值时，路由抑制解除。默认为 750，取值范围为 1-20000。</p> <p>suppress：抑制上限，当路由的惩罚值超过该值时，路由被抑制。默认为 2000，取值范围为 1-20000。</p> <p>max-suppress-time：最大抑制时间，路由能被抑制的最长时间。默认为 4 * half-life-time。单位为分钟，取值范围为 1-255。</p>

6.4.15. 管理距离

命令	<p><b>配置管理距离</b></p> <p>FRR(config-router)#<b>distance bgp</b> <i>external-distance internal-distance local-distance</i></p>
----	--

	<b>取消配置</b> FRR(config-router)#no distance bgp ( <i>external-distance internal-distance local-distance</i>   )
描述	BGP 路由模式下进行配置。  管理距离的取值范围为 1-255。 external-distance: 从 EBGPeers 学习到路由的管理距离。默认管理距离为 20。 internal-distance: 从 IBGP Peers 学习到路由的管理距离。默认管理距离为 200。 local-distance: 后门路由的管理距离（通过 network backdoor 命令配置的路由）。默认管理距离为 200。

#### 6.4.16. 定时器

##### ■ 配置邻居保活定时器

命令	<b>全局配置邻居保活定时器</b> FRR(config-router)#timer bgp <i>keepalive holdtime</i>  <b>取消配置</b> FRR(config-router)#no timer bgp ( <i>keepalive holdtime</i>   )
描述	BGP 路由模式下进行配置。  BGP 使用 Keepalive 定时器来维持和对等体的有效连接，使用 Holdtime 定时器来判断对等体是否有效。 缺省情况下，Keepalive 定时器的值为 60 秒，Holdtime 定时器的值为 180 秒。 当 BGP Speakers 之间建立 BGP 连接时，双方将对 Holdtime 进行协商，值更小的 Holdtime 将被选择，而 Keepalive 定时器值的将选择协商后的 Holdtime 的 1/3 和配置的 Keepalive 的值的较小者。 keepalive 和 holdtime 参数的单位为秒，取值范围 0-65535。 本命令会控制所有邻居。

命令	<b>基于邻居配置邻居保活定时器</b> FRR(config-router)#neighbor <i>PEER</i> timer <i>keepalive holdtime</i>  <b>取消配置</b> FRR(config-router)#no neighbor <i>PEER</i> timer ( <i>keepalive holdtime</i>   )
描述	BGP 路由模式下进行配置。 PEER 表示对等体，可以是 IP 地址或者对等体组的名称。  BGP 使用 Keepalive 定时器来维持和对等体的有效连接，使用 Holdtime 定时器来判断对等体是否有效。

	缺省情况下，Keepalive 定时器的值为 60 秒，Holdtime 定时器的值为 180 秒。 keepalive 和 holdtime 参数的单位为秒，取值范围 0-65535。 本命令仅控制指定的邻居。
--	--

#### ■ 配置邻居重连定时器

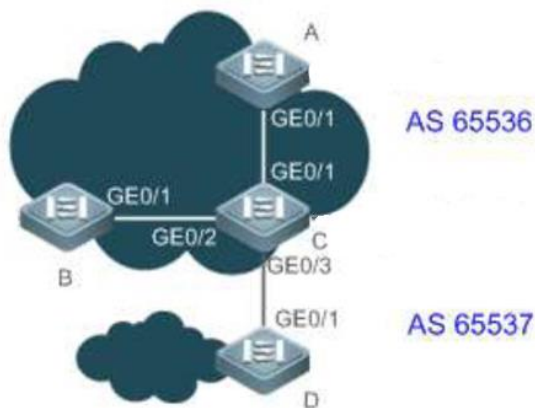
命令	<b>配置邻居重连定时器</b> FRR(config-router)#neighbor <i>PEER</i> timer connect <i>connect-retry</i>  <b>取消配置</b> FRR(config-router)#no neighbor <i>PEER</i> timer connect ( <i>connect-retry</i>   )
描述	BGP 路由模式下进行配置。 PEER 表示对等体，可以是 IP 地址或者对等体组的名称。  为降低 BGP 频繁尝试与连接失败的邻居进行重连对网络带宽的影响，BGP Speaker 检测到与邻居建立连接失败之后，将在 connect-retry 定时器到期之后再尝试进行重连。 缺省情况下，connect-retry 定时器的值为 15 秒，取值范围 0-65535。

#### ■ 配置路由通告定时器

命令	<b>配置路由通告定时器</b> FRR(config-router)#neighbor <i>PEER</i> advertisement-interval <i>seconds</i>  <b>取消配置</b> FRR(config-router)#no neighbor <i>PEER</i> advertisement-interval ( <i>seconds</i>   )
描述	BGP 路由模式下进行配置。 PEER 表示对等体，可以是 IP 地址或者对等体组的名称。  为减少路由更新报文对网络带宽的影响，BGP Speaker 在检测到网络拓扑发生变化后，并不立即将路由更新通告给邻居。而是采用定时更新的机制，将所有发生变化的路由信息一起通告给邻居设备。缺省情况下，IBGP 对等体 0 秒（即时通告），EBGP 对等体为 30 秒。取值范围 0-600。

## 6.5. 配置案例

### 6.5.1. 配置 BGP 对等体



各接口所属的 VLAN 和 SVI 的 IP 地址如下所示：（所有路由设备以交换机为例）

A : GE 0/1 VLAN10 192.168.1.1/24

Router ID 10.1.1.1

B : GE 0/1 VLAN20 192.168.2.2/24

Router ID 10.1.1.2

C : GE 0/1 VLAN10 192.168.1.3/24

GE 0/2 VLAN20 192.168.2.3/24

GE 0/3 VLAN30 192.168.3.3/24

Router ID 10.1.1.3

D : GE0/1 VLAN30 192.168.3.4/24

Router ID 10.1.1.4

#### ■ 配置路由设备 A

- 主 CLI：配置接口 VLAN，配置对应 SVI 的 IP 地址。

```

SWITCH(config)#vlan 10
SWITCH(config)#interface gi 0/1
SWITCH(config-if)#switch access vlan 10
SWITCH(config-if)#exit
SWITCH(config)#int Vlan10
SWITCH(config-if)#ip address 192.168.1.1/24
  
```

- FRR CLI：

- ✧ 配置全局 Router ID
- ✧ 启动 OSPF。
- ✧ 启动网段的 OSPF，并指定对应 Area。
- ✧ 启动 BGP 65536。
- ✧ 与 B 及 C 建立 IBGP 邻居。

```
FRR#configure terminal
FRR(config)#router-id 10.1.1.1
FRR(config)#router ospf
FRR(config-router)#network 192.168.1.0/24 area 0
FRR(config-router)#exit
FRR(config)#router bgp 65536
FRR(config-router)#neighbor 192.168.1.3 remote-as 65536
FRR(config-router)#neighbor 192.168.2.2 remote-as 65536
```

#### ■ 配置路由设备 B

- 主 CLI：配置接口 VLAN，配置对应 SVI 的 IP 地址。（省略）
- FRR CLI：

- ✧ 配置全局 Router ID。
- ✧ 启动 OSPF。
- ✧ 启动网段的 OSPF，并指定对应 Area。
- ✧ 启动 BGP 65536。
- ✧ 与 A 及 C 建立 IBGP 邻居

```
FRR#configure terminal
FRR(config)#router-id 10.1.1.2
FRR(config)#router ospf
FRR(config-router)#network 192.168.2.0/24 area 0
FRR(config-router)#exit
FRR(config)#router bgp 65536
FRR(config-router)#neighbor 192.168.2.3 remote-as 65536
FRR(config-router)#neighbor 192.168.1.1 remote-as 65536
```

#### ■ 配置路由设备 C

- 主 CLI：配置接口 VLAN，配置对应 SVI 的 IP 地址。（省略）
- FRR CLI：

- ✧ 配置全局 Router ID。
- ✧ 启动 OSPF。
- ✧ 启动网段的 OSPF，并指定对应 Area。
- ✧ 启动 BGP 65536。
- ✧ 创建对等体组 ibgp-group，将 A,B 加入对等体组。
- ✧ 与对等体组 ibgp-group 建立 IBGP 邻居。

✧ 与 D 建立 EBGp 邻居。

```
FRR#configure terminal
FRR(config)#router-id 10.1.1.3
FRR(config)#router ospf
FRR(config-router)#network 192.168.1.0/24 area 0
FRR(config-router)#network 192.168.2.0/24 area 0
FRR(config-router)#exit
FRR(config)#router bgp 65536
FRR(config-router)#neighbor ibgp-group peer-group
FRR(config-router)#neighbor 192.168.1.1 peer-group ibgp-group
FRR(config-router)#neighbor 192.168.2.2 peer-group ibgp-group
FRR(config-router)#neighbor ibgp-group remote-as 65536
FRR(config-router)#neighbor 192.168.3.4 remote-as 65537
```

#### ■ 配置路由设备 D

➤ 主 CLI：配置接口 VLAN，配置对应 SVI 的 IP 地址。（省略）

➤ FRR CLI：

✧ 配置全局 Router ID。

✧ 启动 BGP 65537。

✧ 与 C 建立 EBGp 邻居。

```
FRR#configure terminal
FRR(config)#router-id 10.1.1.4
FRR(config)#router bgp 65537
FRR(config-router)#neighbor 192.168.3.4 remote-as 65537
```

#### ■ 配置效果

➤ 路由设备 A：（B 和 C 均作为 IBGP 邻居）

```
FRR# show ip bgp neighbors
BGP neighbor is 192.168.1.3, remote AS 65536, local AS 65536, internal
link
Hostname: SWITCH-C
  BGP version 4, remote router ID 10.0.0.3
  BGP state = Established, up for 00:00:05
  Last read 00:00:02, Last write 00:00:02
  Hold time is 9, keepalive interval is 3 seconds
  Neighbor capabilities:
    4 Byte AS: advertised and received
  AddPath:
    IPv4 Unicast: RX advertised IPv4 Unicast and received
  Route refresh: advertised and received(old & new)
  Address Family IPv4 Unicast: advertised and received
```



Hostname Capability: advertised (name: SWITCH-A, domain name: n/a)  
received (name: SWITCH-C, domain name: n/a)

Graceful Restart Capabilty: advertised and received

Remote Restart timer is 120 seconds

Address families by peer:

none

Graceful restart informations:

End-of-RIB send: IPv4 Unicast

End-of-RIB received: IPv4 Unicast

Message statistics:

Inq depth is 0

Outq depth is 0

	Sent	Rcvd
Opens:	1	1
Notifications:	0	0
Updates:	1	1
Keepalives:	2	2
Route Refresh:	0	0
Capability:	0	0
Total:	4	4

Minimum time between advertisement runs is 0 seconds

For address family: IPv4 Unicast

Update group 1, subgroup 1

Packet Queue length 0

Community attribute sent to this neighbor(all)

0 accepted prefixes

Connections established 1; dropped 0

Last reset never

Local host: 192.168.1.1, Local port: 34073

Foreign host: 192.168.1.3, Foreign port: 179

Nexthop: 192.168.1.3

Nexthop global: fe80::2aa:bbff:fe09:2616

Nexthop local: fe80::2aa:bbff:fe09:2616

BGP connection: shared network

BGP Connect Retry Timer in Seconds: 10

Estimated round trip time: 10 ms

Read thread: on Write thread: on

BGP neighbor is 192.168.2.2, remote AS 65536, local AS 65536, internal link

Hostname: SWITCH-B

BGP version 4, remote router ID 10.0.0.2

BGP state = Established, up for 00:00:05

Last read 00:00:02, Last write 00:00:02

Hold time is 9, keepalive interval is 3 seconds

Neighbor capabilities:

4 Byte AS: advertised and received

AddPath:

IPv4 Unicast: RX advertised IPv4 Unicast and received

Route refresh: advertised and received(old & new)

Address Family IPv4 Unicast: advertised and received

Hostname Capability: advertised (name: SWITCH-A, domain name: n/a)  
received (name: SWITCH-B, domain name: n/a)

Graceful Restart Capabilty: advertised and received

Remote Restart timer is 120 seconds

Address families by peer:

none

Graceful restart informations:

End-of-RIB send: IPv4 Unicast

End-of-RIB received: IPv4 Unicast

Message statistics:

Inq depth is 0

Outq depth is 0

	Sent	Rcvd
Opens:	1	1
Notifications:	0	0
Updates:	1	1
Keepalives:	2	2
Route Refresh:	0	0
Capability:	0	0
Total:	4	4

Minimum time between advertisement runs is 0 seconds

For address family: IPv4 Unicast

Update group 1, subgroup 1

Packet Queue length 0

Community attribute sent to this neighbor(all)

0 accepted prefixes

Connections established 1; dropped 0

Last reset never

Local host: 192.168.1.1, Local port: 34073

```
Foreign host: 192.168.2.2, Foreign port: 179
```

```
Nexthop: 192.168.1.3
```

```
Nexthop global: fe80::2aa:bbff:fe09:2616
```

```
Nexthop local: fe80::2aa:bbff:fe09:2616
```

```
BGP connection: shared network
```

```
BGP Connect Retry Timer in Seconds: 10
```

```
Estimated round trip time: 10 ms
```

```
Read thread: on Write thread: on
```

- 路由设备 B: (A 和 C 均作为 IBGP 邻居)

```
FRR# show ip bgp
```

```
BGP neighbor is 192.168.2.3, remote AS 65536, local AS 65536, internal link
```

```
Hostname: SWITCH-C
```

```
BGP version 4, remote router ID 10.0.0.3
```

```
BGP state = Established, up for 00:00:05
```

```
Last read 00:00:02, Last write 00:00:02
```

```
Hold time is 9, keepalive interval is 3 seconds
```

```
Neighbor capabilities:
```

```
4 Byte AS: advertised and received
```

```
AddPath:
```

```
IPv4 Unicast: RX advertised IPv4 Unicast and received
```

```
Route refresh: advertised and received(old & new)
```

```
Address Family IPv4 Unicast: advertised and received
```

```
Hostname Capability: advertised (name: OLT, domain name: n/a) received
```

```
(name:
```

```
SWITCH, domain name: n/a)
```

```
Graceful Restart Capabilty: advertised and received
```

```
Remote Restart timer is 120 seconds
```

```
Address families by peer:
```

```
none
```

```
Graceful restart informations:
```

```
End-of-RIB send: IPv4 Unicast
```

```
End-of-RIB received: IPv4 Unicast
```

```
Message statistics:
```

```
Inq depth is 0
```

```
Outq depth is 0
```

	Sent	Rcvd
Opens:	1	1
Notifications:	0	0
Updates:	1	1
Keepalives:	2	2
Route Refresh:	0	0

```
Capability:          0          0
Total:               4          4
Minimum time between advertisement runs is 0 seconds
```

```
For address family: IPv4 Unicast
Update group 1, subgroup 1
Packet Queue length 0
Community attribute sent to this neighbor(all)
0 accepted prefixes
```

```
Connections established 1; dropped 0
Last reset never
Local host: 192.168.2.2, Local port: 34073
Foreign host: 192.168.2.3, Foreign port: 179
Next hop: 192.168.2.3
Next hop global: fe80::2aa:bbff:fe09:2616
Next hop local: fe80::2aa:bbff:fe09:2616
BGP connection: shared network
BGP Connect Retry Timer in Seconds: 10
Estimated round trip time: 10 ms
Read thread: on Write thread: on
```

```
BGP neighbor is 192.168.1.1, remote AS 65536, local AS 65536, internal
link
Hostname: SWITCH-A
BGP version 4, remote router ID 10.0.0.1
BGP state = Established, up for 00:00:05
Last read 00:00:02, Last write 00:00:02
Hold time is 9, keepalive interval is 3 seconds
Neighbor capabilities:
  4 Byte AS: advertised and received
AddPath:
  IPv4 Unicast: RX advertised IPv4 Unicast and received
Route refresh: advertised and received(old & new)
Address Family IPv4 Unicast: advertised and received
Hostname Capability: advertised (name: OLT, domain name: n/a) received
(name:
SWITCH, domain name: n/a)
Graceful Restart Capabilty: advertised and received
Remote Restart timer is 120 seconds
Address families by peer:
  none
```

Graceful restart informations:

End-of-RIB send: IPv4 Unicast

End-of-RIB received: IPv4 Unicast

Message statistics:

Inq depth is 0

Outq depth is 0

	Sent	Rcvd
Opens:	1	1
Notifications:	0	0
Updates:	1	1
Keepalives:	2	2
Route Refresh:	0	0
Capability:	0	0
Total:	4	4

Minimum time between advertisement runs is 0 seconds

For address family: IPv4 Unicast

Update group 1, subgroup 1

Packet Queue length 0

Community attribute sent to this neighbor(all)

0 accepted prefixes

Connections established 1; dropped 0

Last reset never

Local host: 192.168.2.2, Local port: 34073

Foreign host: 192.168.1.1, Foreign port: 179

Nexthop: 192.168.1.3

Nexthop global: fe80::2aa:bbff:fe09:2616

Nexthop local: fe80::2aa:bbff:fe09:2616

BGP connection: shared network

BGP Connect Retry Timer in Seconds: 10

Estimated round trip time: 10 ms

- 路由设备 C: (A 和 B 作为 IBGP 邻居, D 作为 EBGp 邻居)

FRR# show ip bgp neighbors

BGP neighbor is 192.168.1.1, remote AS 65536, local AS 65536, internal link

Hostname: SWITCH-A

BGP version 4, remote router ID 10.0.0.1

BGP state = Established, up for 00:00:05

Last read 00:00:02, Last write 00:00:02

Hold time is 9, keepalive interval is 3 seconds

Neighbor capabilities:

```
4 Byte AS: advertised and received
AddPath:
  IPv4 Unicast: RX advertised IPv4 Unicast and received
Route refresh: advertised and received(old & new)
Address Family IPv4 Unicast: advertised and received
Hostname Capability: advertised (name: SWITCH-C, domain name: n/a)
received (name:
SWITCH-A, domain name: n/a)
Graceful Restart Capabilty: advertised and received
  Remote Restart timer is 120 seconds
Address families by peer:
  none
Graceful restart informations:
  End-of-RIB send: IPv4 Unicast
  End-of-RIB received: IPv4 Unicast
Message statistics:
  Inq depth is 0
  Outq depth is 0

```

	Sent	Rcvd
Opens:	1	1
Notifications:	0	0
Updates:	1	1
Keepalives:	2	2
Route Refresh:	0	0
Capability:	0	0
Total:	4	4

```

Minimum time between advertisement runs is 0 seconds

For address family: IPv4 Unicast
  Update group 1, subgroup 1
  Packet Queue length 0
  Community attribute sent to this neighbor(all)
  0 accepted prefixes

Connections established 1; dropped 0
Last reset never
Local host: 192.168.1.3, Local port: 34073
Foreign host: 192.168.1.1, Foreign port: 179
Nexthop: 192.168.1.1
Nexthop global: fe80::2aa:bbff:fe09:2616
Nexthop local: fe80::2aa:bbff:fe09:2616
BGP connection: shared network
```

BGP Connect Retry Timer in Seconds: 10

Estimated round trip time: 10 ms

Read thread: on Write thread: on

BGP neighbor is 192.168.1.1, remote AS 65536, local AS 65536, internal link

Hostname: SWITCH-B

BGP version 4, remote router ID 10.0.0.2

BGP state = Established, up for 00:00:05

Last read 00:00:02, Last write 00:00:02

Hold time is 9, keepalive interval is 3 seconds

Neighbor capabilities:

4 Byte AS: advertised and received

AddPath:

IPv4 Unicast: RX advertised IPv4 Unicast and received

Route refresh: advertised and received(old & new)

Address Family IPv4 Unicast: advertised and received

Hostname Capability: advertised (name: SWITCH-C, domain name: n/a) received (name:

SWITCH-B, domain name: n/a)

Graceful Restart Capabilty: advertised and received

Remote Restart timer is 120 seconds

Address families by peer:

none

Graceful restart informations:

End-of-RIB send: IPv4 Unicast

End-of-RIB received: IPv4 Unicast

Message statistics:

Inq depth is 0

Outq depth is 0

	Sent	Rcvd
Opens:	1	1
Notifications:	0	0
Updates:	1	1
Keepalives:	2	2
Route Refresh:	0	0
Capability:	0	0
Total:	4	4

Minimum time between advertisement runs is 0 seconds

For address family: IPv4 Unicast

Update group 1, subgroup 1

```
Packet Queue length 0
Community attribute sent to this neighbor(all)
0 accepted prefixes
```

```
Connections established 1; dropped 0
Last reset never
Local host: 192.168.2.3, Local port: 34073
Foreign host: 192.168.2.2, Foreign port: 179
Next hop: 192.168.2.2
Next hop global: fe80::2aa:bbff:fe09:2616
Next hop local: fe80::2aa:bbff:fe09:2616
BGP connection: shared network
BGP Connect Retry Timer in Seconds: 10
Estimated round trip time: 10 ms
Read thread: on Write thread: on
```

```
BGP neighbor is 192.168.3.4, remote AS 65537, local AS 65536, external
link
```

```
Hostname: SWITCH-D
BGP version 4, remote router ID 10.0.0.4
BGP state = Established, up for 00:00:05
Last read 00:00:02, Last write 00:00:02
Hold time is 9, keepalive interval is 3 seconds
Neighbor capabilities:
4 Byte AS: advertised and received
AddPath:
IPv4 Unicast: RX advertised IPv4 Unicast and received
Route refresh: advertised and received(old & new)
Address Family IPv4 Unicast: advertised and received
Hostname Capability: advertised (name: SWITCH-C, domain name: n/a)
received (name:
SWITCH-D, domain name: n/a)
Graceful Restart Capability: advertised and received
Remote Restart timer is 120 seconds
Address families by peer:
none
Graceful restart informations:
End-of-RIB send: IPv4 Unicast
End-of-RIB received: IPv4 Unicast
Message statistics:
Inq depth is 0
Outq depth is 0
```

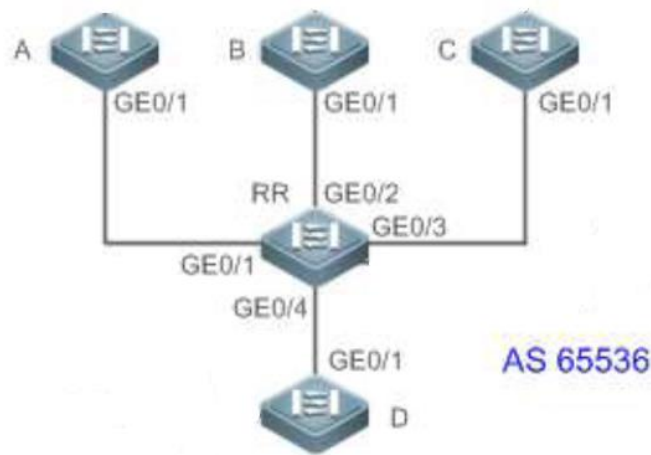


	Sent	Rcvd
Opens:	1	1
Notifications:	0	0
Updates:	1	1
Keepalives:	2	2
Route Refresh:	0	0
Capability:	0	0
Total:	4	4
Minimum time between advertisement runs is 0 seconds		

For address family: IPv4 Unicast  
Update group 1, subgroup 1  
Packet Queue length 0  
Community attribute sent to this neighbor(all)  
0 accepted prefixes

Connections established 1; dropped 0  
Last reset never  
Local host: 192.168.3.3, Local port: 34073  
Foreign host: 192.168.3.4, Foreign port: 179  
Nexthop: 192.168.3.4  
Nexthop global: fe80::2aa:bbff:fe09:2616  
Nexthop local: fe80::2aa:bbff:fe09:2616  
BGP connection: shared network  
BGP Connect Retry Timer in Seconds: 10  
Estimated round trip time: 10 ms  
Read thread: on Write thread: on

6.5.2. 配置路由反射器



各接口所属的 VLAN 和 SVI 的 IP 地址如下所示：（所有路由设备以交换机为例）

A : GE 0/1 VLAN10 192.168.1.1/24

Router ID 10.1.1.1

B : GE 0/1 VLAN20 192.168.2.2/24

Router ID 10.1.1.2

C : GE 0/1 VLAN30 192.168.3.3/24

Router ID 10.1.1.3

D : GE 0/1 VLAN40 192.168.4.4/24

Router ID 10.1.1.4

RR: GE 0/1 VLAN10 192.168.1.5/24

GE 0/2 VLAN20 192.168.2.5/24

GE 0/3 VLAN30 192.168.3.5/24

GE 0/4 VLAN40 192.168.4.5/24

Router ID 10.1.1.5

#### ■ 配置路由设备 A

- 主 CLI: 配置接口 VLAN, 配置对应 SVI 的 IP 地址。

```
SWITCH(config)#vlan 10
```

```
SWITCH(config)#interface gi 0/1
```

```
SWITCH(config-if)#switch access vlan 10
```

```
FRR(config-if)#exit
```

```
SWITCH(config)#int Vlan10
```

```
SWITCH(config-if)#ip address 192.168.1.1/24
```

- FRR CLI:

- ✧ 配置 Router ID。

- ✧ 启动 OSPF。

- ✧ 启动网段的 OSPF, 并指定对应 Area。

- ✧ 启动 BGP 65536。

- ✧ 与 RR 建立 IBGP 邻居

```
FRR#configure terminal
```

```
FRR(config)#router-id 10.1.1.1
```

```
FRR(config)#router ospf
```

```
FRR(config-router)#network 192.168.1.0/24 area 0
```

```
FRR(config-router)#exit
```

```
FRR(config)#router bgp 65536
```

```
FRR(config-router)#neighbor 192.168.1.5 remote-as 65536
```

## ■ 配置路由设备 B

➤ 主 CLI：配置接口 VLAN，配置对应 SVI 的 IP 地址。（省略）

➤ FRR CLI：

- ✧ 配置 Router ID。
- ✧ 启动 OSPF。
- ✧ 启动网段的 OSPF，并指定对应 Area。
- ✧ 启动 BGP 65536。
- ✧ 与 RR 建立 IBGP 邻居

```
FRR#configure terminal
FRR(config)#router-id 10.1.1.2
FRR(config)#router ospf
FRR(config-router)#network 192.168.2.0/24 area 0
FRR(config-router)#exit
FRR(config)#router bgp 65536
FRR(config-router)#neighbor 192.168.2.5 remote-as 65536
```

## ■ 配置路由设备 C

➤ 主 CLI：配置接口 VLAN，配置对应 SVI 的 IP 地址。（省略）

➤ FRR CLI：

- ✧ 配置 Router ID。
- ✧ 启动 OSPF。
- ✧ 启动网段的 OSPF，并指定对应 Area。
- ✧ 启动 BGP 65536。
- ✧ 与 RR 建立 IBGP 邻居

```
FRR#configure terminal
FRR(config)#router-id 10.1.1.3
FRR(config)#router ospf
FRR(config-router)#network 192.168.3.0/24 area 0
FRR(config-router)#exit
FRR(config)#router bgp 65536
FRR(config-router)#neighbor 192.168.3.5 remote-as 65536
```

## ■ 配置路由设备 D

➤ 主 CLI：配置接口 VLAN，配置对应 SVI 的 IP 地址。（省略）

➤ FRR CLI：

- ✧ 配置 Router ID。
- ✧ 启动 OSPF。
- ✧ 启动网段的 OSPF，并指定对应 Area。
- ✧ 启动 BGP 65536。
- ✧ 与 RR 建立 IBGP 邻居

```
FRR#configure terminal
FRR(config)#router-id 10.1.1.4
FRR(config)#router ospf
FRR(config-router)#network 192.168.4.0/24 area 0
FRR(config-router)#exit
FRR(config)#router bgp 65536
FRR(config-router)#neighbor 192.168.4.5 remote-as 65536
```

#### ■ 配置路由设备 RR

➤ 主 CLI：配置接口 VLAN，配置对应 SVI 的 IP 地址。（省略）

➤ FRR CLI：

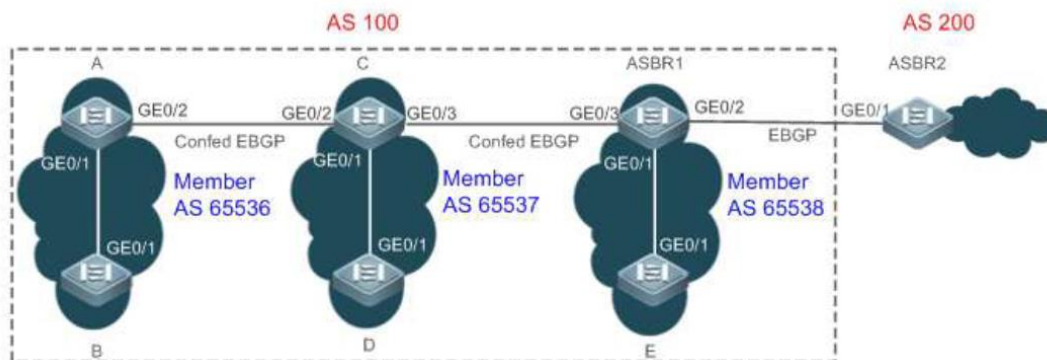
- ✧ 配置 Router ID。
- ✧ 启动 OSPF。
- ✧ 启动网段的 OSPF，并指定对应 Area。
- ✧ 启动 BGP 65536。
- ✧ 与 RR 建立 IBGP 邻居

```
FRR#configure terminal
FRR(config)#router-id 10.1.1.5
FRR(config)#router ospf
FRR(config-router)#network 192.168.1.0/24 area 0
FRR(config-router)#network 192.168.2.0/24 area 0
FRR(config-router)#network 192.168.3.0/24 area 0
FRR(config-router)#network 192.168.4.0/24 area 0
FRR(config-router)#exit
FRR(config)#router bgp 65536
FRR(config-router)#neighbor 192.168.1.1 remote-as 65536
FRR(config-router)#neighbor 192.168.1.1 route-reflector-client
FRR(config-router)#neighbor 192.168.2.2 remote-as 65536
FRR(config-router)#neighbor 192.168.2.2 route-reflector-client
FRR(config-router)#neighbor 192.168.3.3 remote-as 65536
FRR(config-router)#neighbor 192.168.3.3 route-reflector-client
FRR(config-router)#neighbor 192.168.4.4 remote-as 65536
FRR(config-router)#neighbor 192.168.4.4 route-reflector-client
```

#### ■ 配置效果

通过 `show ip bgp neighbor` 查看邻居建立情况。具体过程省略。

### 6.5.3. 配置 AS 联盟



各接口所属的 VLAN 和 SVI 的 IP 地址如下所示：（所有路由设备以交换机为例）

A : GE 0/1 VLAN10 192.168.1.1/24

GE 0/2 VLAN20 192.168.2.1/24

Router ID 10.1.1.1

B : GE 0/1 VLAN10 192.168.1.2/24

Router ID 10.1.1.2

C : GE 0/1 VLAN30 192.168.3.3/24

GE 0/2 VLAN20 192.168.2.3/24

GE 0/3 VLAN40 192.168.4.3/24

Router ID 10.1.1.3

D : GE 0/1 VLAN30 192.168.3.4/24

Router ID 10.1.1.4

E : GE 0/1 VLAN50 192.168.5.6/24

Router ID 10.1.1.6

ASBR1: GE 0/1 VLAN50 192.168.5.5/24

GE 0/2 VLAN60 192.168.6.5/24

GE 0/3 VLAN40 192.168.4.5/24

Router ID 10.1.1.5

ASBR1: GE 0/1 VLAN60 192.168.6.7/24

Router ID 10.1.1.7

## ■ 配置路由设备 A

- 主 CLI：配置接口 VLAN，配置对应 SVI 的 IP 地址。

```
SWITCH(config)#vlan 10
SWITCH(config)#interface gi 0/1
SWITCH(config-if)#switch access vlan 10
SWITCH(config-if)#exit
SWITCH(config)#interface gi 0/2
SWITCH(config-if)#switch access vlan 20
SWITCH(config-if)#exit
SWITCH(config)#int Vlan10
SWITCH(config-if)#ip address 192.168.1.1/24
SWITCH(config-if)#exit
SWITCH(config)#int Vlan20
SWITCH(config-if)#ip address 192.168.2.1/24
```

- FRR CLI：

- ✧ 配置 Router ID。
- ✧ 启动 OSPF。
- ✧ 启动网段的 OSPF，并指定对应 Area。
- ✧ 启动 BGP 65536。（子 ASN 为 65536）
- ✧ 配置联盟的 ASN。（联盟 ASN 为 100）
- ✧ 配置联盟的成员。（即子 ASN 65537）
- ✧ 与 B 建立 IBGP 邻居。
- ✧ 与 C 建立 EBGP 邻居（指定最大跳数为 2）。

```
FRR#configure terminal
FRR(config)#router-id 10.1.1.1
FRR(config)#router ospf
FRR(config-router)#network 192.168.1.0/24 area 0
FRR(config-router)#exit
FRR(config)#router bgp 65536
FRR(config-router)#bgp confederation identifier 100
FRR(config-router)#bgp confederation peers 65537
FRR(config-router)#neighbor 192.168.1.2 remote-as 65536
FRR(config-router)#neighbor 192.168.2.3 remote-as 65537
FRR(config-router)#neighbor 192.168.2.3 ebgp-multihop 2
```

## ■ 配置路由设备 B

- 主 CLI：配置接口 VLAN，配置对应 SVI 的 IP 地址。（省略）

- FRR CLI：

- ✧ 配置 Router ID。
- ✧ 启动 OSPF。

✧ 启动网段的 OSPF，并指定对应 Area。

✧ 启动 BGP 65536。

✧ 与 A 建立 IBGP 邻居。

```
FRR#configure terminal
FRR(config)#router-id 10.1.1.2
FRR(config)#router ospf
FRR(config-router)#network 192.168.1.0/24 area 0
FRR(config-router)#exit
FRR(config)#router bgp 65536
FRR(config-router)#neighbor 192.168.1.1 remote-as 65536
```

#### ■ 配置路由设备 C

➤ 主 CLI：配置接口 VLAN，配置对应 SVI 的 IP 地址。（省略）

➤ FRR CLI：

✧ 配置 Router ID。

✧ 启动 OSPF。

✧ 启动网段的 OSPF，并指定对应 Area。

✧ 启动 BGP 65537。（子 ASN 为 65537）

✧ 配置联盟的 ASN。（联盟 ASN 为 100）

✧ 配置联盟的成员。（即子 ASN 65536, 65538）

✧ 与 D 建立 IBGP 邻居。

✧ 与 A 和 ASBR1 建立 EBGP 邻居（指定最大跳数为 2）。

```
FRR#configure terminal
FRR(config)#router-id 10.1.1.3
FRR(config)#router ospf
FRR(config-router)#network 192.168.3.0/24 area 0
FRR(config-router)#exit
FRR(config)#router bgp 65537
FRR(config-router)#bgp confederation identifier 100
FRR(config-router)#bgp confederation peers 65536 65538
FRR(config-router)#neighbor 192.168.3.4 remote-as 65537
FRR(config-router)#neighbor 192.168.2.1 remote-as 65536
FRR(config-router)#neighbor 192.168.2.1 ebgp-multihop 2
FRR(config-router)#neighbor 192.168.4.5 remote-as 65538
FRR(config-router)#neighbor 192.168.4.5 ebgp-multihop 2
```

#### ■ 配置路由设备 D

➤ 主 CLI：配置接口 VLAN，配置对应 SVI 的 IP 地址。（省略）

➤ FRR CLI：

✧ 配置 Router ID。

✧ 启动 OSPF。

✧ 启动网段的 OSPF，并指定对应 Area。

✧ 启动 BGP 65537。

✧ 与 C 建立 IBGP 邻居。

```
FRR#configure terminal
FRR(config)#router-id 10.1.1.4
FRR(config)#router ospf
FRR(config-router)#network 192.168.3.0/24 area 0
FRR(config-router)#exit
FRR(config)#router bgp 65537
FRR(config-router)#neighbor 192.168.3.3 remote-as 65537
```

#### ■ 配置路由设备 E

➤ 主 CLI：配置接口 VLAN，配置对应 SVI 的 IP 地址。（省略）

➤ FRR CLI：

✧ 配置 Router ID。

✧ 启动 OSPF。

✧ 启动网段的 OSPF，并指定对应 Area。

✧ 启动 BGP 65538。

✧ 与 C 建立 IBGP 邻居。

```
FRR#configure terminal
FRR(config)#router-id 10.1.1.6
FRR(config)#router ospf
FRR(config-router)#network 192.168.5.0/24 area 0
FRR(config-router)#exit
FRR(config)#router bgp 65538
FRR(config-router)#neighbor 192.168.5.5 remote-as 65538
```

#### ■ 配置路由设备 ASBR1

➤ 主 CLI：配置接口 VLAN，配置对应 SVI 的 IP 地址。（省略）

➤ FRR CLI：

✧ 配置 Router ID。

✧ 启动 OSPF。

✧ 启动网段的 OSPF，并指定对应 Area。

✧ 启动 BGP 65538。（子 ASN 为 65538）

✧ 配置联盟的 ASN。（联盟 ASN 为 100）

✧ 配置联盟的成员。（即子 ASN 65537）

✧ 与 E 建立 IBGP 邻居。

✧ 与 C 建立 EBGP 邻居（指定最大跳数为 2）。

✧ 与 ASBR2 建立 EBGP 邻居。

```
FRR#configure terminal
```



```

FRR(config)#router-id 10.1.1.5
FRR(config)#router ospf
FRR(config-router)#network 192.168.5.0/24 area 0
FRR(config-router)#exit
FRR(config)#router bgp 65538
FRR(config-router)#bgp confederation identifier 100
FRR(config-router)#bgp confederation peers 65537
FRR(config-router)#neighbor 192.168.5.6 remote-as 65538
FRR(config-router)#neighbor 192.168.4.3 remote-as 65537
FRR(config-router)#neighbor 192.168.4.3 ebgp-multihop 2
FRR(config-router)#neighbor 192.168.6.7 remote-as 200

```

#### ■ 配置路由设备 ASBR2

- 主 CLI：配置接口 VLAN，配置对应 SVI 的 IP 地址。（省略）
- FRR CLI：
  - ✧ 配置 Router ID。
  - ✧ 启动 BGP 200。
  - ✧ 与 ASBR2 建立 EBGp 邻居。

```

FRR#configure terminal
FRR(config)#router-id 10.1.1.7
FRR(config)#router bgp 200
FRR(config-router)#neighbor 192.168.6.6 remote-as 100

```

#### ■ 配置效果

通过 `show ip bgp neighbor` 查看邻居建立情况。具体过程省略。

## 6.6. 显示命令

通过 `show ip bgp` 和 `show bgp` 是完全等效的。由于内容较多，此章节只介绍命令，不列出显示的详细内容。

#### ■ 显示 BGP 路由信息

- 显示路由概述信息
 

```
show [ip] bgp summary
```
- 显示所有路由信息
 

```
show [ip] bgp [detail]
```
- 显示某个路由信息
 

```
show [ip] bgp A.B.C.D/MASK (bestpath | only-multipath | longer-prefixes)
```
- 显示 CIDR 路由信息（掩码长度非自然掩码长度的路由）
 

```
show [ip] bgp cidr-only
```
- 显示 AS-PATH 属性匹配指定正则表达式的 BGP 路由信息
 

```
show [ip] bgp regexp regular-expression
```

- 显示 BGP 的概述信息  
`show [ip] bgp summary`
- 显示 BGP 的邻居信息
  - 显示所有邻居  
`show [ip] bgp neighbor`
  - 显示某个邻居  
`show [ip] bgp neighbor A.B.C.D`
- 显示 BGP 属性信息  
`show [ip] bgp attribute-info`
- 显示 BGP COMMUNITY 属性  
`show [ip] bgp community (AA:NN|local-AS|no-advertise|no-export|)`
- 显示 BGP COMMUNITY 列表  
`show [ip] bgp community-list (id | name)`
- 显示路由衰减
  - 显示因为路由衰减抑制的路径（路由）  
`show [ip] bgp dampening dampened-paths`
  - 显示路由震荡统计信息  
`show [ip] bgp dampening flap-statistics`
  - 显示路由衰减配置参数  
`show [ip] bgp dampening parameters`
- 显示 filter-list  
`show [ip] bgp filter-list as_path_name`
- 显示 prefix-list  
`show [ip] bgp prefix-list pl_name`
- 显示 route-map  
`show [ip] bgp route-map rm_name`
- 显示 BGP 占用内存统计  
`show [ip] bgp memory`
- 显示下一跳  
`show [ip] bgp nexthop [detail]`
- 显示 BGP 路径信息  
`show [ip] bgp paths`
- 显示对等体组  
`Show [ip] bgp peer-group [PEER_GROUP_NAME]`
- 显示 BGP 通告统计信息

Show [ip] bgp statistics

## 6.7. 清除命令

通过 clear ip bgp 和 clear bgp 是完全等效的。

### ■ 清除对等体

clear [ip] bgp *PEER*

其中 PEER 有如下几种情况：

- \* : 表示所有对等体。
- peer-group: 表示所有对等体组。
- peer-group *pg\_name*: 表示某个特定的对等体组。
- *A.B.C.D*: 用 IP 地址表示某个特定的对等体。
- *ASN*: 表示某个自治系统的所有对等体。取值 1-4294967295。

### ■ 清除最优路径

- 清除所有最优路径

clear [ip] bgp prefix

- 指定前缀清除最优路径

Clear [ip] bgp prefix *A.B.C.D/M*

### ■ 清除衰减路由

- 清除所有衰减路由

clear [ip] bgp dampening

- 指定前缀清除衰减路由

clear [ip] bgp dampening *A.B.C.D/M*

### ■ 软复位对等体

具体参见前文关于软复位的说明。

- 同时软复位 in 和 out

clear [ip] bgp *PEER* soft

- 软复位 in

Clear [ip] bgp *PEER* [soft] in

- 软复位 out

clear [ip] bgp *PEER* [soft] out

其中 PEER 有如下几种情况：

- \* : 表示所有对等体。
- peer-group: 表示所有对等体组。
- peer-group *pg\_name*: 表示某个特定的对等体组。
- *A.B.C.D*: 用 IP 地址表示某个特定的对等体。
- *ASN*: 表示某个自治系统的所有对等体。取值 1-4294967295。

**■ 软复位最优路径**

具体参见前文关于软复位的说明。

- 同时软复位 in 和 out

```
clear [ip] bgp prefix [A.B.C.D/M] soft
```

- 软复位 in

```
Clear [ip] bgp prefix [A.B.C.D/M] [soft] in
```

- 软复位 out

```
clear [ip] bgp prefix [A.B.C.D/M] [soft] out
```

**■ 软复位衰减路由**

具体参见前文关于软复位的说明。

- 同时软复位 in 和 out

```
clear [ip] bgp dampening [A.B.C.D/M] soft
```

- 软复位 in

```
Clear [ip] bgp dampening [A.B.C.D/M] [soft] in
```

- 软复位 out

```
clear [ip] bgp dampening [A.B.C.D/M] [soft] out
```