

在路由协议 A 中将一个接口使用 **Network** 语句宣告进协议 A, 会实现该接口对于该协议报文的收发

收：邻居传递过来的所有路由条目

发：该路由器所有被宣告进协议 A 的接口 C 路由，以及通过这些接口获悉的邻居传递过来的属于该协议的并且被加入路由表的路由。

静态路由第二种用途，路由过滤

在 DV 协议环境中使用静态路由覆盖通过 DVIGP 获悉的动态路由条目可以实现该路由条目的传递过滤，在 LSIGP，静态路由无法实现路由过滤。

```
ip route 1.1.1.0 255.255.255.0 fastEthernet 0/0 12.1.1.1
```

对于 PC，如果该设备收到了路由器传递的 Proxy ARP replay，则该 PC 会无条件信任这个 Reply，并且将其加入 ARP 表中。

对于路由器，如果该设备收到了 proxy-Arp replay，则该路由器会优先判断该 replay 中应答者 IP 地址所在的网段是否可达，如果是，则接受，如果不是，则直接丢弃。

Rip 特性

#### 1. 自动汇总

当启用 RipV1 的时候，自动汇总是默认开启的，并且无法关闭，当启用自动汇总之后，路由器将下述两类路由进行自动汇总发送

该路由的本地路由

通过邻居获悉的 Rip 路由

#### 2. 手工汇总

对于 RipV2 而言，当配置手工汇总的时候需要在尽可能接近控制层面路由始发源的发送路由条目的出借口进行配置

```
R1: (config-if) #ip summary-address rip 1.1.0.0 255.255.255.0
```

当配置了手工汇总之后只要该路由器要通过该接口发送该汇总路由条目的明细路由的时候，那么此时明细路由被抑制，汇总路由被发送

当汇总路由条目内的所有明细路由条目都 Down 的时候，汇总路由才会消失，如果汇总路由条目内的所有明细路由条目的 Metric 值不同，那么汇总后的路由条目会启用最小的 Metric 值作为本身的 Metric

Rip 使用手工汇总形成汇总路由并通告给邻居之后本地路由表不会产生一条前缀掩码同该汇总路由一致并且指向 Null0 接口的放环路由。

当在一台路由器上即开启手工汇总又开启自动汇总的时候，自动汇总的优先级高于手工汇总，Rip 的汇总原则是先考虑是否将路由发送，再考虑是否汇总。

Rip 特性 3：像 Rip 域内注入缺省路由

1: 在 AS 的出口路由器上配置一条 0.0.0.0/0 的缺省静态路由指向外网，并且在该路由器上将这条缺省路由重分发进 RIP 进程

```
R1 (config) #ip route 0.0.0.0 0.0.0.0 fastEthernet 0/0 15.1.1.5
```

```
R1 (config) #router rip
```

R1 (config-router) # redistribute static

该方式的局限性是园区网内网的标远路由器访问外网也只能通过缺省路由

方式 2: 在 AS 的出口路由器上配置一条 0.0.0/0 的只关联出站接口的缺省静态路由, 并且在该路由器的 rip 进程中, 使用 network 0.0.0.0 将该缺省路由引入 Rip 域

R1 (config) # ip route 0.0.0.0 0.0.0.0 fastEthernet 0/0

R1 (config) # Router rip

R1 (config-router) # network 0.0.0.0

包含的第一层概念就是将本路由器的所有接口都宣告进 Rip 进程, 并且将该路由器本地拥有一条 0.0.0.0/0 并且只关联出站接口的静态路由时, 该命令也会讲该缺省路由以 rip 更新的形式通告。

方式 3 =在 AS 的出口路由器上通过一条 ip default-network 命令向域内注入缺省路由

R1 (config) # ip default-network 15.0.0.0

该方式的优势是, 出口路由器访问外网既可以使用缺省路由又可以由 BGP 使用明细路由

方式四

在 AS 的出口路由器上通过进程内的一条命令 default-information originate

R1 (config) # router rip

R1 (config-router) # default-information originate

Rip 特性 4: 被动接口

R1 (config-router) # passive-interface loopback 0

当将一个接口置为被动接口后, 该接口不会主动的向外发送任何的 rip 组播或广播更新, 但是该行为不会影响该路由器其他被动宣告进 rip 的接口通告该被动接口的直连网段路由, 以及该接口接收到的假如路由表的 Rip 路由

当把一个接口置为被动接口之后, 该接口可以接受组播, 广播以及单播的 Rip 报文, 该接口只能发送单播的 Rip 报文, 但是不能发送组播和广播的 Rip 报文

Rip 特性 5: 单播更新

R1 (config-router) # neighbor 123.1.1.2

特性 4 和特性 5 联合使用可以实现 Rip 的纯单播更新, 一般该情况出现在 MA 网段

Rip 特性 6

使用广播发送 RipV2 的更新

R1 (config-if) # ip rip v2-broadcast

特性 7

兼容性开关

R3 (config-if) # ip rip receive version 1 2

R3 (config-if) # ip rip send vesion 1 2

## 特性 8

### Rip 认证

#### 明文认证

R1 (config) # key chain R1 该钥匙链的名称值具有本地意义

R1 (config-Keychain ) # key 10

R1(config-Keychain -key)# key -string Cisco

R1(config-if) # ip rip authentication mode text

R1(config-if) # ip rip authentication key -chain R1

建议在路由器的物理接口开启认证，使用认证的时候需要注意，认证是基于网段的概念，建议在同一个网段内的所有路由器接口启用相同的认证类型，调用相同的密钥，但是在不同的网段间，认证的类型以及密钥没有必要相同

#### 密文认证

R3(config-if) # ip rip authentication mode md5

R3(config-if) # ip rip authentication key-chain R3

依然无需优先定义钥匙链，在调用的接口，第一语句的 mode 改为 md5

## 特性 9

### Offset-list

R1(config-router)# offset-list 10 out 2 fastEthernet 0/1

偏移列表可以调用标准 ACL 精准的命中路由条目后修改其度量值发送

R2 (config-router) # offset-list 0 in 1

当偏移列表既没有调用 ACL 又没有调用接口的时候能为所有接口接收到的所有 RIP 路由表修改度量值。

## 特性 10

### 关闭 RIP 的水平分割

R1 (config-subif) # no ip split-horizon 一般建议在 FR 的 Hub 节点关闭多点子接口的水平分割

## Rip 特性 11

### 关闭 Rip 的更新源检测

当一台路由器接收到了一个 RIP 更新，该路由器会优先查看该更新报文的 3 层报头中的源 IPV4 地址，并判断该地址和接收的 IP 地址是否在同一个 IP 子网段内，如果在，那么更新报文被接受，如果不在，该报文被丢弃

R1 (config-router) # no validate-update-source，使用该命令关闭一台路由器的 RIP 更新源检测功能。

## RIP 特性 12 修改 RIP 报文间延迟

R2 (config-router) # output-delay 25 定义报文间的延迟为 25ms

## Circuit on demand

按虚电路

特性 13

纯触发更新

该特性只能在 WAN 链路启用，目的是让 WAN 链路两端只发送出发更新，不发送周期性的更新，为 WAN 链路提供优化，当配置的时候需要在 WAN 链路两端同时开启该特性，基于这个特性链路两端的节点会建立一个纯触发更新的高级连接关系，建立完毕后周期性的更新就停止了，仅当拓扑出现了改变影响到路由表的时候，才会回复发送周期性更新。

## EIGRP 向域内注入缺省路由 4 种

1. 在 AS 边界路由器上使用一条缺省的全 0/0 路由指向运营商端设备（外网），在其 EIGRP 进程中用路由重分发（redistribute static）将该缺省路由以 EIGRP 路由形式引入 EIGRP 域发送给其他 EIGRP 路由（为外部路由，AD=170）

```
R1(config)#ip route 0.0.0.0 0.0.0.0 fa0/0 14.1.1.4
R1(config)#router eigrp 90
R1(config-router)#redistribute static
```

2. 在 AS 边界路由器指定一条全 0/0 并且只关联出站接口的静态路由，并在该路由器的 EIGRP 进程中

使用 Network 0.0.0.0，将该路由引入 EIGRP 域（对于 EIGRP 而言 Network 0.0.0.0 等同 RIP）

```
R1(config)#ip route 0.0.0.0 0.0.0.0 fasterEthernet 0/0
R1(config)#router eigrp 90
R1(config-router)#network 0.0.0.0
```

3. 在 AS 边界路由器指定 ip default-network+主类地址段（该路由器连接外网接口的地址所属的主网段）；在该路由器上创建该主类路由；在该路由器 EIGRP 进程中 network 该主类地址段。

```
R1(config)#ip default-network 14.0.0.0
R1(config)#ip route 14.0.0.0 255.0.0.0 fa0/0 14.1.1.4
R1(config-router)#network 14.0.0.0
```

4. 在 AS 边界路由器连接内网接口的通过使用路由聚合实现缺省路由的下放

```
R1(config)#int fa0/1
R1(config-if)#ip summary-address eigrp 90 0.0.0.0 0.0.0.0
```

Eigrp 的自动汇总规则如同 RipV2，不同的是，EIGRP 仅仅支持将本地路由汇总不会将邻居传递过来的路由汇总。

EIGRP 管理距离 内部 90 外部 170 防环路由 Null0 5（只有本地意义）

手工汇总：

自动汇总只能汇总本地产生路由，不能汇总邻居传递来的路由，而手工汇总可以邻居传递的条目进行汇总

手工汇总的路由器，其自身也会产生该条汇总路由，下一跳指向 NULL 接口，是为避免环路

无论收到内部路由或外部路由，发送时总是内部路由

靠近源，控制层面发送路由条目的出接口进行路由汇总配置

Conf t

Interface fa 0/1

Ip summary-address eigrp 90 192.168.8.0 255.255.252.0

EIGRP 支持超网宣告

**Leak-Map**: 该工具用来放行手工汇总条目内的某些明细路由条目

**Route-Map**: 在该例子中用来调用 ACL 抓取控制层面需要被放行的明细路由条目

**ACL**: 直接用来抓取路由条目

Conf t

Int fa 0/1

Ip summary-address eigrp 90 192.168.8.0 255.255.252.0 leak-map TEST 调用 Router-map

Conf f

Access-list 10 permit 192.168.8.0 0.0.1.0

Route-map TEST permit 10 调用 ACL

Match ip address 10 调用 ACL

Leak-map 调用 Route map 调用 ACL 抓取明细路由

手工汇总能够汇总本地路由和邻居传递来的路由，都是打 D，可以修改 Null0 放环路由管理距离，支持 Leak-Map

EIGRP Load Balancing

Equal-cost load balancing

值为 1 只支持等价，默认 4，最大 16

Unequal-cost load balancing

R1(config-router)#**variance 3** 缺省值为 1，取值 1-128，非等价一定要大于等于 2

delay 改的值直接是 10 的负 5 次方秒

Configuring WAN Links

EIGRP 默认最多占用接口可用带宽的 50%，若配置了管理带宽，使用管理的 50%

R1(config-router)#bandwidth 100000

R1(config-router)#ip bandwidth-percent eigrp 90 10 占用 10%带宽

## EIGRP Diffusing Update Algorithm

### 1. FC

### 2. DUAL

当一台运行 EIGRP 的路由器通过其邻居收到了一个 **query** 报文，假定对于该接收者路由器，发送查询的路由器对于该路由器而言不是该路由器的后继站，该路由器会直接将路由表中的后继站路由以 **reply** 的形式发给查询者。后继站（最优路由下一条邻居就是关于这条条目的后继站，即下一跳路由器）。可行后继站（备份路由的下一跳路由器）

假定对于该接收者路由器，发送查询的路由器对该路由而言是路由的后继站，则该路由器会判定自己本地拓扑表内是否拥有关于该路由的备份路由（可行后继站路由），如果有，则该路由器会优先更新本地路由表，将最优路由切换为可行后继站路由，并且将该路由器以 **reply** 的形式发给查询者，若没有则该路由器会判断自己是否拥有除查询者之外的其他 EIGRP 邻居，若有邻居，则该路由器会将拓扑表内该路由条目置为 **Active** 并且欠着查询者的查询报文，转而发送查询给其他的 EIGRP 邻居。若该路由器并没有其他的 EIGRP 邻居，则该路由器会直接将拓扑表以及路由表中关于该路由的信息删除，并且直接发送 **reply** 给查询者告知该路由不可达。

假定接收者到查询的路由器在接收查询之前本地路由表和拓扑表内均没有该被查询路由，则该路由器会直接向查询者发送 **Reply** 告知该路由不可达

## 限制查询包发送

### 1.手工汇总

### 2.EIGRP Stub 终结

R1(config-router)#eigrp stub

Router eigrp 90

Redistribute rip metric 1000 100 255 1 1500

带宽 延迟 可靠性 负载 MTU

## 最底层 ACL

Config t

Access-list 10 permit 3.3.3.0 0.0.0.0

Route-map STUB permit 10

Match ip address 10

Exit

Router Eigrp 90

Eigrp stub leak-map STUB

中层 Route-Map

最高层 Leak-Map

EIGRP STUB 参数

EIGRP Stub 后面跟的 summary 是让该路由器只能发送!本地汇总产生的路由  
summary 参数能发送该路由器汇总的本地路由和邻居发送过来的路由（只要是他汇总的）

static 参数是由静态重分发进 EIGRP 路由中

```
R1(config-router)#redistribute static
```

redistributed 与 connected summary 一起的

会将所有重分发进 EIGRP 进程的外部路由都通告给其他路由器

```
R1(config-router)#redistribute rip metric 10000 100 255 1 1500
```

receive-only 只收不发

leak-map

```
R1(config)#access-list 10 permit 3.3.3.0 0.0.0.0 （全 0 可不写）
```

```
R1(config)#route-map AAA permit 10
```

```
R1(config-route-map)#match ip address 10
```

```
R1(config-router)#eigrp stub leak-map AAA
```

### 重置邻居方式

3 倍 HELLO 时间

16 次重传

Active timer

重传实验:

R1:

```
R1(config)#access-list 100 deny 88 host 12.1.1.2 host 12.1.1.1
```

```
R1(config)#access-list 100 deny 88 host 12.1.1.2 host 224.0.0.10 (deny 组播)
```

```
R1(config)#access-list 100 permit ip any any
```

```
R1(config)#int fa0/1
```

```
R1(config-if)#ip access-group 100 in
```

R2:

```
R2(config-router)#no network 2.0.0.0
```

```
R2(config-router)#no network 23.1.1.2
```

```
R2(config)#int fa0/0
```

```
R2(config-if)#shutdown
```

```
R2#debug eigrp packets
```

```
R2(config)#int fa0/0
```

```
R2(config-if)#no shutdown
```

由 debug 看出 16 次重传失败: retry

EIGRP 建立邻接关系条件 4 点

1.同 AS 号

2.不同 RID

3.相同 K 值（K1-K5，用于决定 EIGRP 计算路由的度量值所使用参数的公式: show ip pro）

```
R2(config-router)#metric weights 0 K1 K2 K3 K4 K5
```

#### 4.相同认证

修改 hello， HELLO 时间不同不影响

```
R2(config-if)# ip hello-interval eigrp 90 8 通过 show run int fa0/0 看这条命令
```

```
R2(config-if)# ip hold-time eigrp 90 24 建议 holdtime 为 hello 3 倍
```

一端的 hello 要比对端 hold 时间要小

改 active time

```
R1(config-router)#timers active-time 1 (单位分钟)默认 180S, disable 为禁用, 导致不会 Dwon  
邻居, 勿用
```

明文认证: IS-IS ; OSPF ;RIPv2

MD5 认证: OSPF ; RIPv2 ;BGP ;EIGRP ;ISIS(后期支持)

钥匙链认证:

R1:

```
R1(config)#key chain R1 钥匙链为本地意义
```

```
R1(config-keychain)#key 1 (key、key-string 一致) 密钥 ID,
```

```
R1(config-keychain-key)#key-string CISCO
```

```
R1(config)#int fa0/1
```

```
R1(config-if)#ip authentication key-chain eigrp 90 R1 (定义密钥)
```

```
R1(config-if)#ip authentication mode eigrp 90 md5 (开启认证)
```

R2:

```
R2(config)#key chain R2
```

```
R2(config-keychain)#key 1
```

```
R2(config-keychain-key)#key-string CISCO
```

```
R2(config)#int fa0/0
```

```
R2(config-if)#ip authentication key-chain eigrp 90 R2
```

```
R2(config-if)#ip authentication mode eigrp 90 md5
```

一个钥匙链若有多把密钥，基于 key id 排序，从小到大，默认发送 ID 最小的

R1 给 R2 发送密钥审核报文(ID 最小的)，R2 逐一认证

```
R2(config-keychain-key)#key-string text
```

```
R2(config-keychain-key)#accept-lifetime start-time {infinite | end-time | duration seconds} 审  
核时间
```

```
R2(config-keychain-key)#send-lifetime start-time {infinite | end-time | duration seconds}
```

高级特性:

1.修改度量值:

(1) 改延迟和带宽

(2) 偏移列表 (用于精确增加路由条目的度量值)



可以出、入接口做

```
R2(config)#access-list 10 permit 3.3.3.0
```

```
R2(config)#router eigrp 90
```

```
R2(config-router)#offset-list 10 out 600 fa0/0 (不加 10 对所有 ACL 生效, 可不加 fa0/0)
```

```
R2#clear ip route *
```

```
R1#show ip route
```

2.被动接口 (节约资源, 避免将环回口、PC 的网段宣告进路由)

```
R1(config)#router eigrp 90
```

```
R1(config-router)#passive-interface fa0/1
```

置为被动接口后, 不能发送和接收任何方式的 EIGRP 报文, 将不能建立任何邻接关系

3.单播发送 (FR 环境—伪广播报文)

```
R1(config-router)#neighbor 12.1.1.2 fa0/1 邻居接口的地址 | 本地连邻居的接口
```

要邻居双方都开启单播

```
R2(config-router)#neighbor 12.1.1.1 fa0/0
```

4.关闭 EIGRP 水平分割 (FR 环境) 与 RIP 不同: 需关闭逻辑

```
R1(config)#int fa0/1
```

```
R1(config-if)#no ip split-horizon (RIP 到此即可)
```

```
R1(config-if)#no ip split-horizon eigrp 90
```

## OSPF

1.IGP 支持中大型网络

2.LS, 不发路由, 发更新(LSA)

3.无类, VLSM/CIDR

4. L2-> IPv4-> OSPF-> FCS

89-三层报头的上层协议号, 非端口号

224.0.0.5 224.0.0.6

7 级邻接关系

OSPF 的 COST 即 Metric

neighbor table-adjacency database

topology table-LSDB

routing table

## LS Routing Protocols

1.收集更多信息比 DV

2.一个 AS 内的每台 R 关于这个区域内的整网拓扑都有相同的信息

3.转发作出更精确的决策, 无环

LS 协议 structure network hierarchy

2 类区域

—transit area(backbone or area 0)  
—regular areas(nonbackbone areas)  
单区域可以非 area0，区域划分基于接口

OSPF area characteristics:

- Minimizes routing table entries 通过汇总实现
- Localizes impact of a topology change within an area
- Detailed LSA flooding stops at the area boundary
- Requires a hierarchical network design

OSPF 无域间汇总，只能域内和域外汇总，原因是只能对包含纯路由信息的进行汇总  
LSA 基于泛洪机制传递  
划分区域实现优化

backbone routers make up area 0

ABR: area border router 亦是 backbone router

ABRs attach all other areas to area 0

OSPF Adjacencies

5 hello packets 三层直接为邻居，建立七层关系叫邻接—Adjacency

- P to P WAN links:
  - both neighbors become fully adjacent
- LAN links:
  - Neighbors form a full adjacency with the DR and BDR
  - DROTHERs two-way state
- 路由器间只有建立完全邻接关系后才能交互更新
- once an adjacency is formed, LSDBs are synchronized by exchanging LSAs
- LSAs are flooded reliably throughout the area(or network)

OSPF Calculation

Dijkstra

- 域内每台 R 有完全一致的 LSDB
- 每台 R 把自己作为 ROOT 计算路径
- 计算路径使用分段带宽， $COST, 10^8/BW(\text{bit/s})$ -每段累加
- 最优路由条目放入路由表中来转发

LSA Operation

LSA 30min 重发一次，

Aging-time

Sequence no. 0x80000001 min  
0x7FFFFFFF max

OSPF Packet

1.hello 10s / 30s × 4 时间取决于接口 OSPF 网络类型

- 2.database description          DBD 包含所有 LSA 报头  
使用 隐式确认
- 3.link-state request          LSR  
使用 显式确认 用 LSU 确认
- 4.link-state update          LSU 包含完整的 LSA  
使用 LSack 确认，基于每条 LSA 来确认
- 5.link-state acknowledgment    LSack

## OSPF 两大确认机制

显式确认：收到可靠报文，用单独报文回复

隐式确认（基于序列号的）：使用相同报文回复，相同的序列号

## OSPF Packet

Version- Type- Packet-RouterID-AreaID-Check-Authentication-Authentication-Data

Number          Length          sum    Type

V3 对于 IPv6

type 描述哪类报文对应 12345 个值

RID：用来标识一台路由器；标识发送的 LSA（为 EIGRP 所不能）

- 1.手工配置
- 2.在所有状态为 UP 的环回口中选最大 IP 地址
- 3.物理接口最大的 IP 地址（UP 的）

## Authentication

3 级认证级别

0—不认证；1—明文；2—密文

## Data

Hello 报文中打\*的均为必要条件

\*相同的 Hello 时间和 Dead 时间（EIGRP 没这条）

\*相同 Area ID

\*相同认证类型与密钥

\*若把一非骨干 Area 部署为特殊 Area，Area 内所有路由器要把 Area 部署为相同 Area 类型

## 邻接建立过程

7 个状态

- 1: Down          初始状态，接口被宣告进 OSPF，未发送任何报文
- 2: Init          通过接口发送一份 HELLO
- 3: Two-Way      通过接口收到一份 Neighbor 字段包含自身的 RID 的 Hello
- 4: Exstart      交互 3 个不带 LSA 报头(First)的 DBD 选择 Master/Slave
- 5: Exchange    由 Master 发起的带有 LSA 报头的 DBD 信息交互
- 6: Loading      交互 LSR、LSU 以及 LSack 实现 LSDB 的同步

7: Full                    一旦同步，邻接关系到达 Full

P2P:

MA: two-way

DBD 中 Flag 位: I->M->M/S, 初始 111->0x7

Exstart 中 3 个 DBD 选 M/S, 两台 R 的 MTU 不一致可能一直卡在 Exstart 状态

Area 0 = 0.0.0.0

1 = 0.0.0.1

255 = 0.0.0.255

256 = 0.0.1.0

Show ip ospf interface

实验一邻接

R1->R2->R3

串口连接点到点网段，无优先级

```
R1:      lo0: 1.1.1.1
        s1/1:12.1.1.1
        R1(config)#router ospf 110
        R1(config-router)#router-id 1.1.1.1
        R1(config-router)#network 1.1.1.1 0.0.0.0 Area 0.0.0.1
        R1(config-router)#network 12.1.1.1 0.0.0.0 Area 0.0.0.1
```

```
R2:      lo0:2.2.2.2
        s1/0:12.1.1.2
        s1/1:23.1.1.2
        R2(config)#router ospf 11 (不同进程号不影响邻接)
        R2(config-router)#router-id 2.2.2.2
        R2(config-router)#network 2.2.2.2 0.0.0.0 Area 1
        R2(config-router)#network 12.1.1.2 0.0.0.0 Area 1
        R2(config-router)#network 23.1.1.2 0.0.0.0 Area 1
```

```
R3: lo0:3.3.3.3
    s1/0:23.1.1.3
    R3(config)#router ospf 1
    R3(config-router)#router-id 3.3.3.3
    R3(config-router)#network 3.3.3.3 0.0.0.0 Area 1
    R3(config-router)#network 23.1.1.3 0.0.0.0 Area 1
```

Show ip ospf interface (brief)

邻接建立过程:

```
R1(config)#int s1/1
R1(config-if)#shutdown
R1#debug ip ospf packet
R1#debug ip ospf adj
```

```
R2(config)#int s1/1
R2(config-if)#shutdown
R2(config)#int s1/0
R2(config-if)#shutdown
R2#debug ip ospf packet
R2#debug ip ospf adj
R2(config)#int s1/0
R2(config-if)#no shutdown
```

无视 MTU

```
R1(config)#int s1/1
R1(config-if)#mtu 1492
R1#clear ip ospf process 选 yes
R1#show ip ospf neighbor 看到状态卡在 extart 上
R1(config)#int s1/1
R1(config-if)#ip ospf mtu-ignore 建议链路两端都 ignore
```

改 Hello 时间

```
R1(config-if)#ip ospf hello-interval 12
R1#clear ip ospf process 选 yes
R1#show ip ospf int s1/1 发现 Dead 和 Wait 时间自动改为其 4 倍 (EIGRP 不能)
```

```
R2(config)#int s1/0
R2(config-if)#ip ospf dead-interval 48
R2#show ip ospf int s1/0 发现 hello 时间未自动改
R2(config-if)#ip ospf hello-interval 12 邻接恢复
```

```
R1#show ip route
```

只要把一环回口宣告进 OSPF, 不管其本身配置的环回口掩码多少位, 都会以 32 位主机路由通告出来, 优化路由传递  
如果要恢复/24 使用命令

```
Conf t
Int loopback 0
Ip ospf network point-to-point
```

在 MA 网段建立 OSPF 邻接关系时 DR 和 BDR 的选举原则

1: 参与该 MA 网段的路由接口的 OSPF 优先级, 越高越好(0-255), 默认 1

2: 该 MA 网段所连接的路由器的 RID, 越高越好

wait 40s/120s-选举时间, 根桥实时选举

MA 网段内, 第一台到达 2-way 邻接关系的路由器会立即宣布选举开始, 此为 wait 倒计时, 选完后, DR/BDR 身份固定了

\* OSPF MA 网段接口的 OSPF 优先级如果值为 0, 代表的不是最小优先级, 而是该接口没有资格在此网段参选 DR 与 BDR, 只能成为 DROther

FR 环境: Hub->DR, 没 BDR

修改优先级

Conf t

Int fa 0/1

Ip ospf priority 10

特点

1.DR 和 BDR 无法被抢占

2.DR 挂了 BDR 会立即抢占成为新的 DR, 而新的 BDR 通过在所有 DROther 之间重新选举得出

3.DR 和 BDR 是基于接口的概念, 每个 MA 网段的 DR 和 BDR 都是通过相同的机制单独选出的

4.在 Ethernet 环境中建议拥有 DR 和 BDR 实现备份, 而在 FR 环境: 只能是 Hub 节点成为 DR, 任何 Spoke 结点都不能成为 DR 或 BDR

5.如果一个 MA 网段没有 DR 和 BDR, 没有任何邻接关系存在也不会有任何 LSA 的传递

一台运行 OSPF 的路由器, 只要在一个接口开启 OSPF 进程, 则该接口会立即监听发往 224.0.0.5 的组播组流量, 而仅当一个节点成为 DR 或 BDR 时, 该接口才会同时监听发往 224.0.0.5 和 224.0.0.6 的组播组流量。

在一个 MA 网段内, 所有路由器发送给 DR 和 BDR 的报文的目的地址都是.6, 而 DR 将 LSA 整合之后以.5 的地址发送给网段内所有其他的路由器。

OSPF

设计区域之好处:

1.限制 LSA 传递, 节约其他区域内 R 关于非本地区域路由信息的精简

2.当一区域内链路出问题时, 只影响到区域内 R

3

建议

1.一个 ABR 最多关联 3 个区域

2.一个区域内最多 50 台 R

3.对于一 OSPF 的 R, 其邻接状态的邻居最多 60 台

ASBR

## LSA Type

### T1. Router LSAs

- 每台 R 会为他所连接的每个区域生成一条 1 类 LSA （LSA 纯拓扑信息）
  - 1 台 R 无论一区域内多少接口，只发一条。
  - 描述该 R 的所有直连的链路
  - 这些链路的前缀、掩码及类型
- 每条 1 类 LSA 都有唯一标识符
- Floods within its area only; doesn't cross ABR

实验：

R1: lo0:1.1.1.1  
s1/1:12.1.1.1

R2: lo0:2.2.2.2  
s1/0:12.1.1.2

show ip ospf database

一台 1 类 LSA 的通告者 R 的标识是通告该 LSA 的 R 的 RID，唯一标识符也是 RID

show ip ospf database router

把一个串口宣告进 OSPF 进程，会在 LSA 中形成关于这条串行链路形成两条路径信息，一条为 Point to Point, 另一条为 Stub 末节网络信息，看到串行接口，数量减 1

### 1.Router LSA

传播范围：只能在一个 Area 内传递，不能穿越 ABR

通告者：每台属于一个 Area 的 R 都会基于该 Area 通告一条 1 类 LSA

包含内容：拓扑信息，描述该路由器所有宣告进该 Area 直连接口的链路的的前缀，掩码，链路类型，度量值

Link-ID:通告该 LSA 的 R 的 RID

ADV Router:通告该 LSA 的 R 的 RID

### 2.Network LSA

传播范围：只能在一个 Area 内传递，不能穿越 ABR

通告者：MA 网段中的 DR

包含内容：纯拓扑信息，包含该 MA 网段直接的所有 Rrouter 的 RID 信息，该 MA 网段的掩码

Link-ID:该 MA 网段 DR 接口的 IP 地址

ADV Router:该 DR 的 RID

\*注：在 OSPF 中，关于一个区域内的 R，所获悉的非直连 MA 网段的路由是同时通过 1 类和 2 类 LSA 加一起才能获悉的

### 3.Summary Network LSA

传播范围：除了该区域外的整个 OSPF 路由选择域

通告者：ABR

包含内容：一条 3 类 LSA 包含一条 OSPF 域间路由，O IA

Link-ID: 3 类 LSA 路由的前缀

ADV Router: ABR 的 RID

为了实现 3 类 LSA（域间路由）可达，接收到 3 类 LSA 的 R 一定要知道通告者在哪，故 3 类 LSA 在域内传递的时候，每经过一个 ABR，其 ADV Router 都会自动被改写为该 ABR 的 RID

### 4.Summary ASB LSA

传播范围：除了 ASBR 所在区域之外的整个路由选择域

通告者：和 ASBR 在同一个区域的 ABR 路由器

包含内容：纯拓扑信息，描述了 ASBR 所在位置

Link-ID: ASBR 的 RID

ADV Router: 通告者 ABR 的 RID，并且该值每路跨越一个 ABR 都会自动改变，同 3 类 LSA

### 5.External LSA （通过重分发引入的 LSA）

传播范围：整个 OSPF 路由选择域

通告者：ASBR

包含内容：纯路由信息，一条 OSPF 域外路由对应一条 5 类 LSA

Link-ID: 域外路由的路由前缀

ADV Router: ASBR 的 RID，该 LSA 在 OSPF 域内传递的时候，ADV Router 不会发生任何改变

EIGRP 重分发进 OSPF:

R4(config)#router ospf 110

R4(config-router)#redistribute eigrp 90 subnets

显示边界路由：show ip ospf border-routers

Seed Metric（OE2）:种子度量值。对于 OSPF 而言如果将 BGP 路由重分发进入，则值为 1，所有其他外部路由缺省值为 20

### Summary

域间汇总：需在 ABR 上部署，实现对 3 类 LSA 的汇总传递

域外汇总：需在 ASBR 上部署，实现对 5 类 LSA 的汇总传递

域间路由汇总：会生成 Null0

R1(config-router)#area 0 range 202.10.8.0 255.255.252.0 在所有 ABR 上做

R2(config-router)#area 0 range 202.10.8.0 255.255.252.0



域外汇总 会生成 Null0

Conf t

Router ospf 110

Summary-address 192.168.8.0 255.255.252.0

OSPF LSDB Overload Protection 12.4 以上能部署，性能较差，收到大量 LSA，LSDB 过大，这样可以不接收到过多的 LSA

R4(config-router)#max-lsa 50 最大 50 条

修改度量值：

R4(config-if)#ip ospf cost

改分子大小（对于大带宽）

R4(config-router)#auto-cost reference-bandwidth 10000 （单位： Mbit/s）

在所有 R 上改

ip prefix-list 10 seq 10 deny 202.10.8.0/23 ge 24 le 24

ip prefix-list 10 seq 10 permit 0.0.0.0/0 le 32

router ospf 110

area 1 filter-list prefix 10 in

OSPF Special Area:

OSPF 建立邻居

- 1 相同 Hello Dead 时间
- 2 直连接口属于相同区域
- 3 相同认证类型和密钥
- 4 相同的末节网络标示
- 5 相同的 MTU
- 6 相同的网络类型

\* STUB

- 建议一个区域内只有一个 ABR
- 当把一个区域部署为 Stub 区域时，保证此 Area 内所有 R 都把此 Area 同时部署为 Stub 区域
- 当把一个区域部署为 Stub 区域时，此 Area 内不能包含 ASBR
- 此 Area 不能为 Area 0
- 此 Area 内不允许虚电路（即边上不能连接其他区域）

Stub 区域实现 2 点

- 1.外部过来的 5 类 LSA 当想进入区域 1 时，此 Area 的 ABR 会把 5 类 LSA 直接丢弃，同时过滤 4 类 LSA
- 2.ABR 会主动向区域内 R1.R2 下放一条缺省路由，到达 R1.R2 后，拥有一条指向 R3dr

如果将一个 OSPF 区域部署为 Stub，该区域的 ABR 会将入区域方向的 4、5 类 LSA 同时过滤，同时该 ABR 会主动向区域内部发送一个 o IA 的 0.0.0.0/0 的 3 类缺省路由，Seed Metric 为 1

谁下放的路由在下放者上修改 Seed Metric  
area 1 default-cost 36

#### \* Totally Stubby Area

在 Stub 区域基础之上 ABR 路由会同时将 3、4、5 类入向传递的 LSA 过滤掉，同时会主动向该区域注入一条 o IA\*的 0.0.0.0/0 的缺省路由，Seed Metric 为 1

R3(config-router)#narea 1 stub no auto-summary

#### \* Not-So-Stubby Areas

- 允许 ASBR

实验：

(EIGRP)->R4 ~ R2 ~ R1 ~ R3 - R5  
Area1 0 2 RIP

ASBR: 一台路由器只要可以产生 5 类 LSA，其就是 ASBR

NSSA 总结：

当把一个 Area 置为 NSSA，此 Area 内可有 ASBR，ASBR 重分发进入的路由以 7 类 LSA 的形式在区域内传递，7 类 LSA 到达 ABR，若 ABR 只有一台，其必为 translator，转换器会把 7 类 LSA 转成 5 类

通过其他 Area 发送，并且 NSSA 区域的 ABR 会阻止外部进入的 4、5 类 LSA，坑爹的是，它不会主动地向 Area 内下放缺省路由，所以要通过 default-info-指定它让它向 NSSA 下放一条 ON2，seed metric 值为 1 的缺省路由（area 2 nssa default-information-originate）。若该 Area 的 ABR 同时为 ASBR，这时如果重分发工作已经做完，那这台 R 会把外部路由以 5 类的形式在其他区域传递，以 7 类形式在 NSSA 区域传递。故进一步优化 NSSA 区域，不建议这些外部路由进入它，需要做另五参数 no redistribution。

Totally NASA:

- 1.ABR 会同时过滤掉 3、4、5 类即将进入 Area 的 LSA
- 2.ABR 会主动向 Area 内下放一条 O\*IA 的全 0/0 的, SM=1 的缺省路由

NSSA 区域

在 NSSA 区域内可以拥有 ASBR, 并且重分发进入 OSPF 的路由是以 7 类 LSA 形式存在, 该类型的 LSA 只能存在于 NSSA 区域内, 并且该 Area 所有 ABR 会通过比较 RRID 选举一个转换器 (最大 RID 者), 该转换器会将内部传递给外部的 NSSA LSA 转换成 5 类 LSA 并且通告给其他 Area, 所有该 Area 内的 ABR 都会过滤从外部进入 该 Area 的 4、5 类 LSA, 但是该 Area 的任何 ABR 都不会主动向内部下放缺省路由, 为实现内部路由器的外网可达性, 需要在该 Area 的 ABR 上手工下放缺省路由,

O N2 0.0.0.0/0 Seed Metric=1

Totally NASA

基于 NSSA 区域的概念基础, ABR 会主动阻止 3、4、5 类 LSA 进入该 Area, 并且 ABR 会主动向 Area 内下放 O IA 的 0.0.0.0/0 SM=1 的缺省路由

加表优先级:

O> O IA> O E1/E2 = O N1/N2

- 1.远离骨干 Area 的非骨干 Area
- 2.被分割的 Area 0

Solution:

1:在出现问题的 ABR 上(没有和 Area 0 直连的 ABR 上),使用双 OSPF 进程, 并执行单点双向重分发

```
R3(config-router)#redistribute OSPF 110 subnets
R3(config-router)#redistribute OSPF 100 subnets
```

2:在出现问题的 ABR 上建立一个 Tunnel 链路连接到离其最近的 Area0 中的 ABR 路由器上

```
R3(config)#int tunnel 3
R3(config-if)#tunnel source 3.3.3.3
R3(config-if)#tunnel destination 1.1.1.1          tunnel 为二层接口, 故配 IP:
R3(config-if)#ip address 31.1.1.3 255.255.255.0
R3(config-if)#no shutdown
R3(config)#router ospf 110
R3(config-router)#network 31.1.1.3 area 0
R3(config)#ip route 1.1.1.1 255.255.255.255 serial 1/0 13.1.1.1
```

```
R1(config)#int tunnel 1
R1(config)#tunnel source 1.1.1.1
R1(config-if)#tunnel destination 3.3.3.3
```

```
R1(config-if)#ip address 31.1.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config)#router ospf 110
R1(config-router)#network 31.1.1.1 area 0
R1(config)#ip route 3.3.3.3 255.255.255.255 serial 1/1 13.1.1.3
```

注：不要将 tunnel 源、目的地址宣告入 OSPF，再写静态以路由

3.使用 Virtual-link 在出问题的 ABR 以及离他最近的 Area 0 中的 ABR 上部署

```
R3(config)#router ospf 110
R3(config-router)#area 2 virtual-link 91.1.1.1 (路由器 ID)
```

```
R1(config)#router ospf 110
R1(config-router)#area 2 virtual-link 93.3.3.3(路由器 ID)
```

Virtual-link 条件：

只能一个 Area 内的两台路由器间建 (必须能收到 1 类 LSA)

OSPF Authentication

1.明文：

```
R2(config)#int s1/0
R2(config-if)#ip ospf authentication-key cisco 两
R2(config-if)#ip ospf authentication 组

R4(config)#int s1/1
R4(config-if)#ip ospf authentication-key cisco
R4(config-if)#ip ospf authentication
```

2.密文：(链路级)

```
R1(config)#int s1/1
R1(config-if)#ip ospf message-digest-key 13 md5 cisco
R1(config-if)#ip ospf authentication message-digest

R3(config)#int s1/0
R3(config-if)#ip ospf message-digest-key 13 md5 cisco
R3(config-if)#ip ospf authentication message-digest
```

区域级认证：

明文：接口定义密钥，进程中声明

```
R1(config)#int s1/0
R1(config-if)#ip ospf authentication-key H3C
R1(config)#router ospf 110
R1(config-router)#area 0 authentication
```

```
R2(config)#int s1/0
R2(config-if)#ip ospf authentication-key H3C
R2(config)#router ospf 110
R2(config-router)#area 0 authentication
```

密文:

```
R1(config)#int s1/0
R1(config-if)#ip ospf message-digest-key 12 md5 cisco
R1(config)#router ospf 110
R1(config-router)#area 0 authentication message-digest
```

```
R1(config)#int s1/0
R1(config-if)#ip ospf message-digest-key 12 md5 cisco
R2(config)#router ospf 110
R1(config-router)#area 0 authentication message-digest
```

虚链路级认证:

```
R3(config-router)#area 2 virtual-link 91.1.1.1 authentication-key cisco
R3(config-router)#area 2 virtual-link 91.1.1.1 authentication
  启用 VL 的明文认证（只有在 VL 初始化建立邻接关系的时候生效）
```

```
R1(config-router)#area 2 virtual-link 91.3.3.3 message-digest-key 12 md5 cisco
R1(config-router)#area 2 virtual-link 91.3.3.3 authentication message-digest
  启用 VL 的密文认证（同明文认证用途）
```

No frame-relay inverse-arp

No arp frame-relay (在客户端路由器上使用该命令关闭自动 ARP 映射)

OSPF Network Type:

- |                                      |                  |                                  |
|--------------------------------------|------------------|----------------------------------|
| 1: Loopback                          | loopback         | 无论接口掩码多少，都以/32 主机路由通告            |
| 2: Point-to-Point                    | Serial/ISDN BRI/ | 支持组播，无 DR 串口，                    |
| FR p2p(帧中继的点到点)                      | Subif            | 支持组播 没有 DR (Hello)               |
| 3: Broadcast                         | Ethernet         | 支持组播，有 DR                        |
| 4: NBMA                              | FR 主接口/          | 不支持组播，有 DR(只能以单播发送)              |
|                                      | FR 多点子接口         |                                  |
| 5: P-T-Multipoint                    | -----            | 支持组播，无 DR，自动生成关于直连邻居接口的/32 的主机路由 |
| 6: Point to-Multipoint Non-Broadcast | --               | 不支持组播，无 DR，自动/32 路由。需要指 neighbor |

链路两端链路类型要一致，特例

一段点到多点，一段点到点

两端都是非广播需要指定 Neighbor router ospf 90 neighbor 12.1.1.2 只需一端指 neighbor，因为需要确认报文。定会回复报文。

Rip 需要双向指 Neighbor

Eigrp 也要双向指

hub 和 spoke 结点一端 P2P，一端 P2MP，注意修改 hello 时间，hub 为 30s

在 FR 环境中部署 OSPF

#### 1: 网络类型使用 NBMA

为了建立邻居，需要在 Hub 结点手工指 Neighbor,

为了保证路由传递问题，需要手工接口的 OSPF 优先级，保证 Hub 成为 DR，Spoke 什么都不是

为了保证 Spoke 节点所连接的下游网段内的 PC 可以互访，需在 Spoke 节点彼此指手工 FR 映射

#### 2.网络类型使用 Broadcast

由于支持组播放送，因此不需要手工指 Neighbor(FR Map 开启伪广播功能)

需要修改接口 OSPF 优先级改变 DR 位置

需要手工配置 FR 的映射，实现 Spoke 节点彼此访问

#### 3: 网络类型使用 P2P-Multipoint Non-Broadcast

需要手工指 Neighbor 建邻居

不需要手工接口 OSPF 优先级，因为没 DR/BDR

不需要手工 FR 映射，因为/32 的主机路由

#### 4: 网络类型使用 P2P-Multipoint

不需要手工指 Neighbor

不需要手工接口 OSPF 优先级

不需要手工 FR 映射

R2#ping 3.3.3.3 source 2.2.2.2

OSPF 注入缺省路由

```
R1(config)#router OSPF 110
```

```
R1(config-router)#default-information originate
```

```
R1(config)#ip route 0.0.0.0 0.0.0.0 null 0
```

FR

- 2 层，星型（轴辐）
- 承载在 PVC 基础上
- DLCI
- LMI

两条一并使用，关闭一个接口的自动 ARP

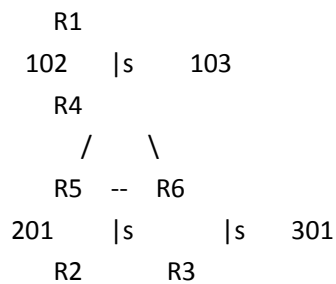
```
no frame-relay inverse-arp
```

no arp frame-relay

IARP 只适用于 FR 环境：把对端 IP 映射到本地 DLCI

- 1 封装 R2
- 2.在 DCE 端配时钟率
- 3.数据链路层 DCE
- 4.定义 LMI 类型
- 5.PVC 组建

实验：FR



R1:为 HUB

```
R1(config)#int s1/1
R1(config-if)#encapsulation frame-relay ietf
R1(config-if)#no shutdown
R1(config-if)#ip address 123.1.1.1 255.255.255.0
```

R2:

```
R2(config)#int s1/1
R2(config-if)#encapsulation frame-relay ietf
R2(config-if)#no shutdown
R2(config-if)#ip address 123.1.1.2 255.255.255.0
R2 到 R3 映射:
R2(config-if)#frame-relay map ip 123.1.1.3 201 broadcast ietf
```

R3:

```
R3(config)#int s1/1
R3(config-if)#encapsulation frame-relay ietf
R3(config-if)#no shutdown
R3(config-if)#ip address 123.1.1.3 255.255.255.0
R3 到 R2:
R3(config-if)#frame-relay map ip 123.1.1.2 301 broadcast ietf
```

R4:

```
FR-R4(config)#int s1/0
FR-R4(config-if)#encapsulation frame-relay ietf
FR-R4(config-if)#no shutdown

FR-R4(config-if)#int fa0/1
FR-R4(config-if)#ip address 46.1.1.4 255.255.255.0
FR-R4(config-if)#no shutdown
FR-R4(config-if)#int fa0/0
FR-R4(config-if)#ip address 45.1.1.4 255.255.255.0
FR-R4(config-if)#no shutdown

FR-R4(config)#router eigrp 90
FR-R4(config-router)#no auto-summary
FR-R4(config-router)#network 45.1.1.4 0.0.0.0
FR-R4(config-router)#network 46.1.1.4 0.0.0.0

FR-R4(config)#frame-relay switching
FR-R4(config)#int s1/0
FR-R4(config-if)#frame-relay intf-type dce
FR-R4(config-if)#frame-relay lmi-type ansi

FR-R4(config)#interface tunnel 45
FR-R4(config-if)#tunnel source 45.1.1.4
FR-R4(config-if)#tunnel destination 45.1.1.5
FR-R4(config)#interface tunnel 46
FR-R4(config-if)#tunnel source 45.1.1.4
FR-R4(config-if)#tunnel destination 45.1.1.6

FR-R4(config)#int s1/0
FR-R4(config-if)#frame-relay route 102 interface tunnel 45 500
FR-R4(config-if)#frame-relay route 103 interface tunnel 46 501
```

R5:

```
FR-R5(config)#int s1/0
FR-R5(config-if)#encapsulation frame-relay ietf
FR-R5(config-if)#no shutdown

FR-R5(config-if)#int fa0/1
FR-R5(config-if)#ip address 45.1.1.5 255.255.255.0
FR-R5(config-if)#no shutdown
FR-R5(config-if)#int fa0/0
FR-R5(config-if)#ip address 56.1.1.5 255.255.255.0
```



FR-R5(config-if)#no shutdown

FR-R5(config)#router eigrp 90

FR-R5(config-router)#no auto-summary

FR-R5(config-router)#network 45.1.1.5 0.0.0.0

FR-R5(config-router)#network 56.1.1.5 0.0.0.0

FR-R5(config)#frame-relay switching

FR-R5(config)#int s1/0

FR-R5(config-if)#frame-relay intf-type dce

FR-R5(config-if)#frame-relay lmi-type ansi

FR-R5(config)#int s1/0

FR-R5(config)#interface tunnel 54

FR-R5(config-if)#tunnel source 45.1.1.5

FR-R5(config-if)#tunnel destination 45.1.1.4

FR-R5(config-if)#frame-relay route 201 interface tunnel 54 500

R6:

FR-R6(config)#int s1/0

FR-R6(config-if)#encapsulation frame-relay ietf

FR-R6(config-if)#no shutdown

FR-R6(config-if)#int fa0/1

FR-R6(config-if)#ip address 56.1.1.6 255.255.255.0

FR-R6(config-if)#no shutdown

FR-R6(config-if)#int fa0/0

FR-R6(config-if)#ip address 46.1.1.6 255.255.255.0

FR-R6(config-if)#no shutdown

FR-R6(config)#router eigrp 90

FR-R6(config-router)#no auto-summary

FR-R6(config-router)#network 46.1.1.6 0.0.0.0

FR-R6(config-router)#network 56.1.1.6 0.0.0.0

FR-R6(config)#frame-relay switching

FR-R6(config)#int s1/0

FR-R6(config-if)#frame-relay intf-type dce

FR-R6(config-if)#frame-relay lmi-type ansi

FR-R6(config)#interface tunnel 64

FR-R6(config-if)#tunnel source 46.1.1.6

FR-R6(config-if)#tunnel destination 46.1.1.4

```
FR-R6(config)#int s1/0
```

```
FR-R6(config-if)#frame-relay route 301 interface tunnel 64 501
```

若要求 PING 通所有接口

要手工映射自己:

```
R1(config)#int s1/1
```

```
R1(config-if)#frame-relay map ip 123.1.1.1 102 broadcast ietf
```

CLNP: NASP 地址 Network service access point

AS-AS 存在一条骨干链路，他有连续的 L2 以及 L1/L2 路由器互联而成。

L1 大多数包含拓扑信息，L2 大多数包含路由信息。

IDP: Initial Domain part

AFI: Authority Format ID 组织格式标识符 45: 代表美国政府

IDI: 0005 军事化部门 0006 非军事化

45.0005 45.0006

DSP: Domain Specific Part

HODSP: 高位区域指定部分，用来描述设备所属的区域，区域 1（两个字节） 0001

System ID: 系统用来表示一个区域内的某台设备本身。 6Byte

0000.0000.0001 192.168.000.001

1921.6800.0001

NSEL: NSAP 选择位。 类似 Protocol。 不为零应用程序，0 设备本身。 1Byte 00

Voice Gateway

Isis 配置

Conf t

Rout0er isis1

ONet 49.0001.0120.0100.1001.00 (12.1.1.1 0120.0100.1001.00)

log-adjacency-changes all (提示日志信息，必打)

Int loopback 0

Ip router isis

Exi

Int fa 0/1

Ip router isis

Exi

搞定

清理邻居信息

Clear isis \*

或者

Clear clns neighbor

显示邻居

Show clns neighbors

SNPA: MAC 地址

Show clns is-neighbors

Show isis neighbors

Show isis neighbors detail

Show isis hostname

Show ip protocols 信息有限，一般用

Show clns protocol

Show clns interface 显示接口信息

修改 isis 类型

Router isis

Is-type level 1

修改路径类型

Int fa 0/0

Isis circuit-type level-2-only

路由泄露

Conf t

Access-list 10 permit 9.9.9.0

Route-map L2-L1 permit 10

Match ip address 10

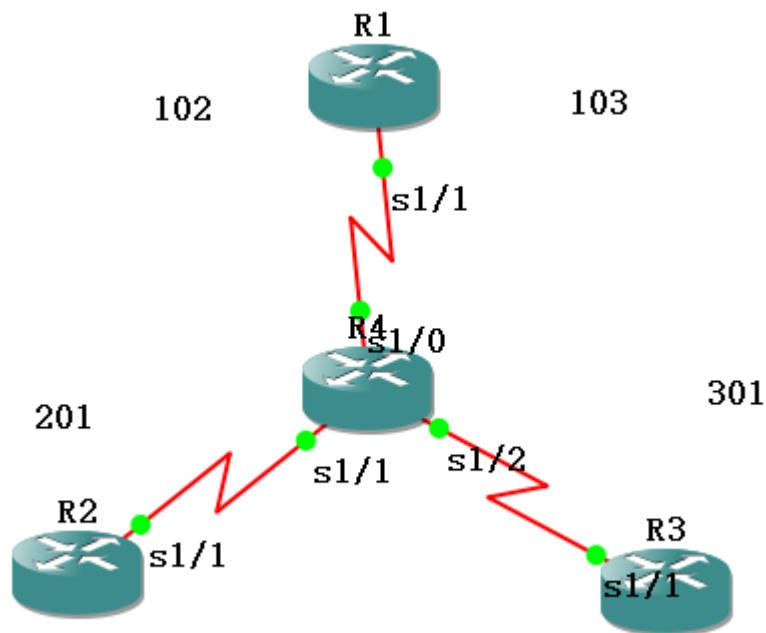
Exit

Router isis

Redistribute isis level-2 into level-1 rout-map L2-L1

帧中继环境中配置 ISIS

第一步配置帧中继



```

R1
Conf t
Int loopback 0
Ip add 1.1.1.1 255.255.255.0
Exi
Int serial 1/1
R1(config-if)#encapsulation frame-relay
R1(config-if)#ip address 123.1.1.1 255.255.255.0
No shut down

```

```

R4 上
FR(config)#interface serial 1/0
FR(config-if)#encapsulation frame-relay
FR(config-if)#frame-relay intf-type dce
FR(config-if)#frame-relay lmi-type cisco
FR(config-if)#frame-relay route 102 interface serial 1/1 201
FR(config-if)#frame-relay route 103 interface serial 1/2 301
FR(config-if)#no shutdown
FR(config)#interface serial 1/1
FR(config-if)#encapsulation frame-relay
FR(config-if)#frame-relay intf-type dce
FR(config-if)#frame-relay lmi-type cisco
FR(config-if)#frame-relay route 201 interface serial 1/0 102
FR(config-if)#no shutdown

```

```
FR(config)#interface serial 1/2
FR(config-if)#encapsulation frame-relay
FR(config-if)#frame-relay intf-type dce
FR(config-if)#frame-relay lmi-type cisco
FR(config-if)#frame-relay route 301 interface serial 1/0 103
```

下一步部署 ISIS

```
R1(config)#router isis
R1(config-router)#net 49.0001.1111.1111.1111.00
R1(config-router)#log-adjacency-changes all
R1(config-router)#exit
```

```
R1(config)#interface loopback 0
R1(config-if)#ip router isis
R1(config)#interface serial 1/1
R1(config-if)#ip router isis
Exit
```

查看 isis 邻居

```
R1#show clns neighbors
R1#show is-clns neighbors
R1#show isis neighbors
```

解决办法

```
R1(config)#default interface s 1/1 （先 default 一下）
R1#clear frame-relay inarp （第二步清除表项）
R1(config)#interface serial 1/1 （第三部）
R1(config-if)#encapsulation frame-relay
R1(config-if)#no shutdown
R1(config-if)#no frame-relay inverse-arp （第四部关闭主接口自动映射）
R1(config)#interface serial 1/1.102 point-to-point
R1(config-subif)#no shutdown
R1(config-subif)#ip address 12.1.1.1 255.255.255.0
R1(config-subif)#no shutdown
R1(config-subif)#frame-relay interface-dlci 102
R1(config-fr-dlci)#no shutdown
R1(config-subif)#exit
R1(config)#interface serial 1/1.103 point-to-point
R1(config-subif)#no shu
R1(config-subif)#ip address 13.1.1.1 255.255.255.0
R1(config-subif)#frame-relay interface-dlci 103
R1(config-fr-dlci)#no shu
R1(config-subif)#exi
```

再次启用 isis

```
R1(config)#interface serial 1/1.102
```

```
R1(config-subif)#ip router isis
```

```
R1(config)#interface serial 1/1.103
```

```
R1(config-subif)#ip router isis
```

子接口创建后删不掉

解决办法

先 No 掉

Write

然后重启

Show ARP 查看 MAC 地址

Show isis neighbors 查看 CID

查看优先级

```
Show clns interface fa0/1
```

修改优先级

```
Int fa 0/1
```

```
Isis priority 66 level-1
```

Show isis database

Show isis database verbose

ATT 位

1 当一台路由器是 LEVEL-1/level2 路由器时候，该路由器可以发送 ATT 置位的 LSP

2 当该路由器收到了其他 level-2 邻居通告的 level-2LSP 时候才会发送 ATT 位置的 level-1 LSP

只有 level-1 的路由器收到 ATT 置为的 level-1 LSP 的时候，会指该路由器缺省路由。

邻居关系的过滤

## 邻居关系的过滤

比如说一个MA网络里，有3台路由器：R1,R2,R3。默认情况下，配置正确后将可以互相建立邻居，但此时R1只想和R2建立邻居，而不想和R3建立邻居，可以在R1上通过该方法实现：

第一步：(if)# isis adjacency-filter ccnp

第二步：(config)# clns filter-set ccnp deny  
49.0123.0000.0000.0002.00

注意：两边都的打，不然会造成不打命令的一方可以看到邻居，但会卡在init状态。

一定要在邻居之间双向过滤

ISIS 汇总

Summary-address 4.4.0.0 255.255.252.0

汇总只能在始发路由器上进行

ISIS 认证

Isis password cisco

老式的接口下配置明文邻居认证

Area-password cisco

老式的进程下配置明文区域认证

Domain-password cisco

老式进程下配置明文域认证

新认证

接口下密文认证：

```
(if)#isis authentication mode { text | md5 } { level-1 | level-2 }
```

接口下设置ISIS邻居认证模式

```
(if)#isis authentication key-chain duxin { level-1 | level-2 }
```

接口下设置ISIS邻居认证key-chain

进程下密文认证：

```
(config-router)#authentication mode { text | md5 } { level-1 | level-2 }
```

进程下设置ISIS区域认证模式或域认证模式

```
(config-router)#authentication key-chain duxin { level-1 | level-2 }
```

进程下设置ISIS区域认证或域认证的key-chain。

缺省路由下放

Router isis

Default-information originate

路由重分发

将路由协议 A 重分发进 Rip, seed metric 为 0 代表不可达, 需要手工修改,

R1(config-router)#redistribute ospf 110 metric 5

将静态路由重分发进 Rip, seed metric 为 1, 可达, 无需修改, 并且缺省路由 0.0.0.0/0 缺省路由可以进入进程

R1(config-router)#redistribute static

直连路由重分发进 Rip。Seed Metric 为 1, 可达, 无需修改

Default-metric 命令只会影响协议 A 重分发进 Rip 的路由, 以及 Static 重分发进 Rip 的路由, 但是不会修改直连 connected 重分发进 Rip 的 seed metric

OSPF 重分发

将路由协议 A 重分发进 OSPF, 缺省 seed Metric 为 20 Metric-type 为 0 E2, 可以使用 default-Metric 命令修改这类重分发进路由的 seedMetric, 将 static 路由重分发进 OSPF, 缺省 seed Metric 为 20, type 为 0 E2, 只有明细 static 路由可以进入, 缺省路由无法进入

将 connected 路由重分发进 OSPF, 类似重分发 static,

default-Metric 可以修改 static 和来自于协议 A 的重分发路由的 seed Metric, 对 connected 路由无效

将 Rip 重分发进 OSPF

如果在重分发路由器上开启的是 RIPV1 或者开启的是局域自动汇总的 RIPV2, 则重分发进入的路由依旧会遵循自动汇总原则

R1(config-router)#redistribute rip subnets metric-type 1 metric 30

isis 重分发进 EIGRP 修改 Metric

Router eigrp 90

Default-metric 10000 100 255 1 1500

Redistribute isis level-1-2 metric 10000 100 255 1 1500

将协议 A 重分发进 EIGRP, seed metric 为 0, 不可达, 需手工修改

将静态路由重分发进我 eigrp, 缺省 seed Metric 不为 0, 可达, 并且缺省路由可以进入

将直连路由重分发进 EIGRP, 缺省路由不为 0, 可达

default-Metric 可以修改 static 和来自于协议 A 的重分发路由的 seed Metric, 对 connected 路由无效

默认将 ISIS 重分发进任何其他协议的时候, 都只会将 level-2 路由发送过去, 并且不能携带直连路由, 只能携带通过 isis 学习到的打 i 的路由

将路由选择协议 A 的路由重分发进 ISIS, 缺省 seed Metric 为 0, 可达, 并且路由类型是 level-



2

将静态路由重分发进 isis，缺省 seedMetric 为 0，可达，只能包含明细路由，缺省路由无法进入，

将直连路由重分发进 isis，缺省 seed Metric 为 0，可达

在路由器 R 上运行路由选择协议 A 以及路由选择协议 B，此时在 R 上将 A 重分发进 B，R 会将所有本地宣告进协议 A 的直连路由，以及通过协议 A 获悉的，加入路由表的并且加上 A 路由标记的路由引入协议 B。

协议 A 不能是 ISIS 以及 ODR

在 RIP 中可以使用分发列表基于入站和出站方向做路由过滤

Conf t

Access-list 10 deny 3.3.3.0

Access-list 10 permit any

Router rip

Distribute-list 10 in

Access-list 10 deny 2.2.2.0

Access-list permit any

Route rip

Distribute-list 10 out fastEthernet 0/1

EIGRP 中使用分发列表同 RIP

在 LS 协议中，分发列表不能出站调用，因为传递的不是路由条目，是 LSA，分发列表无法基于 ACL 或任何其他工具抓取 LSA，但是在该环境中可以使用入站方向调用分发列表，实现的是路由信息的本地抑制，而不会限制 LSA 的传递，，因此只对本地路由器有效。

Access-list 15 deny 14.1.1.0

Access-list permit any

Distribute-list 15 out ospf 110

基于 IPV4 的前缀列表 Prefix-list 能抓前缀和掩码，ACL 只能抓前缀

IP prefix-list 10 seq 10 permit 2.2.2.0/25

一次加多条路由

GE: greater equal

LE: less equal

例子:

Ip prefix-list 10 seq 20 permit 2.2.2.0/25 GE27



O 大于 OIA 大于 O E1 路由器优先级大于 OE2

## BGP

支持子网化，支持路由聚合 高级距离矢量协议。高级在生成三张表，BGP 路由度量值。

应用层协议，基于 TCP 的端口号 179

### BGP V4 基于 IPV4

企业访问外网只有一家运营商接入

多家运营商接入，但是要求较低，只需要冗余备份。

以上两种只需要缺省路由，不需要 BGP

运营商双接入因特网，

Multihoming，多宿主连接

IGPs announce networks and describe the metric to reach those networks

BGP announces paths and the networks that are reachable at the end of the path. BGP describe the path by using attributes, which are similar to metrics

BGP allows administrators to define policies or rules for how data will flow through the autonomous system.

Hello 报文 4 种

Open keep alive update notification

BGP 邻居类型：EBGP IBGP

BGP Speaker：运行 BGP 的路由器

BGP peer BGP 路由器的邻居

两台路由器不在同一个 AS 就是 EBGP 连接关系，传递的路由就是 EBGP 路由

IBGP 概念：描述连接关系，收到路由类型

在同一个 AS 内就是 IBGP 连接关系，传递的路由就是 IBGP 路由

解决 BGP 数据层面路由黑洞的方式

- 1: 在 AS 内使用物理线路全互联。物理的 full mesh
- 2: AS 内 IBGP 对等体连接关系的全互联。逻辑的 Full mesh
- 3: 只获取路由条目，不运行 BGP。在 ASBR 上做重分发  
将 AS 内部的边缘路由器上的 BGP 路由重分发进 IGP 中。
- 4: 在 AS 内部的边缘路由器之间建立 Tunnel
- 5: 在 AS 内所有路由器上启用 MPLS (multi-protocol label switch) LFIB

一台 BGP 会话者收到了一条 IBGP 路由，该路由器只可能将该路由传递给它 EBGP 对等体，而不会将该路由传递给任何其他的 IBGP 对等体

在 EBGP 中有 AS-path

一台 BGP 会话者收到了一条 EBGP 路由，只要该 EBGP 路由内包含接受者所在的 AS 号，则

该路由会立即被丢弃。

#### BGP 路由的传递原则

1: 对于一条 BGP 路由, 如果一台路由器是该路由的始发路由器, 该路由器会将该路由传递给其所有 IBGP 对等体, 以及所有 EBGP 对等体

2 对于一条 BGP 路由, 如果该路由器不是该路由的始发路由器, 如果 对该路由器而言该路由条目是一条 EBGP 路由, 该路由器会将该路由转发给所有 IBGP 对等体以及所有其他的 EBGP 对等体

如果对于该路由器而言该路由是一条 IBGP 路由, 则该路由器会将该路由条目转发给所有 EBGP 对等体, 而不会转发给任何 IBGP 对等体

#### BGP 配置

Router bgp autonomous-system (一台路由器上只能运行一个 BGP)

使用 neighbor 和另外 bgp 路由器建立关系

Neighbor ip-address | peer-group-name remote-as autonomous-system

BGP 邻接关系即便建立完毕, 路由器之间也不会传递任何 BGP 路由。

想让 BGP 路由器彼此传递 BGP 路由, 需要在 BGP 进程中要么使用 1; 使用 network 语句。2 使用 redistribute 进行路由重分发

#### BGP 的邻接关系状态

1: IDLE

2: Connected

3: Active (该邻接关系状态为问题状态)

4: Open sent

5: Open confirm

6: Established

#### 显示 bgp 路由表

Show ip bgp summary

BGP table version ,修改过一次加一。

V 版本号, V 4, V4+ (IPV6, mpls, 组播)

Show tcp brief 看端口号

#### 获悉对端的环回口路由

1 使用 EBGP 多跳命令 R3(config-router)#neighbor 5.5.5.5 ebgp-multihop

2 使用静态路由 R3(config)#ip route 5.5.5.0 255.255.255.0 serial 1/1 35.1.1.5

必须把路由表中有的路由条目转成 BGP 通告。使用 show ip route 查看

R4(config-router)#network 4.4.4.0 mask 255.255.255.0

如果 BGP 表中的一条 BGP 路由没有表示 > 则该路由不是最优的, 不是最优的路由没有资格

被添加进路由表，也没有资格被传递给其他任何其他邻居路由器

导致 BGP 路由不由得原因

1: BGP 路由的下一条的可达性 R2(config-router)#neighbor 3.3.3.3 next-hop-self

2: 同步原则

当一台路由器通过一个 IBGP 对等体 收到了一条 IBGP 路由，该路由条目不能被放入路由表，也不能被传递给任何其他邻居，除非该路由器同时通过某种 IGP 获悉了该路由条目

通过 Next-hop-self

一条路由条目如果打 r 和>则代表该路由条目是最优的，但是由于管理距离的问题无法被加入路由表，但是该路由可以被传递给其他 BGP 对等体

EBGP 20 IBGP 200

ICMP Redirect

当一台路由器 通过一个接口接收到了一个报文，该路由器查表发现需要转发这个报文需要将其通过接受接口再次转发出去。

当一台 BGP Speaker 将一条 BGP 路由传递给同 MA 网段的下一跳 EBGP 邻居时，该路由器如果发现该路由条目的上一条邻居传递该路由是的接口 IP 地址和写一条邻居接受该路由的接口 IP 地址在同一个 IP 子网段，此时该路由器会主动将该路由条目的下一跳地址改写为上一条邻居的发送路由接口的 IP 地址

关于 BGP 路由条目的下一跳地址

1. 如果一台路由器将本地路由通告进 BGP 进程，则对于这些被通告路由，该路由器本地 BGP 表中关于他们的下一跳都为 0.0.0.0 （本地路由：直连，静态 S）
2. 如果一台路由器将通过 IGP 获悉的路由通告进 BGP 进程，则这些路由在该路由器的 BGP 表中下一跳会继承相应的 IGP 路由的下一跳地址
3. 如果一台路由器将其本地通告的本地路由传递给任何 BGP 对等体，则会将该路由条目的下一跳改为本地对于这些邻居的更新源
4. 如果一台路由器通过 EBGP 学习到了一条路由，则该路由在传递给 IBGP 对等体时，默认情况下一跳不变，除非做 next-hop-self
5. 如果一台路由器将任何 BGP 路由通告给其 EBGP 对等体，则路由的下一跳会变成该路由器对于该邻居的 BGP 更新源地址

**When establishing a BGP session, BGP goes through the following states:**

1. **Idle:** Router is searching routing table to see whether a route exists to reach the neighbor.
2. **Connect:** Router found a route to the neighbor and has completed the three-way TCP handshake.
3. **Open sent:** Open message sent, with the parameters for the BGP session.
4. **Open confirm:** Router received agreement on the parameters for establishing session.
  - Alternatively, router goes into **active** state if no response to open message
5. **Established:** Peering is established; routing begins.

TCP 承载 BGP 报文，单播。先查路由表，指 neighbor (IDLE)。三次握手 Connected。建邻居报文，open sent。合法，建邻居：open confirm，失败 active。最后 established

**Active:** The router has sent an open packet and is waiting for a response. The state may cycle between active and idle. The neighbor may not know how to get back to this router because of the following reasons:

- Neighbor does not have a route to the source IP address of the BGP open packet generated by this router.
- Neighbor is peering with the wrong address.
- Neighbor does not have a neighbor statement for this router.
- AS number is misconfiguration.

BGP 认证

Neighbor {ip-address | peer-group-name} password string

Show ip bgp rib-failure

Clear ip bgp \* 硬重置

Clear ip bgp \* soft (in/out) 软重置

Show ip bgp neighbors 12.1.1.1 advertised-routes

显示本地把那些条目发了

Neighbor 12.1.1.2 soft-reconfiguration inbound

Show ip bgp neighbors 12.1.1.2 received-routes

显示收到了哪些路由

Debug ip bgp updates

扩展

Auto-summary (ripv1,rip v2(会汇总邻居传递过来的路由 EIGRP 不会),eigrp,)

BGP 的 auto-summary

在早期 IOS 版本中默认情况一台路由器的 BGP 进程的 auto-summary 是开启的，在后期新版本的 ios 中 auto-summary 是自动关闭的

无论在路由器上是否开启 auto-summary 都不会影响 BGP 精确通告的 BGP 路由该特性只有两个作用，

1: 当在路由器上使用汇总通告的时候，如果该路由器路由表中拥有汇总条目内的明细路由的时候，并且该路由器开启了自动汇总，则该路由器会将明细路由抑制并且将其在主类网络边界汇总后发送给邻居

2: 当在路由器的 BGP 进程中重分发外部路由时，如果开启了 auto-summary，那么该路由器会将这些路由以主类的形式发送给邻居。还会将重分发进入路由的下一跳地址写为全 0 即便这些路由本身携带 Metric，在 BGP 表中也不会继承。

发送接口的 ip 地址和路由的前缀不在同一个主类地址段中

进入 BGP3 条必须命令

No synchronization

No auto-summary

Bgp router-id

BGP 的手工汇总

Ip route 192.168.8.0 255.255.252.0 null0

Network 192.168.8.0 mask 255.255.252.0

1 在本地创建指向 null 0 接口的聚合路由，并且在该路由器的 BGP 进程中使用 Network 语句通告该路由聚合，而不需要通告任何一条明细路由

@@@2 BGP 定义的手工聚合

Network 192.168.8.0 mask 255.255.255.0

Network 192.168.9.0 mask 255.255.255.0

Network 192.168.10.0 mask 255.255.255.0

Network 192.168.11.0 mask 255.255.255.0

Aggregate-address 192.168.8.0 255.25.252.0 summary-only

2

BGP 路由聚合原则，只要聚合命令配置了，该路由器如果在 BGP 表中拥有该聚合内的明细路由，则会直接在本地 bgp 表中生成该聚合路由，并且在通告给其他邻居

IP prefix-list 10 permit x.x.x.x/X GE Y LE Z X<Y<=Z

Aggregate-address 192.168.8.0 255.25.252.0 summary-only as-set

BGP 强制属性

AS path\*

Next-hop\*

Origin\* 用来描述一条 BGP 路由是通过何种方式进入的  
修改方法:

Ip prefix-list 10 permit 1.1.1.0/24

Route-map O permit 10

Match ip address prefix-list 10

Set origin egp 1

Exit

Route-map O permit 20

Exit

Router bgp 1

Neighbor 12.1.1.1 route-map O in

Clear ip bgp \* soft

使用 route map 切记加空语句，记得清邻居

Weight 权重属性

- 1, 传递范围，该属性只能在路由器本地有意义，路由器发送任何 BGP 路由的时候不会携带该属性
- 2, 缺省值，对于下一跳地址为 0.0.0.0 的 BGP 路由，在该路由器本地 BGP 表中该路由的缺省 weight 是 32768.如果该路由是邻居通告的，无论 IGBP 过 EBGp 都是缺省 0，如果该路由是本地通告但是来源于 IGP，则该路由缺省权重也是 0 0—65535
- 3, 比较方式，weight 属性值越大，该路由条目越优。

1

Access- 100 permit ip host 4.44.0 host 255.255.255.0

2

Route-map W permit 10

match ip address 100

Set weight 1

Route-map W permit 20

3

Router bgp 1

Neighbor 1.1.1.1 route-map W in

## 2. Local preference

传递范围 只能在一个 AS 内传递（只能在传递 IGBP 路由的时候修改）

缺省值：只要是 BGP 路由无论是否本地产生，无论是 IGBP、EBGP，缺省值都为 100 比较原则越大越好

R1（config-router） bgp default local-preference 101

1 本地产生的



- 2.EBGP 路由
- 3.IBGP 路由
- 4.aggragate 路由

```
Ip prefix-list 10 seq 10 permit 4.4.4.0/24
Route-map LP permit 10
Match ip address prefix-list 10
Set local-preference 101
Exit
Route-map LP permit 20
Router bgp 1
Neighbor 14.1.1.4 route-map LP in
End
```

设置思科路由器上 MED  
Bgp bestpath med missing-as-worst

打破 IBGP 路由传递原则的两大方式

1: 路由反射器 Router Reflector

Cluster, IBGP, RR (路由反射器 server) 其他为 RRC (client)

RR 收到了一条 EBGP 路由, 会将其转发给所有其他 EBGP 对等体以及所有 IBGP 对等体 (包含 Client 以及 Non-client)

RR 收到了一条 IBGP 路由 (该路由是 Client 传递的), RR 会将其转发给所有其他的 RR 以及所有 IBGP 的 Non-client 以及所有 EBGP 对等体

RR 收到了一条 IBGP 对等体 (该路由是 Non-Client 传递的) RR 会将其转发给所有 Client 以及所有 EBGP 对等体, 但是不传递给任何其他的 Non-Client

命令

R5: Neighbor 2.2.2.2 router-reflector-client

R5 变为 server, R2 变为 Client

2 联邦 confederation

```
Router Bgp 65001
No synchronization
No auto-summary
Bgp router-id
Bgp confederation identifier
```

```
Neighbor 14.1.1.4 remote-as 4
```

```
Neighbor 5.5.5.5 remote-as 65001 (联邦内指主 AS 号)
```

```
Neighbor 5.5.5.5 update-source loopback 0
```

```
Neighbor 5.5.5.5 next-hop-self
```

R5  
Router bgp 65001  
No auto-summary  
No synchronization  
Bgp router-id 5.5.5.5

Bgp confederation identifier 1  
Neighbor 1.1.1.1 update-source loopback 0  
Neighbor 2.2.2.2 remote-as 65002  
Neighbor 2.2.2.2 ebgp-multihop 1.1.1.1 up  
Bgp confederation peers 65002

R2  
Router bgp 65002  
No auto-summary  
No synchronization  
Bgp router-id 2.2.2.2  
Bgp confederation identifier 1  
Neighbor 5.5.5.5 remote-as 65001  
Neighbor 5.5.5.5 update-source loopback 0

1. 所有联盟路由器启用 BGP 进程的 AS 号都是子 AS 号，联邦建邻居指的是对方的子 AS 号，外部路由器指联邦内邻居指的是主 AS 号
2. 所有联邦内路由器都要宣称自己属于主 AS
3. 联邦内路由器要建立联邦内 EBGP 链接式需要指定本地和什么子 AS 邻接

Community 属性（团体属性）MPLS VPN 基于这个属性

Well know 公认自由属性 不可传递

#### 1. Standard

No-Advertise 当路由器收到了带有该团体属性的 BGP 路由的时候，路由无法传递给任何其他 BGP 对等体

No-export 不传递性。当路由器收到了带有该团体属性的 BGP 路由的时候，路由无法传递给其他的 AS，只能在 AS 内传递，如果该 AS 内起了联邦，则该路由还可以在联邦内子 AS 之间传递

Local-AS 本地 AS 当路由器收到了该有该团体属性的 BGP 路由的时候，路由只能在接受者所在的 AS 内传递，无论该 AS 是一个主 AS 还是一个联邦内子 AS

以上三者限制了 BGP 路由传递

```
Route-map COM permit 10
Match ip address prefix-list 20
Set community no-advertise
Exit
Router-map COM permit 20
Exit
Neighbor 14.1.1.1 route-map COM out
```

Neighbor 14.1.1.1 send-community

设置 Tag

## 2. Extend MPLS VPN

Ip community-list standard deny permit 3276850

Route-map COM deny 10

Match community Deny

Route-map COM permit 20

Router bgp 65001

Neighbor 1.1.1.1 route-map COM in

BGP ORF outbound route filter 出站路由过滤（优化特性）

原理：当路由器通过其对等体接受路由时如果该路由器使用前缀列表过滤所接收的路由，默认情况该邻居不会知道路由的传递被拒绝，该路由器当拓扑变更或软清进程的时候依旧会给本路由发送这些被过滤路由从而浪费了邻居的 CPU 资源，为了优化需要在路由器双方启用该特性，路由过滤方会通告 OFR 报文发送给路由传递方告知其路由过滤情况，而路由发送方得知情况后无论何时都不会再将被过滤路由发送给过滤方

1 启用 address-family ipv4

2 在该地址簇中激活邻居 active

3 在路由过滤方定义前缀列表指定路由发送放入过滤路由

4 在过滤方指定发送做 ORF，并指定 receive

5 在路由发送指定过滤方做 ORF，并指定 Receive

注意事项：如果在部署 ORF 之前邻接关系已经建立，则一定要硬重置邻接关系

抓路由

标准 ACL 扩展 ACL 前缀列表

高级工具：前缀列表 Route map

前缀列表只能使用：标准 ACL 以及前缀列表抓路由

Route-map 3 种都能使用

前面抓前缀，后面抓掩码，类似前缀列表

Peer-group

Router bgp 1

Neighbor IBGP peer-group

Neighbor IBGP remote-as 1

Neighbor IBGP update-source loopback 0

Neighbor IBGP next hop self

Neighbor 2.2.2.2 peer group IBGP

Neighbor 3.3.3.3 peer group IBGP

Neighbor 5.5.5.5 peer group IBGP

组播 (multicast)

Unicast broadcast Multicast

组播缺点：组播基于 UDP (数据层面)

PIM 动态选择协议，最重要的组播协议 (解决重复报文)

1 Best-effort delivery

2 no congestion avoidance

3 duplicates 重复报文

4 out of sequence delivery

PIM protocol independent multicast

保留的地址

Reserved link local address 224.0.0.0—224.0.0.255

224.0.0.1 三层设备只要联网，会默认监听此地址，只要发送到 224.0.0.1，在同一广播域的节点都会处理此节点

224.0.0.2 只有三层网络设备成了路由器之后才会监听此地址，相当于发往同一个广播域的路由器

224.0.0.5 OSPF 发送报文常用地址

224.0.0.6 发给 DR BDR

224.0.0.9 RIP V2

224.0.0.10 EIGRP

224.0.0.13 PIM 发送 hello 的地址

Globally Scoped address 224.0.1.0-238.255.255.255

Source specific multicast 232.0.0.0—232.255.255.255 SSM (指定源组播)

GLOP addresses 233.0.0.0—233.255.255.255

GLOP AS—Multicast

1—65535

12345 30 39 12345 转换成 16 进制，再转换会 10 进制

233.48.57.0---233.48.57.255

IGMP internet group management protocol

Query 60s

Holdtime 180s

查询者选举原则，比较最后一条路由器连接下游网段的接口的 IP 地址，谁的地址小，谁就充当查询者

检测查询者状态：查询者超时计时器 120S。

## PIM DR

设置基于 IPV4 的组播路由

Ip multicast-routing(开启组播)

Ip pim sparse-mode（启用询问）

Show ip igmp interface fastEthernet 0/0（显示信息）

Show ip igmp group（显示加入的组播组）

路由器模拟 PC 加入广播组

Inf fa 0/0

Ip igmp join-group 224.1.1.1

CGMP：路由器连接交换机接口 IP cgmp

交换机全局配置模式 CGMP

**RPF 校验 Reverse path forwarding:** 一台路由器收到了一个组播组信源发送的组播流量。当路由收到了该组播流量，会提取三层报头源 IP 地址，并在其单播路由表内查找是否拥有去往信源所在网段的单播路由条目，如果没有，则该路由器对于该组播信源没有 RPF 接口，报文在接受接口被丢弃，如果该路由器路由表内拥有去往信源所在网段的单播路由，则查看该路由对应的出站接口和接收到该报文的接口是否为同一个接口，如果是，则转发该报文，如果不是则丢弃该报文

RPF 接口若负载均衡，则出站接口 IP 地址越大，越有可能成为 RPF 接口

组播静态路由

Ip mroute x.x.x.x(组播组服务器的源地址) mask interface

Ip mroute 1.1.1.2 255.255.255.255 serial 0/0

运行 PIM 路由器接口的工作改变

1. 对于第一跳路由器的接收组播流量接口，如果该接口没有启用 PIM，则无论收到什么组播报文，都会本地拆包后将报文丢弃
2. 对于最后一跳路由器连接接受者所在网段的接口如果该接口没有启用 PIM 则路由器不会周期性的发送 IGMP QUERY 报文
3. 对于中间路由器彼此互联的物理接口，如果没有启用 PIM，这些路由器不会通过任何接口转发任何组播报文

DM-push-SPT

SM-Pull-Spt+RPT

Initial flooding

Show ip mroute

使用 auto-RP 原则

1. 整网迁移使用 sparse-dense-mode
2. 依旧是用 sparse-mode 但是所有路由器启用 ip pim auto-rp listener

BSR (bootstrap)C/S 模型    RPC BSRC  
配置

Conf t

Ip pim rp-candidate loopback 10 priority 10 (越低越好先比较) 比 IP 地址也是谁低谁好

Swi

Config t

Ip pim bsr-candidate loopback 0

R5

Show ip pim rp mapping

对于思科路由器优先级 auto-rp    bsr    static

PIM 的 DR

在 IGMPv1 中充当查询者，在 IGMPv2 中无用

DR 的作用主要体现在 SM 中，负责发送 (\*, G) 的 Join 报文，以及 (S, G0) 的 Register 报文（先比优先级越高越好，再比 ip 地址越大越好）

IPV6 特性

巨大地址空间

全球可达性和灵活性

Aggregation 聚合 减少路由表条目数量

Multihoming 多宿主

Autocofiguration

Plug and play

End to end without nat

Renumbering

报头简单

Routing efficiency

Performance and forwarding rate scalability

No broadcast

No checksums

Extension headers

Flow labels

## IPV6 简写

开头的 0 可以省略，一串 0 可以简写为 0，一段 0 可以省略成：：

一个节点想要运行 IPV6，该接口一定会生成一个 link-local 地址，而一个接口有且只有一个 link-local，一个借口可以拥有任意个 AGUA，无论使用什么样的 IGP，通告路由的下一跳都是邻居接口的 link-local 地址

## (EUI) -64

借助 mac 地址 48 位

把 MAC 地址从中分开添加 FFFE

从左往右数第 7bit，0,1 互换

一个节点通过无状态地址自动获悉了接口的基于 EUI64 的 AGUA 地址的同时，如果该设备是一台局域 IPV6 的 PC，则该设备同时会指定给其分配网段前缀的路由器为其缺省网管

ICMPv6 type 135 136 取代 ARP，检测重复地址，DAD

TYPE 133 134， stateless address auto configuration renumbering（路由器接口定期发送 RA，路由器接口地址换了，发送新的 RA，新的前缀，PC 自动改变地址）

不发送 RA

ipv6 nd ra suppress(以太网接口抑制)

## IPV6 ACL

ipv6 access-l any

Permit tcpist TEST

Deny ipv6 2001::1/128

Permit ipv6 host 2001::2 any

Exit

Interface fa 0/0

ipv6 traffic-filter TEST out

## IPV6 隐式 ACE

Permit icmp any any nd-ns (135)

Permit icmp any any nd-na (136)

Deny ipv6 any any

## IPv6 静态路由

### 1 Static

一台路由器没有启用 IPv6 unicast-routing 一样可以配置静态路由，此时路由只能实现去往邻居路由器直连接口的访问，无法隔跳访问，如需隔跳访问，需要在路由器上启用 ipv6 unicast-routing

对于出站接口是 MA 网段接口,写 IPv6 静态路由的时候要伴随下一跳接口,不然无法访问,如果是 P2P 可以直接携带出站接口

## 2 RRPng

该协议工作在应用层,UDP 封装,端口号 521,距离矢量协议,无类协议,默认不开启自动汇总。30 秒发送更新报文,包括所有被选购接口的直连路由和打 R 的路由,水平分割生效

```
R2(config)#ipv6 router rip A
```

```
R2(config)#interface fastEthernet 0/0
```

```
R2(config-if)#ipv6 rip A enable
```

## EIGRP

4 层协议,协议号 88 无类协议,默认不开启自动汇总,依旧是思科私有的,通过邻居发现以及恢复机制,发给 FF02::10,建邻居,传拓扑,加入拓扑表,找最优路由,备份路由(DUAL)只支持触发更新。相同的进程号,不同的路由器 ID,相同的 K 值,相同的认证信息

## Conf t

```
IPv6 router eigrp 110
```

```
Router-id 2.2.2.2
```

```
No shutdown
```

宣告接口

```
Interface loopback 0
```

```
IPv6 eigrp 100
```

使用了 link-local 建邻居

查看邻居 show ipv6 eigrp neighbor

显示接口信息

```
Show ipv6 eigrp interfaces fastethernet 0/0
```

显示路由表

```
Show ipv6 route eigrp
```

```
Show ipv6 eigrp 100 traffic
```

## OSPF

在 ipv6 中运行的 ospf 是 v3,LSA 传入 LSDB,链路状态协议,4 层,协议号 89.

7 级状态

Down, initial, two-way, ex-start(master, slave), exchange (交互 LSA 摘要) loading (lsr, lsu, ls-ack), full

```
IPv6 router ospf 110(本地意义)
```

```
Router-id 2.2.2.2 (手工指定,环回口最大 ip,物理接口上最大 ip,没有必要可达,标识)
```

```
Interface loopback 0
```

```
IPv6 ospf 110 area 0.0.0.0
```

```
Show ipv6 ospf neighbor
```

```
Show ipv6ospf interface
```



Show ipv6 ospf interface brief

Show ipv6 ospf database

Area 0 authentication ipsec spi 256 md5 1234567890ABCDEF1234567890abcdef

Area 1 virtual-link 2.2.2.2 authentication ipsec spi 256 md5 密钥

Area 0 nssa

Isis

Router isis

Net 49.0001.2222.2222.2222.00

Log-adjacency-changes all

Int loopback 0

Ipv6 router isis

Show isis neighbor

Show isis database

Show isis database verbose

Show ipv6 route

Isis 充分发

Address-family ipv6

Redistribute connected level-1-2

BGP 路由

Router bgp 2

No auto-summary

No sunchrnoization bgp router-id 2.2.2.2

Ipv4 ipv6

Tunnel, dual stack, translation

Overlay tunnels(手工 tunnel)

GRE tunnel 用 IPV4 报头封装 IPv6 报头

IPv6IP 3 层 tunnel

Site-local, AGUA, link-local

1 A B 直接启 tunnel, ipv6ip

2 申请 agua 地址, tunnel 两端配置

3 基于 tunnel 口启 IGP

1. 在 IPv6 边界路由器之间建立一个 tunnel 口，建议将 tunnel 的源和目的设置为可达的环回口地址
2. 将 tunnel 口的模式改变为 ipv6ip，实现让 tunnel 将 ipv6 报文封装成 ipv4 数据报
3. 在 tunnel 起 AGUA 地址，保证 tunnel 两端的地址在同一个 ipv6 网段内
4. 在 tunnel 口两端将其宣告进某 igp 协议，建立邻接关系并传路由
5. 在两台边界路由器上将通过 tunnel 口建立的协议和本地 as 的协议单点双向重分发

R2

Interface tunnel 2

Tunnel source 2.2.2.2

Tunnel destination 4.4.4.4

Tunnel mode ipv6ip

Exit

R4

Interface tunnel 4

Tunnel source 4.4.4.4

Tunnel destination 2.2.2.2

Tunnel mode ipv6ip

Ipv6 address 2001:0:0::24::4/64

No shutdown

R2

Int tunnel 2

Ipv6 address 2001:0:0:24::2/64

No shutdown

Ipv6 router eigrp

Router-id 2.2.2.2

Ipv6 eigrp 90

R4

Ipv6 router eigrp 90

No shutdown

Router-id 4.4.4.4

Exit

Int tunnel 4

Ipv6 eigrp 90

重分发

Ipv6 router eigrp 90

Redistribute ospf 90 include-connected metric 1000 100 255 1 1500

Ipv6 router ospf 110

Redistribute eigrp 90 include-connected

6to4tunneling 推荐

```
Interface tunnel 4'  
Tunnel source 4.4.4.4  
Tunnel mode ipv6ip 6to4  
Ipv6 unnumbered loopback 0  
写静态路由  
Ipv6 route 2002::/16 tunnel 4
```

```
R2  
Interface tunnel 2  
Tunnel source 2  
Tunnel source 2.2.2.2  
Tunnel mode ipv6ip 6to4  
Ipv6 unnumbered loopback 0  
Exit  
Ipv6 route 2002::/16 tunnel 4
```

```
下放缺省路由  
Ipv6 route ospf 110  
Default-information originate always
```

```
R4 下放路由  
Int fa 0/0  
Ipv6 rip A default-information originate
```

1. 将 ipv6 园区网内所有节点的地址迁移到 2002（边界路由器 Tunnel 源）
2. 将边界路由器启用 6to4tunnel，只用指定 tunnel source 给该接口分配一个已经在本地其他接口使用的 2002 的 ipv6 地址 ipv6 unnumbered
3. 边界路由器指定一条去往 2002::/16 的聚合路由直接指定出站接口为 tunnel 口
4. 在该边界路由器上将聚合静态路由重分发进 IGP，或向 IGP 域内下放缺省路由

MPLS  
Multi-protocol label switching

由运营商端的路由器添加标签，当报文传递到运营商端路由器时添加，  
FEC forwarding equal ant class（转发等价类。逻辑分类）就是一条路由条目  
去往相同的目的网段

FIB adjacency table  
Forwarding information base

Ip cef 启用 cef

在一台路由器上，不能为不同的路由条目分发相同的标签，每条路由条目对应一个本地唯一的标签，例外是 0-15 标签，如果给路由条目分发的标签取值范围在 0-15 之间，此时多条路由可以对应相同的被保留标签

TDP LDP 只能为静态路由，直连路由，以及 igb 路由分发标签，bgp 不分发标签

1. IP routing protocols build the IP routing table.
2. Each LSR assigns a label to every destination in the IP routing table independently. <sup>^</sup> TDP LDP
3. LSRs announce their assigned labels to all other LSRs.
4. Every LSR builds its LIB, LFIB, and FIB data structures based on the received labels.

LIB 本地标签，邻居传来的标签，LFIB 标签映射，收到什么标签换成什么标签。FIB 启用三层路由后的 download

对于一条路由条目，如果该路由器路由表汇总该路由条目的出站接口是一个没有启用 mpls 的接口，该路由器就是最后一跳路由器，或者该路由条目对应的下一条邻居不是本地的 TDP/LDP 邻居时，该路由器同样为最后一跳路由器，只要一台路由器收到了一条路由条目的标签是 3，则该路由器就会判断自己就是倒数第二条路由器

FEC LDP/TDP 为本地路由条目分发标签，把本地标签分发给邻居， LIB/LFIB  
先查 LIB，查被抑制路由远程标签进行绑定 CEF（先运行 cef 才能运行 MPLS，形成两张表  
FIB（标签插入） adj table

部署 MPLS

0.先运行 IGP

1. Configure CEF
2. Configure MPLS on a frame mode interface
3. (Optional) Configure the MTU size in label switching

IPMTU

修改 ldp 路由器 id

Mpls ldp router-id loopback 0 force

修改 MTU

R1(config)#interface fastEthernet 0/0

R1(config-if)#mpls mtu 1504

邻居 Show 用于排错

R1#show mpls ldp neighbor

查看 fib

R1#show ip cef detail

查看 LIB

R1#show mpls ldp bindings

查看 Ifib

Show mpls forwarding-table

R2#traceroute ip 3.3.3.3 source 2.2.2.2

1 12.1.1.1 [MPLS: Label 17 Exp 0] 52 msec 44 msec 40 msec

2 13.1.1.3 64 msec 60 msec 80 msec

VRF virtual routing forwarding 一个 VRF 就是一个 MPLS VPN 中的实例（进程）

一台 PE 为一个公司提供 MPLS VPN 就要为该公司定义一个本地唯一的 VRF 进程

PE 创建了 VRF 以后，一定要将其和某个连接 CE 接口关联

Router distinguishers 64bits X:Y 只能在域内进行区分，只能添加一个

Route targets 具有全局意义，可以添加多个，一定要设定为相同的值

只有 PE 需要启用 VRF

配置方法：

R3(config)#ip vrf A

R3(config-vrf)#rd 10:10

R3(config-vrf)#route-target 10:10

R3(config)#interface serial 1/0

R3(config-if)#ip vrf forwarding A

R3(config-if)#ip address 35.1.1.3 255.255.255.0

R3(config)#router bgp 1

R3(config-router)#no bgp default ipv4-unicast

R3(config-router)#no auto-summary

R3(config-router)#no syn

R3(config-router)#bgp router-id 3.3.3.3

R3(config-router)#neighbor 2.2.2.2 remote-as 1

R3(config-router)#neighbor 2.2.2.2 update-source loopback 0

R3(config-router)#address-family vpnv4

R3(config-router-af)#neighbor 2.2.2.2 activate

R2(config-router)#address-family ipv4 vrf A

R2(config-router-af)#network 4.4.4.0 mask 255.255.255.0

```
show ip bgp vpnv4 all 4.4.4.0 255.255.255.0
```

```
R2(config-router)#address-family vpnv4
```

```
R2(config-router-af)#neighbor 3.3.3.3 send-community both
```

第一步把 IP 启用好，在 MPLS 域启用 MPLS。Pe 端 vrf，rt，rd，pe 上把连接 ce 的接口和相应的 vrf 关联，在 ce 和 pe 之间运行 igp 建立连接关系。Pe 和另一台 pe 之间建立 vpnv4 的连接关系，address-family vpnv4，激活邻居 neighbor 3.3.3.3 send-community both

默认通过 igp 获得的路由，重分发，或者 network，在 address-family ipv4 vrf A 相应的参数下做，两台一样，先在 pe 段 show 路由，再在 ce 段 show 路由，如果不同一般是 ce 没有获得路由，错在 pe 上，如果 peok，有可能 mpls 有问题。在 pe 路由器上 show mpls 邻居，如果 lib，lfib 正常应该 ok。问题 1 路由传递有问题，2 数据层面 mpls 有问题