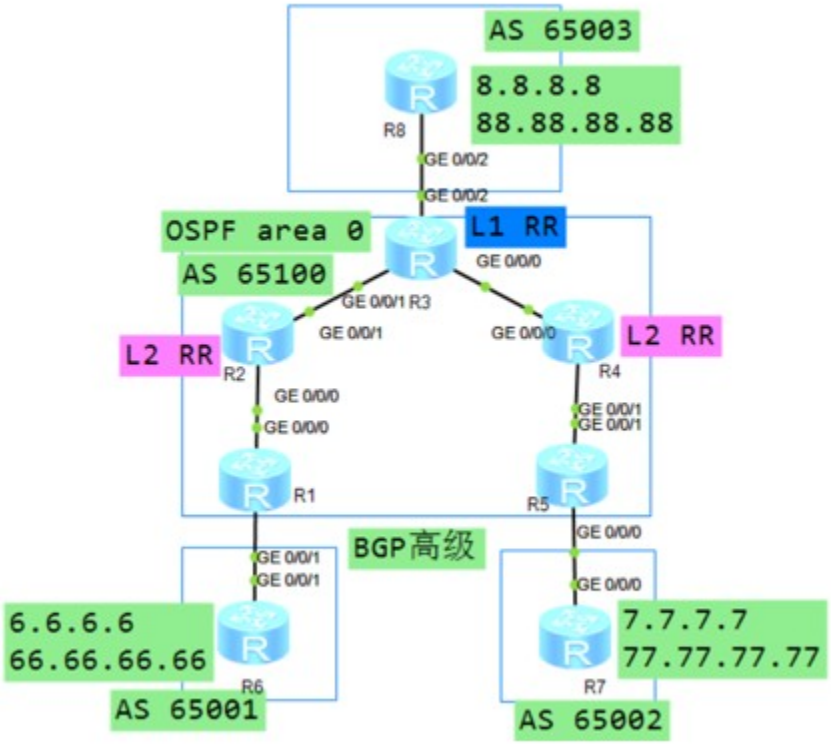
HCIP-Datacom 分解实验 - BGP 高级特性

臧家林制作

BGP 高级特性

某企业存在两个分公司与一个总公司，公司共有两个业务：OA 办公和财务。
OA：R6、R7、R8 的 Loopback0 接口网段是 OA 业务网段。分支之间，分支与总公司之间能够互相传递 OA 数据，对于 OA 业务相关路由需要标注始发 AS。
财务：R6、R7、R8 的 Loopback1 接口网段是财务业务网段，由于财务业务较为机密，因此只允许分公司与总公司之间传递财务数据，分公司之间禁止传递财务数据。
网络管理员需要搭建一个满足这些需求的同时又有一定安全性的网络。



实验要求：

1. 在分公司与骨干网络之间部署 GTSM 与 BGP 认证，保证 BGP 网络安全。
2. R1、R3、R5 配置与 R2、R4 的 IBGP 对等体关系，同时将 R1、R3、R5 配置为 R2、R4 的反射器客户端。
3. R3 作为一级 RR 需要配置与 R2、R4 的 IBGP 对等体关系，同时将 R2、R4 配置为 R3 的反射器客户端。
4. 在 R1、R2、R3 上给 Loopback0 接口路由打上 Community 值，用于标注 OA 业务的始发 AS。
5. 在 R1、R3、R5 上配置路由策略，使用 AS-Path Filter 工具过滤 Loopback1 接口路由。

宣告 OSPF 接口时，使用精确宣告的方式

基本配置

R1：

```
undo ter mo
```

```
sys
sysname R1
user-interface console 0
idle-timeout 0 0
int loo0
ip add 1.1.1.1 24
int g0/0/0
ip add 192.168.12.1 24
int g0/0/1
ip add 192.168.16.1 24
q
ospf router-id 1.1.1.1
area 0
net 192.168.12.1 0.0.0.0
net 1.1.1.1 0.0.0.0
q
```

R2:

```
undo ter mo
sys
sysname R2
user-interface console 0
idle-timeout 0 0
int loo0
ip add 2.2.2.2 24
int g0/0/0
ip add 192.168.12.2 24
int g0/0/1
ip add 192.168.23.2 24
q
ospf router-id 2.2.2.2
area 0
net 192.168.12.2 0.0.0.0
net 192.168.23.2 0.0.0.0
```

net 2.2.2.2 0.0.0.0
q

R3:
undo ter mo
sys
sysname R3
user-interface console 0
idle-timeout 0 0
int loo0
ip add 3.3.3.3 24
int g0/0/0
ip add 192.168.34.3 24
int g0/0/1
ip add 192.168.23.3 24
int g0/0/2
ip add 192.168.38.3 24
ospf router-id 3.3.3.3
area 0
net 192.168.34.3 0.0.0.0
net 192.168.23.3 0.0.0.0
net 3.3.3.3 0.0.0.0
q

R4:
undo ter mo
sys
sysname R4
user-interface console 0
idle-timeout 0 0
int loo0
ip add 4.4.4.4 24
int g0/0/0
ip add 192.168.34.4 24

```
int g0/0/1
ip add 192.168.45.4 24
ospf router-id 4.4.4.4
area 0
net 192.168.34.4 0.0.0.0
net 192.168.45.4 0.0.0.0
net 4.4.4.4 0.0.0.0
q
```

R5:

```
undo ter mo
sys
sysname R5
user-interface console 0
idle-timeout 0 0
int loo0
ip add 5.5.5.5 24
int g0/0/0
ip add 192.168.57.5 24
int g0/0/1
ip add 192.168.45.5 24
ospf router-id 5.5.5.5
area 0
net 192.168.45.5 0.0.0.0
net 5.5.5.5 0.0.0.0
q
```

R6:

```
undo ter mo
sys
sysname R6
user-interface console 0
idle-timeout 0 0
int loo0
```

```
ip add 6.6.6.6 24
int loo1
ip add 66.66.66.66 24
int g0/0/1
ip add 192.168.16.6 24
q
```

R7:

```
undo ter mo
sys
sysname R7
user-interface console 0
idle-timeout 0 0
int loo0
ip add 7.7.7.7 24
int loo1
ip add 77.77.77.77 24
int g0/0/0
ip add 192.168.57.7 24
q
```

R8:

```
undo ter mo
sys
sysname R8
user-interface console 0
idle-timeout 0 0
int loo0
ip add 8.8.8.8 24
int loo1
ip add 88.88.88.88 24
int g0/0/2
ip add 192.168.38.8 24
q
```

配置 BGP

配置 EBGP 对等体，在 EBGP 对等体之间部署 GTSM 与 BGP 认证

valid-ttl-hops 指定需要检测的 TTL 跳数值。 取值范围是 1～255，缺省值是 255。

如果配置为 hops，则被检测的报文的 TTL 值有效范围为[255–hops+1, 255]

R1：

```
bgp 65100
router-id 1.1.1.1
peer 192.168.16.6 as-n 65001
peer 192.168.16.6 password simple huawei
peer 192.168.16.6 valid-ttl-hops 255
q
```

R6：

```
bgp 65001
router-id 6.6.6.6
peer 192.168.16.1 as-n 65100
peer 192.168.16.1 password simple huawei
peer 192.168.16.1 valid-ttl-hops 255
q
```

R5：

```
bgp 65100
router-id 5.5.5.5
peer 192.168.57.7 as-n 65002
peer 192.168.57.7 password simple huawei
peer 192.168.57.7 valid-ttl-hops 255
q
```

R7 :
bgp 65002
router-id 7.7.7.7
peer 192.168.57.5 as-n 65100
peer 192.168.57.5 password simple huawei
peer 192.168.57.5 valid-ttl-hops 255
q

R3 :
bgp 65100
router-id 3.3.3.3
peer 192.168.38.8 as-n 65003
peer 192.168.38.8 password simple huawei
peer 192.168.38.8 valid-ttl-hops 255
q

R8 :
bgp 65003
router-id 8.8.8.8
peer 192.168.38.3 as-n 65100
peer 192.168.38.3 password simple huawei
peer 192.168.38.3 valid-ttl-hops 255
q

检查一下, R1 R3 R5 的 EBGP 邻居已经建立好，邻居关系都到达了“Established”状态

```
[R1-bgp]dis bgp peer
192.168.16.6        4                65001
5             7           0 00:03:18
Established         0
```

配置 IBGP 对等体与多级 RR

R2 与 R4 是二级 RR，R1、R3、R5 是 R2 与 R4 的客户端，同级 RR 为了避免路由互相传递，一般需要修改 Cluster ID，将 Cluster ID 设置为 24.24.24.24。R3 是一级 RR，R2、R4 是 R3 的客户端。
按照拓扑规划部署 IBGP 对等体，基于 Loopback 接口地址建立 IBGP 对等体，由于邻居较多，需使用 peer-group 方式配置。

R1：
```
bgp 65100
group 1
peer 2.2.2.2 group 1
peer 4.4.4.4 group 1
peer 1 next-hop-local
peer 1 connect-interface LoopBack0
q
```

R2:
```
bgp 65100
group 1
peer 1.1.1.1 group 1
peer 3.3.3.3 group 1
peer 4.4.4.4 group 1
peer 5.5.5.5 group 1
peer 1 con loo0
q
```

R3:
```
bgp 65100
group 1
peer 2.2.2.2 group 1
peer 4.4.4.4 group 1
peer 1 next-hop-local
```

peer 1 connect-interface LoopBack0
q

R4:
bgp 65100
group 1
peer 1.1.1.1 group 1
peer 2.2.2.2 group 1
peer 3.3.3.3 group 1
peer 5.5.5.5 group 1
peer 1 con loo0
q

R5:
bgp 65100
group 1
peer 2.2.2.2 group 1
peer 4.4.4.4 group 1
peer 1 next-hop-local
peer 1 connect-interface LoopBack0
q

检查 IBGP 配置结果

基于 R2、R4 的邻居表可以发现 AS65100 内的路由器之间 IBGP 对等体已经建立。

```
[R4]dis bgp peer
  Peer       V           AS   MsgRcvd   MsgSent   OutQ
Up/Down         State Pre    fRcv
 1.1.1.1          4        65100         2         2
0 00:00:30 Established      0
  2.2.2.2          4        65100         2         2
0 00:00:30 Established      0
  3.3.3.3          4        65100         2         2
0 00:00:30 Established      0
```

5.5.5.5 4 65100 2 3
0 00:00:02 Established 0

部署多级 RR

R2 与 R4 是二级 RR，R1、R3、R5 是 R2、R4 的客户端，
R2 与 R4 配置相同的 Cluster ID。
R3 是一级 RR，R2、R4 是 R3 的客户端。
R2:

```
bgp 65100
peer 1 reflect-client
reflector cluster-id 24.24.24.24
q
```

R4:

```
bgp 65100
peer 1 reflect-client
reflector cluster-id 24.24.24.24
q
```

R3:

```
bgp 65100
peer 1 reflect-client
reflector cluster-id 3.3.3.3
q
```

检查 RR 配置结果

```
[R2]dis bgp group 1

 BGP peer-group: 1
 Remote AS: 65100
 PeerSession Members:
    1.1.1.1                 3.3.3.3                 4.4.4.4
5.5.5.5
```

It's route-reflector-client
1.1.1.1 4 65100 31 32
0 00:29:55 Established 0
3.3.3.3 4 65100 30 32
0 00:28:42 Established 0
4.4.4.4 4 65100 13 14
0 00:10:03 Established 0
5.5.5.5 4 65100 11 13
0 00:09:34 Established 0

发布 BGP 路由

R6 R7 R8 上的 Loopback0、Loopback1、接口路由需要发布到 BGP 中，发布后骨干网将通过路由策略控制路由发布。

R6:
```
bgp 65001
net 6.6.6.0 24
net 66.66.66.0 24
q
```

R7:
```
bgp 65002
net 7.7.7.0 24
net 77.77.77.0 24
q
```

R8:
```
bgp 65003
net 8.8.8.0 24
net 88.88.88.0 24
q
```

配置 Route-Policy 为 OA 业务打上标签

通过 Community 属性可以为路由条目打上标签，这样网络

管理员就知道该路由来自哪个 AS。
本实验只需要给 R6 R7 R8 的 Loopback0 接口路由打上标签即可。
Community 属性默认不发送给邻居，需要手工开启功能。

R1:
bgp 65100
peer 1 advertise-community
peer 192.168.16.6 advertise-community
q

R2:
bgp 65100
peer 1 advertise-community
q

R3:
bgp 65100
peer 1 advertise-community
peer 192.168.38.8 advertise-community
q

R4:
bgp 65100
peer 1 advertise-community
q

R5:
bgp 65100
peer 1 advertise-community
peer 192.168.57.7 advertise-community
q

R6:

bgp 65001
peer 192.168.16.1 advertise-community
q

R7:
bgp 65002
peer 192.168.57.5 advertise-community
q

R8:
bgp 65003
peer 192.168.38.3 advertise-community
q

配置路由策略，为 Loopback0 接口路由打上相应 Community 值。
R6:
ip ip-prefix 6 permit 6.6.6.0 24
route-policy 10 permit node 10
if-match ip-prefix 6
apply community 65001:6
route-policy 10 permit node 20
bgp 65001
peer 192.168.16.1 route-policy 10 export
q

R7:
ip ip-prefix 7 permit 7.7.7.0 24
route-policy 10 permit node 10
if-match ip-prefix 7
apply community 65002:7
route-policy 10 permit node 20
bgp 65002
peer 192.168.57.5 route-policy 10 export

q

R8:
ip ip-prefix 8 permit 8.8.8.0 24
route-policy 10 permit node 10
if-match ip-prefix 8
apply community 65003:8
route-policy 10 permit node 20
bgp 65003
peer 192.168.38.3 route-policy 10 export
q

检查配置结果, 在 R1 上查看团体属性值已经打成功

```
[R1]dis bgp routing-table community
 Total Number of Routes: 5
Network                 NextHop          MED
LocPrf      PrefVal Community

 *>    6.6.6.0/24          192.168.16.6     0
0         <65001:6>
 *>i   7.7.7.0/24          5.5.5.5          0
100         0       <65002:7>
 * i                              5.5.5.5          0
100         0       <65002:7>
 *>i   8.8.8.0/24          3.3.3.3          0
100         0       <65003:8>
 * i                              3.3.3.3          0
100         0       <65003:8>
```

配置 Route-Policy，控制财务业务

财务业务比较敏感，只允许在 R6、R8 以及 R7、R8 之间转发流量。在没有 VPN 的情况下，只能通过控制路由收发达到目的。

为了简化过滤配置，可以直接使用 AS-Path Filter 与 Route-P

olicy，在 R1 与 R2 上过滤路由条目。
控制路由时需要特别注意，不要将 Loopback0 接口路由过滤。可使用 Community Filter 将 Loopback0 接口路由提前放通，然后再过滤 Loopback1 接口路由。

R1：
```
ip community-filter basic R7 permit 65002:7
ip as-path-filter R7 permit 65002$
route-policy 10 permit node 10
if-match community-filter R7
route-policy 10 deny node 20
if-match as-path-filter R7
route-policy 10 permit node 30
bgp 65100
peer 192.168.16.6 route-policy   10 export
q
```

R5：
```
ip community-filter basic R6 permit 65001:6
ip as-path-filter R6 permit 65001$
route-policy 10 permit node 10
if-match community-filter R6
route-policy 10 deny node 20
if-match as-path-filter R6
route-policy 10 permit node 30
bgp 65100
peer 192.168.57.7 route-policy   10 export
q
```

检查配置结果

可以看到此时 R6 的 BGP 路由表中关于 R7 Loopback1 接口路由（77.77.77.0）已经被过滤，R7 的 BGP 路由表中关于 R6 Loopback1 接口路由（66.66.66.0）已经被过滤，R8

的 BGP 路由表中依然是完整的路由表。

可以看到 R6 有 7.7.7.0 但没有　77.77.77.0

```
[R6]dis bgp routing-table
 *>    6.6.6.0/24              0.0.0.0           0
0        i
 *>    7.7.7.0/24              192.168.16.1
0        65100 6500   2i
 *>    8.8.8.0/24              192.168.16.1
0        65100 6500   3i
 *>    66.66.66.0/24       0.0.0.0           0
0        i
 *>    88.88.88.0/24       192.168.16.1
0        65100 6500    3i
```

可以看到 R7 有 6.6.6.0 但没有　66.66.66.0

```
[R7]dis bgp routing-table
 *>    6.6.6.0/24              192.168.57.5
0        65100 6500 1i
 *>    7.7.7.0/24              0.0.0.0           0
0        i
 *>    8.8.8.0/24              192.168.57.5
0        65100 6500 3i
 *>    77.77.77.0/24       0.0.0.0           0
0        i
 *>    88.88.88.0/24       192.168.57.5
0        65100 6500   3i
```