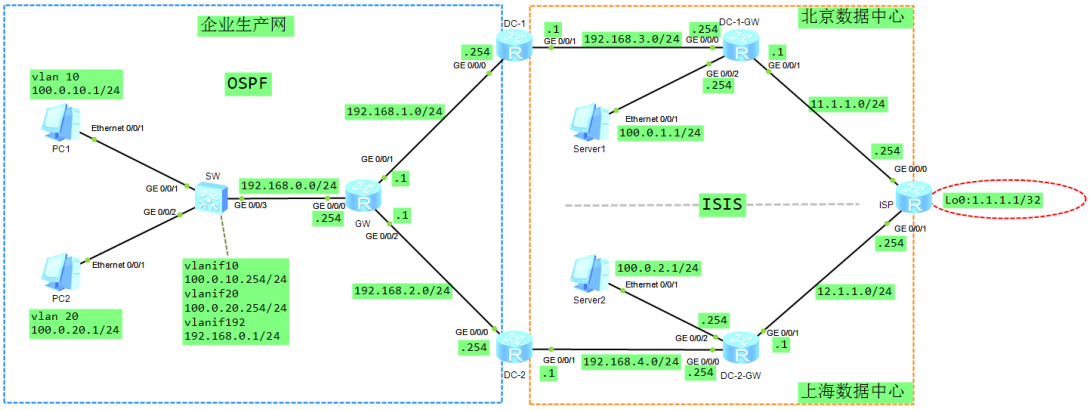
【HCIP 实验 10】路由控制

一、　　实验拓扑



二、　　实验需求及解法

1.企业生产网运行 OSPF，完成以下需求：

1.1 OSPF 进程号为 1，全部划入区域 0

1.2 RID 如下：

DC-1：192.168.100.1

DC-2：192.168.100.2

GW：192.168.100.3

SW：192.168.100.4

1.3 全部使用通配符 0.0.0.0 通告。

1.4 确认 PC1/2 可以访问 DC-1/2

DC-1

```
ospf 1 router-id 192.168.100.1
 area 0.0.0.0
  network 192.168.1.254 0.0.0.0
```

```
#
DC-2：
ospf 1 router-id 192.168.100.2
 area 0.0.0.0
  network 192.168.2.254 0.0.0.0
#
GW:
ospf 1 router-id 192.168.100.3
 area 0.0.0.0
  network 192.168.0.254 0.0.0.0
  network 192.168.1.1 0.0.0.0
  network 192.168.2.1 0.0.0.0
#
SW:
ospf 1 router-id 192.168.100.4
 area 0.0.0.0
  network 100.0.10.254 0.0.0.0
  network 100.0.20.254 0.0.0.0
  network 192.168.0.1 0.0.0.0
```

2.数据中心运行 ISIS，完成以下需求：
2.1 ISIS 进程号为 1.
2.2 北京数据中心区域号为 49.0001，上海数据中心区域号为 49.0002
ISP 的区域号为 49.0100
2.3 设备系统 ID 如下：
DC-1:0000.0001.0001
DC-1-GW:0000.0001.0254
DC-2:0000.0002.0001
DC-2-GW:0000.0002.0254
ISP:0000.0000.0100
2.4 所有 ISIS 路由器都是 Level-2 路由器
2.5 ISP 上引入 6 条外部直连路由，确认 DC 路由器都能收到。

```
DC-1:
isis 1
 is-level level-2
 network-entity 49.0001.0000.0001.0001.00
interface GigabitEthernet0/0/1
 isis enable 1
#
DC-1-GW:
```

```
isis 1
 is-level level-2
 network-entity 49.0001.0000.0001.0254.00
interface GigabitEthernet0/0/0
 isis enable 1
interface GigabitEthernet0/0/1
 isis enable 1
interface GigabitEthernet0/0/2
 isis enable 1
#
DC-2:
isis 1
 is-level level-2
 network-entity 49.0002.0000.0002.0001.00
interface GigabitEthernet0/0/1
 isis enable 1
#
DC-2-GW:
isis 1
 is-level level-2
 network-entity 49.0002.0000.0002.0254.00
interface GigabitEthernet0/0/0
 isis enable 1
interface GigabitEthernet0/0/1
 isis enable 1
interface GigabitEthernet0/0/2
 isis enable 1
#
ISP:
isis 1
 is-level level-2
 network-entity 49.0100.0000.0000.0100.00
 import-route direct
interface GigabitEthernet0/0/0
 isis enable 1
interface GigabitEthernet0/0/1
 isis enable 1
```

3.路由引入

3.1 在 DC-1 将 OSPF 和 ISIS 双向引入。

DC-1:

```
ospf 1 router-id 192.168.100.1
 import-route isis 1
#
isis 1
 import-route ospf 1
```

3.2 在 DC-2 将 OSPF 和 ISIS 双向引入。

DC-2:

```
ospf 1 router-id 192.168.100.2
 import-route isis 1
#
isis 1
 import-route ospf 1
```

3.3 在 GW 查看路由，确认去往北京/上海数据中心的路由，都有 DC-1 和 DC-2 两个下一跳

```
[GW]dis ip routing-table
```

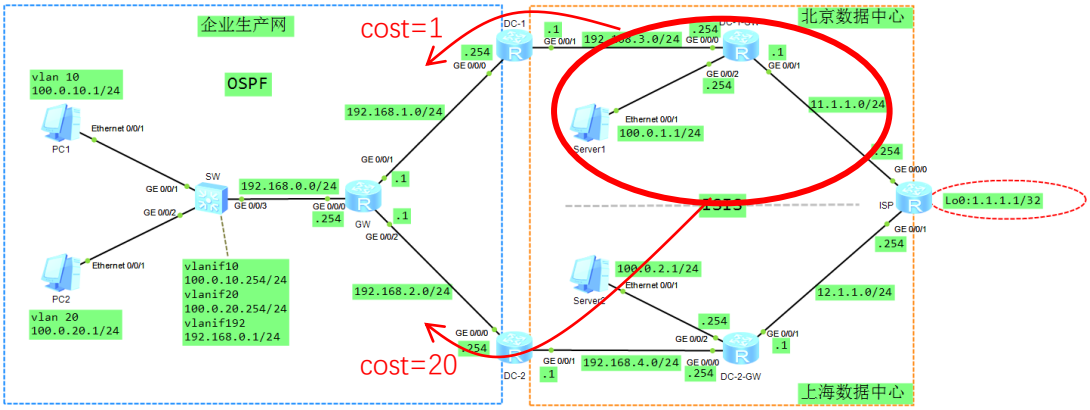
Destination/Mask	Proto	Pre	Cost	Flags	NextHop
1.1.1.1/32	O_ASE	150	1	D	192.168.1.254
	O_ASE	150	1	D	192.168.2.254
11.1.1.0/24	O_ASE	150	1	D	192.168.1.254
	O_ASE	150	1	D	192.168.2.254
12.1.1.0/24	O_ASE	150	1	D	192.168.1.254
	O_ASE	150	1	D	192.168.2.254
100.0.1.0/24	O_ASE	150	1	D	192.168.1.254
	O_ASE	150	1	D	192.168.2.254
100.0.2.0/24	O_ASE	150	1	D	192.168.1.254
	O_ASE	150	1	D	192.168.2.254

4.路由策略

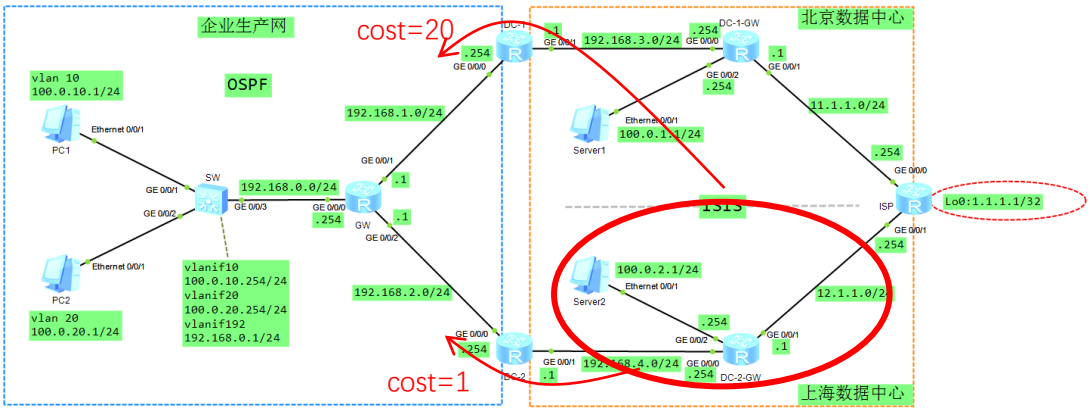
为确保企业生产网去往北京数据中心优先走 DC-1，去往上海数据中心优先走 DC-2 在路由引入时部署以下路由策略：

需求解析：结合需求 3.3，GW 去往北京和上海暂时都有两个下一跳。本需求即是要求北京路由的下一跳是 DC-1，上海路由的下一跳是 DC-2。由于都是 OSPF 协议，影响选路的就是 cost 值，而这些 cost 值目前都是引入时的默认值。

北京数据中心路由在 DC-1 上引入到 OSPF 时，使用默认 cost 为 1，在 DC-2 上引入到 OSPF 时使用策略修改 cost 为 20，那么当企业网 GW 收到北京路由时，会选择 cost 更小的 DC-1 作为最佳下一跳。如下图：



上海数据中心路由正好相反，DC-2 引入到 OSPF 使用默认 cost 1，DC-1 引入到 OSPF 使用策略修改 cost 为 20，那么企业网 GW 收到上海路由时，会选择 cost 更小的 DC-2。如下图：



这一套策略在控制层面修改路由的 cost 值，达到影响选路的目的。

4.1 使用 ip-prefix 匹配路由

DC-1 前缀列表名称为 beijing，index 自动生成，匹配北京数据中心路由：192.168.3.0/24 100.0.1.0/24 11.1.1.0/24

DC-1:

ip ip-prefix beijing permit 192.168.3.0 24

ip ip-prefix beijing permit 100.0.1.0 24
ip ip-prefix beijing permit 11.1.1.0 24
DC-2 前缀列表名称为 shanghai，index 自动生成，匹配上海数据中心路由：192.168.4.0/24 100.0.2.0/24 12.1.1.0/24
DC-2:
ip ip-prefix shanghai permit 192.168.4.0 24
ip ip-prefix shanghai permit 100.0.2.0 24
ip ip-prefix shanghai permit 12.1.1.0 24

4.2 使用 route-policy 修改路由 cost 值，
DC-1 路由策略名称为 bjcost：
node 10 匹配北京数据中心路由，不修改 cost；
node 100 匹配其他所有路由，修改 cost 为 20。
DC-1:
route-policy bjcost permit node 10
 if-match ip-prefix beijing
#
route-policy bjcost permit node 100
 apply cost 20
DC-2 路由策略名称为 shcost：
node 10 匹配上海数据中心路由，不修改 cost；
node 100 匹配其他所有路由，修改 cost 为 20。
DC-2:
route-policy shcost permit node 10
 if-match ip-prefix shanghai
#
route-policy shcost permit node 100
 apply cost 20

4.3 DC-1 和 DC-2 将 ISIS 引入 OSPF 时，分别调用路由策略。
DC-1:
ospf 1
 import-route isis 1 route-policy bjcost
#
DC-2:
ospf 1
 import-route isis 1 route-policy shcost

4.4 在 GW 确认去往北京数据中心的路由下一跳为 DC-1，去往上海数据中心的路由下一跳为 DC-2。

[GW]dis ip routing-table

```
    11.1.1.0/24  O_ASE    150  1           D   192.168.1.254
    12.1.1.0/24  O_ASE    150  1           D   192.168.2.254
  100.0.1.0/24   O_ASE    150  1           D   192.168.1.254
  100.0.2.0/24   O_ASE    150  1           D   192.168.2.254
```

5.策略路由

因生产需要，vlan10 访问 ISP 需通过北京数据中心，vlan20 访问 ISP 需通过上海数据中心。在 GW 上配置 PBR，完成以下需求：

需求解析：本需求有两类流量 vlan10-ISP 和 vlan20-ISP，这两类流量目标相同，无法通过修改路由表来分别选路，必须在转发层面直接改变数据流量的下一跳地址。

5.1 使用 acl3010，规则序号 5，匹配 vlan10 访问 1.1.1.1/32 的流量。

```
acl number 3010
 rule 5 permit ip source 100.0.10.0 0.0.0.255 destination 1.1.1.1 0
```

5.2 使用 acl3020，规则序号 5，匹配 vlan20 访问 1.1.1.1/32 的流量。

```
acl number 3020
 rule 5 permit ip source 100.0.20.0 0.0.0.255 destination 1.1.1.1 0
```

5.3 使用流分类定义感兴趣流，vlan10 的流分类名称为 10，vlan20 的流分类名称为 20.

```
traffic classifier 10
 if-match acl 3010
traffic classifier 20
 if-match acl 3020
```

5.4 使用流行为定义下一跳地址

去往北京数据中心 DC-1 的流行为名称为 to1

去往上海数据中心 DC-2 的流行为名称为 to2

```
traffic behavior to1
 redirect ip-nexthop 192.168.1.254
traffic behavior to2
 redirect ip-nexthop 192.168.2.254
```

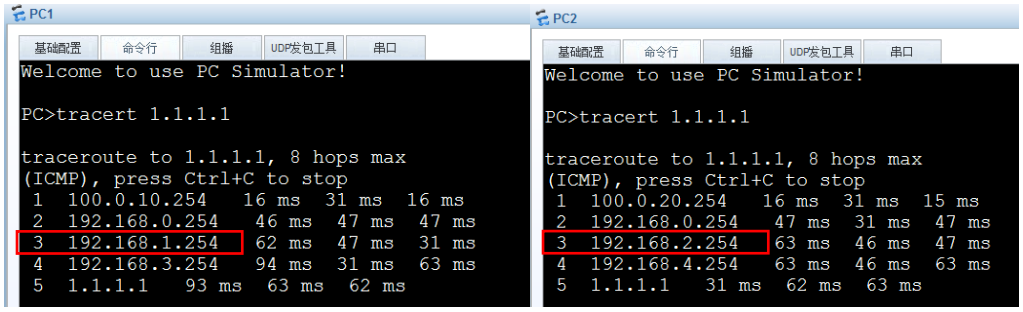
5.5 使用名称为 PBR 的流策略绑定流分类和流行为。

```
traffic policy PBR
 classifier 10 behavior to1
 classifier 20 behavior to2
```

5.6 在 GW 的接口 G0/0/0 上调用流策略。

```
interface GigabitEthernet0/0/0
 traffic-policy PBR inbound
```

5.7 在 PC1 和 PC2 上使用追踪命令确认策略路由的效果。



6.ISP 过滤私网路由

企业申请的公网地址为 100.0.0.0/16，ISP 应仅接收这个网段的路由。

考虑到企业可能进行子网划分，因此使用 ip-prefix+filter-policy 来过滤路由。

在 ISP 上部署策略，完成以下要求：

6.1 ip-prefix 名称为 100，index 10，允许 100.0.0.0/16 及所有子网。其他网段默认拒绝。

```
ip ip-prefix 100 index 10 permit 100.0.0.0 16 greater-equal 16 less-equal 32
\\允许所有子网即是允许可变长子网掩码，所以使用 greater-equal 16 less-equal 32。
```

6.2 isis 中使用过滤策略 filter-polciy 直接调用 ip-prefix。

```
isis 1
 filter-policy ip-prefix 100 import
```

6.3 确认 ISP 上没有 192.168.x.0/24 的私网路由。

```
<ISP>dis ip routing-table
```

Destination/Mask	Proto	Pre	Cost	Flags	NextHop
1.1.1.1/32	Direct	0	0	D	127.0.0.1
11.1.1.0/24	Direct	0	0	D	11.1.1.254
11.1.1.254/32	Direct	0	0	D	127.0.0.1
11.1.1.255/32	Direct	0	0	D	127.0.0.1
12.1.1.0/24	Direct	0	0	D	12.1.1.254
12.1.1.254/32	Direct	0	0	D	127.0.0.1
12.1.1.255/32	Direct	0	0	D	127.0.0.1
100.0.1.0/24	ISIS-L2	15	20	D	11.1.1.1
100.0.2.0/24	ISIS-L2	15	20	D	12.1.1.1
100.0.10.0/24	ISIS-L2	15	84	D	12.1.1.1
	ISIS-L2	15	84	D	11.1.1.1
100.0.20.0/24	ISIS-L2	15	84	D	12.1.1.1
	ISIS-L2	15	84	D	11.1.1.1
127.0.0.0/8	Direct	0	0	D	127.0.0.1
127.0.0.1/32	Direct	0	0	D	127.0.0.1
127.255.255.255/32	Direct	0	0	D	127.0.0.1
255.255.255.255/32	Direct	0	0	D	127.0.0.1