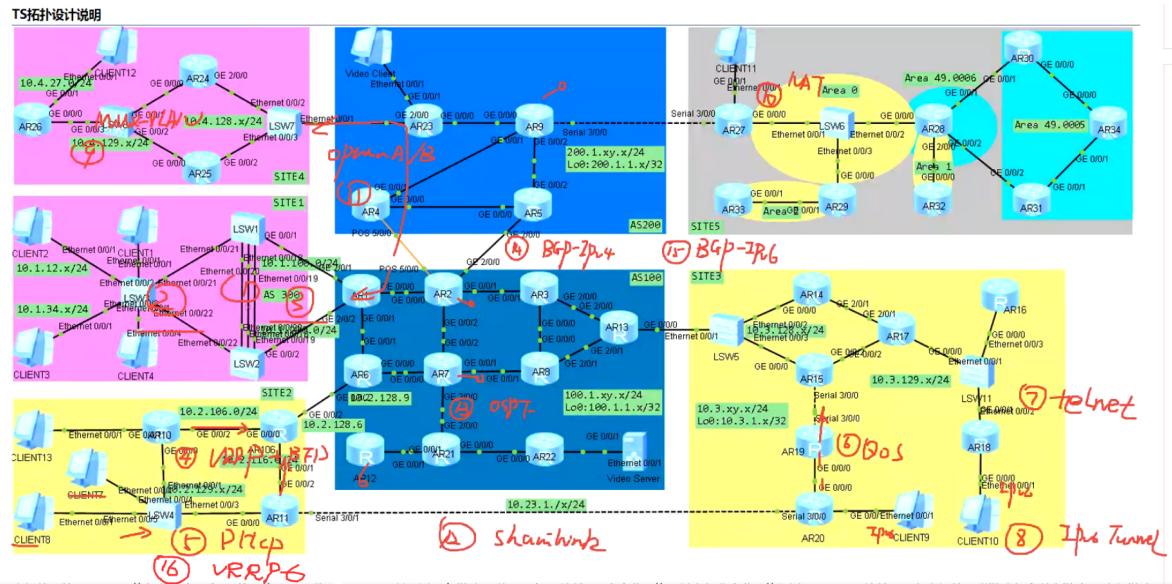


# 排错 TS2.0

16 --> 10



TS 完整需求16题

## 排错 TS2.0

### 1、Eth-Trunk

可能故障原因:

解决方案:

验证

### 2、MSTP

可能故障原因:

解决方案

验证

### 3、EBGP选路

分析

可能故障原因

解决方案

验证 1

验证 2

### 4、MUX-VLAN

可能故障原因

解决方案

### 5、MPLS-VPN实现site1-site4互访

可能故障原因:

解决方案

1. 检查AR23的BGP VPNv4路由---双向引入是否正确
2. 检查所有路由的 VPNv4 邻居关系
3. R7 和 R9 作为 VPNv4 路由反射器，配置正确客户端
4. RR、ASBR 关闭 RT 检测、PE(R1、R23) 开启 RT 值检测
5. 两端 PE 的 RT 配置错误
6. 部分设备 LDP 会话未建立

总结:

### 6、OSPF邻居

检查命令

## 7、VRRP

分析

解决方案

一、配置 BFD

二、配置 VRRP

## 8、DHCP

一、配置 IP 地址池

二、配置接口 `dhcp select global`

三、可能配置 `dhcp snooping trusted`

四、验证 pc 的 dhcp 地址

## 9、VRRP6

解决方案

验证

## 10、QOS

解决方案

一、R19 配置入向复杂流分类将语音流量进行重标记

二、R19配置出向CBQ基于类队列进行优先转发（保证带宽）

验证

## 11、Sham-link

一、解决 MPLS-VPN 单域问题

二、配置 sham-link

三、调整开销值

验证：

## 12、telnet

解决方案

一、R16的 telnet 认证方式为 AAA, admin 用户级别为 15 级, guest 用户级别为 1 级

二、R17 的认证方法为 password

验证

## 13、IPV6

解决方案

一、查看 tunnel, GRE 隧道是否配置错误

二、查看 ospfv3 配置

验证

## 14、BGP IPV4互访

可能故障原因

解决方案

一、检查 bgp 邻居

二、检查路由发布

三、配置下一跳本地

验证

## 15、BGP IPV6互访

分析

可能故障原因

解决方案

验证

## 16、NAT

解决方案

final、TS2.0 完结

## 1、Eth-Trunk

Site1中，LSW1-LSW2之间的所有链路要求做eth-trunk的捆绑，并且此eth-trunk要求做 **src-dst-ip** 负载；

### 可能故障原因：

1. 模式错误，采用 lacp-static
2. 负载方式错误
3. 成员接口未加入或者添加错误
4. Eth-Trunk 未放行所有 VLAN

### 解决方案：

1. 查看 eth 编号是啥 disp port vlan active
2. 进入 eth12 查看 mode 和 loadbalance
3. 修改 mode 时候报错

```
1 [LSW2-Eth-Trunk12]mode lacp-static
2 Error: Error in changing trunk working mode. There is(are) port(s) in the trunk.
```

4. 看到报错提示是说有端口再用
5. disp eth12 查看是哪个接口再用

SW1

```
1 interface Ethernet0/0/18
2   port hybrid tagged vlan 1
3   # 需要用
4   port hybrid untagged vlan 1
```

6. 进入接口，undo eth
7. 进入 eth12，更改模式

### 验证

#### SW1、SW2 配置

```
1 interface Eth-Trunk12
2   port link-type trunk
3   port trunk allow-pass vlan 2 to 4094
4   mode lacp-static
5   gvrp
```

compare1.bash (C:\Users\XuShengjin\PhpstormProjects\larabbs-api\p...)	compare2.bash (C:\Users\XuShengjin\PhpstormProjects\larabbs-api\p...)
✓ interface Eth-Trunk12	1 1 interface Eth-Trunk12 ✓
... port link-type trunk	2 2 ... port link-type trunk
... port trunk allow-pass vlan 2 to 4094	3 3 ... port trunk allow-pass vlan 2 to 4094
... mode manual load-balance	4 4 ... mode lacp-static
... load-balance src-ip	5 5 ... gvrp
... gvrp	6 6

eth 现象 --- 看到三个成员接口以及负载方式 **According to SIP-XOR-DIP** , 工作方式 **WorkingMode: STATIC**

```

1 [LSW1]disp eth 12
2 Local:
3 LAG ID: 12           WorkingMode: STATIC
4 Preempt Delay: Disabled Hash arithmetic: According to SIP-XOR-DIP

5 -----
6 ActorPortName      Status PortType PortPri PortNo PortKey PortState Weight
7 Ethernet0/0/19     Selected 100M    32768   20     3105   10111100  1
8 Ethernet0/0/20     Selected 100M    32768   21     3105   10111100  1
9 Ethernet0/0/18     Selected 100M    32768   19     3105   10111100  1

```

## 2、MSTP

Site1中，CLIENT1、CLIENT2属于VLAN12，CLIENT3、CLIENT4属于VLAN34；  
MSTP中的VLAN12属于instance1，vlan34属于instance2；两个instance的主备根桥分别在SW1和SW2上，  
要求CLIENT1访问R1时经过的路径是SW3-SW1-R1；同时要求CLIENT3访问R1时经过的路径是SW3-SW2-R1；

### 可能故障原因：

1. STP 未开或者模式错误
2. MSTP 三要素错误
3. SW1 和 SW2 主备根桥错误
4. 接口 cost 错误
5. 接口 vlan 划分错误
6. SW 之间 trunk 配置错误

## 解决方案

1. 所有交换机配置 MSTP --- 已知 SW3 错误

```

1 stp enable
2 stp mode mstp

```

2. 所有交换机配置 MSTP 三要素

```

1 stp region-configuration
2 region-name HCIE
3 instance 1 vlan 12
4 instance 2 vlan 34
5 active region-configuration

```

3. 配置主备根桥

### SW1 配置

```

1 stp instance 1 root primary
2 stp instance 2 root secondary

```

### SW2 配置

```

1 stp instance 1 root secondary
2 stp instance 2 root primary

```

4. 接口开销值配置错误 ----- 只会发生在SW3上

```

1 interface e0/0/22
2 # 假设有
3 stp instance 1 cost 10

```

## 5. 划分vlan

SW3

设备	接口	放行 VLAN
SW3	e0/0/1, e0/0/2	12
SW3	e0/0/3, e0/0/4	34

## 6. SW 上接口未放行 vlan

设备	接口	放行 VLAN
SW3	e0/0/21, e0/0/22	2 to 4094
SW1	e0/0/21	2 to 4094
SW2	e0/0/22	2 to 4094

## 验证

```

1 [LSW3]disp stp instance 1 brief
2 MSTID Port Role STP State Protection
3   1  Ethernet0/0/1 DESI LEARNING NONE
4   1  Ethernet0/0/2 DESI LEARNING NONE
5   1  Ethernet0/0/21 ROOT FORWARDING NONE
6   1  Ethernet0/0/22 ALTE DISCARDING NONE
7 [LSW3]disp stp instance 2 brief
8 MSTID Port Role STP State Protection
9   2  Ethernet0/0/3 DESI FORWARDING NONE
10  2  Ethernet0/0/4 DESI FORWARDING NONE
11  2  Ethernet0/0/21 ALTE DISCARDING NONE
12  2  Ethernet0/0/22 ROOT FORWARDING NONE

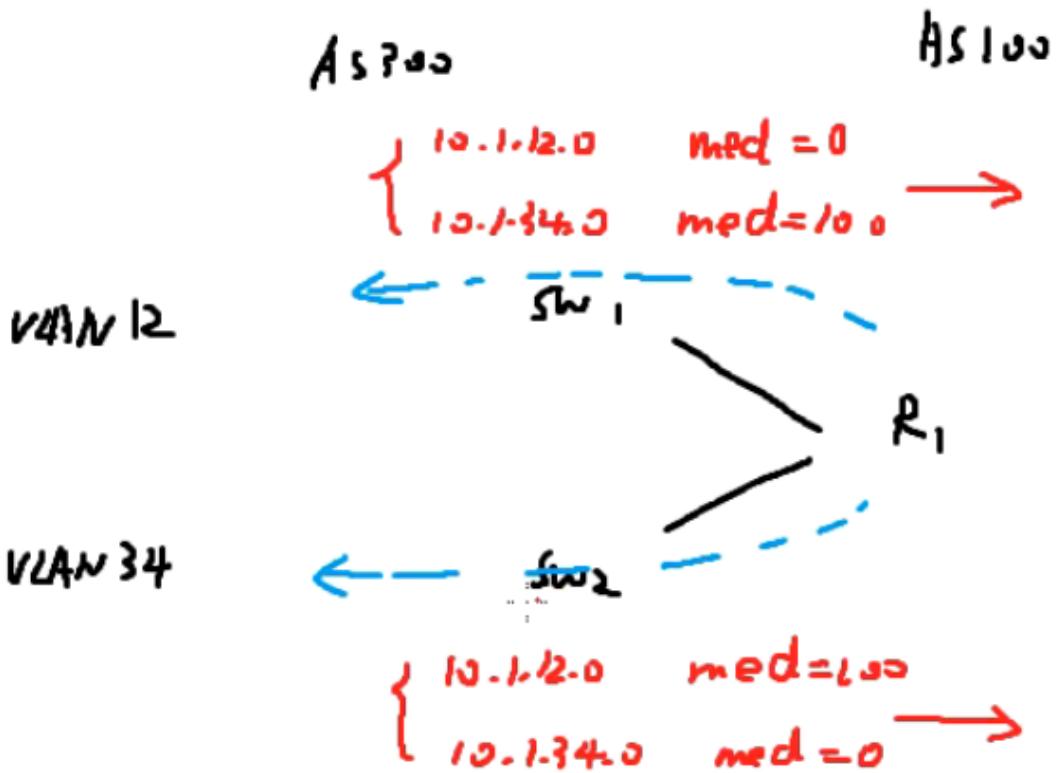
```

## 3、EBGP选路

R1访问VLAN12时经过的路径是R1-LSW1-LSW3;访问VLAN34时经过的路径是R1-LSW2-LSW3;  
只允许在AS300中实现， 并且确保你的解决方案不要影响AS100 AS300以外的其他AS；

## 分析

1. 只允许在AS300中实现 ---- 只能在 SW1、 SW2 上配置
2. 并且确保你的解决方案不要影响AS100 AS300以外的其他AS --- 使用 **med** 值属性 --- 只在相邻 AS 之间传递



### 可能故障原因

1. RR1 和 SW1、SW2 之间 EBGP 对等体无法建立 (直连接口)
  - A. 直连不通 --- SW1 和 SW2 VLAN 划分错误、网段配置错误
  - B. EBGP router-id 冲突
  - C. EBGP 对等体 AS 号冲突
  - D. R1 接口没有绑定实例
  - E. R1 基于实例与 SW1、SW2 建立对等体配置错误
2. SW1、SW2 未发布路由
3. SW1、SW2 发布路由，配置错误选路策略

### 解决方案

1. 直连不通

设备	vlan	ip address	对端设备
SW1	VLANIF 100	10.1.100.100	R1
SW2	VLANIF 200	10.1.200.200	R1

SW1、SW2

```

1 ping 10.1.100.1
2 ping 10.1.200.1

```

- B. EBGP router-id 冲突
- C. EBGP 对等体 AS 号冲突
- D. R1 接口没有绑定实例

## E. R1 基于实例与 SW1、SW2 建立对等体配置错误

### AR1 bgp 配置

```
1 [AR1]bgp 100
2 [AR1-bgp]disp this
3 [V200R003C00]
4 #
5 bgp 100
6 router-id 100.1.1.1
7 peer 100.1.1.7 as-number 100
8 peer 100.1.1.7 connect-interface LoopBack0
9 #
10 ipv4-family unicast
11     undo synchronization
12     peer 100.1.1.7 enable
13 #
14 ipv4-family vpnv4
15     policy vpn-target
16     peer 100.1.1.7 enable
17 #
18 ipv4-family vpn-instance 1
19     import-route direct
20     peer 10.1.100.100 as-number 300
21     peer 10.1.200.200 as-number 400
```

可以发现以下问题

1. vpn-instance 1 下对 SW2 对等体 AS 号错误

```
1 # 错误
2 ipv4-family vpn-instance 1
3     peer 10.1.200.200 as-number 400
4 # 正确
5 ipv4-family vpn-instance 1
6     peer 10.1.200.200 as-number 300
```

### AR1 接口配置

```
1 interface GigabitEthernet2/0/1
2     ip address 10.1.100.1 255.255.255.0
3 interface GigabitEthernet2/0/2
4     ip binding vpn-instance 1
5     ip address 10.1.200.1 255.255.255.0
```

可以发现 g2/0/1 接口未绑定 vpn 实例

```
1 interface GigabitEthernet2/0/1
2     ip binding vpn-instance 1
3     ip address 10.1.100.1 255.255.255.0
```

### SW1 bgp 配置

```
1 bgp 300
2     router-id 10.1.200.200
3     peer 10.1.100.1 as-number 100
4 #
5     ipv4-family unicast
6         undo synchronization
7         network 10.1.12.0 255.255.255.0 route-policy AS
8         network 10.1.34.0 255.255.255.0 route-policy MED
9     peer 10.1.100.1 enable
```

## SW2 bgp 配置

```
1 bgp 300
2     peer 10.1.200.1 as-number 100
3 #
4     ipv4-family unicast
5         undo synchronization
6         network 10.1.12.0 255.255.255.0
7         network 10.1.34.0 255.255.255.0 route-policy MED
8     peer 10.1.200.1 enable
```

## 可以发现以下问题：

1. SW1 bgp.router-id 错误

```
1 # 改正
2 bgp 300
3 router-id 10.1.100.100
4 Warning: Changing the parameter in this command resets the peer session. Continu
5 e?[Y/N]:y
```

2. SW2 bgp.router-id 未配置

```
1 bgp 300
2     router-id 10.1.200.200
```

## 验证 1

```
1 disp bgp vpnv4 all peer
```

2. SW1、SW2 未发布路由

可以看到有发布路由

3. SW1、SW2 发布路由，配置错误选路策略

SW1 发布路由策略错误

```
1 # 错误
2 ipv4-family unicast
3     network 10.1.12.0 255.255.255.0 route-policy AS
4     network 10.1.34.0 255.255.255.0 route-policy MED
```

SW1 是对 **10.1.12.0/24** 正常发布，**10.1.12.0/24** 修改 **MED** 值

改正如下：

```
1 # 正确
2 ipv4-family unicast
3   network 10.1.12.0 255.255.255.0
4   network 10.1.34.0 255.255.255.0 route-policy MED
```

查看 route-policy med --- 发现是通过把 `med` 值改大

```
1 route-policy MED permit node 1
2   apply cost 100
```

SW2 发布路由策略错误

SW2 是对 `10.1.12.0/24` 修改 `MED` 值, `10.1.12.0/24` 正常发布

正确如下

```
1 ipv4-family unicast
2   network 10.1.12.0 255.255.255.0 route-policy MED
3   network 10.1.34.0 255.255.255.0
```

## 验证2

R1

```
1 [AR1]disp bgp vpnv4 all routing-table
2   *> 10.1.12.0/24      10.1.100.100    0          0      300i
3   *      10.1.200.200  100          0          0      300i
4   *> 10.1.34.0/24      10.1.200.200  0          0      300i
5   *      10.1.100.100  100          0          0      300i
```

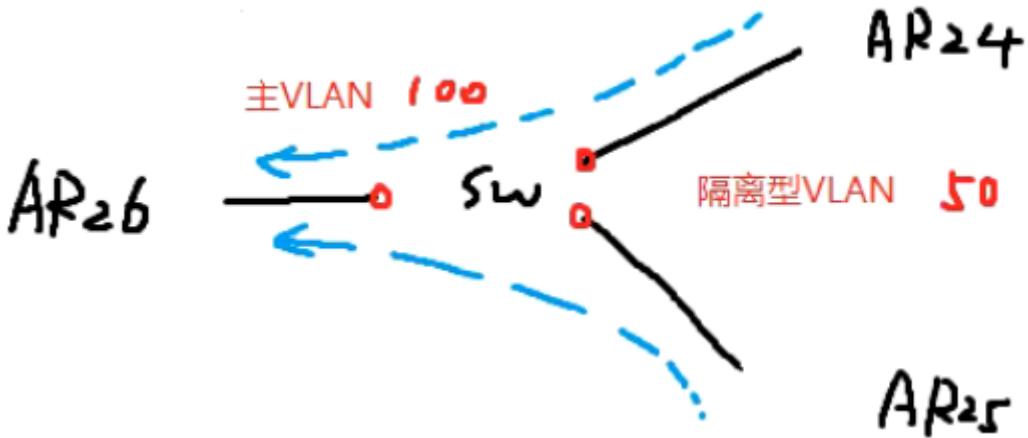
tracert 看一下 --- 可以看到没问题

```
1 [AR1]tracert -vpn-instance 1 10.1.12.11 # 访问 PC1
2
3 traceroute to 1 10.1.12.11(10.1.12.11), max hops: 30 ,packet length: 40,press
CTRL_C to break
4
5 1 10.1.100.100 40 ms 20 ms 20 ms
6 2 10.1.12.11 60 ms 70 ms 60 ms
7
8 [AR1]tracert -vpn-instance 1 10.1.34.33 # 访问 RC4
9 traceroute to 1 10.1.34.33(10.1.34.33), max hops: 30 ,packet length: 40,press
CTRL_C to break
10
11 1 10.1.200.200 20 ms 20 ms 20 ms
12 2 10.1.34.33 110 ms 60 ms 80 ms
```

## 4、MUX-VLAN

Site4中，AR24、AR25、AR26在一个网段中，同时都运行了ISIS协议，要求AR26能和AR24、AR25都能形成邻居关系，**但是AR24与AR25不能形成邻居关系**；通过LSW8的二层VLAN技术以及其他设备排除错误点来实现此要求，

注意：配置过程中不能在LSW8上删除和增加新的VLAN



## 可能故障原因

1. 交换机 MUX-VLAN、VLAN 问题
  1. 交换机 MUX-VLAN 划分错误
  2. 交换机接口 MUX-VLAN 未开启
  3. 交换机接口 VLAN 划分错误
2. IS-IS 邻居无法建立
  1. 全部采用 Level-2, 层级配置错误
  2. system-id 冲突
  3. 接口认证错误
  4. 接口未开启 isis 功能

## 解决方案

### 一、交换机 MUX-VLAN、VLAN 问题

#### 1. 检查 MUX-VLAN SW8 配置

```

1 [LSW8]vlan 100
2 [LSW8-vlan100]disp this
3   vlan 100
4     mux-vlan
5     subordinate group 50

```

改正为

```

1   vlan 100
2     undo subordinate group 50
3     subordinate separate 50

```

#### 2. 检查接口 VLAN 划分以及是否开启 MUX-VLAN

```
1 interface GigabitEthernet0/0/1
2   port link-type access
3   port default vlan 50
4   port mux-vlan enable # 未开
5 interface GigabitEthernet0/0/1
6   port link-type access
7   port default vlan 50
8   port mux-vlan enable # 未开
9 interface GigabitEthernet0/0/3
10  port link-type access
11  port default vlan 100 # 划分错误为 50
12  port mux-vlan enable # 未开
```

### 3. 验证结果

```
[LSW8]disp mux-vlan
Principal Subordinate Type      Interface
-----
100      -      principal    GigabitEthernet0/0/3
100      50     separate     GigabitEthernet0/0/1 GigabitEthernet0/0/2
-----
```

## 二、IS-IS 邻居无法建立

### 检查 isis 配置

#### 1. 检查 R26

```
1 disp cu con isis # 查看进程号
2 isis 100
3   is-level level-1
4   network-entity 47.0004.0000.0000.0026.00
```

发现进程号为 100，且等级配置错误、区域号配置错误，进行改正

```
1 isis 100
2   is-level level-2
3   network-entity 49.0004.0000.0000.0026.00
```

#### 2. 检查 R24

```
1 <AR24>disp cu con isis
2 [V200R003C00]
3 isis 100
4   is-level level-2
5   network-entity 49.0004.0000.0000.0026.00
```

发现 system-id 配置错误，改正如下

```
1 isis 100
2   is-level level-2
3   network-entity 49.0004.0000.0000.0024.00
```

### 检查 isis 接口以及接口认证

```
1 disp isis int
```

## R24、R25、R26 配置认证

```
1 int g0/0/0
2 isis enable 100
3 isis authentication-mode md5 cipher hcie # 具体密码看考场上题本
```

## 验证

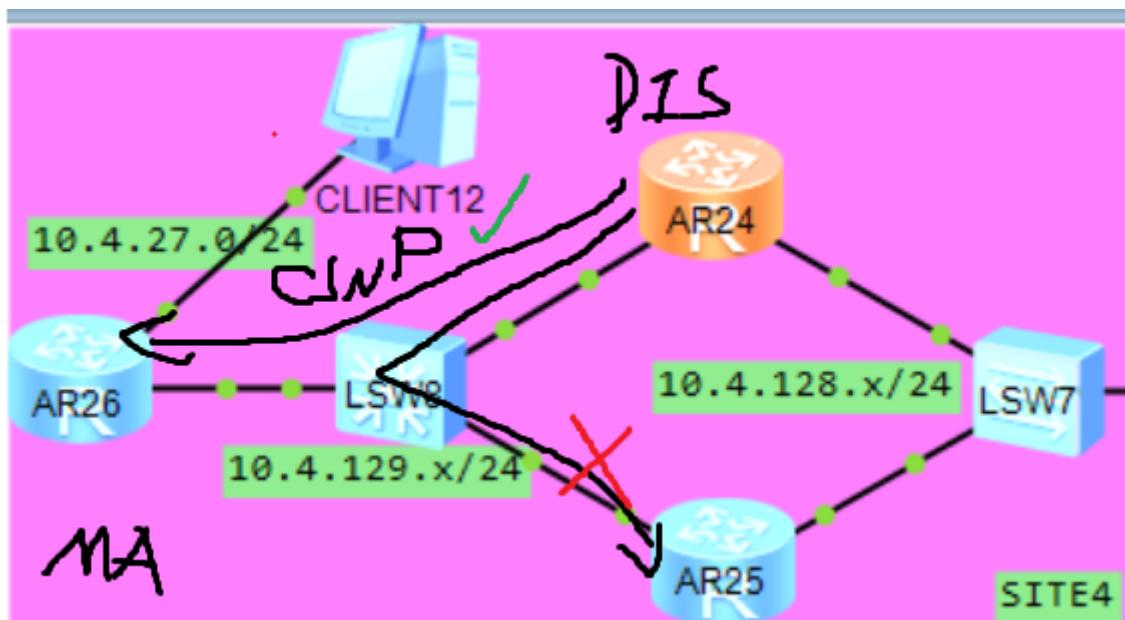
```
[AR24]disp isis peer

Peer information for ISIS(100)

System Id      Interface      Circuit Id      State HoldTime Type      PRI
-----+-----+-----+-----+-----+-----+-----+-----+
0000.0000.0026 GE0/0/0          0000.0000.0024.01 Up    29s       L2       64
0000.0000.0025 GE2/0/0          0000.0000.0024.02 Up    20s       L2       64
0000.0000.0023 GE2/0/0          0000.0000.0024.02 Up    27s       L2       64
Total Peer(s): 3
[AR24]
```

## 隐含需求

上图中可以看出 R24 是 DIS，他会周期性发送 CSNP 报文来同步链路数据库信息，但是因为 隔离型 vlan 无法发送给 R25，所以 R24 不能成为 DIS，得需要 R26 成为 DIS



## R26

```
1 int g0/0/0
2 isis dis-priority 127
```

```
<AR24>disp isis peer

Peer information for ISIS(100)

System Id      Interface      Circuit Id      State HoldTime Type      PRI
-----+-----+-----+-----+-----+-----+-----+-----+
0000.0000.0026 GE0/0/0          0000.0000.0026.01 Up    8s       L2       127
0000.0000.0025 GE2/0/0          0000.0000.0024.02 Up    27s      L2       64
0000.0000.0023 GE2/0/0          0000.0000.0024.02 Up    23s      L2       64
```

## 5、MPLS-VPN实现site1-site4互访

Site1与Site4为同一个VPN客户的两个站点，现在site1里的CLIENTS无法和site4里的CLIENT通信，请解决此问题；

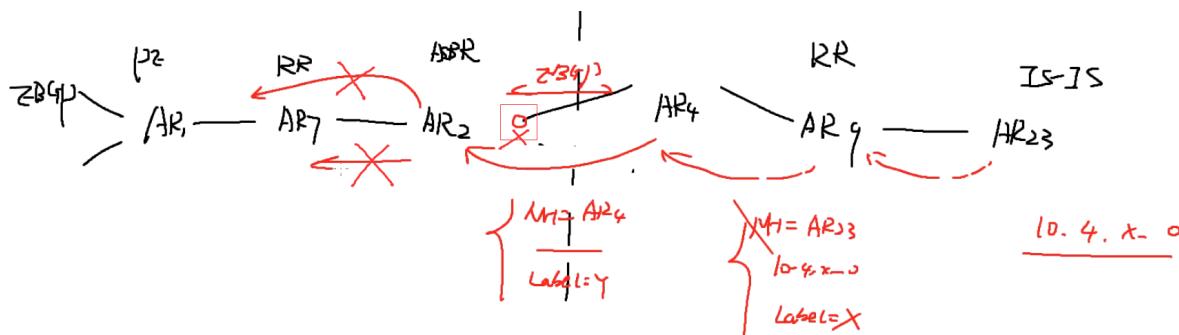
注意：不要删除现有配置，可修改解决

考察 OPTION B

- 直接互传 VPNV4 路由
- 开启的是 MP-BGP 的能力
- 不需要维护实例

可能故障原因：

- 控制层面传递路由故障
  - PE设备(R23) ISIS-BGP 双向引入错误 --- R1 已经在选路的时候解决了
  - VPNv4 对等体建立错误
  - RR 路由反射器客户端配置错误
  - 所有设备（除 PE 设备）都需要参与到 **VPNv4** 路由传递，未关闭 **RT** 值检测
  - PE 设备 **RT** 值配置错误
- 转发层面 --- 底层 LSP 没有成功建立
  - 底层 IGP 存在问题
  - LDP 会话没有建立
- ASBR 之间接口没有开启 **MPLS** 能力



### 解决方案

#### 1. 检查AR23的BGP VPNv4路由----双向引入是否正确

```
1 disp bgp vpnv4 all peer
2   Peer          V      AS  MsgRcvd  MsgSent  OutQ  Up/Down      State
3     200.1.1.9    4      200      608      591      0 09:38:45 Established    0
4 disp bgp vpnv4 all routing
5   VPN-Instance 1, Router ID 200.1.1.23:
6
7   Total Number of Routes: 7
8   Network          NextHop        MED      LocPrf      PrefVal Path/Ogn
9
10  *-> 10.4.1.0/24  0.0.0.0      10      0          ??
11  *-> 10.4.1.23/32 0.0.0.0      0       0          ??
12  *-> 10.4.1.25/32 0.0.0.0      10      0          ??
13  *-> 10.4.1.26/32 0.0.0.0      20      0          ??
14  *-> 10.4.27.0/24 0.0.0.0      30      0          ??
15  *-> 10.4.128.0/24 0.0.0.0      0       0          ??
16  *-> 10.4.129.0/24 0.0.0.0      20      0          ???
```

发现有 Site4 PC 网段地址 10.4.27.0/24

```
1 bgp 200
2     ipv4-family vpn-instance 1
3         import-route isis 100

1     isis 100 vpn-instance 1
2     is-level level-2
3     network-entity 47.0004.0000.0000.0023.00
4     import-route bgp # 加上此行
```

## 2. 检查所有路由的 VPNv4 邻居关系

R9(23、4、5)、R2 (4、5、7) 、R7 (1、2、6、13) 检查

```
1 disp bgp vpnv4 all peer # 没有错误
```

## 3. R7 和 R9 作为 VPNv4 路由反射器，配置正确客户端

### R7 配置

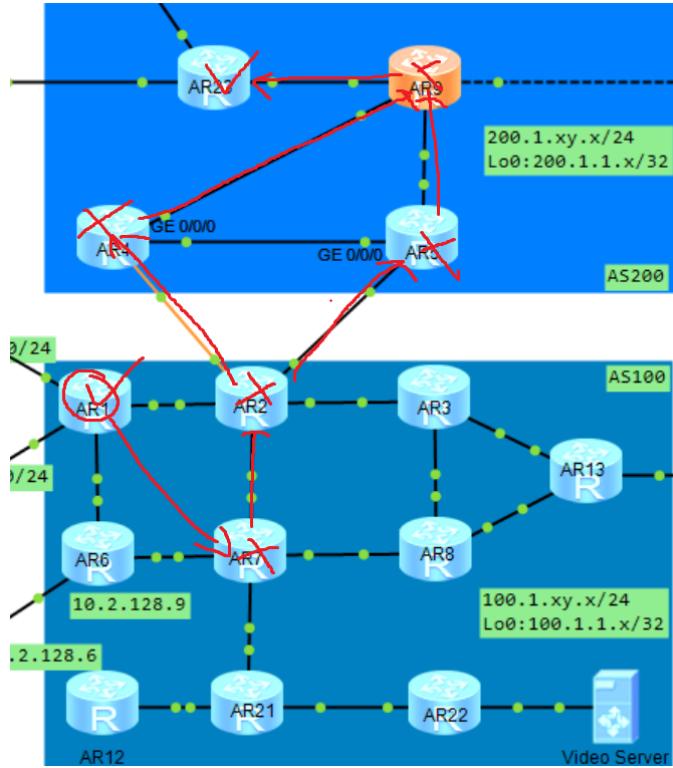
```
1 bgp 200
2     ipv4-family vpnv4
3         policy vpn-target
4             peer 100.1.1.1 enable
5             peer 100.1.1.1 reflect-client
6             peer 100.1.1.2 enable
7             peer 100.1.1.2 reflect-client
```

### R9 配置

```
1 bgp 100
2     ipv4-family vpnv4
3         undo policy vpn-target
4         peer 200.1.1.4 enable
5         peer 200.1.1.4 reflect-client
6         peer 200.1.1.5 enable
7         peer 200.1.1.5 reflect-client
8         peer 200.1.1.23 reflect-client
```

## 4. RR、ASBR 关闭 RT 检测、PE(R1、R23) 开启 RT 值检测

AR7、AR2、AR4、AR5、AR9



```

1  ipv4-family vpnv4
2    undo policy vpn-target

```

R1、R23

```

1  ipv4-family vpnv4
2    policy vpn-target

```

##### 5. 两端 PE 的 RT 配置错误

```

[AR1-vpn-instance-1]disp this
[V200R003C00]
#
ip vpn-instance 1
  description site1-site4
  service-id 14
  ipv4-family
    route-distinguisher 200:100
    vpn-target 200:10 export-extcommunity
    vpn-target 200:10 import-extcommunity
#

```

```
[AR23-vpn-instance-1]disp this
[V200R003C00]
#
ip vpn-instance 1
    description sitel-site4
    service-id 14
    ipv4-family
        route-distinguisher 200:100
        import route-policy import
        vpn-target 200:100 export-extcommunity
        vpn-target 200:100 import-extcommunity
```

R1 修改 RT 值 --- 不删原来的，加一下就行了

```
1 ip vpn-instance 1
2     vpn-target 200:100 both
```

R23 上查看 vpnv4 路由，发现有 **10.1.12.0/24** 和 **10.1.34.0/24**，但是不是最优的

```
1 [AR23]disp bgp vpnv4 all routing-table
2     Route Distinguisher: 200:100
3         Network          NextHop      MED      LocPrf      PrefVal Path/Ogn
4     *>i 10.1.1.1/32   200.1.1.4      100      0      100?
5     *>i 10.1.12.0/24  200.1.1.4      100      0      100 300i
6     *>i 10.1.34.0/24  200.1.1.4      100      0      100 300i
7     *>i 10.1.100.0/24 200.1.1.4      100      0      100?
8     *>i 10.1.200.0/24 200.1.1.4      100      0      100?
9     *> 10.4.1.0/24    0.0.0.0       10      0      ?
10    *> 10.4.1.23/32   0.0.0.0       0      0      ?
11    *> 10.4.1.25/32   0.0.0.0       10      0      ?
12    *> 10.4.1.26/32   0.0.0.0       20      0      ?
13    *> 10.4.27.0/24   0.0.0.0       30      0      ?
14    *> 10.4.128.0/24  0.0.0.0       0      0      ?
15    *> 10.4.129.0/24  0.0.0.0       20      0      ?
16
17     VPN-Instance 1, Router ID 200.1.1.23:
18     Total Number of Routes: 8
19         Network          NextHop      MED      LocPrf      PrefVal Path/Ogn
20     i 10.1.12.0/24    200.1.1.4      100      0      100 300i #
不是最优
21    *> 10.4.1.0/24    0.0.0.0       10      0      ?
22    *> 10.4.1.23/32   0.0.0.0       0      0      ?
23    *> 10.4.1.25/32   0.0.0.0       10      0      ?
24    *> 10.4.1.26/32   0.0.0.0       20      0      ?
25    *> 10.4.27.0/24   0.0.0.0       30      0      ?
26    *> 10.4.128.0/24  0.0.0.0       0      0      ?
27    *> 10.4.129.0/24  0.0.0.0       20      0      ?
```

R4 上查看自己端路由，发现是最优的

```
1 <AR4>disp bgp vpnv4 all routing-table
2     Route Distinguisher: 200:100
3
```

4	Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
5						
6	*> 10.1.1.1/32	200.100.24.2		0	100?	
7	*> 10.1.12.0/24	200.100.24.2		0	100 300i	
8	*> 10.1.34.0/24	200.100.24.2		0	100 300i	
9	*> 10.1.100.0/24	200.100.24.2		0	100?	
10	*> 10.1.200.0/24	200.100.24.2		0	100?	
11	*>i 10.4.1.0/24	200.1.1.23	10	100	0	?
12	*>i 10.4.1.23/32	200.1.1.23	0	100	0	?
13	*>i 10.4.1.25/32	200.1.1.23	10	100	0	?
14	*>i 10.4.1.26/32	200.1.1.23	20	100	0	?
15	*>i 10.4.27.0/24	200.1.1.23	30	100	0	?
16	*>i 10.4.128.0/24	200.1.1.23	0	100	0	?
17	*>i 10.4.129.0/24	200.1.1.23	20	100	0	?

查看是否通告给 R2 --- 发现并没有通告

```
1 <AR4>disp bgp vpnv4 all routing-table peer 200.100.24.2 advertised-routes
```

原因是因为 没有分配去往 200.1.1.23 的 lsp

1	<AR4>disp mpls lsp					
2	<hr/>					
3	LSP Information: L3VPN LSP					
4	<hr/>					
5	FEC	In/Out Label	In/Out IF		Vrf Name	
6	10.1.12.0/24	1025/1031	-/-		ASBR LSP	
7	100.1.136.6/32	1026/1032	-/-		ASBR LSP	
8	10.2.1.11/32	1027/1033	-/-		ASBR LSP	
9	10.2.1.10/32	1028/1034	-/-		ASBR LSP	
10	10.2.116.0/24	1029/1035	-/-		ASBR LSP	
11	10.2.106.0/24	1030/1036	-/-		ASBR LSP	
12	10.2.129.0/24	1031/1037	-/-		ASBR LSP	
13	10.23.1.0/24	1032/1038	-/-		ASBR LSP	
14	10.3.1.20/32	1033/1039	-/-		ASBR LSP	
15	10.3.128.0/24	1034/1040	-/-		ASBR LSP	
16	10.3.1.14/32	1035/1041	-/-		ASBR LSP	
17	10.3.1.17/32	1036/1042	-/-		ASBR LSP	
18	10.3.1.147.0/24	1037/1043	-/-		ASBR LSP	
19	10.3.1.15/32	1038/1044	-/-		ASBR LSP	
20	10.3.210.0/24	1039/1045	-/-		ASBR LSP	
21	10.3.1.19/32	1040/1046	-/-		ASBR LSP	
22	10.3.192.0/24	1041/1047	-/-		ASBR LSP	
23	10.3.159.0/24	1042/1048	-/-		ASBR LSP	
24	100.1.136.13/32	1043/1049	-/-		ASBR LSP	
25	10.3.1.13/32	1044/1050	-/-		ASBR LSP	
26	10.3.157.0/24	1045/1051	-/-		ASBR LSP	
27	10.2.128.0/24	1046/1052	-/-		ASBR LSP	
28	10.1.34.0/24	1047/1053	-/-		ASBR LSP	
29	10.1.100.0/24	1048/1054	-/-		ASBR LSP	
30	10.1.200.0/24	1049/1055	-/-		ASBR LSP	
31	10.1.1.1/32	1050/1056	-/-		ASBR LSP	
32	<hr/>					
33	LSP Information: LDP LSP					
34	<hr/>					
35	FEC	In/Out Label	In/Out IF		Vrf Name	
36	200.1.1.4/32	3/NULL	-/-			
37	200.1.1.5/32	NULL/3	-/GE0/0/0			

38 200.1.1.5/32 1024/3 - /GE0/0/0

## 6. 部分设备 LDP 会话未建立

```
1 <AR4>disp mpls ldp session all
2
3 LDP Session(s) in Public Network
4 Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDDD:HH:MM)
5 A '*' before a session means the session is being deleted.
6 -----
7 PeerID          Status      LAM  SsnRole   SsnAge    KAISent/Rcv
8 -----
9 200.1.1.99:0    NonExistent Passive        0/0      # 未建立成功
10 200.1.1.5:0     Operational DU   Passive 0000:08:07 1951/1951
11 -----
12 TOTAL: 2 session(s) Found.
13
14 Oct 18 2021 21:52:30-08:00 AR4 %%01LDP/4/SSNHOLDTMREXP(1)[0]:Sessions were deleted because the session hold timer expired and the notification of the expiry was sent to the peer 200.1.1.99.
15
16
17
```

看一下是不是环回口不可达 --- 果然是

```
1 <AR4>ping -a 200.1.1.4 200.1.1.5
2 PING 200.1.1.5: 56 data bytes, press CTRL_C to break
3     Reply from 200.1.1.5: bytes=56 Sequence=1 ttl=255 time=30 ms
4     Reply from 200.1.1.5: bytes=56 Sequence=2 ttl=255 time=20 ms
5     Reply from 200.1.1.5: bytes=56 Sequence=3 ttl=255 time=20 ms
6     Reply from 200.1.1.5: bytes=56 Sequence=4 ttl=255 time=10 ms
7     Reply from 200.1.1.5: bytes=56 Sequence=5 ttl=255 time=20 ms
8
9     --- 200.1.1.5 ping statistics ---
10    5 packet(s) transmitted
11    5 packet(s) received
12    0.00% packet loss
13    round-trip min/avg/max = 10/20/30 ms
14
15 <AR4>ping -a 200.1.1.4 200.1.1.99 # 不可达
16 PING 200.1.1.99: 56 data bytes, press CTRL_C to break
17     Request time out
18     Request time out
19     Request time out
20     Request time out
21     Request time out
```

然后得去 R9 上找原因

1. 查看是否 200.1.1.99 是哪个接口  
发现是 Loop1 接口

```

1 [AR9]disp ip int brief
2
3 Interface IP Address/Mask Physical Protocol
4 GigabitEthernet0/0/0 200.1.239.9/24 up up
5 GigabitEthernet0/0/1 200.1.49.9/24 up up
6 GigabitEthernet0/0/2 200.1.59.9/24 up up
7 LoopBack0 200.1.1.9/32 up up(s)
8 LoopBack1 200.1.1.99/32 up up(s)
9 NULL0 unassigned up up(s)
10 Serial2/0/0 unassigned down down
11 Serial2/0/1 unassigned down down
12 Serial3/0/0 200.1.209.9/24 up down
13 Serial3/0/1 unassigned down down

```

## 2. 查看是否宣告进 isis

发现 Loop1 并没有宣告进 isis

```

1 [AR9]disp isis int
2
3 Interface information for ISIS(200)
4 -----
5 Interface Id IPV4.State IPV6.State MTU Type DIS
6 GE0/0/0 001 Up Up 1497 L1/L2 No/Yes
7 GE0/0/1 002 Up Up 1497 L1/L2 No/Yes
8 GE0/0/2 003 Up Up 1497 L1/L2 No/No
9 Loop0 001 Up Up 1500 L1/L2 --

```

## 3. 宣告进 isis

```

1 interface LoopBack1
2 isis enable 200

```

## 4. R9 查看 ldp session 会话

可以看到都已经建立完成了

```

1 [AR9]disp mpls ldp session all
2
3 LDP Session(s) in Public Network
4 Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDDD:HH:MM)
5 A '*' before a session means the session is being deleted.
6 -----
7 PeerID Status LAM SsnRole SsnAge KASent/Rcv
8 -----
9 200.1.1.4:0 Operational DU Active 0000:00:03 15/15
10 200.1.1.5:0 Operational DU Active 0000:00:03 14/14
11 200.1.1.23:0 Operational DU Active 0000:00:03 15/15
12 -----
13 TOTAL: 3 session(s) Found.

```

## 5. 现在在 R4 上检查 mpls 和 通告路由

发现有去往 200.1.1.23/32 的 lsp 了

发现 R4 路由已经通告给 R2 了

```

1 <AR4>disp mpls lsp
2 -----
3             LSP Information: L3VPN  LSP
4 -----
5 FEC          In/Out Label  In/Out IF           Vrf Name
6 -----
7             LSP Information: LDP LSP
8 -----
9 FEC          In/Out Label  In/Out IF           Vrf Name
10 200.1.1.4/32 3/NULL      -/-                -
11 200.1.1.5/32 NULL/3     -/GE0/0/0
12 200.1.1.5/32 1024/3    -/GE0/0/0
13 200.1.1.99/32 NULL/3    -/GE0/0/1
14 200.1.1.99/32 1051/3    -/GE0/0/1
15 200.1.1.9/32  NULL/3    -/GE0/0/1
16 200.1.1.9/32  1052/3    -/GE0/0/1
17 200.1.1.23/32 NULL/1025 -/GE0/0/1
18 200.1.1.23/32 1053/1025 -/GE0/0/1

```

```

1 <AR4>disp bgp vpnv4 all routing-table peer 200.100.24.2 advertised-routes
2 Total Number of Routes: 7
3 Route Distinguisher: 200:100
4       Network          NextHop        MED      LocPrf      PrefVal Path/0gn
5
6  *>i 10.4.1.0/24      200.100.24.4      0        200?
7  *>i 10.4.1.23/32    200.100.24.4      0        200?
8  *>i 10.4.1.25/32    200.100.24.4      0        200?
9  *>i 10.4.1.26/32    200.100.24.4      0        200?
10 *>i 10.4.27.0/24    200.100.24.4      0        200?
11 *>i 10.4.128.0/24   200.100.24.4      0        200?
12 *>i 10.4.129.0/24   200.100.24.4      0        200?

```

## 7. ASBR 之间接口务必开启 MPLS 能力

R2 查看标签 --- 发现接收到的 10.4.27.0 ... 我好不容易传来的路由没有分配标签

```

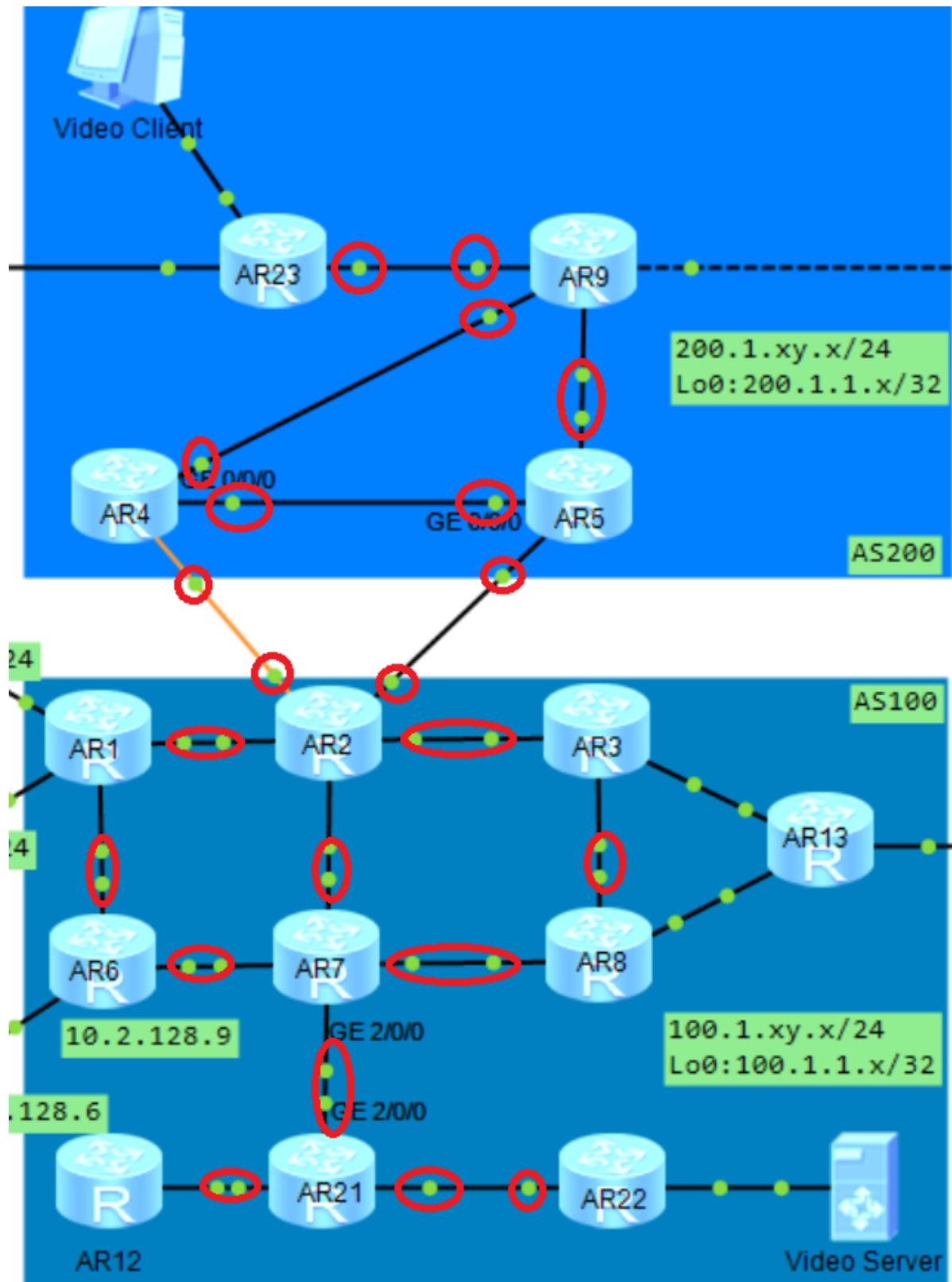
1 <AR2>disp bgp vpnv4 all routing-table label
2
3 Route Distinguisher: 200:100
4       Network          NextHop        In/Out Label
5
6  *>i 10.1.1.1        100.1.1.1      1056/1031
7  *>i 10.1.12.0       100.1.1.1      1031/1035
8  *>i 10.1.34.0       100.1.1.1      1053/1036
9  *>i 10.1.100.0      100.1.1.1      1054/1037
10 *>i 10.1.200.0      100.1.1.1      1055/1034
11 *>  10.4.1.0         200.100.24.4   NULL/1057
12 *   200.100.25.5     200.100.25.5   NULL/1057
13 *>  10.4.1.23        200.100.24.4   NULL/1060
14 *   200.100.25.5     200.100.25.5   NULL/1060
15 *>  10.4.1.25        200.100.24.4   NULL/1058
16 *   200.100.25.5     200.100.25.5   NULL/1058
17 *>  10.4.1.26        200.100.24.4   NULL/1055
18 *   200.100.25.5     200.100.25.5   NULL/1055
19 *>  10.4.27.0        200.100.24.4   NULL/1054

```

20	*		200.100.25.5	NULL/1054
21	*>	10.4.128.0	200.100.24.4	NULL/1059
22	*		200.100.25.5	NULL/1059
23	*>	10.4.129.0	200.100.24.4	NULL/1056
24	*		200.100.25.5	NULL/1056

检查发现 R2 的接口下未开启 MPLS 标签能力，则会导致无法继续为 VPNv4 分配私网标签传递给 AR7 (RR)

1	<AR2>disp mpls int	Status	TE Attr	LSP Count	CRLSP Count	Effective MTU
2	Interface					
3	GE0/0/0	Up	Dis	2	0	1500
4	GE0/0/1	Up	Dis	4	0	1500
5	GE0/0/2	Up	Dis	8	0	1500



现在查看 R2 的 mpls label，发现已经可以分配标签了

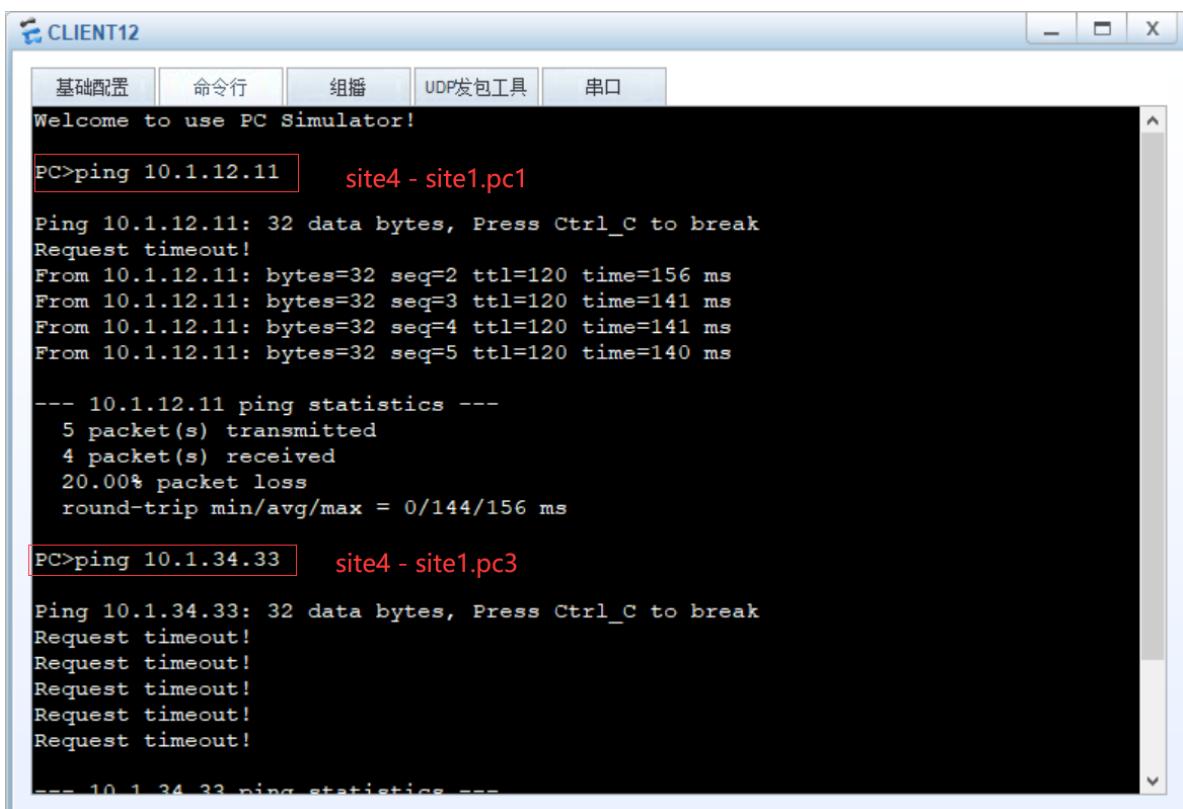
```
[AR2]disp bgp vpnv4 all rou label
Route Distinguisher: 200:100
Network          NextHop      In/Out Label
*>i    10.1.1.1        100.1.1.1  1056/1031
*>i    10.1.12.0       100.1.1.1  1031/1035
*>i    10.1.34.0       100.1.1.1  1053/1036
*>i    10.1.100.0      100.1.1.1  1054/1037
*>i    10.1.200.0      100.1.1.1  1055/1034
```

```

10  *>  10.4.1.0      200.100.24.4    1060/1057
11  *          200.100.25.5    NULL/1057
12  *>  10.4.1.23     200.100.24.4    1057/1060
13  *          200.100.25.5    NULL/1060
14  *>  10.4.1.25     200.100.24.4    1059/1058
15  *          200.100.25.5    NULL/1058
16  *>  10.4.1.26     200.100.24.4    1062/1055
17  *          200.100.25.5    NULL/1055
18  *>  10.4.27.0      200.100.24.4    1063/1054
19  *          200.100.25.5    NULL/1054
20  *>  10.4.128.0     200.100.24.4    1058/1059
21  *          200.100.25.5    NULL/1059
22  *>  10.4.129.0     200.100.24.4    1061/1056
23  *          200.100.25.5    NULL/1056
24

```

### 8. Site4 --- Site1 pc 互访测试



可以发现 ping 通 pc1，但是 ping 不通 pc3 那是怎么回事呢？

1. 可以排除是跨域错误，不然 pc1 也不可能通的
2. 可以在 R23 上查一查

### 1. 查看 vpnv4 路由 --- 发现有 12, 34 的路由

```

1 [AR23]disp bgp vpnv4 all routing-table
2
3 Total number of routes from all PE: 12
4 Route Distinguisher: 200:100
5
6      Network          NextHop        MED      LocPrf      PrefVal Path/Ogn
7
8  *>i  10.1.1.1/32    200.1.1.4      100       0        100?

```

```

 9  *>i 10.1.12.0/24      200.1.1.4          100    0   100 300i #
  这里
10  *>i 10.1.34.0/24      200.1.1.4          100    0   100 300i #
  这里
11  *>i 10.1.100.0/24     200.1.1.4          100    0   100?
12  *>i 10.1.200.0/24     200.1.1.4          100    0   100?
13  *> 10.4.1.0/24        0.0.0.0           10      0   ?
14  *> 10.4.1.23/32       0.0.0.0           0      0   ?
15  *> 10.4.1.25/32       0.0.0.0           10      0   ?
16  *> 10.4.1.26/32       0.0.0.0           20      0   ?
17  *> 10.4.27.0/24       0.0.0.0           30      0   ?
18  *> 10.4.128.0/24      0.0.0.0           0      0   ?
19  *> 10.4.129.0/24      0.0.0.0           20      0   ?

20
21  VPN-Instance 1, Router ID 200.1.1.23:
22  Total Number of Routes: 8
23      Network          NextHop          MED      LocPrf      PrefVal Path/Ogn
24
25  *>i 10.1.12.0/24      200.1.1.4          100    0   100 300i #
  这里
26  *> 10.4.1.0/24        0.0.0.0           10      0   ?
27  *> 10.4.1.23/32       0.0.0.0           0      0   ?
28  *> 10.4.1.25/32       0.0.0.0           10      0   ?
29  *> 10.4.1.26/32       0.0.0.0           20      0   ?
30  *> 10.4.27.0/24       0.0.0.0           30      0   ?
31  *> 10.4.128.0/24      0.0.0.0           0      0   ?
32  *> 10.4.129.0/24      0.0.0.0           20      0   ?

33

```

2. 那就奇了怪了，但是仔细发现 VPN-Instance 1 下只有 12，没有 34 路由  
所以 R23 检查一下 vpn-instance 看看

```

1  ip vpn-instance 1
2    description site1-site4
3    service-id 14
4    ipv4-family
5      route-distinguisher 200:100
6      import route-policy import  # 这里有个入向策略
7      vpn-target 200:100 export-extcommunity
8      vpn-target 200:100 import-extcommunity

```

3. 发现一个入向策略，我们查看一下

```

1  route-policy import permit node 1
2    if-match acl 2000

```

4. 在追查一下 acl 2000

```

1  acl number 2000
2    rule 1 permit source 10.1.12.0 0

```

5. 好家伙呢？只匹配了 10.1.12.0，藏得够深啊，怪不得呢？  
现在不删除原有配置情况下，加上 10.1.34.0 就好了

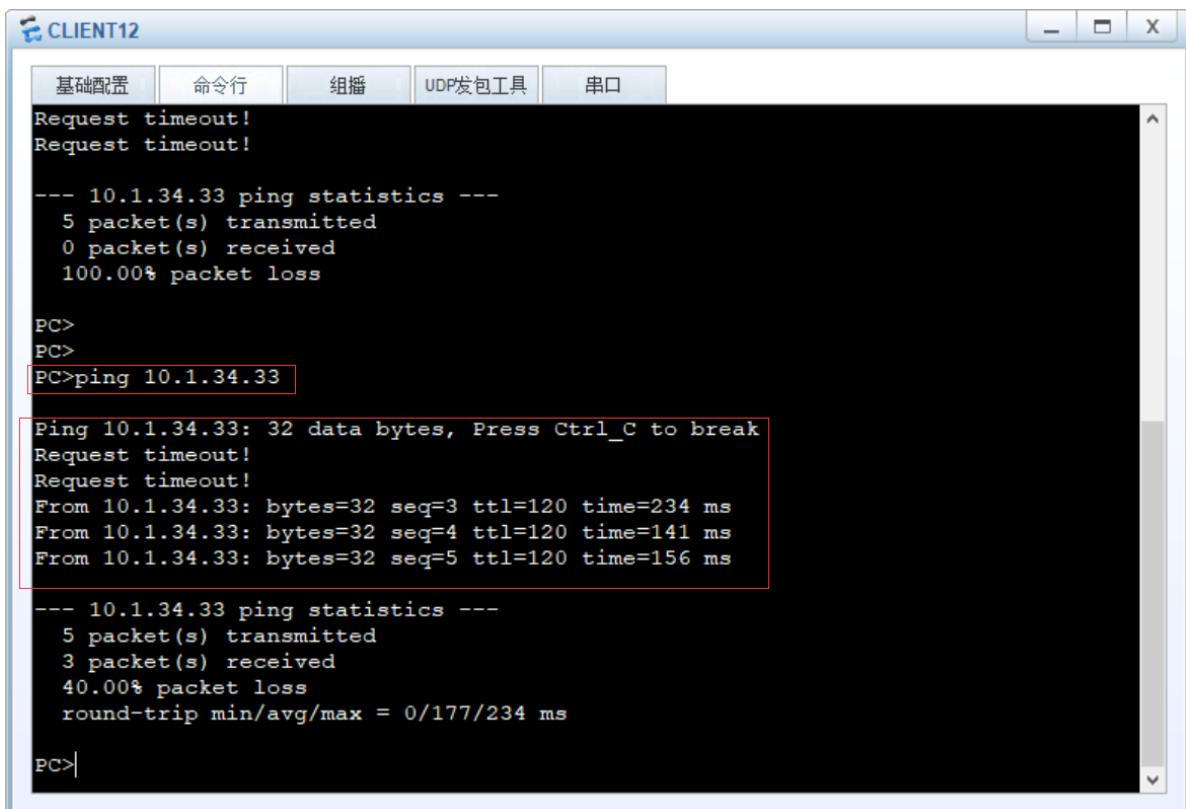
```
1 rule 5 permit source 10.1.34.0 0
```

## 6. R23 检查 vpn-instance 路由

```
1 [AR23]disp ip rou vpn-instance 1
2 Route Flags: R - relay, D - download to fib
3 -----
4 Routing Tables: 1
5 Destinations : 12 Routes : 15
6
7 Destination/Mask Proto Pre Cost Flags NextHop Interface
8
9     10.1.12.0/24 IBGP 255 0 RD 200.1.1.4
   GigabitEthernet0/0/0
10    10.1.34.0/24 IBGP 255 0 RD 200.1.1.4
   GigabitEthernet0/0/0
11
```

7. pc 互访看下，可以 ping 通了

8. tracert 有断层正常



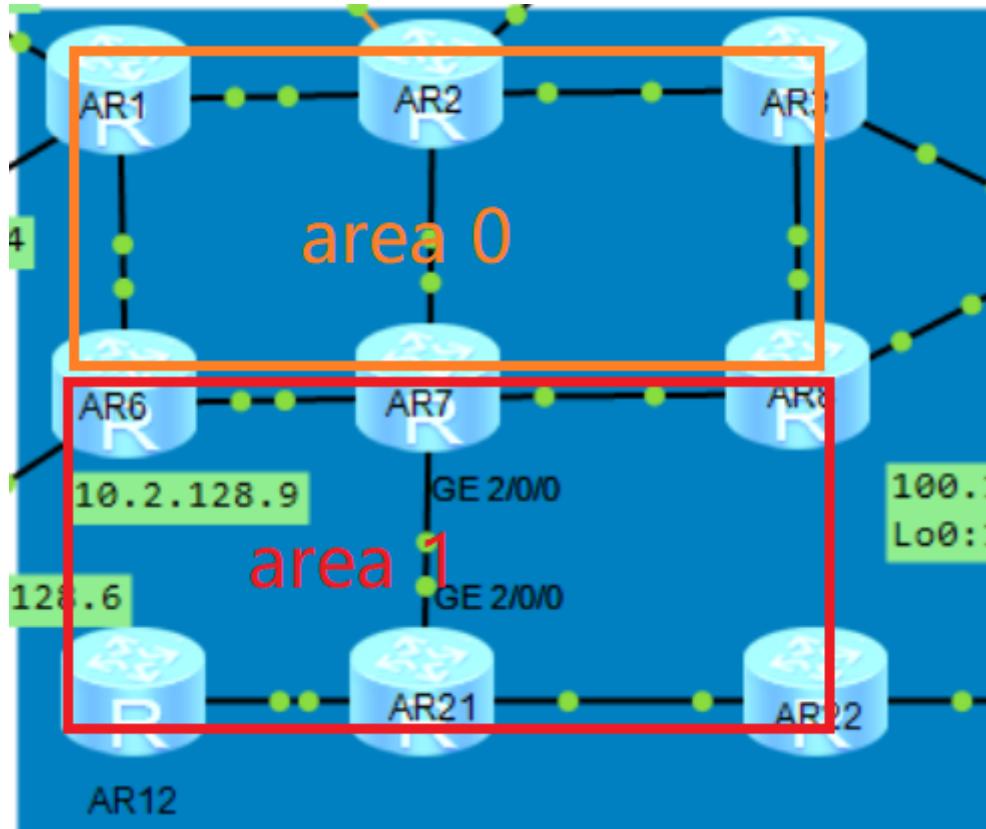
## 总结：

1. 考场上频繁发生的，ASBR 没有开启 mpls 能力
2. R9 上环回口没有宣告进 isis
3. R23 没有把路由从 bgp 引入进 isis
4. 一直再强调哪些错误的可能性是什么
  1. 你 R2 上什么路由都没有的话，可能性最大的就是没有关闭 RT 值检测

2. 如果只有本端没有对端的，是不是对端和你的对等体没有建立好，或者对端的域内出现一些问题
- 

## 6、OSPF 邻居

AS100中所部分设备的邻居关系有问题，解决此问题



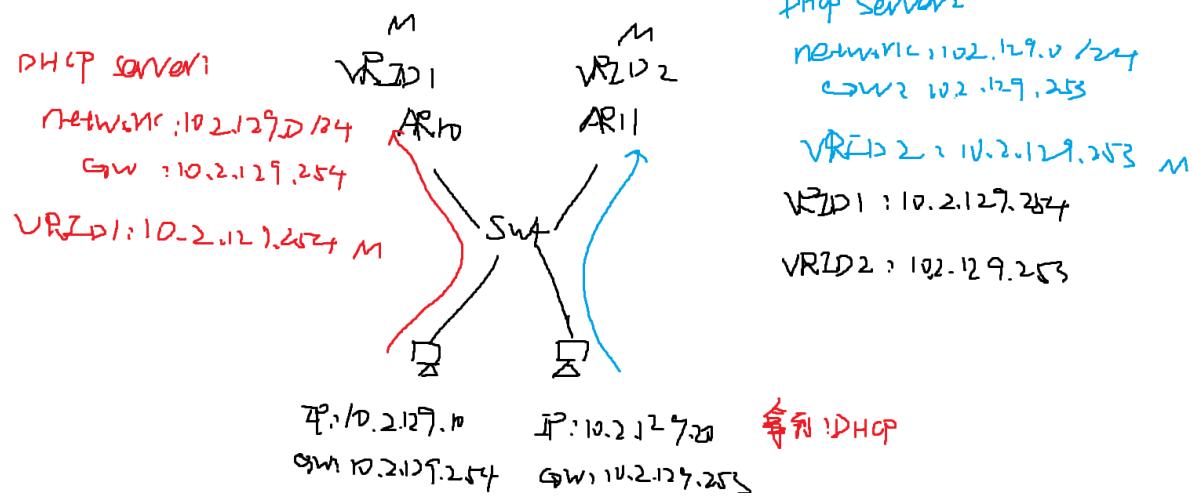
### 检查命令

1. `disp ospf peer brief`
  2. `disp ospf error int g0/0/0`
  3. `disp ospf int`
- 

## 7、VRRP

Site2中AR10与AR11要为LSW4的PC4提供第一跳网关冗余服务，虚拟网关地址为10.2.129.254和10.2.129.253；为了加速VRRP的收敛，使用BFD跟踪上行链路状态以及VRRP的邻居关系；

### 分析



准备好两个 虚拟路由器作为网关 10.2.129.254, 10.2.129.253, R10 作为 vrid 1 的 master, R11 作为 vrid 2 的 master

准备好两个 `dhcp server`, 分别维护同一个网段 10.2.129.0/24, 但是下发的网关不同, 一个是 V1、另一个是 V2

## 解决方案

### 一、配置 BFD

#### 1. R10 配置

```

1  bfd
2  q
3  bfd 1 bind peer-ip 10.2.106.6 source-ip 10.2.106.10 auto
4  commit
5  q
6  bfd 2 bind peer-ip 10.2.129.11 source-ip 10.2.129.10 auto
7  commit

```

#### 2. R11 配置

```

1  bfd
2  q
3  bfd 1 bind peer-ip 10.2.116.6 source-ip 10.2.116.11 auto
4  commit
5  q
6  bfd 2 bind peer-ip 10.2.129.10 source-ip 10.2.129.11 auto
7  commit

```

#### 3. R106 配置

```

1  bfd 1 bind peer-ip 10.2.106.10 source-ip 10.2.106.6 auto
2  commit
3  q
4  bfd 2 bind peer-ip 10.2.116.11 source-ip 10.2.116.6 auto
5  commit

```

#### 4. 验证

R10、R11、R106

```
1  disp bfd session all # 双双 up 就好了
```

## 二、配置VRRP

### 1. R10 配置

```
1 interface GigabitEthernet0/0/0
2   vrrp vrid 1 virtual-ip 10.2.129.254
3   vrrp vrid 1 priority 200
4   vrrp vrid 1 preempt-mode timer delay 1
5   vrrp vrid 1 track bfd-session session-name 1 reduced 120      # 易错 加上
6   vrrp vrid 1 authentication-mode md5 hcie
7
8   vrrp vrid 2 virtual-ip 10.2.129.253
9   vrrp vrid 2 preempt-mode timer delay 1
10  vrrp vrid 2 track bfd-session session-name 2 increase 120
11  vrrp vrid 2 authentication-mode md5 hcie
```

### 2. R11 配置

```
1 interface GigabitEthernet0/0/0
2   vrrp vrid 1 virtual-ip 10.2.129.254
3   vrrp vrid 1 preempt-mode timer delay 1
4   vrrp vrid 1 track bfd-session session-name 2 increase 120
5   vrrp vrid 1 authentication-mode md5 hcie
6
7   vrrp vrid 2 virtual-ip 10.2.129.253
8   vrrp vrid 2 priority 200
9   vrrp vrid 2 preempt-mode timer delay 1
10  vrrp vrid 2 track bfd-session session-name 1 reduced 120
11  vrrp vrid 2 authentication-mode md5 hcie
```

### 3. 验证

```
disp vrrp 1
disp vrrp brief
```

注意：部分配置不会直接覆盖，建议删除重新配置

```
[AR10]disp vrrp brief
Total:2      Master:1      Backup:1      Non-active:0
VRID  State       Interface           Type      Virtual IP
-----
1     Master       GE0/0/0          Normal    10.2.129.254
2     Backup       GE0/0/0          Normal    10.2.129.253
```

```
[AR11]disp vrrp brief
Total:2      Master:1      Backup:1      Non-active:0
VRID  State       Interface           Type      Virtual IP
-----
1     Backup       GE0/0/0          Normal    10.2.129.254
2     Master       GE0/0/0          Normal    10.2.129.253
```

## 8、DHCP

Site2中，AR10 AR11是DHCP服务器并且相互备份，要求CLIENT7能通过DHCP服务器获取到地址10.2.129.100；

要求CLIENT8只能获取指定地址为10.2.129.101；现在CLIENT8有时无法获取地址，请解决；

### 一、配置IP地址池

#### 1. R10配置

```
1 ip pool HCIE
2   gateway-list 10.2.129.254
3   network 10.2.129.0 mask 255.255.255.0
4   excluded-ip-address 10.2.129.1 10.2.129.99    # 加上
5   static-bind ip-address 10.2.129.100 mac-address 5489-9833-3389
6   static-bind ip-address 10.2.129.101 mac-address 5489-9812-4E45
7   dns-list 8.8.8.8
8   domain-name huawei.com
```

#### 2. R11配置

```
1 ip pool HCIE
2   gateway-list 10.2.129.253
3   network 10.2.129.0 mask 255.255.255.0
4   excluded-ip-address 10.2.129.1 10.2.129.99
5   static-bind ip-address 10.2.129.100 mac-address 5489-9833-3389
6   static-bind ip-address 10.2.129.101 mac-address 5489-9812-4E45
7   dns-list 8.8.8.8
8   domain-name huawei.com
```

### 二、配置接口 **dhcp select global**

R10、R11

```
1 int g0/0/0
2   dhcp select global
```

### 三、可能配置 **dhcp snooping trusted**

SW4

```
1 vlan 1
2   dhcp snooping enable
3   dhcp snooping trusted interface Ethernet0/0/1
4   dhcp snooping trusted interface Ethernet0/0/3
```

### 四、验证pc的dhcp地址

```
1 ipconfig /renew
2 # 如果考试刷不出来就不要刷了，接着往后面做
```

#### 1. PC7

```
PC>ipconfig /renew

IP Configuration

Link local IPv6 address.....: fe80::5689:98ff:fe33:3389
IPv6 address.....: :: / 128
IPv6 gateway.....: ::
IPv4 address.....: 10.2.129.100
Subnet mask.....: 255.255.255.0
Gateway.....: 10.2.129.254
Physical address.....: 54-89-98-33-33-89
DNS server.....: 8.8.8.8

PC>
```

2. PC8

```
PC>ipconfig /renew

IP Configuration

Link local IPv6 address.....: fe80::5689:98ff:fe12:4e45
IPv6 address.....: :: / 128
IPv6 gateway.....: ::
IPv4 address.....: 10.2.129.101
Subnet mask.....: 255.255.255.0
Gateway.....: 10.2.129.253
Physical address.....: 54-89-98-12-4E-45
DNS server.....: 8.8.8.8
```

## 9、VRRP6

正确部署VRRP6，要求AR10成为Master设备

### 解决方案

R10

```
1 interface GigabitEthernet0/0/0
2   ipv6 enable
3   ip address 10.2.129.10 255.255.255.0
4   ipv6 address 2002:10:2:129::10/64
5   ipv6 address FE80::10 link-local
6   vrrp6 vrid 1 virtual-ip FE80::254 link-local
7   vrrp6 vrid 1 virtual-ip 2002:10:2:129::254
```

R11

```
1 interface GigabitEthernet0/0/0
2   ipv6 enable
3   ip address 10.2.129.11 255.255.255.0
4   ipv6 address 2002:10:2:129::254/64 # 这里的 ipv6 地址
5   ipv6 address FE80::11 link-local
6   vrrp6 vrid 1 virtual-ip FE80::254 link-local
7   vrrp6 vrid 1 virtual-ip 2002:10:2:129::254 # 与 vrrp6 地址一致
```

会导致，优先级变为 255

即使 R10 配置了，也不会成为 master

```
1 int g0/0/0
2 vrrp6 vrid 1 priority 120
```

R11 上查看

1 disp vrrp6

```
[AR11-GigabitEthernet0/0/0]disp vrrp6  
GigabitEthernet0/0/0 | Virtual Router 1  
    State : Master  
    Virtual IP : FE80::254  
                  2002:10:2:129::254  
    Master IP : FE80::11  
    PriorityRun : 255  
    PriorityConfig : 100  
    MasterPriority : 255  
    Preempt : YES      Delay Time : 0 s  
    TimerRun : 100 cs  
    TimerConfig : 100 cs  
    Virtual MAC : 0000-5e00-0201  
    Check hop limit : YES  
    Config type : normal-vrrp  
    Create time : 2021-10-19 15:19:09 UTC-08:00  
    Last change time : 2021-10-19 15:23:29 UTC-08:00
```

因为 R11 的 ipv6 地址，与 yrrp6 的 virtual-ip 冲突，所以更改 ipv6 地址

```
1 int g0/0/0
2     undo ipv6 address 2002:10:2:129::254/64
3 # 此时 vrrp6 vrid 1 virtual-ip 2002:10:2:129::254 也会消失
4     ipv6 address 2002:10:2:129::11 64
5     vrrp6 vrid 1 virtual-ip 2002:10:2:129::254
```

验证

注意：考场观察一下新增 client14 的网关，虚拟IP地址与网关地址一致

R10

R11

## 10、QoS

Site3中AR20上一个用户（loopback0模拟）和AR18的一个用户（loopback0模拟）要进行语音通信，每路语音需要64Kbps的带宽，目前从AR20到AR18的语音质量不够好，需要在AR19上部署QoS，以保证语音流量的服务质量；**语音流量基于UDP目标端口号详见题本**

### 解决方案

#### 一、R19 配置入向复杂流分类将语音流量进行重标记

##### 1. 定义 ACL

查看 acl

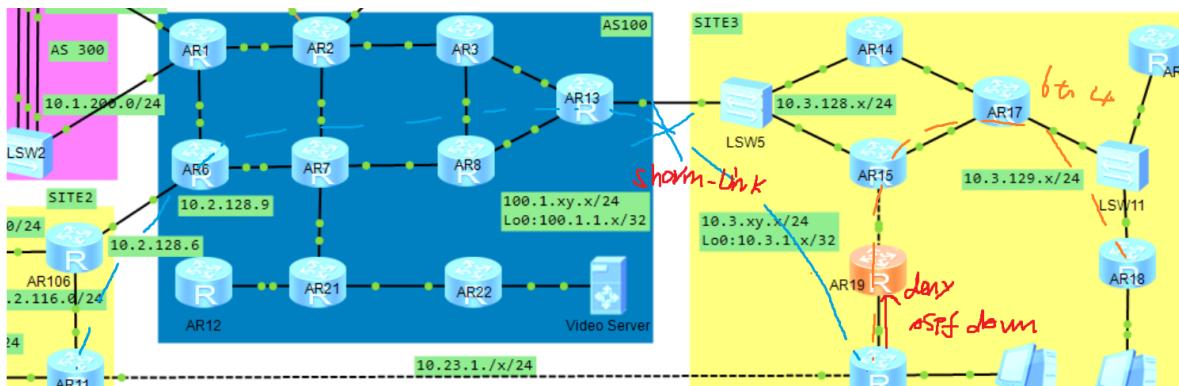
```
1 disp acl all
2     Total quantity of nonempty ACL number is 1
3     Advanced ACL UDP 3999, 1 rule
4     Acl's step is 5
5     rule 2 deny ip (10607 matches)
```

```
1 acl name UDP 3999
2     rule 2 deny ip # 务必删除
```

加上 rule 1, 用来匹配去往 R18 的语音流量

```
1 rule 1 permit udp source 10.3.1.20 0 destination 10.3.1.18 0 destination-port
range 16384 32767
```

注意：不然会影响 ospf 邻居等等问题



```
1 rule 2 deny ip # 该规则会导致所有其他流量被丢弃，务必删除，哪怕没考察到 QoS，该错误也 务必
删除
2 undo rule 2
```

##### 2. 定义流分类

```
1 traffic classifier Match-UDP
2 if-match acl UDP
```

##### 3. 定义流行为

```
1 traffic behavior Remark-EF
2 remark dscp ef
```

##### 4. 定义流策略

```
1 traffic policy Remark-EF
2 classifier Match-UDP behavior Remark-EF
```

## 5. R19 接口入向调用流策略

```
1 interface GigabitEthernet0/0/0
2     undo traffic-policy outbound
3     traffic-policy Remark-EF inbound
```

## 二、R19配置出向CBQ基于类队列进行优先转发（保证带宽）

### 1. 定义流分类

```
1 traffic classifier Match-EF
2     if-match dscp ef
```

### 2. 定义流行为

```
1 traffic behavior CBQ
2     queue llq bandwidth 64 cbs 1600
```

### 3. 定义流策略

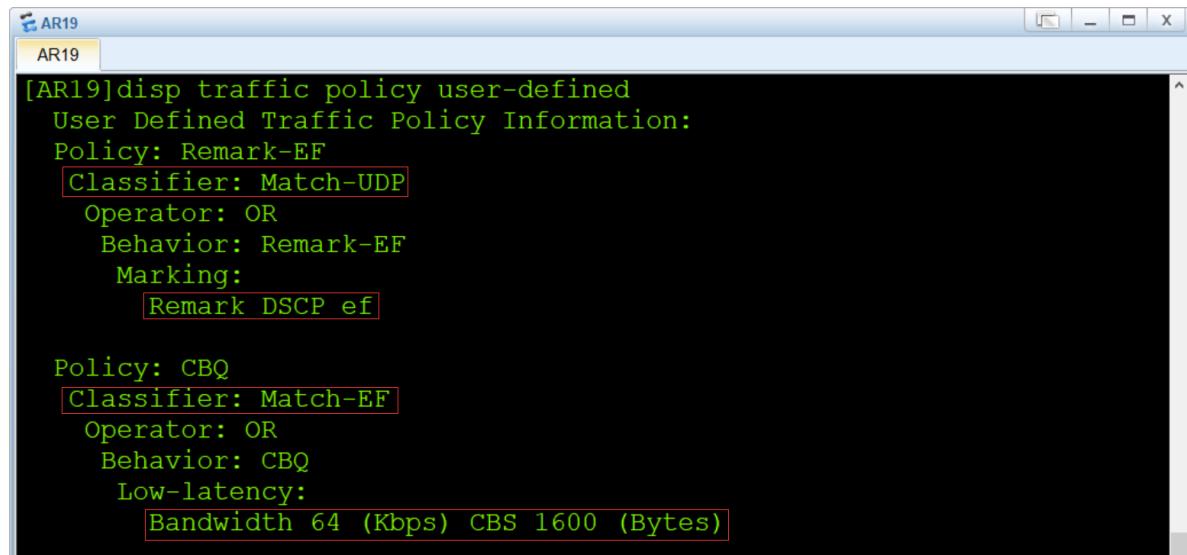
```
1 traffic policy CBQ
2     classifier Match-EF behavior CBQ
```

### 4. 接口下出向调用流策略 CBQ

```
1 interface Serial3/0/0
2     traffic-policy CBQ outbound
```

## 验证

`disp traffic policy user-defined` : 查看用户自定义策略



```
[AR19]disp traffic policy user-defined
User Defined Traffic Policy Information:
Policy: Remark-EF
Classifier: Match-UDP
Operator: OR
Behavior: Remark-EF
Marking:
    Remark DSCP ef

Policy: CBQ
Classifier: Match-EF
Operator: OR
Behavior: CBQ
Low-latency:
    Bandwidth 64 (Kbps) CBS 1600 (Bytes)
```

`disp traffic-policy applied-record` : 查看策略调用结果

```

[AR19]disp traffic-policy ap
[AR19]disp traffic-policy applied-record
-----
Policy Name: Remark-EF
Policy Index: 0
Classifier:Match-UDP Behavior:Remark-EF
-----
*interface GigabitEthernet0/0/0
traffic-policy Remark-EF inbound
slot 0 : success
-----
Policy Name: CBQ
Policy Index: 1
Classifier:Match-EF Behavior:CBQ
-----
*interface Serial3/0/0
traffic-policy CBQ outbound
slot 3 : success

```

## 11、Sham-link

Site2与Site3为同一个VPN客户的两个站点，现在AR10与AR20上面的客户（loopback0模拟）都能互通；请解决此问题；并且要求当AS100连接正常的时候，两个客户的数据包通信必须经过AS100；但是AS100出现问题的时候，两个站点可以通过备份链路进行通信；

### 一、解决 MPLS-VPN 单域问题

#### 1. 控制层面故障

A. PE设备是否做了路由的引入 --- 发现都有

R7 配置

```

1 ospf 110 router-id 10.3.128.6 vpn-instance 2
2 import-route bgp

1 bgp 100
2 ipv4-family vpn-instance 2
3 import-route ospf 110

```

B. PE借助RR(R7)传递路由时，对等体建立错误 --- 无错误

	Peer	V	AS	MsgRcvd	MsgSent	OutQ	Up/Down	State
	PrefRcv							
3	100.1.1.1	4	100	1022	1114	0	16:51:49	Established
	5							
4	100.1.1.2	4	100	1875	1954	0	0029h59m	Established
	7							
5	100.1.1.6	4	100	1829	1849	0	0029h43m	Established
	21							
6	100.1.1.13	4	100	1079	1042	0	16:51:27	Established
	21							

C. RR配置错误，没有指定特定的客户端 --- R6、R13没指定客户端

D. RR 没有关闭 RT 值检测 --- 在做 option b 时已关

R7 配置

```
1 bgp 100
2     ipv4-family vpnv4
3         undo policy vpn-target
4         peer 100.1.1.1 enable
5         peer 100.1.1.1 reflect-client
6         peer 100.1.1.2 enable
7         peer 100.1.1.2 reflect-client
8         peer 100.1.1.6 enable
9         peer 100.1.1.6 reflect-client
10        peer 100.1.1.13 enable
11        peer 100.1.1.13 reflect-client
```

这里可以在 R13 上查看 vpnv4 路由了 --- 如果没有就要检查下 RT 值了

```
disp bgp vpnv4 all routing-table
```

```
disp ip rou vpn-instance 2
```

```
1 VPN-Instance 2, Router ID 100.1.1.3:
2
3 Total Number of Routes: 28
4      Network          NextHop          MED      LocPrf  PrefVal Path/Ogn
5  *>  10.2.1.10/32    0.0.0.0       100          0      ?
6  * i                100.1.1.6      3        100          0      ?
7  *>  10.2.1.11/32    0.0.0.0       99          0      ?
8  * i
```

E. PE 两端 RT 值配置错误

R6、R13

```
1 ip vpn-instance 2
2 disp this
```

2. 转发层面故障

A. 底层 IGP 故障

```
1 disp ospf peer brief
```

B. 底层 LDP 故障 --- 接口 mpls 未开

```
1 disp mpls ldp session all
```

## 二、配置 sham-link

1. R6 和 R13 之间建立 sham-link

A. 使用 LoopBack2 作为 sham-link 源目地址

OSPF 私网进程的下 area 1 配置 sham-link

R6 配置

```
1 ospf 110 router-id 10.3.128.6 vpn-instance 2
2 import-route bgp
3 area 0.0.0.0
4 sham-link 100.1.136.13 100.1.136.6
```

发现 sham-link 区域错误以及源目地址错误

```
1 area 0.0.0.1
2 sham-link 100.1.136.6 100.1.136.13
```

R13 配置

```
1 area 0.0.0.1
2 sham-link 100.1.136.6 100.1.136.13
```

发现 sham-link 源目地址错误

```
1 area 0.0.0.1
2 sham-link 100.1.136.13 100.1.136.6
```

---

B. 该接口务必绑定进 **VPN-instance 2**

R6 配置

```
1 [AR6]disp ip vpn-instance 2 int
2 VPN-Instance Name and ID : 2, 1
3 Interface Number : 2
4 Interface list : GigabitEthernet0/0/2, # 有对 ospf 私网的接口
5 LoopBack2 # 有 loop2
```

R13 配置 --- 可能考场是 **LoopBack2** 未宣告

```
1 [AR13]disp ip vpn-instance 2 interface
2 VPN-Instance Name and ID : 2, 1
3 Interface Number : 3
4 Interface list : GigabitEthernet0/0/0, # 有对 bgp 私网的接口
5 LoopBack1,
6 LoopBack2 # 发现也有
```

---

C. 该接口地址必须通过 bgp 私网实例进行通告

R6 配置 --- 发现有

```
1 bgp 100
2 ipv4-family vpn-instance 2
3 network 100.1.136.6 255.255.255.255
```

R13 配置 --- **未宣告**

```
1 bgp 100
2 ipv4-family vpn-instance 2
3 network 100.1.136.13 255.255.255.255
```

---

D. 该接口 **不能** 宣告进 ospf 私网当中 --- 会导致 sham-link 起不来

R6 配置

```

1 ospf 110 router-id 10.3.128.6 vpn-instance 2
2 import-route bgp
3 area 0.0.0.1
4 network 10.2.1.6 0.0.0.0
5 network 10.2.128.9 0.0.0.0
6 network 100.1.136.6 0.0.0.0 # 发现有将自己的 LoopBack2 宣告进来
7 network 100.1.136.13 0.0.0.0 # 宣告 R13 的 LoopBack2 干嘛? 删掉
8 sham-link 100.1.136.6 100.1.136.13
9

```

改正

```

1 ospf 110
2 area 1
3 undo network 100.1.136.6 0.0.0.0
4 undo network 100.1.136.13 0.0.0.0

```

R13 配置

```

1 ospf 110 router-id 10.3.128.13 vpn-instance 2
2 import-route bgp
3 area 0.0.0.1
4 network 10.3.1.13 0.0.0.0
5 network 10.3.128.13 0.0.0.0
6 network 100.1.136.13 0.0.0.0 # 发现有将自己的 LoopBack2 宣告进来
7 sham-link 100.1.136.13 100.1.136.6

```

改正

```

1 ospf 110
2 area 1
3 undo network 100.1.136.13 0.0.0.0

```

验证 sham-link

R6

```
[AR6]disp ospf sham-link

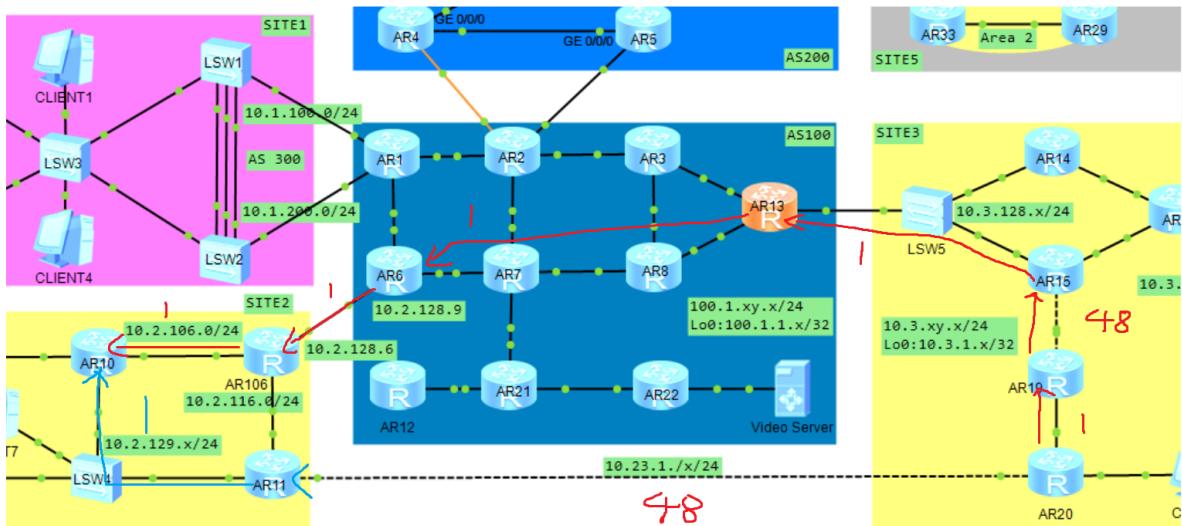
    OSPF Process 100 with Router ID 100.1.1.6
Sham Link:
Area          NeighborId      Source-IP        Destination-IP   State Cost
          0.0.0.1      10.3.128.13      100.1.136.6      100.1.136.13   P-2-P 1
          0.0.0.1      10.3.128.13      100.1.136.6      100.1.136.13   P-2-P 1
```

R13

```
[AR13]disp ospf sham-link

    OSPF Process 100 with Router ID 100.1.1.13
Sham Link:
Area          NeighborId      Source-IP        Destination-IP   State Cost
          0.0.0.1      10.3.128.6       100.1.136.13      100.1.136.6   P-2-P 1
          0.0.0.1      10.3.128.6       100.1.136.13      100.1.136.6   P-2-P 1
```

### 三、调整开销值



如图所示

R20 --- R10

1. 从 **mpls 骨干网** 的 cost =  $1 + 48 + 1 + 1 + 1 + 1 = 53$
2. 从 备份链路的 cost =  $48 + 1 = 49$

所以我们 R11、R20 的链路开销为 100

R11 配置

```
1 interface Serial3/0/1
2 ospf cost 100
```

R20 配置

```
1 interface Serial3/0/0
2 ospf cost 100
```

**验证：**

R10 --- R20

```
1 [AR10]ping -r -a 10.2.1.10 10.3.1.20
2 PING 10.3.1.20: 56 data bytes, press CTRL_C to break
3 Reply from 10.3.1.20: bytes=56 Sequence=1 ttl=251 time=130 ms
4 Record Route:
5 10.2.128.6
6 10.2.128.9
7 10.3.128.13
8 10.3.159.15
9 10.3.192.19
10 10.3.1.20
11 10.3.159.19
12 10.3.128.15
13 10.3.128.13
```

哎，怎么回来的时候到 13 就没有了呢？--- 后面百度知道 **由于 ping -r 命令最多只能跟踪到9个路由，多以后面的不予显示**，后来查文档，-r 后面没有<参数>可跟

接着分段验证

我先 tracert R10 --- R20, 看看走的是哪个网络 --- 发现走的是 mpls 骨干网

```
1 <AR10>tracert -a 10.2.1.10 10.3.1.20
2 traceroute to 10.3.1.20(10.3.1.20), max hops: 30 ,packet length: 40,press CTRL
3 _C to break
4 1 10.2.106.6 30 ms 10 ms 20 ms
5 2 10.2.128.9 10 ms 10 ms 10 ms
6 3 100.1.67.7 40 ms 30 ms 40 ms
7 4 100.1.78.8 40 ms 40 ms 40 ms
8 5 10.3.128.13 50 ms 40 ms 40 ms
9 6 10.3.128.15 50 ms 80 ms 60 ms
10 7 10.3.159.19 70 ms 60 ms 70 ms
11 8 10.3.192.20 50 ms 90 ms 60 ms
12
```

再 tracert R20 --- R10, 看看回去走的哪个网络 --- 发现走的是 mpls 骨干网

```
1 [AR20]tracert -a 10.3.1.20 10.2.1.10
2 traceroute to 10.2.1.10(10.2.1.10), max hops: 30 ,packet length: 40,press CTRL
3 _C to break
4 1 10.3.192.19 20 ms 20 ms 20 ms
5 2 10.3.159.15 30 ms 40 ms 30 ms
6 3 10.3.128.13 50 ms 60 ms 70 ms
7 4 100.1.138.8 80 ms 80 ms 50 ms
8 5 100.1.78.7 90 ms 70 ms 80 ms
9 6 10.2.128.9 60 ms 90 ms 60 ms
10 7 10.2.128.6 60 ms 80 ms 70 ms
11 8 10.2.106.10 80 ms 70 ms 70 ms
```

```
1 rule 5 permit source 10.0.1.10 0.0.0.0
2 rule 5 permit source 10.0.1.10 0.0.0.255
```

上面两条命令的区别?

## 12、telnet

Site3中，AR16 AR17 AR18帧中继网络中运行ospf，使用默认的网络类型；要求AR18能通过telnet远程管理AR16、AR17；现在AR18 无法远程管理；解决此问题并满足以下条件：

- 要求AR16的telnet认证方式为AAA，AR16上存在两个用户：admin用户级别为15级，guest用户级别为1级，要求两个用户都能通过telnet登录；
- 要求AR17的认证方法为password，支持命令要求与截图一致-----考场具体看图，我不贴了

### 解决方案

#### 一、R16的 telnet 认证方式为 AAA，admin 用户级别为 15 级，guest 用户级别为 1 级

1. 先去看下 aaa

```
1 aaa
2   local-user admin password cipher hcie
3   local-user admin privilege level 15
4   local-user admin service-type telnet
5   local-user guest password cipher hcie
6   local-user guest privilege level 1
7   local-user guest service-type telnet
```

## 2. 再去看下 vty --- 改下认证方式为 aaa

```
1 user-interface vty 0 4  
2 authentication-mode aaa
```

### 3. 注意：考场可能会加上以下错误

- vty 下只放行了 ssh， 并未放行 telnet

```
1 user-interface vty 0 4  
2 protocol inbound ssh
```

直接改成 telnet 就好了

```
1 user-interface vty 0 4  
2 protocol inbound telnet
```

- 可能存在流量过滤

```
1 acl number 2000  
2 rule 5 deny  
3 user-interface vty 0 4  
4 acl 2000 inbound
```

不删除 acl， 加上业务网段规则就好了

```
1 rule 1 permit source 10.3.0.0 0.0.255.255
```

## 二、R17 的认证方法为 password

```
1 user-interface vty 0 4  
2 authentication-mode password  
3 set authentication password cipher hcie # 修改  
4 user privilege level 3 # 加上
```

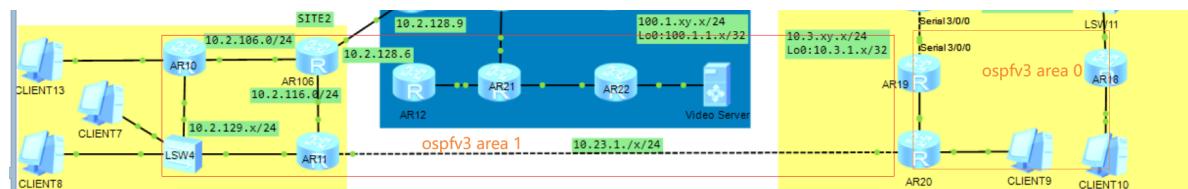
## 验证

看考场图

## 13、IPV6

Site2与Site3配置了IPV6，并且运行OSPFV3协议；参与的设备有AR10、AR11、AR18、AR20；AR18与AR20之间通过tunnel相通；

现在环境中的IPV6 CLIENT 13、IPV6 CLIENT 9、IPV6 CLIENT10无法实现互相通信，请解决；



## 解决方案

### 一、查看 tunnel, GRE 隧道是否配置错误

#### 1. R20 配置

```
1 interface Tunnel0/0/100
2   description 10.3.1.18
3   ipv6 enable
4   ipv6 address 2002:100:100::20/64
5   ipv6 address FE80::20 link-local
6   ospfv3 1 area 0.0.0.0
7   tunnel-protocol gre
8   source LoopBack0
9   destination 10.3.1.18
10  gre key 122  # 这里有误
```

#### 改正

```
1 interface Tunnel0/0/100
2   gre key 123
```

#### 1. R18 配置 --- 没问题

```
1 interface Tunnel0/0/100
2   description 10.3.1.20
3   ipv6 enable
4   ipv6 address 2002:100:100::18/64
5   ipv6 address FE80::18 link-local
6   ospfv3 1 area 0.0.0.1
7   tunnel-protocol gre
8   source LoopBack0
9   destination 10.3.1.20
10  gre key 123
```

---

### 二、查看 ospfv3 配置

#### 1. 检查 ospfv3 邻居关系

```
1 disp ospfv3 peer
```

发现 R20 --- R11 邻居关系没起来

发现 R20 --- R18 邻居关系没起来

#### 2. R20 配置

```
1 ospfv3 1
2   router-id 10.3.1.20
3   area 0.0.0.0
4   abr-summary 2002:10:3:209:: 64 not-advertise
```

看见有个汇总，一看是 client9 的，他是不通告，相当于过滤

```
1 ospfv3 1
2   area 0.0.0.0
3   abr-summary 2002:10:3:209:: 64
```

#### 3. R11 配置

```
1 ospfv3 1
2 router-id 10.3.1.20
```

发现 **route-id** 冲突

```
1 ospfv3 1
2 undo router-id
3 router-id 10.3.1.11
```

4. 检查 ospfv3 邻居关系 --- 发现 R11 已经和 R10, R20 建立好了

```
1 [AR11]disp ospfv3 peer
2 OSPFv3 Process (1)
3 OSPFv3 Area (0.0.0.1)
4 Neighbor ID      Pri  State          Dead Time Interface      Instance
ID
5   10.2.1.10        1   Full/DR       00:00:34  GE0/0/0
6   10.3.1.20        1   Full/-        00:00:34  S3/0/1
```

5. R18 配置

发现 tunnel0/0/100 中 ospfv3 区域配错了

```
1 int t0/0/100
2 ospfv3 1 area 0.0.0.0
```

6. R20 配置错误静默接口

```
1 ospfv3 1
2 silent-interface Tunnel0/0/100
```

改正

```
1 ospfv3 1
2 undo silent-interface Tunnel0/0/100
```

7. 查看 R20 ospfv3 邻居关系 --- 没问题了

```
1 [AR20]disp ospfv3 peer
2 OSPFv3 Process (1)
3 OSPFv3 Area (0.0.0.0)
4 Neighbor ID      Pri  State          Dead Time Interface      Instance
ID
5   10.3.1.18        1   Full/-        00:00:35  Tun0/0/100
6   0
6 OSPFv3 Area (0.0.0.1)
7 Neighbor ID      Pri  State          Dead Time Interface      Instance
ID
8   10.3.1.11        1   Full/-        00:00:30  S3/0/0
9   0
```

## 验证

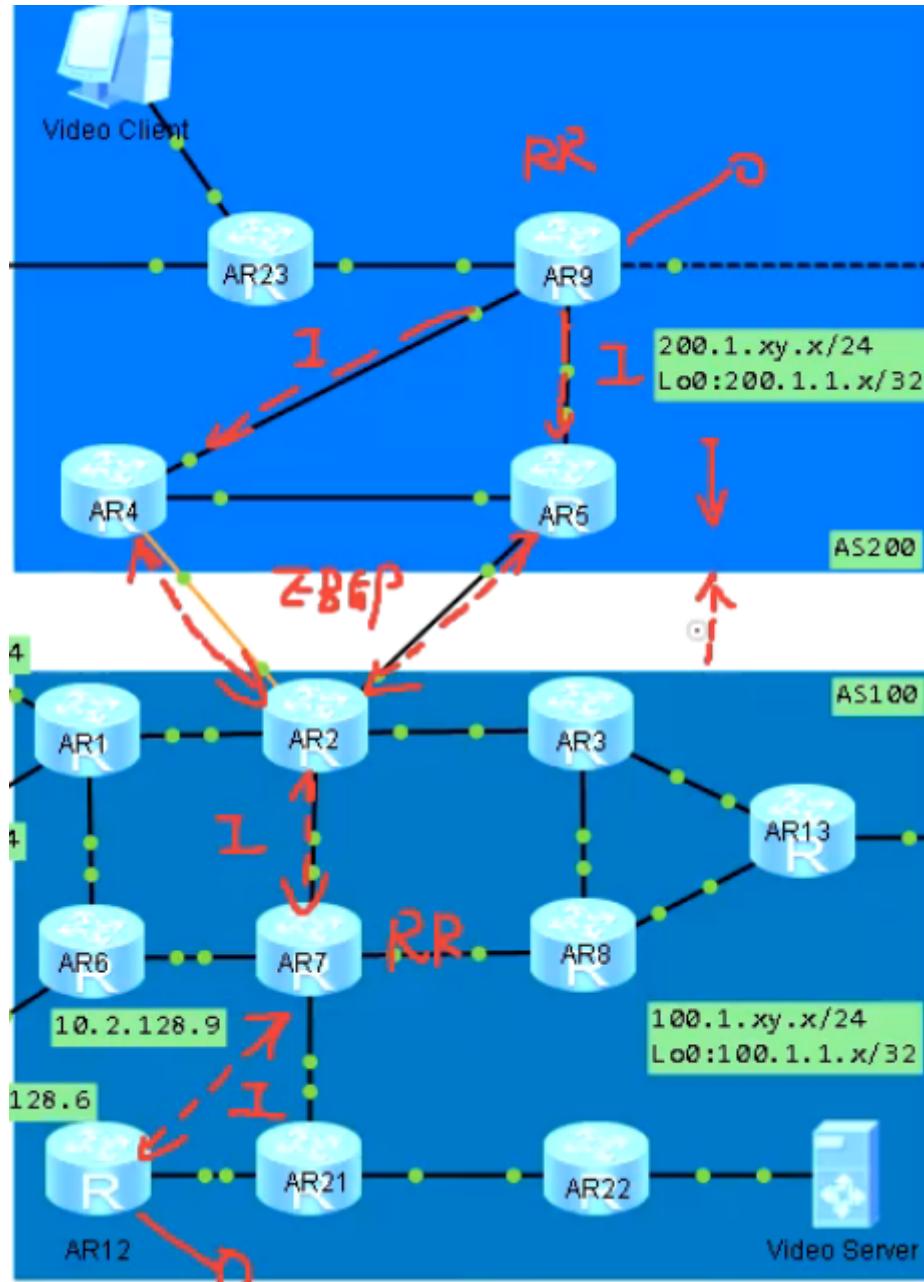
所有 IPv6 客户端验证互访即可，如果存在无法互访检查连接客户端对应接口 OSPFv3 是否启用

IPV6 CLIENT13、IPV6 CLIENT9、IPV6 CLIENT10 互访成功

注意：VRRP6 需求中新增 Clinet14 可能无法通信成功，VRRP6 在 ENSP 中有 bug

## 14、BGP IPV4互访

要求AS100中AR12的loopback0口能够访问AS200中的AR9的loopback0口；但是现在两个loopback0口地址无法访问；请解决该问题



### 可能故障原因

1. 对等体没有建立好
2. RR 客户端没有指定
3. ASBR 上未把 IGP 引入进 BGP
4. 各环回口没有宣告进 IGP
5. AR2、AR4、AR5 需要配置下一跳本地

注意：

```
1 bgp 100
2     bgp # 错误输入
3     # 则会添加如下命令
4     # 导致路由只存在于BGP路由表，不加入IP路由表
5     bgp 100 bgp-rib-only
```

## 解决方案

### 一、检查 bgp 邻居

1. R12 配置 --- 发现没有与 R7 建立邻居

进入 bgp 100 查看 没有用 更新源 LoopBack0

```
1 bgp 100
2     router-id 100.1.1.12
3     peer 100.1.1.7 as-number 100
4     peer 100.1.1.7 connect-interface LoopBack0
```

2. R7 配置 --- 发现对 R12 的 as 号错误，删掉配置，并且未配置客户端

```
1 bgp 100
2     peer 100.1.1.12 as-number 200
3     peer 100.1.1.12 connect-interface LoopBack0
4     peer 100.1.1.12 reflect-client
5     # 注意该条命令不是错误配置，题本要求 R13 不要承载 IPv4 单播路由，只传递 VPNv4
6     undo peer 100.1.1.13 enable
```

### 二、检查路由发布

1. AS200 在 R4 和 R5 上将 IS-IS 引入进 BGP

```
1 bgp 200
2     ipv4-family unicast
3     import-route isis 200
```

2. AS100 在 R2 上将 OSPF 引入进 BGP

```
1 bgp 100
2     ipv4-family unicast
3     import-route ospf 100 route-policy ospf_bgp
```

发现有一个 route-policy，查看一下

```
1 [AR2-bgp]disp route-policy ospf_bgp
2 Route-policy : ospf_bgp
3     permit : 1 (matched counts: 164)
4         Match clauses :
5             if-match acl 2000
```

接着查看 acl 2000 --- 发现就是 匹配环回口的

```
1 acl 2000
2     rule 5 permit source 100.1.1.8 0
3     rule 10 permit source 100.1.1.21 0
4     rule 15 permit source 100.1.1.22 0
5     rule 30 permit source 100.1.1.2 0
6     rule 1000 deny
```

加上

```
1 rule 1 permit source 100.1.1.0 0.0.0.255
```

### 3. 逐个检查路由

R12 --- R7 --- R2 --- R4 --- R5 --- R9

```
1 [AR2]disp bgp routing-table # 发现自己 AS 环回口都有了, 对面的也有了
2
3 BGP Local router ID is 100.1.1.2
4 Status codes: * - valid, > - best, d - damped,
5 h - history, i - internal, s - suppressed, S - Stale
6 Origin : i - IGP, e - EGP, ? - incomplete
7
8 Total Number of Routes: 30
9      Network          NextHop        MED      LocPrf     PrefVal
Path/Ogn
10
11  *>  100.1.1.1/32    0.0.0.0       1        0        ?
12  *>  100.1.1.2/32    0.0.0.0       0        0        ?
13  *>  100.1.1.3/32    0.0.0.0       1        0        ?
14  *>  100.1.1.6/32    0.0.0.0       2        0        ?
15  *>  100.1.1.7/32    0.0.0.0       1        0        ?
16  *>  100.1.1.8/32    0.0.0.0       2        0        ?
17  *>  100.1.1.12/32   0.0.0.0       3        0        ?
18  *>  100.1.1.13/32   0.0.0.0       2        0        ?
19  *>  100.1.1.21/32   0.0.0.0       2        0        ?
20  *>  100.1.1.22/32   0.0.0.0       3        0        ?
21  *>  200.1.1.4/32    200.100.24.4  0        0        200?
22  *           200.100.25.5   10       0        200?
23  *>  200.1.1.5/32    200.100.25.5  0        0        200?
24  *           200.100.24.4   10       0        200?
25  *>  200.1.1.9/32    200.100.24.4  10      0        200?
26  *           200.100.25.5   10       0        200?
27  *>  200.1.1.23/32   200.100.24.4  20      0        200?
28  *           200.100.25.5   20       0        200?
29  *>  200.1.1.99/32   200.100.24.4  10      0        200?
30  *           200.100.25.5   10       0        200?
31  *>  200.1.29.0      200.100.24.4  30      0        200?
32  *           200.100.25.5   30       0        200?
33  *>  200.1.45.0      200.100.24.4  0        0        200?
34  *           200.100.25.5   0        0        200?
35  *>  200.1.49.0      200.100.24.4  0        0        200?
36  *           200.100.25.5   20       0        200?
37  *>  200.1.59.0      200.100.25.5  0        0        200?
38  *           200.100.24.4   20       0        200?
39  *>  200.1.239.0     200.100.24.4  20      0        200?
40  *           200.100.25.5   20       0        200?
```

```
1 [AR9]disp bgp routing-table # 发现自己 AS 环回口都有了, 对面的也有了
2
3 BGP Local router ID is 200.1.1.9
4 Status codes: * - valid, > - best, d - damped,
5 h - history, i - internal, s - suppressed, S - Stale
6 Origin : i - IGP, e - EGP, ? - incomplete
7
8 Total Number of Routes: 40
```

9	Network Path/Ogn	NextHop	MED	LocPrf	PrefVal
10					
11	*>i 100.1.1.1/32	200.1.1.4	1	100	0 100?
12	* i	200.1.1.5	1	100	0 100?
13	*>i 100.1.1.2/32	200.1.1.4	0	100	0 100?
14	* i	200.1.1.5	0	100	0 100?
15	*>i 100.1.1.3/32	200.1.1.4	1	100	0 100?
16	* i	200.1.1.5	1	100	0 100?
17	*>i 100.1.1.6/32	200.1.1.4	2	100	0 100?
18	* i	200.1.1.5	2	100	0 100?
19	*>i 100.1.1.7/32	200.1.1.4	1	100	0 100?
20	* i	200.1.1.5	1	100	0 100?
21	*>i 100.1.1.8/32	200.1.1.4	2	100	0 100?
22	* i	200.1.1.5	2	100	0 100?
23	*>i 100.1.1.12/32	200.1.1.4	3	100	0 100?
24	* i	200.1.1.5	3	100	0 100?
25	*>i 100.1.1.13/32	200.1.1.4	2	100	0 100?
26	* i	200.1.1.5	2	100	0 100?
27	*>i 100.1.1.21/32	200.1.1.4	2	100	0 100?
28	* i	200.1.1.5	2	100	0 100?
29	*>i 100.1.1.22/32	200.1.1.4	3	100	0 100?
30	* i	200.1.1.5	3	100	0 100?
31	*>i 200.1.1.4/32	200.1.1.5	10	100	0 ?
32	i	200.1.1.4	0	100	0 ?
33	*>i 200.1.1.5/32	200.1.1.4	10	100	0 ?
34	i	200.1.1.5	0	100	0 ?
35	*>i 200.1.1.9/32	200.1.1.4	10	100	0 ?
36	* i	200.1.1.5	10	100	0 ?
37	*>i 200.1.1.23/32	200.1.1.4	20	100	0 ?
38	* i	200.1.1.5	20	100	0 ?
39	*>i 200.1.1.99/32	200.1.1.4	10	100	0 ?
40	* i	200.1.1.5	10	100	0 ?
41	*>i 200.1.29.0	200.1.1.4	30	100	0 ?
42	* i	200.1.1.5	30	100	0 ?
43	*>i 200.1.45.0	200.1.1.4	0	100	0 ?
44	* i	200.1.1.5	0	100	0 ?
45	*>i 200.1.49.0	200.1.1.4	0	100	0 ?
46	* i	200.1.1.5	20	100	0 ?
47	*>i 200.1.59.0	200.1.1.5	0	100	0 ?
48	* i	200.1.1.4	20	100	0 ?
49	*>i 200.1.239.0	200.1.1.4	20	100	0 ?
50	* i	200.1.1.5	20	100	0 ?

### 三、配置下一跳本地

#### 1. AR2 配置

```
1 bgp 100
2 peer 100.1.1.7 next-hop-local
```

#### 2. AR4、AR5 配置

```
1 bgp 200
2 peer 200.1.1.9 next-hop-local
```

## 验证

```
1 <AR12>ping -a 100.1.1.12 200.1.1.9
2     PING 200.1.1.9: 56 data bytes, press CTRL_C to break
3         Reply from 200.1.1.9: bytes=56 Sequence=1 ttl=251 time=70 ms
4         Reply from 200.1.1.9: bytes=56 Sequence=2 ttl=251 time=50 ms
5         Reply from 200.1.1.9: bytes=56 Sequence=3 ttl=251 time=50 ms
6         Reply from 200.1.1.9: bytes=56 Sequence=4 ttl=251 time=50 ms
7         Reply from 200.1.1.9: bytes=56 Sequence=5 ttl=251 time=40 ms
```

## 15、BGP IPV6互访

AS200中AR9、AR4、AR5上面各有一个IPV6客户站点（loopback1模拟），AS100中有R2、R7上各有一个IPV6客户站点（loopback1模拟），要求这几个站点都能互通，并且要求双向路径要优选AR2-AR4之间的链路，一旦主用链路出现问题在使用备用链路AR2-AR5；现在这几个站点之间的互通存在部分问题，请解决；

**注意：考场上选路策略只允许在 AS100 中配置**

### 分析

站在 R2 视角分析进出路由，使用的策略

1. R2 在发出路由的时候将 `med` 值改大或改小，考场上用的是增加 `as-path` 路径
  - 对于发给 R4 的 `as-path` 不做调整
  - 对于发给 R5 的 `as-path` 加长
2. R2 在接收路由的时候将 `LocalPreference` 改大或改小
  - 对于 R4 发来的路由 `LocalPreference` 改大
  - 对于 R5 发来的路由 `LocalPreference` 不做调整

### 可能故障原因

1. BGP ipv6 邻居关系 down
2. BGP 路由发布错误和传递错误
3. BGP ipv6 反射器配置
4. R2 检查对于 R4 的 `LP` 路由策略错误
  - 方向错误
5. R2 检查对于 R5 的 `AS` 路由策略错误
  - AS 号更改为 200 的系统号 --- 导致 AS200 不接受
  - 方向错误

### 解决方案

1. 检查 BGP ipv6 邻居关系

R2、R9 --- 发现没有问题

```
1 disp bgp ipv6 peer
```

2. 检查路由发布 --- 每台路由器通过network命令发布自身的环回口1接口地址

## 检查自己自治系统的路由发布

AS 100 内

R7 查看 --- 发现并没有发布自己的 LoopBack1

```
1 ipv6-family unicast
2 peer 2002:100:1:1::2 enable
```

加上

```
1 ipv6-family unicast
2 network 2002:100:7:1::1 128
```

R2 查看 --- 发现有

```
1 ipv6-family unicast
2 network 2002:100:2:1::1 128
```

---

AS 200 内 --- 都有

R9 查看

```
1 ipv6-family unicast
2 network 2002:200:9:1::1 128
```

R4 查看

```
1 ipv6-family unicast
2 network 2002:200:4:1::1 128
```

R5 查看

```
1 ipv6-family unicast
2 network 2002:200:5:1::1 128
```

## AR2、AR4、AR5 配置下一跳本地

AR2 配置

```
1 bgp 100
2   ipv6-family unicast
3     peer 2002:100:1:1::7 next-hop-local
```

AR4和AR5配置

```
1 bgp 200
2   ipv6-family unicast
3     peer 2002:200:1:1::9 next-hop-local
```

### 3. 检查 ipv6 RR 配置

- R9 - R4, R5 --- 没有指定

```
1 bgp 200
2   ipv6-family unicast
3     peer 2002:200:1:1::4 enable
4     peer 2002:200:1:1::4 reflect-client
5     peer 2002:200:1:1::5 enable
6     peer 2002:200:1:1::5 reflect-client
```

- R7 - R2 配不配置无所谓，因为 E - I
- 此时 R5 有两个下一跳了，一个是 R2，一个是 R4

- 
- 选路问题

## R2 配置

```
1 ipv6-family unicast
2   peer 2002:100:1:1::7 enable
3   peer 2002:100:1:1::7 next-hop-local
4   peer 2002:200:100:24::4 enable
5   peer 2002:200:100:24::4 route-policy LP import
6   peer 2002:200:100:24::4 route-policy LP export
7   peer 2002:200:100:25::5 enable
8   peer 2002:200:100:25::5 route-policy AS-Path import
```

先看对于 R4 的 LP 策略

明显错误，只能 import 方向有效

```
1 undo peer 2002:200:100:24::4 route-policy LP export
```

不放心，在查看以下 LP，没问题，是改大 LP

```
1 disp route-policy LP
2 Route-policy : LP
3   permit : 1 (matched counts: 0)
4     Apply clauses :
5       apply local-preference 200
```

看对于 R5 的 AS-Path 策略

明显错误，只能 export 方向有效

```
1 undo peer 2002:200:100:25::5 route-policy AS-Path import
2 peer 2002:200:100:25::5 route-policy AS-Path export
```

不放心，在查看以下 AS-Path，怎么添加 AS 号有 200？那么对面 R5 拿到了不就拒收了吗？

```
1 disp route-policy AS-Path
2 Route-policy : AS-Path
3   permit : 1 (matched counts: 0)
4     Apply clauses :
5       apply as-path 200 200 additive
```

```
1 route-policy AS-Path permit node 1
2   apply as-path 100 100 additive
```

## 查看 bgp ipv6 路由表

R2 查看 --- 发现 R4、R5、R9 走的都是 2-4

```
1 [AR2]disp bgp ipv6 routing-table
2   BGP Local router ID is 100.1.1.2
3   Status codes: * - valid, > - best, d - damped,
4           h - history, i - internal, s - suppressed, S - Stale
5           Origin : i - IGP, e - EGP, ? - incomplete
6
7   Total Number of Routes: 8
8   *> Network    : 2002:100:2:1::1          PrefixLen : 128
9     NextHop    : ::                         LocPrf    :
10
11    MED        : 0                          PrefVal   : 0
12
13    Label      :
14    Path/Ogn  : i
15    *>i Network  : 2002:100:7:1::1          PrefixLen : 128
16    NextHop    : 2002:100:1:1::7          LocPrf    : 100
17
18    MED        : 0                          PrefVal   : 0
19
20    Label      :
21    Path/Ogn  : i
22    *> Network  : 2002:200:4:1::1          PrefixLen : 128
23    ### 此处
24    NextHop    : 2002:200:100:24::4          LocPrf    : 200
25
26    MED        : 0                          PrefVal   : 0
27
28    Label      :
29    Path/Ogn  : 200  i
30    *>
31    NextHop    : 2002:200:100:25::5          LocPrf    :
32
33    MED        : 0                          PrefVal   : 0
34
35    Label      :
36    Path/Ogn  : 200  i
37    *> Network  : 2002:200:5:1::1          PrefixLen : 128
38    ### 此处
39    NextHop    : 2002:200:100:24::4          LocPrf    : 200
40
41    MED        : 0                          PrefVal   : 0
42
43    Label      :
44    Path/Ogn  : 200  i
45    *>
46    NextHop    : 2002:200:100:25::5          LocPrf    :
47
48    MED        : 0                          PrefVal   : 0
49
50    Label      :
51    Path/Ogn  : 200  i
52    *> Network  : 2002:200:9:1::1          PrefixLen : 128
53    ### 此处
```



```
33      Path/Ogn : i
```

R5 查看 --- 发现都是走的 R4 --- 那就没问题了

```
1  <AR5>disp bgp ipv6 routing-table
2
3  BGP Local router ID is 200.1.1.5
4  Status codes: * - valid, > - best, d - damped,
5          h - history, i - internal, s - suppressed, S - Stale
6          Origin : i - IGP, e - EGP, ? - incomplete
7
8
9  Total Number of Routes: 7
10 *->i Network  : 2002:100:2:1::1                  PrefixLen : 128
11     ### 此处
12     NextHop   : 2002:200:1:1::4                  LocPrf    : 100
13
14     MED       : 0                                PrefVal   : 0
15
16     Label     :
17     Path/Ogn : 100 i
18     *
19     NextHop   : 2002:200:100:25::2              LocPrf    :
20
21     MED       : 0                                PrefVal   : 0
22
23     Label     :
24     Path/Ogn : 100 100 100 i
25     *
26     NextHop   : 2002:200:100:25::2              LocPrf    :
27
28     MED       : 0                                PrefVal   : 0
29
30     Label     :
31     Path/Ogn : 100 100 100 i
32     *->i Network : 2002:200:4:1::1              PrefixLen : 128
33     NextHop   : 2002:200:1:1::4                  LocPrf    : 100
34
35     MED       : 0                                PrefVal   : 0
36
37     Label     :
38     Path/Ogn : i
39     *->i Network : 2002:200:5:1::1              PrefixLen : 128
40     NextHop   : ::                               LocPrf    :
```

```

41      NextHop : 2002:200:1:1::9          LocPrf : 100
42      MED     : 0                      PrefVal : 0
43      Label   :
44      Path/Ogn : i

```

## 验证

R5 --- R7, 走的是 4 - 2 - 7 没毛病

```

1 <AR5>tracert ipv6 -a 2002:200:5:1::1 2002:100:7:1::1
2
3 1 2002:200:1:45::4 20 ms 20 ms 30 ms
4 2 2002:200:100:24::2 30 ms 30 ms 20 ms
5 3 2002:100:7:1::1 40 ms 30 ms 30 ms

```

回来呢？也是 2 - 4 - 5

```

1 <AR7>tracert ipv6 -a 2002:100:7:1::1 2002:200:5:1::1
2
3 1 2002:100:1:27::2 20 ms 20 ms 20 ms
4 2 2002:200:100:24::4 30 ms 30 ms 20 ms
5 3 2002:200:5:1::1 20 ms 20 ms 40 ms

```

R9 --- R7 都没问题

```

1 <AR9>tracert ipv6 -a 2002:200:9:1::1 2002:100:7:1::1
2
3 1 2002:200:1:49::4 10 ms 20 ms 10 ms
4 2 2002:200:100:24::2 30 ms 20 ms 30 ms
5 3 2002:100:7:1::1 40 ms 30 ms 30 ms

```

R7 --- R9

```

1 <AR7>tracert ipv6 -a 2002:100:7:1::1 2002:200:9:1::1
2
3 1 2002:100:1:27::2 20 ms 30 ms 20 ms
4 2 2002:200:100:24::4 20 ms 20 ms 20 ms
5 3 2002:200:9:1::1 30 ms 20 ms 20 ms

```

现在把 R2 --- R4 之间的 pos5/0/0 shutdown 看下

R2

```

1 bgp 100
2   ebgp-interface-sensitive # 立刻感知到接口的状态变化，从而对等体关系重建，可能跟 pos 链路有
  关，10s 一次
3   interface Pos5/0/0
4     shutdown

```

验证下是不是 pos 链路 10s 轮询时间间隔

**应用场景** --- 文档说明

轮询时间间隔指的是接口发送keepalive报文的周期。

keepalive报文用于链路状态监测维护，接口如果在5个keepalive周期之后仍然无法收到对端的keepalive报文，它就会认为链路发生故障。

说明默认就是  $10 * 5 = 50$ ，就相当于是 ebgp 32s 自动重建了

我按照文档把轮询间隔改为 1s，这样就是 5s 就可以感知到会话 down 了

R2、R4

```
1 int pos5/0/0
2 timer hold 1
```

R2

```
1 int pos5/0/0
2 shutdown
```

发现就在 5s 内 ppp 链路 down 掉，ebgp down 了

---

R5 --- R7，走的是 2 - 7 没毛病

```
1 <AR5>tracert ipv6 -a 2002:200:5:1::1 2002:100:7:1::1
2
3 1 2002:200:100:25::2 30 ms 20 ms 20 ms
4 2 2002:100:7:1::1 20 ms 20 ms 30 ms
```

回来呢？走 2 - 5

```
1 <AR7>tracert ipv6 -a 2002:100:7:1::1 2002:200:5:1::1
2
3 1 2002:100:1:27::2 20 ms 10 ms 10 ms
4 2 2002:200:5:1::1 30 ms 30 ms 20 ms
```

## 16、NAT

Site5中通过安全接入AS,client11现在无法通过网关AR27访问到公网AS100、AS200；  
解决此问题已满足以下表项-----考场具体看图，判断是PAT还是Easy-ip，我不贴了

### 解决方案

#### 1. PPP CHAP 认证

R9 配置

```
1 interface Serial3/0/0
2   ppp authentication-mode chap
3   aaa
4     local-user hcie password cipher hcie
5     local-user hcie service-type ppp
```

R27 配置

```
1 interface Serial3/0/0
2   ppp chap user hcie
3   ppp chap password cipher hcie
```

```
ping R9
```

```
1 [AR27]ping 200.1.209.9
2     PING 200.1.209.9: 56 data bytes, press CTRL_C to break
3     Reply from 200.1.209.9: bytes=56 Sequence=1 ttl=255 time=10 ms
4     Reply from 200.1.209.9: bytes=56 Sequence=2 ttl=255 time=20 ms
5     Reply from 200.1.209.9: bytes=56 Sequence=3 ttl=255 time=30 ms
6     Reply from 200.1.209.9: bytes=56 Sequence=4 ttl=255 time=20 ms
7     Reply from 200.1.209.9: bytes=56 Sequence=5 ttl=255 time=20 ms
```

## 2. NAT 问题

考场具体看图，判断是PAT还是Easy-ip

- PAT 是有地址池的
- Easy-ip 直接使用物理口，pppoe 的话是使用这种

PAT 配置 --- R27

### 1. 先写一个 acl

```
1 acl 2000
2     rule 1 permit
```

### 2. 地址池

```
1 nat address-group 1 200.1.209.1 200.1.209.5
```

### 3. 接口出向调用

```
1 interface Serial3/0/0
2     nat outbound 2000 address-group 1
```

### 4. 默认路由没有配置 --- 考场会给你配好

```
1 ip route-static 0.0.0.0 0.0.0.0 Serial3/0/0
2                                     # 这里直接配置出接口 ok 不?
3                                     # ppp 链路是 ok 的, 因为只有两端
4                                     # MA 只写出接口没有, 因为对端设备很多, 你不知道发给谁
5                                     # 而且你怎么进行数据封装呢? 没有具体下一跳, 无法完成
6     arp
```

验证 1:

```
1 PC>ping 200.1.1.9
2     Ping 200.1.1.9: 32 data bytes, Press Ctrl_C to break
3     From 200.1.1.9: bytes=32 seq=1 ttl=254 time=31 ms
4     From 200.1.1.9: bytes=32 seq=2 ttl=254 time=32 ms
5     From 200.1.1.9: bytes=32 seq=3 ttl=254 time=15 ms
6     From 200.1.1.9: bytes=32 seq=4 ttl=254 time=16 ms
7     From 200.1.1.9: bytes=32 seq=5 ttl=254 time=31 ms
```

```
[AR27]disp nat outbound
NAT Outbound Information:
-----
Interface          Acl      Address-group/IP/Interface      Type
-----
Serial3/0/0        2000
-----
Total : 1
```

### Easy-ip 配置 --- R27

- 先写一个 acl

```
1 acl 2000
2 rule 1 permit
```

- 接口出向调用

```
1 interface Serial3/0/0
2 nat outbound 2000
```

```
[AR27]disp nat outbound
NAT Outbound Information:
-----
Interface          Acl      Address-group/IP/Interface      Type
-----
Serial3/0/0        2000      200.1.209.27            easyip
-----
```

注意：

但是 pc 访问 AS200, AS100 都是不通的

```
1 PC>ping 200.1.1.23
2 PC>ping 100.1.1.2
```

可以在 AS100 R2 设备上查看有没有 nat 转换过去的路由 **200.1.209.0/24**，并没有

```
1 [AR2]disp ip rou 200.1.209.0
2 [AR2]
```

要想有，所以需要 R9 把 **ser3/0/0** 宣告进 isis 200 中

```
1 interface Serial3/0/0
2 isis enable 200
```

R2 查看有没有路由 --- 发现有了

```
1 [AR2]disp ip rou 200.1.209.0
2 Route Flags: R - relay, D - download to fib
3 -----
4 Routing Table : Public
5 Summary Count : 1
6 Destination/Mask   Proto   Pre   Cost       Flags NextHop      Interface
7     200.1.209.0/24 EBGP    255   20           D  200.100.24.4  Pos5/0/0
```

现在 pc 在 ping 一下看看

```
1 PC>ping 200.1.1.23
```

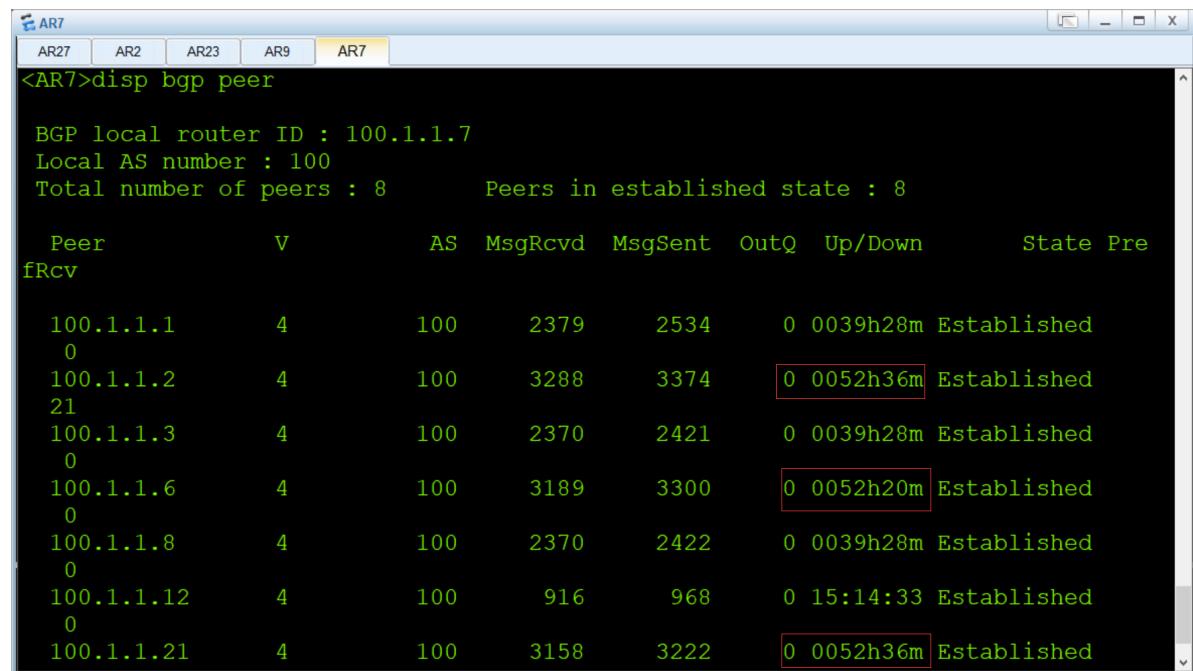
```

2
3 Ping 200.1.1.23: 32 data bytes, Press Ctrl_C to break
4 From 200.1.1.23: bytes=32 seq=1 ttl=253 time=47 ms
5 From 200.1.1.23: bytes=32 seq=2 ttl=253 time=15 ms
6 From 200.1.1.23: bytes=32 seq=3 ttl=253 time=32 ms
7 From 200.1.1.23: bytes=32 seq=4 ttl=253 time=31 ms
8 From 200.1.1.23: bytes=32 seq=5 ttl=253 time=15 ms
9
10 PC>ping 100.1.1.2
11
12 Ping 100.1.1.2: 32 data bytes, Press Ctrl_C to break
13 From 100.1.1.2: bytes=32 seq=1 ttl=252 time=15 ms
14 From 100.1.1.2: bytes=32 seq=2 ttl=252 time=16 ms
15 From 100.1.1.2: bytes=32 seq=3 ttl=252 time=31 ms
16 From 100.1.1.2: bytes=32 seq=4 ttl=252 time=47 ms
17 From 100.1.1.2: bytes=32 seq=5 ttl=252 time=31 ms

```

## final、TS2.0 完结

历经 3 天，终于把这 16 道需求排完了。我将奔赴于 TS3.0 --- 2021 年 10 月 20 日下午 4 点



The screenshot shows a terminal window titled 'AR7' with tabs for AR27, AR2, AR23, AR9, and AR7. The AR7 tab is active. The command entered is <AR7>disp bgp peer. The output displays the following information:

```

BGP local router ID : 100.1.1.7
Local AS number : 100
Total number of peers : 8      Peers in established state : 8

Peer          V     AS  MsgRcvd  MsgSent  OutQ Up/Down      State Pre
fRcv

100.1.1.1    4     100   2379    2534    0 0039h28m Established
0
100.1.1.2    4     100   3288    3374    0 0052h36m Established
21
100.1.1.3    4     100   2370    2421    0 0039h28m Established
0
100.1.1.6    4     100   3189    3300    0 0052h20m Established
0
100.1.1.8    4     100   2370    2422    0 0039h28m Established
0
100.1.1.12   4     100   916     968     0 15:14:33 Established
0
100.1.1.21   4     100   3158    3222    0 0052h36m Established

```