**Trouble Shooting Layer2**

【题目】

User r101 should successfully traceroute server r100 behind sw3, 3 hops

并附有一张trace的截图



【错误点】

1. sw2的e1/0安全绑定的mac地址错误
2. sw2的e1/0划分错了vlan，应该划分进vlan100
3. sw2的e1/0的trunk允许的vlan中没有vlan12
4. sw2的int vlan 100的ip地址配错了
5. r7、r8的dhcp pool中关于pc101和server的client-id配错了
6. r7、r8的ip host域名映射错误

【详解与思路】

在sw2上

sh cdp neigh #发现没有e1/0

sh int status #发现e1/0是err-disable状态，同时vlan是10，找到错点1和2

sh run int e1/0 #发现配了port-security，怀疑mac地址绑定错了

在101上

sh int ee0/0 #找到101的mac地址，括号外面的，发现sw2的e1/0上mac绑定错了

#记录下该mac地址xxxx.xxxx.xxxx

在sw2上

int e1/0

switchport port-security mac-address xxxx.xxxx.xxxx #注意先no掉原来的配置

shutdown

no shutdown

sh int status #看到e1/0的状态变成了connected，排掉错点1

#vlan还是10，错点2尚未排掉

int e1/0

sw acc vl 100 #按照拓扑图修改

sh int trunk #再检查trunk，发现e0/0的vlan12被挖掉了，找到错点3

sh spanning-tree mst 1 #发现只有e0/0是转发状态，其他端口都是block，因此必须补上vl12

int e0/0

switchport trunk allowed vlan add 12 #注意是vlan add 12，排掉错点3

在sw2上

sh int vl 100 #发现ip为172.16.100.10，而图上是.1，找到错点4

int vl 100

ip address 172.16.100.1 255.255.255.0

在101上

ping 172.7.7.7 source vl 100 #测试101的dhcp请求是否能够送达r7和r8

ping 172.8.8.8 source vl 100 #即101所在的网段是否ping通r7、r8的lo0

#通的，说明路由ok

sh int e0/0 #发现地址是.2，和图上的.200不符，错误，找错误原因

sh dhcp lease #查看是从哪台dhcp server获取的地址

在r7上

sh run | se dhcp #看dhcp配置，找到ip dhcp pool PC101

#发现pc101的dhcp配的是.200，说明ip正确

#发现client-id配的是01aa.bbcc.0056.00

#而101的mac是aabb.cc00.6e00，找到错点5

修改方法：

sh run | se dhcp #复制出ip dhcp pool PC101的配置

no ip dhcp pool PC101 #no掉错误的ip dhcp pool PC101

ip dhcp pool PC101 #修改原错误的client-id，刷入正确的ip dhcp pool PC101配置

… #log提示’ a binding for this cient already exists’

sh ip dhcp binding #发现006e已经绑定到了.2

clear ip dhcp binding \* #清掉dhcp绑定再重新刷入ip dhcp pool PC101

sh ip dhcp binding #检查，发现绑定到了.200，排掉错点5

【小结】比较好的修改顺序是

1. sh run | se dhcp #查dhcp pool，找到错点
2. no ip dhcp pool PC101 #删掉错误的PC101的dhcp配置
3. clear ip dhcp binding \* #先清dhcp绑定
4. (config) ip dhcp pool PC101 #再配置正确的dhcp绑定

r8上有dhcp有同样的问题，修改方法同r7

在101上

int e0/0

shutdown #修改完r7、r8的dhcp pool后检查

no shutdown #重新拿dhcp地址，拿到.200，确认排掉错点5

sh ip int br #也可以看到e0/0拿到了.200，再次确认

server r100上也有地址配错的问题，配的是.2，修改方法同pc101

在101上

traceroute 172.16.200.200 #从101 trace server，发现第三行的域名是SERVER1

#而截图是server1，找到错点6

sh ip dns view default #发现dns server的配置是172.7.7.7,172.8.8.8

#写在前面的会被优先使用

在r7上

sh run | se ip host #查看host配置，发现其配置为

#ip host SERVER1.bancobank.org 172.16.200.200

(config) no ip host SERVER1.bancobank.org 172.16.200.200 #删掉错误配置

(config) ip host server1.bancobank.org 172.16.200.200 #重新刷入host配置，排掉错点6

在101上

traceroute 172.16.200.200 #检查，看到截图效果