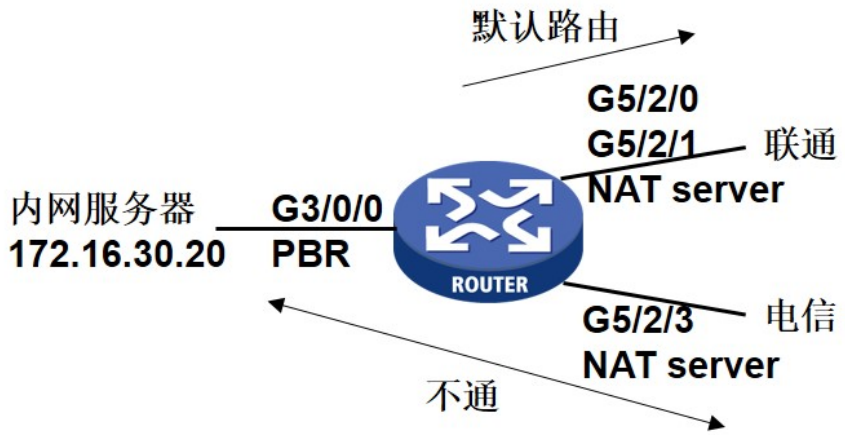
某局点SR6608（V5）双公网出口做nat server来回路径不一致导致不通经验案例

策略路由 郭昊 2018-03-18 发表



设备有两个公网出口Route-agg 1（物理口G5/2/0、G5/2/1）和G5/2/3，分别连接联通和电信公网，**默认路由指向联通接口**。两个公网口都做nat server，映射到内网服务器172.16.30.20。问题现象是联通外网用户经过联通出口访问服务器可以通，电信公网用户经过设备电信公网口访问服务器不通。在SR66上配置指向电信外网用户的明细路由后，电信外网用户访问服务器也可以通。去掉明细路由后，在设备内网口G3/0/0配置了PBR，匹配反向入接口，电信的用户还是无法访问服务器。

联通外网用户可以通过设备访问内网服务器，说明设备联通公网口的NAT server功能正常，设备与内网服务器通信正常。设备上配置了到达电信公网用户的明细路由后，用户与内网服务器可以互通，说明设备电信公网口的NAT server功能正常。而设备取消到达电信用户的明细路由后，用户与内网服务器不通，可以比较明显看出，**问题原因在于设备到电信外网用户的路由**。
明确了现场的需求，即默认路由指向联通公网、无法对电信用户——写明细路由的情况下，需要将服务器回应电信用户的发到电信用户，实现来回路径一致。V5的SR66是没有nat inbound功能的，因此无法通过在公网口做nat inbound的方式实现来回路径一致，只能从路由方面想办法。而V5的SR66也有在该应用场景下实现来回路径一致的功能，即在功内网口做PBR，if-match reverse-input-interface，使内网服务器流量到达设备内网口时，能够通过反向匹配入接口，决定下一跳地址是指向联通公网还是电信公网。
可是我们按照上面所说的方法，在内网接口做了PBR后，电信用户与服务器还是不通。检查配置，PBR配得是没问题的，

```
interface Route-Aggregation1  //联通出口
ip address 1.1.1.1 255.255.255.224
……
nat server protocol tcp global 1.1.1.2 443 inside 172.16.30.20 443

interface GigabitEthernet5/2/3  //电信出口
ip address 2.2.2.1 255.255.255.248
……
nat server protocol tcp global 2.2.2.2 443 inside 172.16.30.20 443

interface GigabitEthernet3/0/0  //内网口
port link-mode route
description test for openvpn
ip address 172.16.30.17 255.255.255.248
ip netstream inbound
ip netstream outbound
natpt enable
ip policy-based-route test
#
policy-based-route test permit node 10
  if-match reverse-input-interface Route-Aggregation1
apply ip-address next-hop 1.1.1.3//联通公网
policy-based-route test permit node 30
```

if-match reverse-input-interface GigabitEthernet5/2/3
apply ip-address next-hop 2.2.2.3//电信公网
#

查看相关配置手册及案例，我们发现现场与案例中唯一不同之处在于，**内外网接口不在同一块FIP板上**，怀疑是流量跨板导致了PBR匹配或处理的异常。之后我们debug ip policy-based-route，发现电信用户访问服务器时没有任何信息打印，而正常情况下流量匹配到PBR进行相应转发时会有类似下面的debug信息打印，
*Jul 15 08:57:44:633 2017 SR6608 DPPBR/7/POLICY-ROUTING: -Slot=3; **IP policy based routing success** : next-hop : 20.0.0.2
在实验室中进行相关测试，发现内外网接口不在同一块板卡时，匹配reverse-input-interface的PBR确实无法被匹配到，而内外网接口在同一块板卡时该功能正常。经研发帮忙确认，这是因为流量从公网口到达设备时所携带的入接口索引在流量跨板后存在变化，内网口反向匹配入接口的PBR无法匹配该入接口索引值，导致PBR不生效。

将内网接口G3/0/0挪到公网接口所在的slot 5，并在新的内网口做PBR，匹配reverse-input-interface，使流量来回路径一致。

PBR匹配反向入接口的功能相对来说应用较少，因此大家平时不易注意到存在跨板的限制。但在此问题中，一旦将问题锁定在PBR环节，通过将现场配置与配置手册、案例进行对比，不难发现跨板这一怀疑点，之后只要进行相关的实验室复现及确认即可。