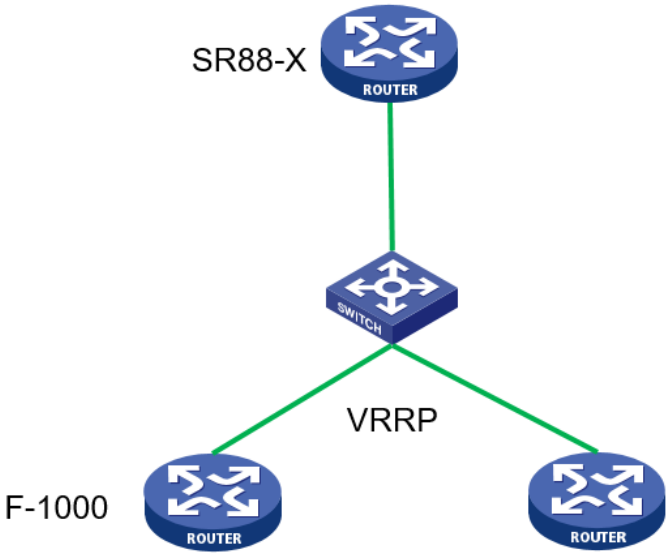
SR88-X路由器因为对端设备配置NAT导致BGP邻居无法建立问题

BGP NAT 何理 2016-04-19 发表



如上图所示，SR88-X路由器为PE设备，下联两个F-1000防火墙作为CE设备，PE与CE之间使用EBGP交换路由；F-1000使用VRRP虚地址与SR88-X建立EBGP邻居；

原本SR88-X与F-1000的EBGP邻居建立正常，业务运行正常；但是有一天SR88-X路由器因为版本升级重启，重启设备后发现EBGP邻居无法建立一直停留在Connect状态，TCP链接无法建立；

查看SR88-X设备上的TCP信息发现：
172.26.20.57:22262 172.26.20.60:179 SYN_SENT 1 0 0 0x000000000000410f
发现SR88-X侧对应的tcp状态一直处于SYN_SENT状态，说明SR88-X侧已经发送了SYN消息但是对端F-1000侧未进行回应导致；

查看F-1000侧信息，发现本端的179端口号一直处于监听状态；
0182ac00 0.0.0.0:179 172.26.20.57:0 Listening

由此可以看到F-1000收到了报文但是没有进行处理；此时将SR88-X侧EBGP邻居地址修改为VRRP接口实地址，EBGP邻居正常建立；所以双方的EBGP邻居建立没有异常，那么VRRP虚地址有什么问题呢？我们查看下F1000接口配置：

```
interface Vlan-interface500
 nat server protocol any global 172.26.20.60 inside 172.26.10.7
 nat server protocol tcp global 172.26.20.60 9222 inside 172.26.10.92 22
 nat server protocol tcp global 172.26.20.60 9280 inside 172.26.10.92 8080
 nat server protocol tcp global 172.26.20.60 13122 inside 172.26.10.131 22
 nat server protocol tcp global 172.26.20.60 13180 inside 172.26.10.131 8080
 nat server protocol tcp global 172.26.20.60 13222 inside 172.26.10.132 22
 nat server protocol tcp global 172.26.20.60 13280 inside 172.26.10.132 8080
 nat server protocol tcp global 172.26.20.60 13322 inside 172.26.10.133 22
 nat server protocol tcp global 172.26.20.60 13380 inside 172.26.10.133 8080
 nat server protocol tcp global 172.26.20.60 13422 inside 172.26.10.134 22
 nat server protocol tcp global 172.26.20.60 13480 inside 172.26.10.134 8080
 nat server protocol tcp global 172.26.20.60 13522 inside 172.26.10.135 22
 nat server protocol tcp global 172.26.20.60 13580 inside 172.26.10.135 8080
 nat server protocol tcp global 172.26.20.60 19322 inside 172.26.10.193 22
 nat server protocol tcp global 172.26.20.60 19380 inside 172.26.10.193 8080
```

ip address 172.26.20.58 255.255.255.248
vrrp vrid 50 virtual-ip 172.26.20.60
vrrp vrid 50 priority 125

通过查看VLAN 500接口配置，发现接口配置了一条nat server protocol any global 172.26.20.60 inside 172.26.10.7命令，该配置将所有的端口都进行了映射，也包括BGP使用的179端口号；

咨询现场人员该配置的作用，答复之前做测试使用，但是没删除；因为之前配置的时候BGP邻居已经建立，所以不会影响BGP邻居状态；但是如果BGP邻居重新建立，此时便会导致上述问题；

将该测试NAT server配置删除后，EBGP邻居正常建立；

删除接口下测试NAT server 配置；