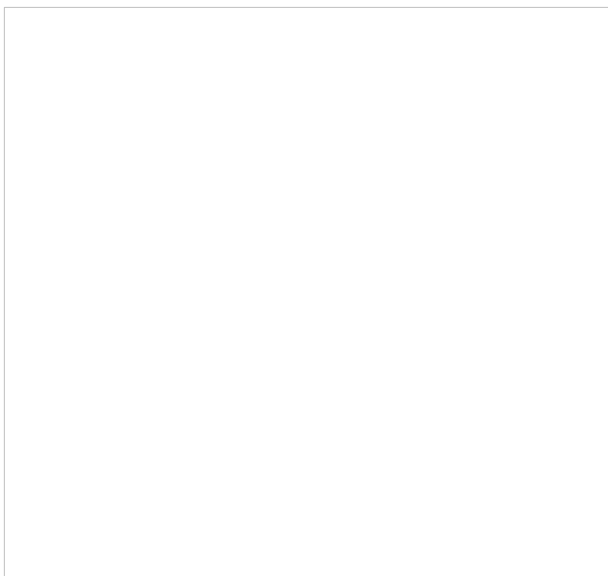


知 MSR做NAT SERVER映射有时生效有时不生效的经验案例

杨勇1 2013-02-21 发表

MSR做NAT SERVER映射有时生效有时不生效的经验案例

一、 组网：



拓扑描述：MSR双出口连接上行31交换机（交换机是hub充当广电转换器）网通和电信各100M，下行G0/1口（服务器网关）连接服务器区交换机。

二、 问题描述：

1. XX市政府使用msr路由器做nat映射后不定时的部分nat应用无法使用。
2. 有时接口地址也无法ping通，能学到对端运营商的arp但是不能通讯（此时有的nat还是可以正常使用的只是接口地址不能访问接口shutdown 然后undo shutdown 就好了），过一会又自动恢复了。

三、 过程分析：

- 1、一线工程师最初怀疑是双出口来回路径不一致的问题作了策略路由故障依然。
- 2、将路由器升级至23XX的版本后观察故障还是存在，和版本无关。
- 3、怀疑arp学习问题，在接口将服务器映射后的公网地址在接口配置成sub地址，并开启免费arp故障还是存在。

四、 解决方法：

从反馈的现象看，怀疑和运营商分配的那3个公网地址的转发有关，当配置成sub地址后，理论上只要运营商把这3个地址的路由分配到这条线路上，那么就可以ping通的，如果ping不通应该是数据包没到路由器上，所以相应的nat映射服务也无法使用，所以为了判断这种情况，可以写个acl，然后在访问不了的时候在路由器进行debug ip packet acl 3500，看运营商是否将报文送到我们路由器上，例如：

```
acl number 3500
```

```
rule 0 permit tcp destination 221.209.11.106 0 destination-port eq www
```

```
rule 5 permit tcp destination 221.209.11.80 0 destination-port eq www
```

```
rule 10 permit tcp destination 221.209.11.110 0 destination-port eq www
```

用这种方法测试，发现在故障复现时，路由器上并没有相应的debug报文，和用户沟通后，让当地运营商排查线路后，问题解决。