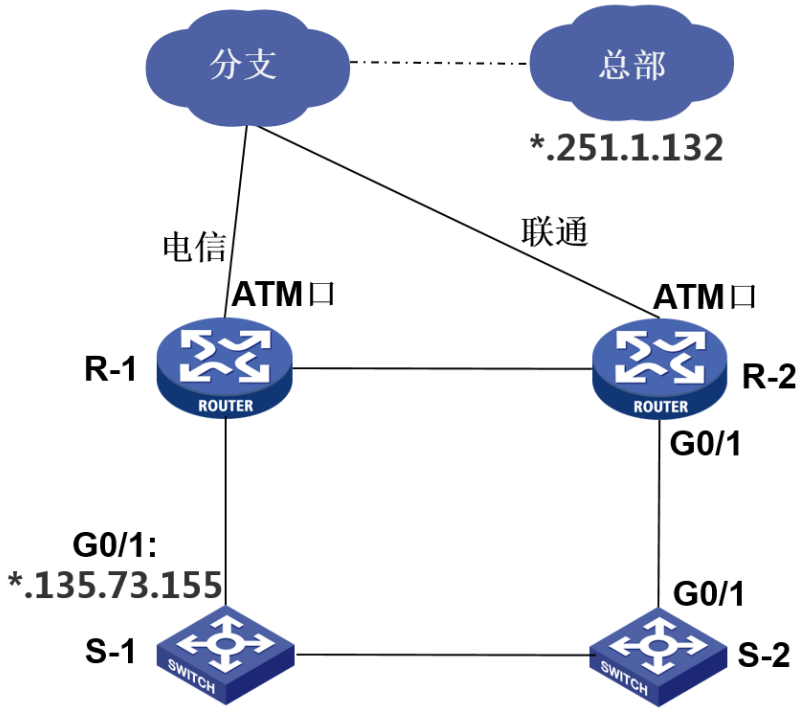
某局点SR6602 路由器丢包问题排查案例

安全域 ASPF 徐猛 2018-06-04 发表

组网及说明

现场组网情况如下图：



问题描述

某局点公司的分支下联终端用户访问总部服务器IP访问不到，跟踪路径已经过了路由器R-1/2，且路径跟踪到了总部服务器前的某个防火墙处。但是其他分支是可以正常访问的，各个分支配置基本一样，总部放行的配置为大段地址，不会有控制某个分支具体访问行为。 注：路由器R设备为SR6602；交换机S设备为我司的S5800：总部地址段为*.251.0.0的地址段（为避免纠纷，本案例中*标识符为同一段地址数值。）

现场做了如下变更测试后发现杭州分支下终端能够正常访问总部服务器了： 在分支下联终端访问不到总部服务器的时候，S-1设备上指了一条静态路由指到了R-2上面（正常是走R1的）后发现杭州分支下终端能够正常访问总部服务器了，现场业务暂时使用用该规避方式进行使用，报文路径为S-1———>S-2———>R-2———>R-1———>电信———>总部。现场工程师需要排查出什么原因导致这种现象，并希望路径改回S-1———>R-1———>电信———>总部后也能正常访问。

过程分析

引导现场工程师进行故障复现，即路径改为为：S-1———>R-1———>电信———>总部，然后引导工程师进行问题定位排查：

1.现场工程师使用分支下联的S-1设备的源地址去ping测试总部的服务器地址，无法ping通，于是使用tracert路径跟踪，发现最多只能跟踪到总部服务器前的某个防火墙上，初始怀疑防火墙域间策略或者路由存在问题。后来排查了域间策略和路由信息，发现域间策略已放通，路由信息也有。让现场进行ping测试后，在防火墙上查看会话和debug信息，发现会话信息正常，debug报文显示发包正常。

2.在出口的两台分别连接电信和联通的出口路由器上开启debug ip packet后，使用S-1设备带源地址*.135.73.155去ping总部服务器地址*.251.1.132 测试，开启ping -a *.135.73.155 *.251.1.132后，收集相应debug信息并分析：
发现如下结果：
R-1设备上能够看到从下联S-1的G0/1接口收到了报文并从上联电信的ATM2/0.1接口发出，但是并未看到回包的debug信息。
但是在R-2设备上发现，总部服务器给的回包从联通接口回给了R-2设备，如下debug信息中可以看到有来自总部地址*.251.1.132给我们进行ping测试的源地址*.135.73.155的报文回包，回包来自联通接口ATM2/0.1，并从debug中可以看出，R-2设备将收到的回包由接口G0/1发出，该接口为与S-2设备相连的接口，按理该接口地址与目的地址地址路由可达，应该是能通的：

*Jan 31 16:29:01:955 2018 R1352-R-2 DPIPFWD/7/debug_case:
Receiving, interface = Atm2/0.1, version = 4, headlen = 20, tos = 0,
pktlen = 84, pktid = 54307, offset = 0, ttl = 246, protocol = 1,
checksum = 63458, s = *.251.1.132, d = *.135.73.155
prompt: Receiving IP packet
*Jan 31 16:29:01:955 2018 R1352-R-2 DPIPFWD/7/debug_case:
Sending, interface = GigabitEthernet0/1, version = 4, headlen = 20, tos = 0,
pktlen = 84, pktid = 54307, offset = 0, ttl = 245, protocol = 1,
checksum = 63714, s = *.251.1.132, d = *.135.73.155
prompt: Sending the packet from Atm2/0.1

3.为了进一步确认丢包的位置，我们引导现场工程师在R-2设备下联的S-2设备的G1/0/1接口上做流量统计，然后发现流量统计入方向匹配的该流量计数为0，即未收到R-2设备发来的回包报文。

4.现场使用S-2直连ping设备R-2的接口，发现没有问题，排除链路质量问题。

5.暂时定位问题出在了R-2上，但不知道是什么原因导致的丢包。于是仔细检查了接口的配置情况，发现了在接口下应用了aspf策略，初始由于该配置中aspf策略未配置具体内容，且aspf为应用层包过滤，一般认为不会对icmp的报文进行拦截，所以没有注意：

```
#
interface GigabitEthernet0/1
 description Link-to-S1352-S-2-G1/0/1
 firewall packet-filter 3101 inbound
 firewall packet-filter 3102 outbound
 firewall aspf 1 inbound
 firewall aspf 1 outbound
 ip address *.135.73.146 255.255.255.240
 vrrp vrid 1 virtual-ip *.135.73.147
 vrrp vrid 1 preempt-mode timer delay 5
 vrrp vrid 2 virtual-ip *.135.73.148
 vrrp vrid 2 priority 200
 vrrp vrid 2 preempt-mode timer delay 5
 vrrp vrid 2 track 1 reduced 110
#
aspf-policy 1
#
```

发现该配置后，我们便对现场测试环境进行复现，并进行测试，测试的同时收集debug aspf packet 发现如下信息：

*Jan 31 08:59:26:232 2018 SR6602X-1 DPASPF/7/debug:
Thread 7, the outbound icmp packet on the interface GigabitEthernet0/0/1 is a status invalid packet, and is denied by ASPF: (1.1.1.1)->(2.2.2.2), 84 bytes.
*Jan 31 08:59:28:395 2018 SR6602X-1 DPASPF/7/debug:
Thread 7, the outbound icmp packet on the interface GigabitEthernet0/0/1 is a status invalid packet, and is denied by ASPF: (1.1.1.1)->(2.2.2.2), 84 bytes.
*Jan 31 08:59:30:595 2018 SR6602X-1 DPASPF/7/debug:
Thread 7, the outbound icmp packet on the interface GigabitEthernet0/0/0 is a status invalid packet, and is denied by ASPF: (1.1.1.1)->(2.2.2.2), 84 bytes.

发现该aspf命令的配置同样会对icmp的会话进行检查。由于分支下的报文去往总部服务器时，走的R-1设备，并未走R-2设备。所以，服务器给回包时，如果回到了R-2设备上，由于R-2设备没有该报文的初始会话，便会认为这是一个无效的数据包，并将报文阻断掉。
引导现场做相同的测试，并收集debug aspf packet信息后，发现了同样的调试记录信息，现场将该aspf的应用关闭后问题解决。

解决方法

关闭接口下的aspf应用

建议与总结：

1.aspf策略应用在接口上时，会对各种会话报文进行检查，如果接口上没有收到过请求包，而收到了响应报文，则会被aspf检查到并丢弃。

2.在复杂组网情况下，当出现不通情况时，需要先通过例如流量统计，debug，查看会话，ping测试以及路径跟踪测试等多种手段先将丢包设备是哪一台定位出来。然后在对特定设备的丢包原因进行定位分析。