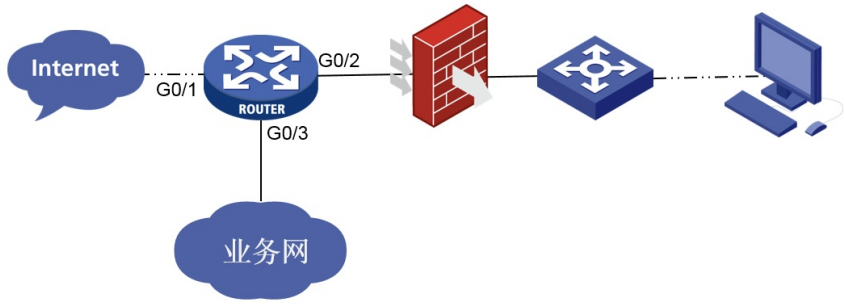
某局点MSR3620DP 部分网页无法访问排查经验案例

静态路由 Web页面 徐猛 2018-09-08 发表

组网及说明

现场一台MSR3620DP设备作为该局点公网网络出口设备，内网连接一台防火墙，防火墙下联交换机，终端直接连接在交换机上。网络拓扑如下：



问题描述

现场描述，之前都能正常访问外网，但是近期该局点用户反馈部分网站无法访问，收到现场的反馈的问题后，这边对该问题立即进行了分析。

过程分析

1. 对于现场描述，部分网站能访问，部分网站不能访问的情况，我们针对现场反馈较为强烈的无法访问的网站使用外部网络进行测试，排除网站本身异常的情况，我们使用了外网进行访问测试，发现外网访问该网站正常。

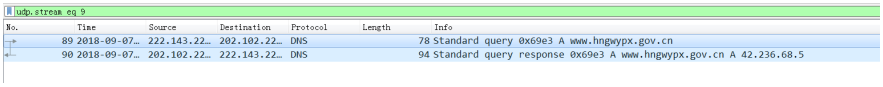
2.通过上述步骤排除了网站异常的原因，然后使用现场的内网电脑ping该网站域名进行测试，发现域名能够正常解析，排除域名解析问题。但是由于通常网站都是禁止ping的，所以ping结果不通也比较正常。

```
C:\Users\x15237>ping www.hngwypx.gov.cn

正在 Ping www.hngwypx.gov.cn [42.236.68.5] 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

42.236.68.5 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),
```

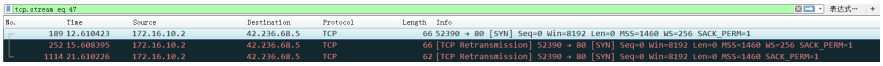
3.由于现场终端到我们MSR3620DP路由器经过了防火墙和交换机，所以为了排除内网其他设备因素，我们使用内网终端直接连接到出口设备MSR3620DP上进行外网访问测试。经过将终端直连路由器测试发现异常现象依旧，由于现场运营商线路为光纤接入，所以暂时无法用终端直连运营商进行测试排查运营商网络问题。于是后续我们在路由器上的内网口和公网出口分别进行了抓包，用于定位具体是设备问题，还是公网侧没回包的问题。

具体抓包情况分析如下：

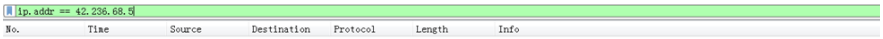
DNS解析报文正常，抓包情况如下，和最初测试结果一致：



在直连测试PC的内网口G0/2抓包情况如下，根据抓包可以发现，报文已经到了内网口并由于三次握手不成功，发生了三次报文重传。



但是在设备的公网出口G0/1侧进行抓包时，并未发现该流量的相关报文：



从该抓包测试结果，基本可以定位，问题出在了我们MSR3620DP路由器上。

4.由于最终问题定位到为我们路由器的问题，于是我们让现场收集了设备的完整诊断信息。

查看主要配置如下，其中1口为正常情况下，访问互联网的出接口，2口为连接内网测试终端的接口，3口为业务网络出口。

```
#
interface GigabitEthernet0/1
 description 互联网出口
 ip address *.143.22.194 255.255.255.248
 ip address *.143.22.195 255.255.255.248 sub
 ip address *.143.22.196 255.255.255.248 sub
 ip address *.143.22.197 255.255.255.248 sub
 ip address *.143.22.198 255.255.255.248 sub
 nat outbound 3000
 vlan-type dot1q vid 416
#
interface GigabitEthernet0/2
 port link-mode route
 description 业务区的防火墙1口
 combo enable fiber
 ip address 172.16.10.1 255.255.255.252
 packet-filter 3003 outbound
#
interface GigabitEthernet0/3
 description 业务网出口
 ip address *.133.255.2 255.255.255.252
 nat outbound 3002
 vlan-type dot1q vid 2416
#
 ip route-static 0.0.0.0 0 *.143.22.193
 ip route-static 16.0.0.0 4 *.133.255.1
 ip route-static 32.0.0.0 4 *.133.255.1
 ip route-static 48.0.0.0 8 *.133.255.1
……..
```

#

检查现场的路由表发现了几条掩码长度较短且下一跳指向3口作为出接口的路由条目，于是我们使用刚才网站访问异常的站点IP进行查看路由表测试：

```
display ip routing-table 42.236.68.5
Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/0          Static  60  0           222.143.22.193  GE0/1
32.0.0.0/4         Static  60  0           32.133.255.1    GE0/3
```

根据路由表查看出来的信息，我们可以发现，现场访问该测试的站点时，路由表应该是会优先匹配掩码更长的第二条路由，且第二条路由条目的下一跳出口是3口，且由于3口对应的是现场的业务网络，并不能访问互联网区域，所以会导致页面无法访问的情况。

后来我们用debug进行验证，发现数据报文却是是从3口发出，从而导致了报文被业务网络丢弃。

```
*Sep  7 11:50:06:880 2018 H3C IPFW/7/IPFW_PACKET:
Receiving, interface = GigabitEthernet0/2                  //2口直连测试PC，报文从2口进入设备
version = 4, headlen = 20, tos = 0
pktlen = 52, pktid = 17511, offset = 0, ttl = 128, protocol = 6
checksum = 37209, s = 172.16.10.2, d = 42.236.68.5
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Receiving IP packet from interface GigabitEthernet0/2.
Payload: TCP
  source port = 53692, destination port = 80
  sequence num = 0x2a3ede9f, acknowledgement num = 0x00000000, flags = 0x2
  window size = 8192, checksum = 0x4f22, header length = 32.


*Sep  7 11:50:06:880 2018 H3C IPFW/7/IPFW_PACKET:
Sending, interface = GigabitEthernet0/3                    //报文匹配路由后从3口发出
version = 4, headlen = 20, tos = 0
pktlen = 52, pktid = 17511, offset = 0, ttl = 127, protocol = 6
checksum = 37465, s = 172.16.10.2, d = 42.236.68.5
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Sending IP packet received from interface GigabitEthernet0/2 at interface
GigabitEthernet0/3.
Payload: TCP
  source port = 53692, destination port = 80
  sequence num = 0x2a3ede9f, acknowledgement num = 0x00000000, flags = 0x2
  window size = 8192, checksum = 0x4f22, header length = 32.
```

5.后来与现场进行确认，由于现场业务网段需要，前期有工作人员在设备上添加了几条默认路由，由于当时未进行互联网访问测试，所以现场工作人员并未联想该异常现象到与该添加的配置有关。

但是由于现场业务比较重要，业务区域的路由条目不能擅自进行更改。故后续让现场在内网接口处配置了策略路由，对于去往非业务网段的互联网访问需求，将报文全部匹配策略路由从1口出去。

解决方法

由于现场业务比较重要，业务区域的路由条目不能擅自进行更改。故后续让现场在内网接口处配置了策略路由，对于去往非业务网段的互联网访问需求，将报文全部匹配策略路由从1口出去。添加策略路由后问题解决，访问互联网网站正常。