某局点L1000-M登录不了163邮箱

其他 部署方式 NAT **肖倩艳** 2018-06-17 发表

组网及说明

无

问题描述

某局点客户反馈经过设备L1000-M NAT之后内网用户登录不了https://email.163.com（解析地址是123.125.50.22） 但是http://email.163.com可以正常使用且其他所有网站访问都正常。

过程分析

第一步

同一个终端直接配置运营商公网地址访问测试是可以打开https 163邮箱的

第二步

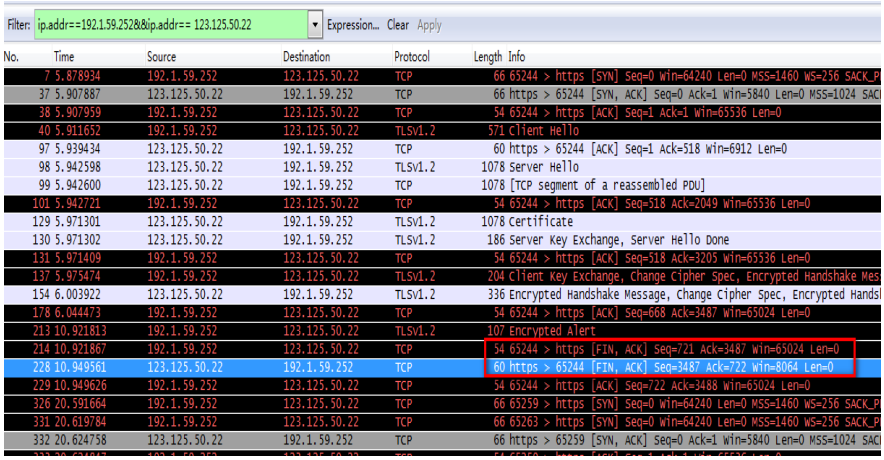
查看LB会话信息 可以看到客户端192.1.59.252 和服务器三次握手是可以建立的

```
  Source      IP/port:  123.125.50.22/443
  Destination IP/port:  218.10.148.122/25900
  DS-Lite tunnel peer:  -
  VPN instance/VLAN ID/Inline ID:  -/-/-
  Protocol:  TCP(6)
  Inbound interface:  GigabitEthernet1/0/16
State:  TCP_ESTABLISHED
Application:  HTTPS
Start time:  2018-04-10 15:14:47  TTL:  596s
Initiator->Responder:            4 packets        793 bytes
Responder->Initiator:            4 packets        348 bytes

Initiator:
  Source      IP/port:  192.1.59.252/65297
  Destination IP/port:  123.125.50.22/443
  DS-Lite tunnel peer:  -
  VPN instance/VLAN ID/Inline ID:  -/-/-
  Protocol:  TCP(6)
  Inbound interface:  Route-Aggregation10
Responder:
  Source      IP/port:  123.125.50.22/443
  Destination IP/port:  218.10.148.122/25904
  DS-Lite tunnel peer:  -
  VPN instance/VLAN ID/Inline ID:  -/-/-
  Protocol:  TCP(6)
  Inbound interface:  GigabitEthernet1/0/16
State:  TCP_ESTABLISHED
Application:  HTTPS
Start time:  2018-04-10 15:14:47  TTL:  595s
Initiator->Responder:            4 packets        793 bytes
Responder->Initiator:            4 packets        348 bytes

Total sessions found:  2
<LB>
<LB>
<LB>
<LB>display session table ipv4 destination-ip 123.125.50.22 verbose
Slot 1:
Total sessions found:  0
<LB>
```

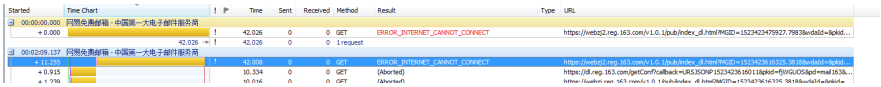
第三步 终端抓包分析

Wireshark抓包只发现终端主动发送了断开三次握手报文，没有具体原因，考虑现场是访问https的，建议使用HttpWatch抓包。

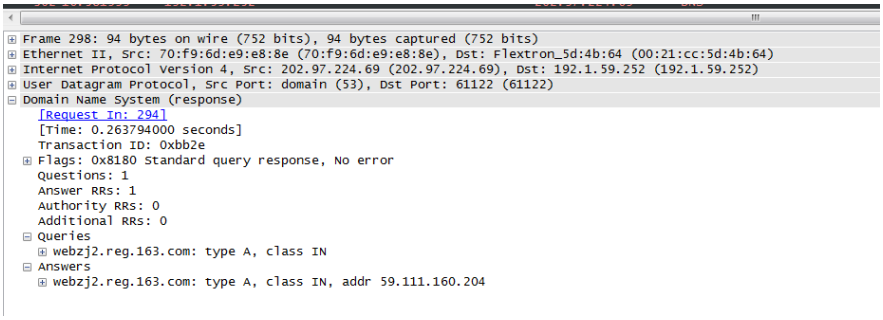
Wireshark抓包



HttpWatch抓包

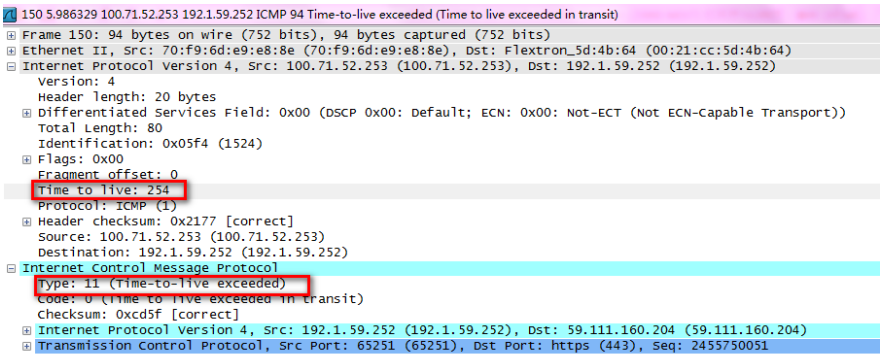


通过上述抓包可以判断出业务异常是因为访问webzj2.reg.163.com时出现异常的，再次分析PC的抓包文件，这个域名解析出地址是59.111.160.204



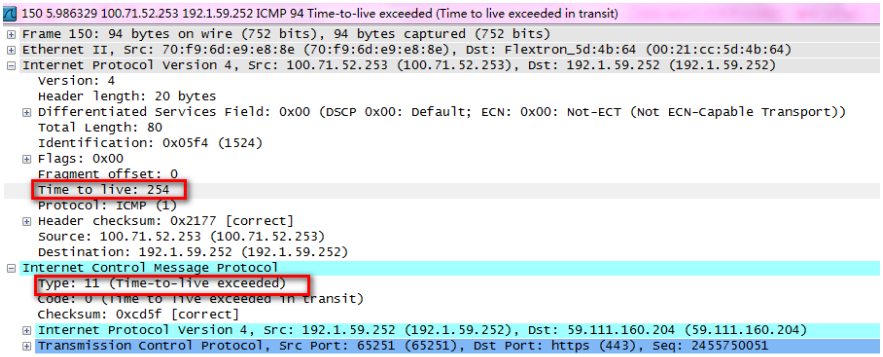
```
Frame 298: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
Ethernet II, Src: 70:f9:6d:e9:e8:8e (70:f9:6d:e9:e8:8e), Dst: Flextron_5d:4b:64 (00:21:cc:5d:4b:64)
Internet Protocol Version 4, Src: 202.97.224.69 (202.97.224.69), Dst: 192.1.59.252 (192.1.59.252)
User Datagram Protocol, Src Port: domain (53), Dst Port: 61122 (61122)
Domain Name System (response)
    [Request In: 294]
    [Time: 0.263794000 seconds]
    Transaction ID: 0xbb2e
  Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  Queries
    webzj2.reg.163.com: type A, class IN
  Answers
    webzj2.reg.163.com: type A, class IN, addr 59.111.160.204
```

继续查看PC抓包发现SYN报文直接被告知TTL超时了



```
150 5.986329 100.71.52.253 192.1.59.252 ICMP 94 Time-to-live exceeded (Time to live exceeded in transit)
Frame 150: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
Ethernet II, Src: 70:f9:6d:e9:e8:8e (70:f9:6d:e9:e8:8e), Dst: Flextron_5d:4b:64 (00:21:cc:5d:4b:64)
Internet Protocol Version 4, Src: 100.71.52.253 (100.71.52.253), Dst: 192.1.59.252 (192.1.59.252)
    Version: 4
    Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 80
    Identification: 0x05f4 (1524)
  Flags: 0x00
    Fragment offset: 0
    Time to live: 254
    Protocol: ICMP (1)
  Header checksum: 0x2177 [correct]
    Source: 100.71.52.253 (100.71.52.253)
    Destination: 192.1.59.252 (192.1.59.252)
Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xcd5f [correct]
  Internet Protocol Version 4, Src: 192.1.59.252 (192.1.59.252), Dst: 59.111.160.204 (59.111.160.204)
  Transmission Control Protocol, Src Port: 65251 (65251), Dst Port: https (443), Seq: 2455750051
```

并且差错报文透露了以下信息：



```
150 5.986329 100.71.52.253 192.1.59.252 ICMP 94 Time-to-live exceeded (Time to live exceeded in transit)
Frame 150: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
Ethernet II, Src: 70:f9:6d:e9:e8:8e (70:f9:6d:e9:e8:8e), Dst: Flextron_5d:4b:64 (00:21:cc:5d:4b:64)
Internet Protocol Version 4, Src: 100.71.52.253 (100.71.52.253), Dst: 192.1.59.252 (192.1.59.252)
    Version: 4
    Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 80
    Identification: 0x05f4 (1524)
  Flags: 0x00
    Fragment offset: 0
    Time to live: 254
    Protocol: ICMP (1)
  Header checksum: 0x2177 [correct]
    Source: 100.71.52.253 (100.71.52.253)
    Destination: 192.1.59.252 (192.1.59.252)
Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xcd5f [correct]
  Internet Protocol Version 4, Src: 192.1.59.252 (192.1.59.252), Dst: 59.111.160.204 (59.111.160.204)
  Transmission Control Protocol, Src Port: 65251 (65251), Dst Port: https (443), Seq: 2455750051
```

TTL为254，说明就相隔2跳，离PC很近，目前怀疑访问59.111.160.204的流量，产生了三层环路，建议现场利用tracert确认环路设备。

解决方法

最后客户排查路由，确实是核心设备到59.111.160.204地址有路由环路，修改路由之后163邮箱访问正常，非LB设备问题。