

知 ERG2/G3 L2TP建立成功后，开始可以ping通网关，但是访问tcp不通并且之后ping也不通

L2TP VPN 徐宁 2022-05-06 发表

组网及说明

内网服务器--ER路由器 (LNS) ---公网----PC终端

#### 问题描述

终端L2TP拨上后，能够ping通内网网关（192.168.x.1），内网服务器地址（192.168.x.250）。当开始访问tcp业务，如浏览器打开192.168.x.1访问路由器web时，网页无法打开，且再ping内网地址无法ping通。

## 过程分析

PC抓包，可以看到在访问192.168.x.1路由器web时，get http一直没有收到回包，然后一直在重传。之后也再没有收到来自192.168.x.1的tcp报文。

No.	Time	Source	Destination	Protocol	Length	Info
133	2022-04-18 13:56:48.56592000	192.168.0.1	172.16.100.2	ICMP	112	Echo (ping) reply id=0x0001, seq=1141/29956, ttl=64 (request in 133)
134	2022-04-18 13:56:49.30958000	172.16.100.2	192.168.0.1	TCP	104	51994 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
135	2022-04-18 13:56:49.31806000	172.16.100.2	192.168.0.1	TCP	104	51995 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
136	2022-04-18 13:56:49.40215000	192.168.0.1	172.16.100.2	TCP	104	80 → 51994 [SYN, ACK] Seq=0 Ack=1 Win=27200 Len=0 MSS=1360 SACK_PERM=1
137	2022-04-18 13:56:49.40251000	172.16.100.2	192.168.0.1	TCP	104	51994 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0
138	2022-04-18 13:56:49.44392700	172.16.100.2	192.168.0.1	HTTP	523	GET / HTTP/1.1
139	2022-04-18 13:56:49.50278000	172.16.100.2	192.168.0.1	ICMP	112	Echo (ping) request id=0x0001, seq=1142/30212, ttl=64 (no response in 139)
142	2022-04-18 13:56:49.83004000	172.16.100.2	192.168.0.1	TCP	523	[TCP Retransmission] 51994 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131840 Len=523
143	2022-04-18 13:56:50.26926000	172.16.100.2	192.168.0.1	TCP	104	[TCP Retransmission] 51995 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
144	2022-04-18 13:56:50.26937000	172.16.100.2	192.168.0.1	TCP	523	[TCP Retransmission] 51994 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131840 Len=523
145	2022-04-18 13:56:51.05422000	172.16.100.2	192.168.0.1	TCP	523	[TCP Retransmission] 51994 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131840 Len=523
146	2022-04-18 13:56:51.33284000	172.16.100.2	172.217.160.100	TCP	104	51997 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
147	2022-04-18 13:56:51.58276700	172.16.100.2	172.217.160.100	TCP	104	51998 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
148	2022-04-18 13:56:52.27011100	172.16.100.2	192.168.0.1	TCP	104	[TCP Retransmission] 51995 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
149	2022-04-18 13:56:52.31301000	172.16.100.2	172.217.160.100	TCP	104	[TCP Retransmission] 51997 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
150	2022-04-18 13:56:52.58316000	172.16.100.2	172.217.160.100	TCP	104	[TCP Retransmission] 51998 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

ER wan口抓包，可以看到我们是有收有发的，并且也能收到PC的重传，但是我们的回包PC全部没有收到。

No.	Time	Source	Destination	Protocol	Length	Info
2459	2022-04-18 13:56:23.99152000	192.168.0.1	172.16.100.2	ICMP	120	Echo (ping) reply id=0x0001, seq=1141/29956, ttl=64 (request in 2458)
2642	2022-04-18 13:56:24.79748100	172.16.100.2	192.168.0.1	TCP	112	51994 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2643	2022-04-18 13:56:24.79748400	172.16.100.2	192.168.0.1	TCP	112	51995 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2644	2022-04-18 13:56:24.79764600	192.168.0.1	172.16.100.2	TCP	112	80 → 51994 [SYN, ACK] Seq=0 Ack=1 Win=27200 Len=0 MSS=1360 SACK_PERM=1
2645	2022-04-18 13:56:24.79771100	192.168.0.1	172.16.100.2	TCP	112	80 → 51995 [SYN, ACK] Seq=0 Ack=1 Win=27200 Len=0 MSS=1360 SACK_PERM=1
2651	2022-04-18 13:56:24.80927400	172.16.100.2	192.168.0.1	TCP	104	51994 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0
2655	2022-04-18 13:56:24.90313100	172.16.100.2	192.168.0.1	HTTP	531	GET / HTTP/1.1
2666	2022-04-18 13:56:24.93044000	192.168.0.1	172.16.100.2	TCP	100	80 → 51994 [ACK] Seq=1 Ack=432 Win=28288 Len=0
2667	2022-04-18 13:56:24.93075000	192.168.0.1	172.16.100.2	TCP	141	80 → 51994 [PSH, ACK] Seq=1 Ack=432 Win=28288 Len=141 [TCP segment of a retransmission (192.168.0.1 → 172.16.100.2) to 192.168.0.1:80: Seq=1, Len=141]
2676	2022-04-18 13:56:24.98045400	172.16.100.2	192.168.0.1	ICMP	120	Echo (ping) request id=0x0001, seq=1142/30212, ttl=64 (reply in 2677)
2677	2022-04-18 13:56:24.98057000	172.16.100.2	192.168.0.1	ICMP	120	Echo (ping) reply id=0x0001, seq=1142/30212, ttl=64 (request in 2676)
2727	2022-04-18 13:56:25.28658500	192.168.0.1	172.16.100.2	HTTP/XML	742	HTTP/1.1 200 OK
2732	2022-04-18 13:56:25.32093000	172.16.100.2	192.168.0.1	HTTP	531	[TCP Sockets] [Retransmission] GET / HTTP/1.1
2751	2022-04-18 13:56:25.32098000	192.168.0.1	172.16.100.2	TCP	112	[TCP Dup ACK 2666#1] 80 → 51994 [ACK] Seq=684 Ack=432 Win=28288 Len=0
2793	2022-04-18 13:56:25.53651000	192.168.0.1	172.16.100.2	TCP	742	[TCP Retransmission] 80 → 51994 [PSH, ACK] Seq=42 Ack=432 Win=28288 Len=742
2811	2022-04-18 13:56:25.75549500	172.16.100.2	192.168.0.1	TCP	112	[TCP Retransmission] 51995 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2843	2022-04-18 13:56:25.75669700	192.168.0.1	172.16.100.2	TCP	112	[TCP Retransmission] 80 → 51995 [SYN, ACK] Seq=1 Ack=1 Win=27200 Len=0 MSS=1360 SACK_PERM=1
2847	2022-04-18 13:56:25.76681000	172.16.100.2	192.168.0.1	HTTP	531	[TCP Sockets] [Retransmission] GET / HTTP/1.1

## 解决方法

从上述现象看，客户端发起TCP连接后，从ER到客户端方向的报文就全部阻断了，怀疑线路上对流量有检测或过滤，请联系运营商排查。

如果想进一步判断设备是否有问题，可以尝试将ER的WAN口与PC直连，WAN口与PC都写静态地址，这样PC跳过公网线路直接拨号L2TP到ER，看看是否还会有问题。如果仍有问题，则可能是设备问题，请联系产品线确认。

补充：之前遇到过很多例这样的问题，是由于运营商在路由器回给终端的报文中又封装了一层L2tp报文头，导致终端无法识别将报文丢弃，更换光猫等操作后解决。如果用户是使用inode进行拨号的话，抓包选择inode网卡会抓不到异常报文，如果选择物理网卡，有可能会抓到两层L2tp头报文。

举例：

下面这个UDP的报文，DATA里的数据，标红的00 02及后面和L2TP头是完全一样的，也就说封装了两层头。

刚开始L2tp拨号后可以ping通，ERG3发送的reply报文和pc收到的一致；当发起tcp连接后，ERG3发送的reply报文没有问题，但是pc收到的报文有2层L2tp头。

```
1456 2022-04-11 14:14:26.769636 172.31.20.7 172.31.50.10 142 UDP 22 + 63335 Len=62
> Frame 1456: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface \Device\NPF_{A5570984-A809-4BAE-9222-9C4D748EA319}, id 0
> Ethernet II, Src: 4a:35:2b:a7:0f:64 (4a:35:2b:a7:0f:64), Dst: a4:6b:b6:31:1e:33 (a4:6b:b6:31:1e:33)
> Internet Protocol Version 4, Src: 222.82.206.103, Dst: 172.20.10.2
> User Datagram Protocol, Src Port: 1781, Dst Port: 60919
> Layer 2 Tunneling Protocol 第一层头
  Packet type: Data Message Tunnel Id=1 Session Id=28504
  Tunnel ID: 1
  Session ID: 28504
  Point-to-Point Protocol
  Address: 0x0f
  Control: 0x03
  Protocol: Internet Protocol version 4 (0x0021)
  > Internet Protocol Version 4, Src: 172.31.20.7, Dst: 172.31.50.10
  > User Datagram Protocol, Src Port: 22, Dst Port: 63335
  > Data (62 bytes)
  Data: 000200010f58ff03002145000034640d40003f063967ac1f. 第二层PPP
  [length: 62]
0000 a4 6b b6 31 1e 33 4a 35 2b a7 0f 64 00 00 00 00 k-1375+-d-E-
0010 00 80 1b 5a 00 00 38 11 43 de 52 ce 67 3c 14 第一层 L2TP R g..
0020 09 02 06 a5 ed 20 06 fc 00 00 00 02 00 01 07 55 第二层 L2TP R g..
0030 ff 03 00 21 45 00 00 5a 1d 3c 00 00 00 00 00 00 第二层 PPP
0040 8c 1f 14 07 8c 1f 22 03 00 16 f7 67 00 46 00 00 .....2...g.F..
0050 00 02 00 01 07 55 00 21 45 00 00 00 00 00 00 第二层 PPP
0060 40 00 3f 00 39 07 8c 1f 22 03 00 16 00 00 00 00 @? 96...2..
0070 f7 67 86 1c 2b 4d 76 a0 e0 21 b9 10 00 e9 34 66 g 4Nv !:....n
0080 00 00 01 01 05 0a 76 a0 e0 0d 76 a0 e0 21 .....
```

总之，无论是否是运营商多封装了一层L2TP头导致的问题，如果设备对报文的处理是没有问题的，请联系运营商进行确认。

