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

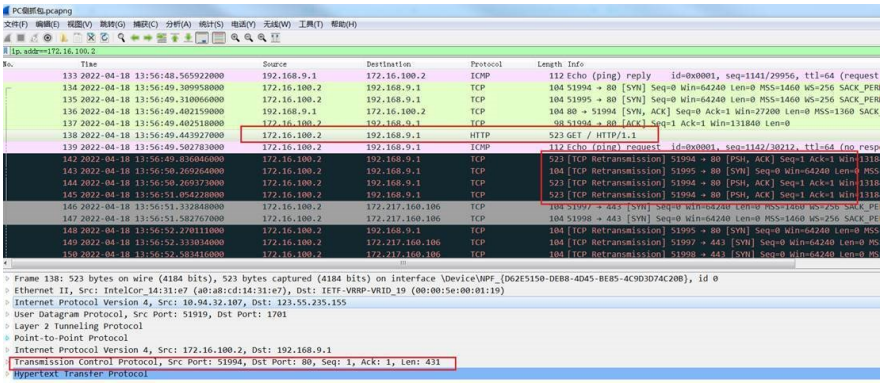
内网服务器--ER路由器（LNS）---公网----PC终端

问题描述

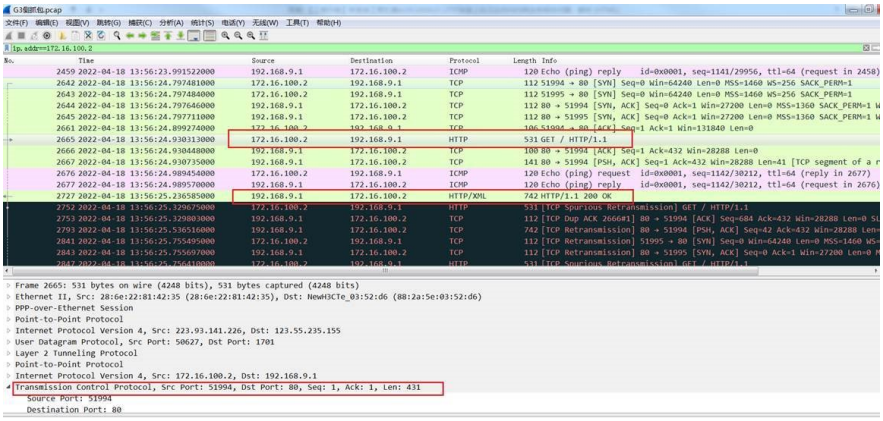
终端L2TP拨上后，能够ping通内网网关（192.168.x.1），内网服务器地址（192.168.x.250）。当开始访问tcp业务，如浏览器打开192.168.x.1访问路由器web时，网页无法打开，且再ping内网地址无法ping通。

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。



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。



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。

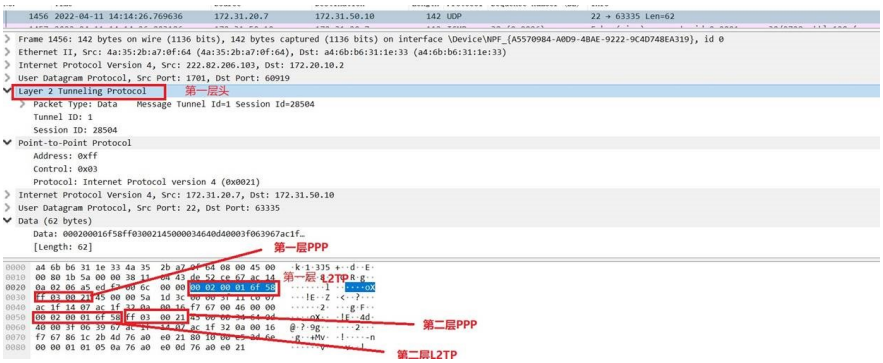
如果想进一步判断设备是否有问题，可以尝试将ER的WAN口与PC直连，WAN口与PC都写静态地址，这样PC跳过公网线路直接拨号L2TP到ER，看看是否还会有问题。如果仍有问题，则可能是设备问题，请联系产品线确认。

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上又封装了一层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。



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。