某局点ER5200G2路由器做LNS侧设备时，外网终端L2TP VPN接入无法访问内网终端问题排查

L2TP VPN 徐猛 2018-06-05 发表

组网及说明

不涉及

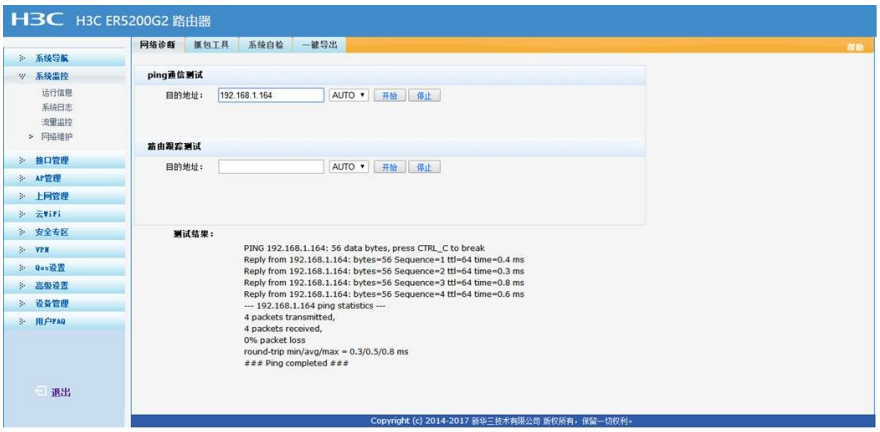
问题描述

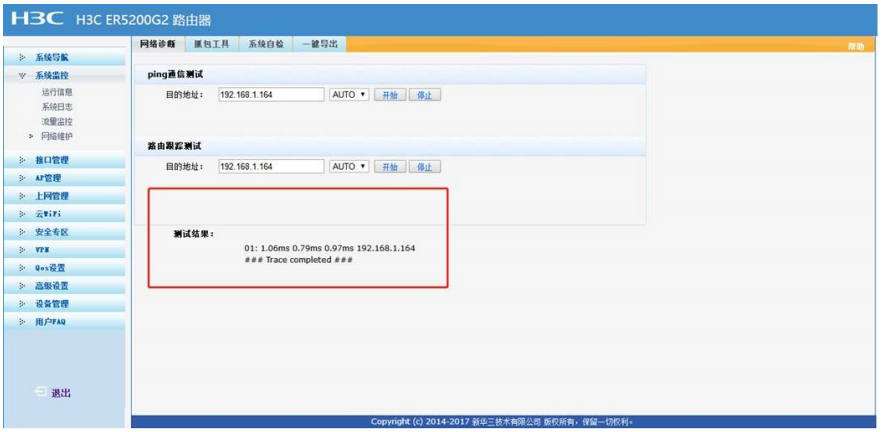
某局点现场配置了L2TP VPN，使用我司的ER5200G2设备做为网络中的LNS设备，L2TP隧道正常建立，LAC侧内网终端使用PPP的方式获取地址，且能够获取地址成功。但是出现了一个奇怪的现象，LAC侧终端能够访问通LNS侧内网终端的内网网关，但是无法ping通内网终端。

过程分析

1.开始怀疑LNS侧内网终端是不是因为没有配置网关，从而导致LAC侧终端的ping报文到了LNS侧终端后，LNS侧终端回包时出现问题。但是现场检查，LNS侧内网终端均正确的配置了网关信息。

2.让现场收集了ER5200G2的相应的配置信息。

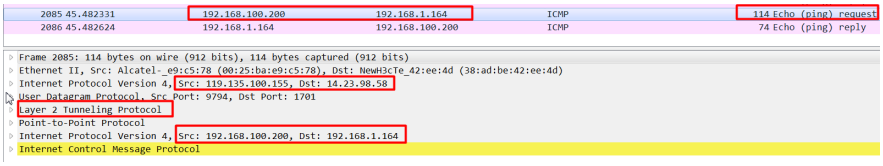




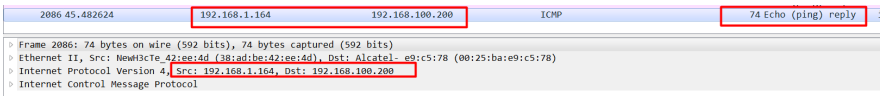
根据现场发来的L2TP相关配置，检查后并未发现L2TP配置存在问题。

3.让现场进行LAC侧终端ping测试LNS侧下联终端，同时在ER5200G2的LAN口和WAN口进行抓包。
抓包后发现：

在设备的WAN口处可以看到经过L2TP封装的，由LAC侧终端地址192.168.100.200到LNS侧终端地址192.168.1.164的ping报文，类型为ping请求报文。同时外层封装使用的公网地址为：源地址119.135.100.155，目的地址14.23.98.58,使用L2TP隧道协议封装。



但是查看回包时发现了问题，在查看由LNS侧终端地址192.168.1.164发给LAC侧终端地址192.168.100.200的ping回应报文时，发现该回应报文并未经过L2TP封装就被从WAN口发了出来。



由于之前现场描述，LAC侧终端能够ping通对端LNS侧内网的网关，且在我司ER设备上对于本地始发的报文是不会匹配策略路由的，回包不会受策略路由配置影响。于是怀疑现场的ER5200G2路由器上是不是因为配置了策略路由，从而在LAC侧终端ping测试对端LNS侧内网的终端时，导致内网终端回包匹配了策略路由，而并未发给L2TP的隧道接口进行封装。

解决方法

现场检查设备的策略路由配置，发现客户之前自行配置了策略路由，与之前的预想原因一致，让现场工程师修改策略路由配置后，问题解决。