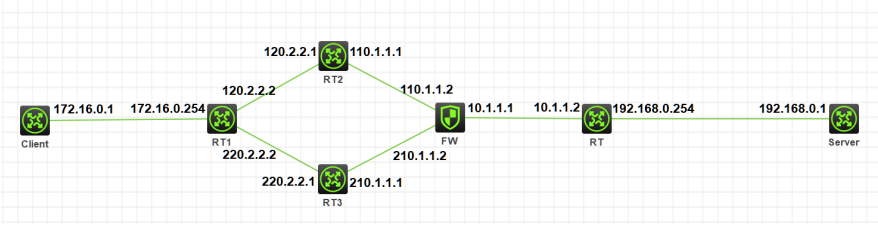
从协议说起（2）——ICMP（Tracert）

Tracert　胡伟　2020-10-15 发表

组网及说明

组网如下：Client 172.16.0.1 需要访问Server 192.168.0.1，FW将192.168.0.1分别映射为两条链路的外网地址

链路1：nat server global 110.1.1.3 inside 192.168.0.1



涉及的所有设备开启下面两个功能

ip ttl-expires enable

ip unreachables enable

配置步骤

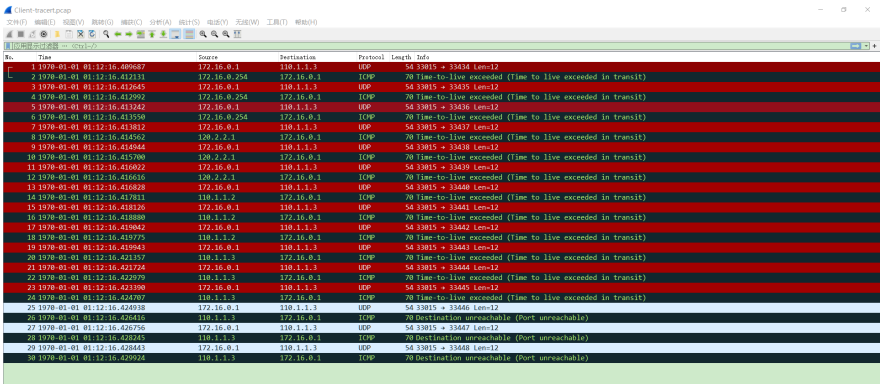
Tracert根据百度百科的解释是（跟踪路由）是路由跟踪实用程序，用于确定 IP 数据包访问目标所采取的路径。Tracert 命令用 IP 生存时间 (TTL) 字段和 ICMP 错误消息来确定从一个主机到网络上其他主机的路由。**其工作原理为通过向目标发送不同IP生存时间 (TTL) 值的“Internet控制消息协议 (ICMP)”回应数据包，Tracert诊断程序确定到目标所采取的路由。要求路径上的每个路由器在转发数据包之前至少将数据包上的 TTL 递减 1。数据包上的 TTL 减为 0 时，路由器应该将“ICMP 已超时”的消息发回源系统。**

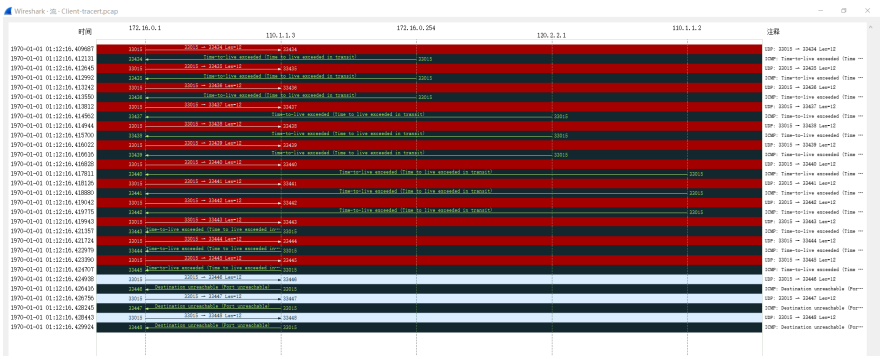
tracert是Windows下常用的命令行工具（基于ICMP协议），UNIX下与之对应的是traceroute（基于UDP协议）。

Comware基于Linux系统开发，使用tracert命令，基于UDP协议。在客户端tracert FW链路1的nat server global地址110.1.1.3回显如下：

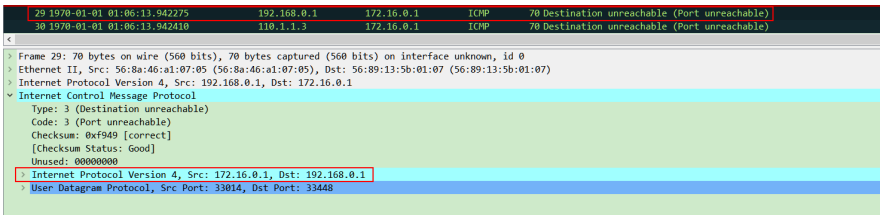
```
[H3C]tracert 110.1.1.3
traceroute to 110.1.1.3 (110.1.1.3), 30 hops at most, 40 bytes each packet, press CTRL_C to break
 1  172.16.0.254 (172.16.0.254)  1.000 ms  0.000 ms  1.000 ms
 2  120.2.2.1 (120.2.2.1)  1.000 ms  1.000 ms  0.000 ms
 3  110.1.1.2 (110.1.1.2)  2.000 ms  2.000 ms  1.000 ms
 4  110.1.1.3 (110.1.1.3)  3.000 ms  5.000 ms  3.000 ms
 5  110.1.1.3 (110.1.1.3)  4.000 ms  4.000 ms  3.000 ms
[H3C]
```

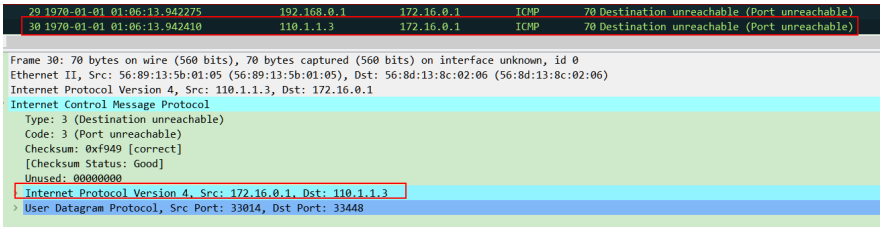
FW上抓包流量图分析如下



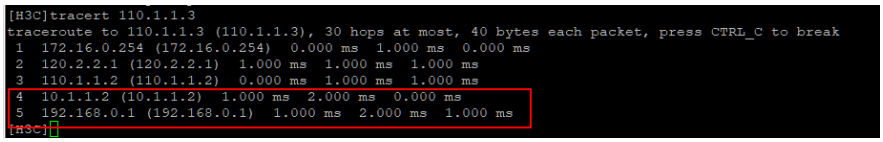


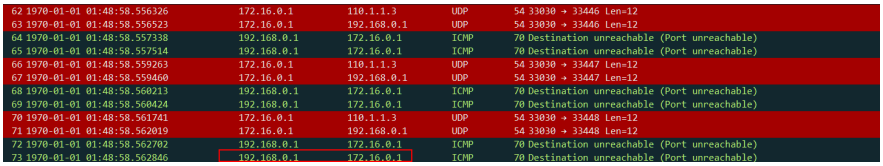
由于FW上默认开启nat alg icmp-error，会对服务器内网返回的icmp-error报文中的IP地址进行修改，这就导致了Client上tracert无法显示NAT后的私网地址。





将FW使能undo nat alg icmp-error，使得icmp-error报文IP不发生改变，这样Client即可显示NAT后的私网地址，如下：





配置关键点

附件下载： Client-tracert.rar