## ****实验一：基于eNSP的ARP协议分析****

****一、环境配置****

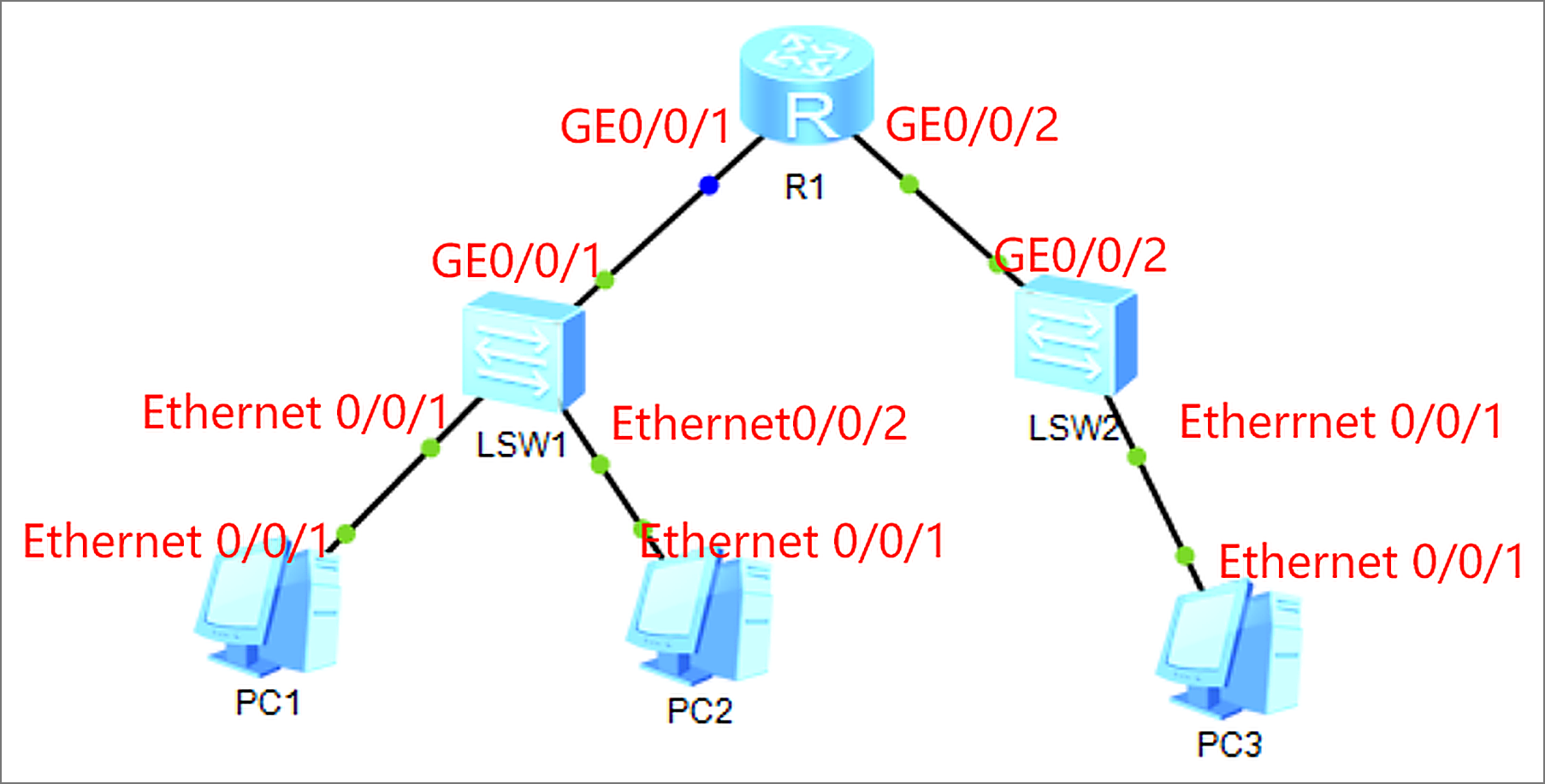
****1. 实验设备****

华为路由器 R1

PC1、PC2、PC3

eNSP[模拟器](https://so.csdn.net/so/search?q=%E6%A8%A1%E6%8B%9F%E5%99%A8&spm=1001.2101.3001.7020" \t "https://blog.csdn.net/2301_79704879/article/details/_blank)

****2. 网络拓扑****



3. IP地址规划

R1接口：

G0/0/1: 10.1.1.254/24

G0/0/2: 10.1.2.254/24

PC地址：

PC1: 10.1.1.1/24（未配置网关）

PC2: 10.1.1.2/24

PC3: 10.1.2.3/24（未配置网关）

二、原理

1. ARP协议工作机制

（1）同网段通信流程

当PC1（10.1.1.1）访问PC2（10.1.1.2）时：

ARP请求（广播）：PC1发送广播ARP请求：“谁是10.1.1.2？请告诉10.1.1.1”

ARP响应（单播）：PC2回复：“我是10.1.1.2，我的MAC是00-11-22-33-44-55”

ICMP通信：

PC1将ICMP报文封装到目标MAC地址（PC2的MAC）中，直接发送。

（2）跨网段通信问题

当PC1（10.1.1.1）尝试访问PC3（10.1.2.3）时：

无网关配置：PC1认为PC3在同一子网，发送ARP请求广播

广播域隔离：路由器默认不转发广播，PC3无法收到请求 → 通信失败

2. Proxy ARP核心原理

路由器介入：

R1在接口G0/0/1收到PC1的ARP请求（目标IP：10.1.2.3）

R1检查路由表，发现10.1.2.0/24是其直连网络

R1以自身G0/0/1接口的MAC地址响应PC1

PC1将数据包发送至R1，R1根据路由表转发至PC3

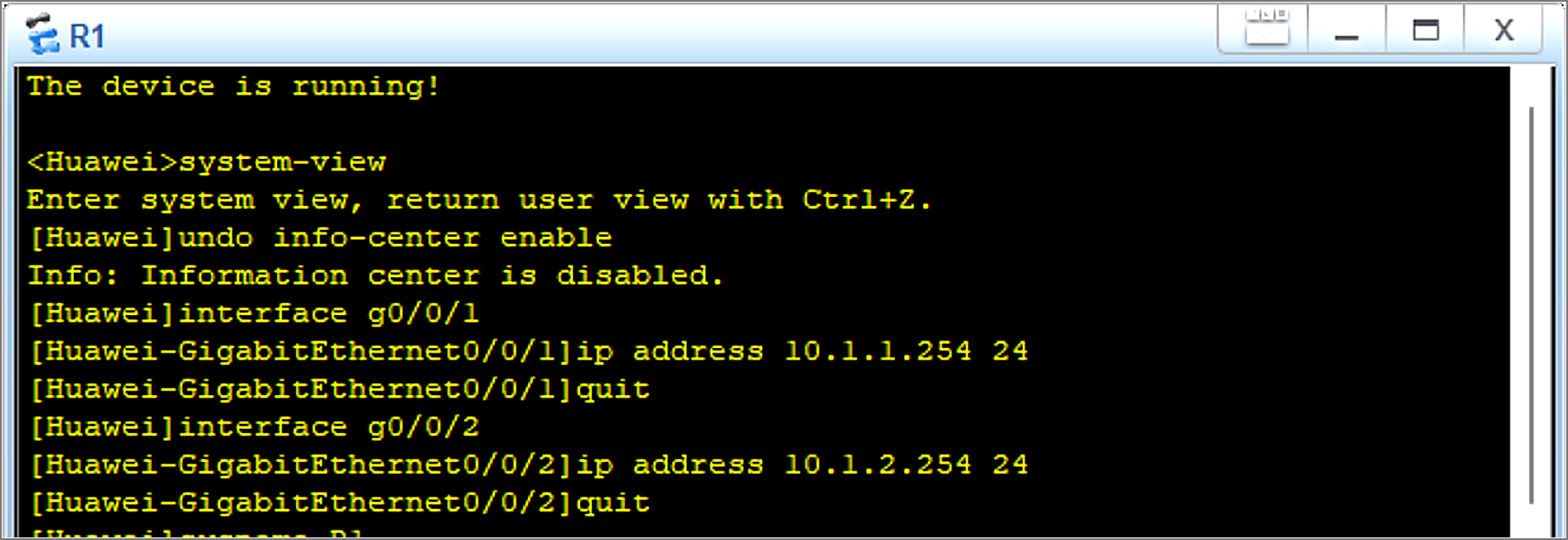
本质：路由器“欺骗”PC1，使PC1误以为目标主机在同一广播域，实际通过路由转发实现跨网段通信。

三、步骤

1. 基础配置

配置路由器接口IP

路由器R1配置（建立两个独立的子网，为后续跨网段通信测试提供基础架构）：



验证直连通信

PC1 ping PC2（同子网）→ 成功

验证逻辑：确认ARP协议在局域网内的正常运作。

PC1 ping G0/0/1接口 PC3 ping g0/0/2→ 成功

验证逻辑：确认终端与网关的基础连通性。

实验结果见（四部分）

2. 跨网段通信问题复现

步骤3：PC1 ping PC3（无Proxy ARP）

现象：请求超时

抓包分析（Wireshark示例）：

ARP请求未响应

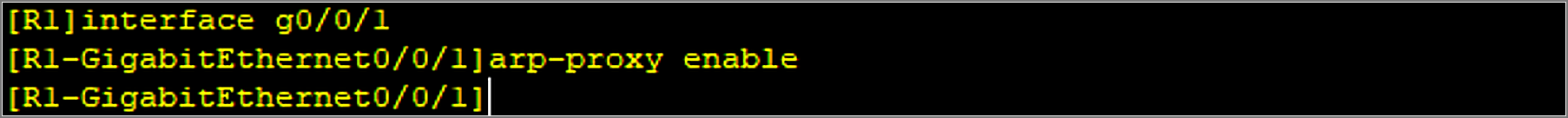
PC1持续发送ARP请求广播，但无设备响应

关键结论：

不同子网的主机无法通过广播ARP直接通信。

3. Proxy ARP功能验证

启用Proxy ARP



配置目的：

允许路由器响应非本子网的ARP请求，突破广播域限制。

再次测试PC1 ping PC3

现象：通信成功

抓包分析：

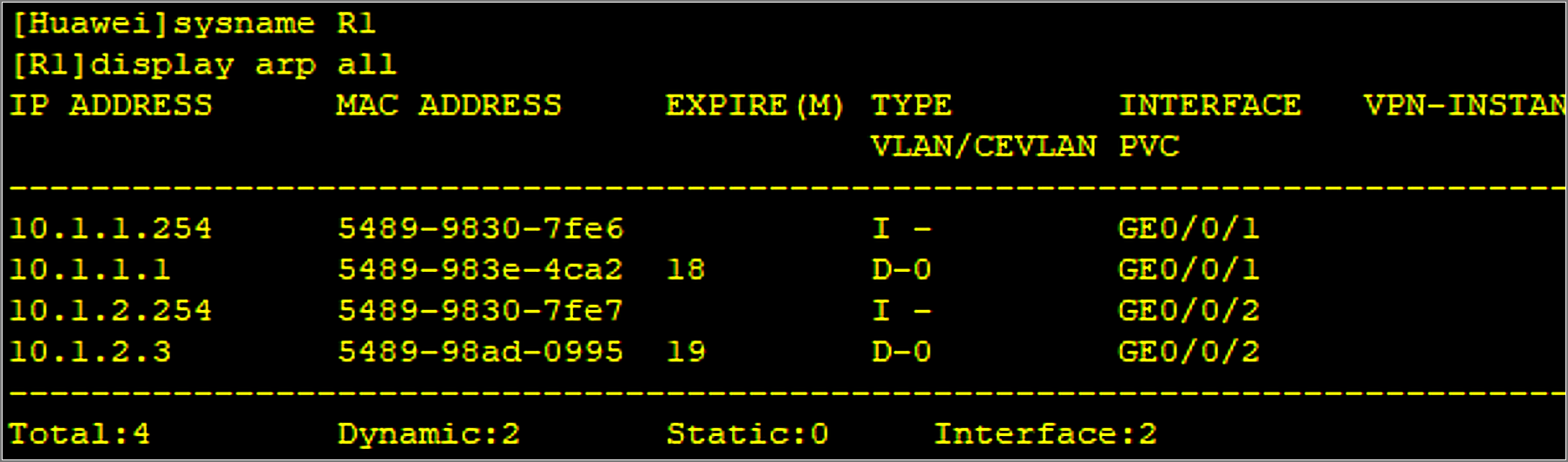
PC1发送ARP请求：“Who has 10.1.2.3?”

R1以自身MAC（00e0-fc12-3456）响应

PC1发送ICMP报文至R1，R1转发至PC3

结果见第四部分

5. 修改ARP表的映射 再次ping测试



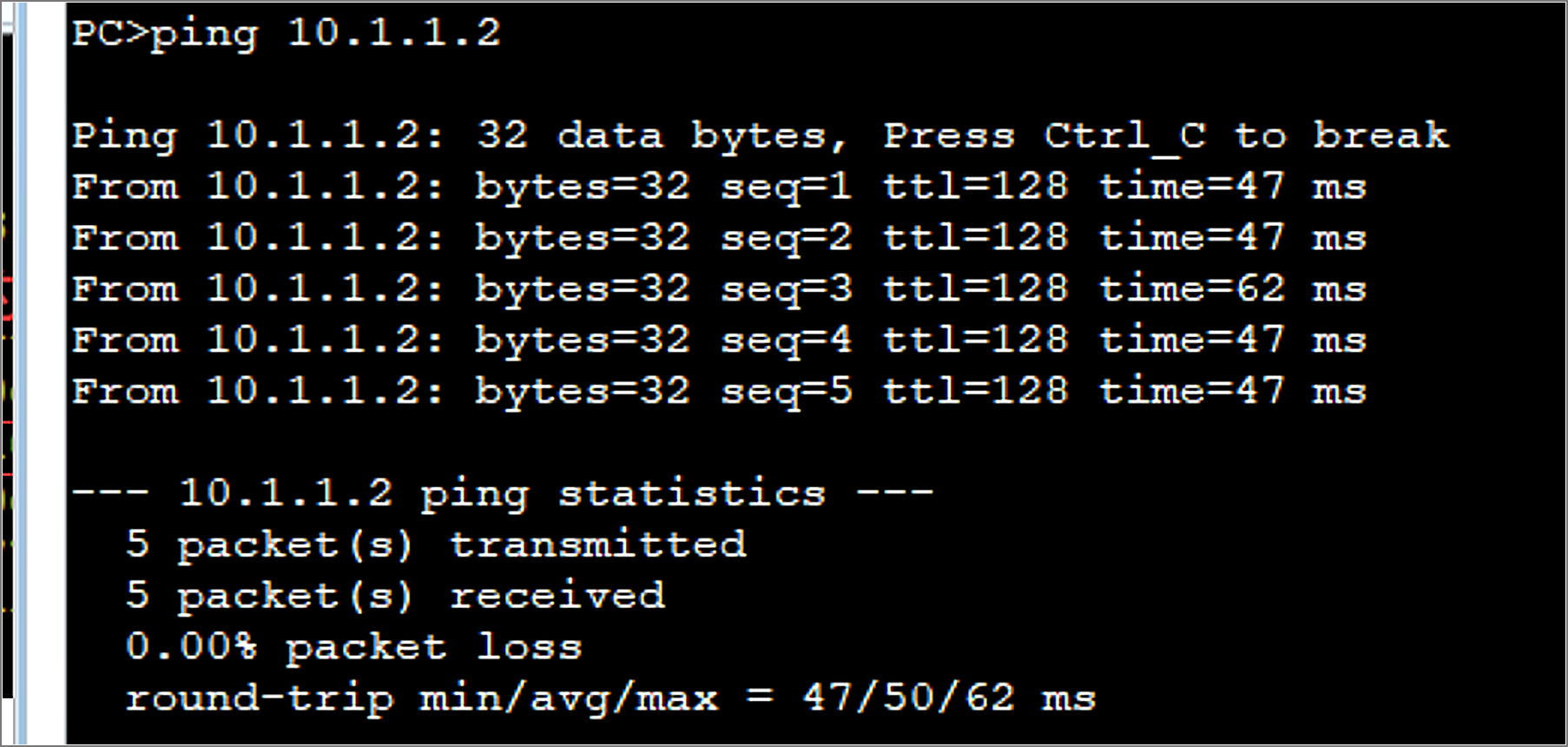
IMG_256

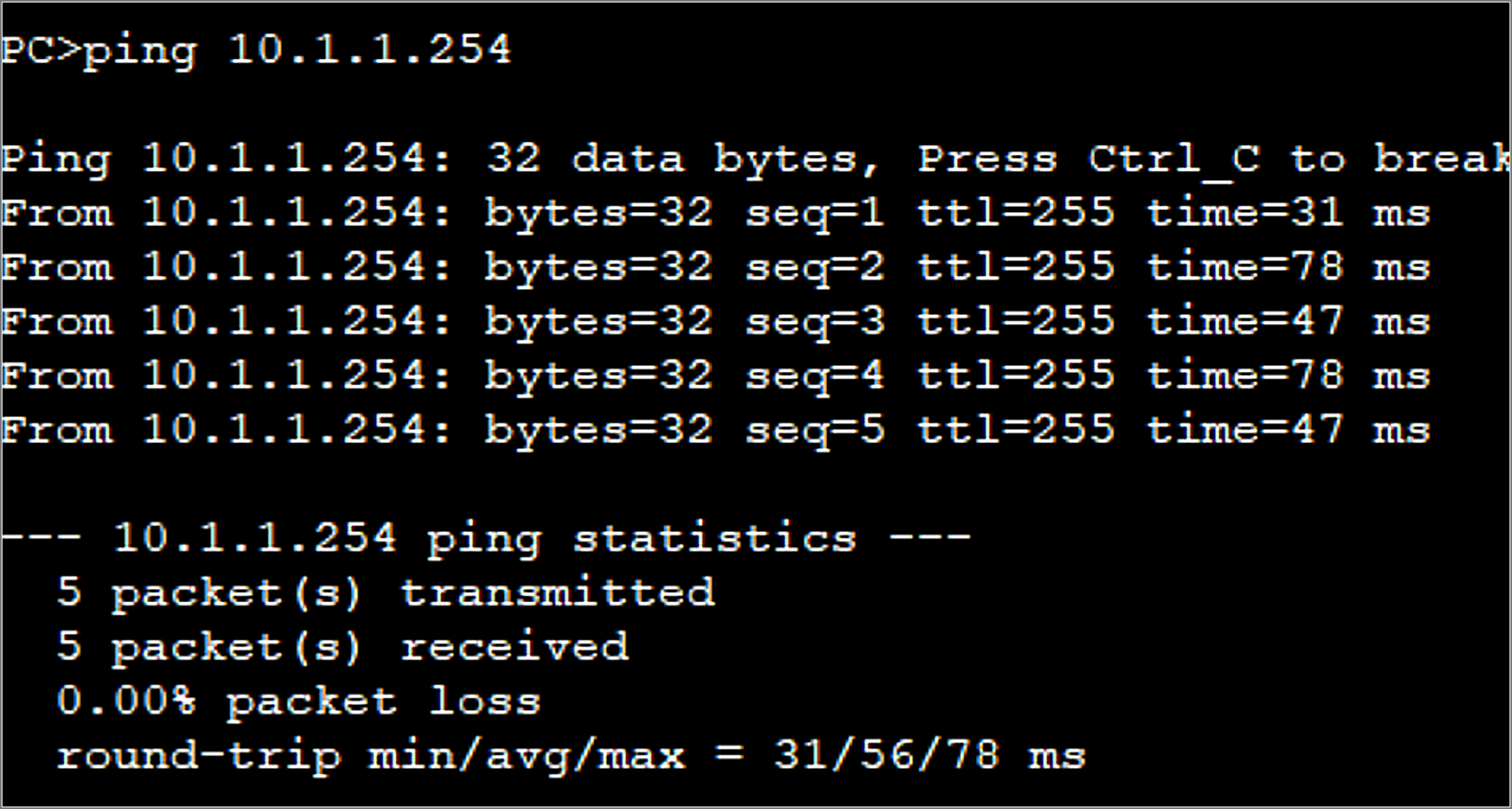
****四、结果****

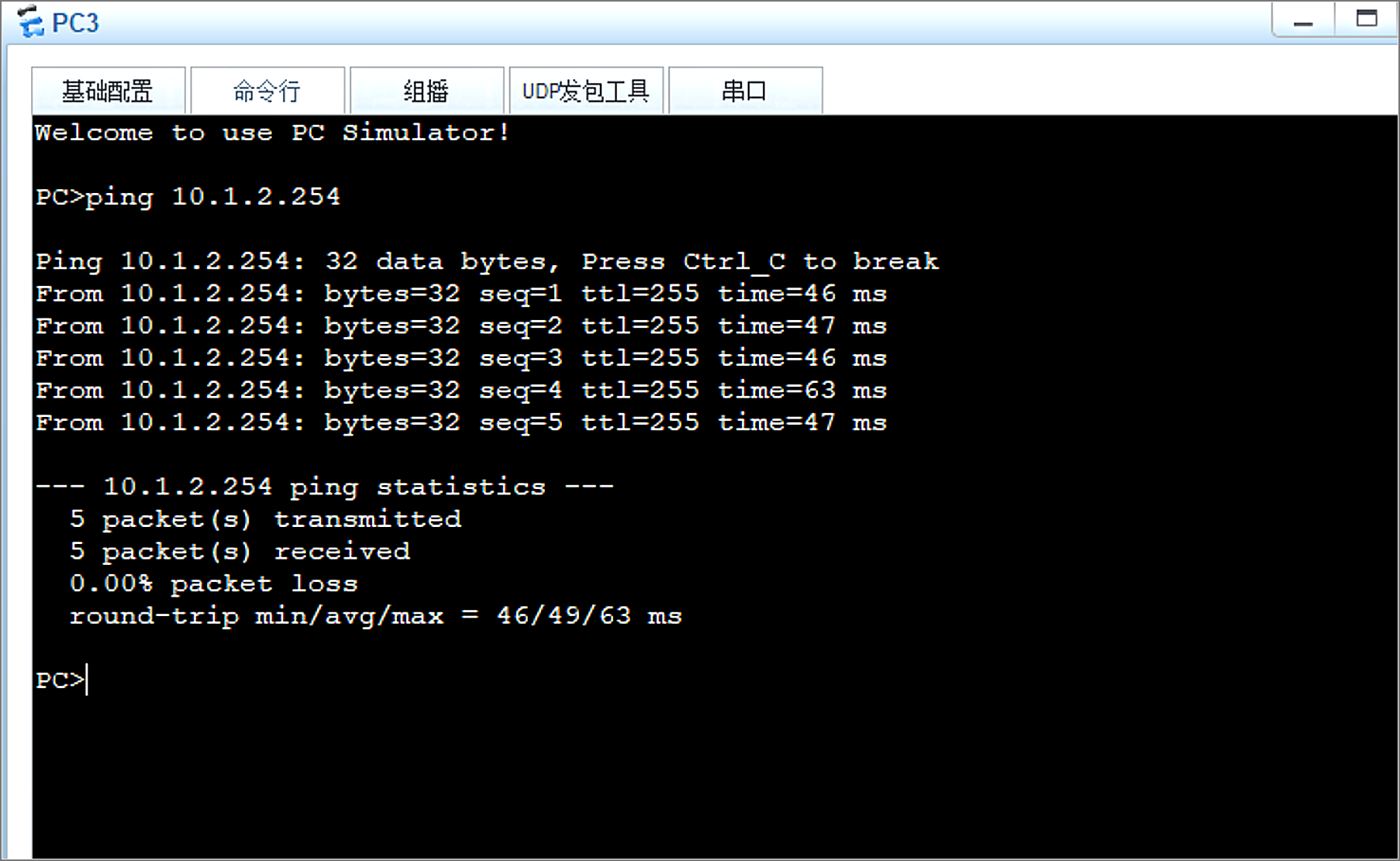
1. 验证直连通信

PC1 ping PC2（同子网）→ 成功

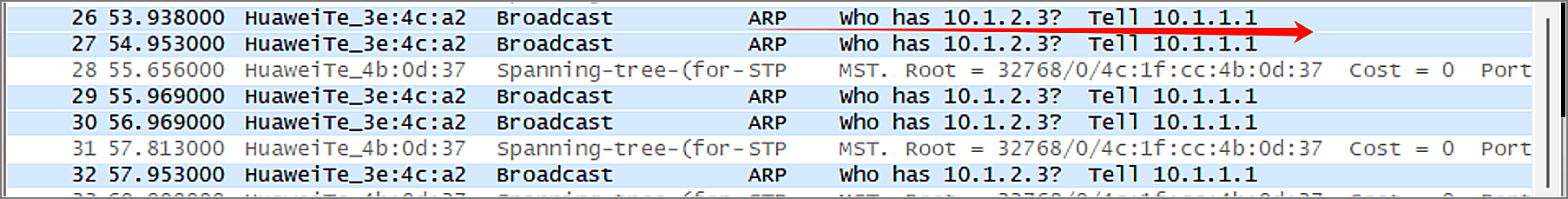
PC1 ping G0/0/1接口 PC3 ping g0/0/2→ 成功



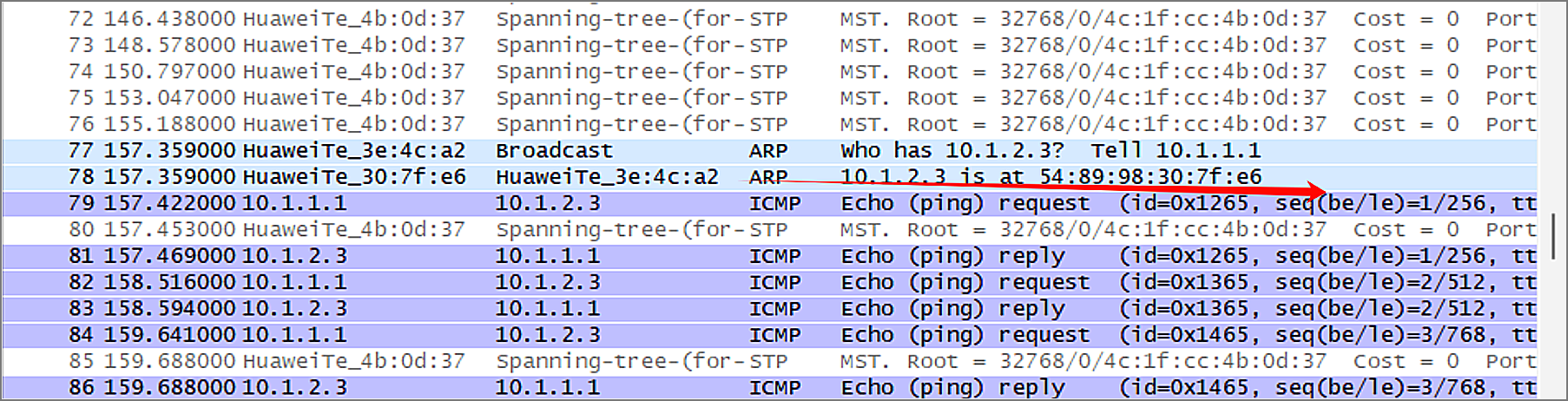


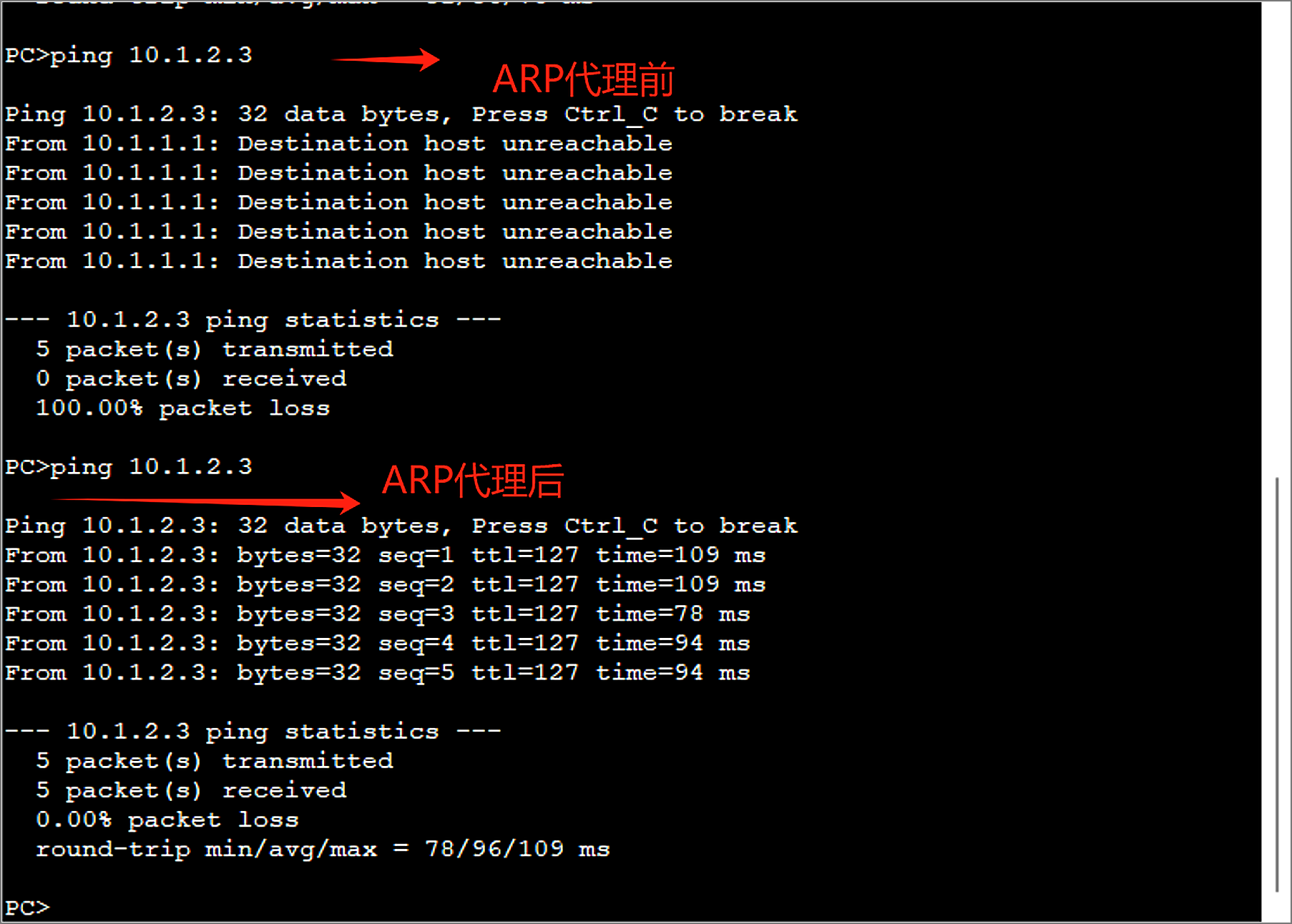


****2.未启动ARP代理是 PC1pingPC3的抓包分析：（ARP请求未响应）****

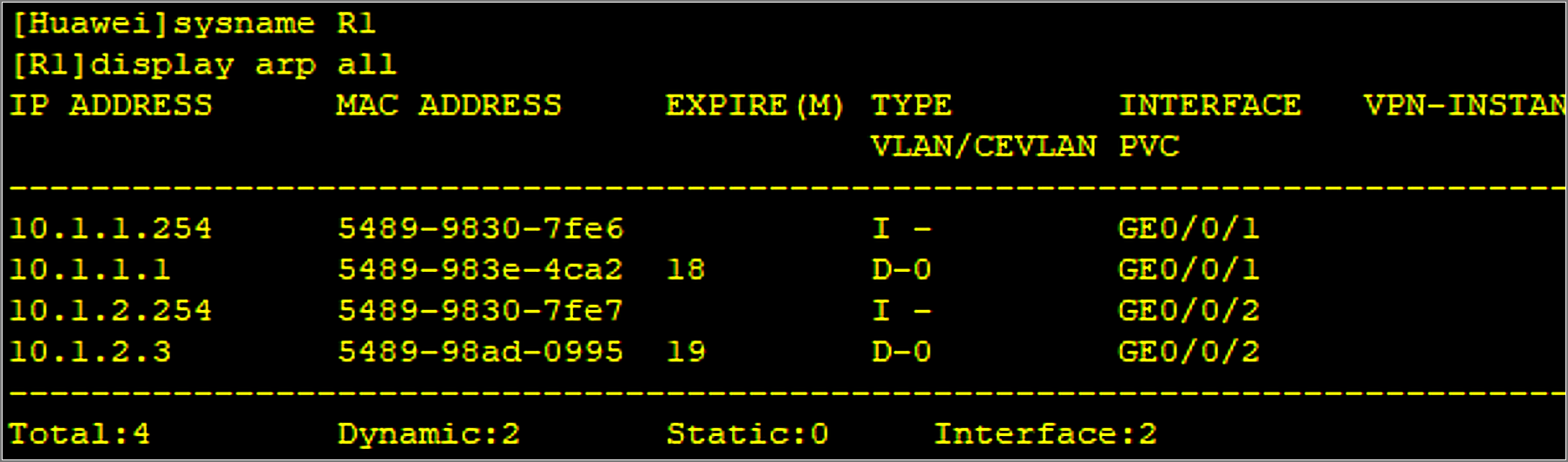


****3.启动AARP代理后PC1 ping PC3结果：****

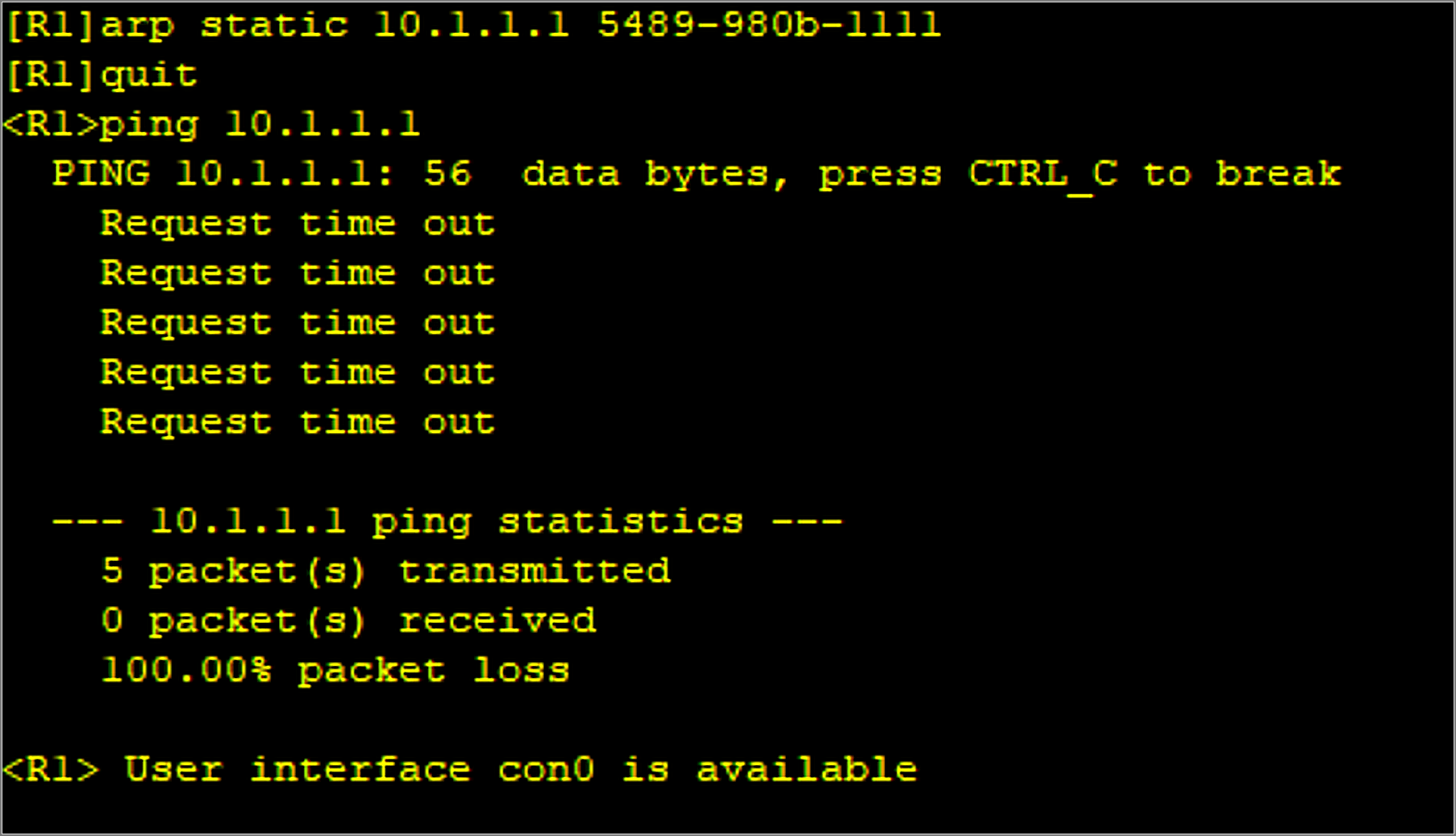




****ARP表：****



****修改映射后无法ping通：****



五、心得体会

通过这次实验，让我掌握了ARP协议和Proxy ARP的配置方法，同时学会了如何用NESP软件搭建网络拓扑结构。我有几个感悟：

动态ARP的脆弱性：

实验中手动修改ARP表项后，PC1误将数据发送到错误MAC地址，导致通信中断。这让我深刻认识到动态ARP易受欺骗攻击的缺陷。

通过抓包分析，直观理解了Proxy ARP并非真正“代理”目标主机，而是路由器通过欺骗性ARP响应，将自身作为数据中转站，实现跨子网通信。

通过抓包我理解了ARP协议原理：启动 ARP 代理后工作流程如下: R1 收到 PC1 寻找PC的MAC 地址的 ARP 请求时先比对 ARP 表，若发现没有适合的 MAC 地址则再将此 IP 地址拿去比对自身的路由表。若路由表中有合适的路由则会回复本接口的 MAC地址给 PC1 ，此后PC1 发送给PC3的数据都是先发送至此端口，接着比对路由表后再将其转运至真正目的地。