**暨南大学本科实验报告专用纸**

课程名称 计算机网络实验 成绩评定

实验项目名称数据链路层和网络层协议分析指导教师 潘 冰

实验项目编号 实验七 实验项目类型 验证性 实验地点 实验室

学生姓名 周录塔 学号 2019050383

学院 智能科学与工程 系 　专业 信息安全

实验时间 2021 年 11 月 2 日 午～ 月 日 午

**【实验目的】**

1. 理解链路层、网络层主要协议格式，以及协议的工作原理
2. 理解网关和子网掩码概念
3. 学会利用网络嗅探器（如**Wireshark**）分析协议格式和协议的工作过程
4. 学会使用ping、tracert、arp等命令并使用嗅探器分析其工作过程。

**【实验内容】**

1. 用嗅探器捕获数据包。
2. 分析以太网帧、ARP协议、IP协议、ICMP协议格式
3. 分析PING、TRACERT、ARP命令的工作过程
4. 通过修改主机的网关为指定默认网关、本机IP地址或不设置网关，观察ping的结果，用嗅探器捕获数据包并分析。

**【实验原理】**

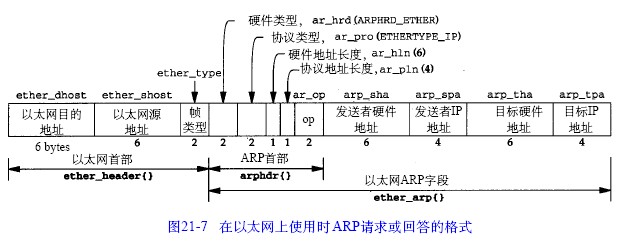
**1、网络嗅探器**

Wireshark是一个网络数据包分析软件。通过该软件可以获取网络数据包，并能进行统计分析网络数据包数据。运行Wireshark时需要将网卡设为**混合模式**。

如果在交换环境里对其他主机进行嗅探，需要对交换机端口进行映射。

**2、协议**

**以太网上使用的ARP协议格式**



**其他协议数据包格式见教材**。

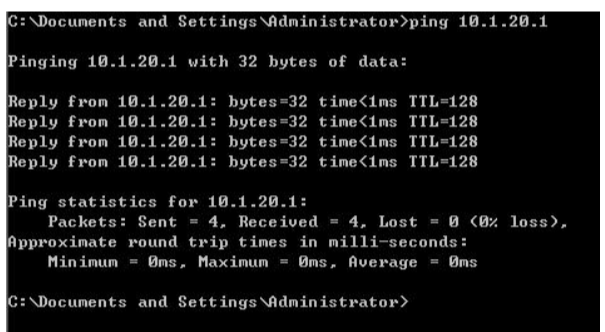
**【实验环境】**

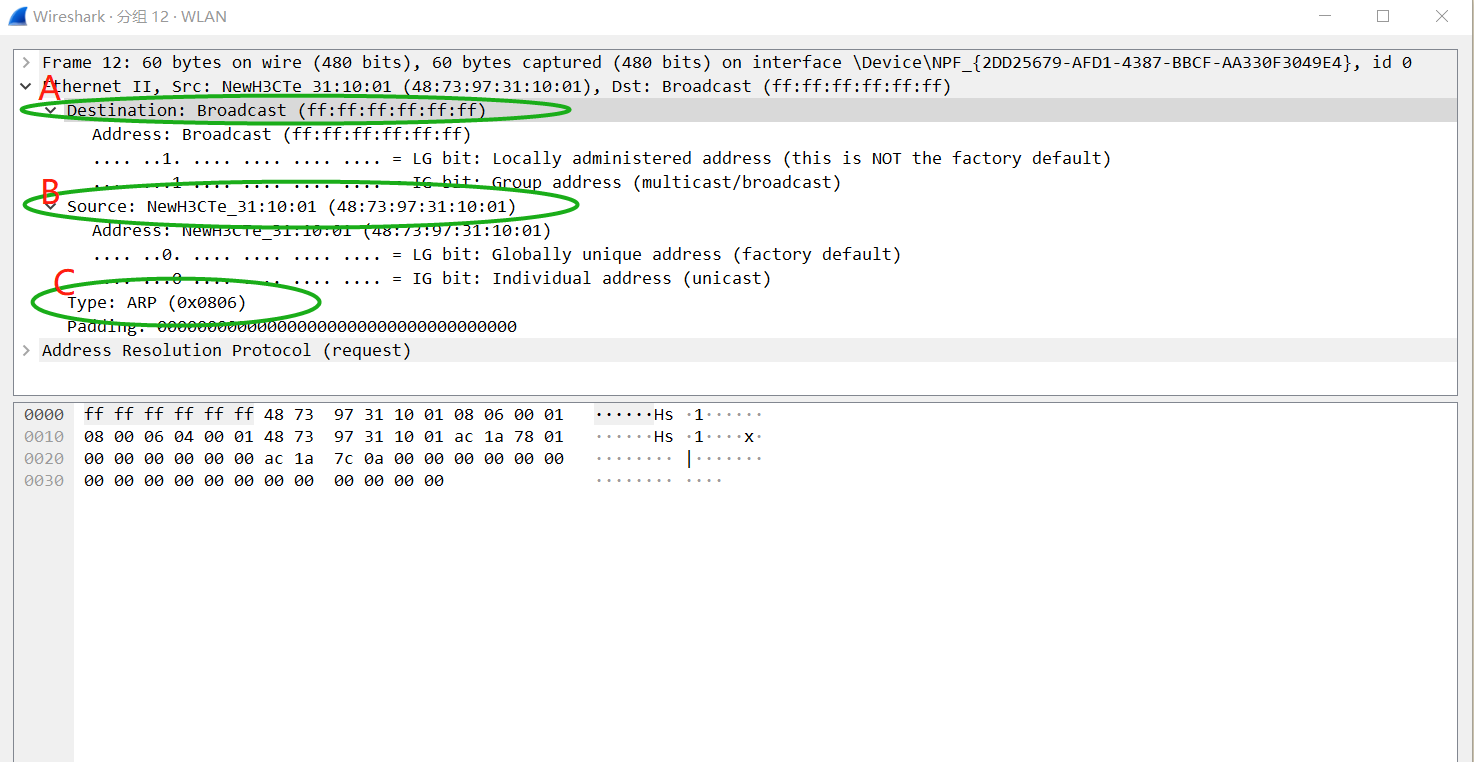
计算机2台，交换机一台。

**【实验步骤】**

1. 安装Wireshark
2. 以太网协议分析

从主机A上向主机B发PING检测报文，捕获以太数据帧，记录并分析MAC帧各字段的含义。





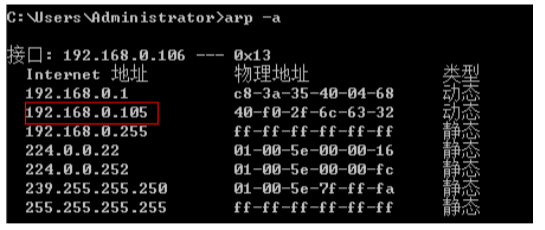
**A：目的地址为全“1”，说明是广播地址。以太网通过广播希望找到目的主机的MAC地址。**

**B：这是源地址，也是个人地址。**

**C:ARP协议，代码为十六进制的0806，表示上一层的协议的ARP，回复的消息交给ARP解封装，就能得到目的主机的MAC地址。**

1. ARP协议分析

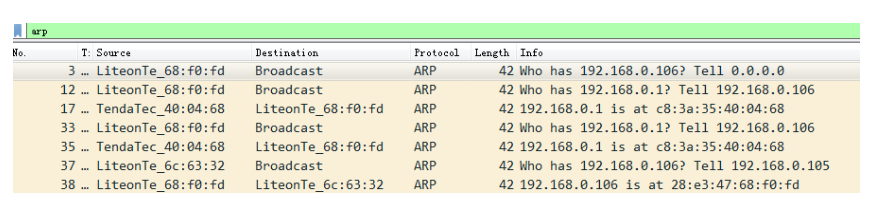
* 进入DOS窗口，用arp – a 查看本机上的ARP表的情况，然后用 arp –d B 删除B的记录（如果有的话）；

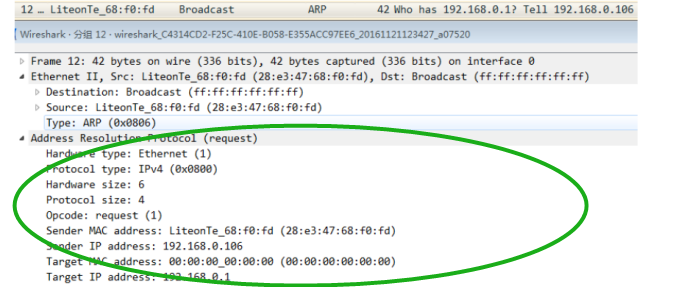




* 运行Wireshark程序；
* 把网线断开1分钟，然后再联网，观察此时是否能捕获ARP报文，如果能，记录并分析各字段的含义；

**此时能捕获到报文：**





**各字段含义：**

**硬件类型：1，也就是以太网。**

**协议类型：IP协议。**

**MAC地址长度：6Bytes**

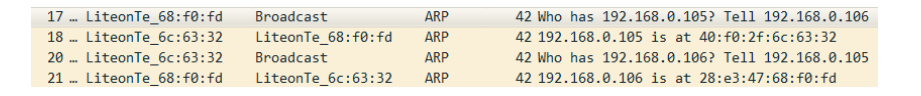
**IP地址长度：4Bytes**

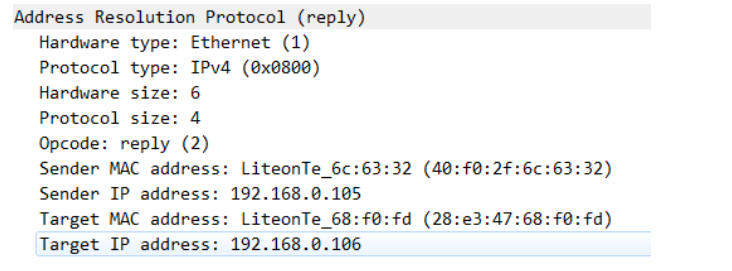
**操作码：1，请求。**

**源主机MAC、IP**

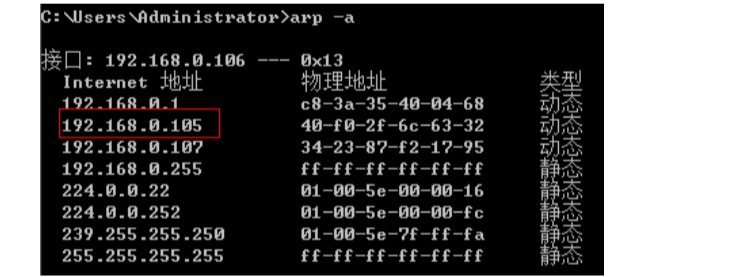
**目的主机MAC、IP**

* 从主机A上向主机B发PING检测报文，观察此时是否能捕获ARP报文，如果能，记录并分析各字段的含义；





* 通过arp - a 查看ARP表的更新情况，记录此时能否看到B对应的MAC地址；



* 再次从主机A上向主机B发PING检测报文，或者再次从主机B上向主机A发PING检测报文，观察看此时是否能捕获ARP报文；

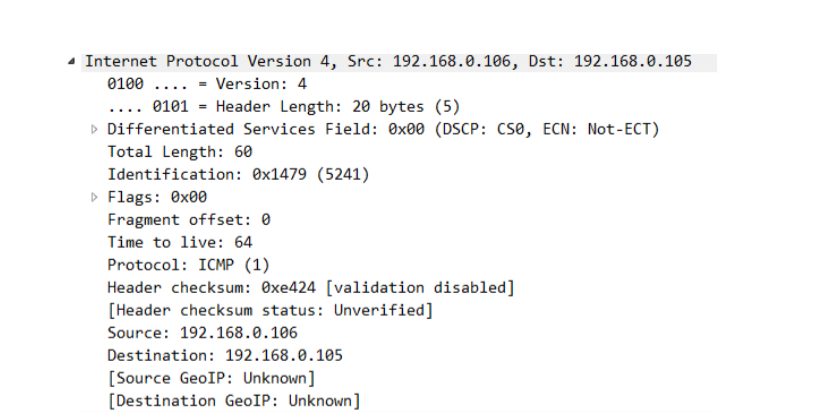
**此时不能捕获报文，因为在通信的时候以太网直接能在ARP表里找到目的主机的MAC地址，所以不在需要通过ARP广播来获得目的主机的MAC。**

* 主机A上和主机B停止进行任何数据通信，5分钟后再次从A向B发PING检测报文，或者从主机B上向主机A发PING检测报文，观察看此时是否能捕获ARP报文。

**此时不能捕获到ARP报文，因为MAC缓存时间是2分钟，如果缓存添加后的两分钟内没有再使用，就会过期，并从ARP表里被删除。**

4、IP协议分析

* 从主机A上向主机B发PING检测报文，捕获IP数据包，记录并分析各字段的含义，并与IP数据包格式进行比较;



**使用IPv4**

**首部长度20bytes**

**区分服务**

**总长度60bytes**

**标识5241，标志0，片偏移0，说明没有分片**

**生存时间（跳数），现在指最多经过的路由器，以前指生存时间**

**ICMP，说明这个数据包还要被ICMP协议封装**

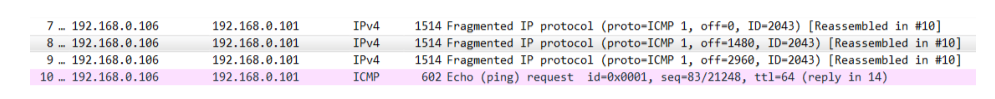
**首部检验**

**源主机和目的主机的IP地址**

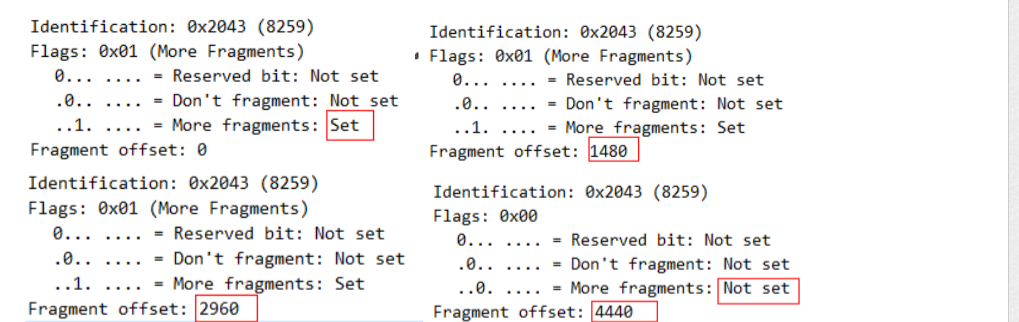
* 使用ping命令，制定数据包长度，如ping -l 2000，使用嗅探器观察IP分片情况，并分析**分片和重组**过程。



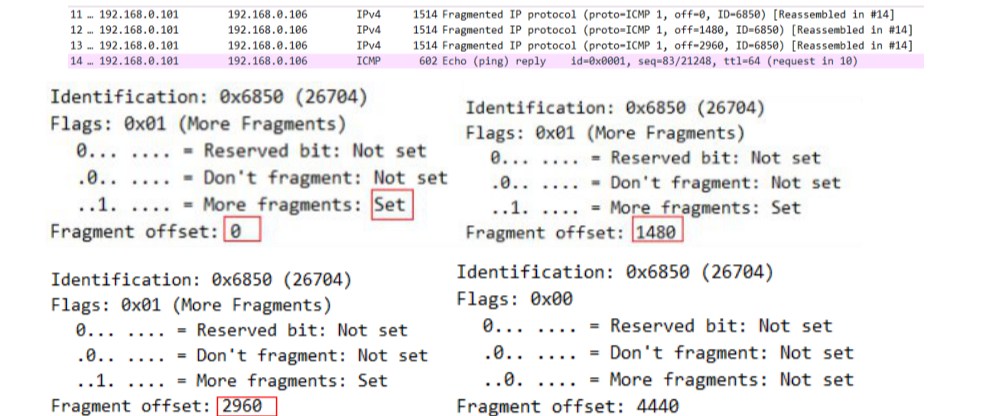
**第一个数据包发送过程：**



**分片过程：四个分片同一个标识，说明这属于同一个数据包，MF为1标识后面还有分片，通过四个包的片偏移量来看，每个数据包最多有1480Bytes。**



**重组过程：IP协议通过MF判断后面是否还有分片，以及通过偏移量来计算各个分片的顺序，以便重组。**

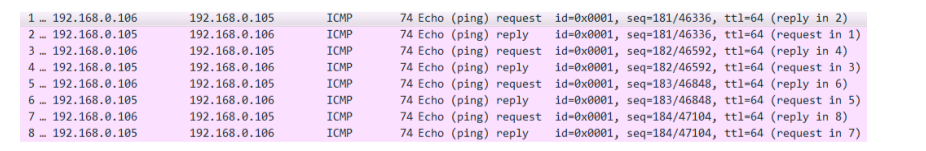


1. ICMP协议分析

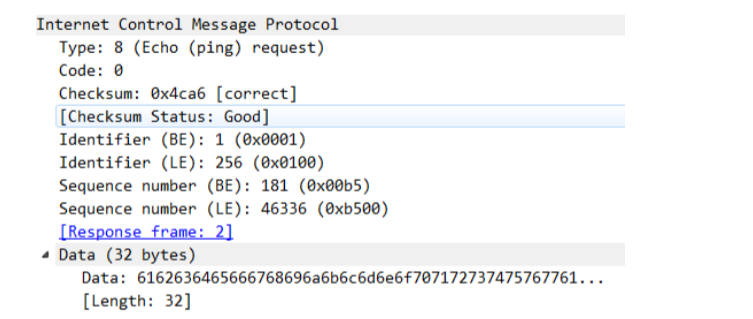
通过ping和tracet命令，了解ICMP协议的使用。

* 从主机A上向主机B发PING检测报文，捕获ICMP请求数据包和应答数据包，记录并分析各字段的含义，并与ICMP数据包格式进行比较；如果返回的差错信息，请分析是由于什么差错引起的。

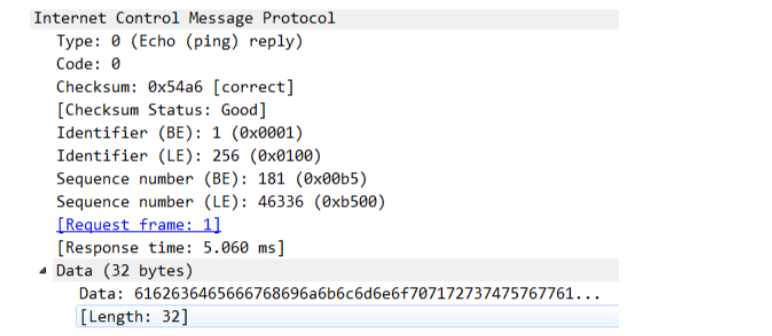
**四个请求四个答复数据包。**



**请求数据包：**



**答复数据包：**



**类型：请求或者答复**

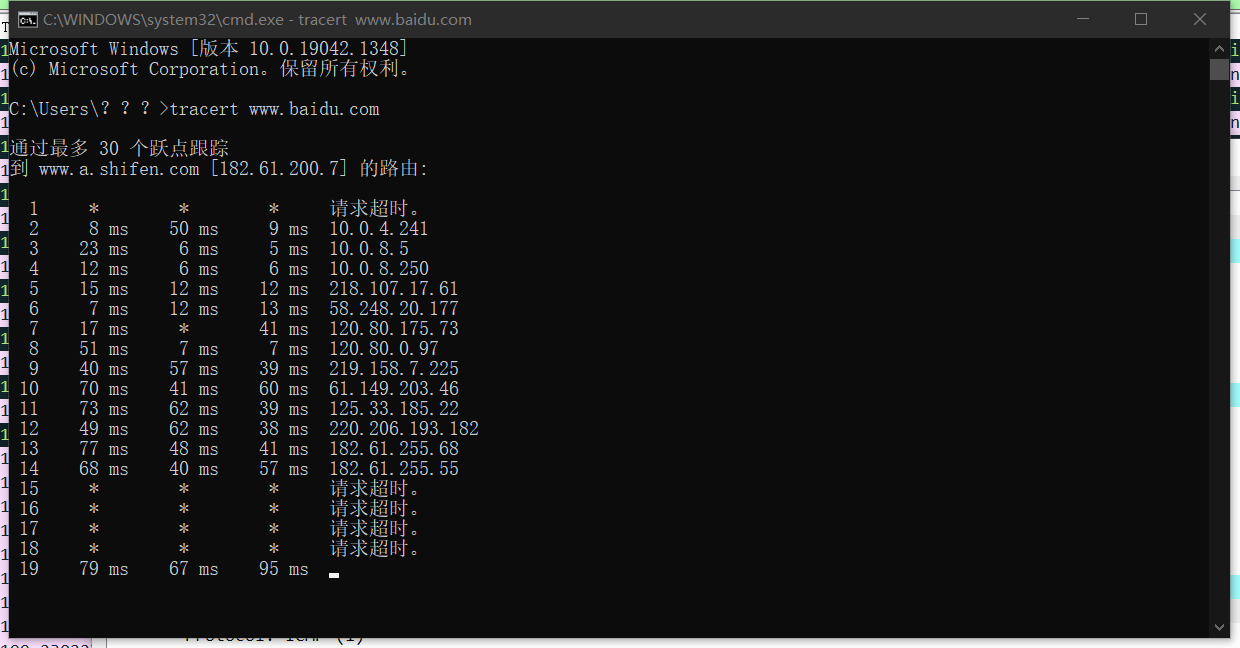
**校验和：correct代表数据正确**

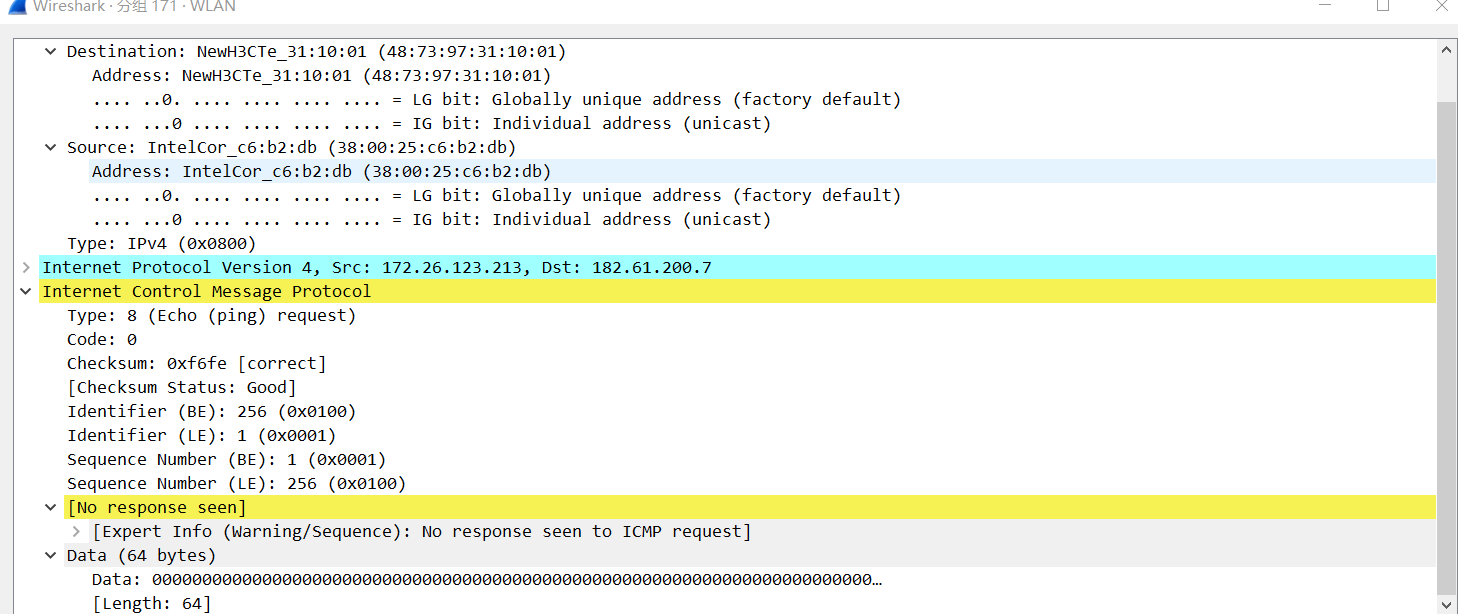
**序号：请求为“1”，回复为“2”，应答数据包的序号为所对应请求数据包的序号+1**

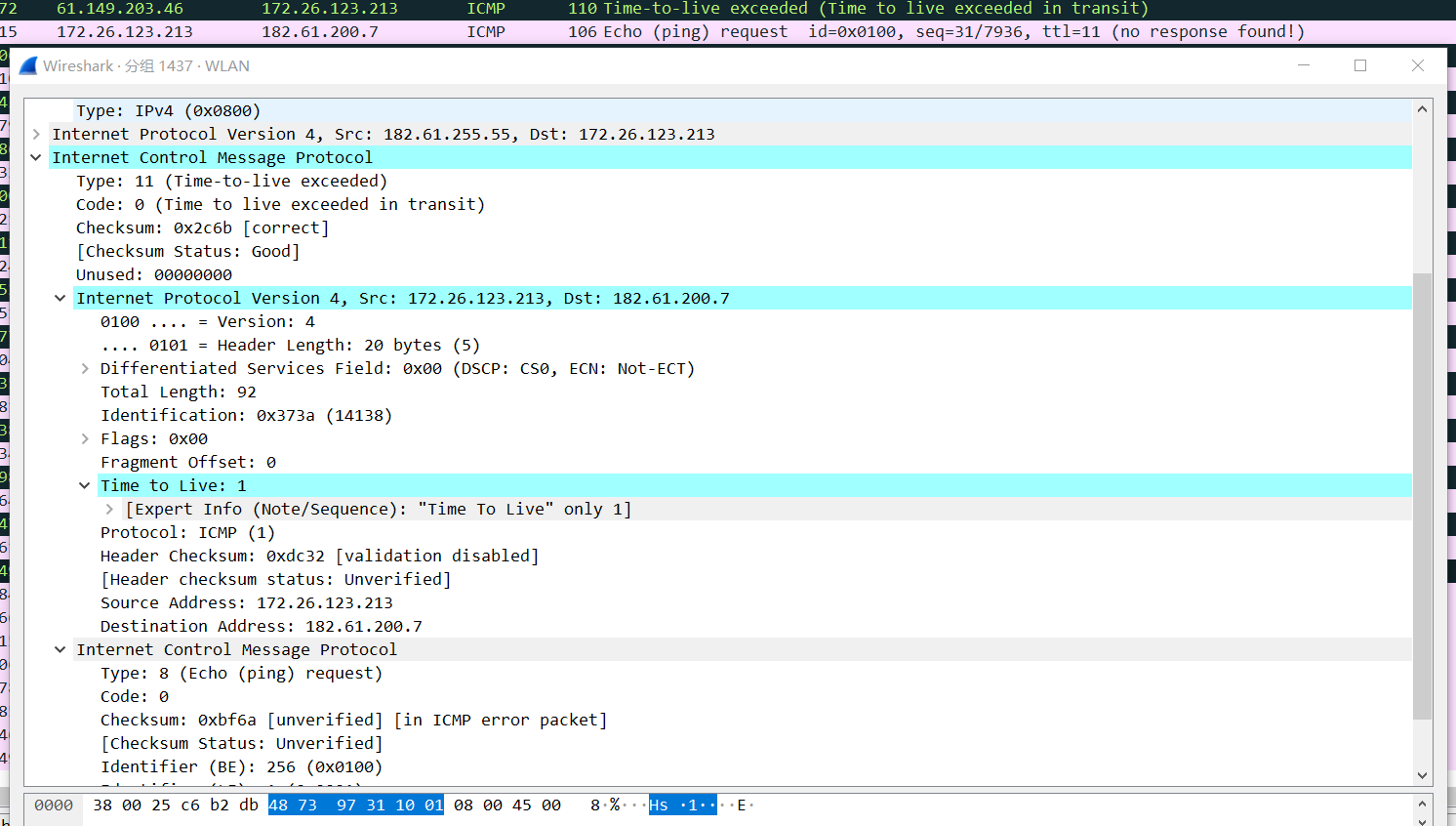
**响应时间**

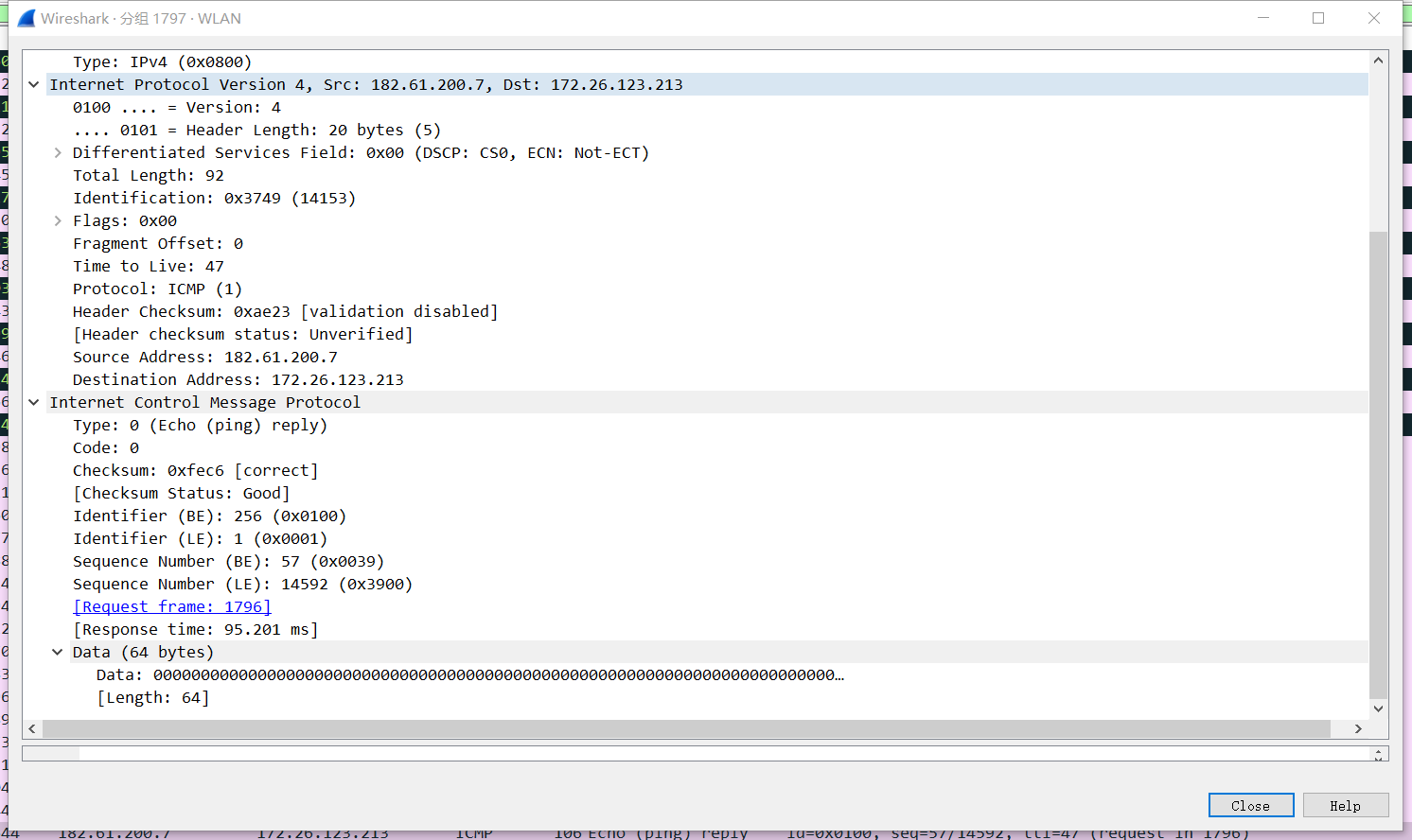
**数据**

* 使用tracert命令，跟踪某台主机，使用wireshark捕获数据包，分析不同类型ICMP响应数据包格式（如type=8,type=0,type=11）。分析tracert工作原理。









**tracert命令用于确定 IP数据包访问目标所采取的路径，显示从本地到目标网站所在网络服务器的一系列网络节点的访问速度，最多支持显示30个网络节点。**

**ICMP报文类型有三种：分别是代码为0、8和11的报文。代码为0 的报文是答复报文，代码为8的报文是请求报文，代码为11的报文是超时报文。超时报文里除了常规的ICMP报文字段外，还封装了IPv4协议和超时的ICMP请求报文。**

**Tracert命令的工作过程：从源主机向目标主机发送IP数据报，并按顺序将TTL设置为从1开始递增的数字（假设为N），导致第N个节点（中间节点 or 目标主机）丢弃数据报并返回出错信息。源主机根据接收到的错误信息，确定到达目标主机路径上的所有节点的IP，以及对应的耗时。**

**【思考题】（分析原因并通过实验验证）**

1. 在ARP包分析实验过程中，为什么A有时能捕获ARP报文，有时却不能捕获ARP报文？

**答：主机A与B一开始进行通信的时候，捕获到了B的MAC地址，并在ARP表中进行缓存操作，只要在主机B的缓存项未过期前进行A与B的通信，源主机就可以直接在ARP表中查询B的MAC，不用进行ARP广播，所以捕获不到ARP报文。**

1. 为什么运行ping 127.0.0.1时，不能捕获到ICMP报文？如果运行ping 本机IP地址能收到报文吗？ 为什么？

**答：因为ping127.0.0.1是回环测试，不会经过本机网卡，没有与其他主机通信，所以没有发送ICMP报文。**

1. 在ping 的过程中，返回信息“Request timed out” 和“Destination Host Unreachable”分别是由哪些情况引起的？

**答：“request timed out”是指数据包经过的路由器路由表中有到达目标主机的路由，只是可能因为对方关机或者请求超时等原因，造成这样的结果。“Destination Host Unreachable”是数据包经过的路由器路由表没有到达目的主机的路由，此时可能是因为DCHP失效。**

4、请通过实验**验证**：

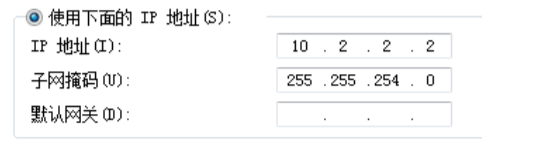
主机如果不设置“网关”，同一网段内的主机可以相互通信。用ping命令测试，用嗅探器测试可以捕获8个ICMP数据包，2个ARP数据包。不同网段的主机不能通信，用PING命令测试，会显示“ Destination Host Unreachable”，因为没有指明网关，无法发送出去，因此显示“目的主机不可达”，用嗅探器捕获不到任何信息。

主机如果设置“网关”，同一网段的主机通信不通过网关转发，用ping命令测试，用嗅探器可以捕获所有测试数据包，能看到对方主机的MAC地址。不同网段的主机之间通信需要网关转发，用ping命令测试，能看到网关的MAC地址（包括能通信或不能通信）。

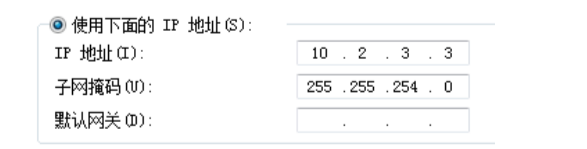
5、通过下面实验**理解网关**

假设主机A的IP地址为10.2.2.2/23，主机B的IP地址为10.2.3.3/23，两台主机均不设置网关，用ping命令测试两主机的连通性，用ARP命令查看物理地址。对结果进行分析。

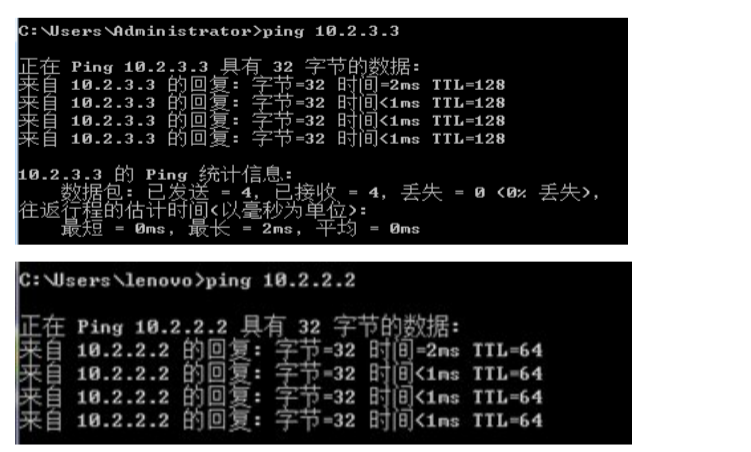
**主机A的配置：**



**主机B的配置：**



**A Ping B &B ping A（都可以通信）:**



**查看ARP表也发现了对方的MAC：**

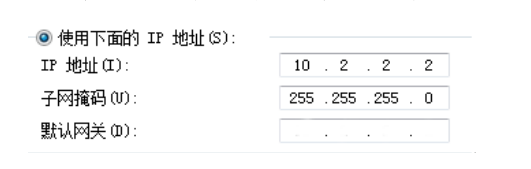


**捕获数据包：**

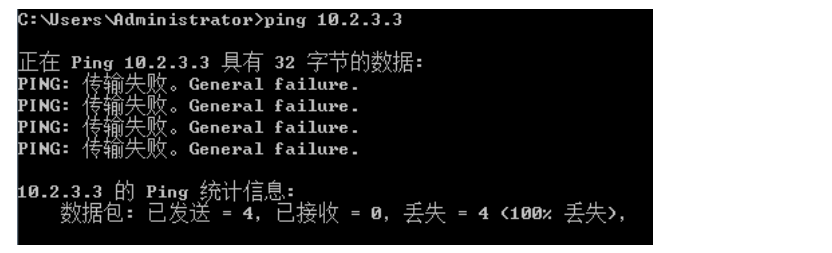


假设主机A的IP地址为10.2.2.2/24，主机B的IP地址为10.2.3.3/23，两主机不设置网关，分别在主机A和主机B上用ping测试与对方的连通性，用ARP查看物理地址。对测试结果进行分析。

**主机B配置不变，A的配置改为：**



**通信失败：**



**ARP没有找到B的MAC：**

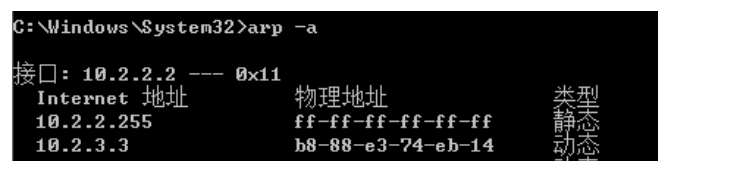


**结果是因为：A将B的IP地址与自己的子网掩码进行与运算后，得到的网络前缀为（10.2.3.0）与A的网络前缀（10.2.2.0）不一样，所以A与B在通信的时候显示传输失败，因此也导致A的ARP表中没有B的MAC地址。**

**B ping A（请求超时）:**



**查看A的ARP表（找到了B的MAC地址）：**



**结果是因为：B将A的IP地址与自己的子网掩码进行与运算，发现A与自己的网络号相同（10.2.2.0），所以B能在广播中找到A的MAC地址，并向A发送报文，但是A不能向B发送回复报文，所以显示请求超时而不是目的主机不可达，又因为B能向A发送ARP请求，所以在双方的ARP表中可以看到对方的MAC地址。**