**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 7 实验项目类型 实验地点 计网实验室

学生姓名 张光华 学号 2019053296

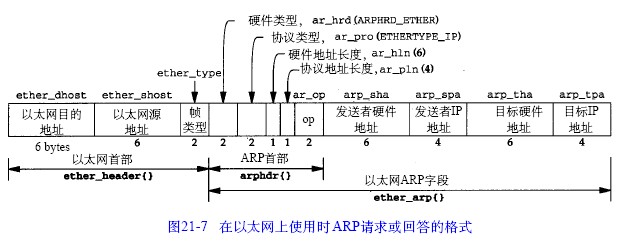
学院 智能科学与工程学院 系 19级 专业 信息安全

实验时间 2021 年11月1日 午～11月14 日 午 温度 21 ℃湿度

1. **实验目的**
2. 理解链路层、网络层主要协议格式，以及协议的工作原理
3. 理解网关和子网掩码概念
4. 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
5. 学会使用ping、tracert、arp等命令并使用嗅探器分析其工作过程。
6. **实验内容和要求**
7. 用嗅探器捕获数据包。
8. 分析以太网帧、ARP协议、IP协议、ICMP协议格式
9. 分析PING、TRACERT、ARP命令的工作过程
10. 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。
11. **主要仪器设备**

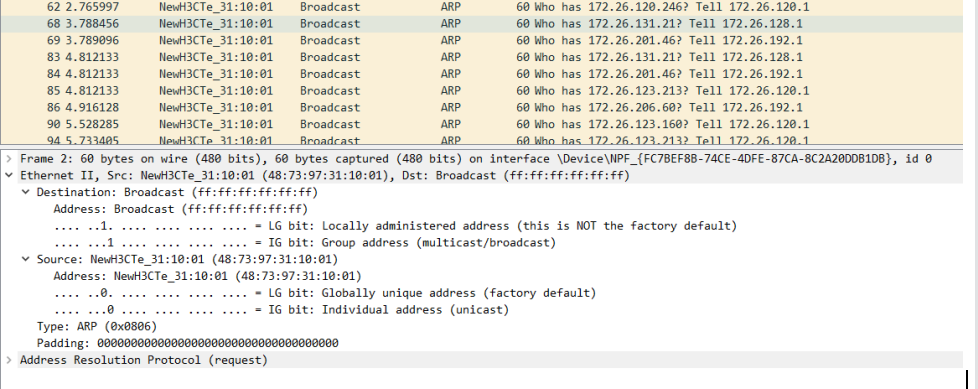
**仪器：**一台二层交换机(S2126G)，一台三层交换机(S3550)，二台PC机。

**实验环境：任何网络环境**



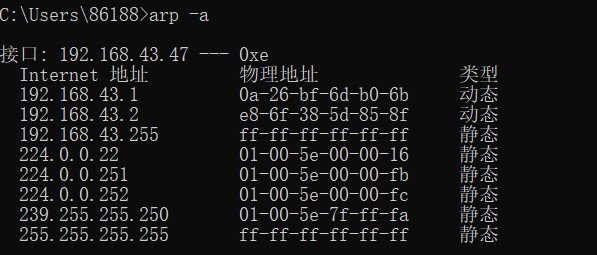
1. **实验过程**
2. 以太网协议分析

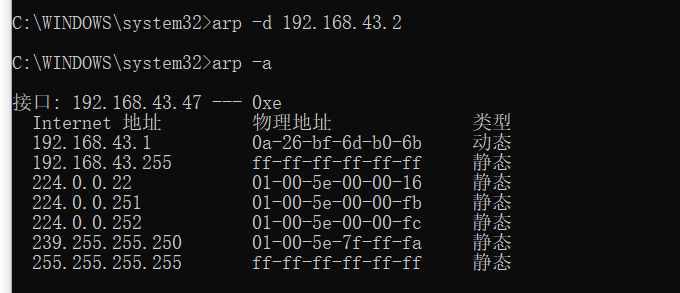
主机A上向主机B发PING检测报文，使用Wireshark 捕获数据



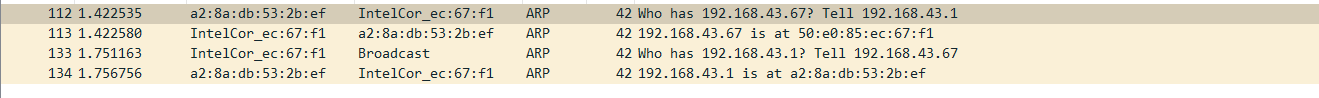
1. ARP协议分析

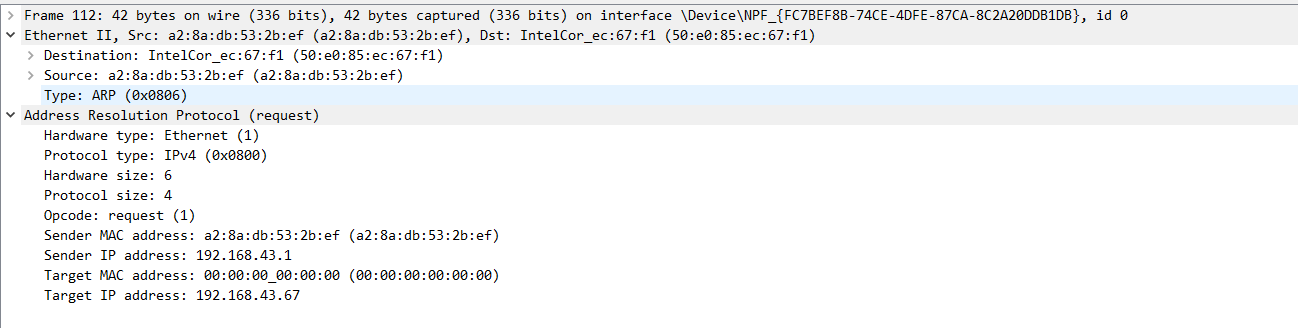
* 进入DOS窗口，用arp – a 查看本机上的ARP表的情况，然后用 arp –d B 删除B的记录（如果有的话）；





* 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；

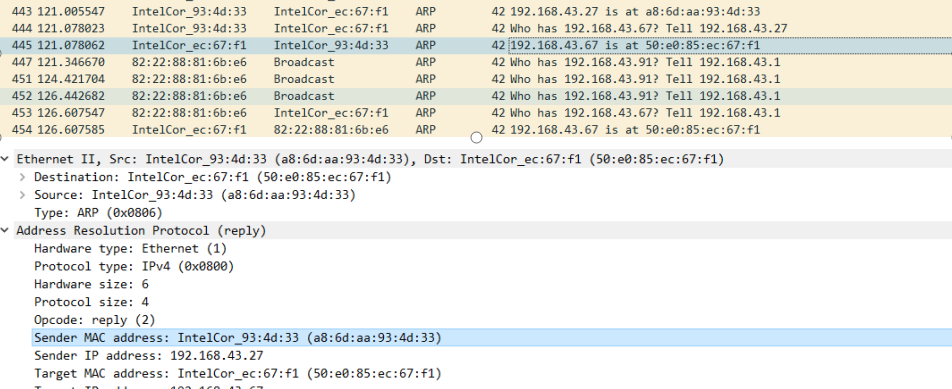




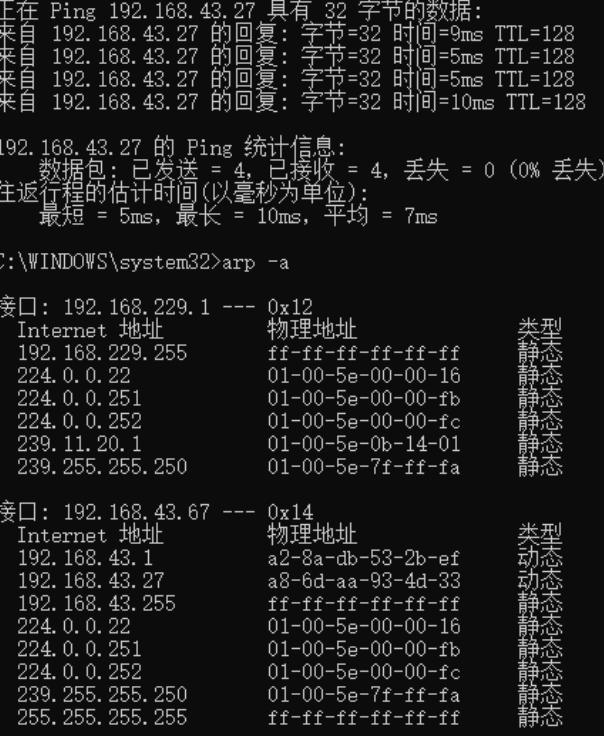
硬件的类型是1，表示以太网，表明ARP实现在以太网类型的网络上；协议的类型是IPv4，用十六进制表示是0x0800，硬件地址长度是6字节，协议地址长度是4字节，ARP报文类型是1的话，说明是请求报文，发送源的MAC地址是a2:8d:db:53:2b:ef，ip地址是192.168.43.1(网关地址)；目的主机的MAC地址是00:00:00\_00:00:00，ip地址是192.168.43.47。

* 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；

上面arp协议分析是同样的思路。



* 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；

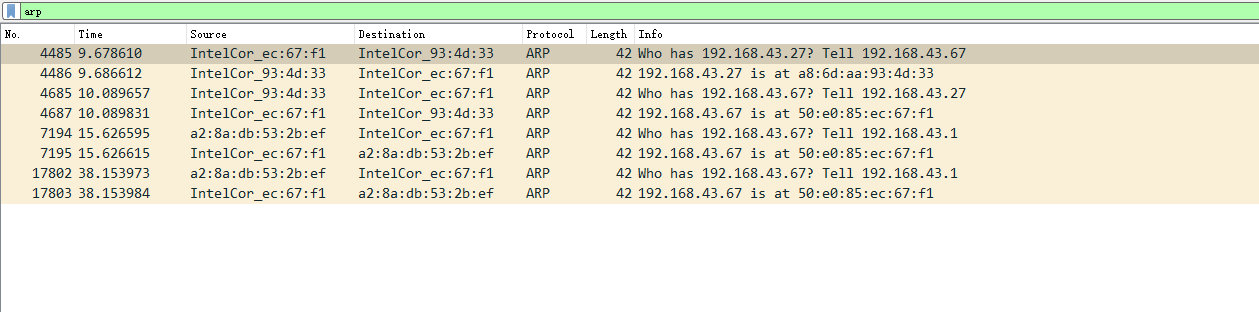


* 再次从主机A上向主机B发PING检测报文，或者再次从主机B上向主机A发PING检测报文，观察看此时是否能捕获ARP报文；

此时ARP表里面有主机B的MAC地址，以太网可以直接获取，所以不需要通过广播去获取B的MAC地址。

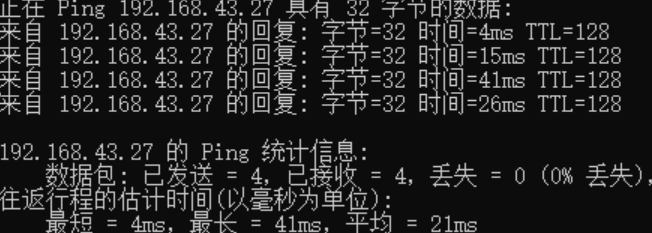
* 主机A上和主机B停止进行任何数据通信，5分钟后再次从A向B发PING检测报文，或者从主机B上向主机A发PING检测报文，观察看此时是否能捕获ARP报文。

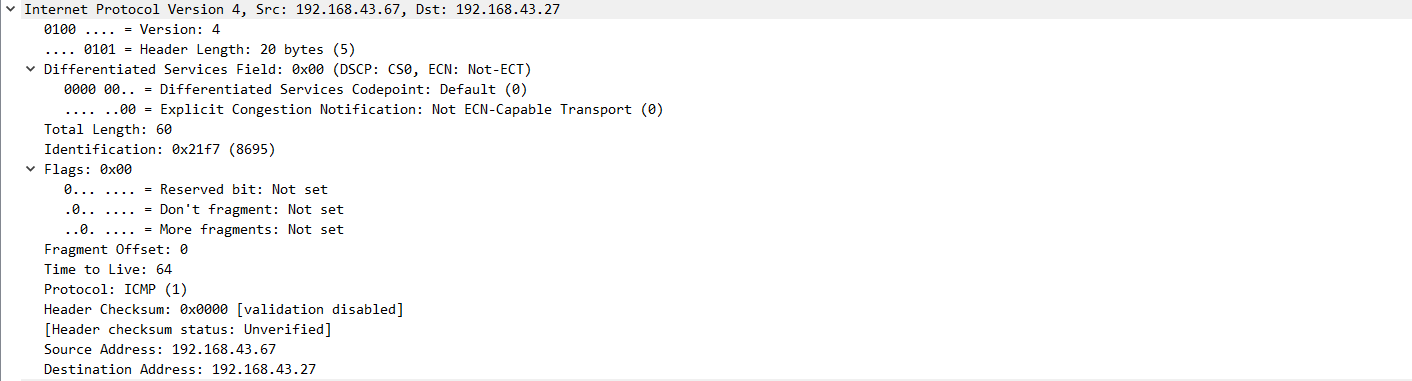
可以捕获到arp报文如下；



3、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;





由上可知；协议是IPv4，源主机的ip是192.168.43.67，目的主机的ip是192.168.43.27。首部长度为20个字节，总长度为60，标识为8695，flag是0，片偏移也是0，生存时间是64，协议类型是ICMP，首部检验和是0x0000。

* 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。



首部长度是20字节，总长度=首部长度加数据段长度=20+1480=1500，DF=0表示可以分片，MF=1，即后面还有分片。

**说明：**为了重组数据报分片，接收主机在第一个分片到达时分配一个存储缓冲区。当数据报的后续分片到达时，数据将被复制到缓冲区存储器中片偏移量字段指出的位置。当所有分片都到达时，完整的未分片的原始数据报就被恢复了。

4、ICMP协议分析

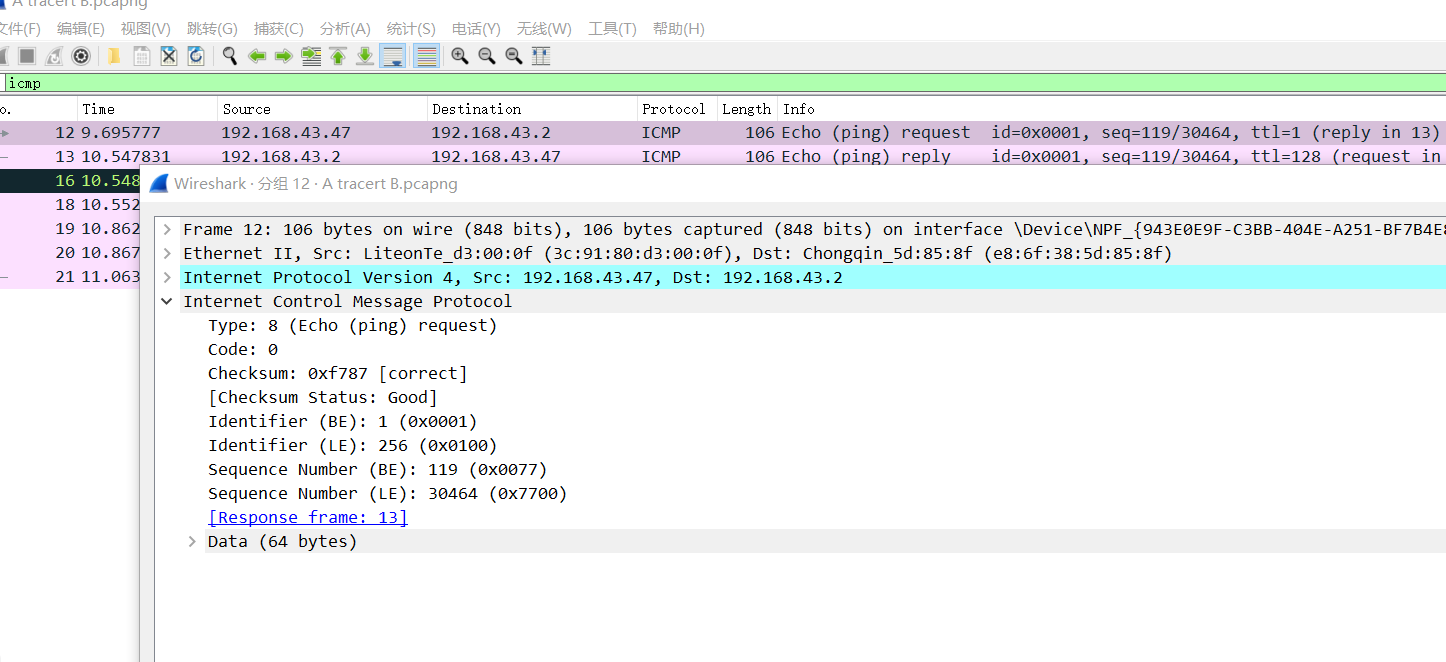
通过ping和tracet命令，了解ICMP协议的使用。

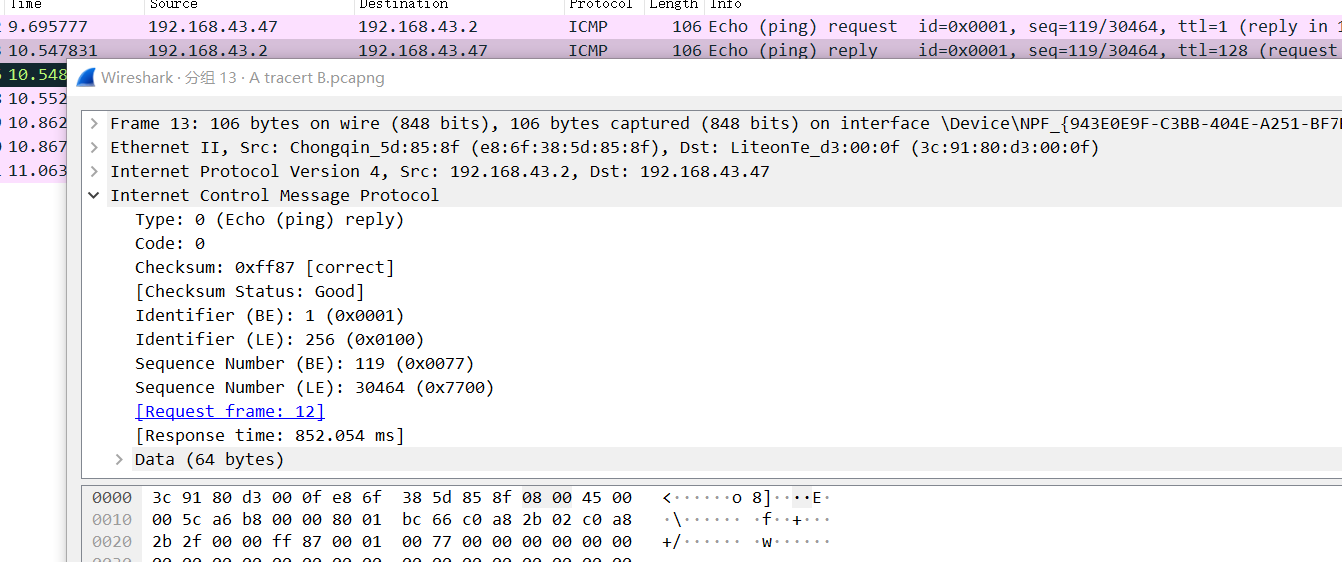
* 从主机A上向主机B发PING检测报文，捕获ICMP请求数据包和应答数据包，记录并分析各字段的含义，并与ICMP数据包格式进行比较；如果返回的差错信息，请分析是由于什么差错引起的。
* **书上的参考表：**

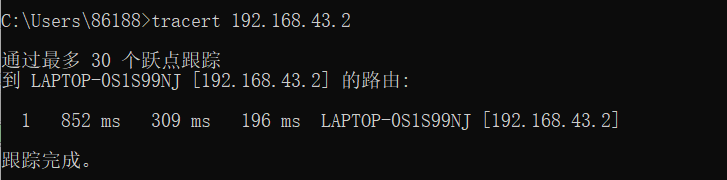
| **ICMP报文种类** | **类型的值** | **ICMP报文的类型** |
| --- | --- | --- |
| 差错报告报文 | 3 | 终点不可达 |
| 差错报告报文 | 11 | 时间超过 |
| 差错报告报文 | 12 | 参数问题 |
| 差错报告报文 | 5 | 改变路由(Redirect) |
| 询问报文 | 8或0 | 回送(Echo)请求或回答 |
| 询问报文 | 13或14 | 时间戳(Timestamp)请求或回答 |

* 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。

Type=0,8同上。







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 先发送 TTL 为 1 的回应数据包，并在随后的每次发送过程将TTL递增 1，直到目标响应或 TTL 达到最大值，从而确定路由。通过检查中间路由器发回的“ICMP 已超时”的消息确定路由。某些路由器不经询问直接丢弃 TTL 过期的数据包，这在 Tracert 实用程序中看不到。

1. **实验结果与分析（思考题）**
2. 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？

如果主机的ARP高速缓存里含有当前想要访问主机IP及其MAC地址，则无需广播寻找，所以有时能捕获到ARP报文有时不能。

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？

ping127.0.0.1属于环回测试，只是检查本地TCP/IP协议是否设置，并不会经过网卡，所以没有存在通信这一过程，因此不能捕获到ICMP报文。ping本机也不能收到报文

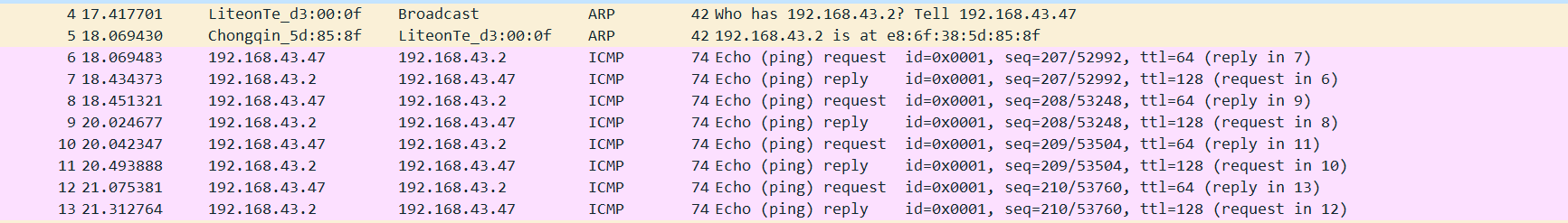
1. 在ping 的过程中，返回信息“Request timed out” 和“Destination Host Unreachable”分别是由哪些情况引起的？

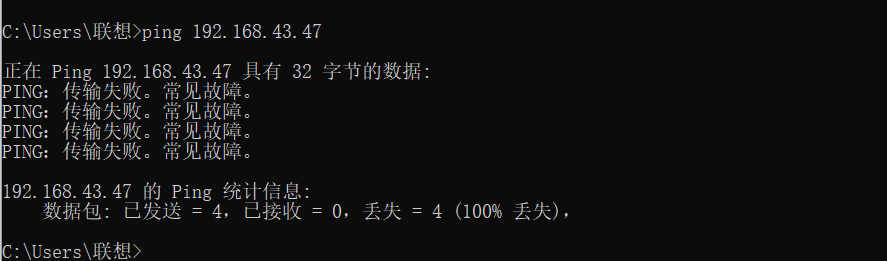
“Request timed out” 指虽然源主机的路由表具有到达目标的路由，但是由于一些原因无法到达，便会出现请求超时的提示，可能是因为对方防火墙没关，或者ip不匹配；“Destination Host Unreachable”表示路由表中没有到达目标的路由。

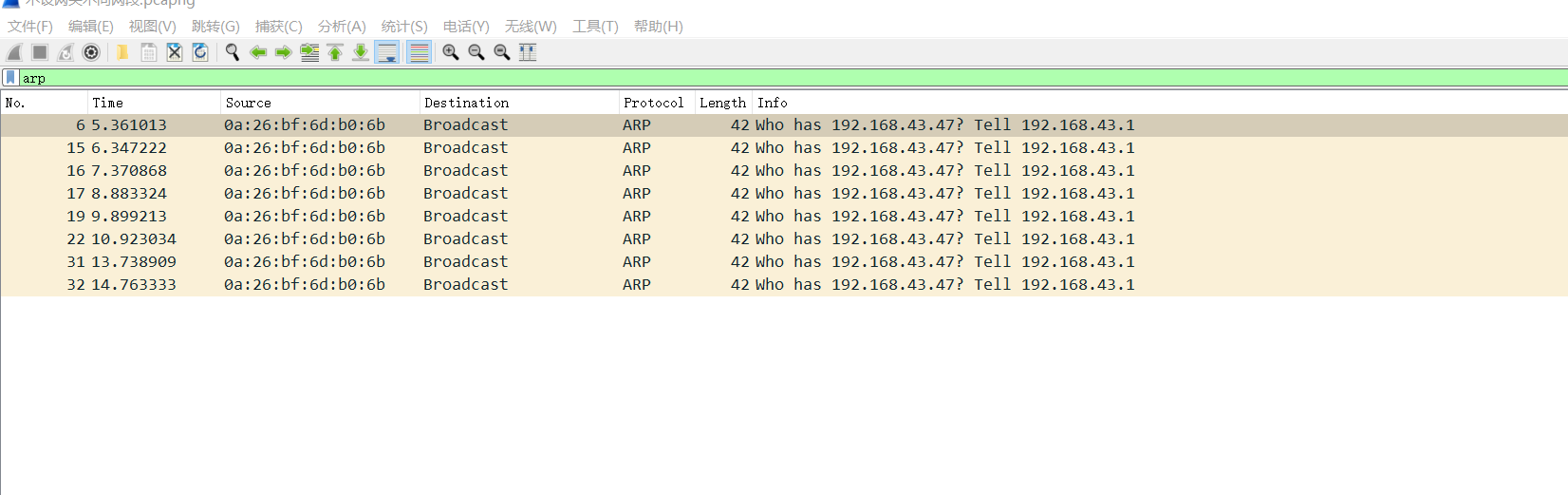
4、请通过实验**验证**：

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。

不设置网关，同一网段







只有广播没有回复。

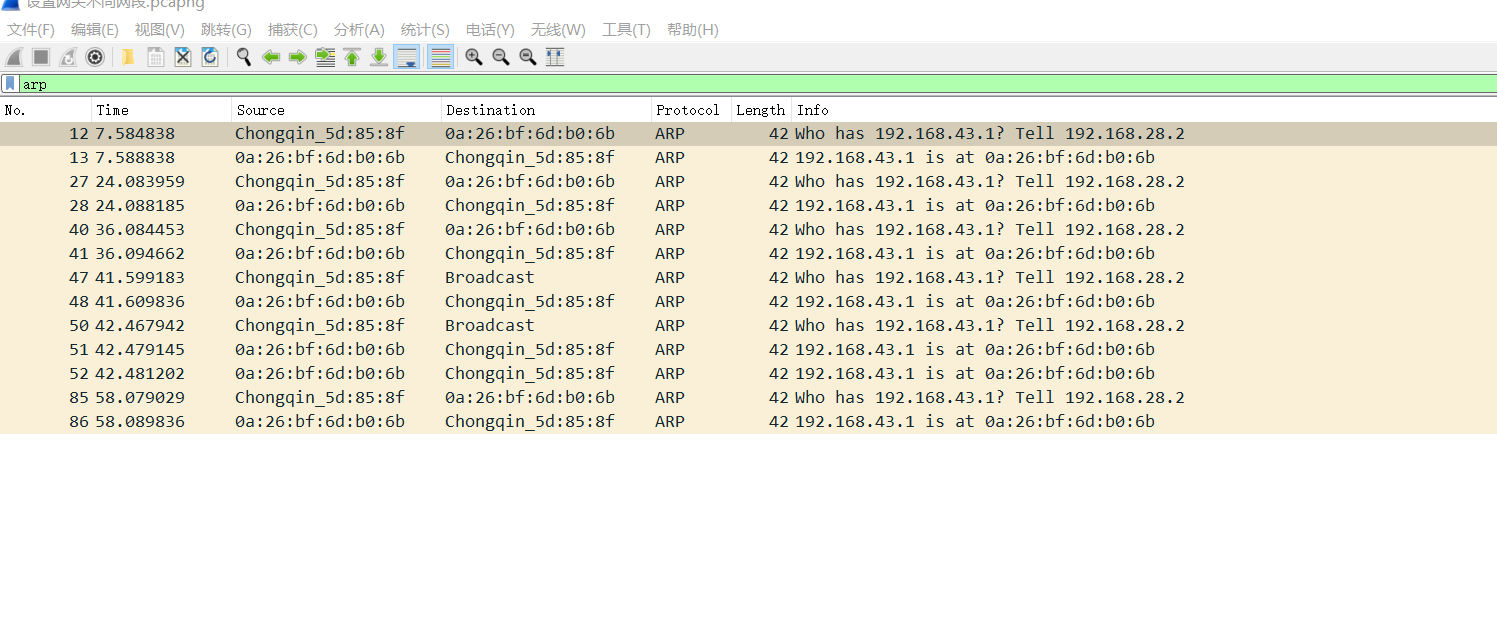
主机如果设置“网关”，同一网段的主机通信不通过网关转发，用ping命令测试，用嗅探器可以捕获所有测试数据包，能看到对方主机的MAC地址。不同网段的主机之间通信需要网关转发，用ping命令测试，能看到网关的MAC地址（包括能通信或不能通信）。

设置网关同一网段



可以捕获到目的主机的mac地址，不经过网关。

设置网关不同网段



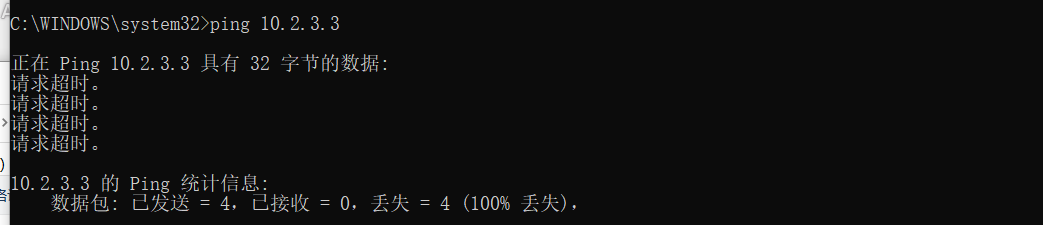
可以看到本机的mac地址和网关的mac地址，但捕获不到目的主机的mac地址。

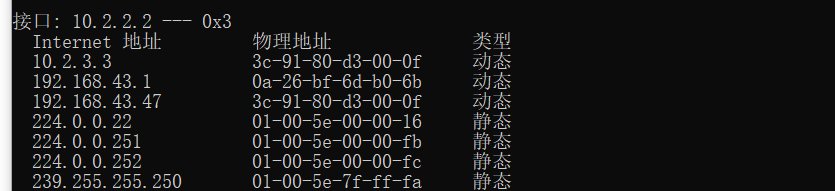
1. 通过下面实验**理解网关**

**给的两种IP地址都在同一网段，于是将第一种设为了不同网段。**

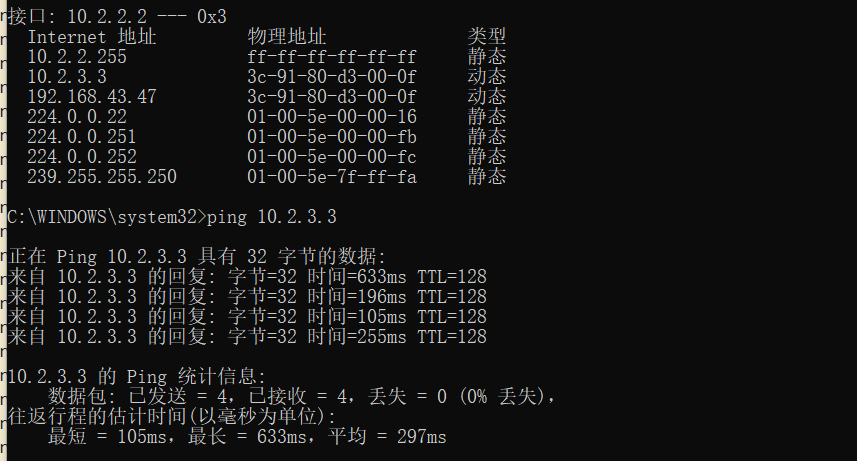
假设主机A的IP地址为10.2.2.2/24，主机B的IP地址为10.2.3.3/24，两台主机均不设置网关，用ping命令测试两主机的连通性，用ARP命令查看物理地址。对结果进行分析。

不同网段不设网关，结果不通。



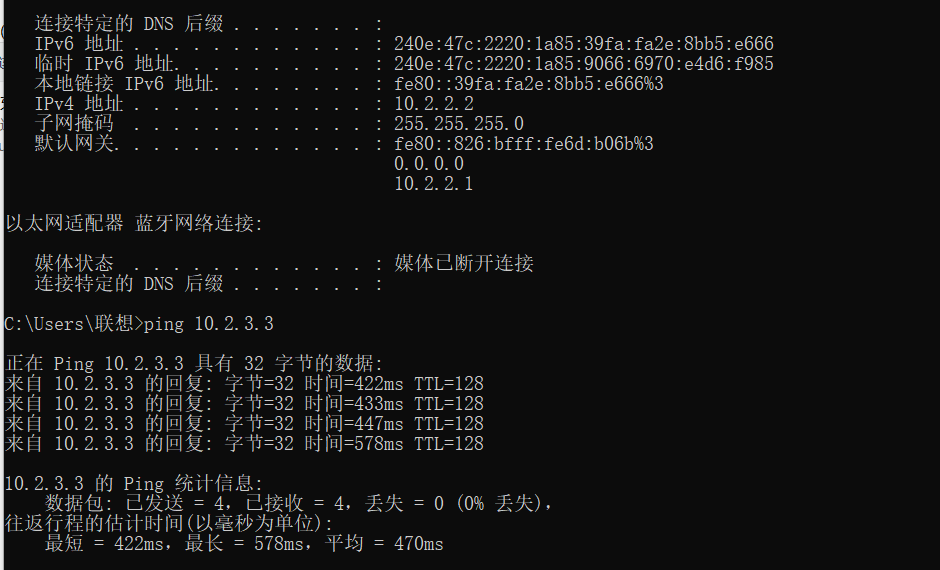


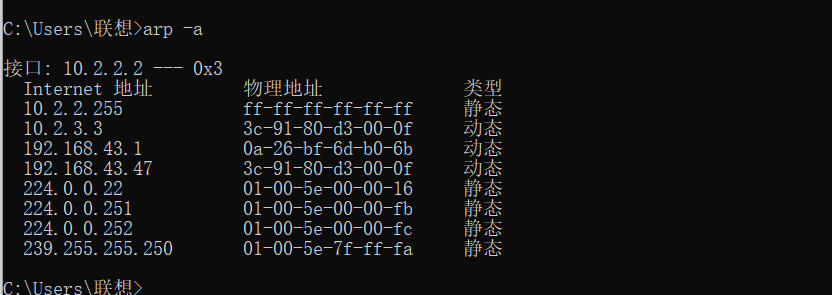
不同网段设置网关。结果是ping通了，但可能由于自己电脑有多个网关被设置了的原因，导致ping通的同时，也存在了ARP表中。



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。

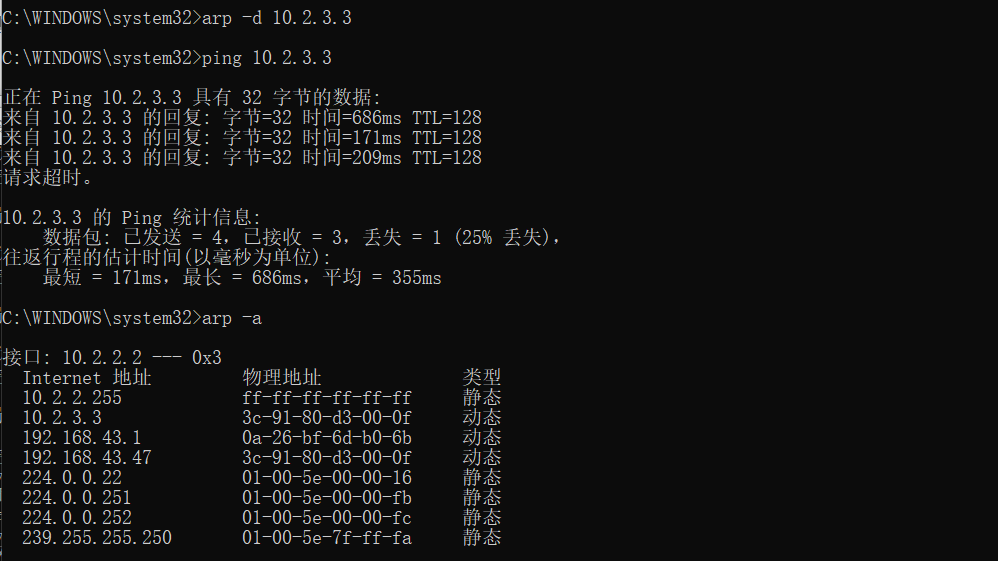
同一网段设置网关，两主机间可以ping通。且地址存在ARP表中。





针对上述情况，分别将主机的网关设置为本机地址，观察测试结果，并分析原因。

同一网段不设网关同样两主机可以ping通。

****

ping的通，arp有对方的物理地址。

**暨南大学本科实验报告专用纸(附页)**