**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 07 实验项目类型 验证型 实验地点 B402

学生姓名 叶世翔 学号 2019051122

学院 智能科学与工程 系 专业 信息安全

实验时间 2021 年 11 月 9 日 下 午～ 11 月 10 日 下 午

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**
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. **实验设备**计算机两台，交换机一台
12. **实验原理**

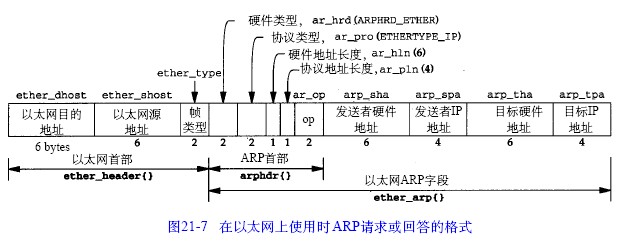
**1、网络嗅探器**

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**



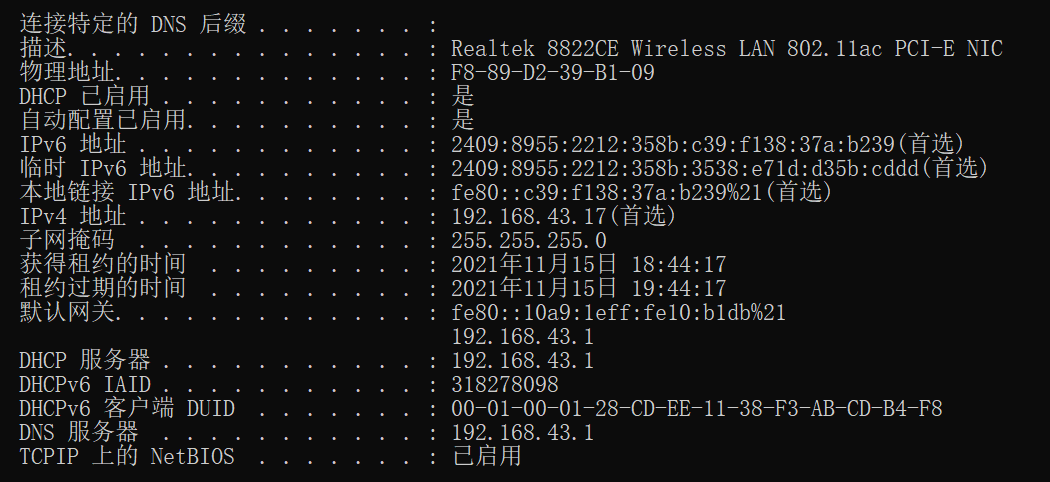
**其他协议数据包格式见教材**。

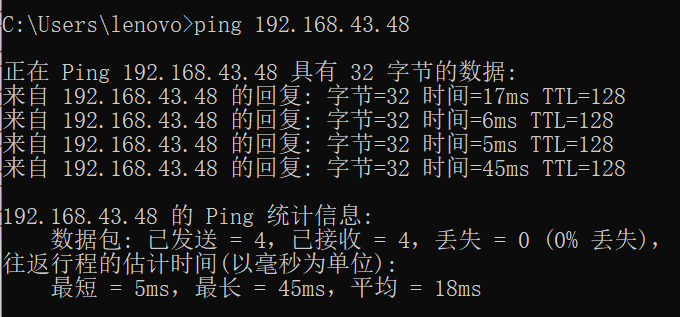
1. **实验步骤**
2. 安装Wireshark
3. 以太网协议分析

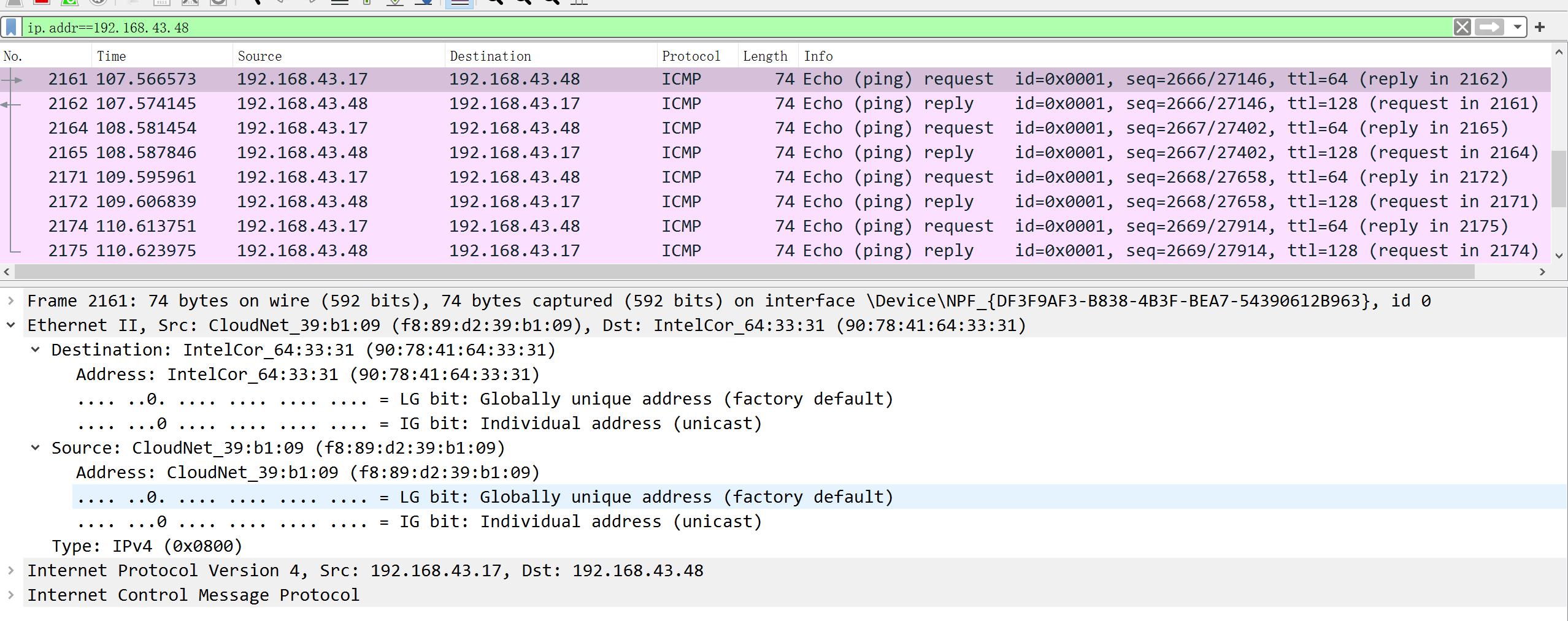
从主机A上向主机B发PING检测报文，捕获以太数据帧，记录并分析MAC帧各字段的含义。

|  |  |  |
| --- | --- | --- |
| 设备 | IP地址 | MAC地址 |
| 主机A | 192.168.43.17 | F8-89-D2-39-B1-09 |
| 主机B | 192.168.43.48 | 90-78-41-64-33-31 |

可知主机A的mac地址为F8-89-D2-39-B1-09





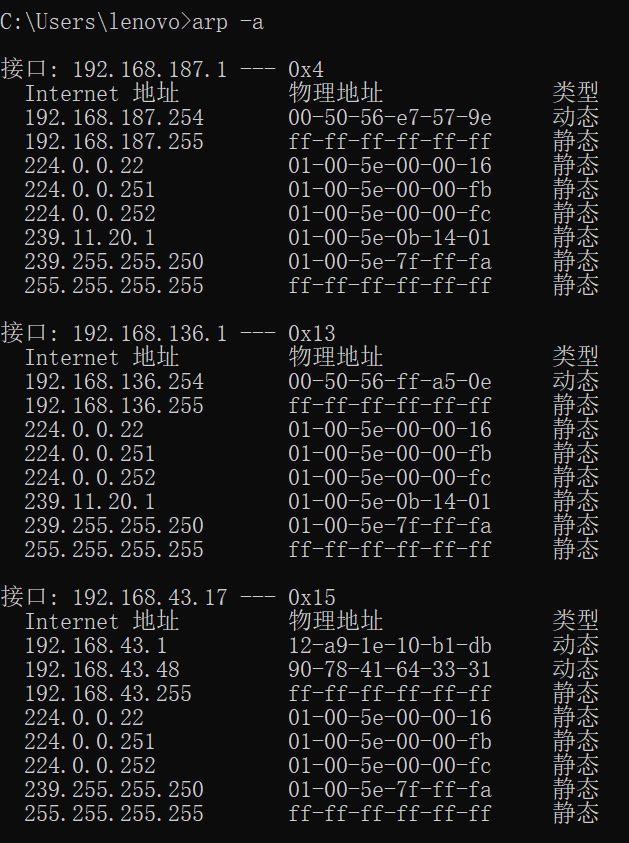


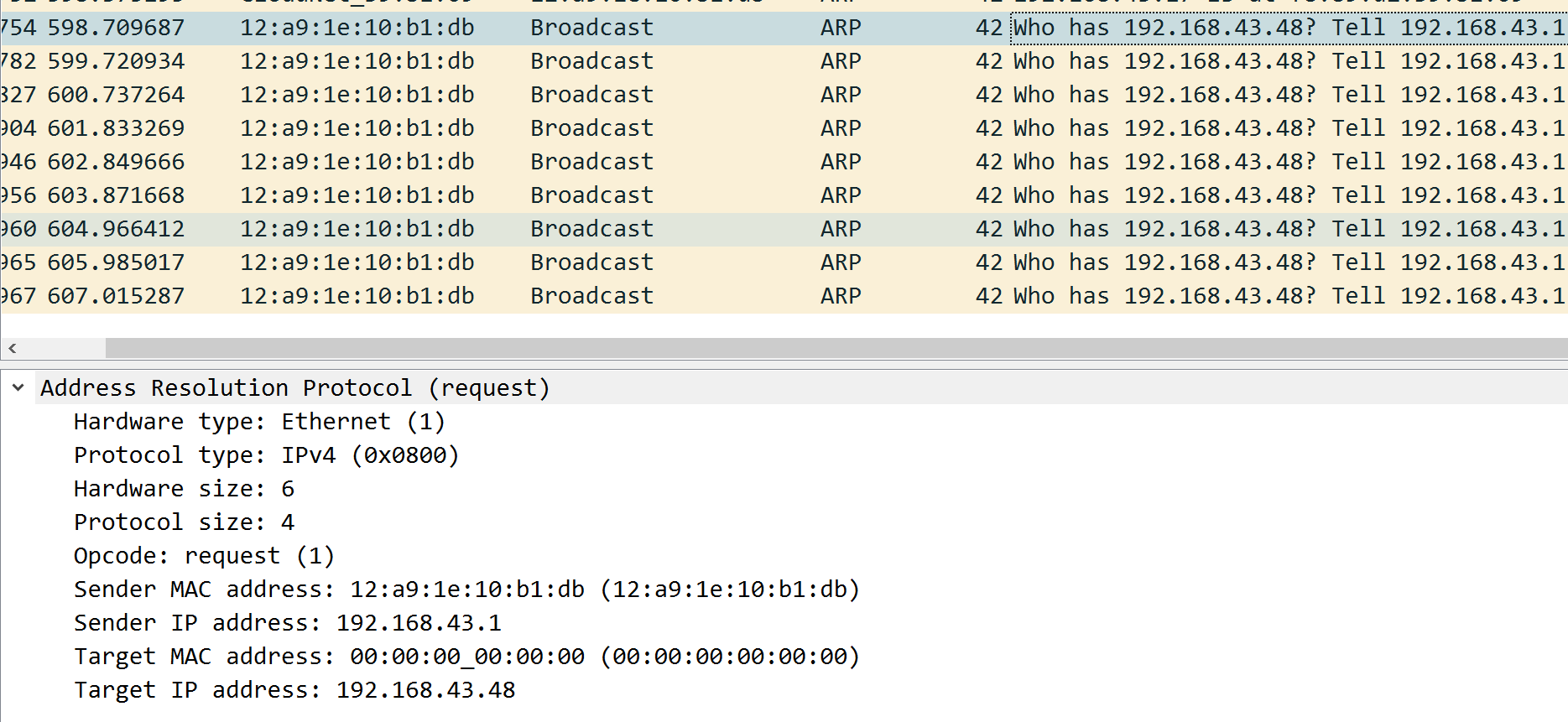
Dst是目的MAC地址。Dst字段长度为6个字节，标识帧的接收者。

Src是源MAC地址。Src字段长度为6个字节，标识帧的发送者。

类型字段（Type）用于标识数据字段中包含的高层协议，该字段长度为2个字节。类型字段取值为0x0800的帧代表IP协议帧；类型字段取值为0806的帧代表ARP协议帧。

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；  
  
Hardware type(硬件地址类型)：该字段表示物理网络类型，，即标识数据链路层使用的是那一种协议，其中0x0001为以太网。

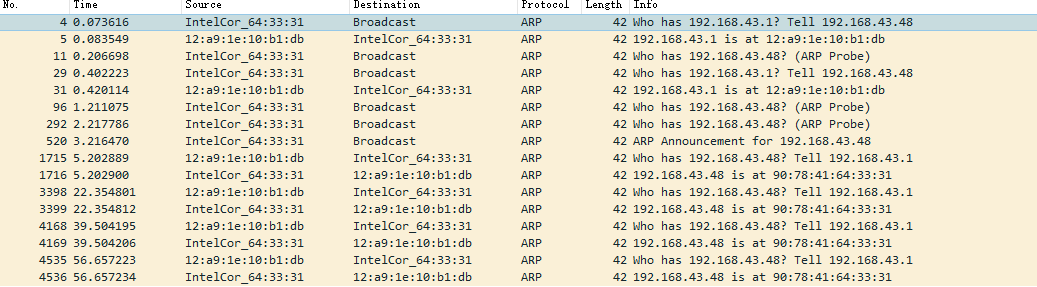
Protocol type(协议地址类型)：该字段表示网络地址类型，即标识网络层使用的是那一种协议，其中0x0800表示为ip。

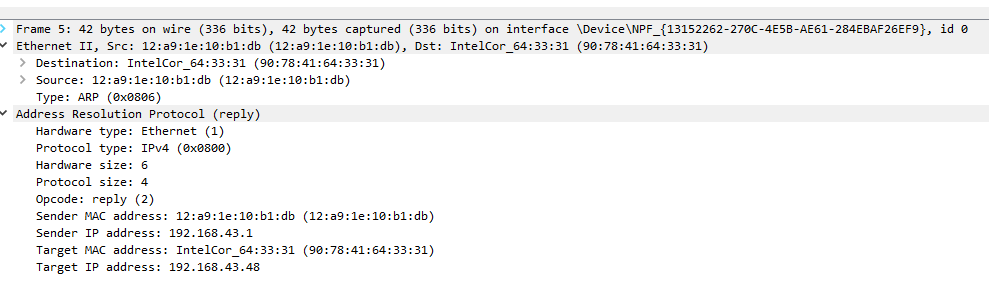
Hardware size(硬件地址长度)：表示源和目的物理地址的长度，单位是字节。

Protocol size(协议地址长度)：表示源和目的的协议地址的长度，单位是字节。

Opcode(操作码)：记录该报文的类型，其中1表示ARP请求报文，2表示ARP响应报文。

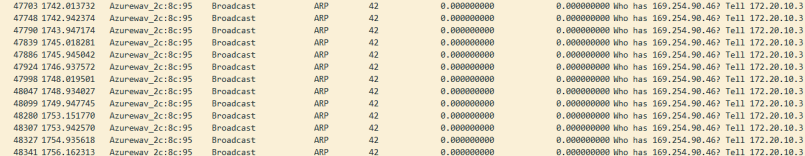
最后是发送方和接收方各自的MAC地址和IP地址，这是广播所以目的mac地址置为全0。

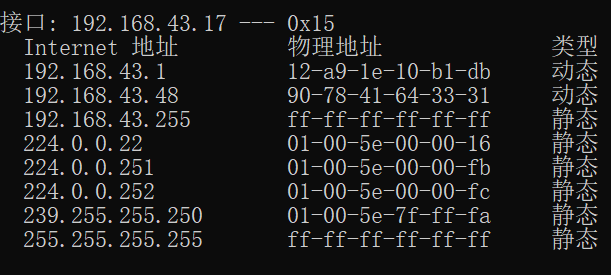




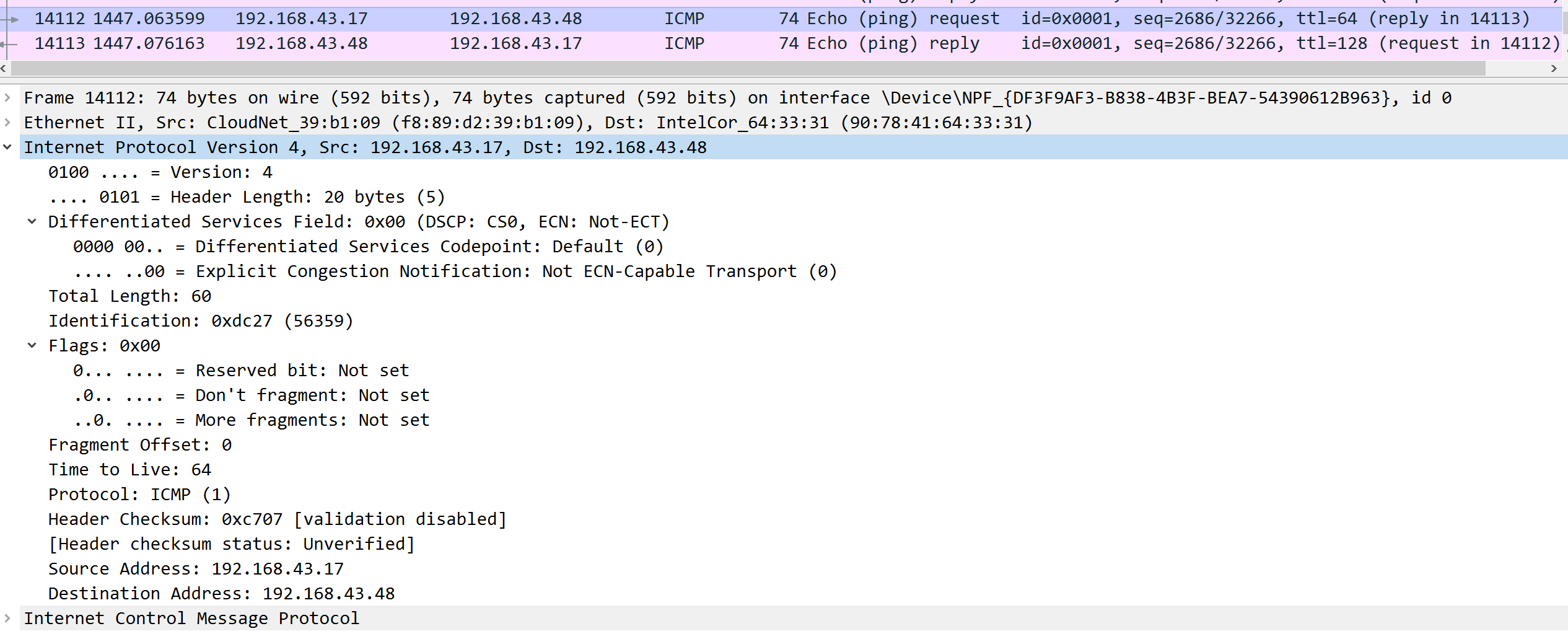
各字段基本相同，除了操作的值为2，表示ARP响应报文。除此之外，响应报文是以单播形式发送的，因为目的地址是确定的。

* 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；  
  捕获不到，因为主机A的ARP表中有主机B的MAC地址，主机Aping主机B时直接从ARP表中获取主机B的MAC地址，而不需要发送ARP包进行获取
* 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。  
   能捕获到，因为五分钟过后ARP表进行了更新，里面没有了主机B的MAC地址

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;  
  
Version:4，说明用的是IPv4

头部长度为20字节

区分服务为0x00，占8位，这里没有使用到这个服务

总长度为60字节

Identification 标识号为0xdc27(56359)，标志为0，片段偏移为0，说明这个数据包长度较小，不需要分片。

生存时间（TTL）为64，说明最多只能经过64个路由器

协议类型为ICMP，说明高层数据包类型为ICMP，所以这个数据包还要再被ICMP协议封装。

首部检验和为0x0000（validation disable，禁用验证）

源主机 IP 为主机A，目的主机IP为主机B  
Differentiated Services Field：区分服务，占8字节。

Total Length表示总长度，占16位，表示为首部长度+数据长度。

Identification是标识，占16位，用来产生IP数据报的表示，通常分片时用。

Flags为标志，占3位，只有最后两位有意义。最后一位MF，如果MF=1表示后面“还有分片”，MF=0表示最后一个分片；倒数第二位DF，如果DF=0表示分片后的分组允许继续分片，DF=1表示不能分片。

Fragment offset表示片偏移，占13位，指出较长的分组在分片后，某片在原分组中的相对位置，并且是以8个字节为偏移单位。

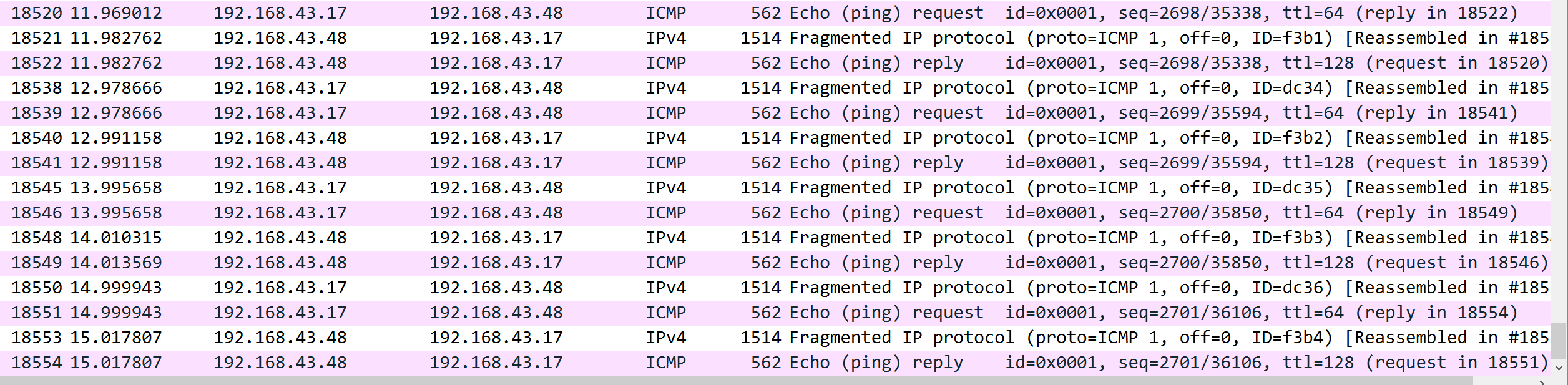
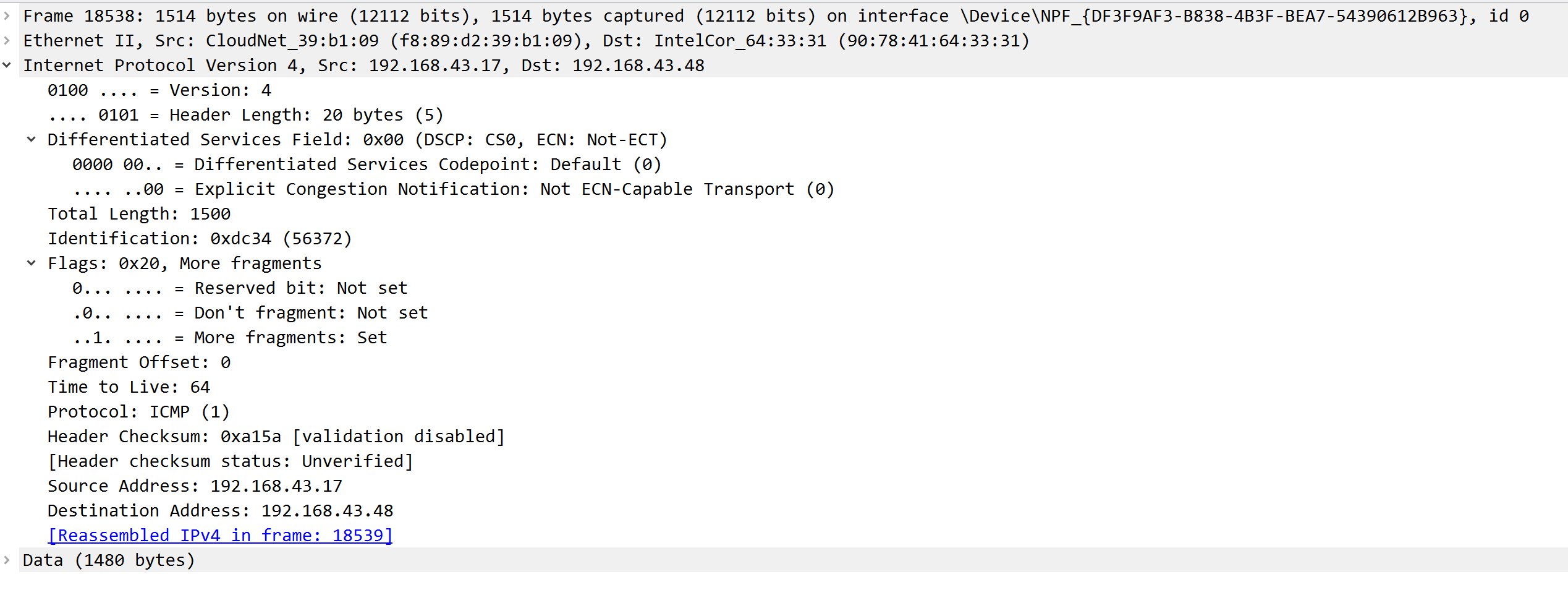
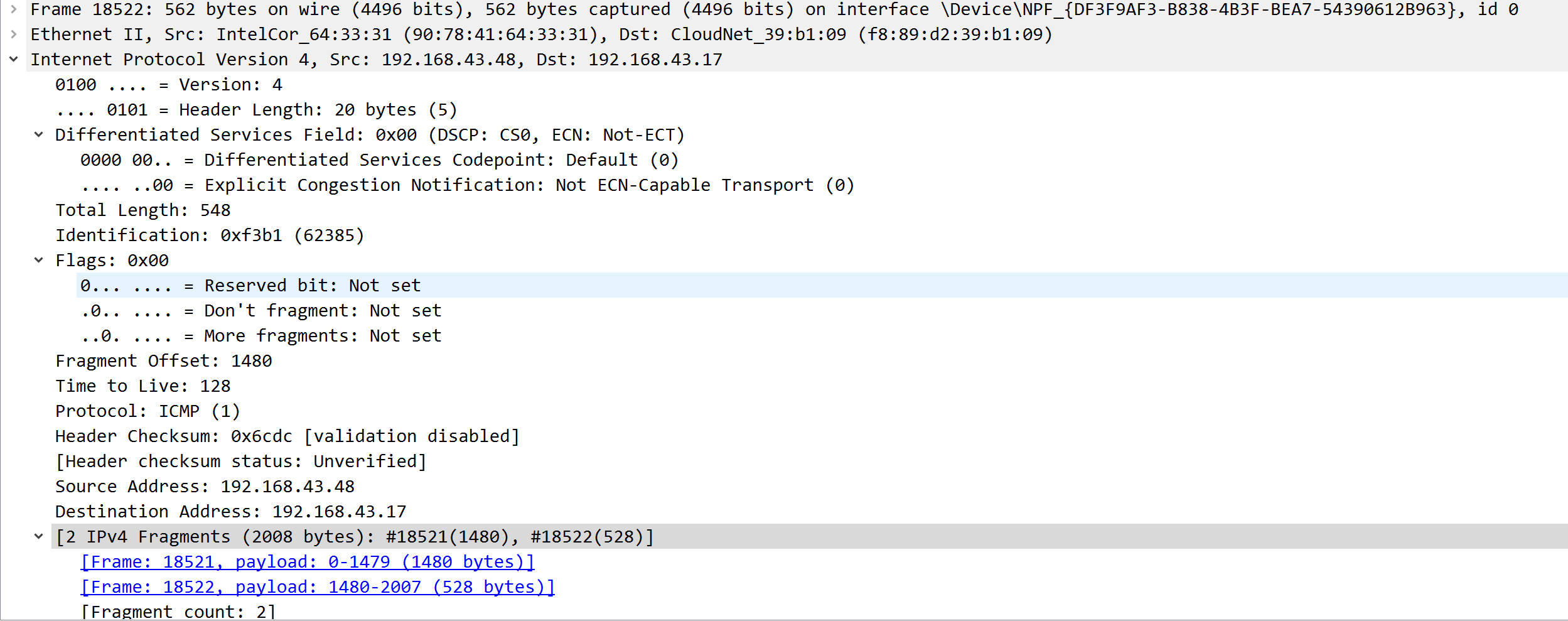
Time to Live表示生存时间，占8位，记为TTL（Time To Live），指示数据报在网络中可通过的路由器数的最大值，这里为128表示可以通过128个路由器寻找目的主机，超过128个路由器发送的数据报将被丢弃

Protocol是协议，占8位，指出此数据报携带的数据使用何种协议，以便目的主机的IP层将数据部分上交给那个协议处理，这里表示的是ICMP协议

Header Checksum是首部校验和，占16位，用于检验数据报的首部

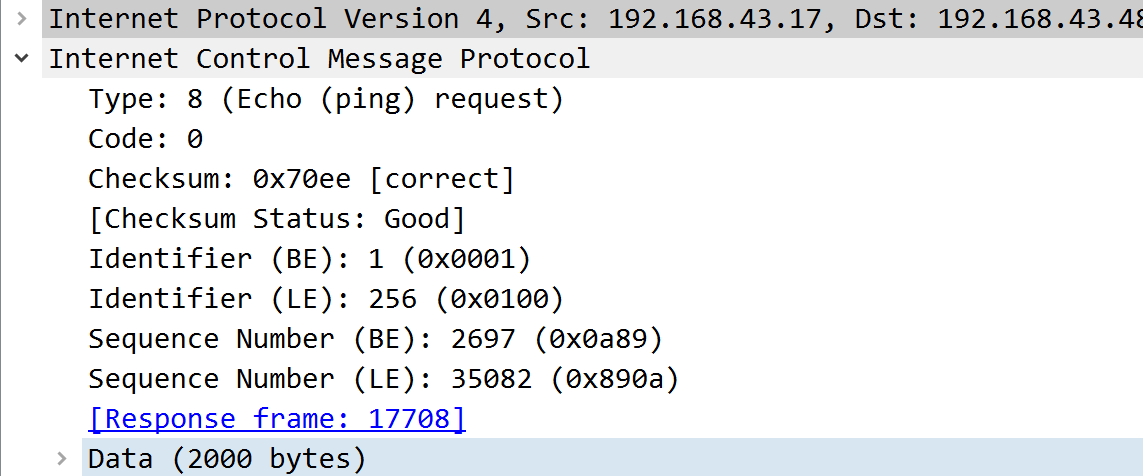
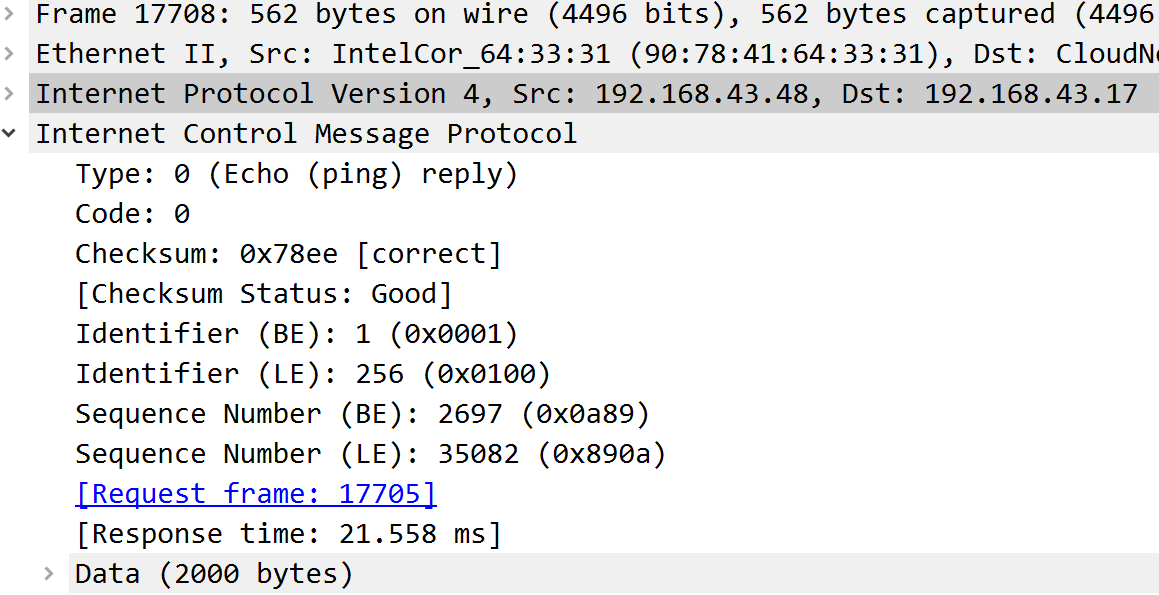
Source Address表示源IP地址

Destination Address表示目的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。  
  
  
  
根据图中可以看出一个2000字节的IP数据包被分成了两片，第一片Total length为1500字节，除去首部20字节，数据部分是1480字节；第二片是Total length是548字节，除去IP首部20字节和ICMP首部8字节，数据部分是520字节，两个切片通过相同的标识进行重组，加起来数据刚好是2000字节。

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。  
  
  
类型，表示这个ICMP数据包是请求包还是应答包，是8则为request，是0则为reply，是3或者其他则是差错类型。

代码部分为0

校验和为correct，说明数据正确

ICMP的类型相关（BE,LE）

序号，请求数据包和应答数据包相邻。

响应时间为1.931ms  
差错信息：

数据域，即发送的数据内容。请求和应答包中的是一致的  
目标主机不可达，type=3

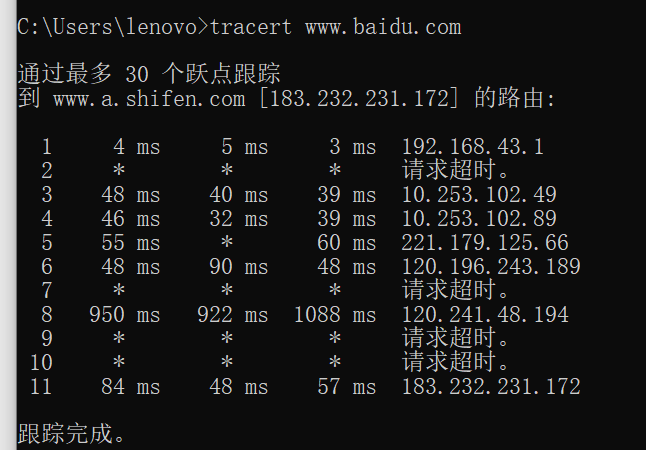
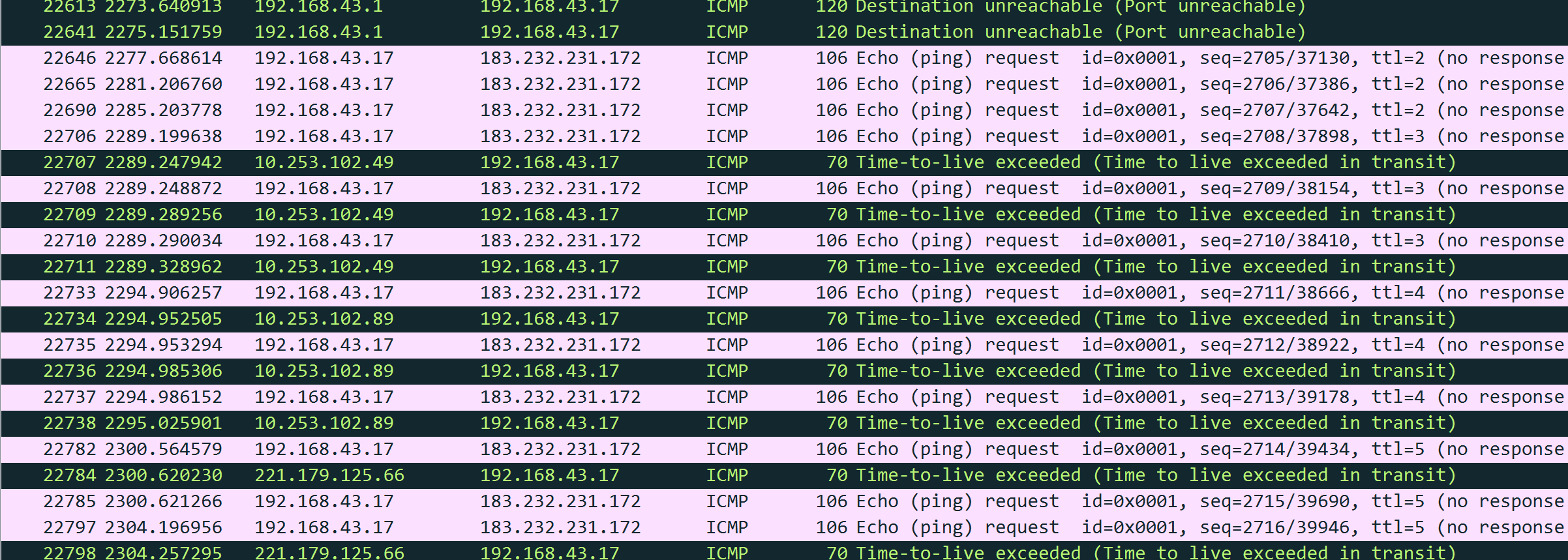
原点抑制，type=4

超时，type=11

参数错误，type=12

重定向，type=5

* 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。

  
  
工作原理：

1）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。

2）首先，tracert送出一个TTL是1的IP 数据包到目的地，当路径上的第一个路由器收到这个数据包时，它将TTL减1。

3）此时，TTL变为0，所以该路由器会将此数据包丢掉，并送回一个「ICMP time exceeded」消息（包括发IP包的源地址，IP包的所有内容及路由器的IP地址）

4）tracert 收到这个消息后，便知道这个路由器存在于这个路径上，接着tracert 再送出另一个TTL是2 的数据包，发现第2 个路由器......

5）tracert 每次将送出的数据包的TTL 加1来发现另一个路由器，这个重复的动作一直持续到某个数据包 抵达目的地。

6）当数据包到达目的地后，该主机则不会送回ICMP time exceeded消息（黑色着色的条目），一旦到达目的地，由于tracert通过UDP数据包向不常见端口(30000以上)发送数据包，因此会收到「ICMP port unreachable」消息，故可判断到达目的地。

**【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？  
 在一个局域网中，计算机通信实际上是依赖于MAC地址进行通信的，而ARP（Address Resolution Protocol）的作用就是根据IP地址查找出对应IP地址的MAC地址。主机A第一次与主机B通信时,可以捕获到添加主机B的MAC到ARP表的报文，再次通信时，由于主机A中的ARP表中已经有主机 B的MAC地址，则不需要再通过ARP协议获得MAC地址

2、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时，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，所以抓不到。Ping本机IP地址也收不到，数据包没有发到网口

3、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？  
（1）Request timed out

对方已关机

对方与自己不在同一网段内，通过路由也无法找到对方

对方确实存在，但设置了ICMP数据包过滤（比如防火墙设置）

检查对方是否存在，可以用带参数 -a 的Ping命令探测，如果能得到对方的NETBIOS名称，则说明对方是存在的，是有防火墙设置，如果得不到，多半是对方不存在或关机，或不在同一网段内。

d.错误设置IP地址

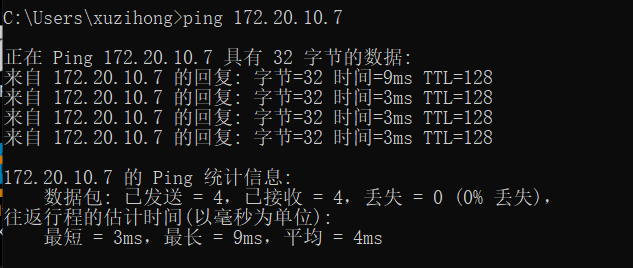
（2）Destination host Unreachable

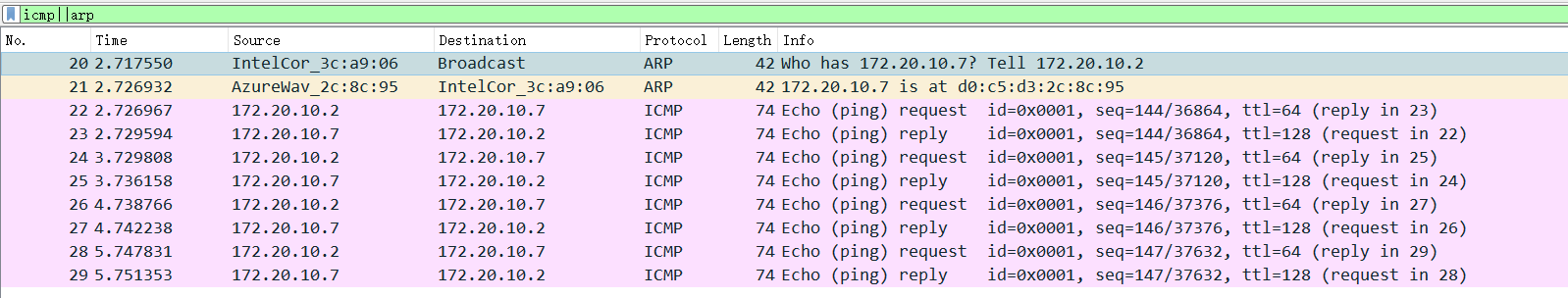
a. 对方与自己不在同一网段内，而自己又未设置默认的路由，或者网络上根本没有这个地址就会出现“Destination host Unreachable”。

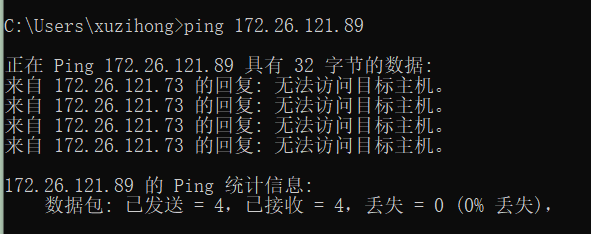
b. 网线出了故障

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）。  




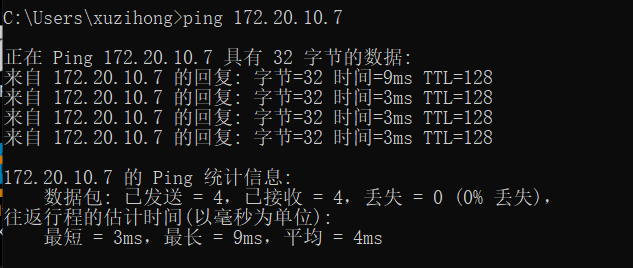


5、通过下面实验**理解网关**

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。

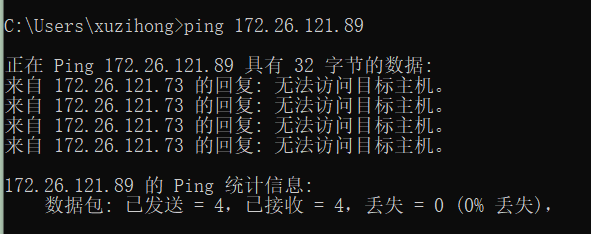
假设主机A的IP地址为10.2.2.2/24，主机B的IP地址为10.2.3.3/23，两主机不设置网关，分别在主机A和主机B上用ping测试与对方的连通性，用ARP查看物理地址。对测试结果进行分析。

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。



ping得通，能看到物理地址。

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。



Ping不通，看不到物理地址

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。