**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 实验项目类型 实验地点 室

学生姓名 蔡佳宏 学号 2019051095

学院 珠海校区智能科学与工程学院/人工智能产业学院 系 　专业 信息安全

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

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

**计算机2台，交换机一台。**

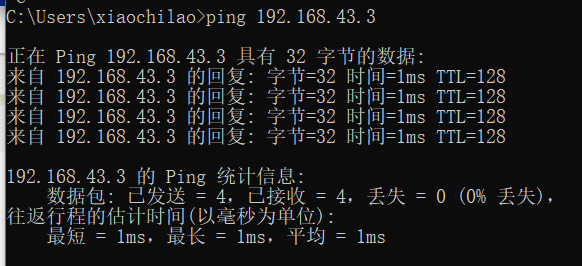
**一台主机ip为：192.168.43.2（A）**

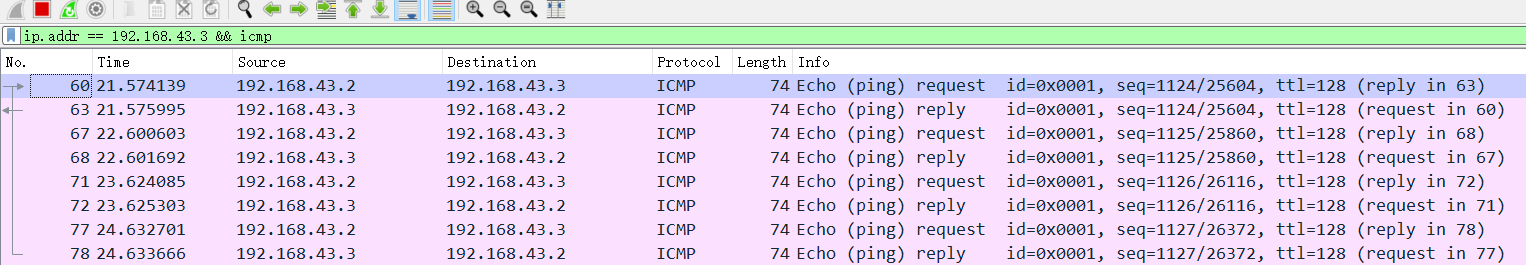
**一台主机ip为：192.168.43.3（B）**

**网关：192.168.43.1**

1. **实验步骤和测试分析**

**Ping192.168.43.3，用wireshark捕获:**

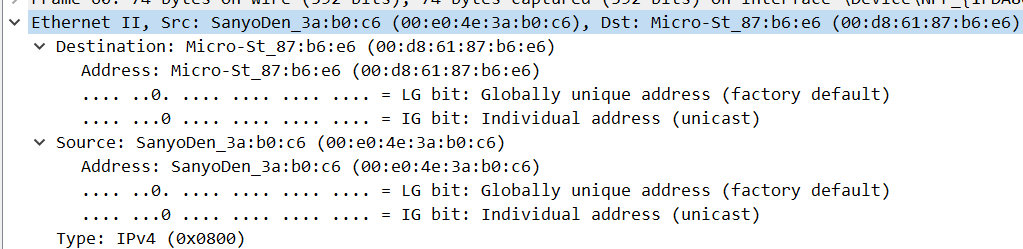
****

****

****

1. **分析MAC帧**

* 捕获到的以太网帧：



1. 

此行为目的地址，为(00:d8:61:87:b6:e6)

1. 

LG表示Local/Global，为0时表示全球管理，可以保证全球没有相同地址；为1时表示本地管理，可以任意分配。

IG表示individual/Group，为0时表示一个单站地址；为1时表示组地址，可进行多播；所有48位都为1时代表广播地址。

1. 

表示源地址为 (00:e0:4e:3a:b0:c6)

1. 

同上，LG表示Local/Global，为0时表示全球管理，可以保证全球没有相同地址；为1时表示本地管理，可以任意分配。

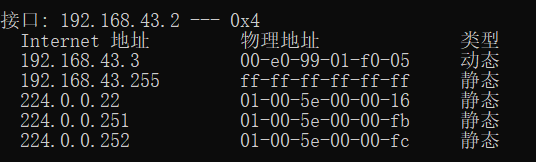
IG表示individual/Group，为0时表示一个单站地址；为1时表示组地址，可进行多播；所有48位都为1时代表广播地址。

1. 

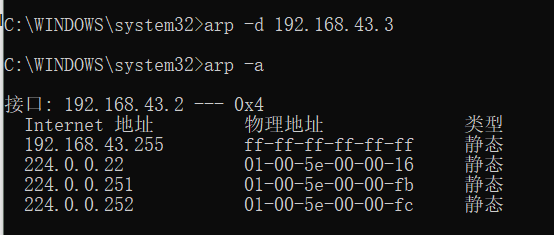
十六进制0800表示上层封装的协议为IPv4

1. **ARP协议分析**

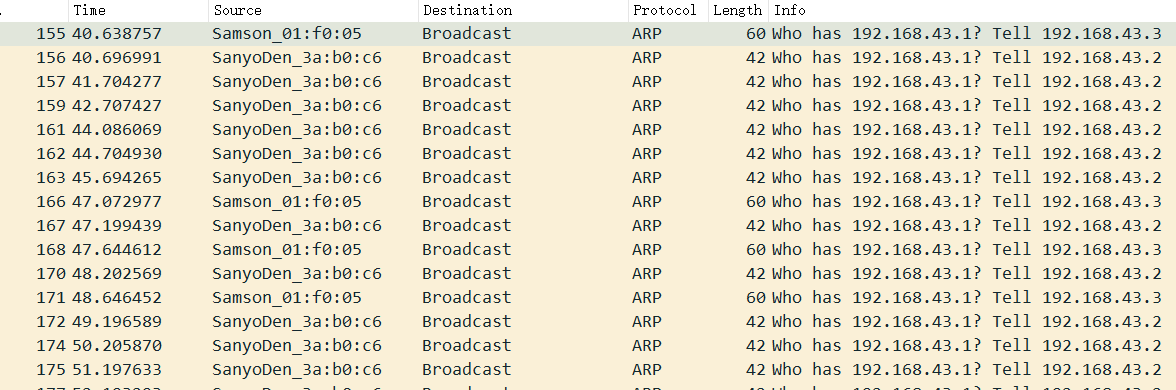
* 进入DOS窗口，用arp –a查看本机上的ARP表的情况，然后用 arp –d 192.168.43.3删除192.168.43.3的记录：



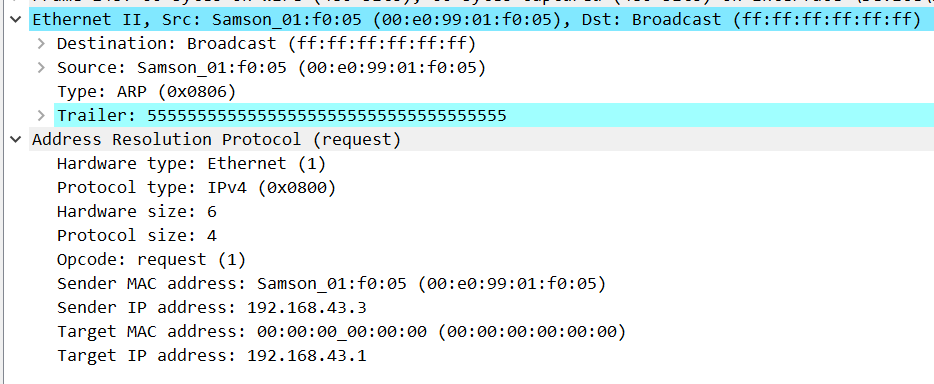
删除后：



* 把网线断开1分钟，然后再联网，能捕获ARP报文：

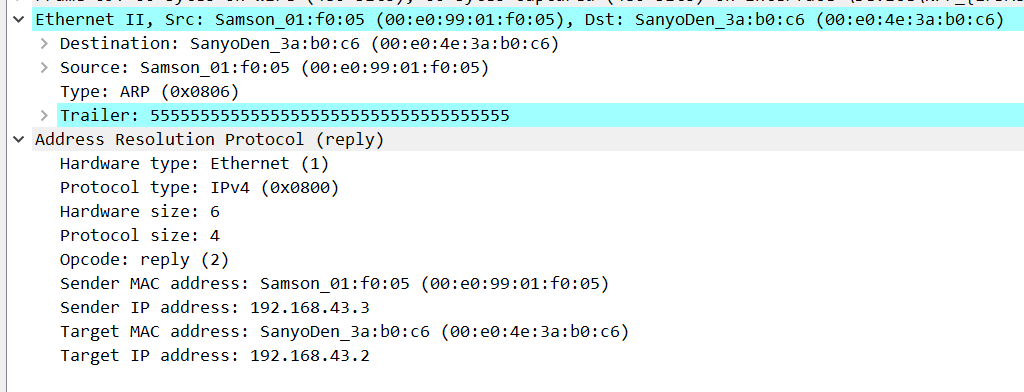


1. 点开一个arp协议包：



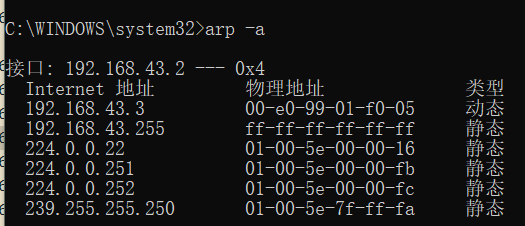
1. 硬件地址：1为以太网
2. 协议类型：十六进制的0800为IPv4，表示映射的协议类型为ipv4
3. 硬件地址长度：mac地址长度为6字节
4. 协议类型长度：ipv4长度为4字节
5. Opcode为一代表此arp报文类型为请求报文
6. 源主机mac地址为： Samson\_01:f0:05 (00:e0:99:01:f0:05)
7. 源主机ip地址为： 192.168.43.3
8. 目的主机mac地址为：00:00:00\_00:00:00 (00:00:00:00:00:00)
9. 目的主机ip地址为： 192.168.43.1
10. 总结：由于主机B的ARP表中网关的mac地址为全0，主机B广播询问目的主机的mac地址。

* 从主机192.168.43.2上向主机192.168.43.3发PING检测报文，能捕获ARP报文：

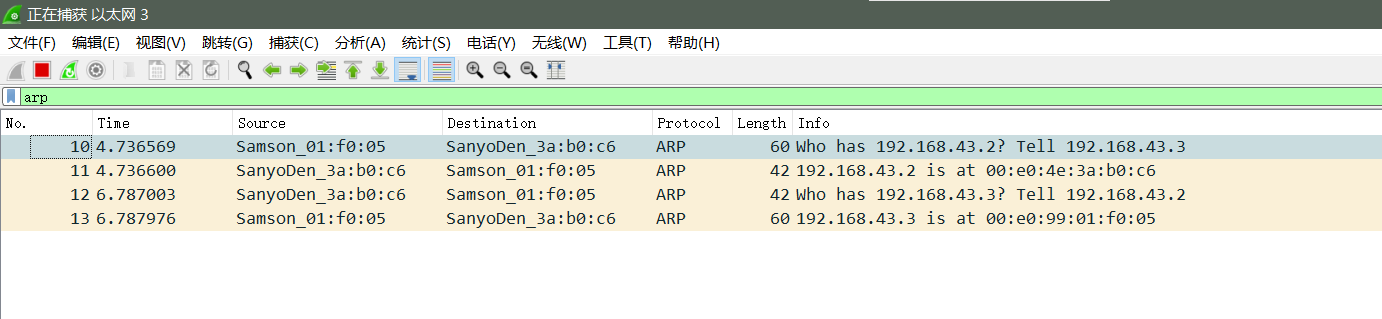


1. Reply说明本数据包为回应报文
2. 硬件地址：1为以太网
3. 协议类型：十六进制的0800为IPv4，表示映射的协议类型为ipv4
4. 硬件地址长度：mac地址长度为6字节
5. 协议类型长度：ipv4长度为4字节
6. Opcode为二代表此arp报文类型为回应报文
7. 源主机mac地址为： Samson\_01:f0:05 (00:e0:99:01:f0:05)
8. 源主机ip地址为： 192.168.43.3
9. 目的主机mac地址为： SanyoDen\_3a:b0:c6 (00:e0:4e:3a:b0:c6)
10. 目的主机ip地址为： 192.168.43.2

* 通过arp - a 查看ARP表的更新情况，此时能看到192.168.43.3对应的MAC地址：

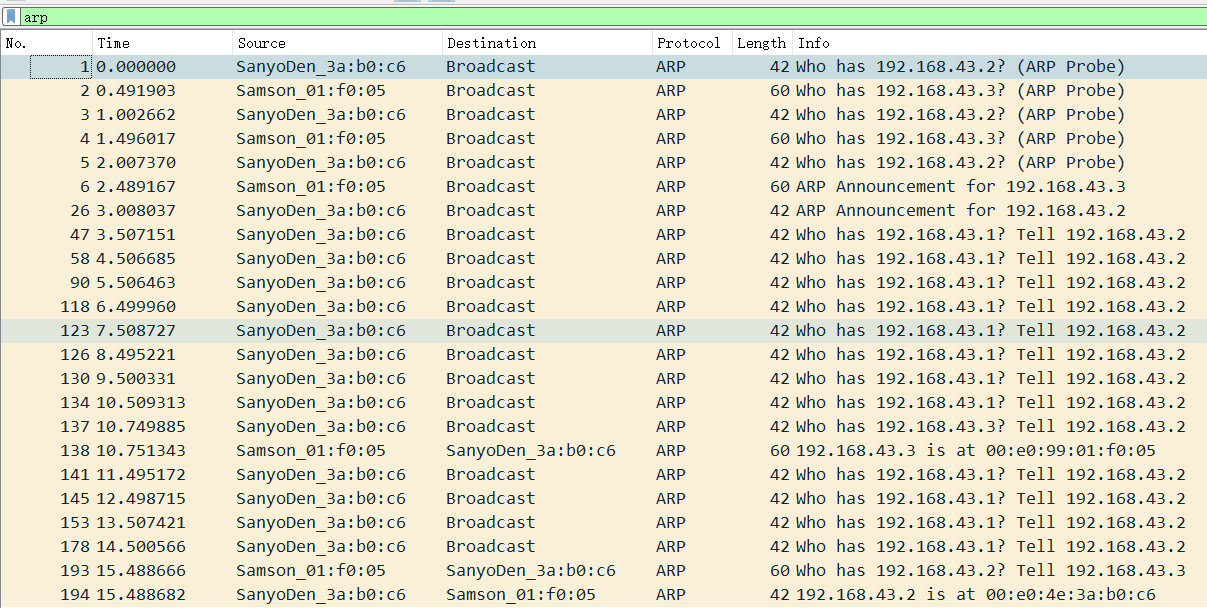


* 再次从主机192.168.43.2上向主机192.168.43.3发PING检测报文，能捕获ARP报文：



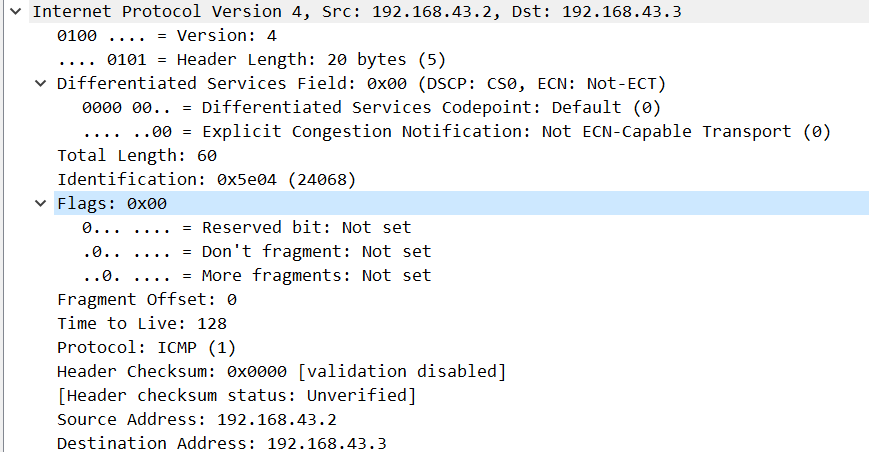
这是由于以太网能直接从arp表获取目的主机的mac地址，不需要广播来获取mac地址。所以这时候的arp包为单播，只播给主机B.

* 主机192.168.43.2上和主机192.168.43.3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，能捕获ARP报文：



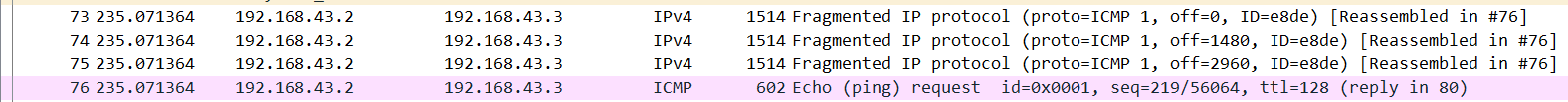
1. **IP协议分析**

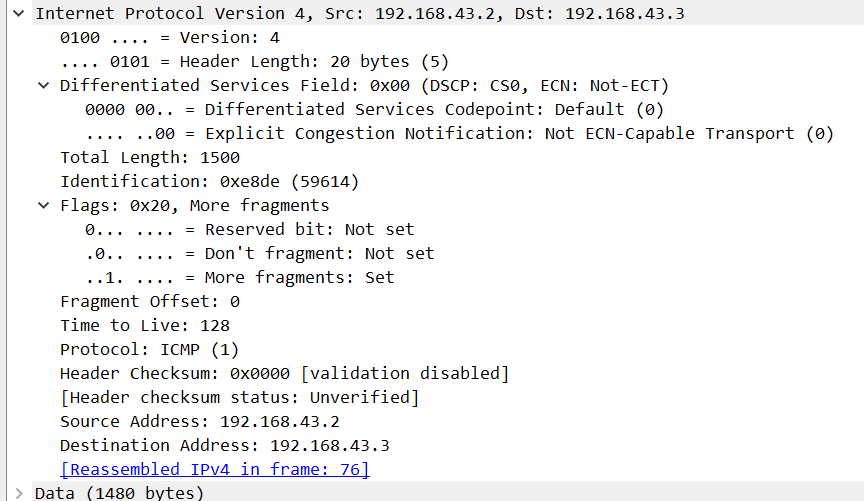
* 从主机A上向主机B发PING检测报文，捕获IP数据包，记录并分析各字段的含义，并与IP数据包格式进行比较;

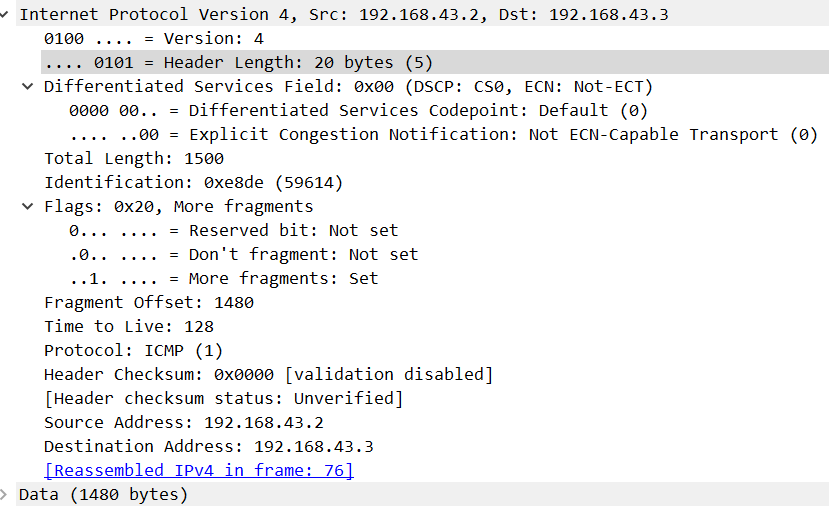


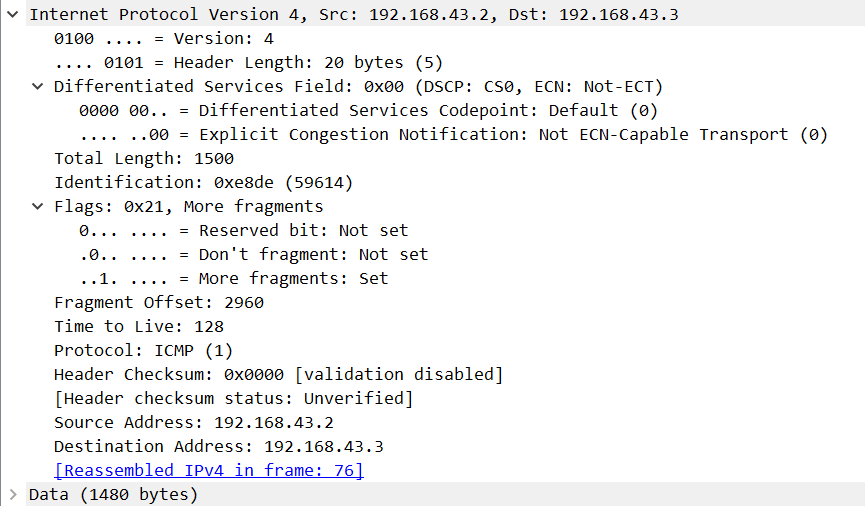
1. 协议版本为ipv4
2. 头部长度为20字节，最大为60字节
3. 区分服务为十六进制的00，共一字节，一直未被使用过，只在使用区分服务是有用
4. 总长度为60字节，共十六位，所以数据最大长度为65535字节
5. 标识为十六进制的00，共占十六位，分片的时候才有用，其中一开始的为保留，MF=1表示还有分片，为0表示最后一个分片；DF=0表示允许继续分片，为1表示不能分片。
6. 片位移为0，是指分片后在原分组里的相对位置，以8字节为单位
7. 生存时间为128，表示能通过路由器数目的最大值
8. 协议为ICMP，表示携带的是那种协议，到目的主机就交给哪个协议
9. 首部检验和为0000，只检验头部。
10. 源地址为192.168.43.2
11. 目的地址为192.168.43.3

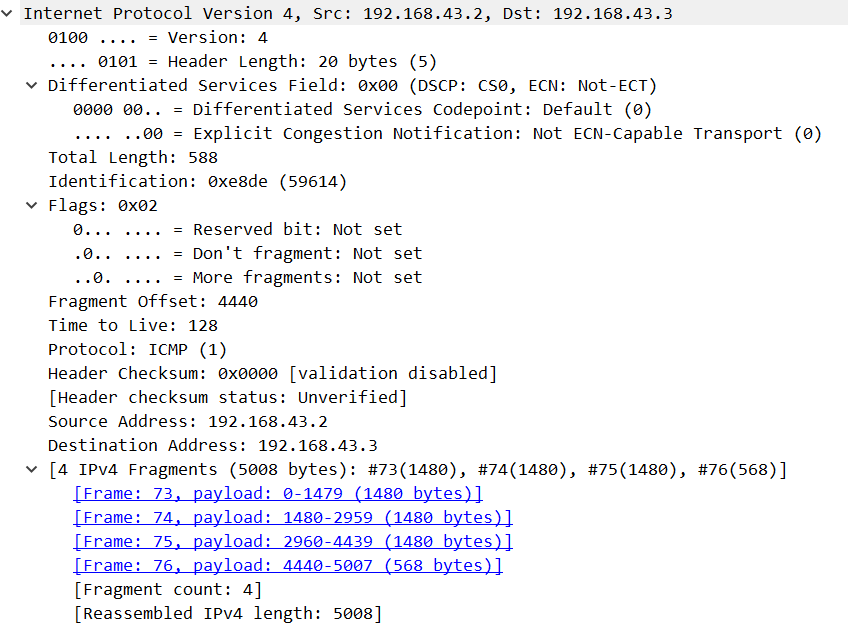
* 使用ping命令，制定数据包长度，如ping -l 2000，使用嗅探器观察IP分片情况，并分析分片和重组过程。











如图，此包被分成了四个包发送，其标识都是同一个：59614



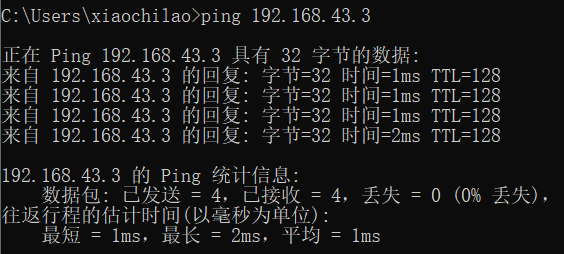
而每个分片通过Fragment Offset来知道自己在原分组的位置，通过[Reassembled IPv4 in frame]来知道自己将在何处重组。

1. **ICMP协议分析**

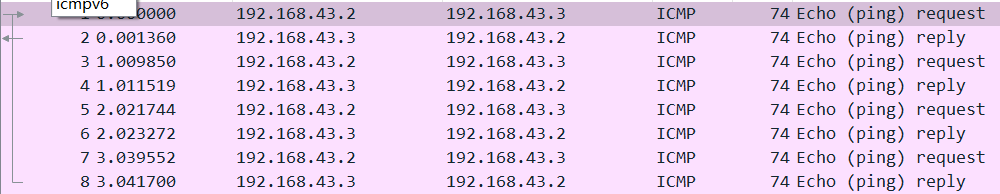
通过ping和tracet命令，了解ICMP协议的使用：

* 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。

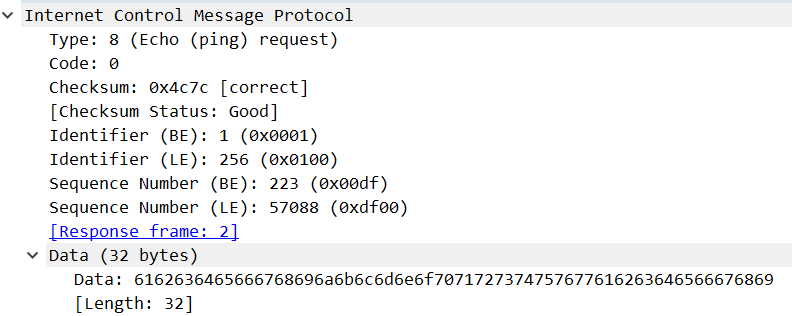
1. 如图，一共ping了四个包：



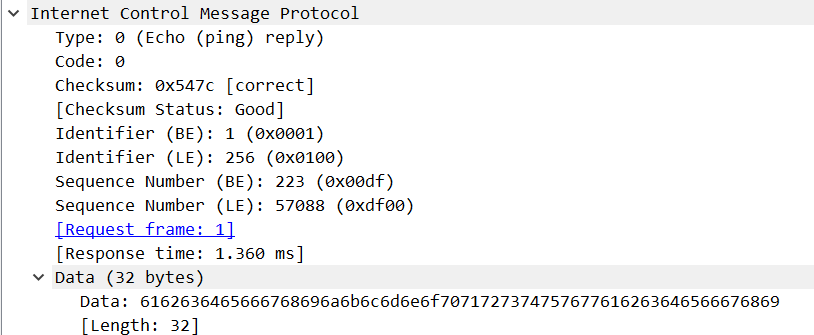
1. Wireshark一共捕获到八个包，四个请求，四个响应：



1. 请求报文：



1. 响应报文：

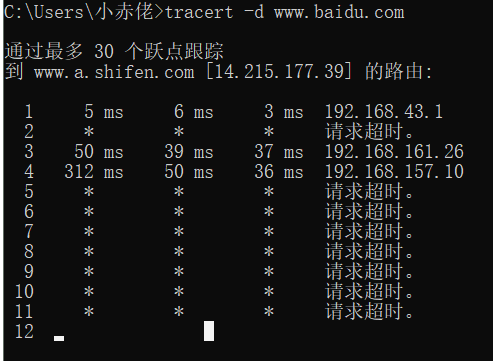


1. 类型，0代表响应包，8代表请求包，为3则为差错类型
2. 代码部分为0
3. 检验和为correct代表数据正确
4. ICMP类型相关
5. 序号，请求为1，响应为2。
6. 响应时间：1，360ms
7. 差错信息有：重点不可达，类型为3

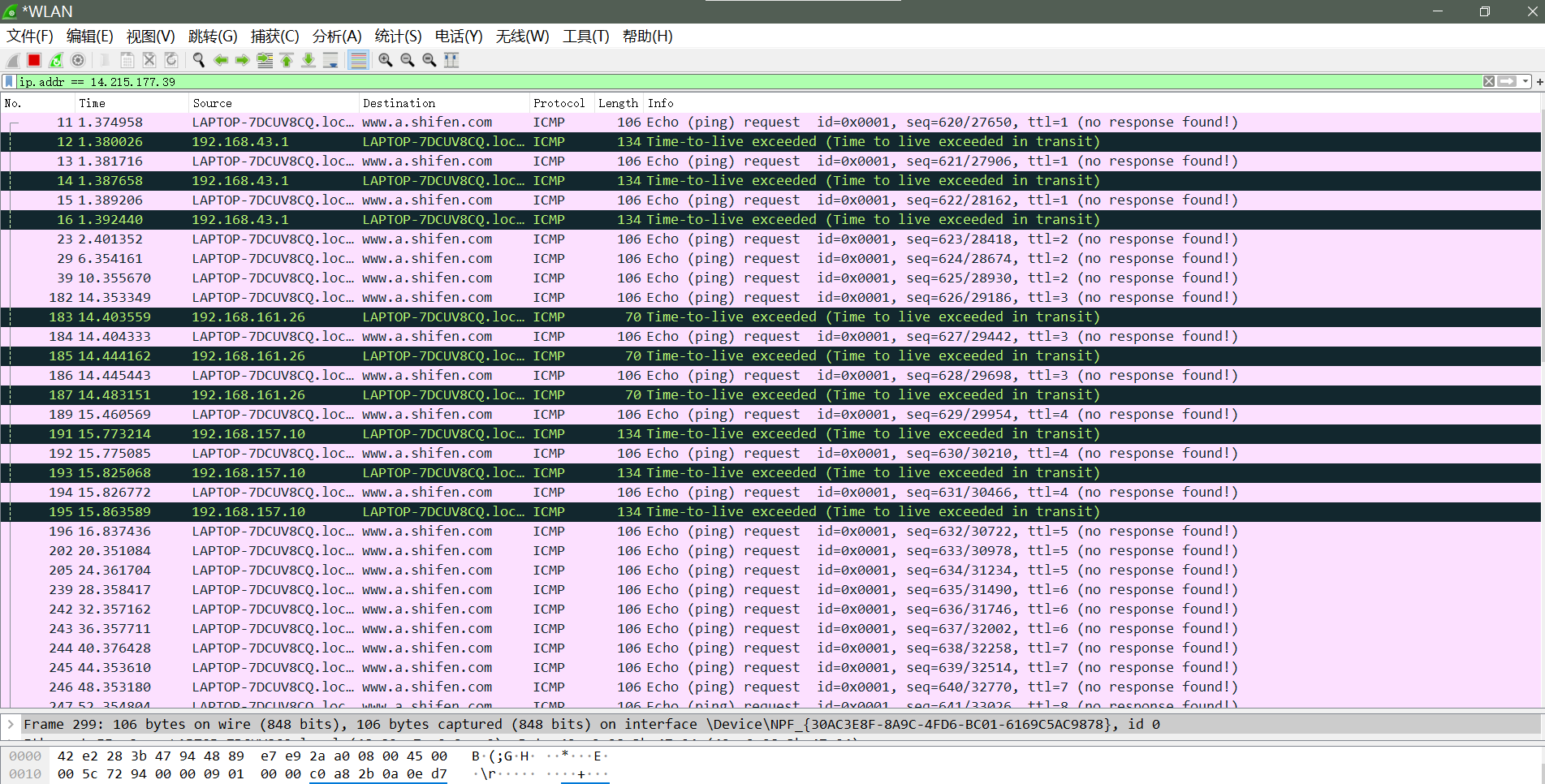
原点抑制，类型4

超过最大时间，类型11等等

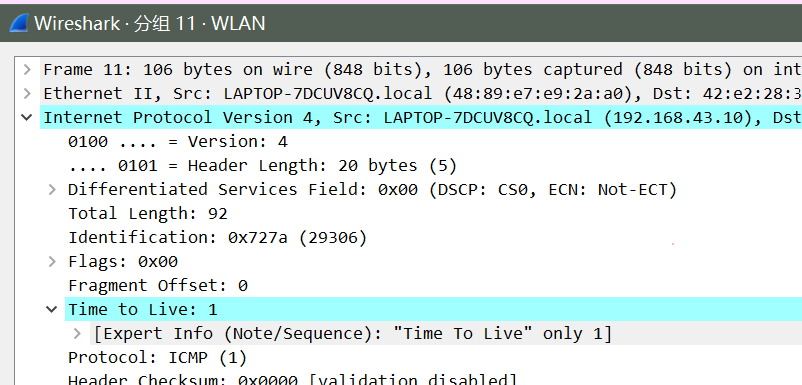
* 使用tracert命令，跟踪某台主机，使用wireshark捕获数据包，分析不同类型ICMP响应数据包格式（如type=8,type=0,type=11）。分析tracert工作原理。
  + 打开cmd输入tracert,由于直接输入tracert www.baidu.com 会将地址解析为主机名，所以太慢了，我们输入tracert -d [www.baidu.com](http://www.baidu.com) 则会快很多



* + 查看wireshark



* + tracert命令首先会发送一个ttl为1的ICMP包，遇到下一个路由导致ttl-1=0，此包丢失。送回一个「ICMP time exceeded」消息。





* 接着tracert 再送出另一个TTL是2 的数据包，发现第2 个路由器，同上当ttl为0时送回一个「ICMP time exceeded」消息。一直发出ttl增加的ICMP包，直到达到目的地。
* tracert 有一个固定的时间等待响应(ICMP TTL到期消息)。如果这个时间过了，它将打印出一系列的\*号表明：在这个路径上，这个设备不能在给定的时间内发出ICMP TTL到期消息的响应。然后，Tracert给TTL记数器加1，继续进行。

1. **实验小结**

* 掌握了数据链路层的协议以及原理