**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 钟颖谦 学号 2019051091

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上午～ 11月 9日上午 温度 ℃湿度

## （一）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。

## （二）实验内容和要求

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。

## （三）实验原理

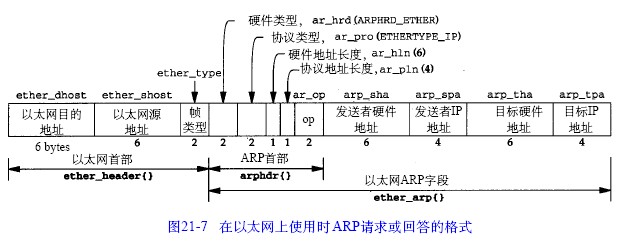
**1、网络嗅探器**

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**。

## （四）实验环境

**仪器：**计算机2台，交换机一台。

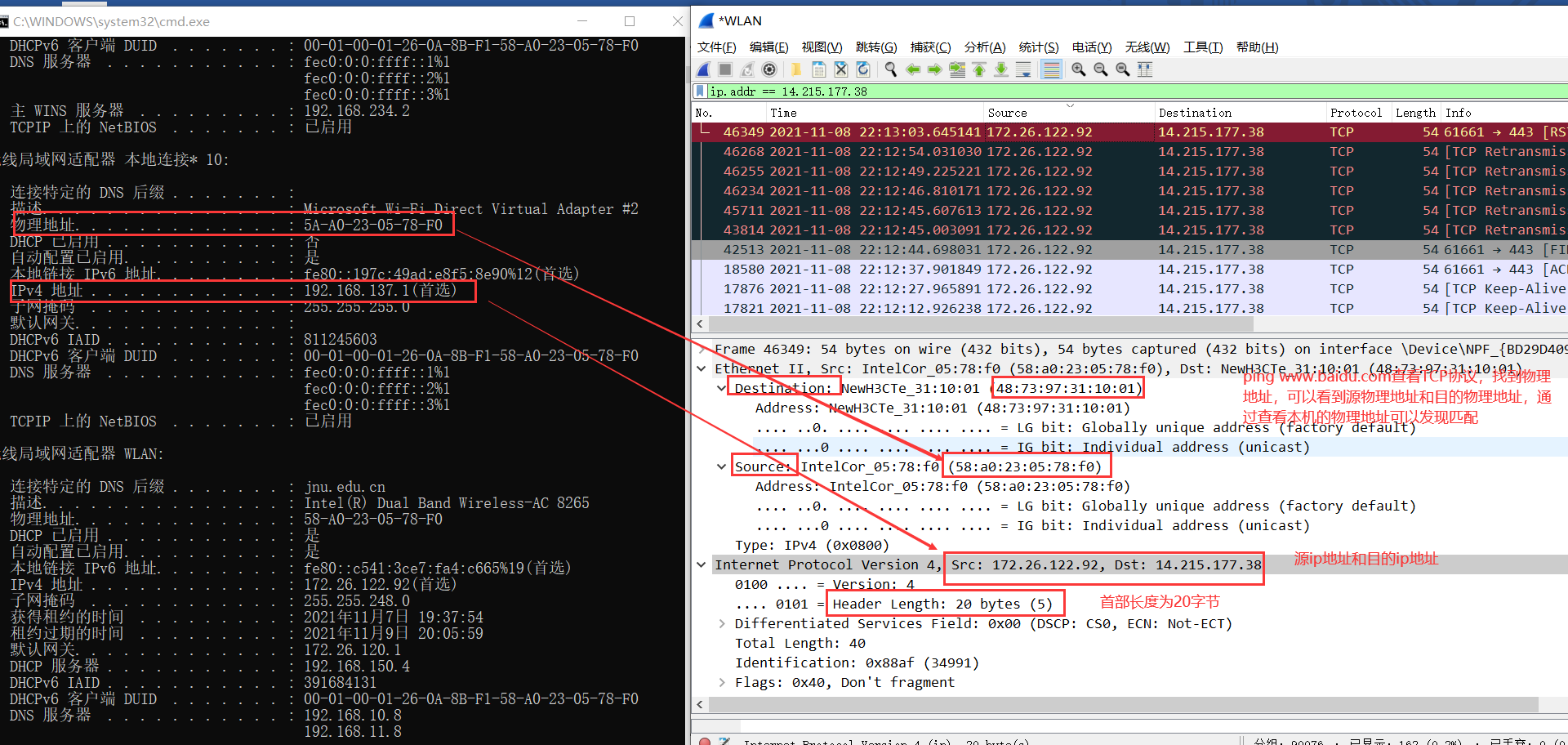
**实验环境：wireshark&cmd**

## （五）实验步骤与调试

### 1.安装Wireshark

### 2.以太网协议分析

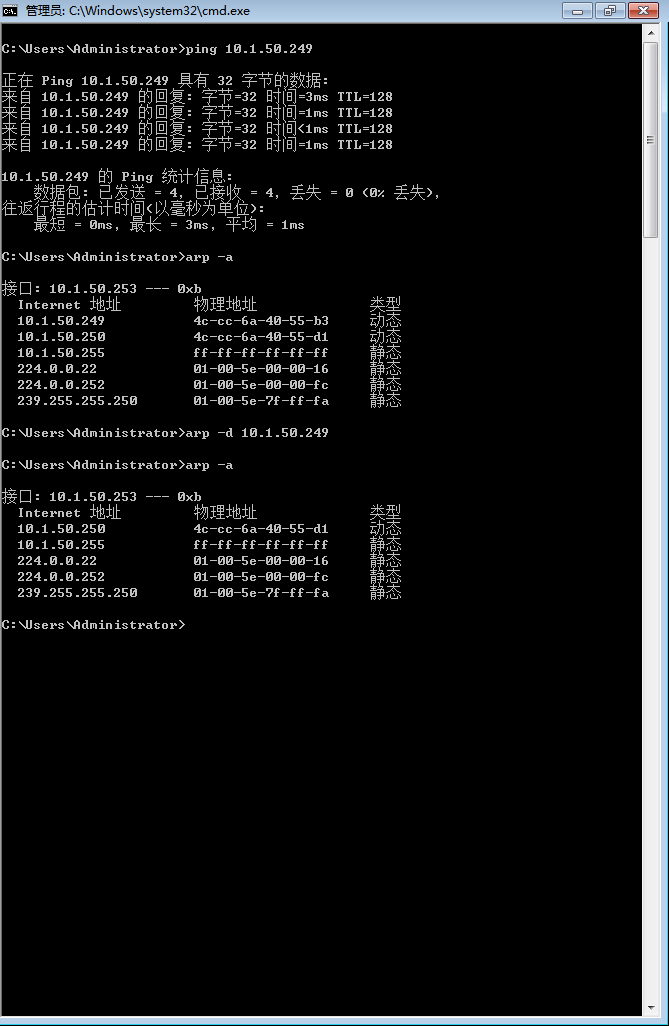
从主机A上向主机B发PING检测报文，捕获以太数据帧，记录并分析MAC帧各字段的含义。



unicast是单一传播方式

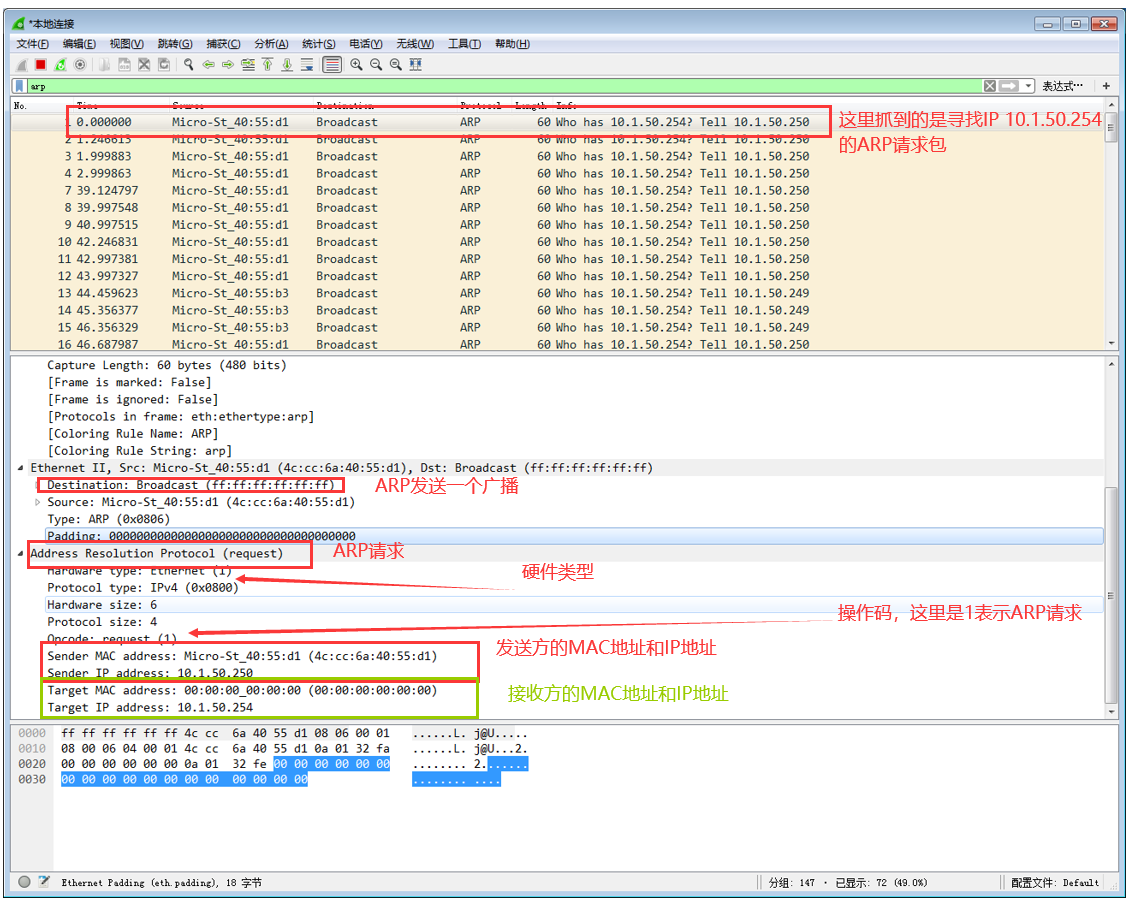
### 3.ARP协议分析

* 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）；



将 10.1.50.249 ip地址删除

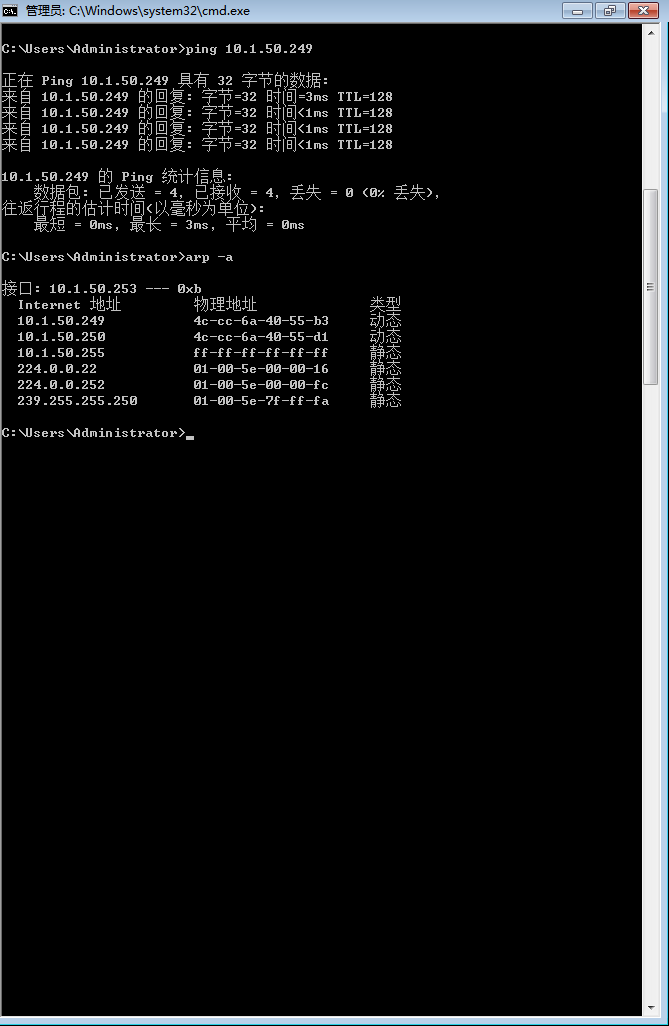
* 运行Wireshark程序；
* 把网线断开1分钟，然后再联网，观察此时是否能捕获ARP报文，如果能，记录并分析各字段的含义；



* 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；

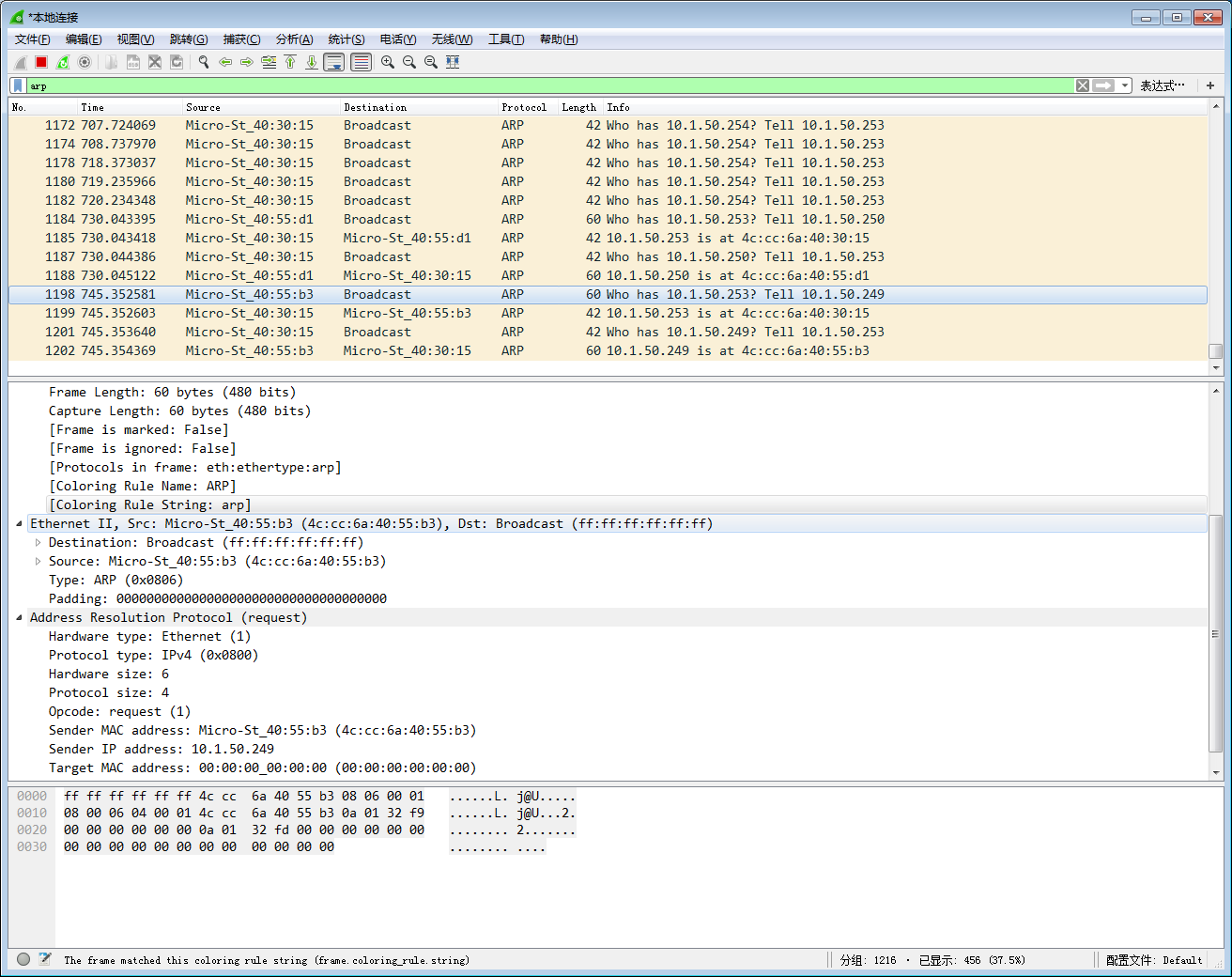


* 通过arp - a 查看ARP表的更新情况，记录此时能否看到B对应的MAC地址；



可以看到删除过的IP地址为10.1.50.249主机，从此可以看到其物理地址

* 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；



这里捕捉到的是主机B向主机A的ARP请求数据包。

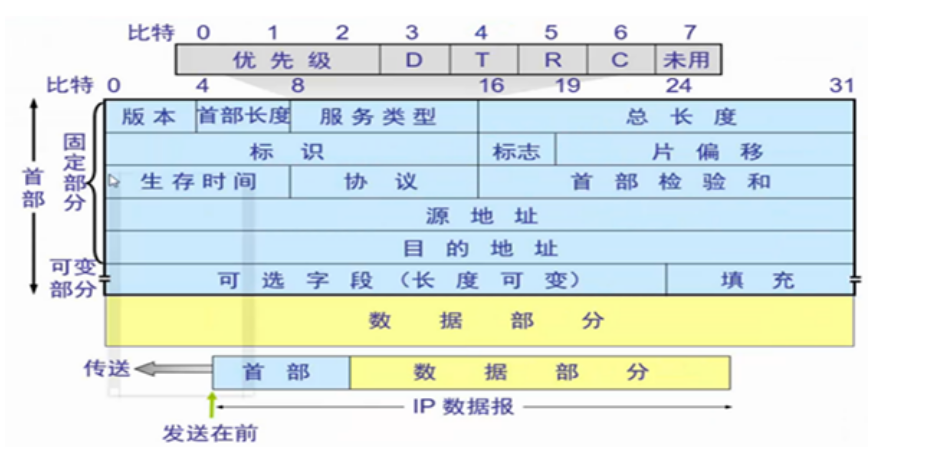
* 主机A上和主机B停止进行任何数据通信，5分钟后再次从A向B发PING检测报文，或者从主机B上向主机A发PING检测报文，观察看此时是否能捕获ARP报文。



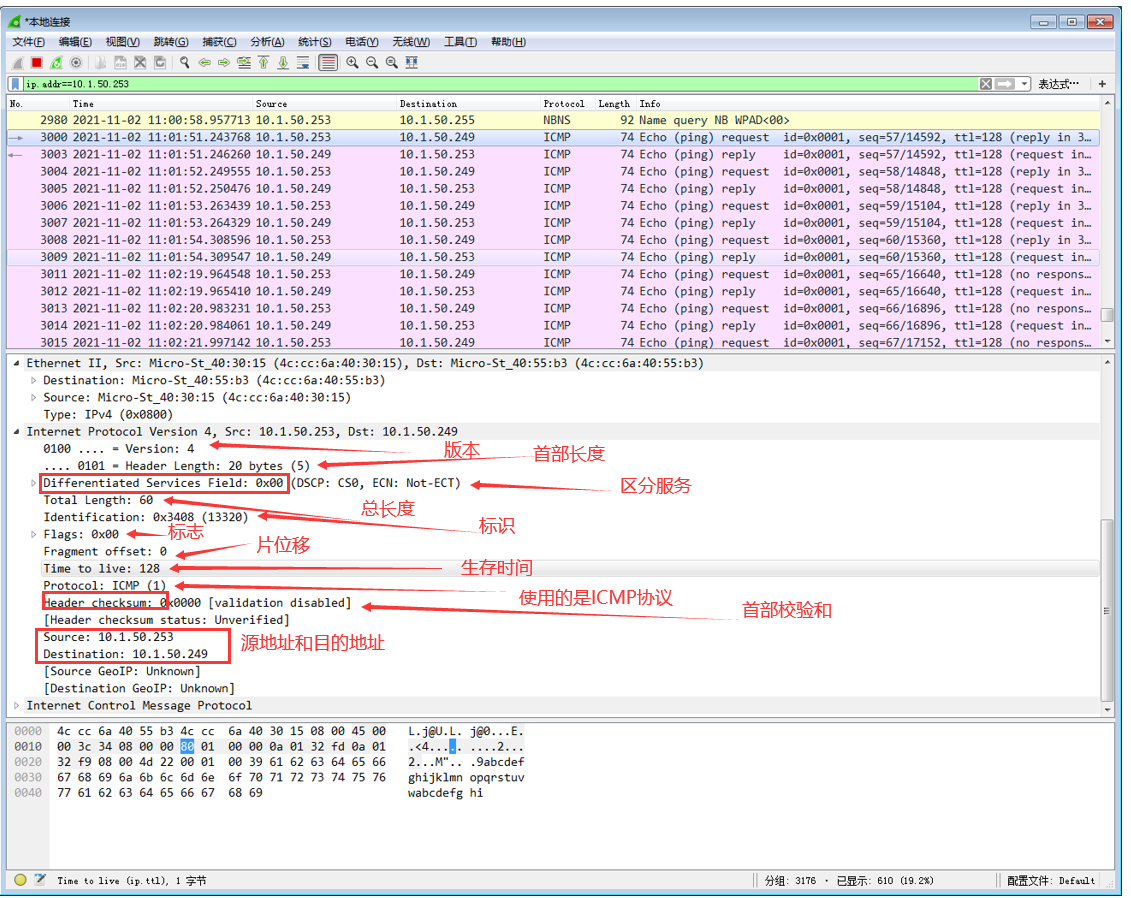
这里捕获的是主机A 10.1.50.253寻找主机B 10.1.50.249的物理地址的ARP请求数据包。

### 4.IP协议分析

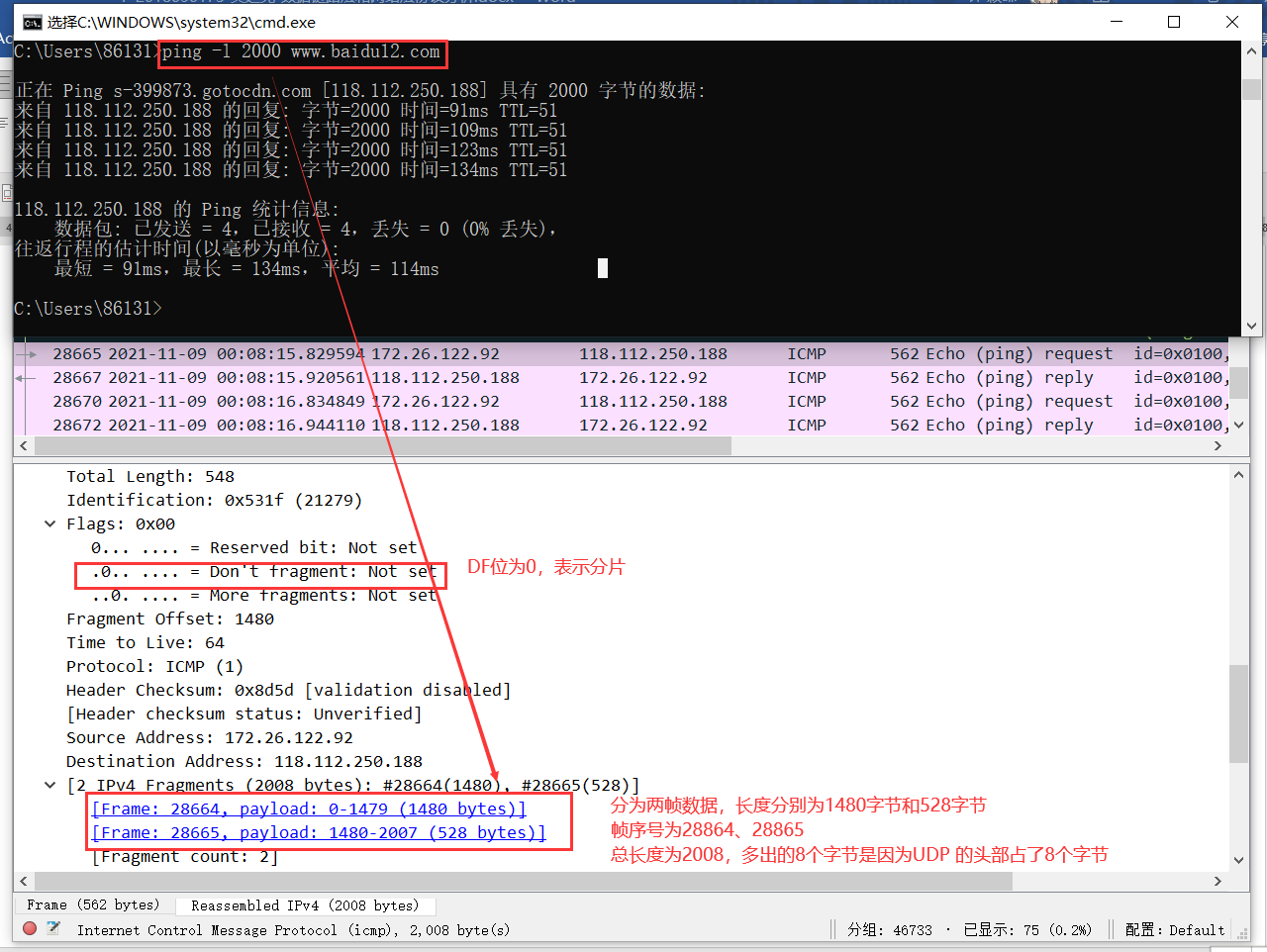
* 从主机A上向主机B发PING检测报文，捕获IP数据包，记录并分析各字段的含义，并与IP数据包格式进行比较;



对照IP数据包格式，分析如下



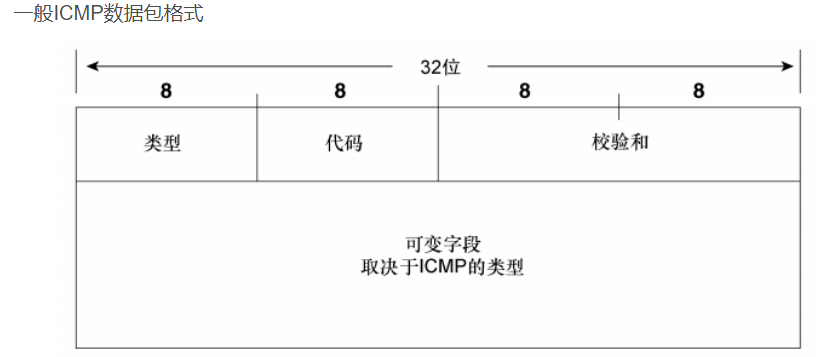
* 使用ping命令，制定数据包长度，如ping -l 2000，使用嗅探器观察IP分片情况，并分析**分片和重组**过程。



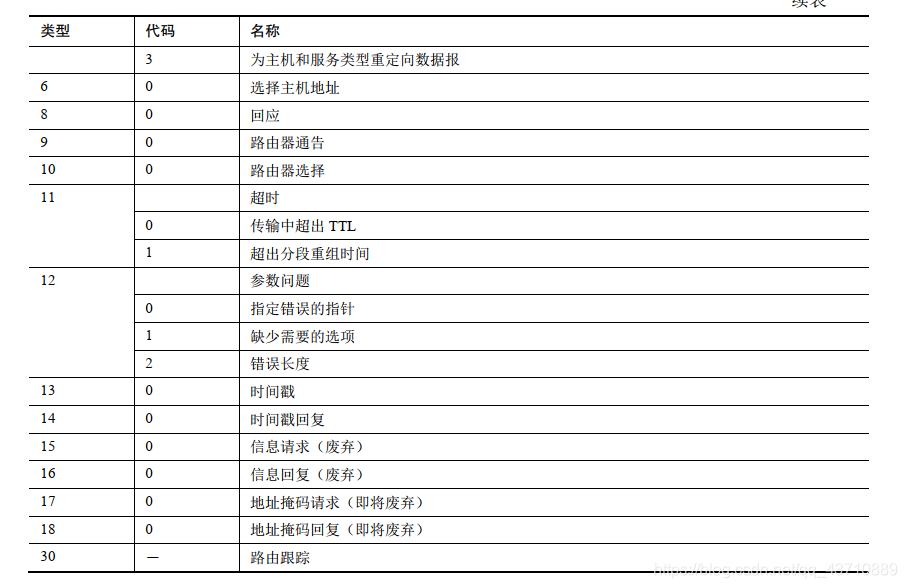
### 5.ICMP协议分析

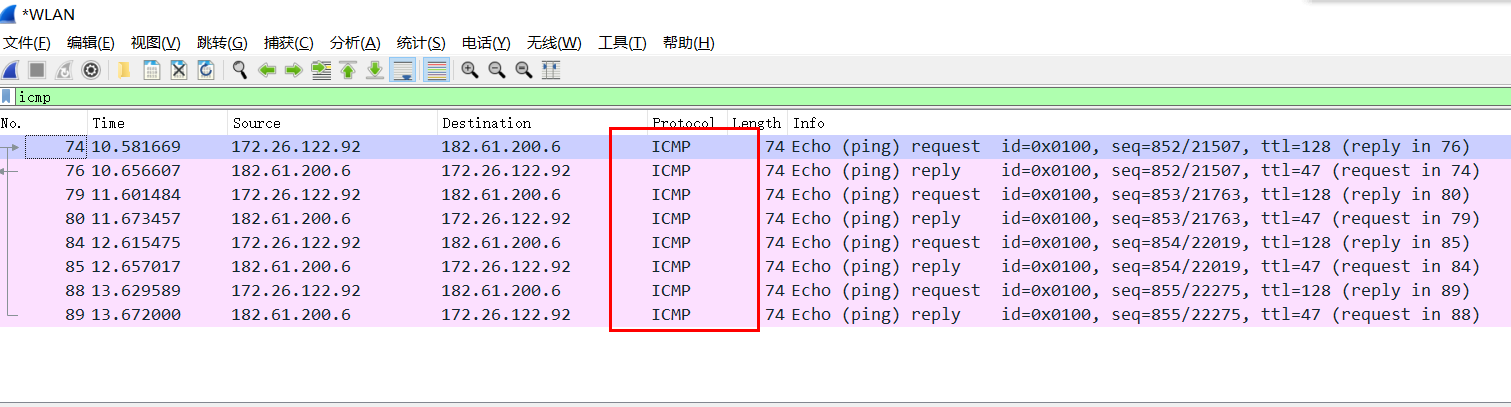
通过ping和tracet命令，了解ICMP协议的使用。

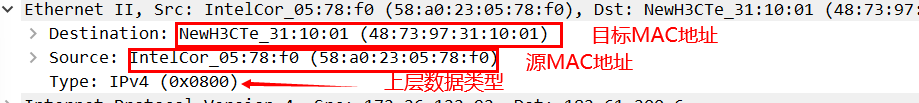
* 从主机A上向主机B发PING检测报文，捕获ICMP请求数据包和应答数据包，记录并分析各字段的含义，并与ICMP数据包格式进行比较；如果返回的差错信息，请分析是由于什么差错引起的。

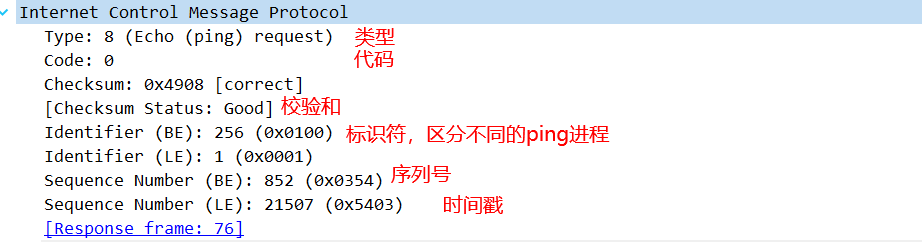
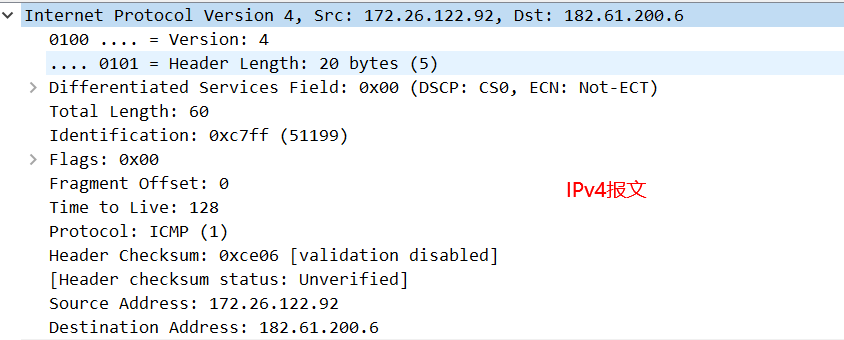










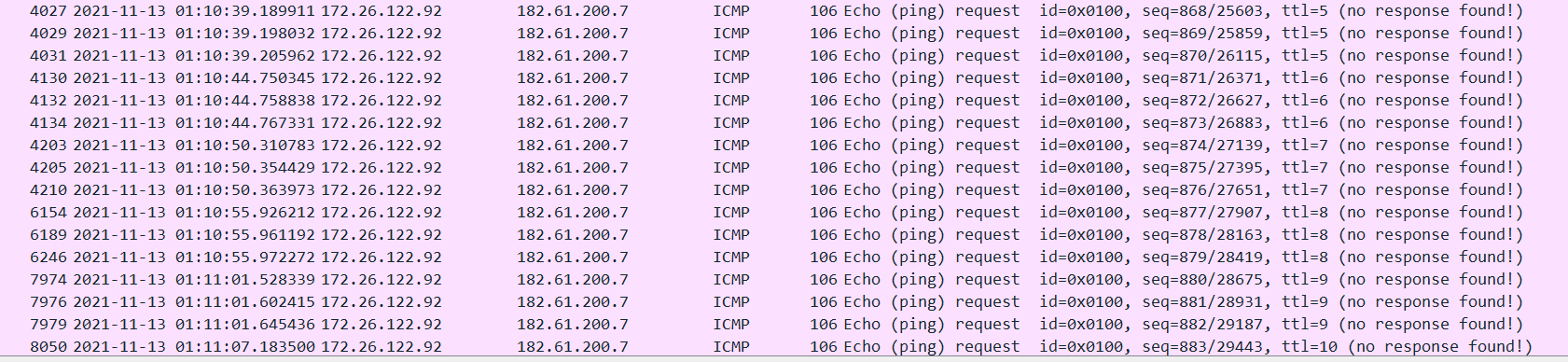


* 使用tracert命令，跟踪某台主机，使用wireshark捕获数据包，分析不同类型ICMP响应数据包格式（如type=8,type=0,type=11）。分析tracert工作原理。

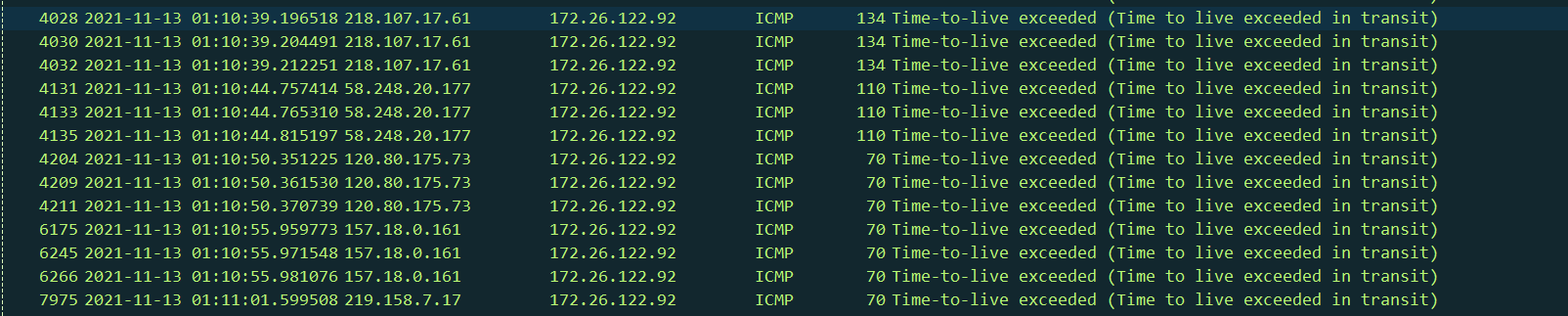
Tracert 命令用 IP 生存时间 (TTL) 字段和 ICMP 错误消息来确定从一个主机到网络上其他主机的路由。

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。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），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...... 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。当数据包到达目的地后，该主机则不会送回ICMP time exceeded消息，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。

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。



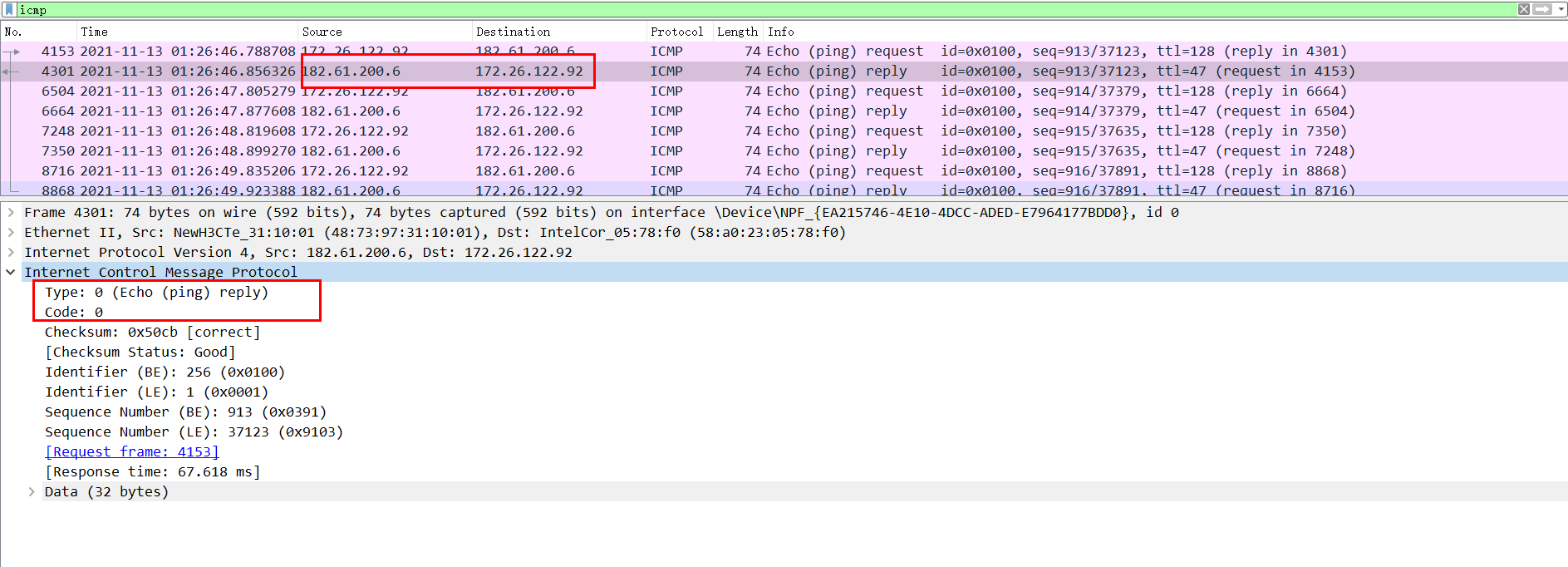
Tracert发送的数据包



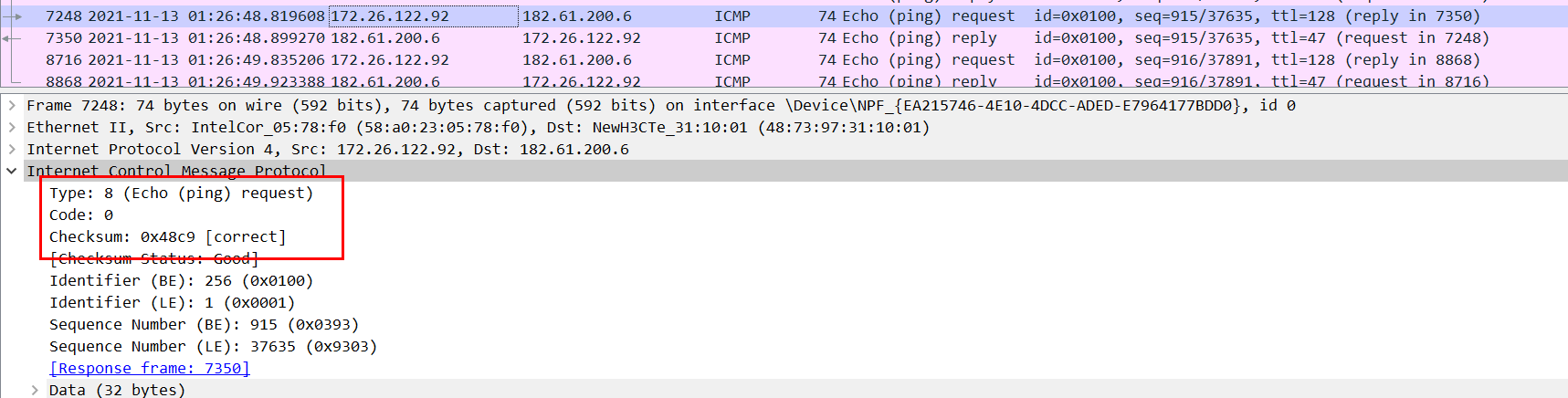
Tracert接收的数据包



类型11代码0，传输时超出TTL，分析可知时本机向目的地址请求超时。



类型0代码0.回应应答。



类型8代码0，表示应答。

## （六）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：如果主机的ARP高速缓存里含有当前想要访问的主机IP及其对应的MAC地址，则无需广播寻找，此时捕获不到ARP报文。反之如果ARP高速缓存里没有包含当前想要访问的主机IP及其对应的MAC地址，则需要广播寻找，此时可以捕获到ARP报文。

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地能收到报文吗？ 为什么？

答：ping 127.0.0.1时不能捕获到ICMP报文，因为ping 127.0.0.1这条命令不经过网卡。

Ping本机IP地址也不能收到报文。Ping本机IP，数据包从网卡协议的最顶层(应用层)接收数据→传输层→IP层，数据包到达IP层的时候，IP层检测到数据包的目的主机是本机，就会将数据包送回接口，然后再送回本机。以上的几个层次，构成了一个IP协议栈，故ping 本机IP也捕获不到报文。

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？

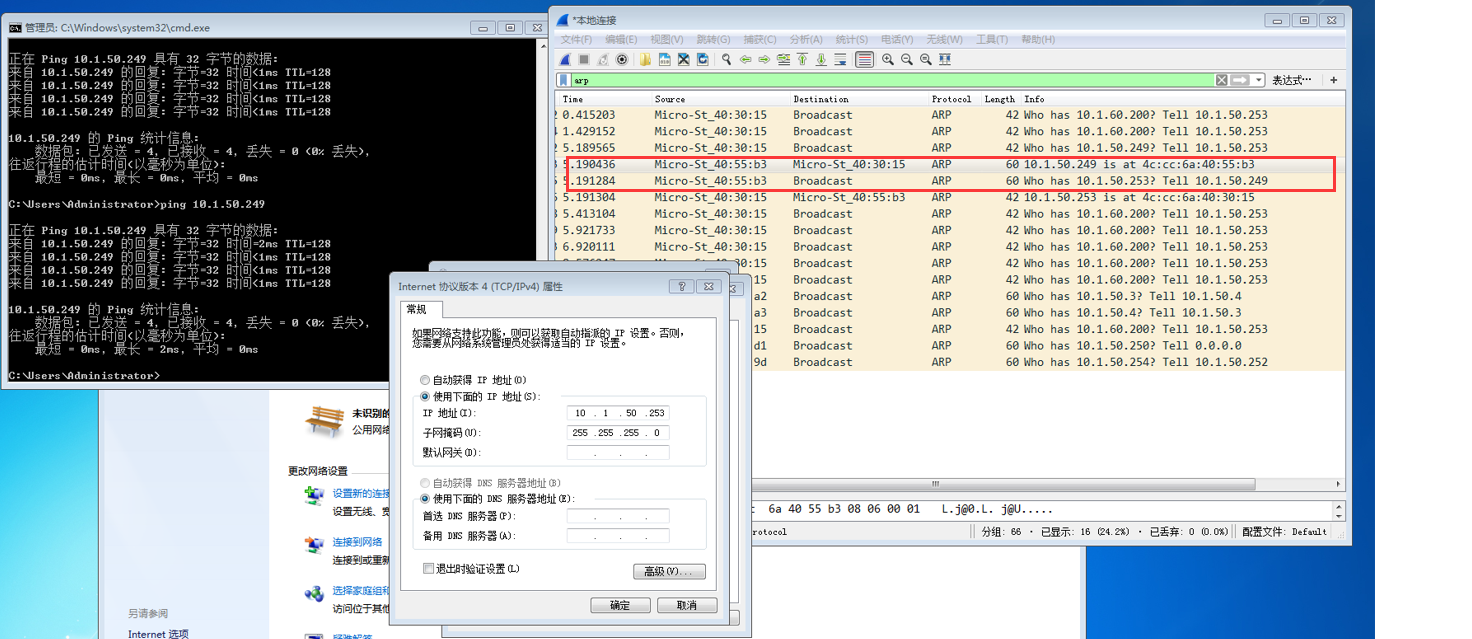
答：(1)“Request timed out”是请求超时，此消息表示在1s的默认时间内没有收到Echo Reply消息。这可能是由于许多不同的原因造成的。最常见的包括网络拥塞，ARP请求失败，包过滤，路由错误或无声丢弃。

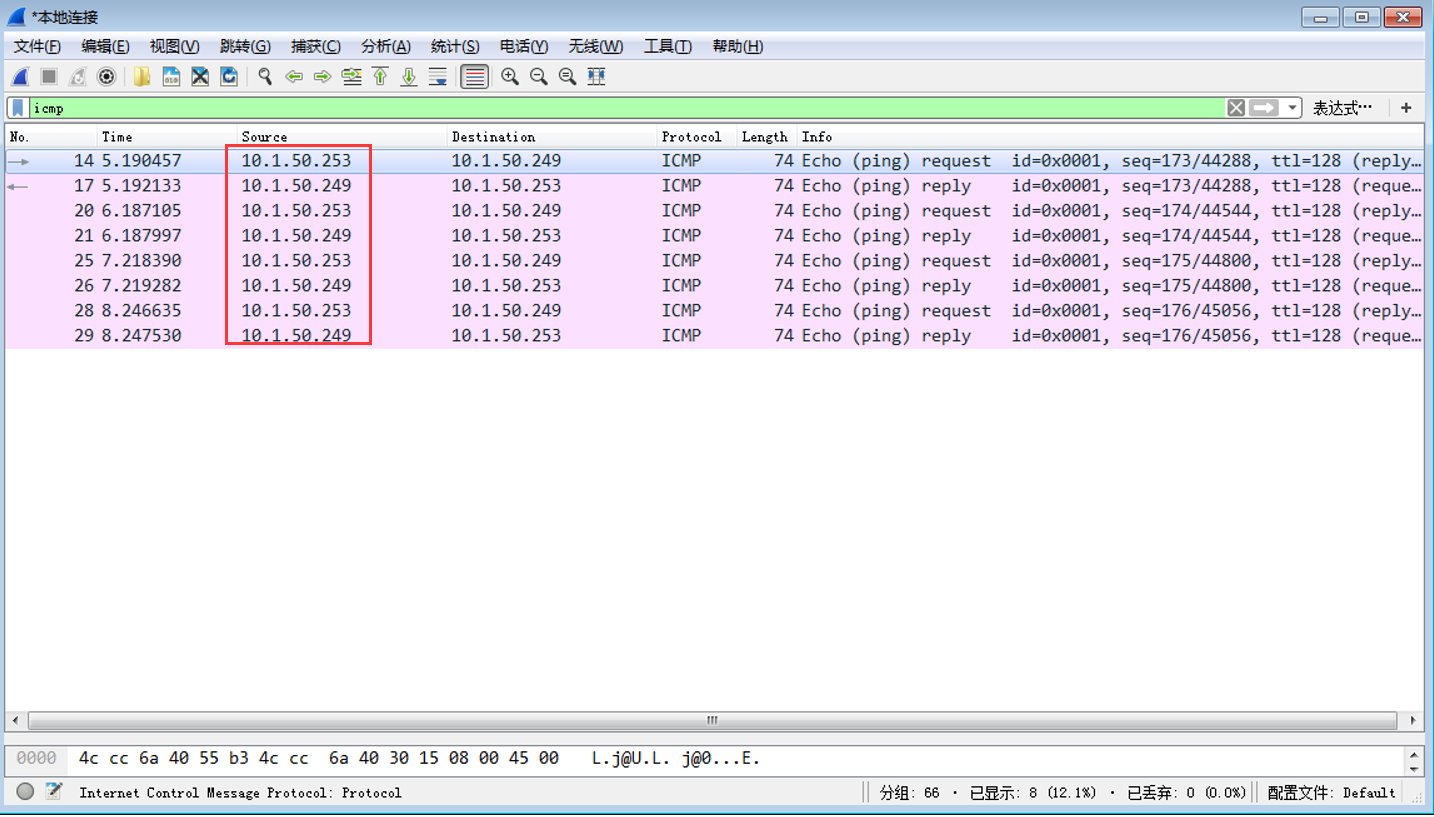
(2)“Destination Host Unreachable”是目标主机不可达，此消息表示本地系统没有到达所需目标的路由，或者远程路由器报告没有到目的地的路由。如果该消息只是“Destination Host Unreachable”，那么没有来自本地系统的路由，并且发送的数据包不会被放在线路上。如果消息是“Reply From <IP address>:Destination Host Unreachable”，则路由问题发生在远程路由器，其地址由“<IP address>”字段指示。

（3）实验中还出现了传输失败的ping失败错误提示信息，考虑时系统版本不一样对于目标主机不可达的另一方是的表示。

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。



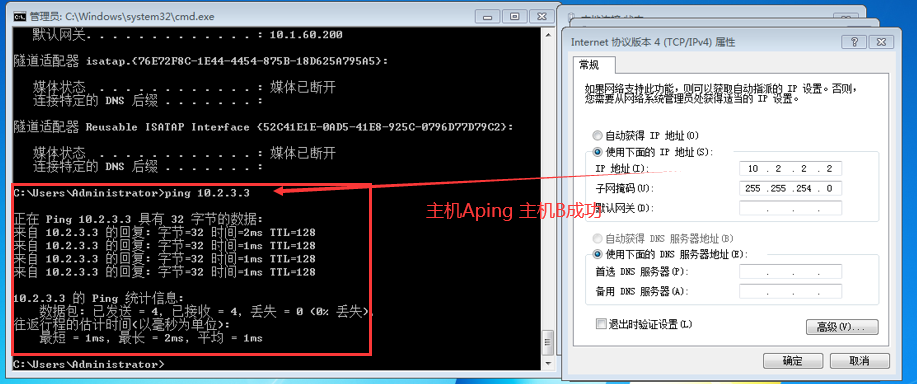


不同网段的主机不能通信，用PING命令测试，会显示“ Destination Host Unreachable”，因为没有指明网关，无法发送出去，因此显示“目的主机不可达”，用嗅探器捕获不到任何信息。

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）。

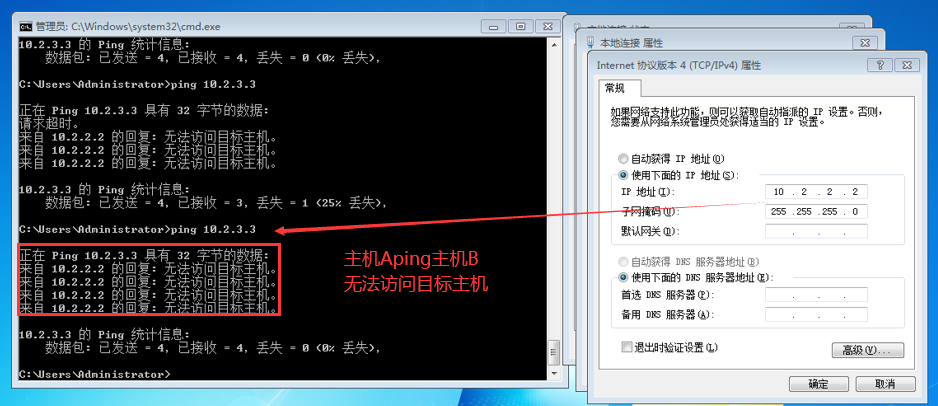
5、通过下面实验**理解网关**

（1）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。

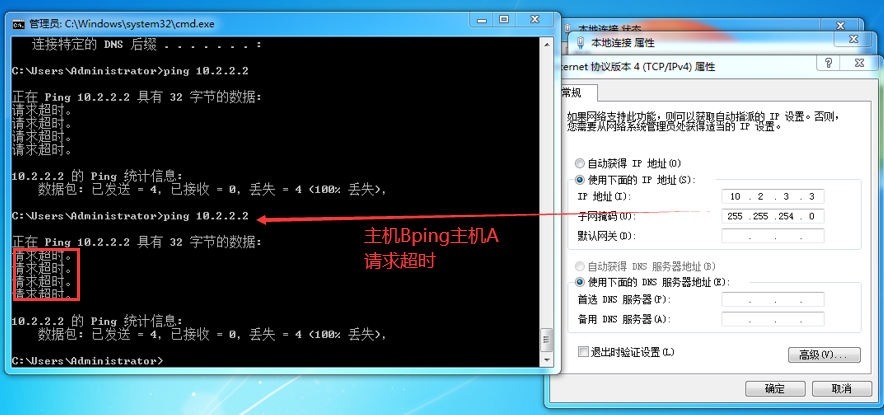


此时主机Aping主机B成功，这是因为主机A利用自身的子网掩码与主机B的IP地址进行与运算，从而得到主机B的IP地址是与主机A本身处于同一个网段，因此可以ping通。

（2）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。

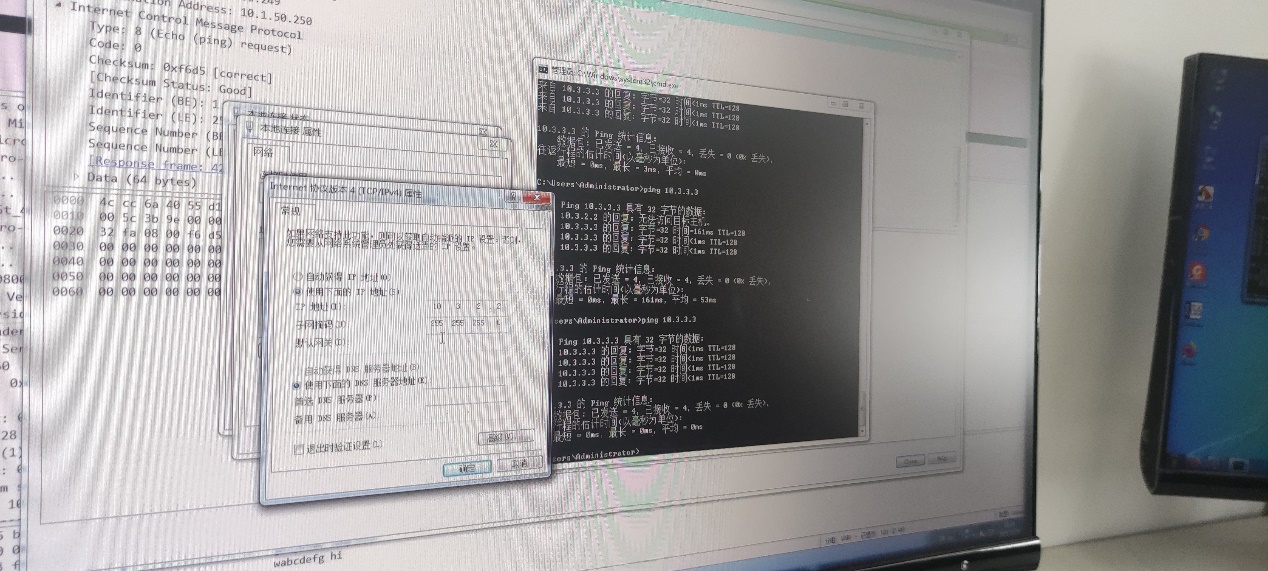
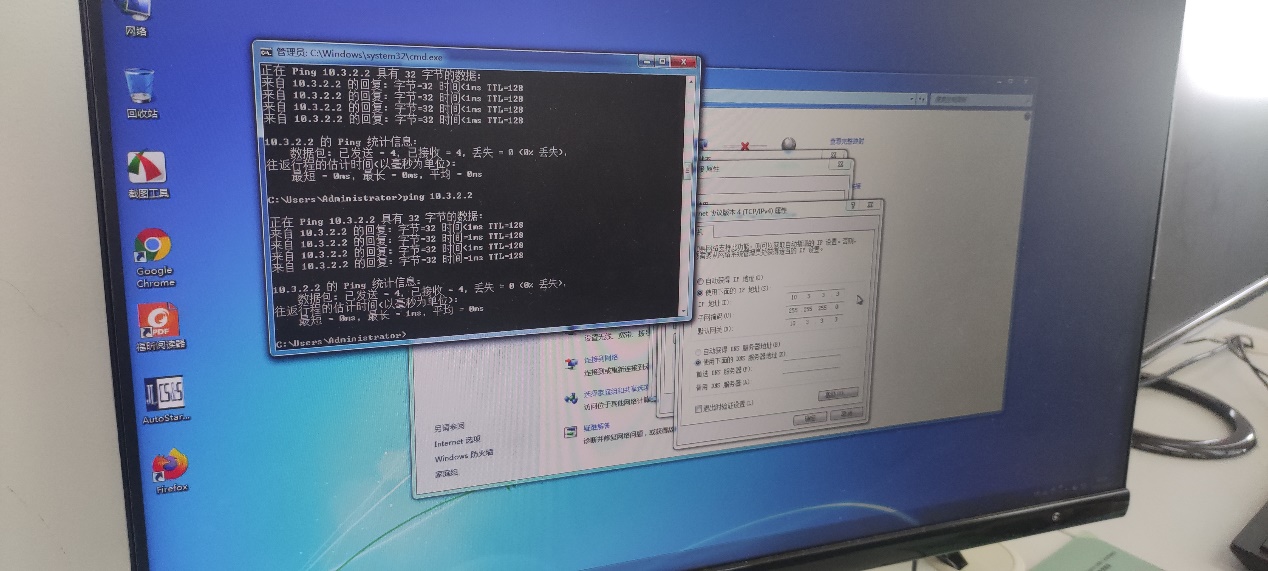


此时主机Aping主机B失败，并且显示“无法访问呢目标主机”，这是因为主机A利用自身的子网掩码与主机B的IP地址进行与运算，从而得到主机B的IP地址不是与主机A本身处于同一个网段，因此不可以向主机B通信，导致ping结果是无法访问目标主机。



此时主机Bping主机A不成功，并且显示“请求超时”，这是因为主机B利用自身的子网掩码与主机A的IP地址进行与运算，从而得到主机B的IP地址是与主机A本身是处于同一个网段，因此向主机A发送ping请求包，但同时，主机A也进行同样的操作，然而判断出主机A与主机B不处于同一个网段，因此主机A无法发送ping响应包，如此便无法发送正常ping通信，而由于主机B发送的ping请求包都未收到相应，则请求超时。

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。



这里发现就能互相通信，将网关设为本身的IP地址后，

## （七）实验小结

通过本次实验，我理解了链路层、网络层的主要协议的格式，以及协议的工作原理。同时，通过对实验中思考问题的实验以及验证，理解了网关和子网掩码的概念。通过使用网络嗅探器Wireshark分析协议格式和协议的工作过程，我对IP协议、ARP协议、ICMP协议等协议的协议格式有了更加深入的了解，以及也知道了Tracert命令的工作原理，同时也对使用Wireshark嗅探器的使用，在对不同命令的工作捕捉数据包后分析其工程，从而也能够更加熟练地运用实验工具。

在实验的过程中，能够在对实验内容的操作后，进行思考问题，了解命令本身工作的原理和应对不同实验结果的不同的分析，也在不清楚实验结果之间的联系时通过询问同学和请教同学去解答疑惑。

**暨南大学本科实验报告专用纸(附页)**