实验七 数据链路层和网络层协议分析

## 【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】

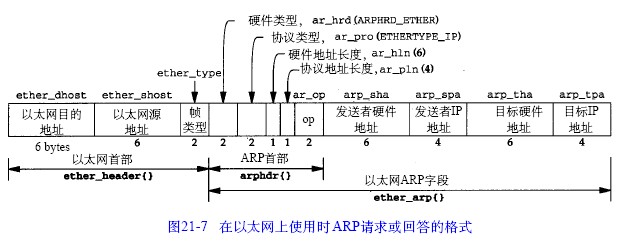
**1、网络嗅探器**

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**



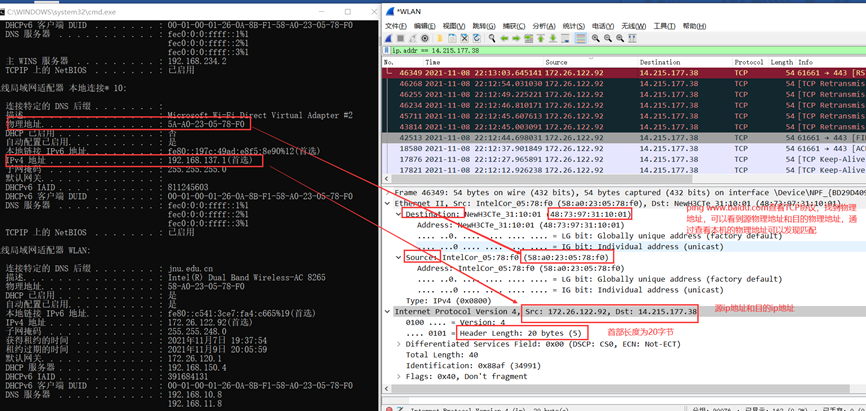
## 【实验环境】

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。

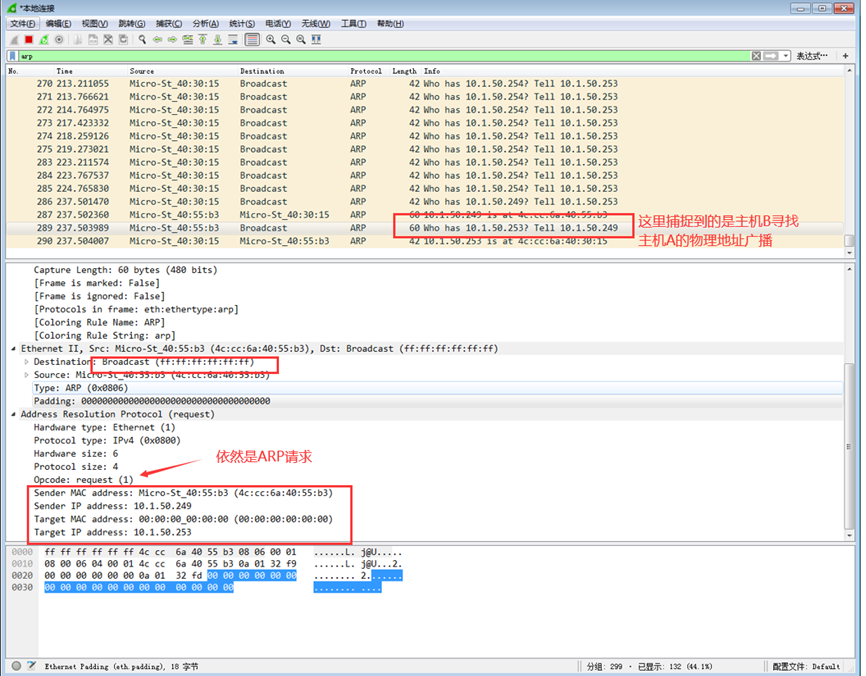


1. ARP协议分析

* 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）；



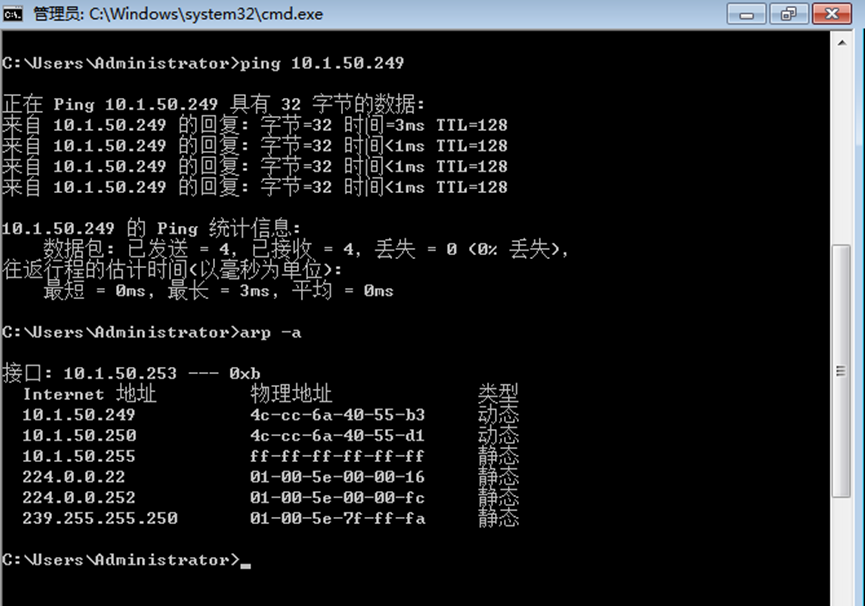
* 运行Wireshark程序；
* 把网线断开1分钟，然后再联网，观察此时是否能捕获ARP报文，如果能，记录并分析各字段的含义；

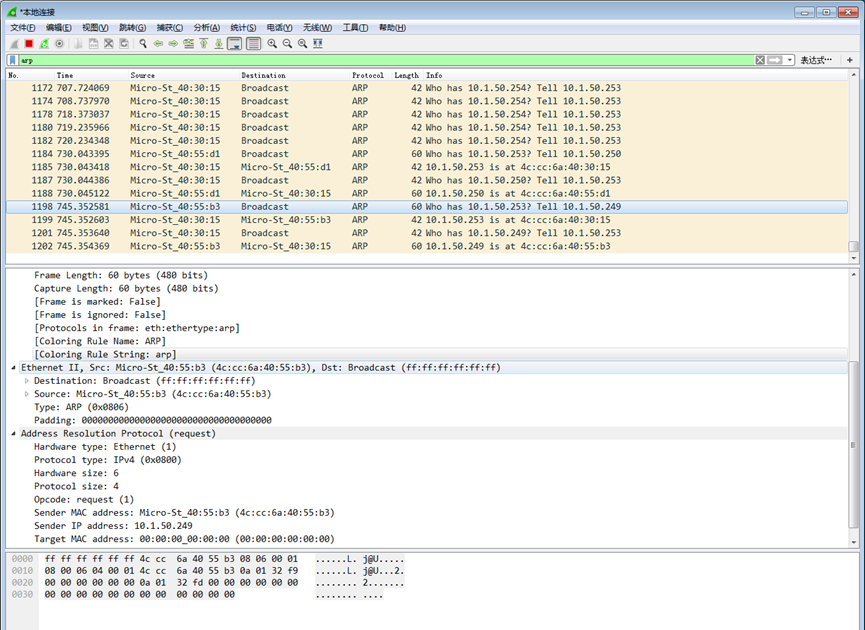


* 从主机A上向主机B发PING检测报文，观察此时是否能捕获ARP报文，如果能，记录并分析各字段的含义；

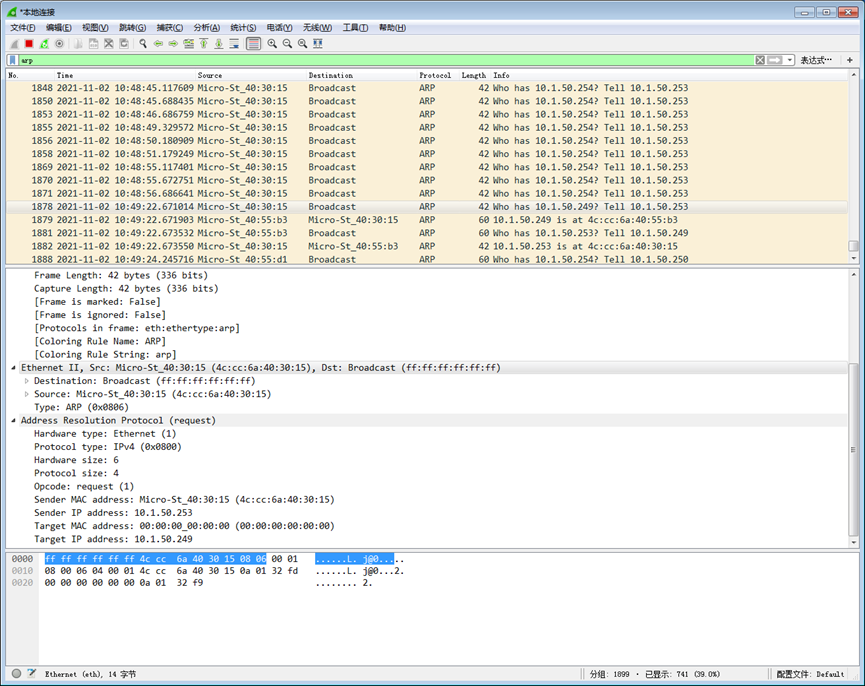
分析：断网后表中只有一个固定的地址，我推测可能是交换机的地址，连上网后，主机A开始发送广播信号，询问某些ip的mac地址是什么，然后该ip地址能给予回应。之后主机A的arp表更新。

* 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；



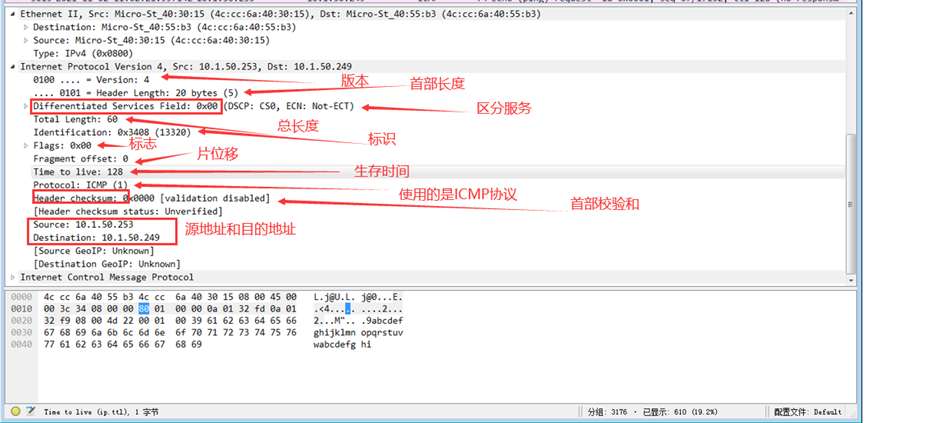
* 再次从主机A上向主机B发PING检测报文，或者再次从主机B上向主机A发PING检测报文，观察看此时是否能捕获ARP报文；
* 
* 主机A上和主机B停止进行任何数据通信，5分钟后再次从A向B发PING检测报文，或者从主机B上向主机A发PING检测报文，观察看此时是否能捕获ARP报文。

可以

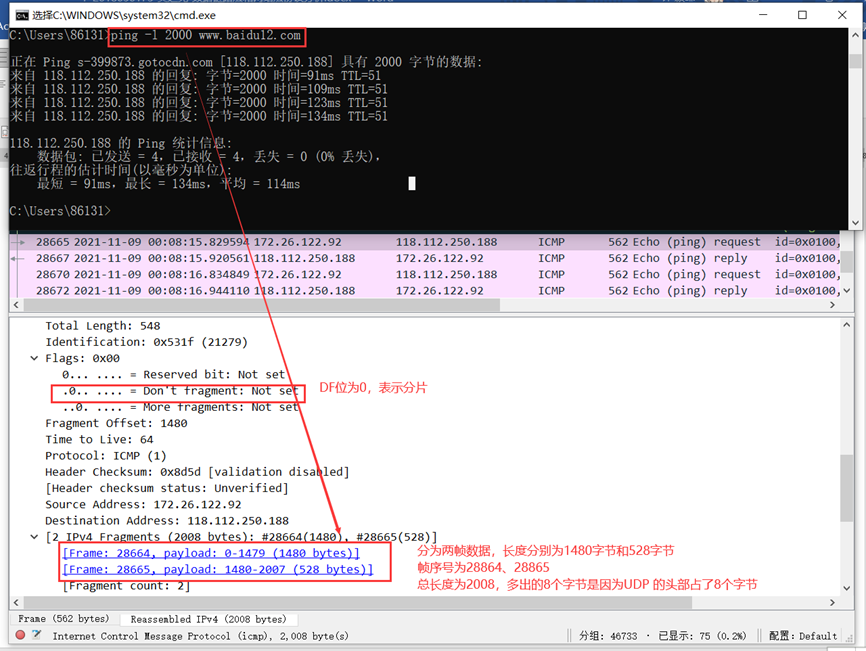


4、IP协议分析

* 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。



注:fragment offset不为0时，用于重组时判断该片相对于数据字段起点的距离。

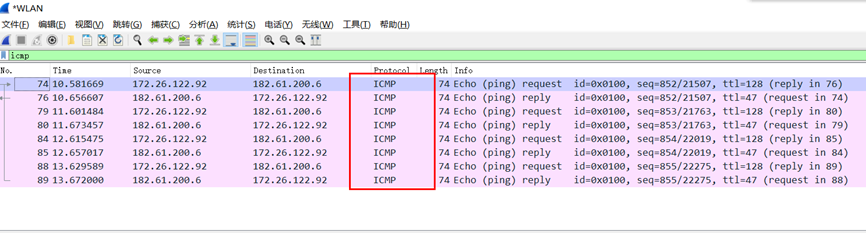
分析：超过1500字节的数据会被IP协议分为两个帧进行封装，猜测Wireshark为了方便用户查看本次ip命令的数据，将icmp存储了所有分片的信息，但是实际上，每个ip片只能有1500字节的数据。对比发现，ICMP和IP的数据包的格式相似。

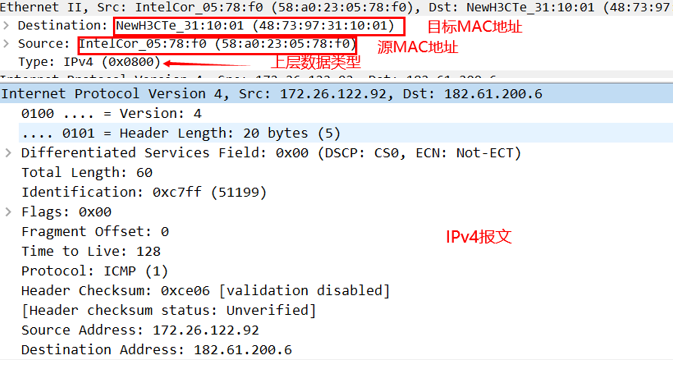
1. ICMP协议分析

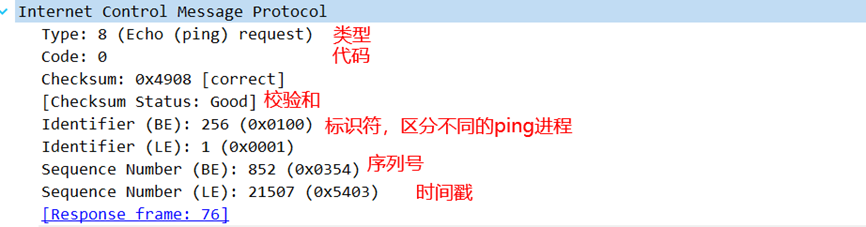
通过ping和tracet命令，了解ICMP协议的使用。

* 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。

正常情况

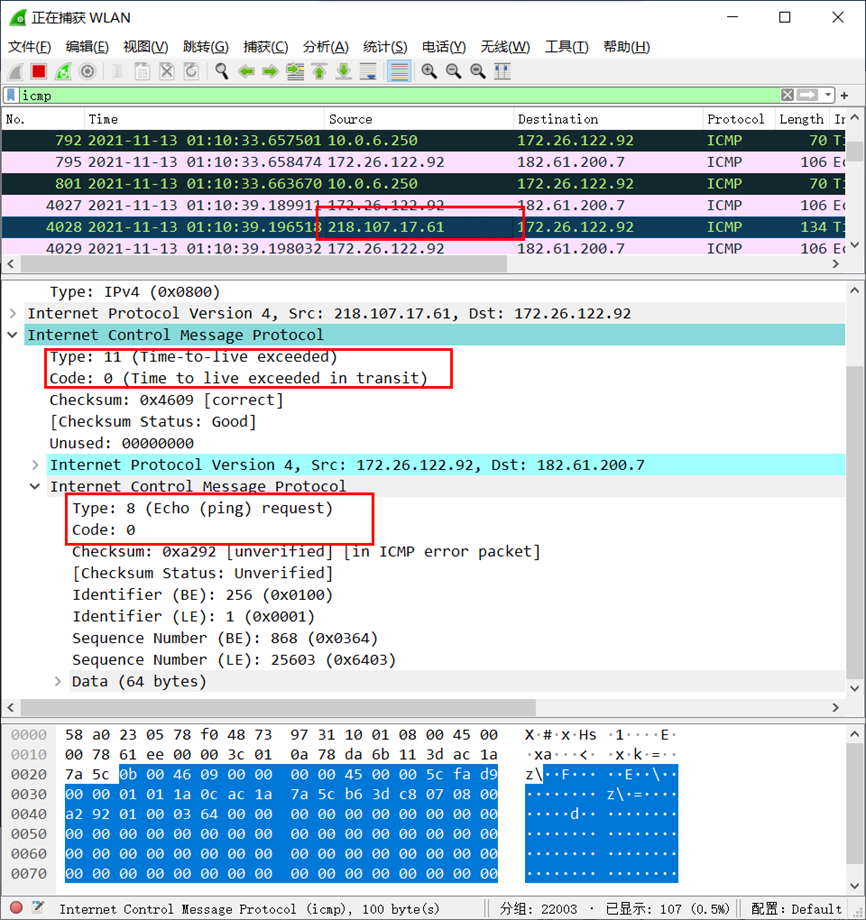




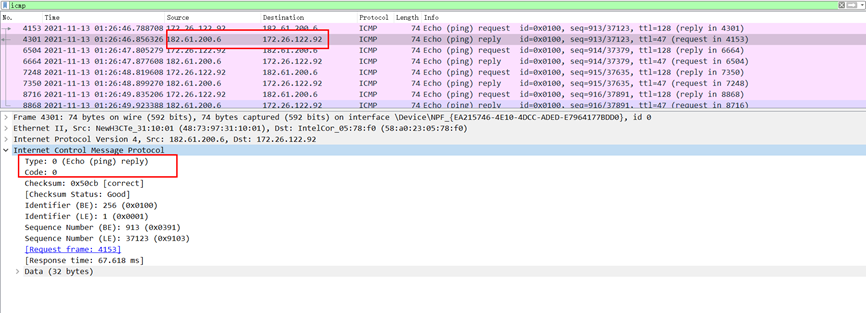


* 使用tracert命令，跟踪某台主机，使用wireshark捕获数据包，分析不同类型ICMP响应数据包格式（如type=8,type=0,type=11）。分析tracert工作原理。

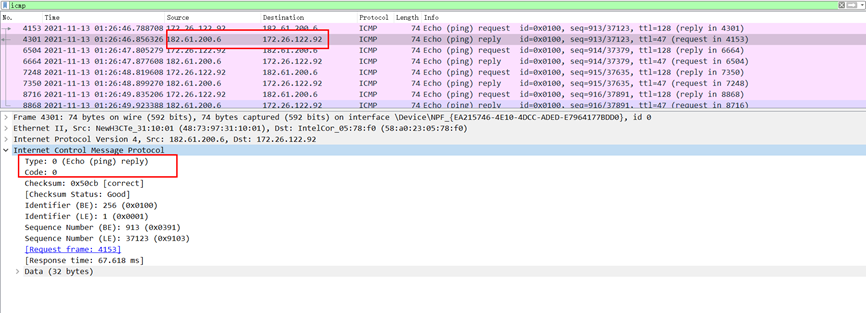
ICMP响应数据包格式 type=0,type=8的情况如上,都是属于正常信息。type=11是属于ICMP超时的差错报文。但是在实验过程中一直没有捕获到type=11情况，所以以分析type=3即“Destination Host Unreachable”来进行替代。



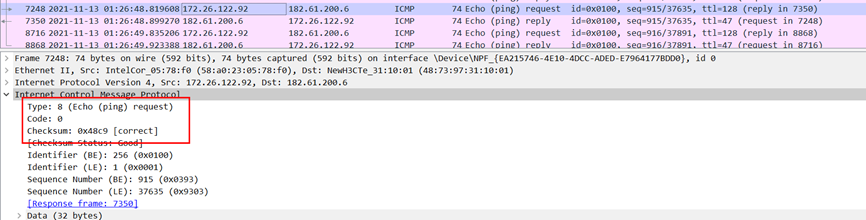
类型11代码0，传输时超出TTL，分析可知时本机向目的地址请求超时。



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

**Tracert工作原理：**

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。

**【思考题】（分析原因并通过实验验证）**

Q1.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？

A1.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。

Q2.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？

A2.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，就会将数据包送回环回接口，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。

Q3.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？

A3.

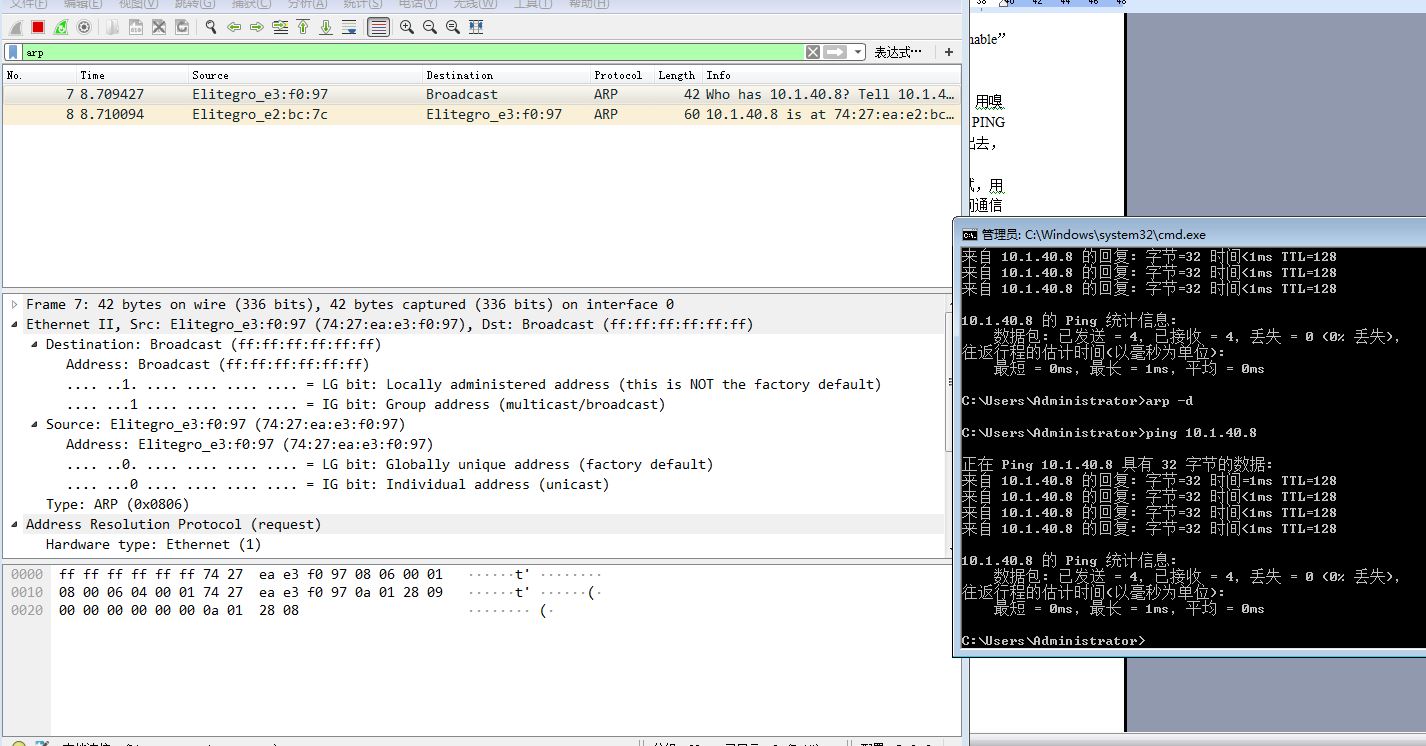
(1)“Request timed out”是请求超时，此消息表示在1s的默认时间内没有收到Echo Reply消息。这可能是由于许多不同的原因造成的。最常见的包括网络拥塞，ARP请求失败，包过滤，路由错误或无声丢弃。

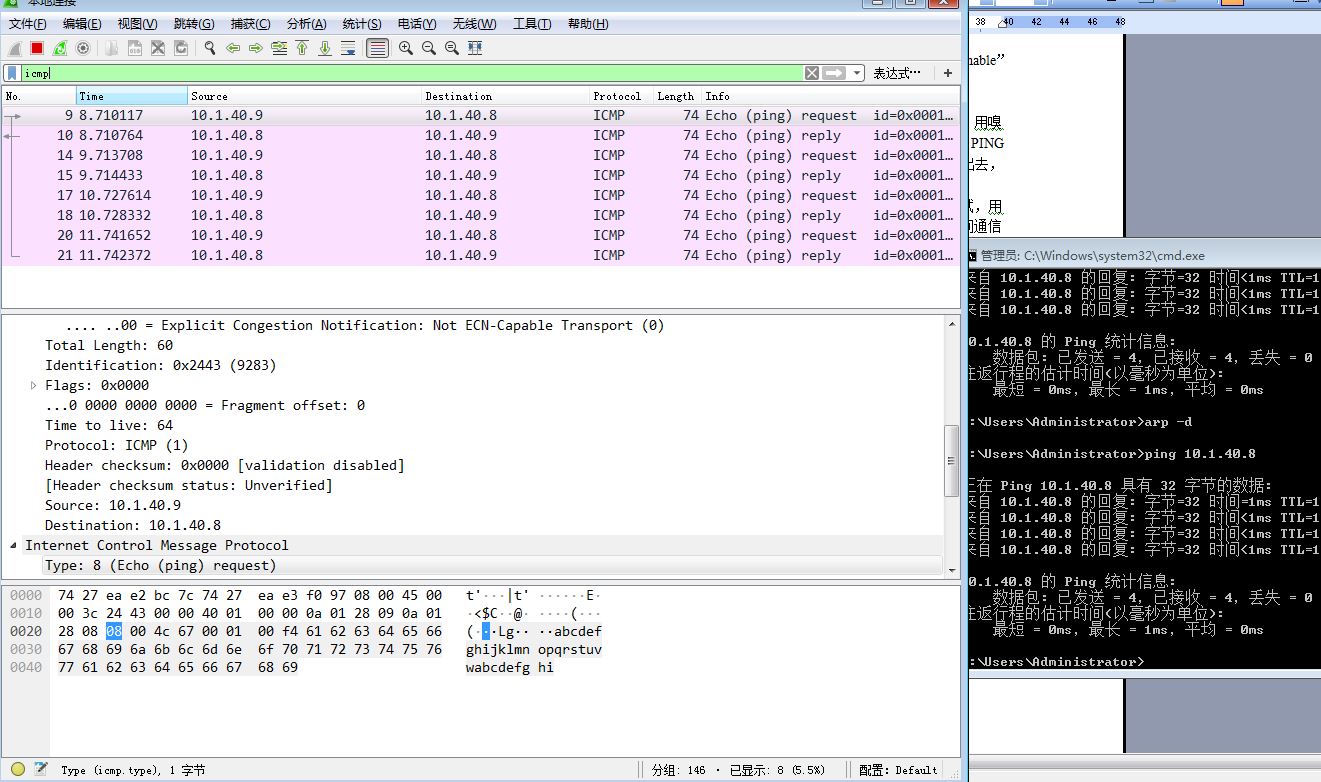
(2) “Destination Host Unreachable”是目标主机不可达，此消息表示本地系统没有到达所需目标的路由，或者远程路由器报告没有到目的地的路由。如果该消息只是“Destination Host Unreachable”，那么没有来自本地系统的路由，并且发送的数据包不会被放在线路上。如果消息是“Reply From <IP address>:Destination Host Unreachable”，则路由问题发生在远程路由器，其地址由“<IP address>”字段指示。

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）。

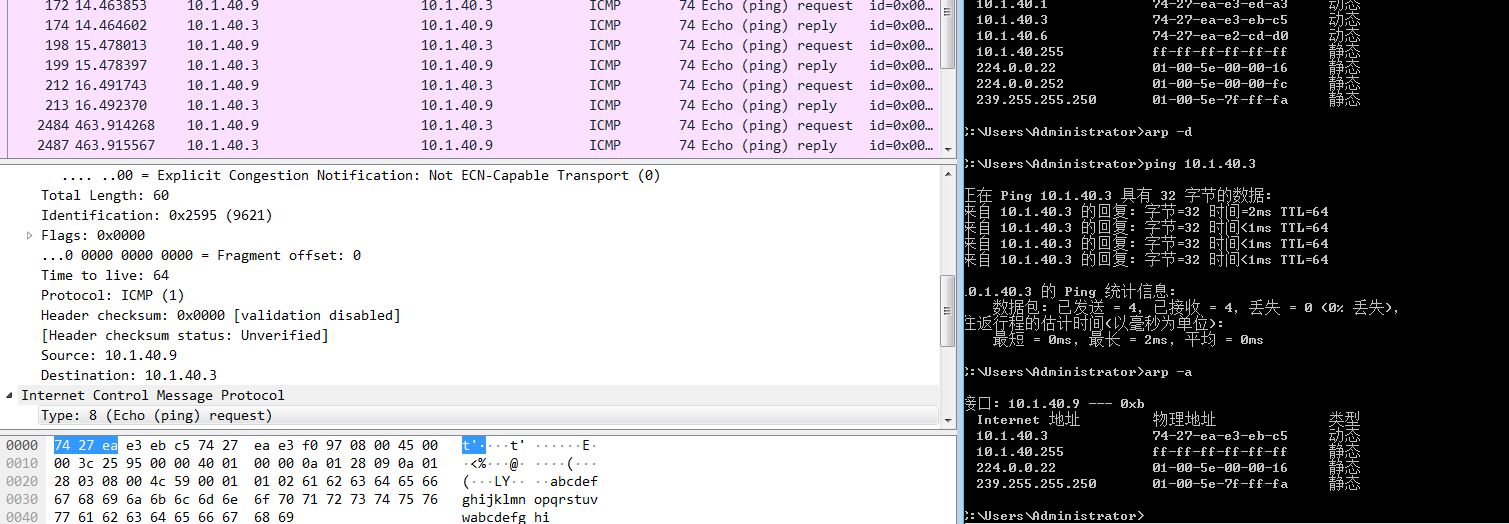


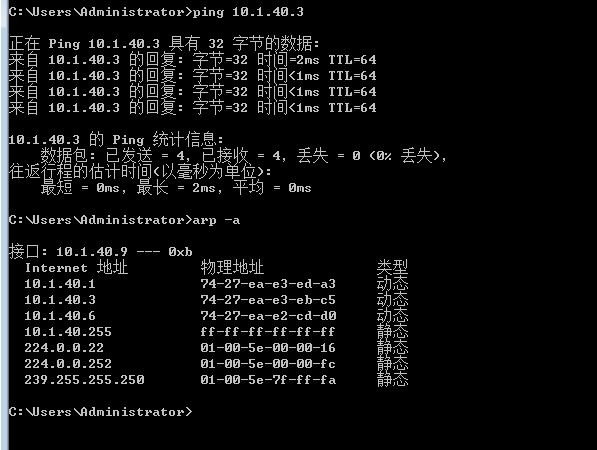


实验结果表明，该猜想正确。

5、通过下面实验**理解网关**

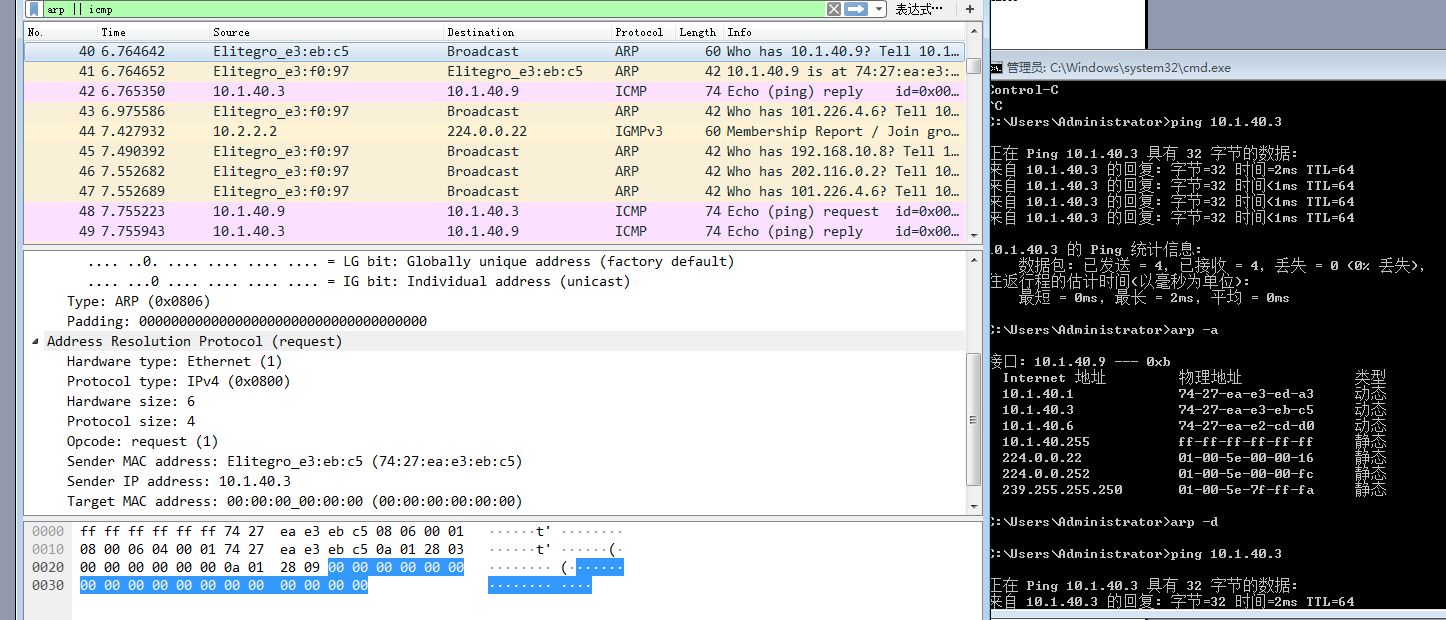
假设主机A的IP地址为10.2.2.2/23，主机B的IP地址为10.2.3.3/23，两台主机均不设置网关，用ping命令测试两主机的连通性，用ARP命令查看物理地址。对结果进行分析。





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。

答:即使没有设置网关，两台主机也是在同一个局域网，即处于同一个网段内，因此互相两台主机之间是可以ping通的，使用ARP命令也可以查看到对方的MAC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。

答：如果将主机的网关设置为本机地址，则无法ping通，因为此时两台主机在逻辑上已经划分为不同的网段了，因此无法ping通。

## 【实验总结】

通过本次实验，我理解了链路层、网络层主要协议格式，以及协议的工作原理。此外，我还理解了网关和子网掩码概念。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。通过查找资料，我了解了Tracert命令的原理，即: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。