**暨南大学本科实验报告专用纸**

课程名称 计算机网络实验 指导教师 潘冰 成绩

实验项目名称 数据链路层和网络协议层分析 实验项目编号 7

实验项目类型 验证 实验地点 计算机网络实验室 学院 智科院 专业信息安全

学生姓名 梁峻铭 学号 2019051103 实验时间 2021 年 11 月 8 日

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**

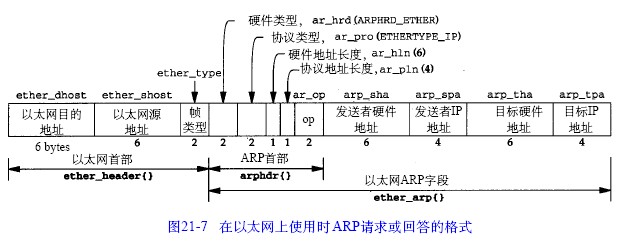
**1、网络嗅探器**

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**

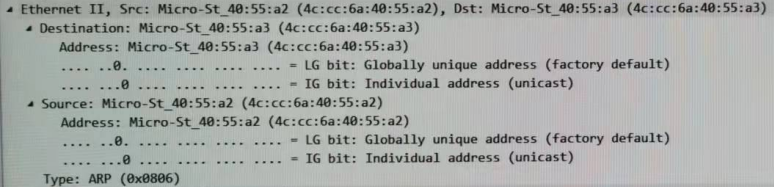


1. **实验环境**

计算机2台，交换机一台。

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

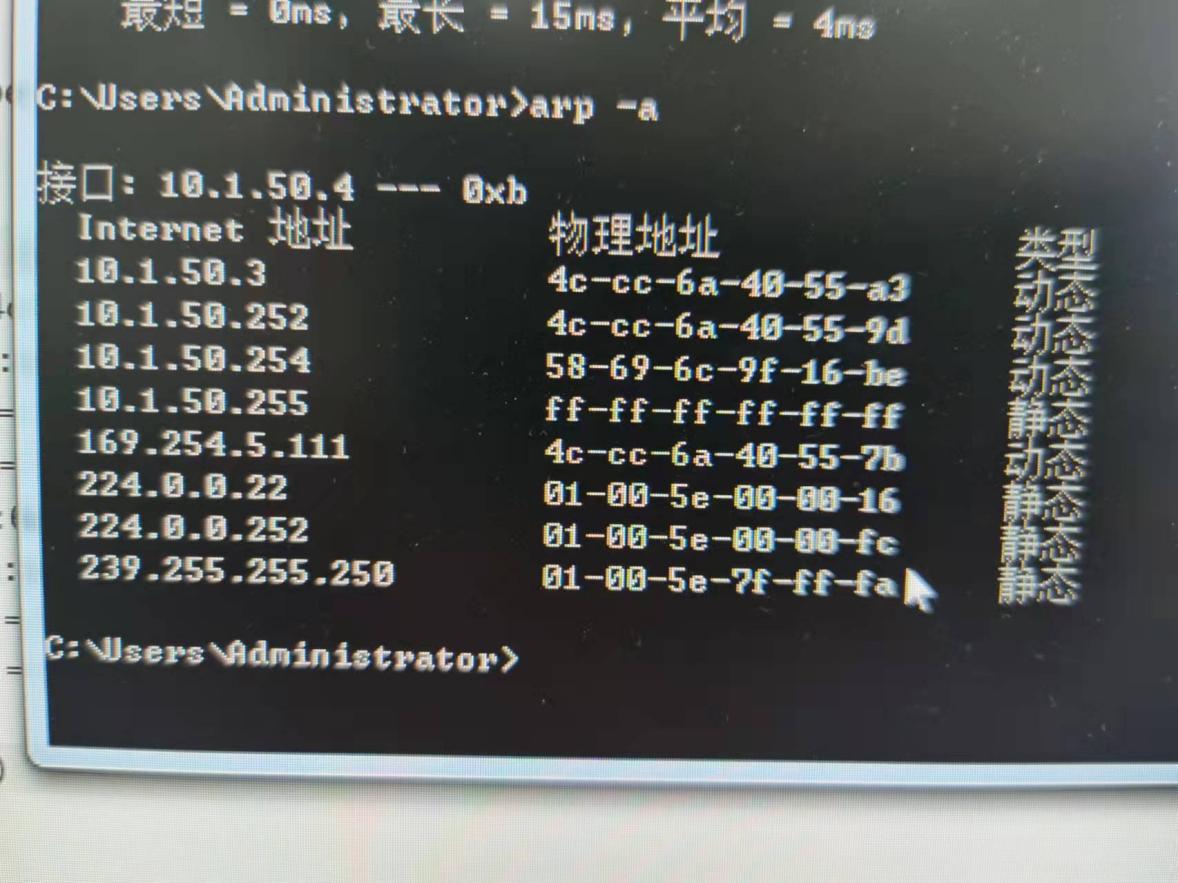
从主机A上向主机B发PING检测报文，捕获以太数据帧，记录并分析MAC帧各字段的含义。



Destination为主机B的硬件地址，而Source则是主机A的硬件地址。

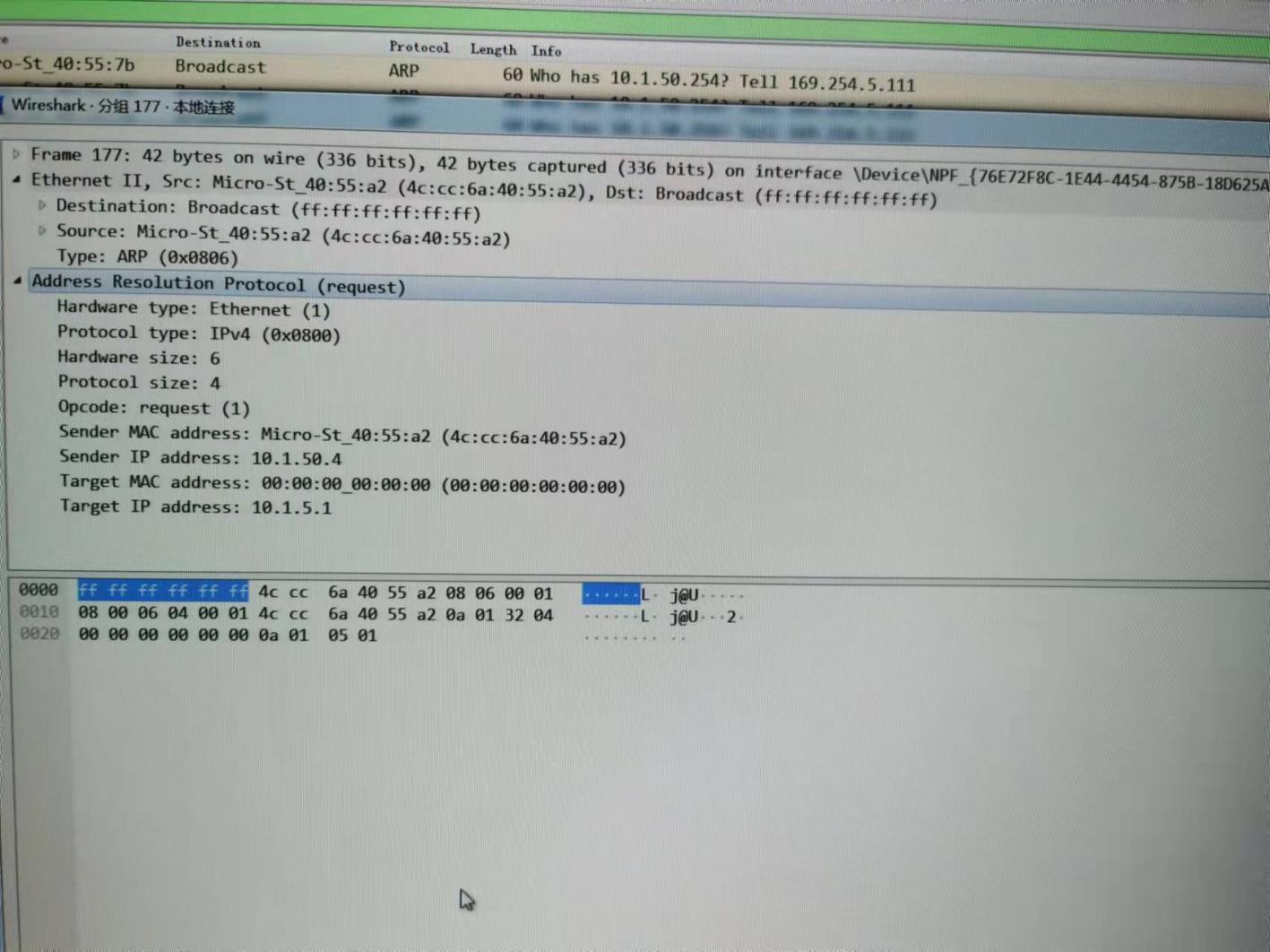
1. **ARP协议分析**

* 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；

能捕获到。



其中，hardware type为硬件类型，portocol type为协议类型（图中为IPV4）。下方则是源/目标MAC地址，源/目标IP地址。而OPCODE则是操作码1代表请求报文。

* 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；

观察到不能，主机A的ARP表中已经存在主机B的硬件地址，无需再广播。

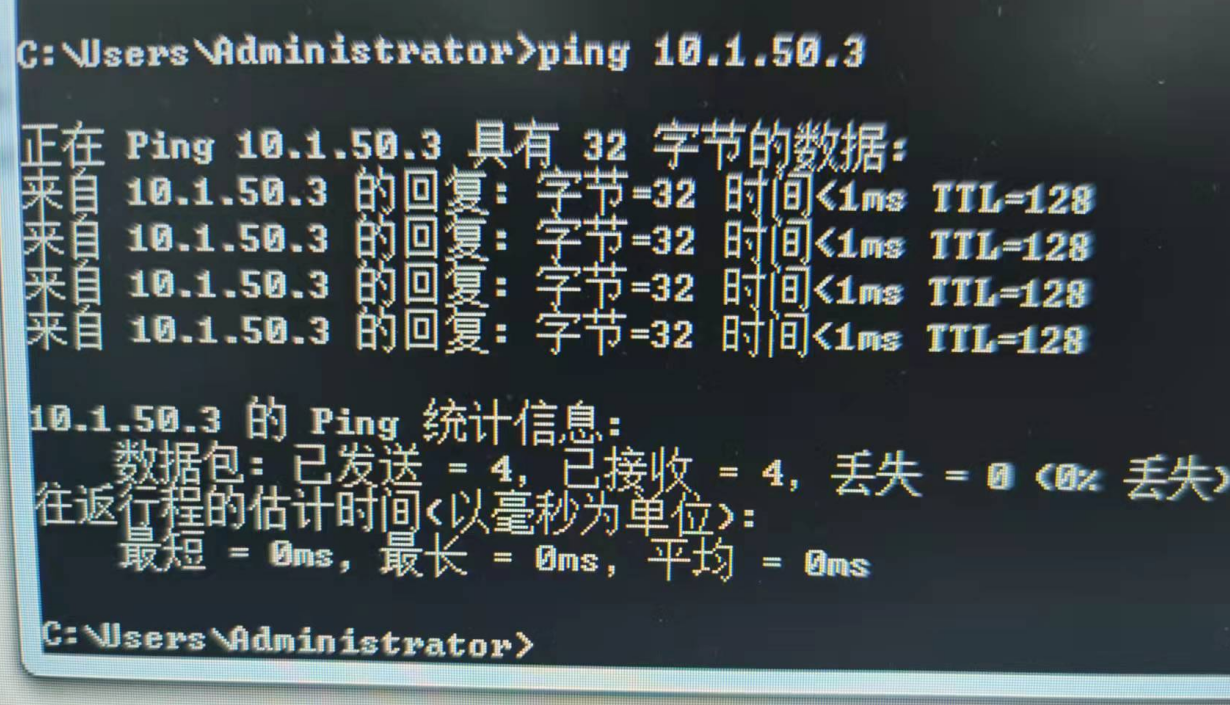
* 主机A上和主机B停止进行任何数据通信，5分钟后再次从A向B发PING检测报文，或者从主机B上向主机A发PING检测报文，观察看此时是否能捕获ARP报文。

观察到，不能够捕获到ARP报文。但是用arp-d命令将主机B的记录删除后则可以捕获的ARP报文，猜测缓冲表中的数据更新时间大于5分钟。

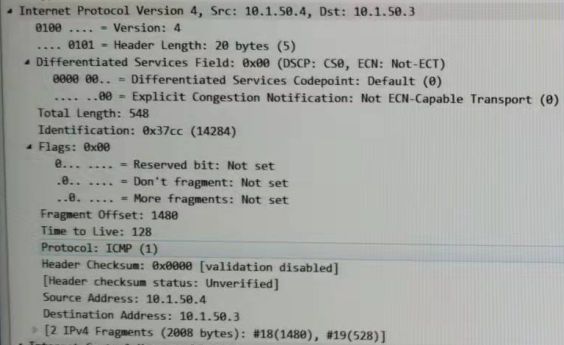
**4、IP协议分析**

* 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;

检测报文如下：

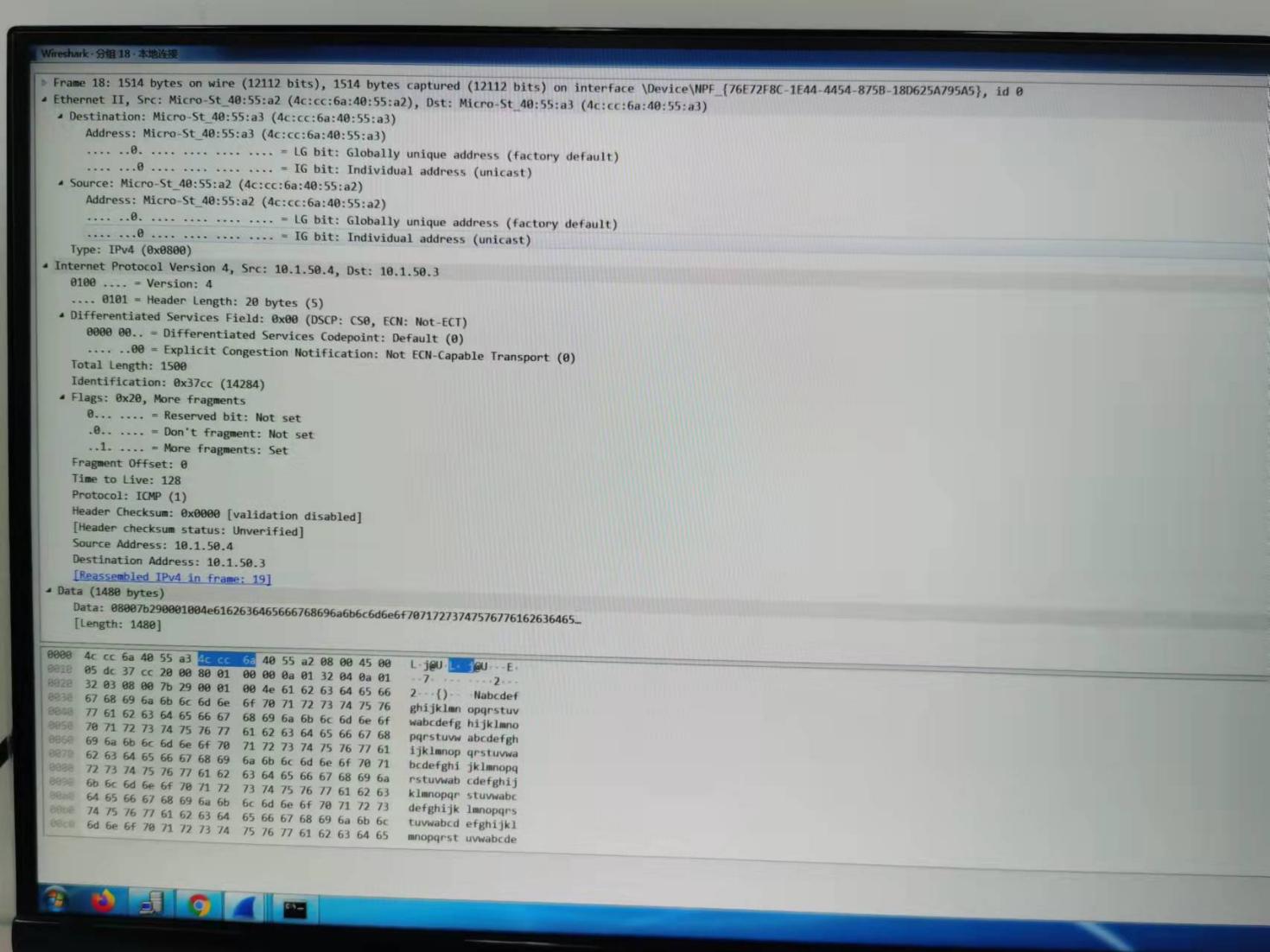


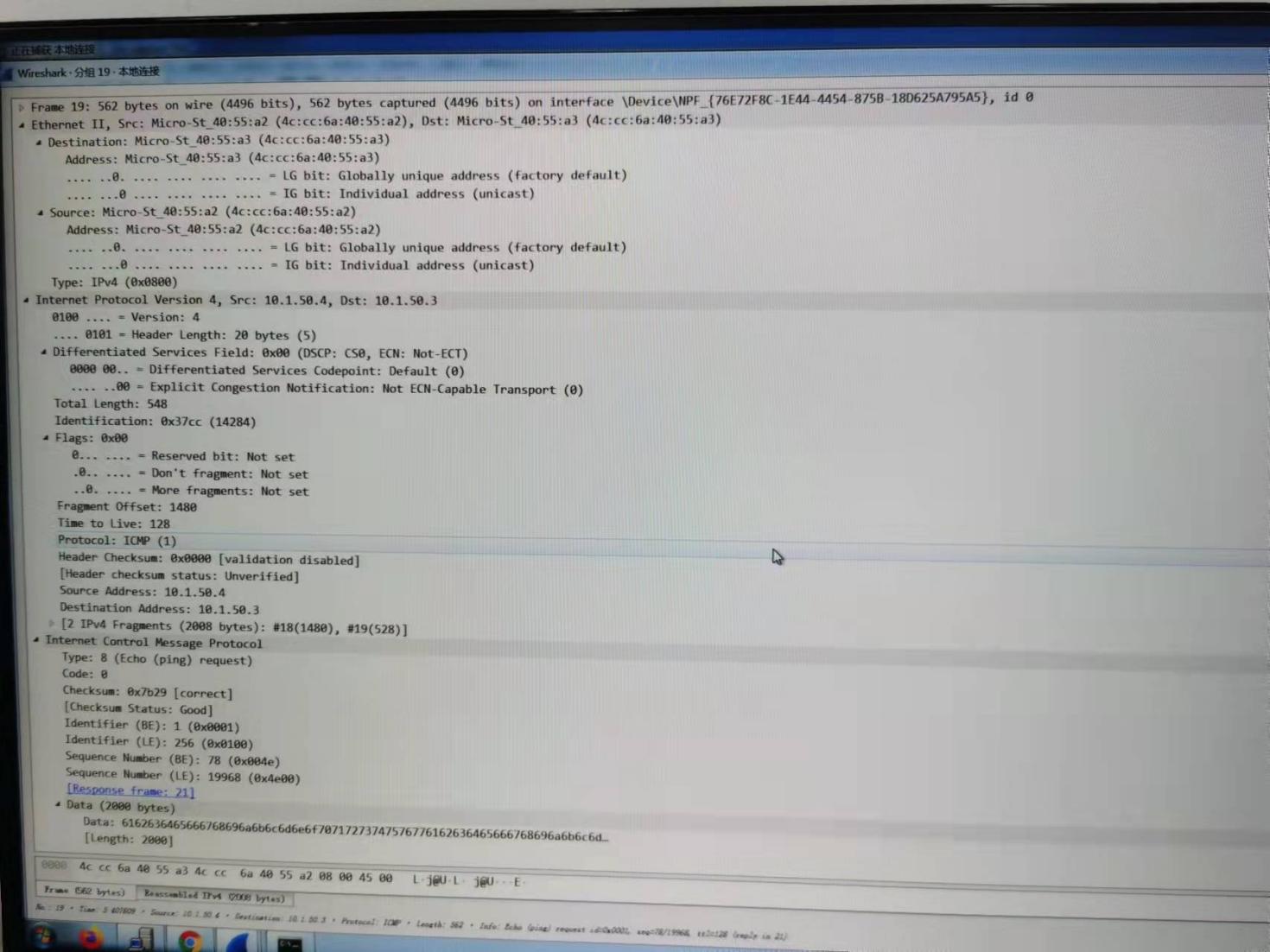
用WIRESHRAK捕获IP数据包：



如图所示，协议的版本号为IPV4，IP头部长度为5，数据总长度为548（头部+数据），标识位是14284，片偏移是0（此处没有发生分片重组），128则是IP数据包被路由器丢弃前允许通过的最大网段数，使用ICMP协议，header checksum则是首部校验。

* 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。





如图所示，图一中MF=1表示后面还有分片，而图二中MF=0则表示当前是最后一个分片。且当中间字段DF位0时才允许分片。图中片位移位1480，与图一中数据段长度相符合。

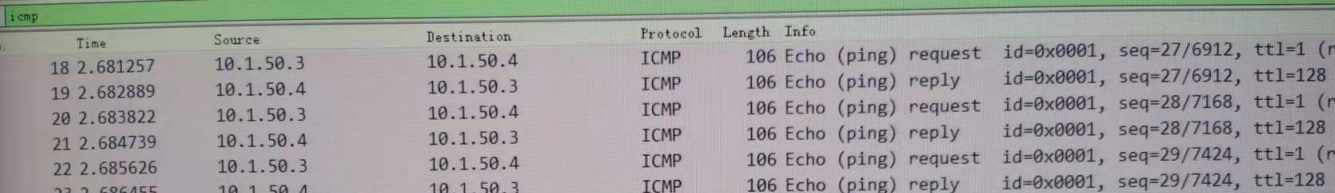
分片过程：IP数据报在传输时需要经过多个物理网络，而由于它们之间的介质和物理性质的不同，在传输时对数据帧的最大长度有一个限制，因此要进行分片。分片时把标识复制再将其分给每个分片的头部。

重组过程：分片后的数据抵达目的主机后，根据片偏移来确定分片的顺序，根据标识来逆向解析。

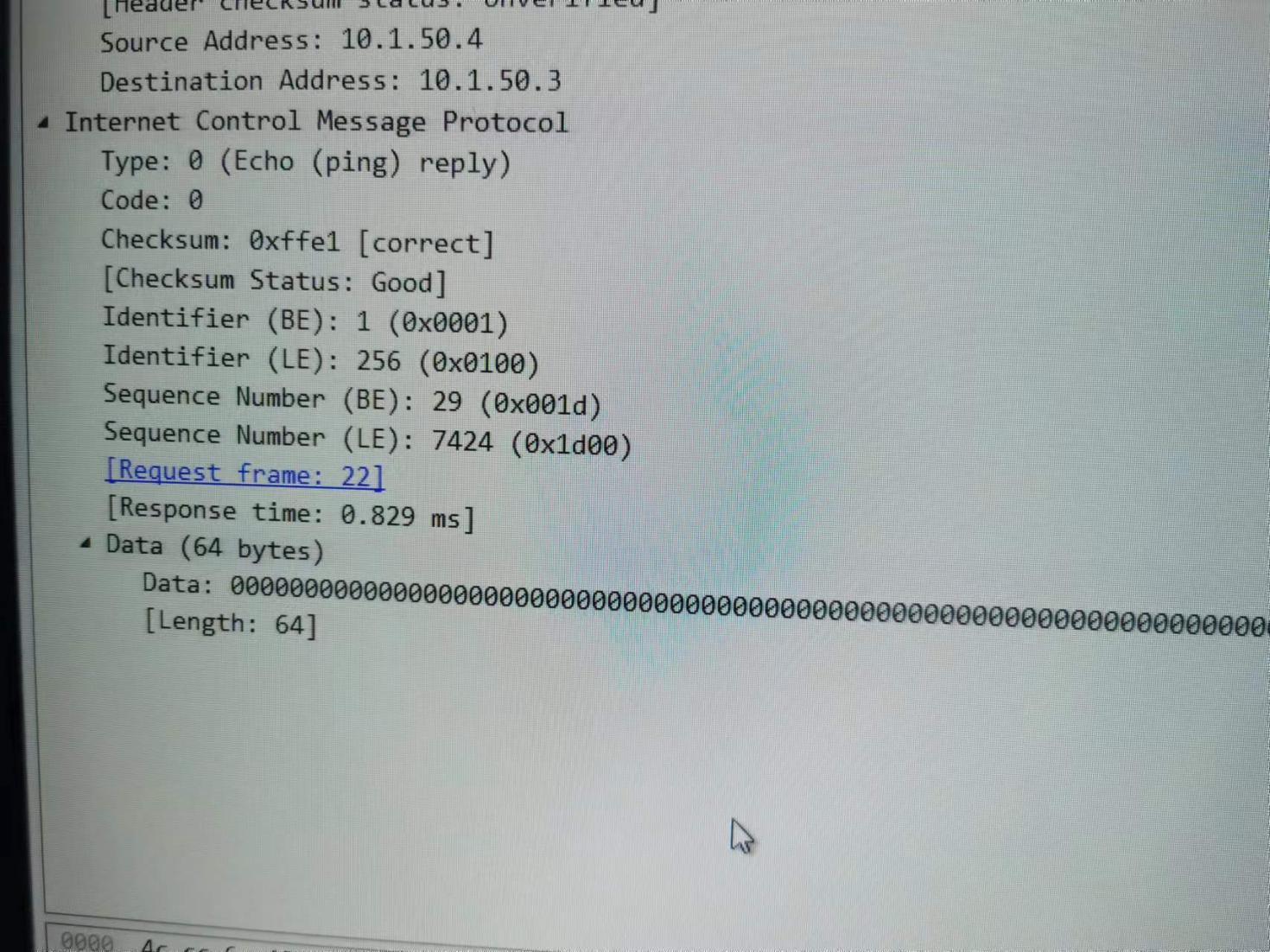
1. **ICMP协议分析**

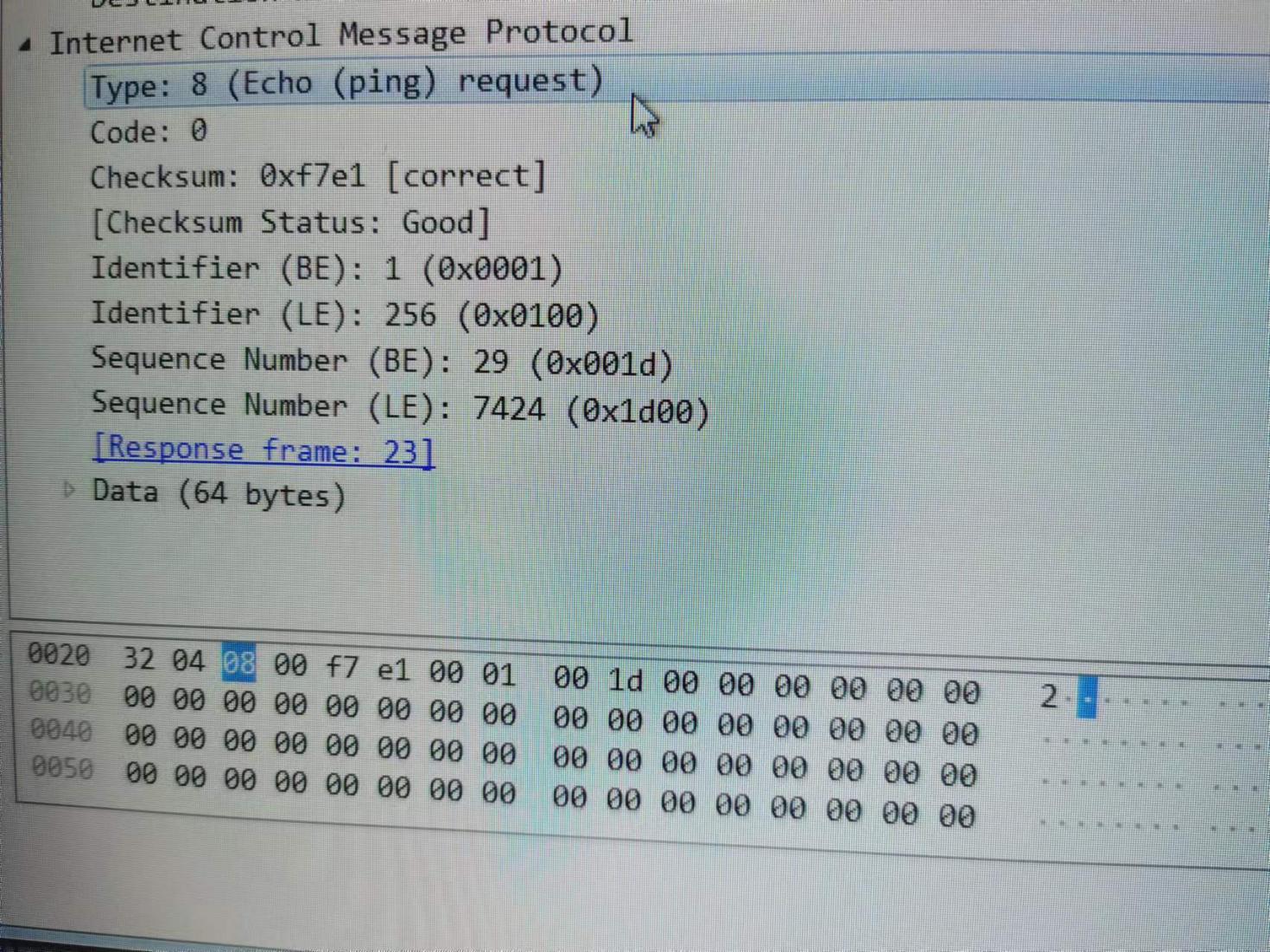
通过ping和tracet命令，了解ICMP协议的使用。

* 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。



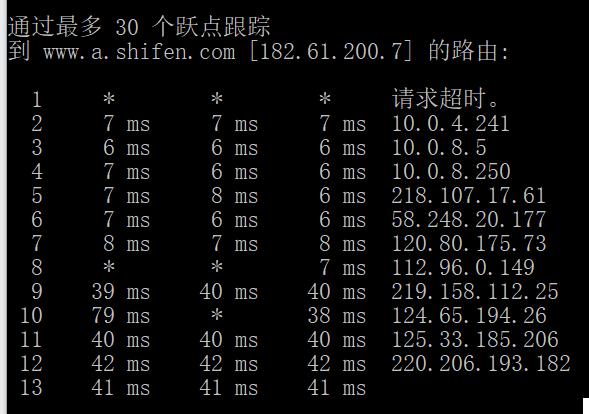
如图所示：TYPE为0表示它是响应报文

如图所示：TYPE为8表示它是请求报文



以上两种均为询问报文。还有实验中未能验证的类型3（终点不可达）、类型4（源点抑制）、类型11（超时）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。



Tracert命令诊断实用程序通过向目标计算机发送具有不同生存时间的ICMP数据包，来确定至目标计 算机的路由，也就是说用来跟踪一个消息从一台计算机到另一台计算机所走的路径。

该诊断实用程序将包含不同生存时间 (TTL) 值的 Internet 控制消息协议 (ICMP) 回显数据包发送到目 标，以决定到达目标采用的路由。要在转发数据包上的 TTL 之前至少递减 1，但必须经过路径上的每 个路由器，所以 TTL 是有效的跃点计数。数据包上的 TTL 到达 0 时，路由器应该将ICMP 已超时 的消息发送回源系统。Tracert 先发送 TTL 为 1的回显数据包，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。路由通过检查中级路由器发送回的ICMP 已 超时的消息来确定路由。

1. **实验总结**

**思考题：**

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：此问题在本实验中已经得到验证，若缓存表中有目的主机的MAC地址则无需通过广播来寻找其地址，因此此时用wireshark可以捕捉不到ARP报文。若缓存表中的目的主机地址被删除或者需要更新则会出现相反的结果。

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？

答：经过实验，发现前者不会捕获到，而后者会。127.0.0.1是本机的环回地址，运行PING127.0.0.1时直接定向本机而不是通过路由器，可以用来检测TCP/IP协议安装是否正确。因此不经过网卡的话就不会产生ICMP报文。PING本机时交给环回驱动程序处理，会经过网卡，因此可以捕获到报文。

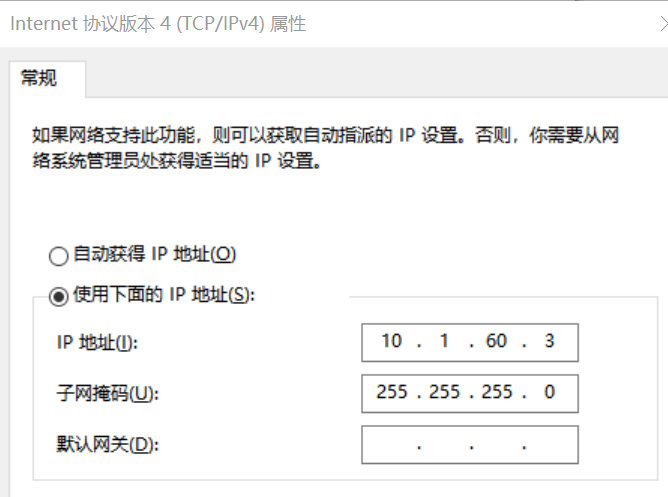
1. 在ping 的过程中，返回信息“Request timed out” 和“Destination Host Unreachable”分别是由哪些情况引起的？

答：“Request timed out”有可能是因为对方主机装有防火墙或者已关机，也有可能是因为本机的IP不正确或者网关设置错误。

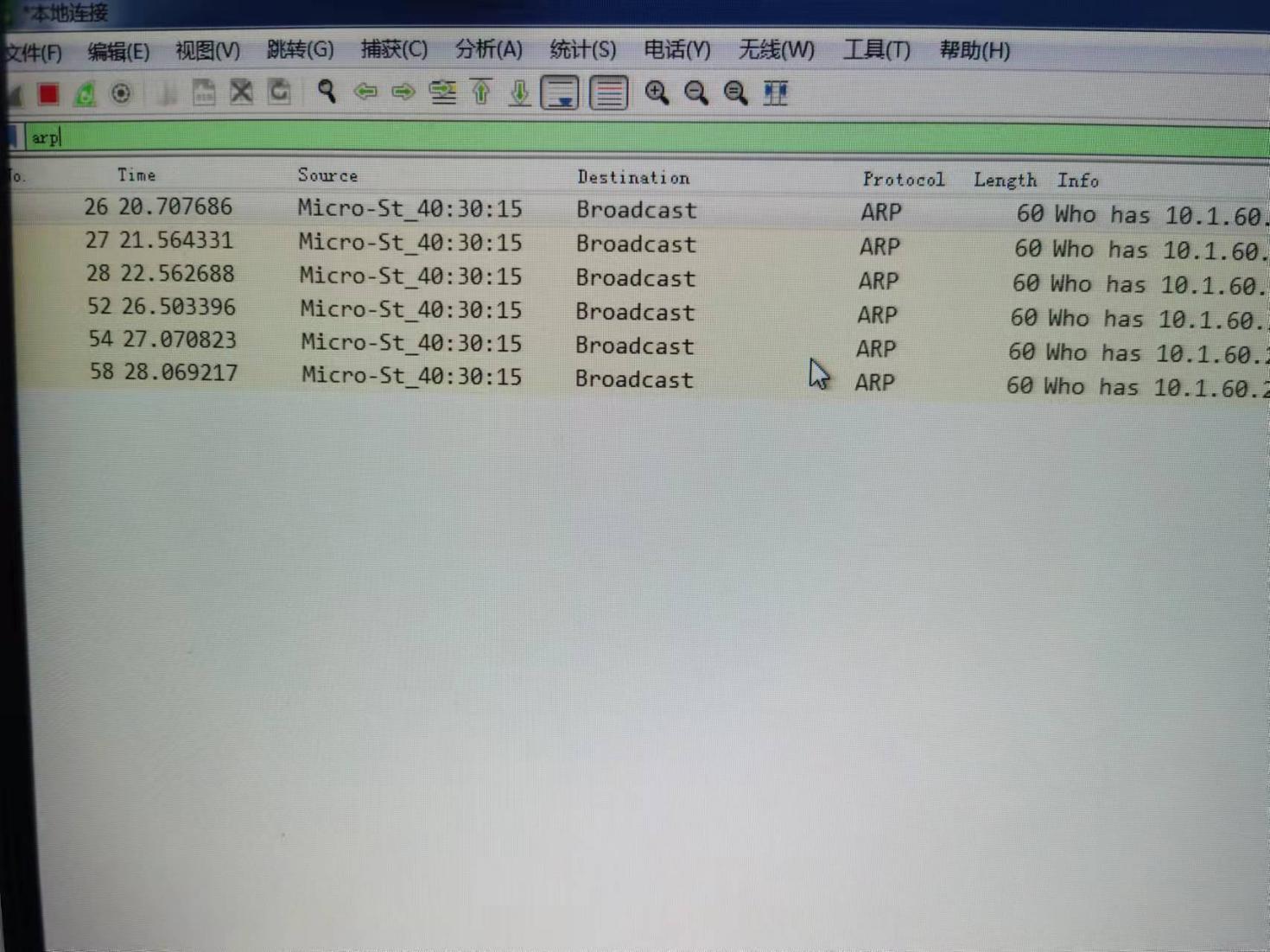
“Destination Host Unreachable”则是目标地址不能到达，有可能是因为DHCP失效或者子网掩码设置错误。

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。



观察到不设置网关时，同一网段的主机可以相互通信，用P嗅探器测试时发现可以捕获到8个ICMP数据包和2个ARP数据包。



在不同网段时，则捕获不到ICMP数据包，同时无法PING通，会显示目的主机不可达。

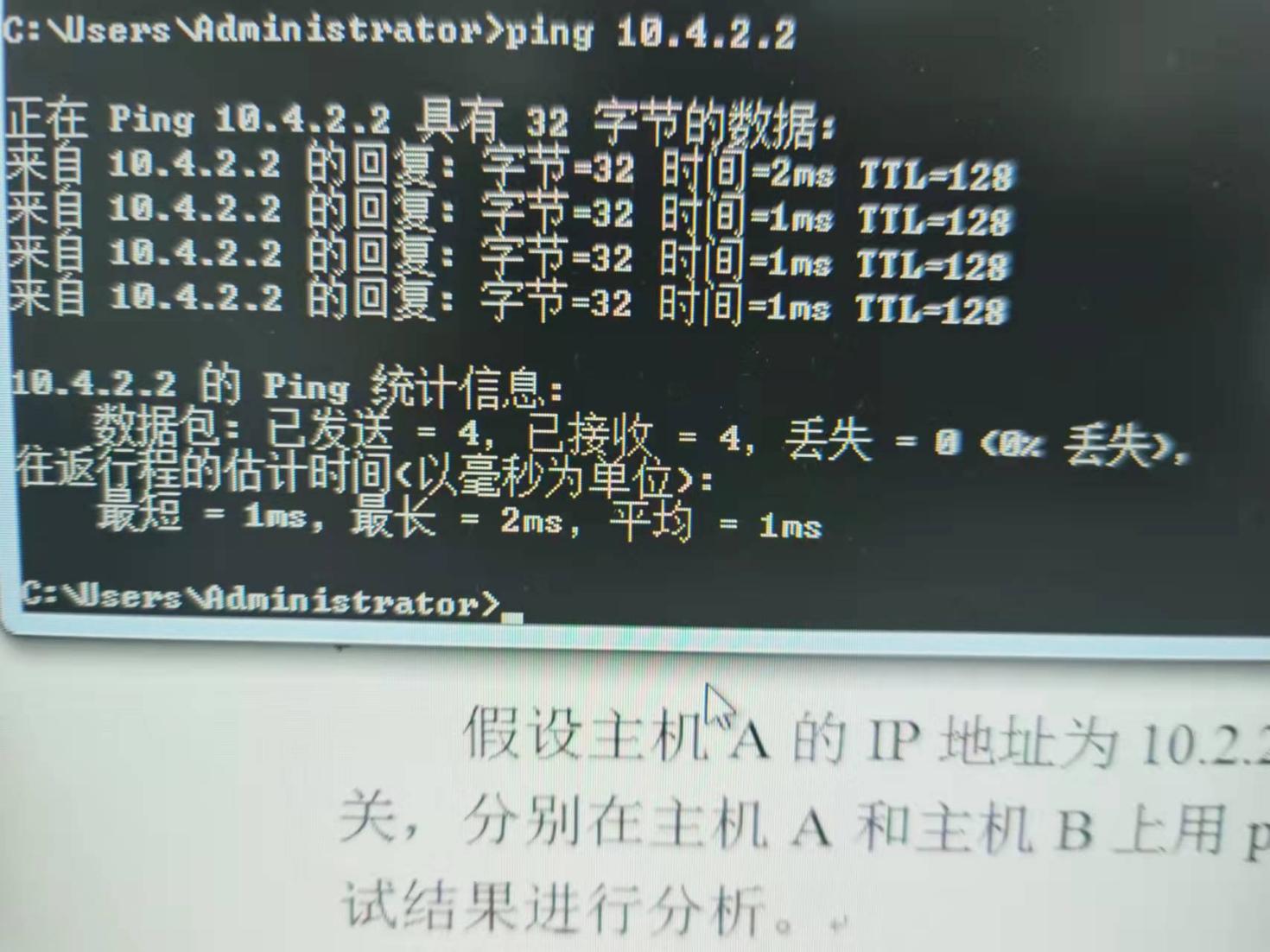
主机如果设置“网关”，同一网段的主机通信不通过网关转发，用ping命令测试，用嗅探器可以捕获所有测试数据包，能看到对方主机的MAC地址。不同网段的主机之间通信需要网关转发，用ping命令测试，能看到网关的MAC地址（包括能通信或不能通信）。

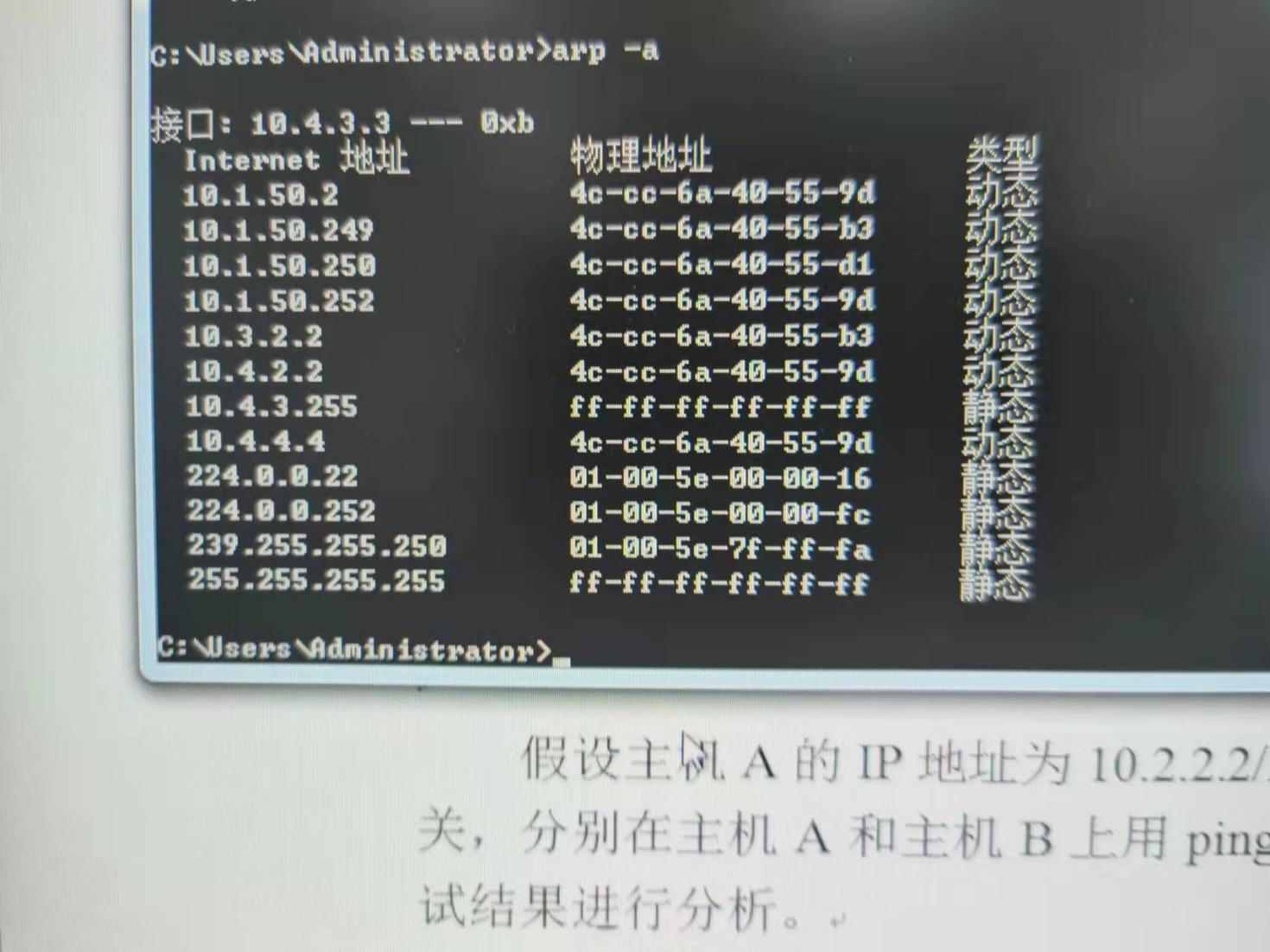
答：设置网关后，同一网段主机无需通过网关转发。修改IP地址，使两台主机处于不同网段，此时可以看到网关和本机的MAC地址。

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。

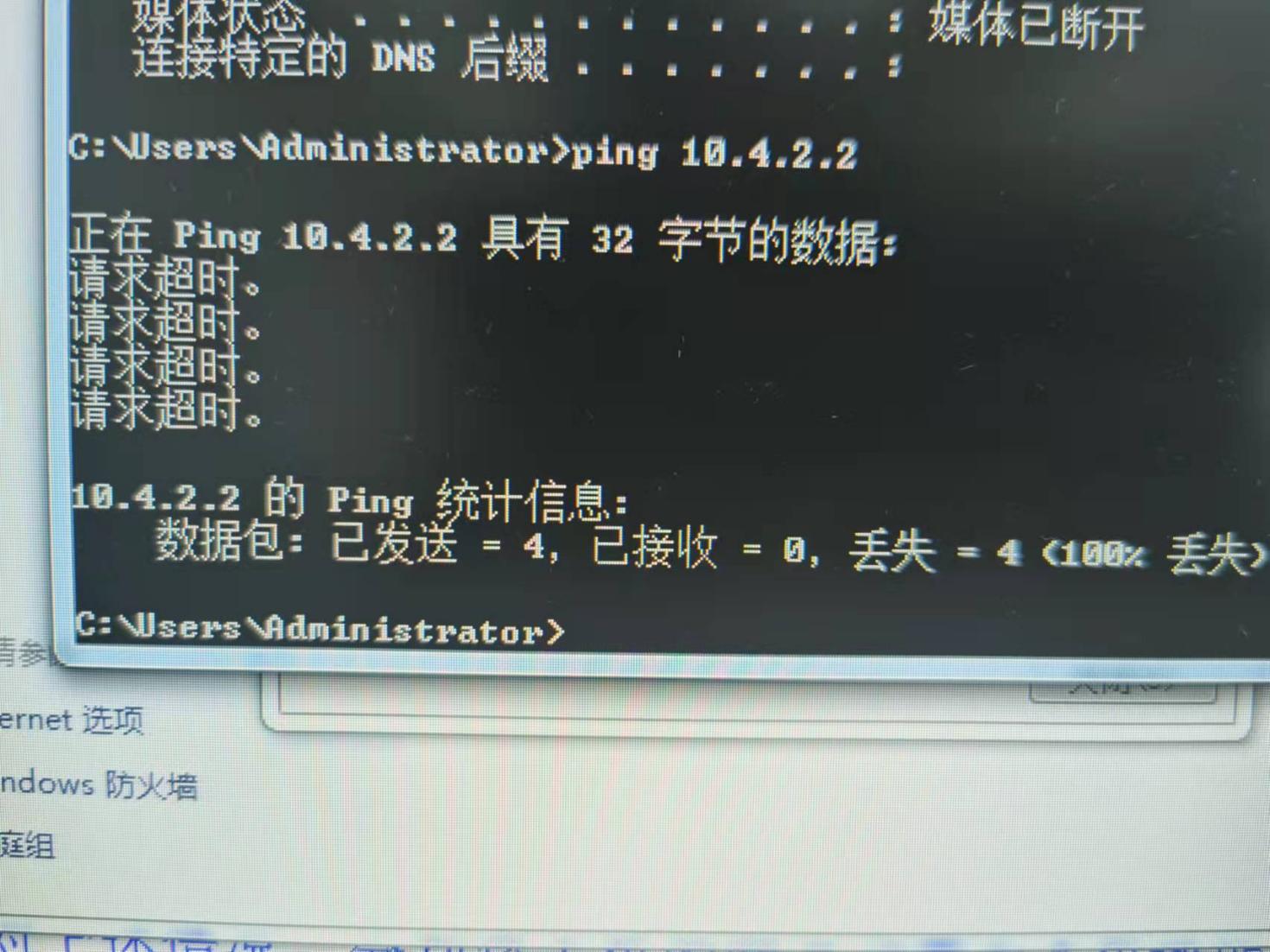
答：本次实验中，设置主机A的IP地址为10.4.3.3，主机B的IP地址为10.4.2.2，设置子网掩码为255.255.254.0此时经过与运算可以得出主机A与主机B处在同一网段，此时两台主机可以相互PING通。





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：将子网掩码修改为255.255.255.0，此时经过与运算后两主机不出在同一网段，在不设置网关的情况下无法PING通，一方显示请求超时而另一台主机显示连接失败，但是在ARP表中可以查看到主机B的硬件地址。



总结：通过本次实验，加强了对链路层网络层相关概念和工作模式的理解，熟悉了各个协议的格式和其基本含义。在一些细碎知识点比如IP数据报的分片和重组方面也通过实践，加强了对这个过程的深入理解、然而本次实验也存在不足之处，比如在机房进行试验时没有做到效率最大化，且粗心大意忘记了一些数据的截图。希望今后的实验能够更加改善不足之处和保留做的好的方面，加强对知识的掌握。