《计算机网络》实验报告

(2023~2024 **学年第一学期**)

实验名称：Wireshark 软件使用与 ARP 协议分析

学　　院：软件学院

姓　　名：陈高楠

学　　号：2112966

指导老师：张圣林

2023 年 11 月 5 日

目录

实验 1:Wireshark 软件使用与 ARP 协议分析

1 实验目的

学习 Wireshark 的基本操作，抓取和分析有线局域网的数据包；掌握以太网 MAC 帧的基本结构，掌握 ARP 协议的特点工作过程。

2 实验条件

设备：PC 机一台，连入局域网；

软件：Wireshark 软件，建议 3.0 以上版本。

3 实验报告内容及原理

3.1 学习 Wireshark 基本操作

学习 Wireshark 基本操作：重点掌握捕获过滤器和显示过滤器。

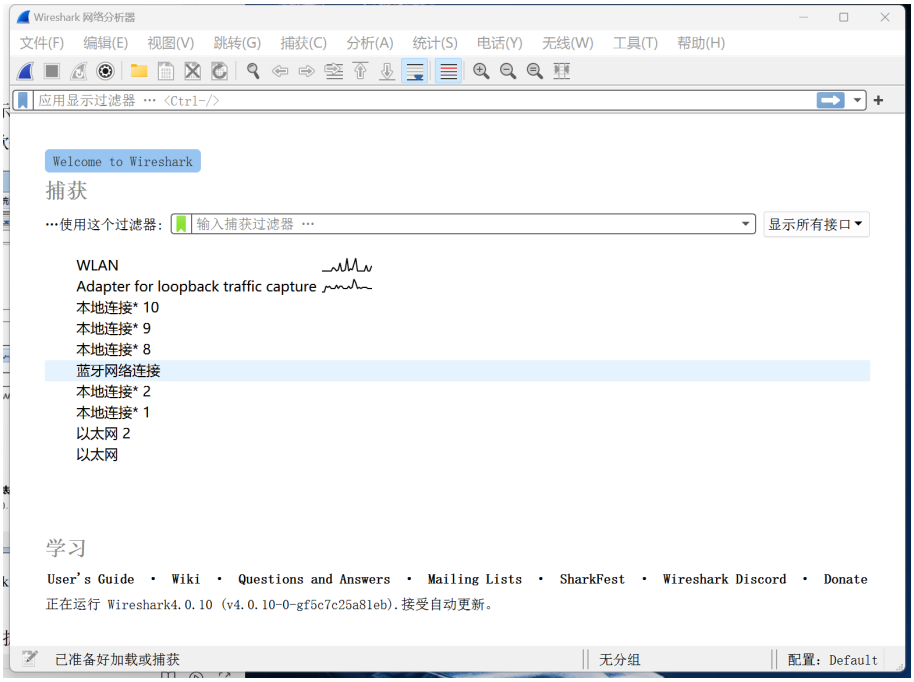

图 1: Wireshark 初始界面

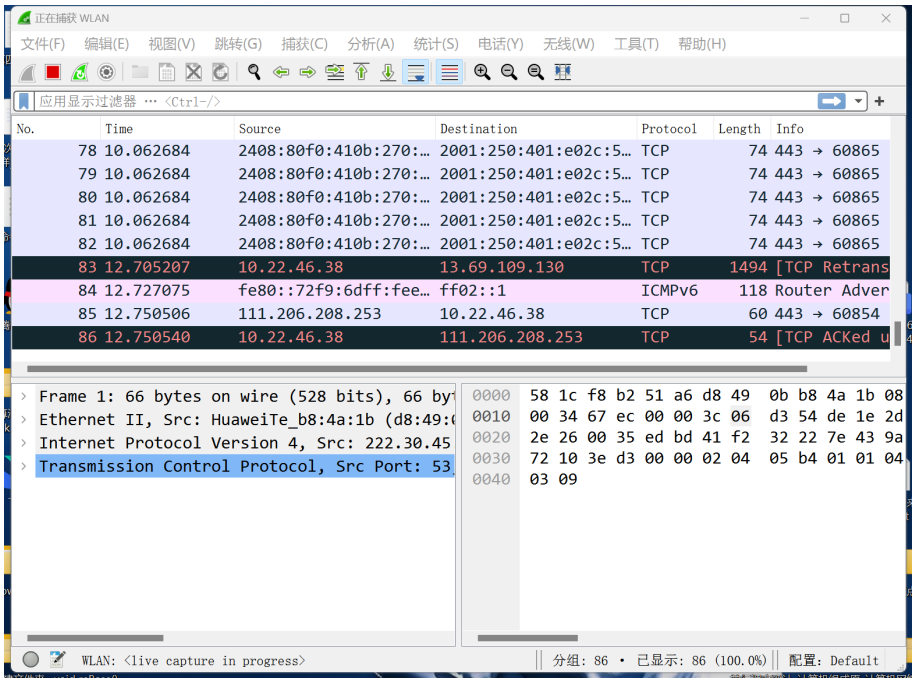

图 2: 进入后的界面

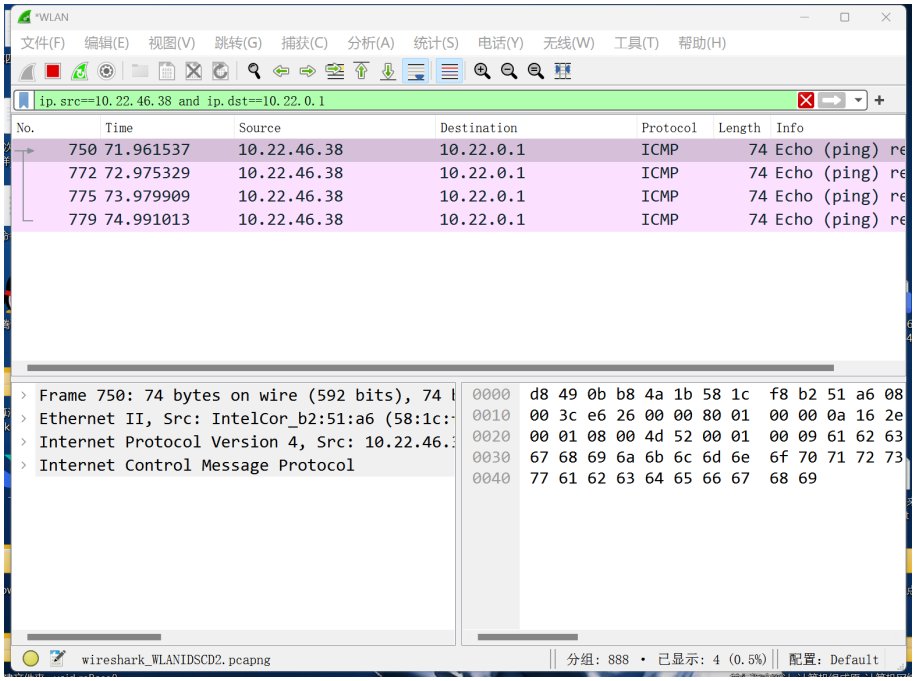

图 3: 筛选器

3.2 观察 MAC 地址

3.2.1. 启动 Wireshark 捕捉数据包，在命令行窗口分别 ping 网关和 ping 同网段的一台主机，分析本机发出的数据包。

先用 ipconfig 查看网关以及本机地址。

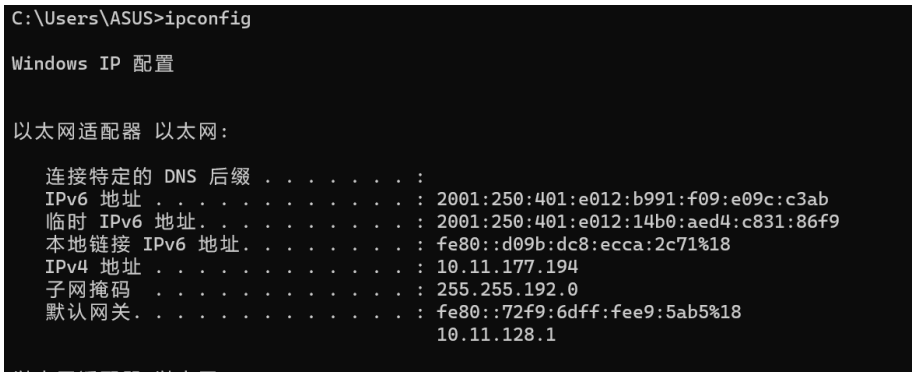

图 4: 查询网关和本地地址

ping 网关如图 5 所示。

```
C:\Users\ASUS>ping 10.11.128.1

正在 Ping 10.11.128.1 具有 32 字节的数据:
来自 10.11.128.1 的回复: 字节=32 时间=2ms TTL=255
来自 10.11.128.1 的回复: 字节=32 时间=2ms TTL=255
来自 10.11.128.1 的回复: 字节=32 时间=2ms TTL=255
来自 10.11.128.1 的回复: 字节=32 时间=2ms TTL=255

10.11.128.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 2ms, 最长 = 2ms, 平均 = 2ms
```

图 5: ping 网关

在 Wireshark 中筛选出，筛选语句为：ip.src==10.11.177.194 and ip.dst==10.11.128.1。筛选结果如图 6 所示。

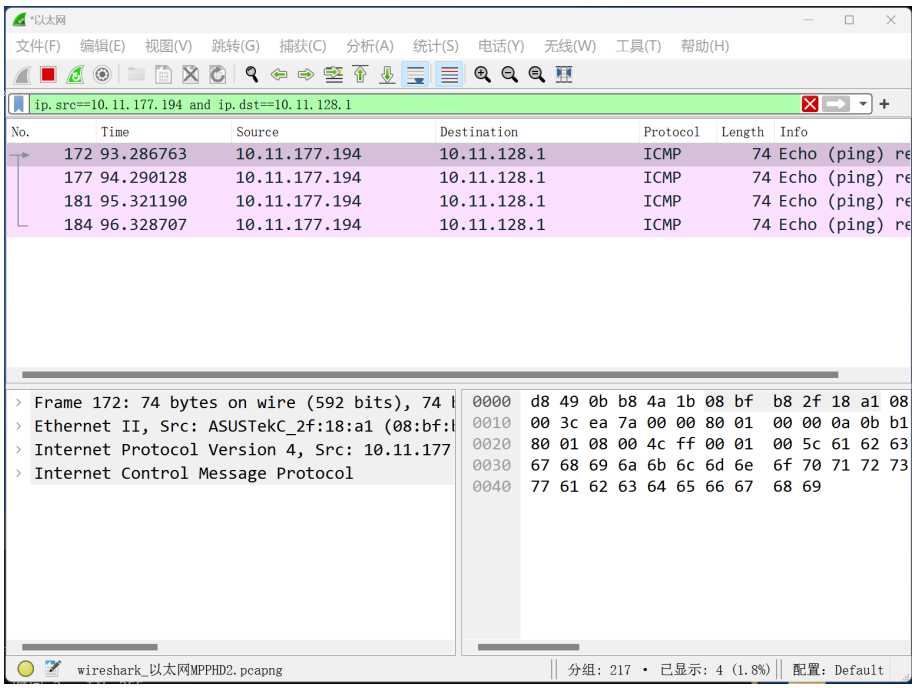

图 6: 筛选结果 1

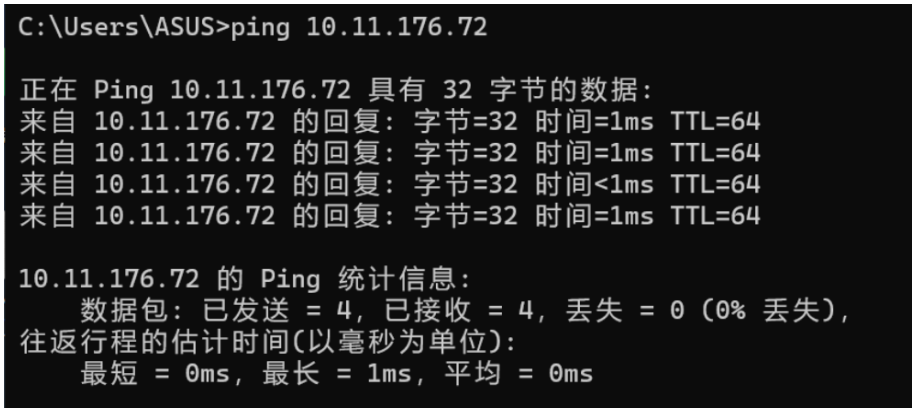

图 7: ping 同网段的一台主机

ping 同网段的一台主机如图 7 所示。在 Wireshark 中筛选出,筛选语句为:ip.src==10.11.177.194 and ip.dst==10.11.176.72。筛选结果如图 8 所示。

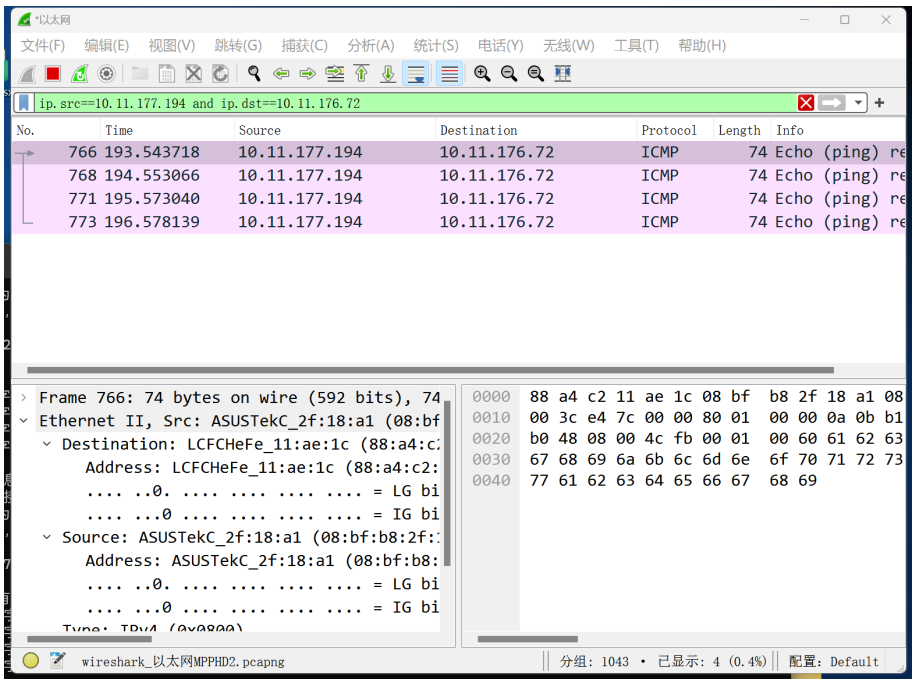

图 8: 筛选结果 2

辨识 MAC 地址类型，如图 9 所示。

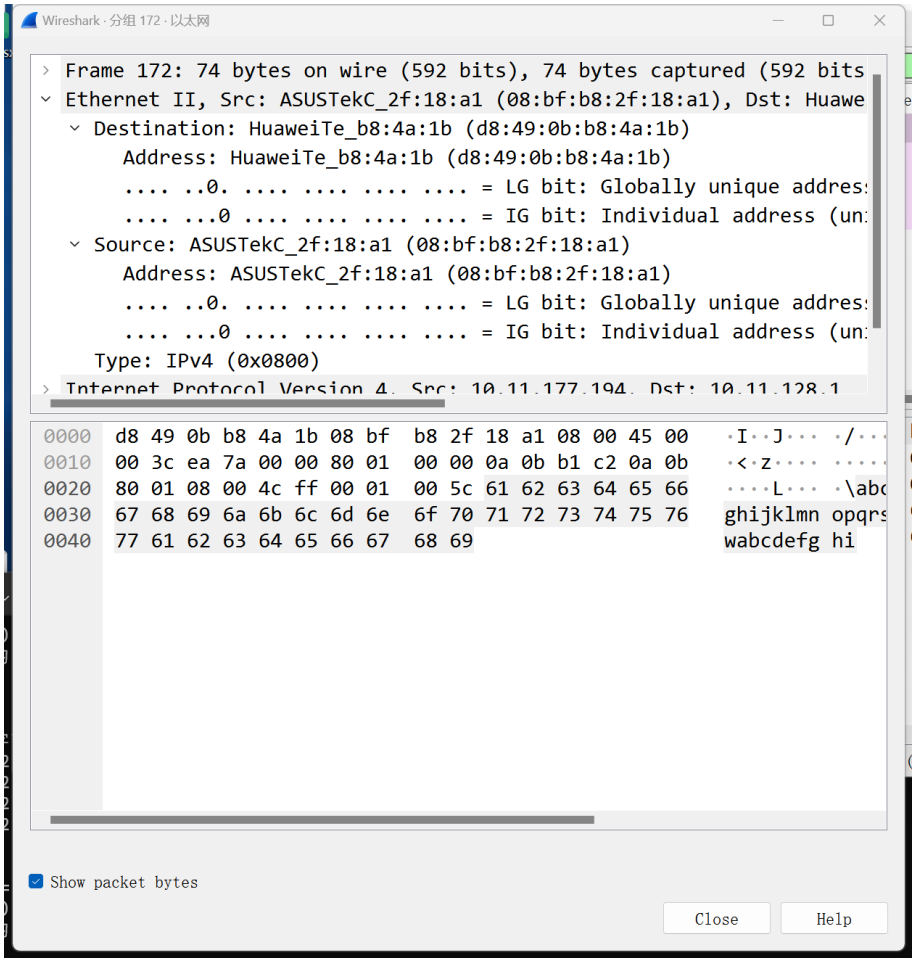

图 9: MAC 地址类型

本机 MAC 地址为：08:bf:b8:2f:18:a1，根据第一个字节 08，转换为二进制为 0001000，最低位为 0，因此 MAC 地址为单播 MAC 地址。

网关 MAC 地址为：d8:49:0b:b8:4a:1b，根据第一个字节 d8，转换为二进制为 11011000，最低位为 0，因此 MAC 地址为单播 MAC 地址。

3.2.2. 解读 OUI 信息

前 3 字节表示 OUI，是 IEEE 的注册管理机构给不同厂家分配的代码，区分不同的厂家。

本机 MAC 地址前三个字节为：08:bf:b8，网关 MAC 地址为前三个字节为：d8：49：0b。

3.2.3. 解读 I/G 和 G/L 位

I/G 位，如果是 0，则是某台设备的 MAC 地址，即单播地址，如果为 1，则是多播地址。如果 G/L=0，则是全局管理地址，由 IEEE 分配；如果 G/L=1，则是本地管理地址，是网络管理员为了加强自己对网络管理而指定的地址。08:bf:b8:2f:18:a1(本机 MAC 地址）I/G 位与 G/L 位都是 0，d8：49：0b：b8：4a：1b(网关 MAC 地址）I/G 位与 G/L 位也都是 0。

3.3 分析以太网的帧结构

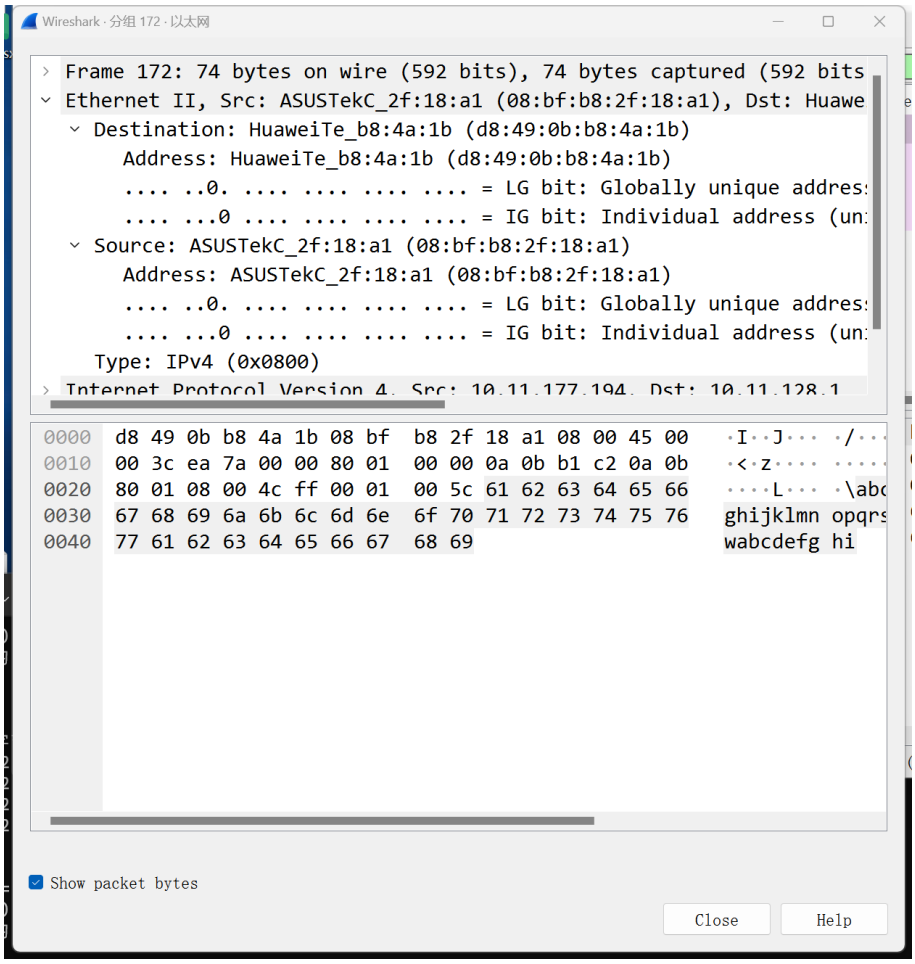

图 10: Enter Caption

Frame 是物理层的数据帧，分组长度是 42 字节。Ethernet II 是数据链路层以太网帧头部信息。点开的 Destination 是目标 MAC 地址，为 (d8：49：0b：b8：4a：1b),Source 是源 MAC 地址, 为 (08:bf:b8:2f:18:a1)。Type 是类型，为 IPv4。

3.4 分析 ARP 协议

先查看 ARP 表，再将要发送的地址删除，如图 11, 图 12 所示。

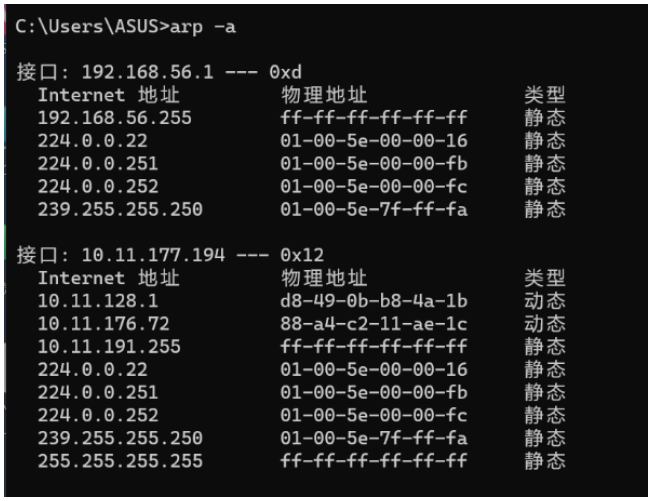

图 11: 查看 arp 缓存表

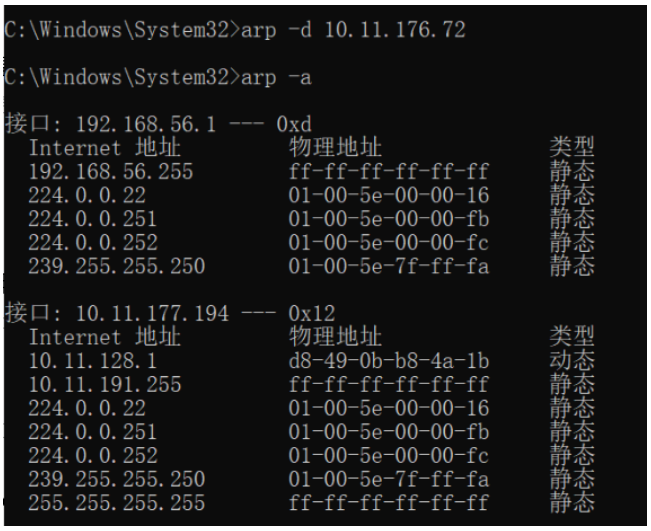

图 12: 删除 arp 表中地址

接着 ping 同网段另一台主机，在 Wireshark 中用 arp 筛选出数据包, 进行查询，截图如下：

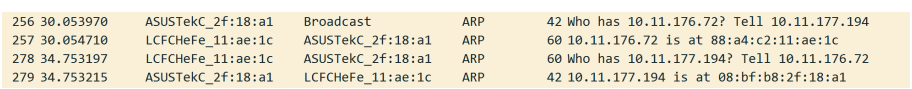

图 13: 筛选出 arp 数据包

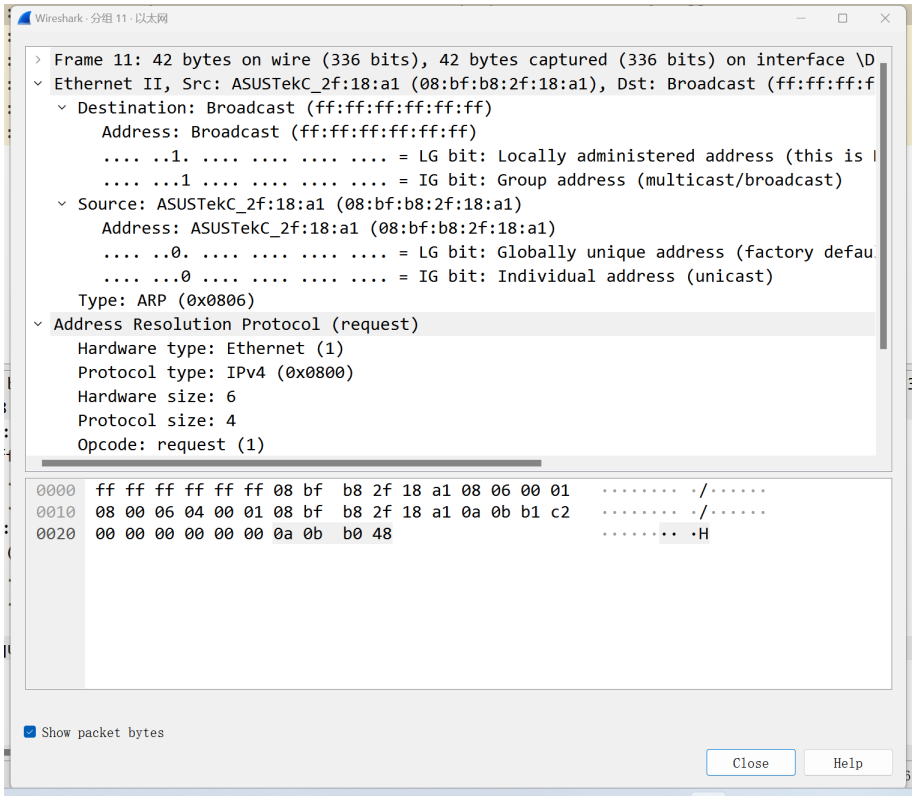

图 14: arp 数据包

对 arp 请求报文进行分析:

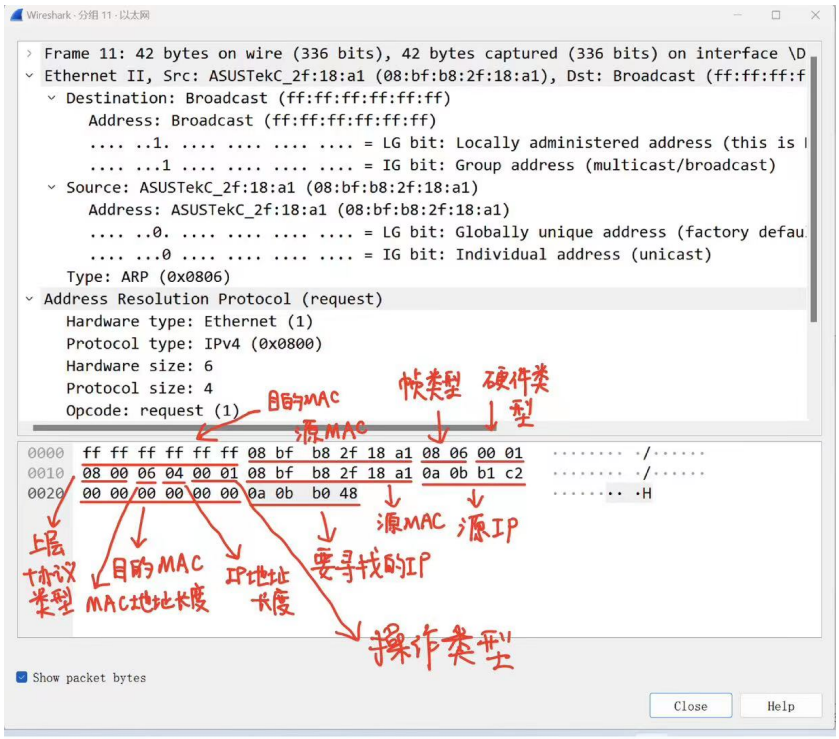

图 15: arp 分析

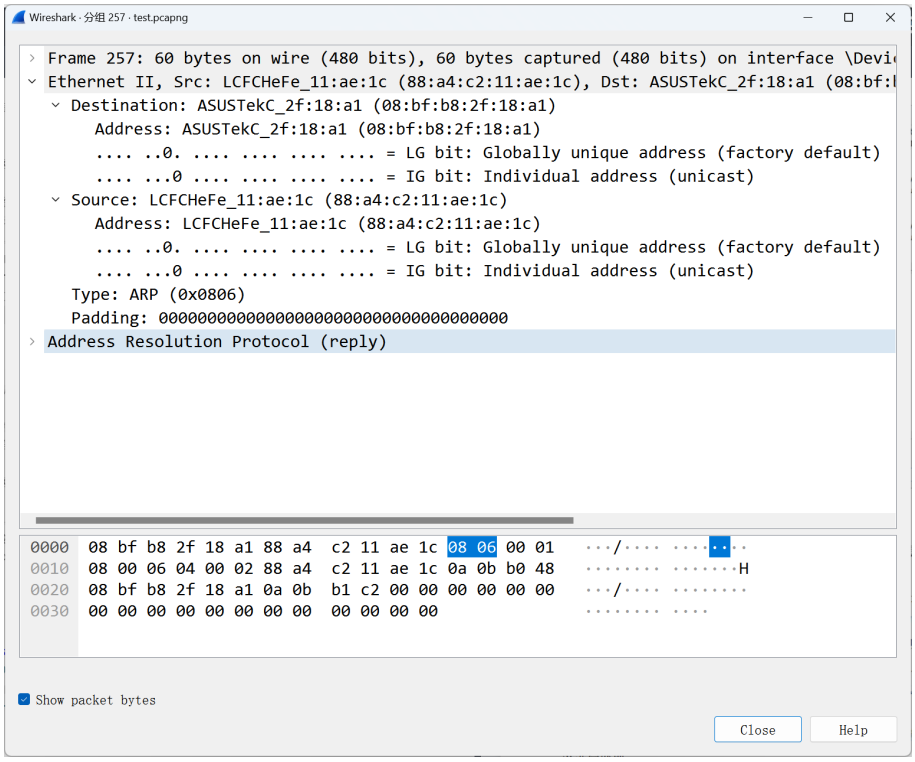

图 16: 响应包

收到的响应包：可以看出，Destination 即我的主机 ip 地址，Source 即我想发的另一台主机 ip 地址。于是分析：

假设主机 A 和主机 B 在同一网段，主机 A 要给主机 B 发送信息，ARP 工作过程如下：

1. 主机 A 先查看自己的 ARP 缓存表是否有主机 B 对应的 ARP 表项。如果有，则会直接利用 ARP 表中的 MAC 地址作为源 MAC 地址封装到数据帧中，再将数据包发送给主机 B。如果找不到对应的 MAC 地址，就缓存该数据报文，然后以广播方式发送一个 ARP 请求报文。请求的目标 IP 地址是主机 B 的 IP 地址，目标 MAC 地址是 MAC 地址的广播帧 (即 FF-FF-FF-FF-FF-FF)，可以看到图 14 中的目标 MAC 地址为 ff:ff:ff:ff:ff:ff。因为 ARP 请求报文以广播的方式发送，所以该网段上所有主机都可接收到该请求，但只有主机 B 会对该请求进行处理。

2. 主机 B 收到广播后，会将自己的 IP 地址和 ARP 请求报文中的目标 IP 地址进行对比，如果一样，则将 ARP 请求报文中的发送端（即主机 A）的 IP 地址和 MAC 地址存入自己的 ARP 表中。然后以单播方式发送 ARP 响应报文给主机 A，其中包含了自己的 MAC 地址。

3. 主机 A 收到 ARP 响应报文后，将主机 B 的 MAC 地址加入到自己的 ARP 表中以用于后续报文的转发，同时将 IP 数据包进行封装后发送出去。

当主机 A 和主机 B 不在同一网段时的 ARP 工作流程如下：

1.A 封装好要发送的信息后，会先用子网掩码计算自己和 B 是否在一个网段，如果不是，他就会通过网关把数据传递给 B。主机 A 就会先向网关发出 ARP 请求，ARP 请求报文中的目标 IP 地址为网关的 IP 地址。当主机 A 从收到的响应报文中获得网关的 MAC 地址后，将报文封装并发给网关。(如果 A 不知道网关地址，就像之前发个 ARP 广播来获取网关 MAC 地址，如下图)。

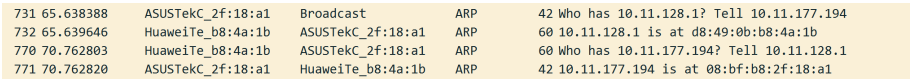

图 17: 寻找网关的广播

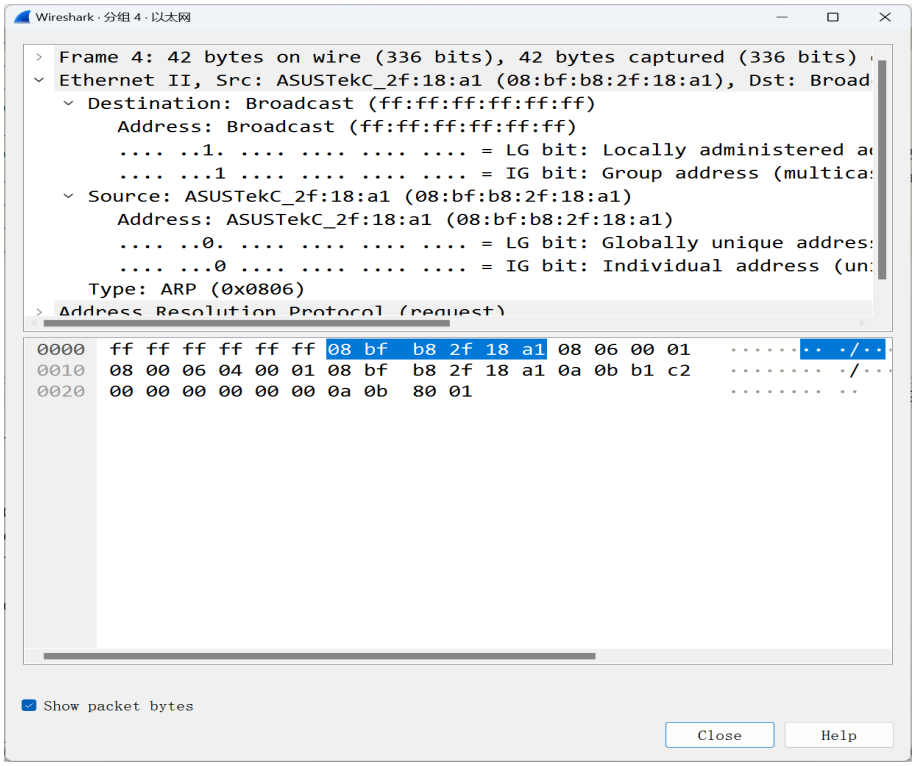

图 18: 寻找网关的广播

2. 网关收到后，发现包的目的地址是自己，然后便拆包发现要发送给 B，此时如果网关有 B 的的 ARP 表项，网关直接把报文发给主机 B。如果网关没有主机 B 的 ARP 表项，网关会广播 ARP 请求，目标 IP 地址为主机 B 的 IP 地址，当网关从收到的响应报文中获得主机 B 的 MAC 地址后，就可以将报文发给主机 B。

4 实验结论及心得体会

本次实验熟悉了 Wireshark 的基础使用，并利用 Wireshark 捕获了数据包，对数据包进行分析，此外进行了 ARP 协议的分析，并了解了 ARP 协议的工作原理以及方式，对 ARP 协议有了更深的认识。