### 【实验内容】

**1.ARP协议分析**

（1）查看本机IP地址与MAC地址

在命令行中输入命令：ipconfig 后显示的结果如图2-5所示：

当前本机IP 172.20.10.2

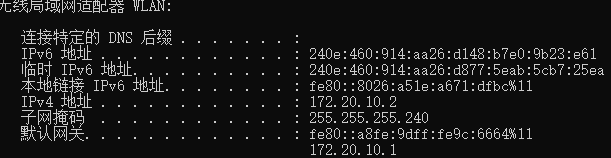


图2-5

（2）操作本机高速缓存中的ARP表

a．查看高速缓存中的ARP表

查看命令：arp -a

运行arp –a命令，查看运行结果如图2-6所示：

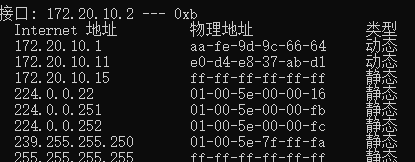
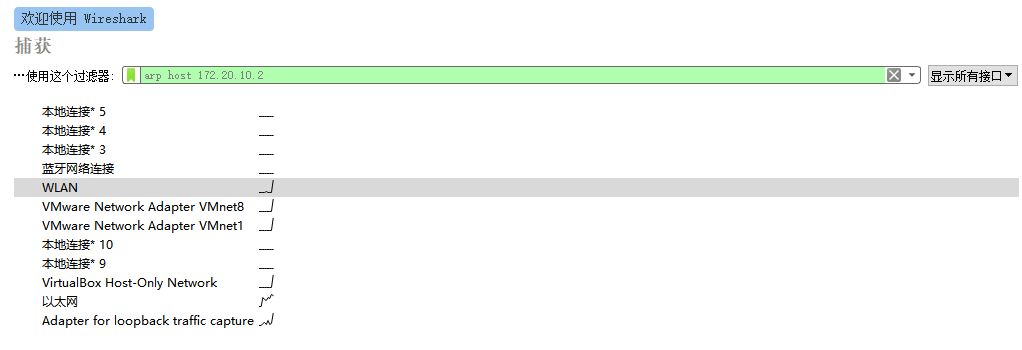


图2-6

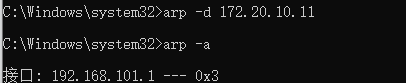
因为ARP表项在没有进行手工配置前，通常都是动态ARP表项，所以不同时间运行arp –a命 令，运行结果也不大相同。

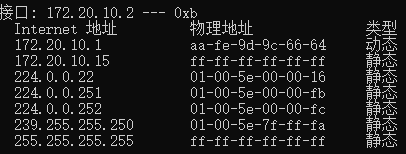
（3）运行WireShark软件，选择capture---options(捕获—选项)，在capture filter（捕获过滤器）文本框中输入**过滤条件arp host 172.20.10.2**，使得只监听进出本机（如IP为172.20.10.2）的arp数据包。点击start开始监听。



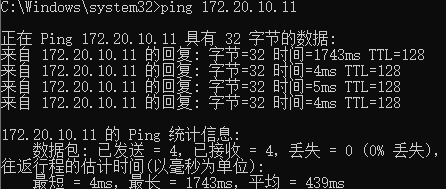
用ping命令去ping局域网中的其它主机B（10.211.55.10），且主机B的IP地址不在本机的ARP高速缓存中（如果想ping的机器的IP地址在缓存内，也可现将该条记录删除在进行实验。删除ARP静态表项的命令：arp  –d  IP地址  例如：arp –d 172.16.120.172；或清空表项：arp –d \*）。

arp –d 后，arp缓存如下





ping 172.20.10.11



WireShark中开始监听到数据包，当没有数据包到来后，停止监听并保存监听记录（黏贴监听记录截图）示例监听结果如图2-7所示：

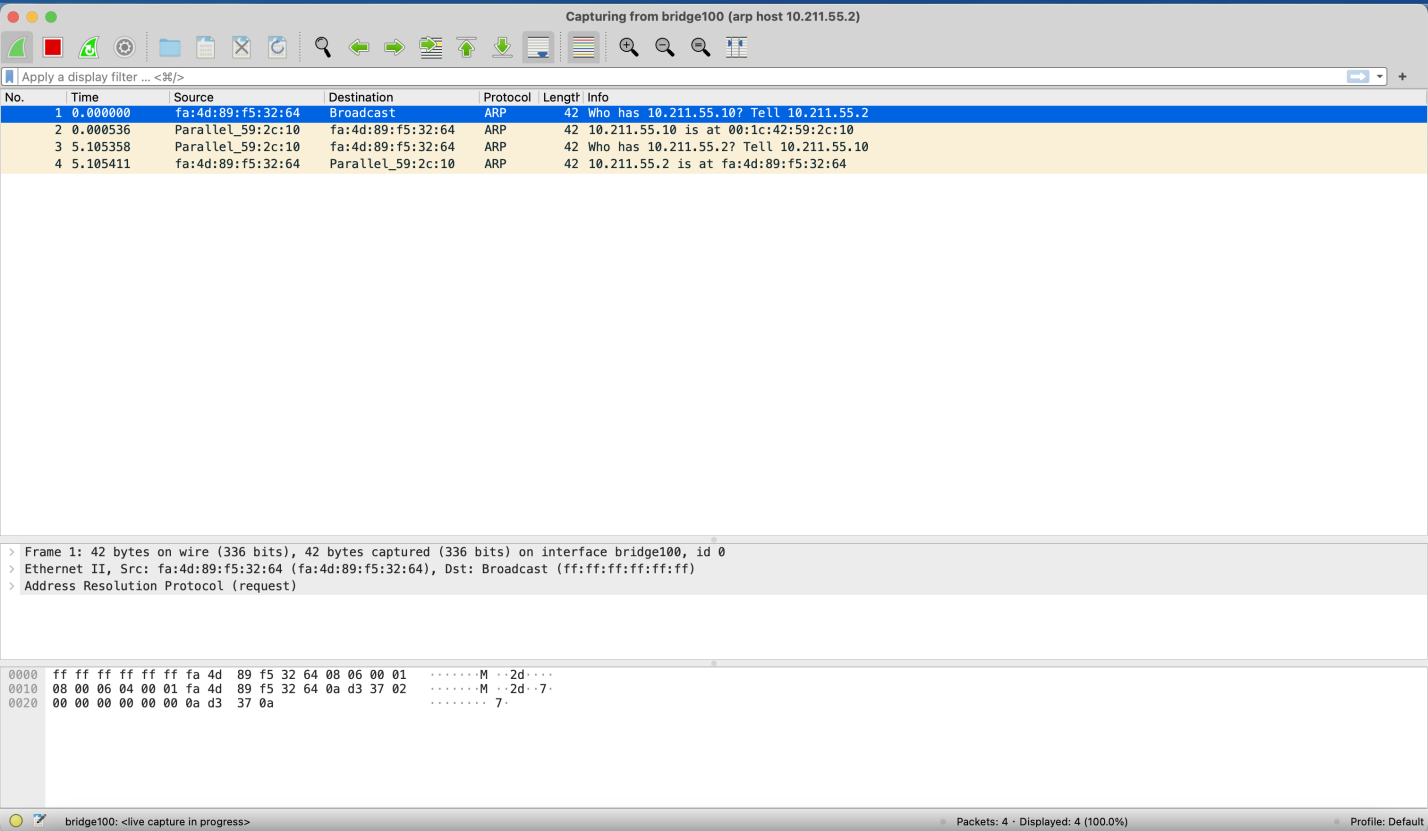
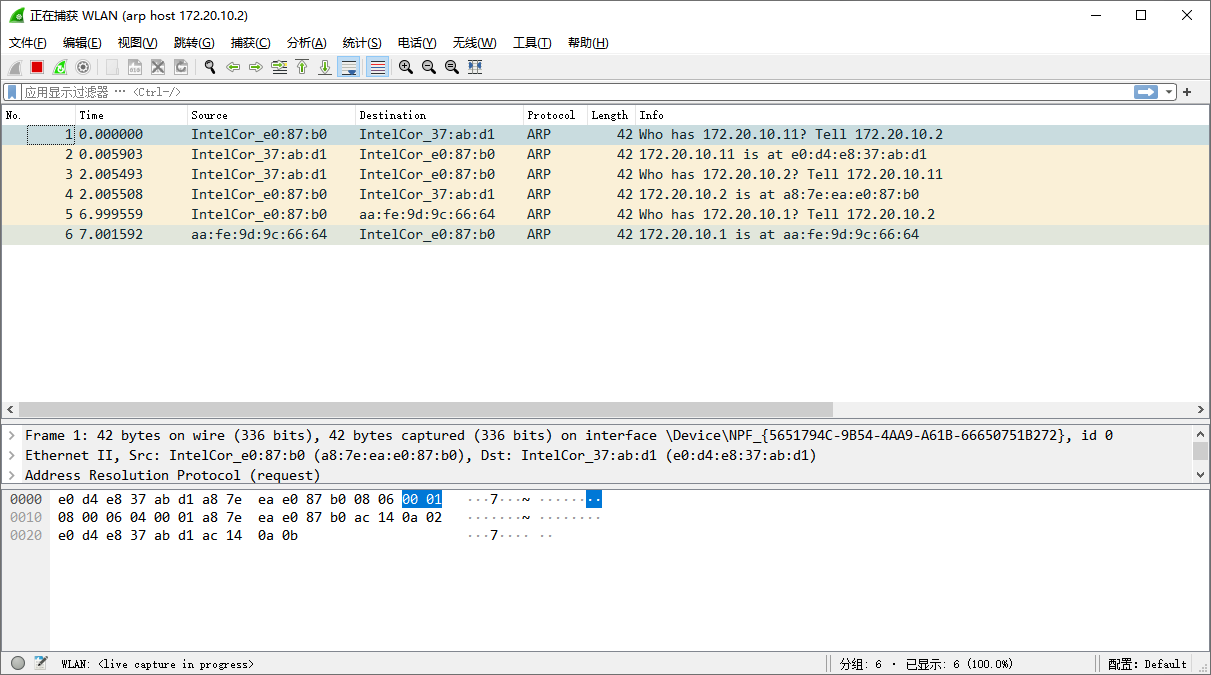


图2-7

（4）对监听到的数据进行分析：结合arp协议工作原理对监听记录进行分析；

**1）选择红圈中的第一条监听记录，即NO.1记录，分析ARP请求报文格式。**

**第一行 帧基本信息分析 （粘贴你的Frame信息）**

Frame Number（ 帧的编号）：\_\_\_\_\_1\_\_\_\_（捕获时的编号）

Frame Length(帧的大小)：\_\_\_\_42\_\_\_\_字节。

Arrival Time(帧被捕获的日期和时间): \_\_\_\_\_\_\_ Dec 7, 2022 21:45:53.972591000 \_\_\_\_\_\_\_\_

Time delta from previous captured frame(帧距离前一个帧的捕获时间差):\_ 0.000000000 seconds\_\_\_\_\_

Time since refernce or first frame(帧距离第一个帧的捕获时间差)：\_\_\_\_\_ 0.000000000 seconds \_\_\_\_\_\_\_\_\_\_

Protocols in frame(帧装载的协议)：\_\_\_\_\_\_eth:ethertype:arp \_\_\_\_\_\_

**第二行 数据链路层： （粘贴你的数据链路层信息）**

Destination（目的地址）： \_\_\_ e0:d4:e8:37:ab:d1\_\_\_\_\_\_

Source （ 源 地 址 ）：\_\_\_a8:7e:ea:e0:87:b0\_\_\_\_\_\_

**第三层 ARP协议： （粘贴你的ARP请求报文）**

Ｈardware type（硬件类型）：\_\_\_\_\_Ethernet (1) \_\_\_\_\_\_\_

Ｐrotocol type（协议类型）：\_\_\_\_\_\_IPv4(0x0800) \_\_\_\_\_\_

Ｈardware size(硬件信息在帧中占的字节数)：\_\_\_\_6\_\_\_\_\_

Ｐrotocol size(协议信息在帧中占的字节数)：\_\_\_\_\_4\_\_\_\_\_

操作码（opcode）：\_\_\_request (1) \_\_\_\_\_

发送方的ＭＡＣ地址（Sender MAC address）：\_\_\_\_\_a8:7e:ea:e0:87:b0\_\_\_\_\_\_\_\_

发送方的IP地址（Sender IP address）：\_\_\_\_\_\_\_\_172.20.10.2\_\_\_\_\_\_\_\_\_\_\_

目标的ＭＡＣ地址（Target MAC address:）：\_\_\_\_\_\_\_e0:d4:e8:37:ab:d1\_\_\_\_\_\_\_\_\_\_\_

目标的IP地址（Target IP address:）：\_\_\_\_\_\_\_\_172.20.10.11\_\_\_\_\_\_\_\_\_\_

**2）分析ARP应答报文，即NO.10记录（同上）**

**第一行 帧基本信息分析 （粘贴你的Frame信息）**

Frame Number（ 帧的编号）：\_\_\_\_\_2\_\_\_\_（捕获时的编号）

Frame Length(帧的大小)：\_\_\_\_42\_\_\_\_字节。

Arrival Time(帧被捕获的日期和时间): \_\_\_\_\_\_\_ Dec 7, 2022 21:45:53.978494000\_\_\_\_\_\_\_\_

Time delta from previous captured frame(帧距离前一个帧的捕获时间差):\_ 0.005903000 seconds\_\_\_\_\_

Time since refernce or first frame(帧距离第一个帧的捕获时间差)：\_\_\_\_\_ 0.005903000 seconds \_\_\_\_\_\_\_\_\_\_

Protocols in frame(帧装载的协议)：\_\_\_\_\_\_eth:ethertype:arp \_\_\_\_\_\_

**第二行 数据链路层： （粘贴你的数据链路层信息）**

Destination（目的地址）： \_\_\_a8:7e:ea:e0:87:b0\_\_\_\_\_\_

Source （ 源 地 址 ）：\_\_\_ e0:d4:e8:37:ab:d1\_\_\_\_\_\_

**第三层 ARP协议： （粘贴你的ARP请求报文）**

Ｈardware type（硬件类型）：\_\_\_\_\_Ethernet (1) \_\_\_\_\_\_\_

Ｐrotocol type（协议类型）：\_\_\_\_\_\_IPv4(0x0800) \_\_\_\_\_\_

Ｈardware size(硬件信息在帧中占的字节数)：\_\_\_\_6\_\_\_\_\_

Ｐrotocol size(协议信息在帧中占的字节数)：\_\_\_\_\_4\_\_\_\_\_

操作码（opcode）：\_\_\_ reply (2)\_\_\_\_\_

发送方的ＭＡＣ地址（Sender MAC address）：\_\_\_\_\_e0:d4:e8:37:ab:d1\_\_\_\_\_\_\_\_

发送方的IP地址（Sender IP address）：\_\_\_\_\_\_\_\_172.20.10.11\_\_\_\_\_\_\_\_\_\_\_

目标的ＭＡＣ地址（Target MAC address:）：\_\_\_\_\_\_\_ a8:7e:ea:e0:87:b0\_\_\_\_\_\_\_\_\_\_\_

目标的IP地址（Target IP address:）：\_\_\_\_\_\_\_\_172.20.10.2\_\_\_\_\_\_\_\_\_\_

再次用命令arp -a查看ARP表项的变化情况，可以发现多了B 172.20.10.11的表项。如图2-8所示：

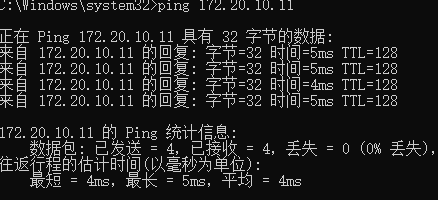


图2-8

**2.ICMP协议分析**

（1）此时，在WireShark中设置capture filter使得只监听进出本机（如IP为172.16.120.221）的ICMP数据包。在capture filter（捕获过滤器）文本框中输入过滤条件icmp，点击start按钮进行监听。

用ping命令再去ping主机B，保存监听记录为2-2.pcap-ng。（黏贴监听记录截图）结果如图2-9所示：



1. 回答：截获的ICMP 报文有几种类型？分别是？

两种类型，分别是请求报文和应答报文

1. 分析截获的 ICMP 报文，填入表中。只需要填写ping主机B产生的ICMP报文信息。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 报文号 | 源IP | 目的IP | 报文格式 | | | |
| 类型 | 代码 | 标识 | 序列号 |
| 1 | 172.20.10.2 | 172.20.10.11 | ICMP | 0 | 0 | 0 |
| 2 | 172.20.10.11 | 172.20.10.2 | ICMP | 0 | 0 | 0 |
| 3 | 172.20.10.2 | 172.20.10.11 | ICMP | 0 | 0 | 0 |
| 4 | 172.20.10.11 | 172.20.10.2 | ICMP | 0 | 0 | 0 |
| 5 | 172.20.10.2 | 172.20.10.11 | ICMP | 0 | 0 | 0 |
| 6 | 172.20.10.11 | 172.20.10.2 | ICMP | 0 | 0 | 0 |
| 7 | 172.20.10.2 | 172.20.10.11 | ICMP | 0 | 0 | 0 |
| 8 | 172.20.10.11 | 172.20.10.2 | ICMP | 0 | 0 | 0 |

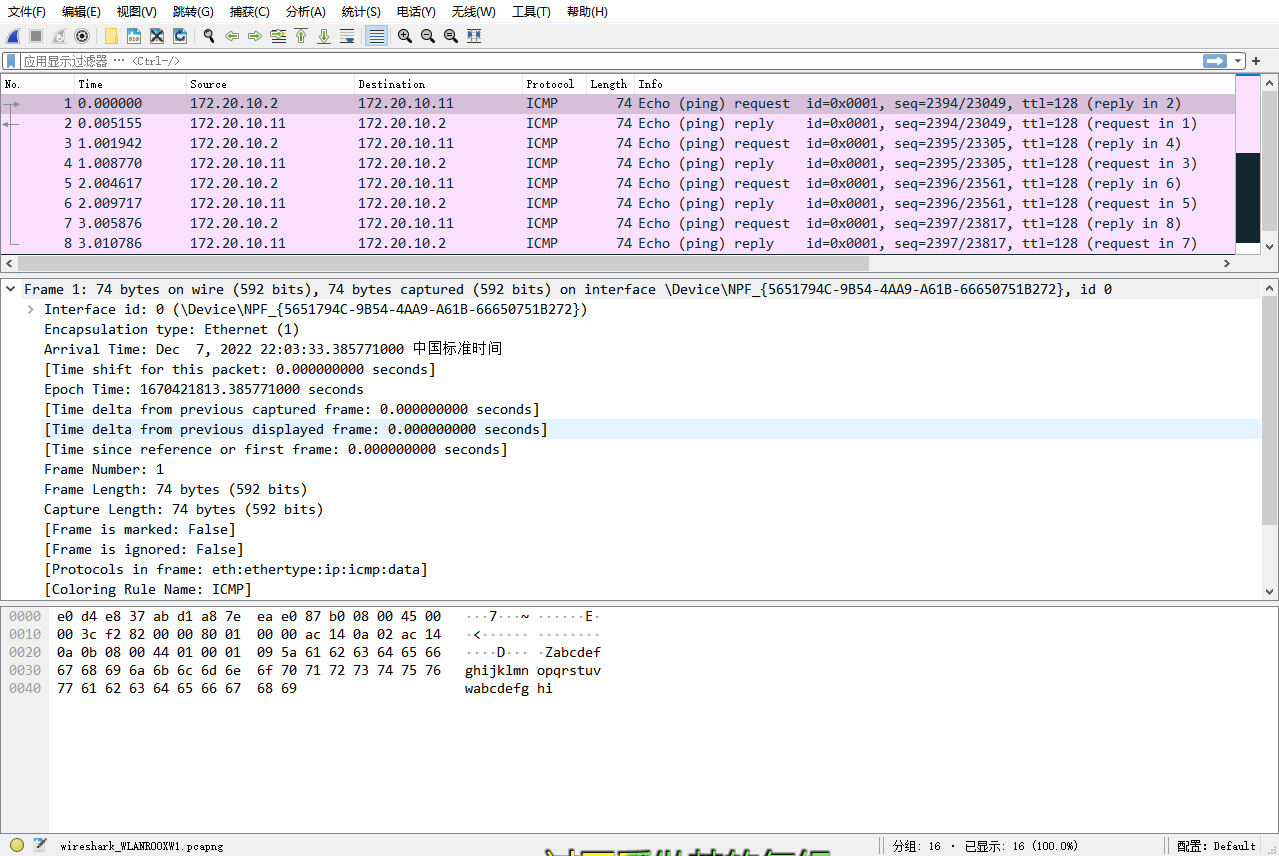


图2-9

### 【实验报告要求】

1、使用wireshark抓包工具完成实验步骤两大项内容ARP协议分析及ICMP协议分析，对于实验内容部分提出的问题要回答，表格要完善。

2、实验报告内容应体现具体的操作流程，除相关的文字说明外，应有一定的截图说明（ping命令、ARP命令及抓包的过程必须要有截图）。