华东师范大学软件工程学院实验报告

实验课程:	计算机网络	年　　级:	2022 级
实验编号:	Lab 04	实验名称:	ARP
姓　　名:	李鹏达	学　　号:	10225101460

1 实验目的

1) 通过 Wireshark 获取 ARP 消息
2) 掌握 ARP 数据包结构
3) 掌握 ARP 数据包各字段的含义
4) 了解 ARP 协议适用领域

2 实验内容与实验步骤

2.1 实验内容

2.1.1 捕获数据

启动 `Wireshark`，在菜单栏的捕获 → 选项中进行设置，选择已连接的以太网，设置捕获过滤器为 `arp`，捕获 `arp` 数据包。

然后在命令行中使用 `ipconfig -all` 命令获取本机的 `IP` 地址和 `MAC` 地址。

在 `Wireshark` 的过滤器中输入 `eth.addr==<yourMAC>`（其中 `<yourMAC>` 为本机的 `MAC` 地址）。

在管理员模式下，使用 `arp -d` 命令清除本机的 `ARP` 缓存。

打开 `Wireshark`，停止捕获。

2.1.2 回答问题

1. 画出你的计算机和本地路由间 ARP 的请求和应答数据包，标记出请求和应答，为每个数据包给出发送者和接受者的 MAC 和 IP 地址。
2. 什么样的操作码是用来表示一个请求？应答呢?
3. 一个请求的 ARP 的报头有多大？应答呢?
4. 对未知目标的 MAC 地址的请求是什么值?
5. 什么以太网类型值说明 ARP 是更高一层的协议?
6. ARP 应答是广播吗?

2.1.3 问题讨论

We encourage you to explore ARP on your own once you have completed this lab. One suggestion is to look at other ARP packets that may have been recorded in your trace; we only examined an ARP request by your computer and the ARP reply from the default gateway.

To see if there is other ARP activity, make sure to clear any Ethernet address filter that is set. Other ARP packets may exhibit any of the following kinds of behavior for you to explore:

1. ARP requests broadcast by other computers. The other computers on the local network are also using ARP. Since requests are broadcast, your computer will receive their requests.
2. ARP replies sent by your computer. If another computer happens to ARP for the IP address of your computer, then your computer will send an ARP reply to tell it the answer.
3. Gratuitous ARPs in which your computer sends a request or reply about itself. This is helpful when a computer or link comes up to make sure that no-one else is using the same IP address. Gratuitous ARPs have the same sender and target IP address, and they have an Info field in Wireshark that identified them as gratuitous.
4. Other ARP requests sent by your computer and the corresponding ARP reply. Your computer may need to ARP for other hosts besides the default gateway after you flush its ARP cache.

2.2 实验步骤

1) 启动 Wireshark，在菜单栏的捕获 → 选项中进行设置，选择已连接的以太网，设置捕获过滤器为 arp，将混杂模式设为关闭，然后开始捕获。
2) 在命令行中使用 ipconfig -all 命令获取本机的 IP 地址和 MAC 地址。

```
1 PS> ipconfig -all
```

3) 回到 Wireshark，设置捕获过滤器为 eth.addr==<yourMAC>
4) 在管理员模式下，使用 arp -d 命令清除本机的 ARP 缓存。

```
1 PS> arp -d
```

5) 打开 Wireshark，停止捕获。
6) 分析捕获到的 ARP 数据包，并回答相关问题。
7) 对捕获到的 ARP 数据包进行数据分析，并回答相关问题。
8) 问题讨论

3 实验环境

- 操作系统：Windows 11 家庭中文版 23H2 22631.2715
- 网络适配器：Killer(R) Wi-Fi 6 AX1650i 160MHz Wireless Network Adapter(201NGW)
- Wireshark：Version 4.2.0 (v4.2.0-0-g54eedfc63953)

- wget: GNU Wget 1.21.4 built on mingw32

4 实验结果与分析

4.1 捕获数据

首先，打开 Wireshark，在菜单栏的捕获 → 选项中进行设置，选择已连接的以太网，设置捕获过滤器为 arp，将混杂模式设为关闭，然后开始捕获。

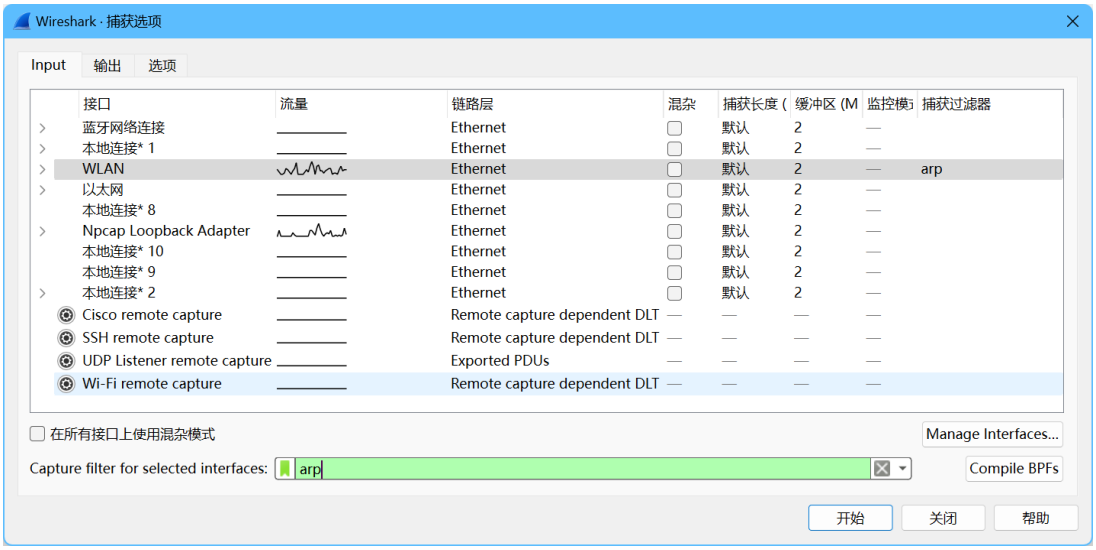

图 1: 设置捕获选项

然后在命令行中使用 ipconfig -all 命令获取本机的 IP 地址和 MAC 地址。

```
无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Killer(R) Wi-Fi 6 AX1650i 160MHz Wireless Network Adapter (201NGW)
   物理地址. . . . . . . . . . . . . : 10-3D-1C-CC-0F-D3
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::d281:e59b:e8b4:5fe4%12(首选)
   IPv4 地址 . . . . . . . . . . . . : 192.168.1.107(首选)
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   获得租约的时间  . . . . . . . . . : 2023年12月22日 1:56:16
   租约过期的时间  . . . . . . . . . : 2023年12月22日 9:05:56
   默认网关. . . . . . . . . . . . . : 192.168.1.1
   DHCP 服务器 . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 135281948
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-2B-EB-EB-3E-08-8F-C3-1C-9A-4C
   DNS 服务器  . . . . . . . . . . . : 180.168.255.118
                                       116.228.111.18
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用
```

图 2: 获取本机 IP 地址和 MAC 地址

可以看到，本机的 IP 地址为 192.168.1.107，MAC 地址为 10-3D-1C-CC-0F-D3。

回到 Wireshark，设置捕获过滤器为 eth.addr==10-3D-1C-CC-0F-D3。

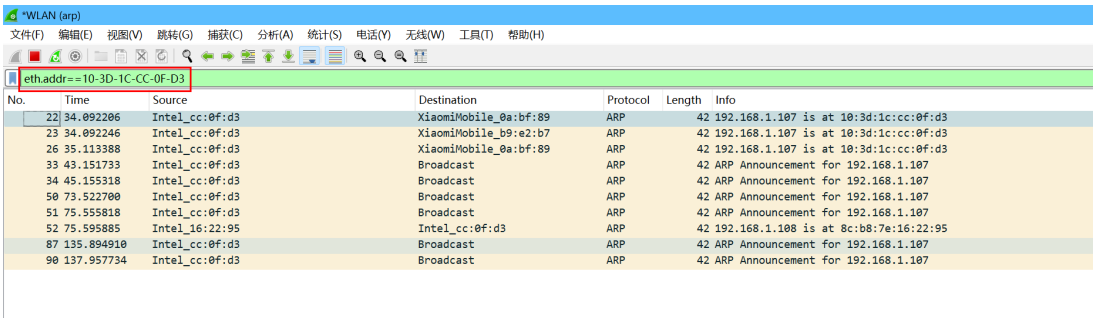

图 3: 设置捕获过滤器

接下来，在管理员模式下，在终端中使用 arp -d 命令清除本机的 ARP 缓存。

图 4: 清除本机 ARP 缓存

打开 Wireshark，停止捕获。捕获结果如下图所示：

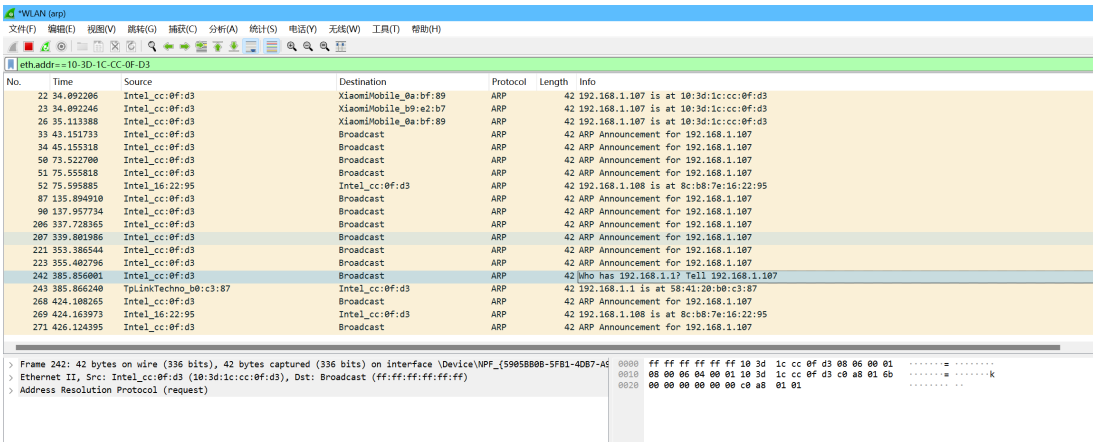

图 5: 捕获结果

4.2 回答问题

1. 画出你的计算机和本地路由间 ARP 的请求和应答数据包，标记出请求和应答，为每个数据包给出发送者和接受者的 MAC 和 IP 地址。
   选择 ARP 请求数据包，如下图所示：

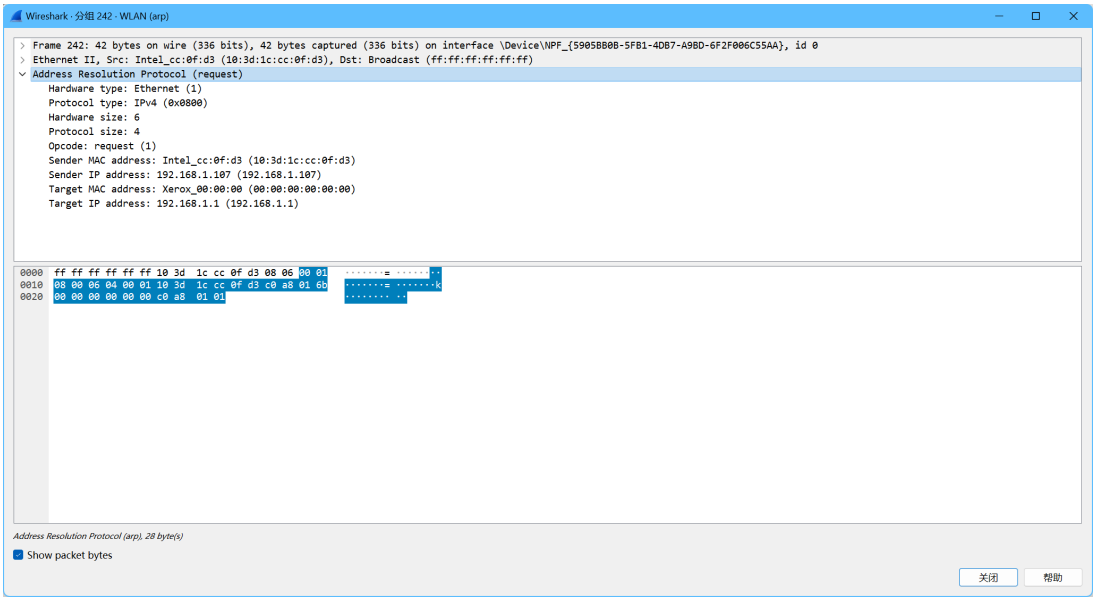

图 6: 选择 ARP 请求数据包

可以看到，它包括了一个长度为 28 字节的 ARP 报头，其中包括了以下字段：

- Hardware type: Ethernet (1)，长度为 2 字节
- Protocol type: `IPv4` (0x0800)，长度为 2 字节
- Hardware size: 6，长度为 1 字节
- Protocol size: 4，长度为 1 字节
- Opcode: request (1)，长度为 2 字节
- Sender MAC address: `10:3d:1c:cc:0f:d3`，长度为 6 字节
- Sender IP address: `192.168.1.107`，长度为 4 字节
- Target MAC address: `00:00:00:00:00:00`，长度为 6 字节
- Target IP address: `192.168.1.1`，长度为 4 字节

画出 ARP 请求数据包，如下图所示：

Hardware type	Protocol type	Hardware size	Protocol size	Opcode	
1	0x0800	6	4	1	
Sender MAC address					Sender IP address
10:3d:1c:cc:0f:d3					192.168.1.107
Target MAC address					Target IP address
00:00:00:00:00:00					192.168.1.1

表 1: ARP 请求数据包

选择一个 ARP 应答数据包，如下图所示：

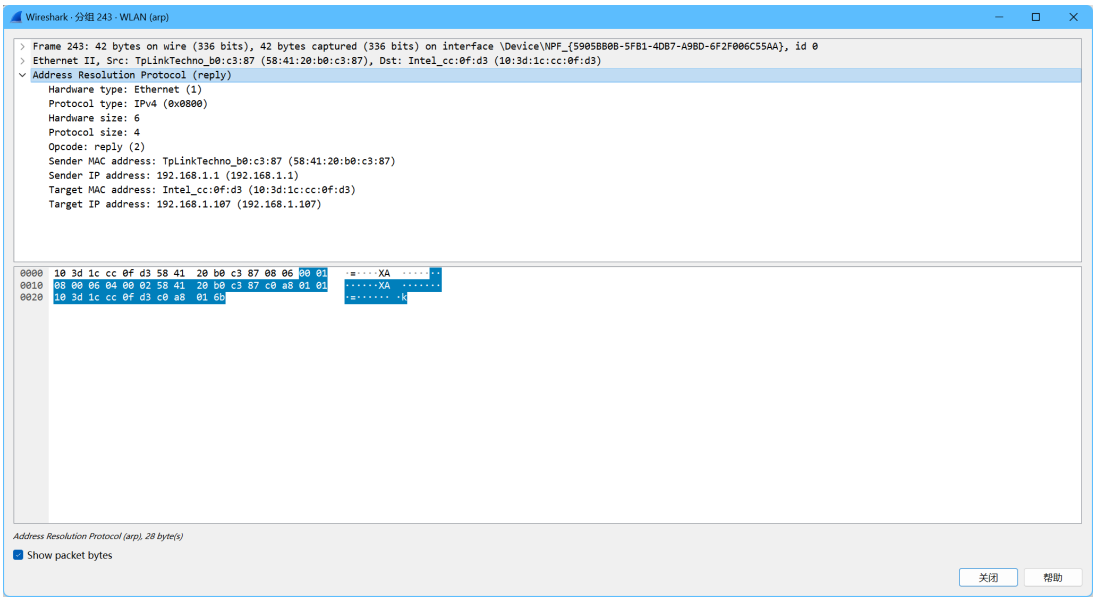

图 7: 选择 ARP 应答数据包

画出 ARP 应答数据包，如下图所示：

Hardware type	Protocol type	Hardware size	Protocol size	Opcode	
1	0x0800	6	4	2	
Sender MAC address				Sender IP address	
58:41:20:b0:c3:87				192.168.1.1	
Target MAC address				Target IP address	
10:3d:1c:cc:0f:d3				192.168.1.107	

表 2: ARP 应答数据包

2. 什么样的操作码是用来表示一个请求？应答呢？
   ARP 报头中的 Opcode 字段用来表示 ARP 请求或应答，其中 Opcode 为 1 表示请求，为 2 表示应答。
3. 一个请求的 ARP 的报头有多大？应答呢？
   长度均为 28 字节。
4. 对未知目标的 MAC 地址的请求是什么值？
   对未知目标的 MAC 地址的请求是 00:00:00:00:00:00。
5. 什么以太网类型值说明 ARP 是更高一层的协议？
   以太网类型值为 0x0806 说明 ARP 是更高一层的协议。

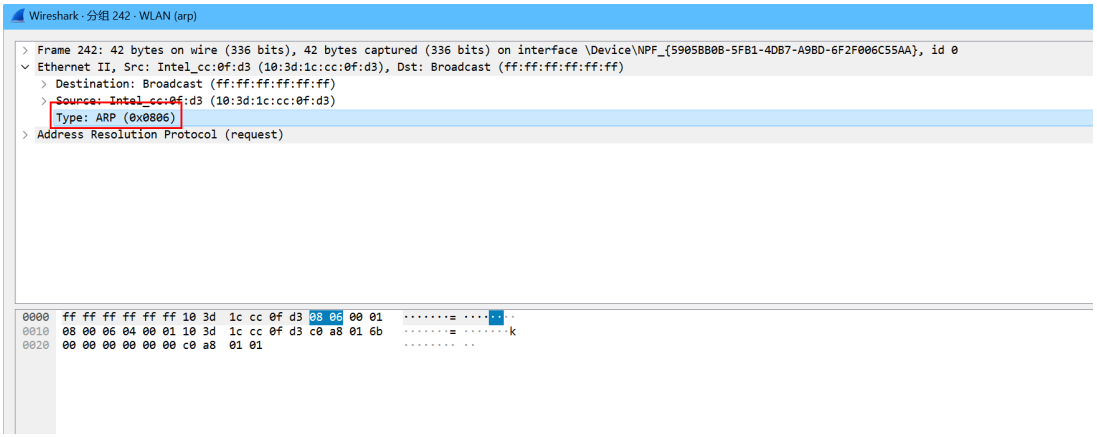

图 8: ARP 的类型值为 0x0806

6. ARP 应答是广播吗?
   在以太网层可以看出，ARP 应答是单播。

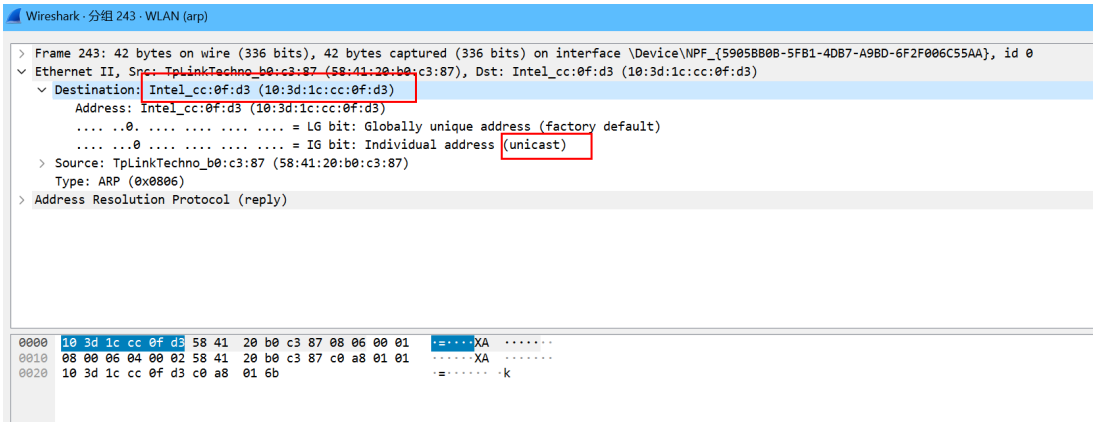

图 9: ARP 应答是单播

4.3 问题讨论

1. ARP requests broadcast by other computers. The other computers on the local network are also using ARP. Since requests are broadcast, your computer will receive their requests.
   清除筛选后，可以看到其他计算机发送的 ARP 请求。

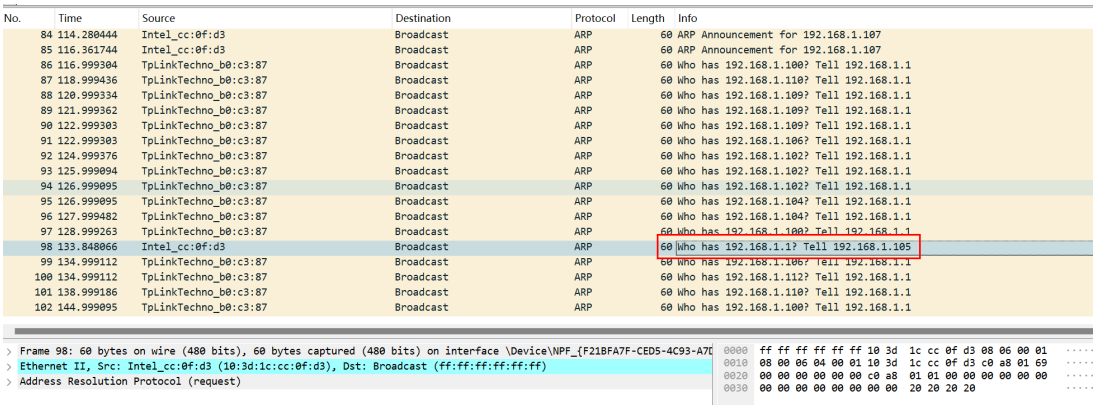

图 10: 其他计算机发送的 ARP 请求

2. ARP replies sent by your computer. If another computer happens to ARP for the IP address of your computer, then your computer will send an ARP reply to tell it the answer.
可以在另一台计算机上使用 `arp -d <Your IP>` 命令清除 ARP 缓存，然后使用 `ping <Your IP>` 命令向本机发送 ICMP 请求，这时也会发起一个 ARP 请求，此时本机会发送 ARP 应答，如下图所示（由于从 WIFI 换到了以太网，IP 地址发生了变化）：

图 11: 本机发送了 ARP 应答

3. Gratuitous ARPs in which your computer sends a request or reply about itself. This is helpful when a computer or link comes up to make sure that no-one else is using the same IP address. Gratuitous ARPs have the same sender and target IP address, and they have an Info field in Wireshark that identified them as gratuitous.
可以在捕获列表中看到 `gratuitous ARP` 数据包。

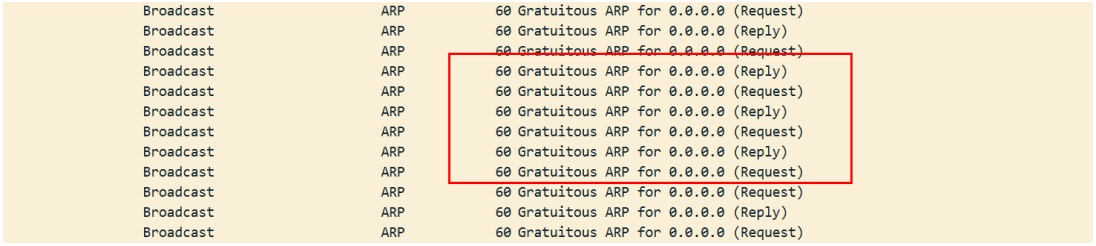

图 12: 捕获到的 `gratuitous ARP` 数据包

4. Other ARP requests sent by your computer and the corresponding ARP reply. Your computer may need to ARP for other hosts besides the default gateway after you flush its ARP cache.
   清除 ARP 缓存后，观察到了相关请求。

786	1089.057544	CompalInform_1c:9a:4c	Broadcast	ARP	42 Who has 192.168.1.1? Tell 192.168.1.111
787	1089.058572	TpLinkTechno_b0:c3:87	CompalInform_1c:9a:4c	ARP	60 192.168.1.1 is at 58:41:20:b0:c3:87
788	1089.993920	TpLinkTechno_b0:c3:87	Broadcast	ARP	60 Who has 192.168.1.106? Tell 192.168.1.1
789	1090.993827	TpLinkTechno_b0:c3:87	Broadcast	ARP	60 Who has 192.168.1.113? Tell 192.168.1.1
790	1090.993828	TpLinkTechno_b0:c3:87	Broadcast	ARP	60 Who has 192.168.1.110? Tell 192.168.1.1
791	1092.993912	TpLinkTechno_b0:c3:87	Broadcast	ARP	60 Who has 192.168.1.100? Tell 192.168.1.1

图 13: 相关请求

5 实验结果总结

本次实验通过 Wireshark 捕获了 ARP 数据包，并对其进行了分析，了解了 ARP 数据包的结构和各字段的含义，进一步增强了对 ARP 协议的理解。

6 附录

无