

# 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:	2023 级
实验编号:	Lab 04	实验名称:	ARP
姓 名:	王海生	学 号:	10235101559

## 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. 通过语句“`eth.addr==01:02:03:04:05:06`”的形式，在 wireshark 中设置过滤器，找出与自己 mac 地址相关的 arp 报文。Arp 报文包括请求报文和应答报文，仔细分析两种报文的格式。
2. 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。
3. (a) 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。  
(b) 什么样的操作码是用来表示一个请求？应答呢？  
(c) 一个请求的 ARP 的报头有多大？应答呢？

- (d) 对未知目标的 MAC 地址的请求是什么值?
- (e) 什么以太网类型值说明 ARP 是更高一层的协议?
- (f) ARP 应答是广播吗?

### 2.1.3 自主探索 ARP 报文

去除过滤器，我们发现还有更多的 arp 报文。请研究这些额外的 arp 报文中，有什么其他的功能作用。在查阅公开资料后，我将研究下列问题：

1. 其他计算机广播的 ARP 请求。本地网络上的其他计算机也在使用 ARP。由于请求是以广播形式发送的，因此您的计算机将会接收到这些请求。
2. 您的计算机发出的 ARP 回复。如果另一台计算机恰好对您的计算机的 IP 地址进行 ARP 查询，那么您的计算机将发送一个 ARP 回复以告知查询结果。
3. 自发 ARP (Gratuitous ARPs)，其中您的计算机发送有关自身的请求或回复。当计算机或链接上线时，这有助于确保没有其他人正在使用相同的 IP 地址。自发 ARP 具有相同的发送方和目标 IP 地址，并且在 Wireshark 中它们的信息字段会标识其为自发 ARP。
4. 您的计算机发出的其他 ARP 请求及相应的 ARP 回复。在您清空其 ARP 缓存后，您的计算机可能需要对其他主机（不仅仅是默认网关）进行 ARP 查询。

## 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。

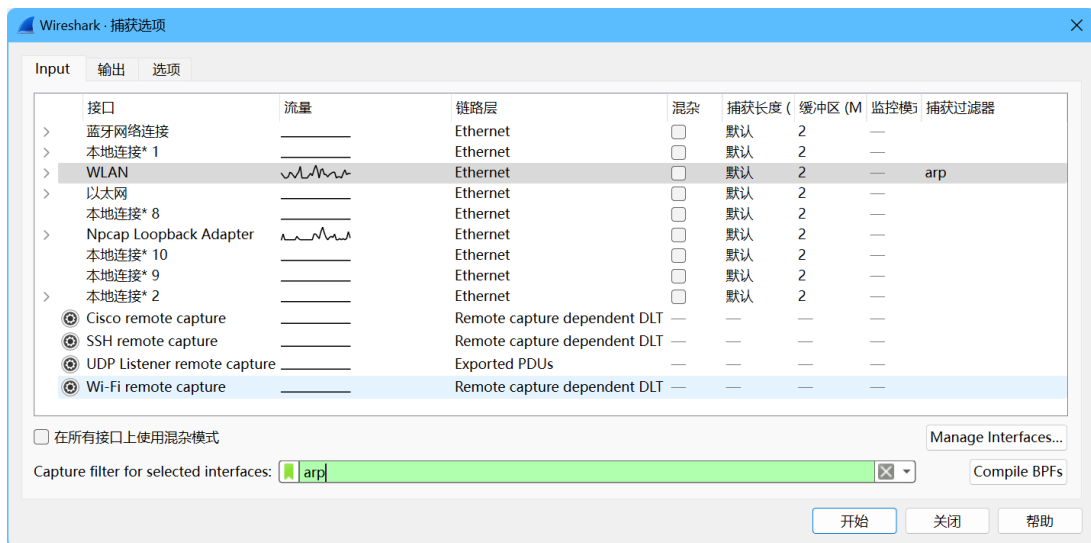


图 1: 设置捕获选项

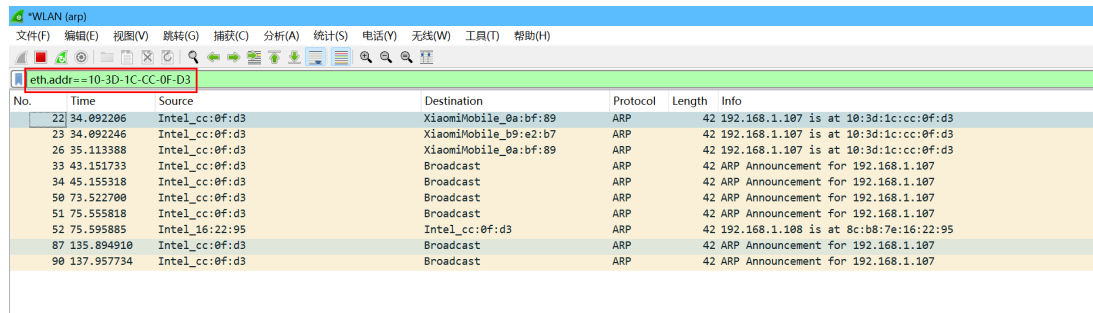
然后在命令行中使用 `ipconfig -all` 命令获取本机的 IP 地址和 MAC 地址。

```
1  无线局域网适配器 WLAN:
2
3  连接特定的 DNS 后缀 . . . . . :
4  描述 . . . . . : Killer (R) Wi-Fi 6 AX1650i 160MHz
   Wireless Network Adapter (201NGW)
5  物理地址 . . . . . : 10-3D-1C-CC-0F-D3
6  DHCP 已启用 . . . . . : 是
7  自动配置已启用 . . . . . : 是
8  本地链接 IPv6 地址 . . . . . : fe80::d281:e59b:e8b4:5fe4%12 (首选)
9  IPv4 地址 . . . . . : 192.168.1.107 (首选)
10 子网掩码 . . . . . : 255.255.255.0
11 获得租约的时间 . . . . . : 2024年12月8日 8:24:21
12 租约过期的时间 . . . . . : 2024年12月8日 12:24:21
13 默认网关 . . . . . : 192.168.1.1
```

```

14    DHCP 服务器 . . . . . : 192.168.1.1
15    DHCPv6 IAID . . . . . : 135281948
16    DHCPv6 客户端 DUID . . . . . : 00-01-00-01-2B-EB-3E-08-F-C3-1C-9A-4C
17    DNS 服务器 . . . . . : 180.168.255.118
18    : 116.228.111.18
19    TCP/IP 上的 NetBIOS . . . . . : 已启用
    
```

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。



No.	Time	Source	Destination	Protocol	Length	Info
22	34.092206	Intel_cc:0f:d3	XiaomiMobile_0a:bf:89	ARP	42	192.168.1.107 is at 10:3d:1c:cc:0f:d3
23	34.092246	Intel_cc:0f:d3	XiaomiMobile_b9:e2:b7	ARP	42	192.168.1.107 is at 10:3d:1c:cc:0f:d3
26	35.113388	Intel_cc:0f:d3	XiaomiMobile_0a:bf:89	ARP	42	192.168.1.107 is at 10:3d:1c:cc:0f:d3
33	43.151733	Intel_cc:0f:d3	Broadcast	ARP	42	ARP Announcement for 192.168.1.107
34	45.155318	Intel_cc:0f:d3	Broadcast	ARP	42	ARP Announcement for 192.168.1.107
50	73.522700	Intel_cc:0f:d3	Broadcast	ARP	42	ARP Announcement for 192.168.1.107
51	75.555818	Intel_cc:0f:d3	Broadcast	ARP	42	ARP Announcement for 192.168.1.107
52	75.595885	Intel_16:22:95	Intel_cc:0f:d3	ARP	42	192.168.1.108 is at 8c:b8:7e:16:22:95
87	135.894910	Intel_cc:0f:d3	Broadcast	ARP	42	ARP Announcement for 192.168.1.107
90	137.957734	Intel_cc:0f:d3	Broadcast	ARP	42	ARP Announcement for 192.168.1.107

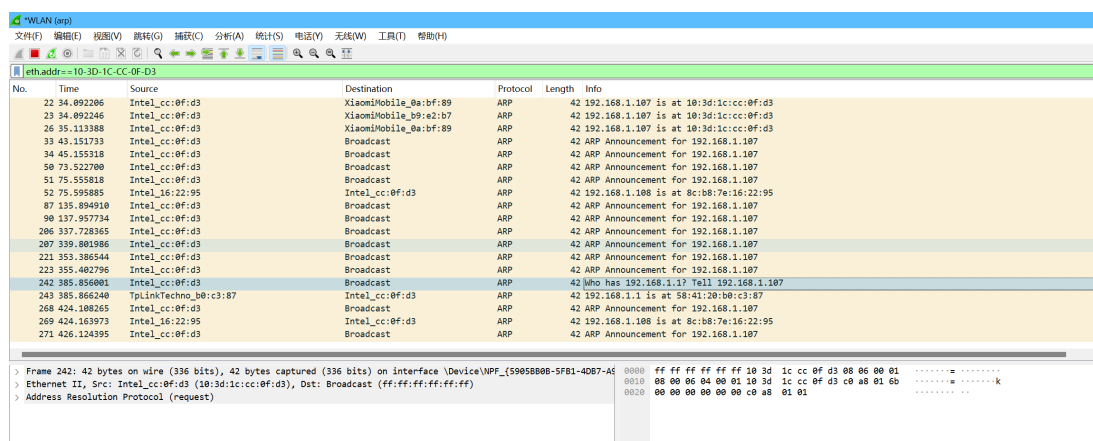
图 2: 设置捕获过滤器

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 3: 清除本机 ARP 缓存

打开 Wireshark，停止捕获。捕获结果如下图所示：



No.	Time	Source	Destination	Protocol	Length	Info
22	34.092206	Intel_cc:0f:d3	XiaomiMobile_0a:bf:89	ARP	42	192.168.1.107 is at 10:3d:1c:cc:0f:d3
23	34.092246	Intel_cc:0f:d3	XiaomiMobile_b9:e2:b7	ARP	42	192.168.1.107 is at 10:3d:1c:cc:0f:d3
26	35.113388	Intel_cc:0f:d3	XiaomiMobile_0a:bf:89	ARP	42	192.168.1.107 is at 10:3d:1c:cc:0f:d3
33	43.151733	Intel_cc:0f:d3	Broadcast	ARP	42	ARP Announcement for 192.168.1.107
34	45.155318	Intel_cc:0f:d3	Broadcast	ARP	42	ARP Announcement for 192.168.1.107
50	73.522700	Intel_cc:0f:d3	Broadcast	ARP	42	ARP Announcement for 192.168.1.107
51	75.555818	Intel_cc:0f:d3	Broadcast	ARP	42	ARP Announcement for 192.168.1.107
52	75.595885	Intel_16:22:95	Intel_cc:0f:d3	ARP	42	192.168.1.108 is at 8c:b8:7e:16:22:95
87	135.894910	Intel_cc:0f:d3	Broadcast	ARP	42	ARP Announcement for 192.168.1.107
90	137.957734	Intel_cc:0f:d3	Broadcast	ARP	42	ARP Announcement for 192.168.1.107
206	337.728365	Intel_cc:0f:d3	Broadcast	ARP	42	ARP Announcement for 192.168.1.107
207	339.801986	Intel_cc:0f:d3	Broadcast	ARP	42	ARP Announcement for 192.168.1.107
221	355.386544	Intel_cc:0f:d3	Broadcast	ARP	42	ARP Announcement for 192.168.1.107
223	355.402796	Intel_cc:0f:d3	Broadcast	ARP	42	ARP Announcement for 192.168.1.107
242	385.856001	Intel_cc:0f:d3	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.107
243	385.866240	TpLinkTechno_b8:c3:87	Intel_cc:0f:d3	ARP	42	192.168.1.1 is at 58:41:20:b0:c3:87
268	424.100265	Intel_cc:0f:d3	Broadcast	ARP	42	ARP Announcement for 192.168.1.107
269	424.163973	Intel_16:22:95	Intel_cc:0f:d3	ARP	42	192.168.1.108 is at 8c:b8:7e:16:22:95
271	426.124395	Intel_cc:0f:d3	Broadcast	ARP	42	ARP Announcement for 192.168.1.107

图 4: 捕获结果

## 4.2 回答问题

1. 通过语句 “eth.addr==01:02:03:04:05:06” 的形式，在 wireshark 中设置过滤器，找出与自己 mac 地址相关的 arp 报文。Arp 报文包括请求报文和应答报文，仔细分析两种报文的格式。

**ARP 请求报文格式：**

字段	长度（字节）	说明
硬件类型	2	表示使用的数据链路层协议, 对于以太网为 1
协议类型	2	表示要映射的上层协议类型, 对于 IPv4 为 0x0800
硬件地址长度	1	硬件地址长度, 对于以太网 MAC 地址为 6
协议地址长度	1	协议地址长度, 对于 IPv4 地址为 4
操作代码	2	ARP 请求的操作代码为 1
发送方硬件地址	6	发送者的硬件地址（MAC 地址）
发送方协议地址	4	发送者的协议地址（IP 地址）
目标硬件地址	6	通常全为 0，因为不知道目标的硬件地址
目标协议地址	4	请求解析的目标协议地址（IP 地址）

**ARP 应答报文格式：**

字段	长度（字节）	说明
硬件类型	2	表示使用的数据链路层协议, 对于以太网为 1
协议类型	2	表示要映射的上层协议类型, 对于 IPv4 为 0x0800
硬件地址长度	1	硬件地址长度, 对于以太网 MAC 地址为 6
协议地址长度	1	协议地址长度, 对于 IPv4 地址为 4
操作代码	2	ARP 应答的操作代码为 2
发送方硬件地址	6	响应者的硬件地址（MAC 地址）
发送方协议地址	4	响应者的协议地址（IP 地址）
目标硬件地址	6	初始请求中的发送方硬件地址
目标协议地址	4	初始请求中的发送方协议地址

2. 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：

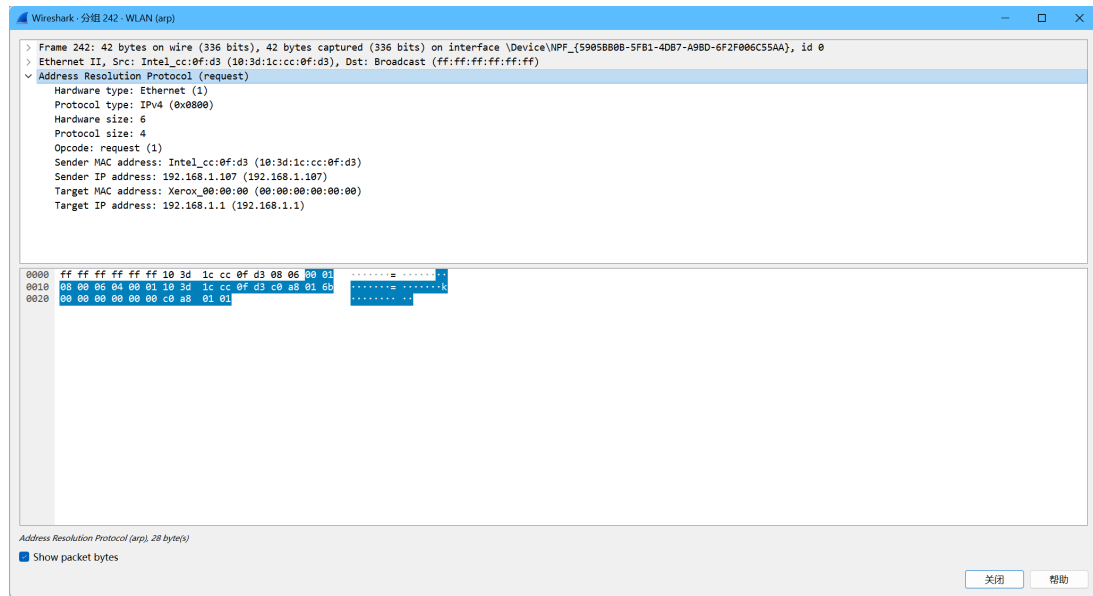


图 5: 选择 ARP 请求数据包

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：

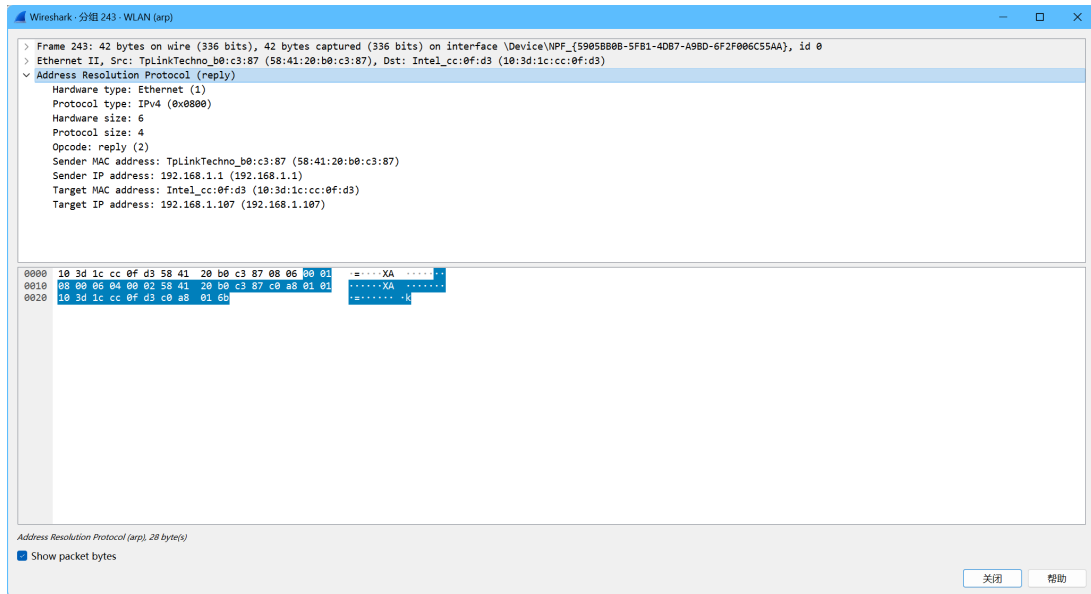


图 6: 选择 ARP 应答数据包

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

3. (a) 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。

(b) 一个请求的 ARP 的报头有多大？应答呢？

长度均为 28 字节。

(c) 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。

(d) 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。

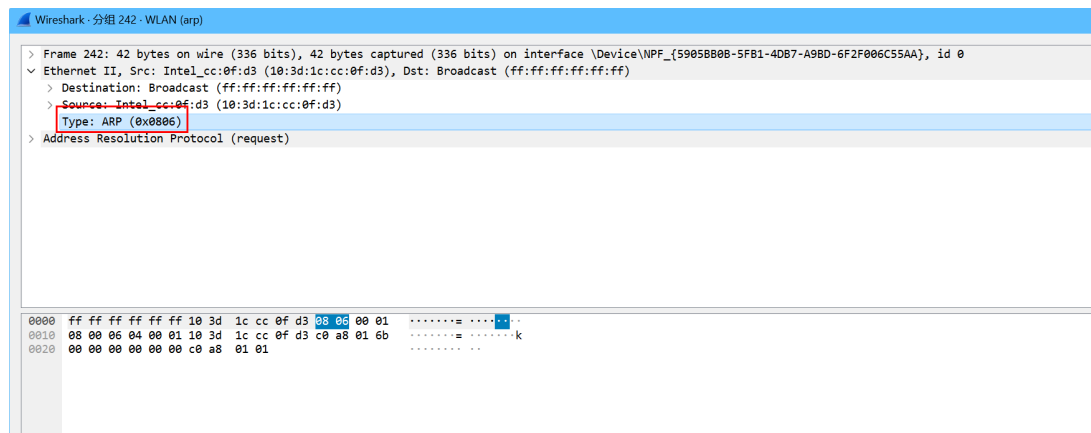


图 7: ARP 的类型值为 0x0806

(e) ARP 应答是广播吗？

在以太网层可以看出，ARP 应答是单播。

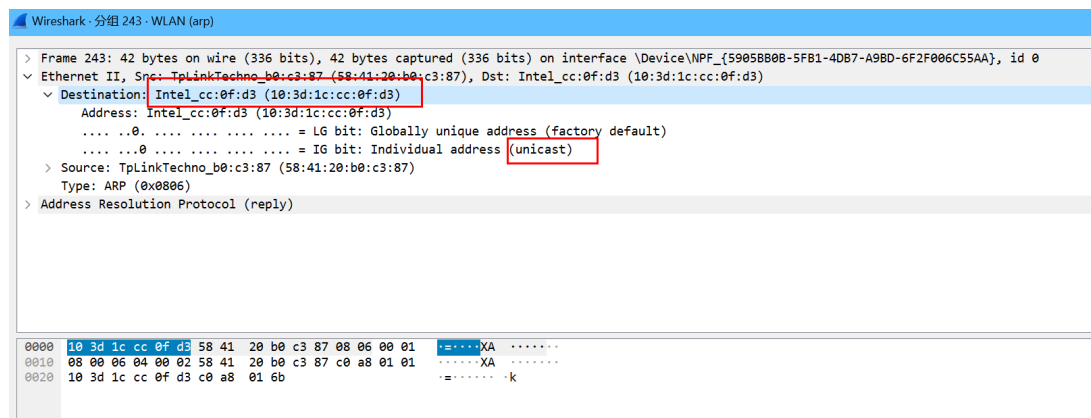


图 8: ARP 应答是单播

### 4.3 自主探索 ARP 报文

1. 其他计算机广播的 ARP 请求。本地网络上的其他计算机也在使用 ARP。由于请求是以广播形式发送的，因此您的计算机将会接收到这些请求。

答：清除筛选后，可以看到其他计算机发送的 ARP 请求。



No.	Time	Source	Destination	Protocol	Length	Info
84	114.280444	Intel_cc:0f:d3	Broadcast	ARP	60	ARP Announcement for 192.168.1.107
85	116.361744	Intel_cc:0f:d3	Broadcast	ARP	60	ARP Announcement for 192.168.1.107
86	116.999304	TpLinkTechno_b0:c3:87	Broadcast	ARP	60	Who has 192.168.1.100? Tell 192.168.1.1
87	118.999436	TpLinkTechno_b0:c3:87	Broadcast	ARP	60	Who has 192.168.1.110? Tell 192.168.1.1
88	120.999334	TpLinkTechno_b0:c3:87	Broadcast	ARP	60	Who has 192.168.1.109? Tell 192.168.1.1
89	121.999362	TpLinkTechno_b0:c3:87	Broadcast	ARP	60	Who has 192.168.1.109? Tell 192.168.1.1
90	122.999303	TpLinkTechno_b0:c3:87	Broadcast	ARP	60	Who has 192.168.1.109? Tell 192.168.1.1
91	122.999303	TpLinkTechno_b0:c3:87	Broadcast	ARP	60	Who has 192.168.1.106? Tell 192.168.1.1
92	124.999376	TpLinkTechno_b0:c3:87	Broadcast	ARP	60	Who has 192.168.1.102? Tell 192.168.1.1
93	125.999094	TpLinkTechno_b0:c3:87	Broadcast	ARP	60	Who has 192.168.1.102? Tell 192.168.1.1
94	126.999095	TpLinkTechno_b0:c3:87	Broadcast	ARP	60	Who has 192.168.1.102? Tell 192.168.1.1
95	126.999095	TpLinkTechno_b0:c3:87	Broadcast	ARP	60	Who has 192.168.1.104? Tell 192.168.1.1
96	127.999482	TpLinkTechno_b0:c3:87	Broadcast	ARP	60	Who has 192.168.1.104? Tell 192.168.1.1
97	128.999263	TpLinkTechno_b0:c3:87	Broadcast	ARP	60	Who has 192.168.1.100? Tell 192.168.1.1
98	133.848066	Intel_cc:0f:d3	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.105
99	134.999112	TpLinkTechno_b0:c3:87	Broadcast	ARP	60	Who has 192.168.1.106? Tell 192.168.1.1
100	134.999112	TpLinkTechno_b0:c3:87	Broadcast	ARP	60	Who has 192.168.1.112? Tell 192.168.1.1
101	138.999186	TpLinkTechno_b0:c3:87	Broadcast	ARP	60	Who has 192.168.1.110? Tell 192.168.1.1
102	144.999095	TpLinkTechno_b0:c3:87	Broadcast	ARP	60	Who has 192.168.1.100? Tell 192.168.1.1

Frame 98: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF\_{F21BFA7F-CED5-4C93-A7C0-000000000000} (0:00:00:00:00:00:00:00) on interface \Device\NPF\_{F21BFA7F-CED5-4C93-A7C0-000000000000} (0:00:00:00:00:00:00:00)

Ethernet II, Src: Intel\_cc:0f:d3 (10:3d:1c:cc:0f:d3), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Address Resolution Protocol (request)

图 9: 其他计算机发送的 ARP 请求

- 您的计算机发出的 ARP 回复。如果另一台计算机恰好对您的计算机的 IP 地址进行 ARP 查询，那么您的计算机将发送一个 ARP 回复以告知查询结果。

答：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）：

259	404.997647	TpLinkTechno_b0:c3:87	Broadcast	ARP	60	Who has 192.168.1.109? Tell 192.168.1.1
260	405.997673	TpLinkTechno_b0:c3:87	Broadcast	ARP	60	Who has 192.168.1.113? Tell 192.168.1.1
261	405.997674	TpLinkTechno_b0:c3:87	Broadcast	ARP	60	Who has 192.168.1.109? Tell 192.168.1.1
262	409.997663	TpLinkTechno_b0:c3:87	Broadcast	ARP	60	Who has 192.168.1.106? Tell 192.168.1.1
263	414.961304	Intel_cc:0f:d3	Broadcast	ARP	60	Who has 192.168.1.111? Tell 192.168.1.105
264	414.961321	CompaInform_1c:9a:4c	Intel_cc:0f:d3	ARP	42	192.168.1.111 is at 08:8f:c3:1c:9a:4c
265	414.997749	TpLinkTechno_b0:c3:87	Broadcast	ARP	60	Who has 192.168.1.100? Tell 192.168.1.1
266	416.997642	TpLinkTechno_b0:c3:87	Broadcast	ARP	60	Who has 192.168.1.102? Tell 192.168.1.1
267	417.997689	TpLinkTechno_b0:c3:87	Broadcast	ARP	60	Who has 192.168.1.113? Tell 192.168.1.1

图 10: 本机发送了 ARP 应答

- 自发 ARP (Gratuitous ARPs)，其中您的计算机发送有关自身的请求或回复。当计算机或链接上线时，这有助于确保没有其他人正在使用相同的 IP 地址。自发 ARP 具有相同的发送方和目标 IP 地址，并且在 Wireshark 中它们的信息字段会标识其为自发 ARP。

答：可以在捕获列表中看到 gratuitous ARP 数据包。

Broadcast	ARP	60	Gratuitous ARP for 0.0.0.0 (Request)
Broadcast	ARP	60	Gratuitous ARP for 0.0.0.0 (Reply)
Broadcast	ARP	60	Gratuitous ARP for 0.0.0.0 (Request)
Broadcast	ARP	60	Gratuitous ARP for 0.0.0.0 (Reply)
Broadcast	ARP	60	Gratuitous ARP for 0.0.0.0 (Request)
Broadcast	ARP	60	Gratuitous ARP for 0.0.0.0 (Reply)
Broadcast	ARP	60	Gratuitous ARP for 0.0.0.0 (Request)
Broadcast	ARP	60	Gratuitous ARP for 0.0.0.0 (Reply)
Broadcast	ARP	60	Gratuitous ARP for 0.0.0.0 (Request)
Broadcast	ARP	60	Gratuitous ARP for 0.0.0.0 (Reply)
Broadcast	ARP	60	Gratuitous ARP for 0.0.0.0 (Request)
Broadcast	ARP	60	Gratuitous ARP for 0.0.0.0 (Reply)

图 11: 捕获到的 gratuitous ARP 数据包

- 您的计算机发出的其他 ARP 请求及相应的 ARP 回复。在您清空其 ARP 缓存后，您的计算机可能需要对其他主机（不仅仅是默认网关）进行 ARP 查询。

答：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 12: 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