

华东师范大学软件工程学院实验报告

实验课程：计算机网络实践

年级：2023 级

实验成绩：

实验名称：ARP

姓名：顾翌炜

实验编号：Lab-4

学号：10235101527

实验日期：2024/12/13

指导教师：王廷

组号：01

实验时间：2024/12/13

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，通过菜单栏中的“捕获 → 选项”进行设置，选择当前连接的以太网接口，并将捕获过滤器设为 `arp`，以捕获 `arp` 数据包。

接着，在命令提示符中运行 `ipconfig -all` 命令，以便获取本机的 IP 地址和 MAC 地址。

随后，在 Wireshark 的显示过滤器中输入 `eth.addr==<yourMAC>`（请将 `<yourMAC>` 替换为本机的实际 MAC 地址）。

然后，以管理员权限打开命令提示符，执行 `arp -d` 命令以清空本机的 ARP 缓存。

最后，重新打开 Wireshark，并停止捕获。

2.1.2 回答问题

1. Hand in your drawing of the ARP exchange.
2. What opcode is used to indicate a request? What about a reply?
3. How large is the ARP header for a request? What about for a reply?
4. What value is carried on a request for the unknown target MAC address?
5. What Ethernet Type value which indicates that ARP is the higher layer protocol?

6. Is the ARP reply broadcast (like the ARP request) or not?

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.

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接口, 将捕获过滤器设置为 `arp`, 并将混杂模式关闭, 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 C:\User\GHOST> ipconfig -all
```

- 3) 返回 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 C:\User\GHOST> 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) 对捕获的 ARP 数据包进行详细分析, 并回答相关问题。
- 8) 讨论问题

3 实验环境

- 操作系统: Windows 11 家庭中文版 23H2 22631.4460

- 网络适配器: Killer(R)Wi-Fi 6E AX1675i 160MHz Wireless Network Adapter(211NGW)
- Wireshark: Version 4.4.1
- wget: GNU Wget 1.21.4 built on mingw32

4 实验过程与分析

4.1 捕获数据

首先, 启动 Wireshark, 通过菜单栏中的“捕获 → 选项”进行设置, 选择已连接的以太网接口, 将捕获过滤器设置为 `arp`, 并将混杂模式关闭, 然后开始捕获。

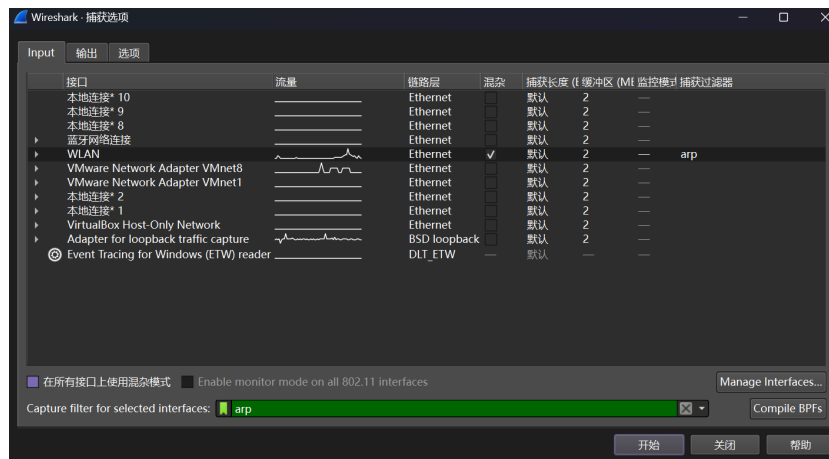


图 1: 设置捕获

然后在命令提示符中使用 `ipconfig -all` 命令获取本机的 IP 地址和 MAC 地址。

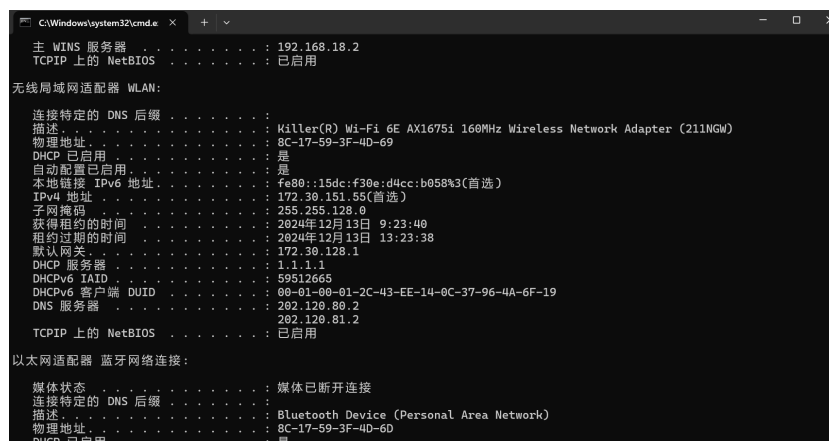


图 2: 获取本机 IP 地址和 MAC 地址

可以看到, 本机的 IP 地址为 172.30.151.55, MAC 地址为 8C-17-59-3F-4D-69。

回到 Wireshark，设置捕获过滤器为 `eth.addr==8C-17-59-3F-4D-69`。

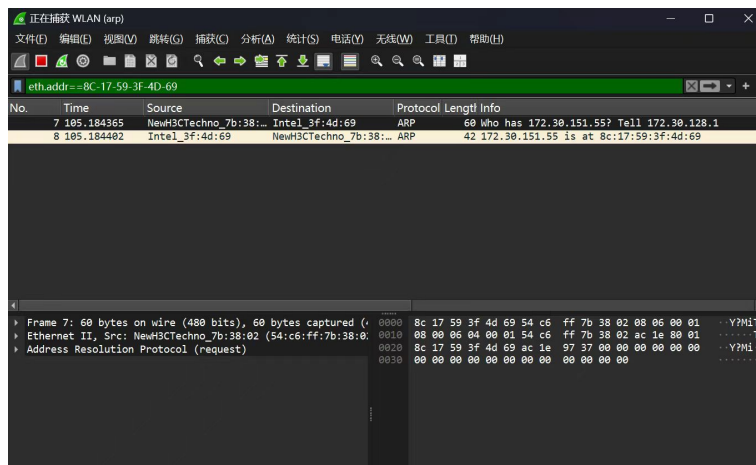


图 3: 设置捕获过滤器

接下来，在管理员模式下，在命令提示符中使用 `arp -d` 命令清除本机的 ARP 缓存。

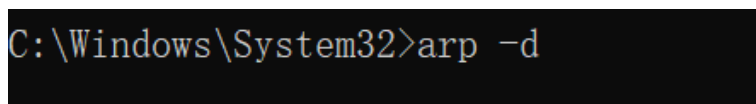


图 4: 清除本机 ARP 缓存

打开 Wireshark，停止捕获。捕获结果如下图所示：

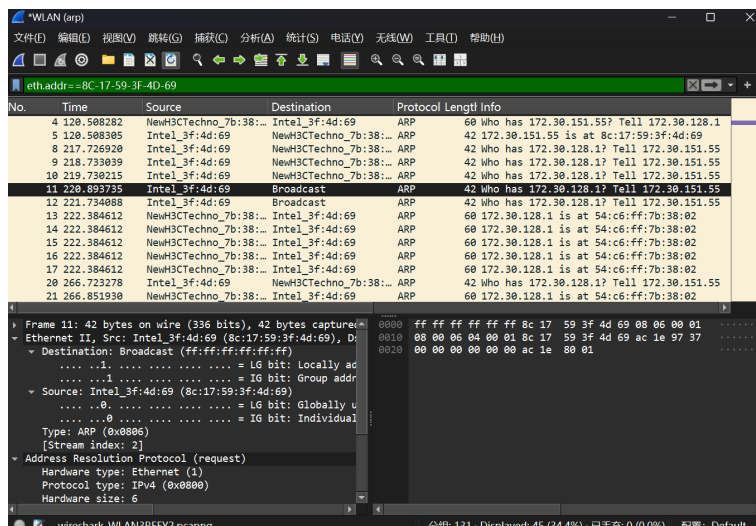


图 5: 捕获结果

4.2 回答问题

1. Hand in your drawing of the ARP exchange.

选择 ARP 请求数据包，如下图所示：

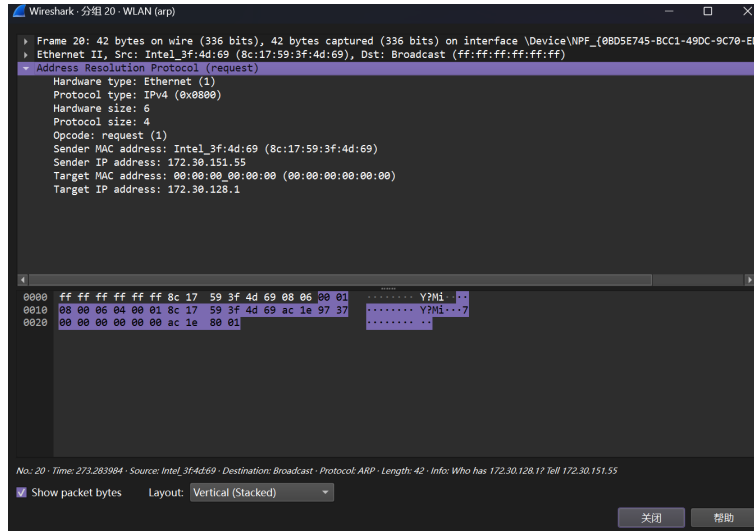


图 6: 选择 ARP 请求数据包

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: 8c:17:59:3f:4d:69，长度为 6 字节
- Sender IP address: 172.30.151.55，长度为 4 字节
- Target MAC address: 00:00:00:00:00:00，长度为 6 字节
- Target IP address: 172.30.128.1，长度为 4 字节

画出 ARP 请求数据包，如下图所示：

Hardware type 2bytes	Protocol type 0x0800(2bytes)	Hardware size: 6 1bytes	Protocol size: 4 1bytes	Opcode 2bytes	
Sender MAC address (6bytes) 8C:17:59:3F:4D:69				Sender IP address (4bytes) 172.30.151.55	
Target MAC address (6bytes) 00:00:00:00:00:00				Target IP address (4bytes) 172.30.128.1	

图 7: ARP 请求数据包

选择一个 ARP 应答数据包，如下图所示：

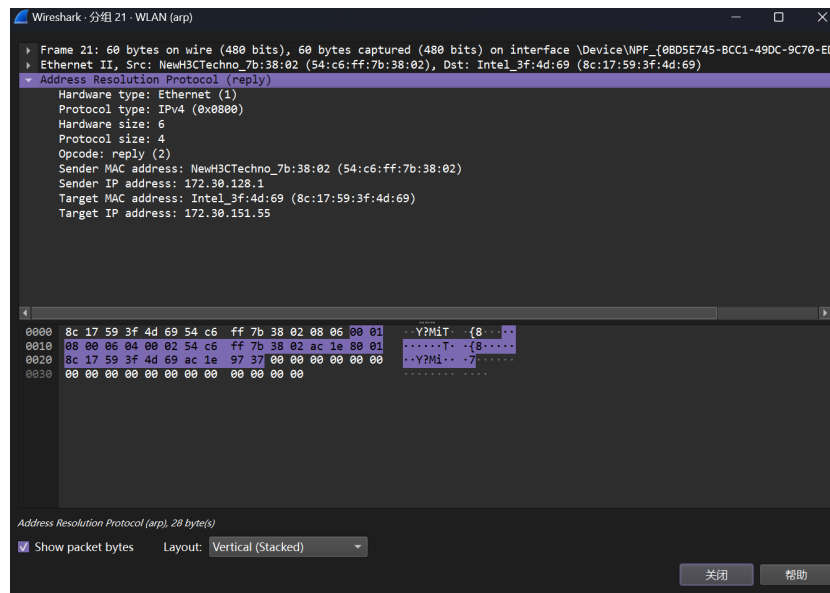


图 8: 选择 ARP 应答数据包

画出 ARP 应答数据包，如下图所示：

Hardware type 2bytes	Protocol type 0x0800(2bytes)	Hardware size 6bytes	Protocol size 4bytes	Opcode 2bytes	
Sender MAC address (6bytes) 54:c6:ff:7b:38:02				Sender IP address (4bytes) 172.30.128.1	
Target MAC address (6bytes) 8c:17:59:3f:4d:69				Target IP address (4bytes) 172.30.151.55	

图 9: ARP 应答数据包

2. What opcode is used to indicate a request? What about a reply?

ARP 报头中的 Opcode 字段用于表示 ARP 请求或应答，其中 Opcode 值为 1 表示请求，值为 2 表示应答。

3. How large is the ARP header for a request? What about for a reply?

二者长度均为 28 字节。

4. What value is carried on a request for the unknown target MAC address?

对未知目标的 MAC 地址的请求是 00:00:00:00:00:00。

5. What Ethernet Type value which indicates that ARP is the higher layer protocol?

以太网类型值为 0x0806 表明 ARP 是更高一层的协议。

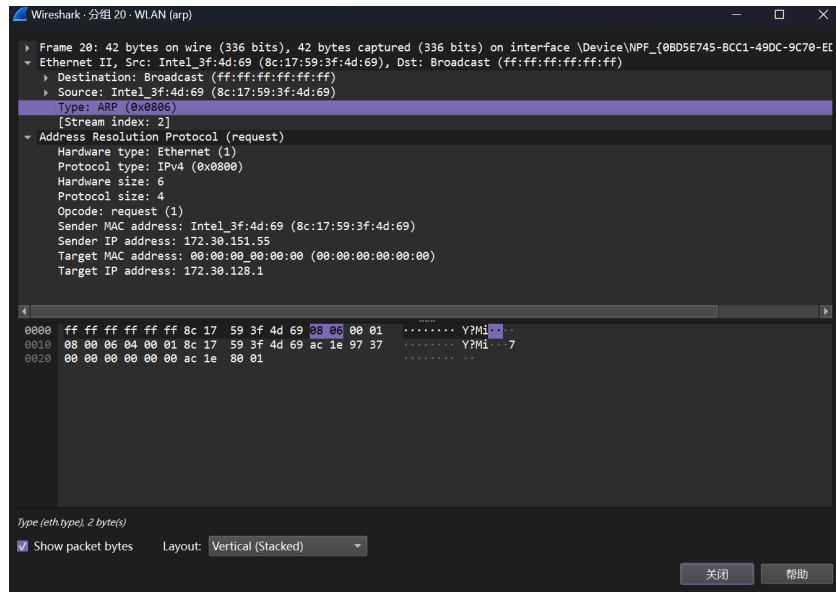


图 10: ARP 的类型值为 0x0806

6. Is the ARP reply broadcast (like the ARP request) or not?

在以太网层可以观察到，ARP 应答是单播。

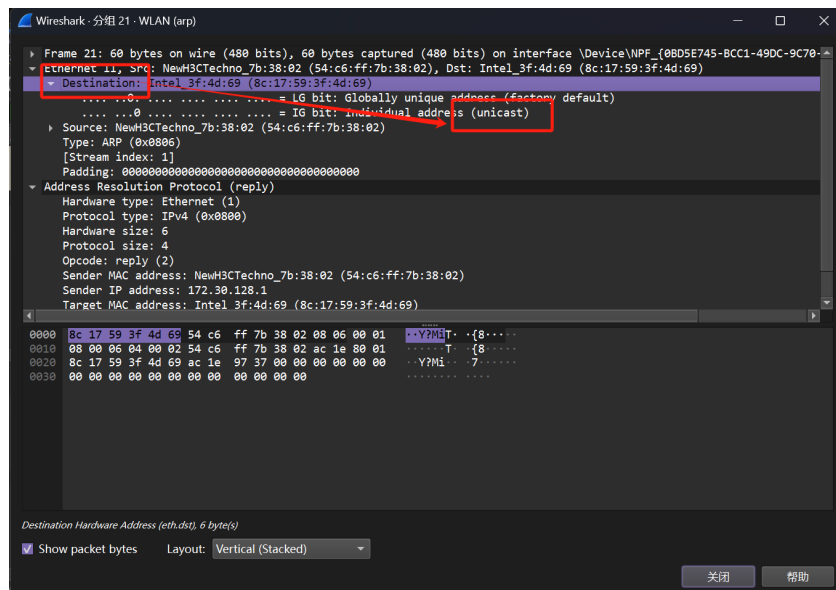


图 11: ARP 应答是单播

4.3 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.

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.

清除过滤器后，可以观察到其他计算机发送的 ARP 请求。

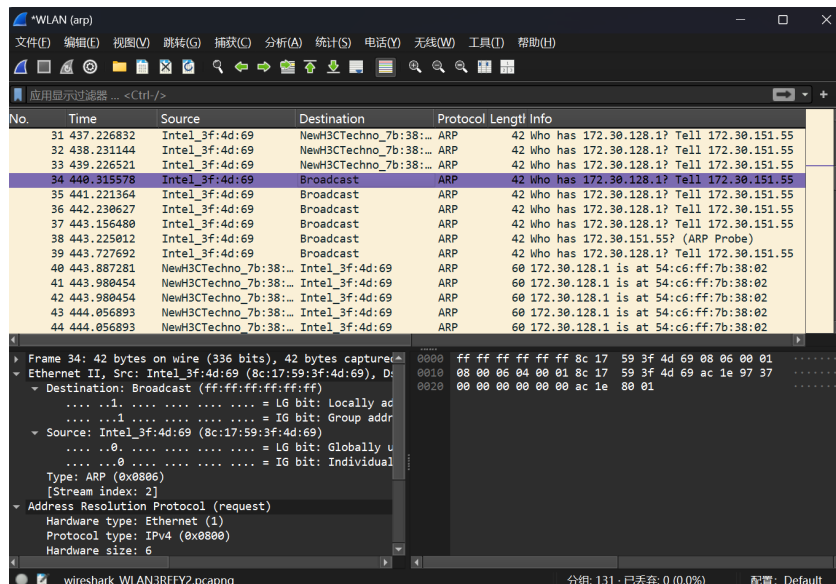


图 12: 其他计算机发送的 ARP 请求

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 172.30.151.55` 命令清除 ARP 缓存，然后使用 `ping 172.30.151.55` 命令向本机发送 ICMP 请求，此时也会发起一个 ARP 请求，本机随后会发送 ARP 应答，如下图所示：

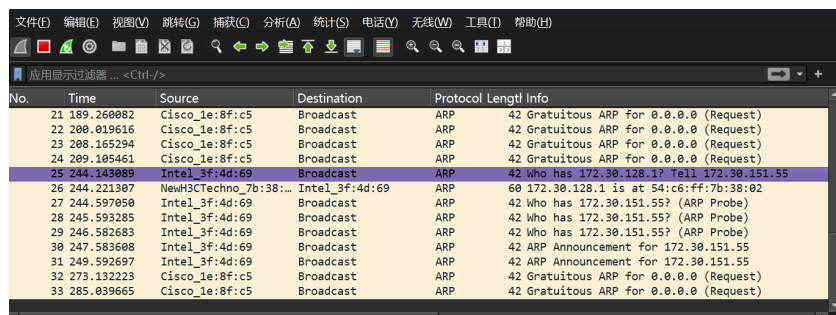
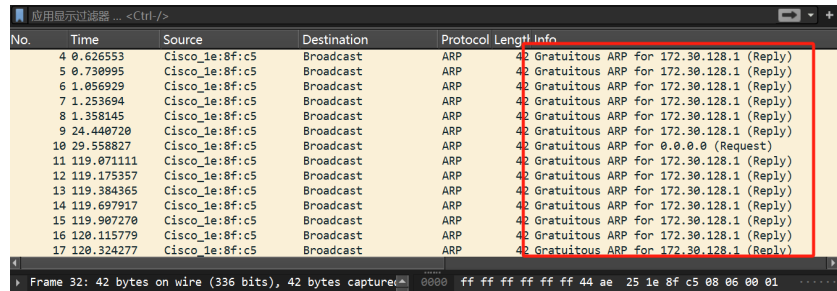


图 13: 本机发送了 ARP 应答

- 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。

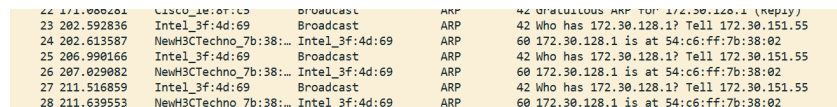


No.	Time	Source	Destination	Protocol	Length	Info
4	0.626553	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 172.30.128.1 (Reply)
5	0.730995	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 172.30.128.1 (Reply)
6	1.056929	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 172.30.128.1 (Reply)
7	1.253694	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 172.30.128.1 (Reply)
8	1.358145	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 172.30.128.1 (Reply)
9	24.440720	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 172.30.128.1 (Reply)
10	29.558827	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 0.0.0.0 (Request)
11	119.071111	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 172.30.128.1 (Reply)
12	119.175357	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 172.30.128.1 (Reply)
13	119.384365	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 172.30.128.1 (Reply)
14	119.697917	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 172.30.128.1 (Reply)
15	119.907270	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 172.30.128.1 (Reply)
16	120.115779	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 172.30.128.1 (Reply)
17	120.324277	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 172.30.128.1 (Reply)

图 14: 捕获到的 gratuitous ARP 数据包

- 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，可以观察到相关请求。



No.	Time	Source	Destination	Protocol	Length	Info
22	171.000401	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 172.30.128.1 (Reply)
23	202.592836	Intel_3f:4d:69	Broadcast	ARP	42	Who has 172.30.128.1? Tell 172.30.151.55
24	202.613587	NewH3CTechno_7b:38:02	Intel_3f:4d:69	ARP	60	172.30.128.1 is at 54:c6:ff:7b:38:02
25	206.990166	Intel_3f:4d:69	Broadcast	ARP	42	Who has 172.30.128.1? Tell 172.30.151.55
26	207.029082	NewH3CTechno_7b:38:02	Intel_3f:4d:69	ARP	60	172.30.128.1 is at 54:c6:ff:7b:38:02
27	211.516859	Intel_3f:4d:69	Broadcast	ARP	42	Who has 172.30.128.1? Tell 172.30.151.55
28	211.639553	NewH3CTechno_7b:38:02	Intel_3f:4d:69	ARP	60	172.30.128.1 is at 54:c6:ff:7b:38:02

图 15: 相关请求

5 实验结果总结

本次实验利用 Wireshark 捕获了 ARP 数据包，并通过对其进行详细分析，深入理解了 ARP 数据包的结构及其各字段的含义，从而进一步加深了对 ARP 协议的认识。

6 附录

无