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` 数据报。

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。

```
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。

```
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 IP 数据报进行数据分析，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

5 实验结果总结

6 附录

无