

廈門大學



软件学院

《计算机网络》实验报告

题 目：用 WinPCAP 监听并分析以太网的帧

姓 名：宋泽涛

学 号：25120222201292

班 级：2022 级网络 2 班

实验时间：2024/4/7

2024 年 4 月 7 日

1 实验目的

通过捕获并分析以太网帧，分析常见数据包的帧格式，熟悉以太网中常用协议及其报文

格式，如 ARP、ICMP、IP 协议。

学会对捕获到的数据帧按指定的条件进行过滤，为网络流量深入分析做基础。所谓的指

定条件可包含：指定的目的 IP 地址、指定的源 IP 地址、指定的协议类型等（参考 Wireshark

的过滤条件），比如当指定协议类型为 IP 时，其它类型的数据帧将被丢弃，仅留下 IP 数据

帧。

2 实验环境

操作系统：Win11

编程语言：C/C++

3 实验结果

1. 使用 Windows 自带的“命令提示符”或“PowerShell”完成本机 IP、MAC 地址等信息的查询工作

```
管理员: C:\WINDOWS\system
C:\Users\MI>ipconfig

Windows IP 配置

无线局域网适配器 本地连接 * 13:

    媒体状态 . . . . . : 媒体已断开连接
    连接特定的 DNS 后缀 . . . . . :

无线局域网适配器 本地连接 * 14:

    媒体状态 . . . . . : 媒体已断开连接
    连接特定的 DNS 后缀 . . . . . :

无线局域网适配器 WLAN 2:

    连接特定的 DNS 后缀 . . . . . : xmu.edu.cn
    IPv6 地址 . . . . . : 2409:8734:1a70:7e2:ad7b:2eff:22a7:c5e9
    临时 IPv6 地址 . . . . . : 2409:8734:1a70:7e2:6d58:98fa:5210:df82
    本地链接 IPv6 地址 . . . . . : fe80::b47e:a4aa:2720:4d9b%6
    IPv4 地址 . . . . . : 10.30.44.240
    子网掩码 . . . . . : 255.255.224.0
    默认网关 . . . . . : fe80::42fe:95ff:fefe:8001%6
                        10.30.32.1

以太网适配器 以太网:

    媒体状态 . . . . . : 媒体已断开连接
    连接特定的 DNS 后缀 . . . . . :

C:\Users\MI>
```

```
管理员: C:\WINDOWS\system
C:\Users\MI>ipconfig /all

Windows IP 配置

    主机名 . . . . . : LAPTOP-MNST1K25
    主 DNS 后缀 . . . . . :
    节点类型 . . . . . : 混合
    IP 路由已启用 . . . . . : 否
    WINS 代理已启用 . . . . . : 否
    DNS 后缀搜索列表 . . . . . : xmu.edu.cn

无线局域网适配器 本地连接 * 13:

    媒体状态 . . . . . : 媒体已断开连接
    连接特定的 DNS 后缀 . . . . . :
    描述 . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #5
    物理地址 . . . . . : E6-AA-EA-55-0C-71
    DHCP 已启用 . . . . . : 是
    自动配置已启用 . . . . . : 是

无线局域网适配器 本地连接 * 14:

    媒体状态 . . . . . : 媒体已断开连接
    连接特定的 DNS 后缀 . . . . . :
    描述 . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #6
    物理地址 . . . . . : F6-AA-EA-55-0C-71
    DHCP 已启用 . . . . . : 是
    自动配置已启用 . . . . . : 是

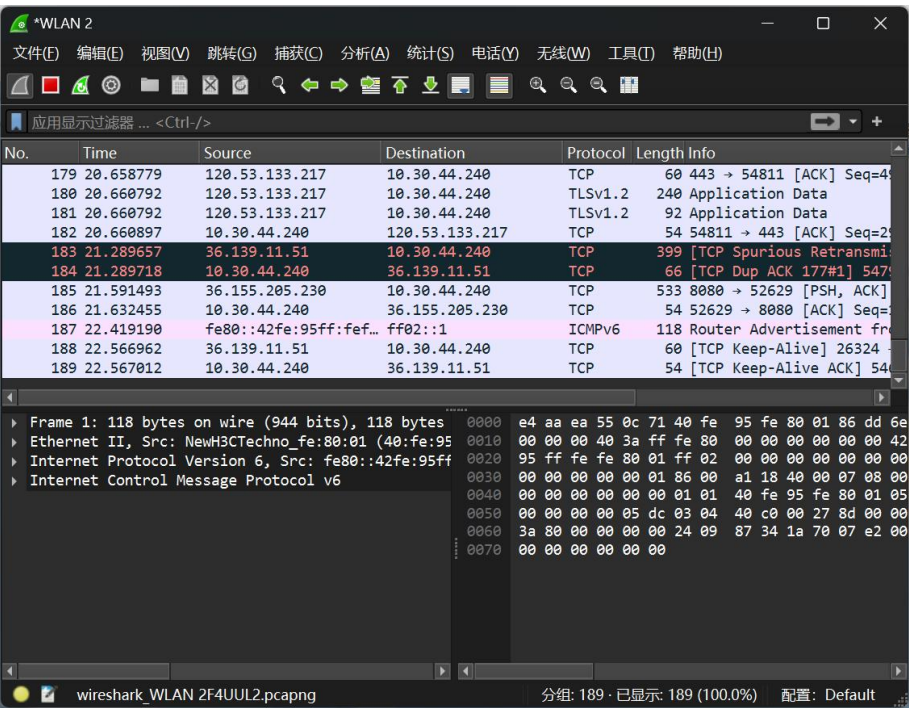
无线局域网适配器 WLAN 2:

    连接特定的 DNS 后缀 . . . . . : xmu.edu.cn
```

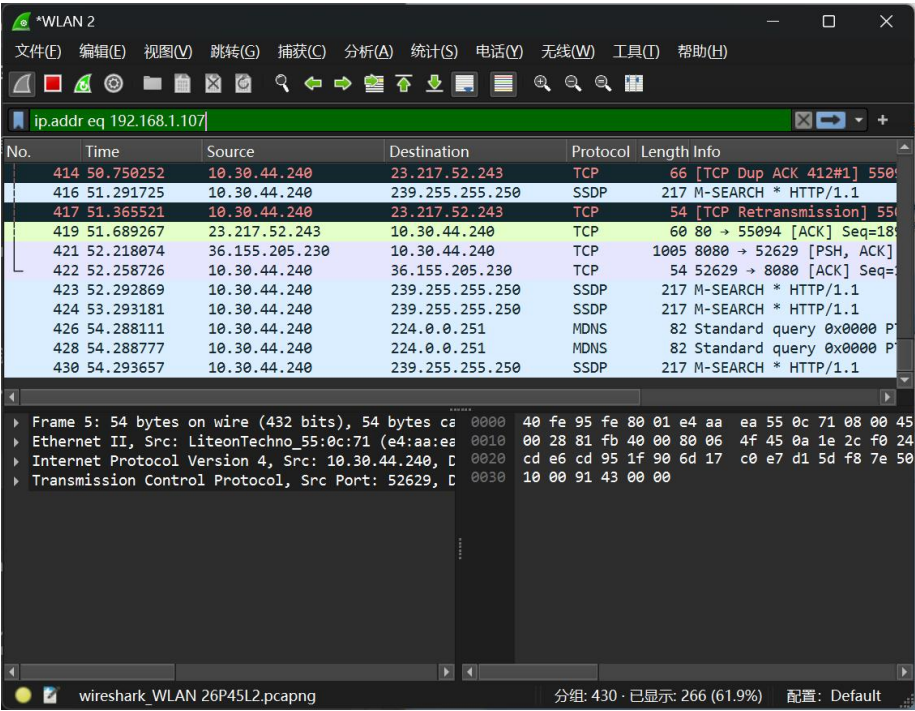
2. 使用 Windows 自带的“命令提示符”或“PowerShell”完成“本机与具有某个 IP 的主机是否连通”的检测



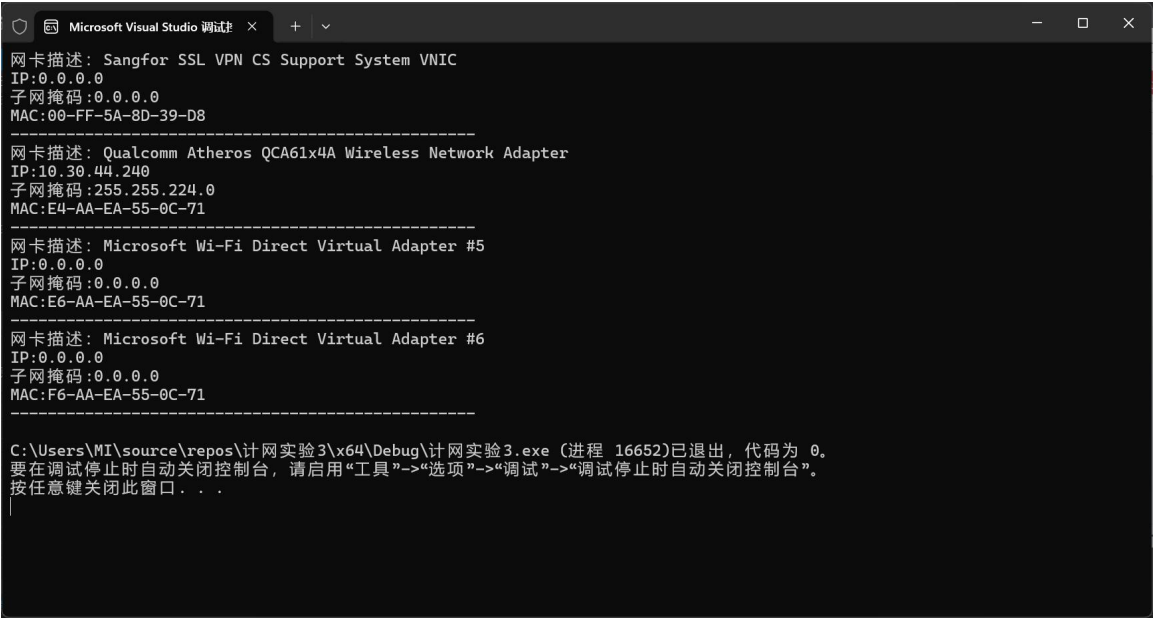
3. 熟悉 Wireshark 的使用，会设置过滤条件，如过滤出指定 IP 的数据帧
过滤前结果如下



过滤后结果如下



4. 配置好实验环境，在控制台打印出网卡设备列表



5. 捕获到以太网帧，并能够解析出目的MAC、源MAC

```
C:\Users\MI\source\repos\itj x + v
协议版本:4
首部长度:20
服务类型:Priority: 0,Service: 0
IP包总长度:1202
标识:17665
标志位:DF=0,MF=0
片偏移:64
生存周期:128
协议类型:6
首部校验和:28456
源地址:10.30.44.240
目的地址:104.46.162.224
=====

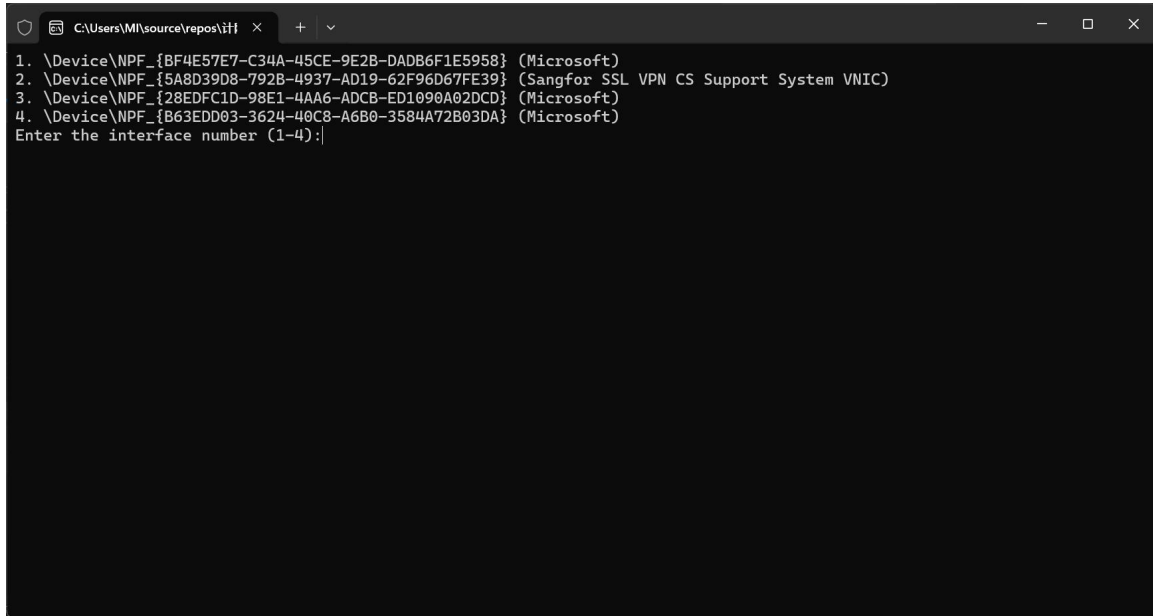
第 72 个 IP 数据包信息:
协议版本:4
首部长度:20
服务类型:Priority: 0,Service: 0
IP包总长度:933
标识:21012
标志位:DF=0,MF=0
片偏移:64
生存周期:128
协议类型:6
首部校验和:15987
源地址:10.30.44.240
目的地址:36.139.11.51
=====
```

```
C:\Users\MI\source\repos\itj x + v
协议版本:4
首部长度:20
服务类型:Priority: 0,Service: 0
IP包总长度:40
标识:21520
标志位:DF=0,MF=0
片偏移:64
生存周期:128
协议类型:6
首部校验和:16372
源地址:10.30.44.240
目的地址:36.139.11.51
=====

第 13 个 IP 数据包信息:
协议版本:4
首部长度:20
服务类型:Priority: 0,Service: 0
IP包总长度:332
标识:21521
标志位:DF=0,MF=0
片偏移:64
生存周期:128
协议类型:6
首部校验和:16079
源地址:10.30.44.240
目的地址:36.139.11.51
=====
```

6. 能够过滤出特定类型的数据包，指定类型的为 ARP，ICMP 等

选择需要监听的网卡



```
C:\Users\MI\source\repos\jij > netsh interface portmon <enter>
1. \Device\NPF_{BF4E57E7-C34A-45CE-9E2B-DADB6F1E5958} (Microsoft)
2. \Device\NPF_{5A8D39D8-792B-4937-AD19-62F96D67FE39} (Sangfor SSL VPN CS Support System VNIC)
3. \Device\NPF_{28EDFC1D-98E1-4AA6-ADCB-ED1090A02DCD} (Microsoft)
4. \Device\NPF_{B63E0D03-3624-40C8-A6B0-3584A72B03DA} (Microsoft)
Enter the interface number (1-4):
```

监听结果如下



```
09:23:57.574583 len:92
get an ip packet
DEST MAC:ff:ff:ff:ff:ff:ff
SRC MAC:08:d2:3e:cb:17:cc

09:23:58.324606 len:92
get an ip packet
DEST MAC:ff:ff:ff:ff:ff:ff
SRC MAC:08:d2:3e:cb:17:cc

09:24:01.453020 len:129
get an ip packet
DEST MAC:08:d2:3e:cb:17:cc
SRC MAC:e4:ca:d9:3e:d7:59
```

4 实验总结

1. 理解以太网帧：通过本实验，我对捕获和分析以太网帧进行了实际操作。通过这个过程，我深入了解了常见数据包的结构和格式，例如 ARP、ICMP 和 IP 协议；

2. 过滤捕获的帧：我学会了根据指定的条件过滤捕获的帧，如目标 IP 地址、源 IP 地址和协议类型。通过应用过滤器，我能够集中精力分析特定类型的网络流量，有助于深入分析网络行为；

3. WinPCAP 使用：本实验涉及使用 WinPCAP，在 Windows 平台上进行数据包捕获和分析。通过实际应用，我熟悉了 WinPCAP 的功能，可以捕获和解析网络数据包。