

****

信息学院软件工程系

《计算机网络》实验报告

**题　　目 实验三 用 PCAP 库侦听并分析网络流量**

**班　　级 软件工程2018级3班**

**姓　　名 饶龙宇**

**学　　号 24320182203256**

**实验时间 2020年3月22日**

**2020 年 3 月 22 日**

# 实验目的

本实验是“用 PCAP 库侦听并解析 FTP 口令”实验的第一部分。

用 WinPCAP 或 libPcap 库侦听并分析以太网的帧，记录目标与源 MAC 和 IP 地 址。

基于 WinPCAP 工具包制作程序，实现侦听网络上的数据流，解析发送方与接收 方的 MAC 和 IP 地址，并作记录与统计，对超过给定阈值（如：1MB）的流量进行告 警。对 Linux 用户，可以使用 libpcap 编程实现。

程序在文件上输出形如下列 CSV 格式的日志：

时间、源 MAC、源 IP、目标 MAC、目标 IP、帧长度（以逗号间隔）

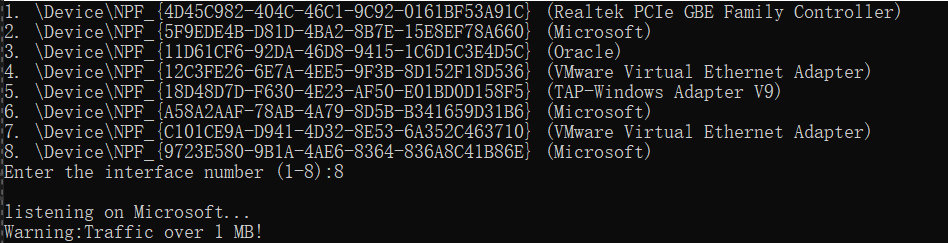
每隔一段时间（如 1 分钟），程序统计来自不同 MAC 和 IP 地址的通信数据长度， 统计发至不同 MAC 和 IP 地址的通信数据长度。

# 实验环境

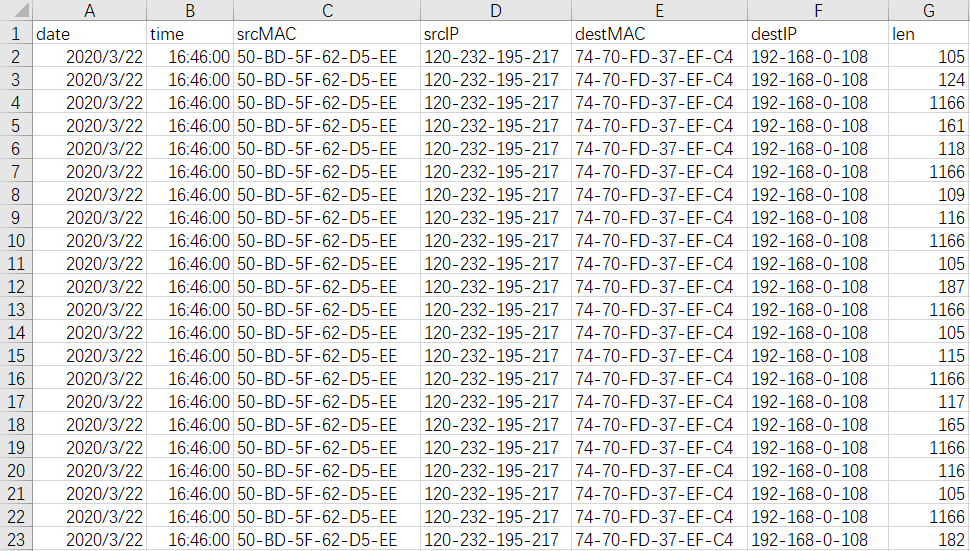
编程环境：Windows10 Visual Studio 2019

编程语言：C++

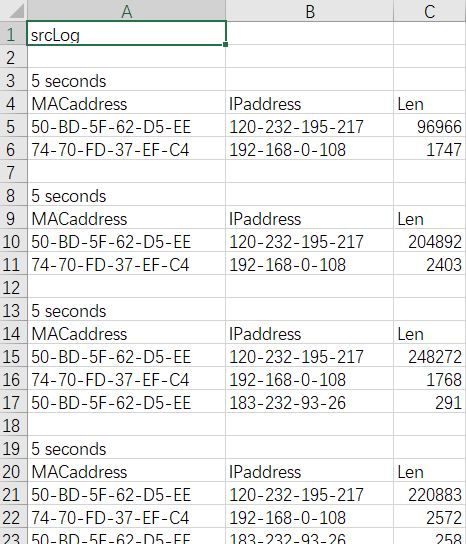
# 实验结果



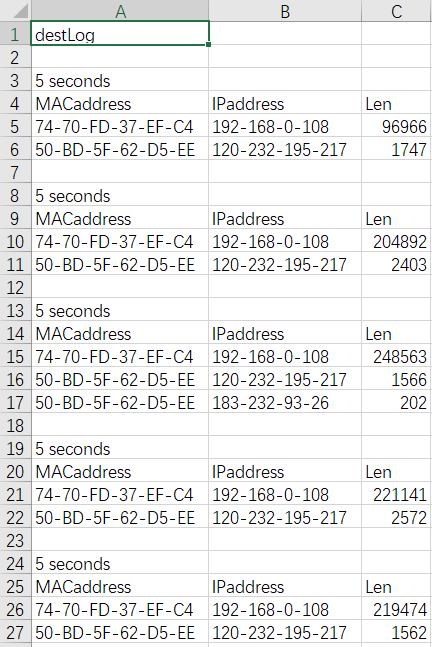
1.流量超过给定阈值(1MB)告警



侦听网络上的数据流，解析发送方与接收方的 MAC 和 IP 地址，并作记录，形成CSV格式的日志。



每隔一段时间（5秒），程序统计来自不同 MAC 和 IP 地址的通信数据长度



每隔一段时间（5秒），程序统计发至不同 MAC 和 IP 地址的通信数据长度

# 实验总结

通过本次实验，我初步掌握了winPcap库的使用。在观看黄老师精心讲解的视频后，对于编程中遇到的问题，我能更准确地寻求搜索引擎的帮助，这个宝贵经验不仅作用于本次实验，还会对我往后的学习生活产生正向影响，让我认识到我需要努力掌握的其实是学习方法。