

廈門大學



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 宋润涵

学 号 24320182203266

实验时间 2020 年 3 月 11 日

2020 年 3 月 15 日

1 实验目的

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

程序在文件上输出形如下列 CSV 格式的日志：

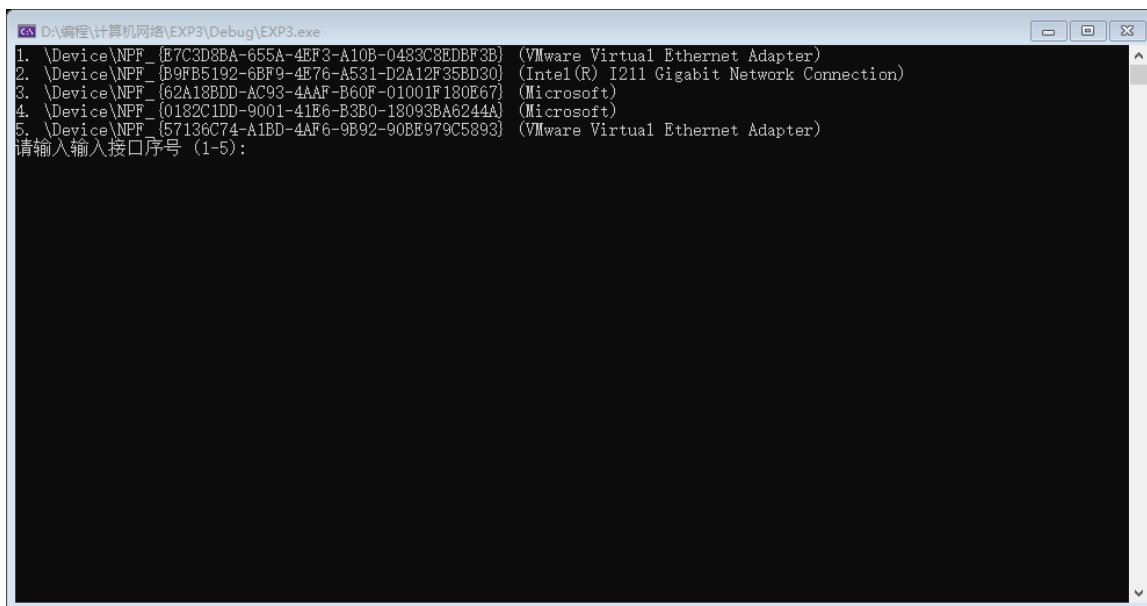
时间、源 MAC、源 IP、目标 MAC、目标 IP、帧长度（以逗号间隔）

2015-03-14 13:05:16,60-36-DD-7D-D5-21,192.168.33.1,60-36-DD-7D-D572,192.168.33.2,1536 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。

2 实验环境

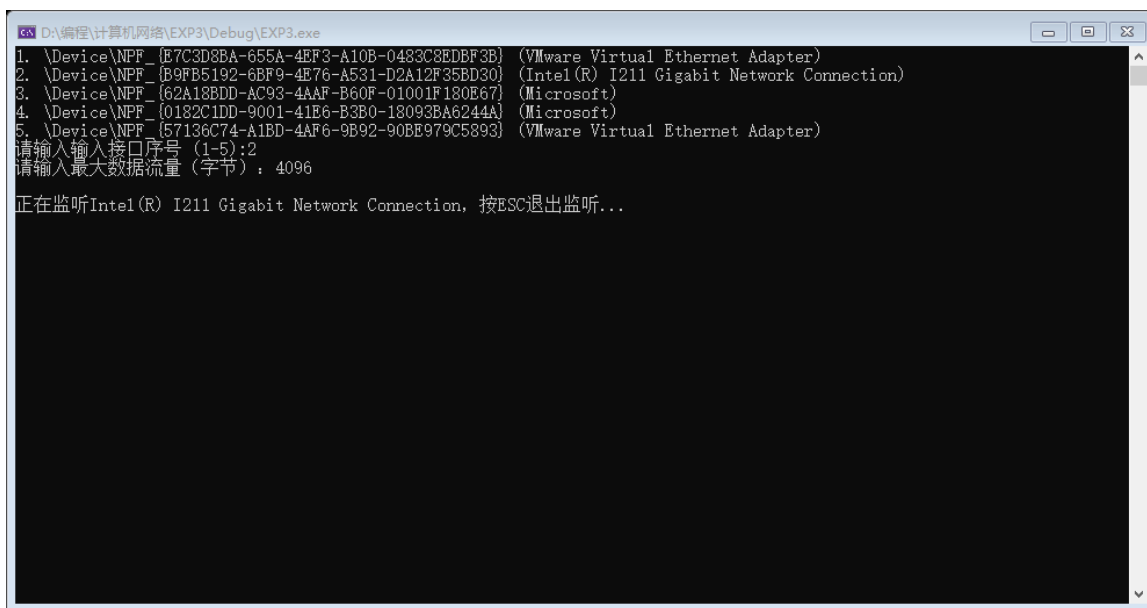
Windows 10, Visual Studio 2019, C++, WinPcap 4.1.2。

3 实验结果



```
D:\编程\计算机网络\EXP3\Debug\EXP3.exe
1. \Device\NPF_{E7C3D8BA-655A-4EF3-A10B-0483C8EDBF3B} (VMware Virtual Ethernet Adapter)
2. \Device\NPF_{B9FB5192-6BF9-4E76-A531-D2A12F35BD30} (Intel(R) I211 Gigabit Network Connection)
3. \Device\NPF_{62A18BDD-AC93-4AAF-B60F-01001F180E67} (Microsoft)
4. \Device\NPF_{0182C1DD-9001-41E6-B3B0-18093BA6244A} (Microsoft)
5. \Device\NPF_{57136C74-A1BD-4AF6-9B92-90BE979C5893} (VMware Virtual Ethernet Adapter)
请输入输入接口序号 (1-5):
```

选择需要监听的适配器名称。



```
D:\编程\计算机网络\EXP3\Debug\EXP3.exe
1. \Device\NPF_{E7C3D8BA-655A-4EF3-A10B-0483C8EDBF3B} (VMware Virtual Ethernet Adapter)
2. \Device\NPF_{B9FB5192-6BF9-4E76-A531-D2A12F35BD30} (Intel(R) I211 Gigabit Network Connection)
3. \Device\NPF_{62A18BDD-AC93-4AAF-B60F-01001F180E67} (Microsoft)
4. \Device\NPF_{0182C1DD-9001-41E6-B3B0-18093BA6244A} (Microsoft)
5. \Device\NPF_{57136C74-A1BD-4AF6-9B92-90BE979C5893} (VMware Virtual Ethernet Adapter)
请输入输入接口序号 (1-5):2
请输入最大数据流量 (字节): 4096

正在监听Intel(R) I211 Gigabit Network Connection, 按ESC退出监听...
```

再输入流量限制后程序就会开始监听，按 ESC 可以退出。

4 实验总结

本次实验使用了颇有年代感的 WinPcap。在使用的时候加深了对于函数指针（回调函数）的理解。另外也发现了 IP 地址不光可以同结构体表示，也可以用 4 字节整数表示。

除此以外还学习了如何设计使用定时器（虽然不是异步），如何使用 C++ 的 map 等。