

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 1 班

姓 名 刘久一

学 号 24320182203235

实验时间 2020 年 3 月 16 日

2020 年 3 月 16 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。

2 实验环境

Microsoft Windows 10

Microsoft Visual Studio 2019

WinPcap V4.1.3

WireShark V3.2.2

3 实验结果

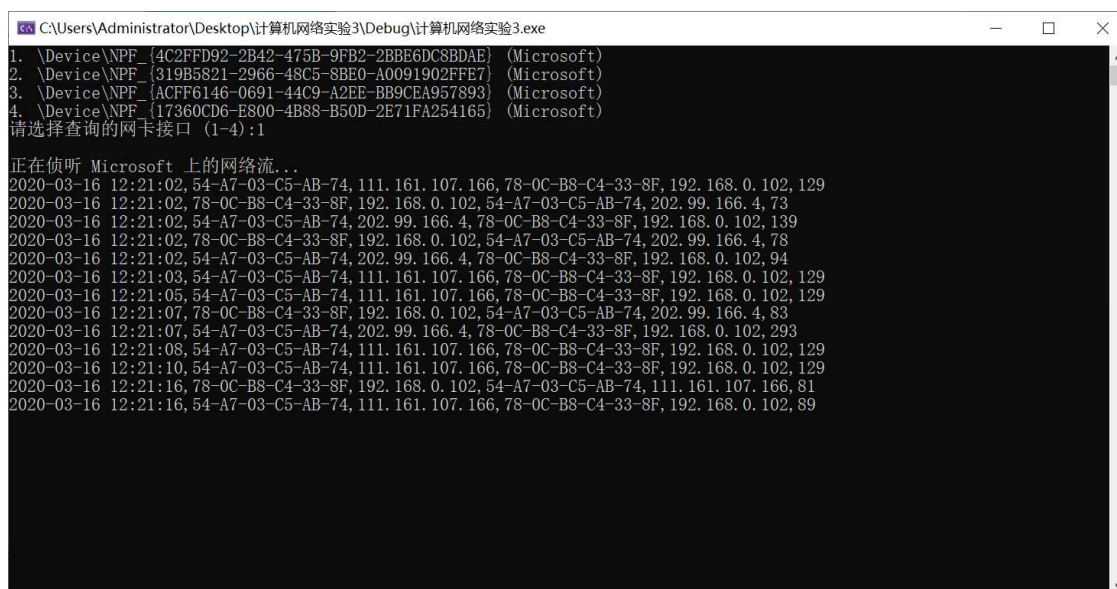
```

1 struct macinfo
1 {
1     u_char dstmac[6];
1     u_char srcmac[6];
1     u_char type[2];
1     macinfo() {}
1     macinfo(const u_char*src)
1     {
1         int tot = 0;
1         for (int i = 0; i < 6; i++)dstmac
1         for (int i = 0; i < 6; i++)srcmac
1         for (int i = 0; i < 2; i++)type[
1     }
1     void printdstmac()
1     {
1         for (int i = 0; i < 6; i++)
1         {
1             if (i)printf("-");
1             printf("%02X", dstmac[i]);
1         }
1     }
1     void printsrcmac()
1     {
1         for (int i = 0; i < 6; i++)

```

新建 macinfo 类专门为提取 mac 地址信

息;



```

C:\Users\Administrator\Desktop\计算机网络实验3\Debug\计算机网络实验3.exe
1. \Device\NPF_{4C2FFD92-2B42-475B-9FB2-2BBE6DC8BDAE} (Microsoft)
2. \Device\NPF_{319B5821-2966-48C5-SBE0-A0091902FFE7} (Microsoft)
3. \Device\NPF_{ACFF6146-0691-44C9-A2EE-BB9CEA957893} (Microsoft)
4. \Device\NPF_{17360CD6-E800-4B88-B50D-2E71FA254165} (Microsoft)
请选择查询的网卡接口 (1-4):1

正在侦听 Microsoft 上的网络流...
2020-03-16 12:21:02, 54-A7-03-C5-AB-74, 111.161.107.166, 78-0C-B8-C4-33-8F, 192.168.0.102, 129
2020-03-16 12:21:02, 78-0C-B8-C4-33-8F, 192.168.0.102, 54-A7-03-C5-AB-74, 202.99.166.4, 73
2020-03-16 12:21:02, 54-A7-03-C5-AB-74, 202.99.166.4, 78-0C-B8-C4-33-8F, 192.168.0.102, 139
2020-03-16 12:21:02, 78-0C-B8-C4-33-8F, 192.168.0.102, 54-A7-03-C5-AB-74, 202.99.166.4, 78
2020-03-16 12:21:02, 54-A7-03-C5-AB-74, 202.99.166.4, 78-0C-B8-C4-33-8F, 192.168.0.102, 94
2020-03-16 12:21:03, 54-A7-03-C5-AB-74, 111.161.107.166, 78-0C-B8-C4-33-8F, 192.168.0.102, 129
2020-03-16 12:21:05, 54-A7-03-C5-AB-74, 111.161.107.166, 78-0C-B8-C4-33-8F, 192.168.0.102, 129
2020-03-16 12:21:07, 78-0C-B8-C4-33-8F, 192.168.0.102, 54-A7-03-C5-AB-74, 202.99.166.4, 83
2020-03-16 12:21:07, 54-A7-03-C5-AB-74, 202.99.166.4, 78-0C-B8-C4-33-8F, 192.168.0.102, 293
2020-03-16 12:21:08, 54-A7-03-C5-AB-74, 111.161.107.166, 78-0C-B8-C4-33-8F, 192.168.0.102, 129
2020-03-16 12:21:10, 54-A7-03-C5-AB-74, 111.161.107.166, 78-0C-B8-C4-33-8F, 192.168.0.102, 129
2020-03-16 12:21:16, 78-0C-B8-C4-33-8F, 192.168.0.102, 54-A7-03-C5-AB-74, 111.161.107.166, 81
2020-03-16 12:21:16, 54-A7-03-C5-AB-74, 111.161.107.166, 78-0C-B8-C4-33-8F, 192.168.0.102, 89

```

在每次捕获的数据包中分析出数据包长度，ip 地址，mac 地址即可。

【update】

```
std::map<std::string, int>srcmac;
std::map<std::string, int>dstmac;//记录源mac和目的mac的发送信息之和
std::map<std::string, int>srcip;
std::map<std::string, int>dstip;//记录源ip和目的ip的发送信息之和
```

利用 STL 中的 map 实现 mac 和 ip 地址的存储，之后每隔一段时间计算所有已记录 mac 和 ip 地址的信息；

```
不同源mac地址的发送情况：
54-A7-03-C5-AB-74 一共发送了13072长度的信息
78-0C-B8-C4-33-8F 一共发送了4073长度的信息
不同目的mac地址的发送情况：
01-00-5E-7F-FF-FA 一共发送了3985长度的信息
54-A7-03-C5-AB-74 一共发送了4073长度的信息
78-0C-B8-C4-33-8F 一共发送了8717长度的信息
FF-FF-FF-FF-FF-FF 一共发送了370长度的信息
```

```
不同源ip地址的发送情况：
125. 39. 132. 237 一共发送了22794长度的信息
192. 168. 0. 1 一共发送了3846长度的信息
192. 168. 0. 101 一共发送了1903长度的信息
不同目的ip地址的发送情况：
125. 39. 132. 237 一共发送了1903长度的信息
192. 168. 0. 101 一共发送了22794长度的信息
192. 168. 0. 255 一共发送了185长度的信息
239. 255. 255. 250 一共发送了3661长度的信息
```

如图所示。

```
2020-03-21 19:44:35, 54-A7-03-C5-AB-74, 192. 168. 0. 1, 01-00-5E-7F-FF-FA, 239. 255. 255. 250, 372
数据已经超过0.05M, 流量预警!
2020-03-21 19:44:35, 54-A7-03-C5-AB-74, 192. 168. 0. 1, 01-00-5E-7F-FF-FA, 239. 255. 255. 250, 333
数据已经超过0.05M, 流量预警!
2020-03-21 19:44:35, 54-A7-03-C5-AB-74, 192. 168. 0. 1, 01-00-5E-7F-FF-FA, 239. 255. 255. 250, 392
数据已经超过0.05M, 流量预警!
```

流量预警机制。

4 实验总结

通过这次试验，我初步掌握了 Wincap 库的简单运用，如何正确阅读复用已完备的代码，以及对数字链路层中以太网的帧格式又有了进一步的巩固理解。