

# 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 2 班

姓    名 林晖

学    号 24320182203231

实验时间 2020 年 3 月 11 日

2020 年 3 月 22 日

## 1 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）

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

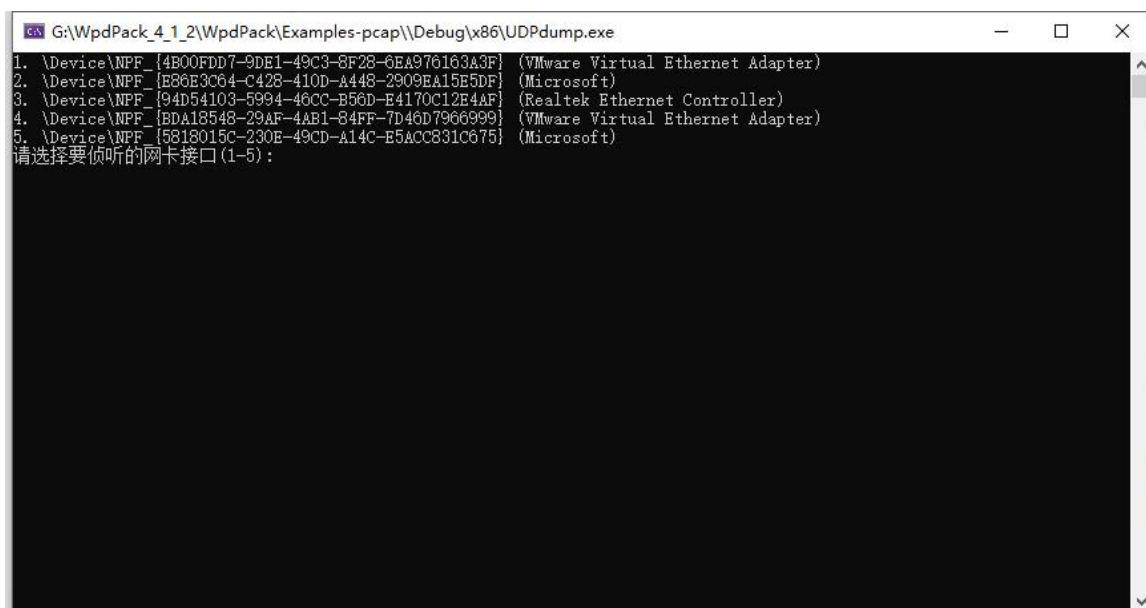
60-36-DD-7D-D5-72,192.168.33.2,1536

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。

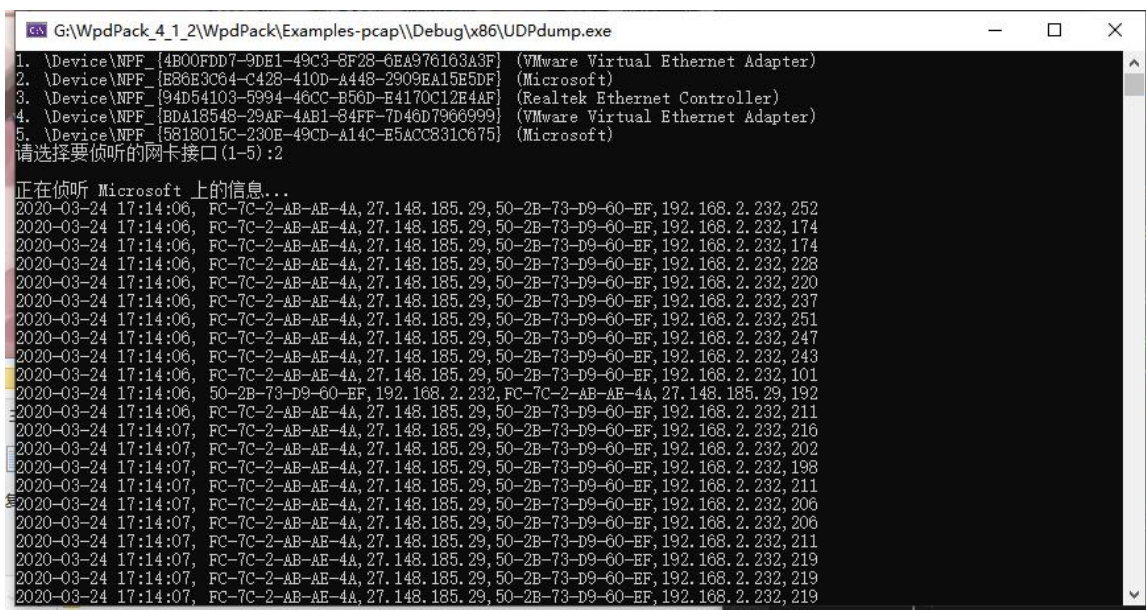
## 2 实验环境

操作系统：Windows 10，编程语言：C。

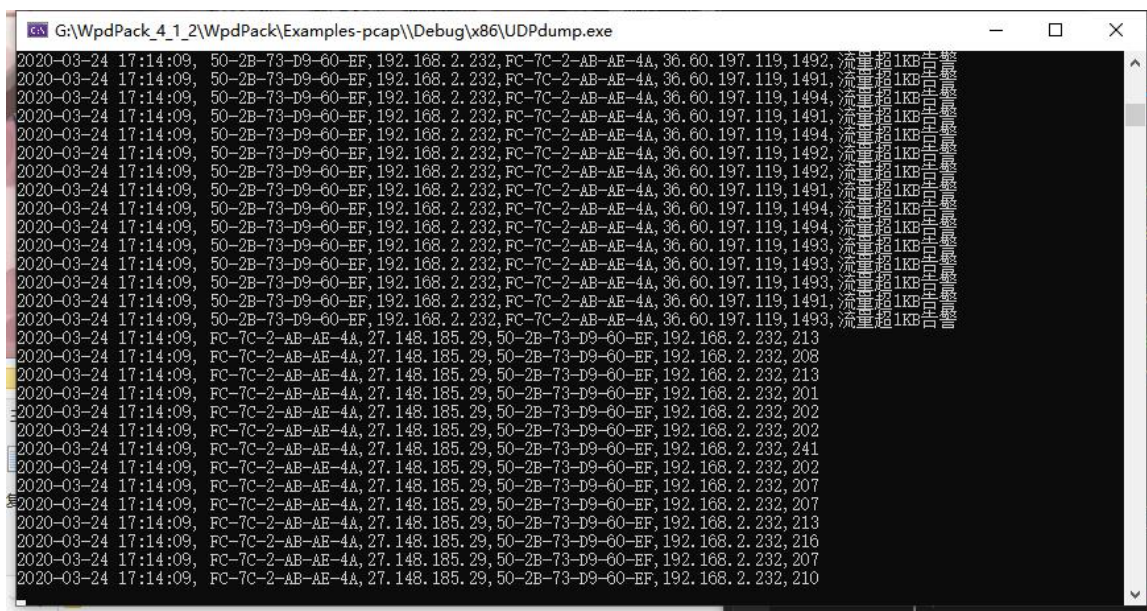
### 3 实验结果



选择网卡界面



接收信息



```
G:\WpdPack_4_1_2\WpdPack\Examples-pcap\Debug\x86\UDPDump.exe
2020-03-24 17:14:09, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 36.60.197.119, 1492, 流量超过1024 警告
2020-03-24 17:14:09, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 36.60.197.119, 1491, 流量超过1024 警告
2020-03-24 17:14:09, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 36.60.197.119, 1494, 流量超过1024 警告
2020-03-24 17:14:09, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 36.60.197.119, 1491, 流量超过1024 警告
2020-03-24 17:14:09, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 36.60.197.119, 1494, 流量超过1024 警告
2020-03-24 17:14:09, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 36.60.197.119, 1492, 流量超过1024 警告
2020-03-24 17:14:09, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 36.60.197.119, 1492, 流量超过1024 警告
2020-03-24 17:14:09, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 36.60.197.119, 1491, 流量超过1024 警告
2020-03-24 17:14:09, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 36.60.197.119, 1491, 流量超过1024 警告
2020-03-24 17:14:09, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 36.60.197.119, 1494, 流量超过1024 警告
2020-03-24 17:14:09, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 36.60.197.119, 1494, 流量超过1024 警告
2020-03-24 17:14:09, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 36.60.197.119, 1493, 流量超过1024 警告
2020-03-24 17:14:09, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 36.60.197.119, 1493, 流量超过1024 警告
2020-03-24 17:14:09, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 36.60.197.119, 1493, 流量超过1024 警告
2020-03-24 17:14:09, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 36.60.197.119, 1491, 流量超过1024 警告
2020-03-24 17:14:09, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 36.60.197.119, 1493, 流量超过1024 警告
2020-03-24 17:14:09, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 213
2020-03-24 17:14:09, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 208
2020-03-24 17:14:09, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 213
2020-03-24 17:14:09, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 201
2020-03-24 17:14:09, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 202
2020-03-24 17:14:09, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 202
2020-03-24 17:14:09, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 241
2020-03-24 17:14:09, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 202
2020-03-24 17:14:09, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 207
2020-03-24 17:14:09, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 207
2020-03-24 17:14:09, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 213
2020-03-24 17:14:09, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 216
2020-03-24 17:14:09, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 207
2020-03-24 17:14:09, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 210
```

对于长度超过 1024 的流量进行告警



G:\WpdPack\_4.1.2\WpdPack\Examples-pcap\Debug\x86\UDPDump.exe

```
2020-03-24 17:24:02, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 215
2020-03-24 17:24:02, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 215, 流量超1KB告警
2020-03-24 17:24:02, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 1129, 流量超1KB告警
2020-03-24 17:24:02, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 860
2020-03-24 17:24:02, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 821
2020-03-24 17:24:02, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 209
2020-03-24 17:24:02, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 213
2020-03-24 17:24:02, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 850
2020-03-24 17:24:02, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 207
2020-03-24 17:24:02, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 216
2020-03-24 17:24:02, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 751
2020-03-24 17:24:02, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 221
2020-03-24 17:24:02, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 388
2020-03-24 17:24:02, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 214
2020-03-24 17:24:02, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 590
2020-03-24 17:24:02, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 226
2020-03-24 17:24:02, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 208
2020-03-24 17:24:02, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 555
2020-03-24 17:24:02, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 216
2020-03-24 17:24:02, FC-7C-2-AB-AE-4A, 27.148.185.29, 50-2B-73-D9-60-EF, 192.168.2.232, 222
```

不同源IP的发送情况:

```
27.148.185.29 发送了长度为: 1797704的数据, 流量超1MB警告
192.168.2.232 发送了长度为: 472632的数据
183.3.254.125 发送了长度为: 172的数据
61.151.163.83 发送了长度为: 172的数据
122.238.121.64 发送了长度为: 10979的数据
59.36.119.111 发送了长度为: 1379的数据
119.84.152.121 发送了长度为: 172的数据
123.151.67.97 发送了长度为: 172的数据
223.166.138.24 发送了长度为: 2383的数据
58.251.121.80 发送了长度为: 86的数据
60.28.190.41 发送了长度为: 172的数据
27.159.72.37 发送了长度为: 654的数据
116.128.128.192 发送了长度为: 172的数据
192.168.2.1 发送了长度为: 22293的数据
183.192.165.167 发送了长度为: 172的数据
120.241.189.198 发送了长度为: 172的数据
195.154.179.2 发送了长度为: 153的数据
111.10.35.206 发送了长度为: 172的数据
113.96.223.57 发送了长度为: 172的数据
61.151.164.218 发送了长度为: 172的数据
113.250.22.47 发送了长度为: 172的数据
123.151.76.123 发送了长度为: 172的数据
185.45.195.166 发送了长度为: 319的数据
183.3.254.56 发送了长度为: 172的数据
123.151.177.69 发送了长度为: 172的数据
113.250.22.95 发送了长度为: 172的数据
61.148.198.222 发送了长度为: 630的数据
195.154.181.225 发送了长度为: 306的数据
203.205.236.30 发送了长度为: 86的数据
```

不同目的IP的接收情况:

```
192.168.2.232 接收了长度为: 1818713的数据, 流量超1MB警告
183.3.254.125 接收了长度为: 172的数据
27.148.185.29 接收了长度为: 33250的数据
61.151.163.83 接收了长度为: 172的数据
122.238.121.64 接收了长度为: 428201的数据
121.51.64.114 接收了长度为: 172的数据
119.84.152.121 接收了长度为: 172的数据
123.151.67.97 接收了长度为: 172的数据
120.131.14.109 接收了长度为: 302的数据
223.166.138.24 接收了长度为: 3600的数据
58.251.121.80 接收了长度为: 172的数据
60.28.190.41 接收了长度为: 172的数据
27.159.72.37 接收了长度为: 881的数据
116.128.128.192 接收了长度为: 172的数据
121.51.40.92 接收了长度为: 172的数据
239.255.255.250 接收了长度为: 21887的数据
183.192.165.167 接收了长度为: 172的数据
111.30.160.145 接收了长度为: 172的数据
120.241.189.198 接收了长度为: 172的数据
195.154.179.2 接收了长度为: 153的数据
59.36.119.111 接收了长度为: 81的数据
111.10.35.206 接收了长度为: 172的数据
113.96.223.57 接收了长度为: 172的数据
61.151.164.218 接收了长度为: 172的数据
113.250.22.47 接收了长度为: 172的数据
123.151.76.123 接收了长度为: 172的数据
185.45.195.166 接收了长度为: 153的数据
192.168.2.1 接收了长度为: 305的数据
183.3.254.56 接收了长度为: 172的数据
123.151.177.69 接收了长度为: 172的数据
113.250.22.95 接收了长度为: 172的数据
61.148.198.222 接收了长度为: 845的数据
195.154.181.225 接收了长度为: 306的数据
203.205.236.30 接收了长度为: 86的数据
```

每 1 分钟输出一次统计情况，将源 IP 发送情况和目的 IP 的接收情况进行汇报，对流量超过 1MB 的发送与接收进行警告。

## 4 实验总结

实际实现了侦听流量和获取 MAC、IP 地址的操作，并在编程中对数据帧格式有了更好的理解，更清晰地了解了帧格式的划分，过程中也积累了很多编程的知识，例如 `u_char` 类型的相关知识、`time.h` 库的使用等。