

# 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 胡曼珑

学    号 24320182203199

实验时间 2020 年 3 月 18 日

2020 年 3 月 24 日

## 1 实验目的

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

win10, c, winCap。

## 3 实验结果

```
1. \Device\NPF_{63F7272E-3643-4776-9CCA-A63729FB31FE} (NdisWan Adapter)
2. \Device\NPF_{9725C0E7-A5BA-434D-A332-D4DC2E00570D} (Microsoft)
3. \Device\NPF_{6A7AF4B9-25B3-456C-AFD8-A99443E0C5AD} (Microsoft)
4. \Device\NPF_{FAE3994E-E7F4-49DC-AC0E-1011293004A0} (Microsoft)
5. \Device\NPF_{15322E3D-0C67-4899-AF88-FEF74A0A0FE1} ( )
6. \Device\NPF_{84795A73-ESB5-44A4-96F9-E6750F6F18E3} (NdisWan Adapter)
7. \Device\NPF_{B111F955-D5D0-42D8-B782-18CEE77D10F5} (NdisWan Adapter)
8. \Device\NPF_{6C0D4180-FFA3-494D-AA8E-2EF34710BFC8} (Microsoft)
9. \Device\NPF_{Loopback (Adapter for loopback traffic capture)}
10. \Device\NPF_{4A26712F-3854-4B7E-87DF-D324277DE15F} (Netease UU TAP-Win32 Adapter V9.21)
11. \Device\NPF_{F946FA65-B17C-4396-91A8-AE923EB4CCD4} (Realtek PCIe GBE Family Controller)
Enter the interface number (1-11):3

listening on Microsoft...
21:00:32.278556 2C-6F-C9-37-0A-57, 192.168.31.202.64372, 50-64-2B-44-D3-F1, 121.14.142.114.8000, 555
21:00:32.286342 50-64-2B-44-D3-F1, 121.14.142.114.8000, 2C-6F-C9-37-0A-57, 192.168.31.202.64372, 185
21:00:32.378120 2C-6F-C9-37-0A-57, 192.168.31.202.64372, 50-64-2B-44-D3-F1, 121.14.142.114.8000, 161
21:00:32.409325 50-64-2B-44-D3-F1, 121.14.142.114.8000, 2C-6F-C9-37-0A-57, 192.168.31.202.64372, 83
21:00:32.410663 2C-6F-C9-37-0A-57, 192.168.31.202.64372, 50-64-2B-44-D3-F1, 121.14.142.114.8000, 192
21:00:33.147463 50-64-2B-44-D3-F1, 59.36.119.88.8000, 2C-6F-C9-37-0A-57, 192.168.31.202.4001, 129
21:00:33.381515 2C-6F-C9-37-0A-57, 192.168.31.202.64372, 50-64-2B-44-D3-F1, 121.14.142.114.8000, 161
21:00:34.280478 2C-6F-C9-37-0A-57, 192.168.31.202.64372, 50-64-2B-44-D3-F1, 121.14.142.114.8000, 555
21:00:34.287755 50-64-2B-44-D3-F1, 121.14.142.114.8000, 2C-6F-C9-37-0A-57, 192.168.31.202.64372, 185
21:00:34.417973 50-64-2B-44-D3-F1, 121.14.142.114.8000, 2C-6F-C9-37-0A-57, 192.168.31.202.64372, 83
21:00:34.418215 2C-6F-C9-37-0A-57, 192.168.31.202.64372, 50-64-2B-44-D3-F1, 121.14.142.114.8000, 192
21:00:36.282968 2C-6F-C9-37-0A-57, 192.168.31.202.64372, 50-64-2B-44-D3-F1, 121.14.142.114.8000, 555
21:00:36.291923 50-64-2B-44-D3-F1, 121.14.142.114.8000, 2C-6F-C9-37-0A-57, 192.168.31.202.64372, 185
21:00:36.421266 50-64-2B-44-D3-F1, 121.14.142.114.8000, 2C-6F-C9-37-0A-57, 192.168.31.202.64372, 83
21:00:36.421605 2C-6F-C9-37-0A-57, 192.168.31.202.64372, 50-64-2B-44-D3-F1, 121.14.142.114.8000, 192
21:00:37.252060 50-64-2B-44-D3-F1, 59.36.119.88.8000, 2C-6F-C9-37-0A-57, 192.168.31.202.4001, 129
```

输出结果

```
source:
58-20-59-75-AA-FD, 192.168.31.74, len=885
50-64-2B-44-D3-F1, 192.168.31.1, len=20244
50-64-2B-44-D3-F1, 59.36.119.88, len=2024
50-64-2B-44-D3-F1, 121.14.142.114, len=7957
2C-6F-C9-37-0A-57, 192.168.31.202, len=28003
dest:
50-64-2B-44-D3-F1, 59.36.119.88, len=81
01-00-5E-7F-FF-FA, 239.255.255.250, len=876
2C-6F-C9-37-0A-57, 239.255.255.250, len=21129
2C-6F-C9-37-0A-57, 192.168.31.202, len=9981
50-64-2B-44-D3-F1, 121.14.142.114, len=27046
```

一分钟以后的统计结果

```
21:25:20.114962 2C-6F-C9-37-0A-57, 192.168.31.202.64372, 50-64-2B-44-D3-F1, 121.14.142.114.8000, 554
超出范围！
```

设阈值为 500 时，超出阈值的输出结果

## 4 实验总结

1、学习了解 winCap（主要在捕获、分析数据包方面）