

# 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 詹世彬

学 号 24320182203321

实验时间 2020 年 3 月 11 日

2020 年 3 月 11 日

## 1 实验目的

利用 winpcap 库监听并分析以太网的帧，记录目标与源 MAC 和 IP 地址，通过实验加深对以太网帧格式的认识。

## 2 实验环境

Windows10 操作系统，Visual studio 2019, C 语言，winpcap

## 3 实验结果

### 1 选择适配器

```
C:\Users\Administrator\Desktop\WpdPack\Examples-pcap\Debug\x86\UDPDump.exe
1. rpcap://Device\NPF_{19F67360-EEA8-4A48-9B90-B5E35ACC33DE} (Network adapter 'Microsoft' on local host)
2. rpcap://Device\NPF_{A36BD0DF-E4B1-45E0-A33C-A27A0B5DA1D5} (Network adapter 'Microsoft' on local host)
3. rpcap://Device\NPF_{50D4FDA0-A1EB-4740-ABDB-27CDC0A902F7} (Network adapter 'Microsoft' on local host)
4. rpcap://Device\NPF_{7710E20A-8804-464A-9A83-04833FE11E58} (Network adapter 'Realtek PCIe GBE Family Controller' on local host)
Enter the interface number (1-4):
```

### 2 对接受到的帧进行分析并输出

输出格式为：

时间，源 MAC，源 IP 源，目标 MAC，目标 IP，帧长度

```
listening on Network adapter 'Microsoft' on local host...
2020-3-18 19:57:20, D0-C7-C0-11-C6-D2, 69. 4. 0. 68, D8-9C-67-3D-6D-1F, 150. 119. 64. 0, 82
2020-3-18 19:57:20, D8-9C-67-3D-6D-1F, 69. 0. 0. 177, D0-C7-C0-11-C6-D2, 125. 211. 0. 0, 191
2020-3-18 19:57:20, D0-C7-C0-11-C6-D2, 69. 4. 0. 68, D8-9C-67-3D-6D-1F, 150. 139. 64. 0, 82
2020-3-18 19:57:20, D8-9C-67-3D-6D-1F, 69. 0. 0. 177, D0-C7-C0-11-C6-D2, 125. 212. 0. 0, 191
2020-3-18 19:57:20, D8-9C-67-3D-6D-1F, 69. 0. 0. 147, D0-C7-C0-11-C6-D2, 125. 213. 0. 0, 161
2020-3-18 19:57:21, D8-9C-67-3D-6D-1F, 69. 0. 2. 30, D0-C7-C0-11-C6-D2, 125. 214. 0. 0, 556
2020-3-18 19:57:21, D0-C7-C0-11-C6-D2, 69. 4. 0. 171, D8-9C-67-3D-6D-1F, 150. 166. 64. 0, 185
2020-3-18 19:57:21, D8-9C-67-3D-6D-1F, 69. 0. 0. 147, D0-C7-C0-11-C6-D2, 125. 215. 0. 0, 161
2020-3-18 19:57:22, D0-C7-C0-11-C6-D2, 69. 4. 0. 68, D8-9C-67-3D-6D-1F, 151. 78. 64. 0, 82
2020-3-18 19:57:22, D8-9C-67-3D-6D-1F, 69. 0. 0. 177, D0-C7-C0-11-C6-D2, 125. 216. 0. 0, 191
2020-3-18 19:57:22, D0-C7-C0-11-C6-D2, 69. 4. 0. 68, D8-9C-67-3D-6D-1F, 151. 82. 64. 0, 82
2020-3-18 19:57:22, D8-9C-67-3D-6D-1F, 69. 0. 0. 177, D0-C7-C0-11-C6-D2, 125. 217. 0. 0, 191
2020-3-18 19:57:22, D8-9C-67-3D-6D-1F, 69. 0. 0. 147, D0-C7-C0-11-C6-D2, 125. 218. 0. 0, 161
2020-3-18 19:57:23, D8-9C-67-3D-6D-1F, 69. 0. 2. 30, D0-C7-C0-11-C6-D2, 125. 219. 0. 0, 556
2020-3-18 19:57:23, D0-C7-C0-11-C6-D2, 69. 4. 0. 171, D8-9C-67-3D-6D-1F, 151. 129. 64. 0, 185
2020-3-18 19:57:23, D8-9C-67-3D-6D-1F, 69. 0. 0. 147, D0-C7-C0-11-C6-D2, 125. 220. 0. 0, 161
```

### 3

将结果输出到指定文件夹

record.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
2020-3-19 15:49:56,D8-9C-67-3D-6D-1F,69.0.0.78,FF-FF-FF-FF-FF-FF,254.54.0.0,92
2020-3-19 15:49:57,D8-9C-67-3D-6D-1F,69.0.0.78,FF-FF-FF-FF-FF-FF,254.55.0.0,92
2020-3-19 15:49:58,D8-9C-67-3D-6D-1F,69.0.0.137,D0-C7-C0-11-C6-D2,167.223.0.0,151
2020-3-19 15:49:59,D8-9C-67-3D-6D-1F,69.0.1.22,D0-C7-C0-11-C6-D2,157.229.0.0,292
2020-3-19 15:50:00,D0-C7-C0-11-C6-D2,69.4.0.115,D8-9C-67-3D-6D-1F,83.225.64.0,129
2020-3-19 15:50:07,D0-C7-C0-11-C6-D2,69.4.0.123,D8-9C-67-3D-6D-1F,87.220.64.0,137
2020-3-19 15:50:07,D8-9C-67-3D-6D-1F,69.0.0.83,D0-C7-C0-11-C6-D2,242.67.0.0,97
2020-3-19 15:50:08,D0-C7-C0-11-C6-D2,69.4.0.115,D8-9C-67-3D-6D-1F,88.76.64.0,129
2020-3-19 15:50:11,D0-C7-C0-11-C6-D2,69.4.0.115,D8-9C-67-3D-6D-1F,89.227.64.0,129
2020-3-19 15:50:11,D0-C7-C0-11-C6-D2,69.4.0.115,D8-9C-67-3D-6D-1F,90.76.64.0,129
2020-3-19 15:50:13,D0-C7-C0-11-C6-D2,69.4.0.115,D8-9C-67-3D-6D-1F,90.222.64.0,129
2020-3-19 15:50:16,D0-C7-C0-11-C6-D2,69.4.0.115,D8-9C-67-3D-6D-1F,92.231.64.0,129
2020-3-19 15:50:17,D0-C7-C0-11-C6-D2,69.4.0.115,D8-9C-67-3D-6D-1F,93.78.64.0,129
2020-3-19 15:50:23,D0-C7-C0-11-C6-D2,69.4.0.115,D8-9C-67-3D-6D-1F,96.175.64.0,129
2020-3-19 15:50:30,D8-9C-67-3D-6D-1F,69.0.0.202,01-00-5E-7F-FF-FA,255.35.0.0,216
2020-3-19 15:50:31,D8-9C-67-3D-6D-1F,69.0.0.202,01-00-5E-7F-FF-FA,255.36.0.0,216
2020-3-19 15:50:31,D0-C7-C0-11-C6-D2,69.4.0.115,D8-9C-67-3D-6D-1F,101.25.64.0,129
2020-3-19 15:50:32,D8-9C-67-3D-6D-1F,69.0.0.202,01-00-5E-7F-FF-FA,255.37.0.0,216
2020-3-19 15:50:33,D0-C7-C0-11-C6-D2,69.4.0.115,D8-9C-67-3D-6D-1F,101.183.64.0,129
2020-3-19 15:50:33,D8-9C-67-3D-6D-1F,69.0.0.202,01-00-5E-7F-FF-FA,255.38.0.0,216
2020-3-19 15:50:33,D0-C7-C0-11-C6-D2,69.4.0.115,D8-9C-67-3D-6D-1F,102.23.64.0,129
2020-3-19 15:50:33,D0-C7-C0-11-C6-D2,69.4.0.115,D8-9C-67-3D-6D-1F,102.26.64.0,129
2020-3-19 15:50:35,D0-C7-C0-11-C6-D2,69.4.0.115,D8-9C-67-3D-6D-1F,102.236.64.0,129
2020-3-19 15:50:35,D0-C7-C0-11-C6-D2,69.4.0.115,D8-9C-67-3D-6D-1F,103.55.64.0,129
2020-3-19 15:50:37,D0-C7-C0-11-C6-D2,69.4.0.115,D8-9C-67-3D-6D-1F,104.76.64.0,129
2020-3-19 15:50:38,D8-9C-67-3D-6D-1F,69.0.0.137,D0-C7-C0-11-C6-D2,167.224.0.0,151
2020-3-19 15:50:39,D0-C7-C0-11-C6-D2,69.4.0.115,D8-9C-67-3D-6D-1F,105.40.64.0,129
2020-3-19 15:50:42,D0-C7-C0-11-C6-D2,69.4.0.115,D8-9C-67-3D-6D-1F,106.200.64.0,129
2020-3-19 15:50:45,D8-9C-67-3D-6D-1F,69.0.0.67,D0-C7-C0-11-C6-D2,242.68.0.0,81
2020-3-19 15:50:45,D0-C7-C0-11-C6-D2,69.4.0.75,D8-9C-67-3D-6D-1F,108.123.64.0,89
2020-3-19 15:50:45,D0-C7-C0-11-C6-D2,69.4.0.115,D8-9C-67-3D-6D-1F,108.233.64.0,129
```

4

统计一分钟内收到的数据量并将结果输出

Microsoft Visual Studio 调试控制台

```
2020-3-19 15:32:43, D8-9C-67-3D-6D-1F, 69. 0. 0. 67, D0-C7-C0-11-C6-D2, 241. 191. 0. 0, 81
2020-3-19 15:32:43, D0-C7-C0-11-C6-D2, 69. 4. 0. 75, D8-9C-67-3D-6D-1F, 19. 131. 64. 0, 89
2020-3-19 15:32:45, D0-C7-C0-11-C6-D2, 69. 4. 1. 67, D8-9C-67-3D-6D-1F, 20. 125. 64. 0, 337
2020-3-19 15:32:45, D8-9C-67-3D-6D-1F, 69. 0. 0. 83, D0-C7-C0-11-C6-D2, 241. 192. 0. 0, 97
2020-3-19 15:32:51, D0-C7-C0-11-C6-D2, 69. 4. 1. 83, D8-9C-67-3D-6D-1F, 23. 195. 64. 0, 353
2020-3-19 15:32:51, D8-9C-67-3D-6D-1F, 69. 0. 0. 83, D0-C7-C0-11-C6-D2, 241. 193. 0. 0, 97
2020-3-19 15:32:52, D0-C7-C0-11-C6-D2, 69. 4. 0. 115, D8-9C-67-3D-6D-1F, 24. 123. 64. 0, 129
2020-3-19 15:32:55, D0-C7-C0-11-C6-D2, 69. 4. 0. 115, D8-9C-67-3D-6D-1F, 25. 214. 64. 0, 129
2020-3-19 15:32:55, D0-C7-C0-11-C6-D2, 69. 4. 0. 115, D8-9C-67-3D-6D-1F, 25. 253. 64. 0, 129
2020-3-19 15:32:58, D0-C7-C0-11-C6-D2, 69. 4. 0. 115, D8-9C-67-3D-6D-1F, 27. 91. 64. 0, 129
2020-3-19 15:32:58, D0-C7-C0-11-C6-D2, 69. 4. 1. 91, D8-9C-67-3D-6D-1F, 27. 102. 64. 0, 361
2020-3-19 15:32:58, D8-9C-67-3D-6D-1F, 69. 0. 0. 83, D0-C7-C0-11-C6-D2, 241. 194. 0. 0, 97
2020-3-19 15:33:01, D0-C7-C0-11-C6-D2, 69. 4. 0. 115, D8-9C-67-3D-6D-1F, 28. 191. 64. 0, 129
2020-3-19 15:33:16, D0-C7-C0-11-C6-D2, 69. 4. 0. 115, D8-9C-67-3D-6D-1F, 37. 51. 64. 0, 129
2020-3-19 15:33:18, D8-9C-67-3D-6D-1F, 69. 0. 0. 137, D0-C7-C0-11-C6-D2, 167. 198. 0. 0, 151
2020-3-19 15:33:22, D0-C7-C0-11-C6-D2, 69. 4. 0. 115, D8-9C-67-3D-6D-1F, 40. 122. 64. 0, 129
```

一分钟内接收到的数据量为：10783



## 4 实验总结

基本了解 winpcap 的一些库及其使用方法，加深了对以太网帧格式的认识，在实验的过程中通过阅读提供的代码，提高了代码阅读能力，并且在实验的过程中通过不断完善代码更好地掌握了 visual studio 的调试方式，提高自身的代码水平。