

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 3 用 PCAP 库监听并分析网络流量

班 级 软件工程 2018 级 1 班

姓 名 王奕飞

学 号 24320182203286

实验时间 2020 年 3 月 11 日

2020 年 3 月 13 日

1 实验目的

2 实验环境

Visual studio 2017, C#, 以及 VSPD 虚拟端口设置软件

3 实验结果

```
C:\Users\99534\source\repos\Project2\x64\Debug\Project2.exe
1. \Device\NPF_{6FF1E734-015B-4F7F-8386-910AF69CE74B} (Microsoft)
2. \Device\NPF_{8CA33F2A-8F1D-41DA-9BFC-B7D73BD27493} (Microsoft)
3. \Device\NPF_{4853CCEC-FC97-4E6B-BF9F-2DFEB4FAD1C3} (Microsoft)
4. \Device\NPF_{C83149AE-5369-4702-81AF-3BD659B2909C} (Realtek PCIe GbE Family Controller)
Enter the interface number(1-4) 3
```

开始界面，选择适配器

```
C:\Users\99534\source\repos\Project2\x64\Debug\Project2.exe
1. \Device\NPF_{6FF1E734-015B-4F7F-8386-910AF69CE74B} (Microsoft)
2. \Device\NPF_{8CA33F2A-8F1D-41DA-9BFC-B7D73BD27493} (Microsoft)
3. \Device\NPF_{4853CCEC-FC97-4E6B-BF9F-2DFEB4FAD1C3} (Microsoft)
4. \Device\NPF_{C83149AE-5369-4702-81AF-3BD659B2909C} (Realtek PCIe GbE Family Controller)
Enter the interface number(1-4) 3
2020-3-13 17:13:29, 58-00-e3-34-60-09, 192.168.68.159, 01-00-5e-7f-ff-fa, 239.255.255.250, 323
2020-3-13 17:13:29, 58-00-e3-34-60-09, 192.168.68.159, 01-00-5e-7f-ff-fa, 239.255.255.250, 332
2020-3-13 17:13:29, 58-00-e3-34-60-09, 192.168.68.159, 01-00-5e-7f-ff-fa, 239.255.255.250, 379
2020-3-13 17:13:29, 58-00-e3-34-60-09, 192.168.68.159, 01-00-5e-7f-ff-fa, 239.255.255.250, 387
2020-3-13 17:13:30, 58-00-e3-34-60-09, 192.168.68.159, 01-00-5e-7f-ff-fa, 239.255.255.250, 389
2020-3-13 17:13:30, 58-00-e3-34-60-09, 192.168.68.159, 01-00-5e-7f-ff-fa, 239.255.255.250, 377
2020-3-13 17:13:30, 50-5b-c2-cd-3d-0d, 192.168.68.165, 54-a3-1b-31-00-e4, 61.241.37.152, 86
2020-3-13 17:13:30, 50-5b-c2-cd-3d-0d, 192.168.68.165, 54-a3-1b-31-00-e4, 220.194.108.56, 124
2020-3-13 17:13:30, 54-a3-1b-31-00-e4, 61.241.37.152, 50-5b-c2-cd-3d-0d, 192.168.68.165, 86
2020-3-13 17:13:30, 54-a3-1b-31-00-e4, 220.194.108.56, 50-5b-c2-cd-3d-0d, 192.168.68.165, 300
2020-3-13 17:13:30, 50-5b-c2-cd-3d-0d, 192.168.68.165, 01-00-5e-7f-ff-fa, 239.255.255.250, 216
2020-3-13 17:13:30, 50-5b-c2-cd-3d-0d, 192.168.68.165, 54-a3-1b-31-00-e4, 220.194.108.56, 54
2020-3-13 17:13:30, 58-00-e3-34-60-09, 192.168.68.159, ff-ff-ff-ff-ff-ff, 192.168.68.255, 1292
2020-3-13 17:13:30, 58-00-e3-34-60-09, 192.168.68.159, 01-00-5e-00-00-fb, 224.0.0.251, 1292
```

对接受到的帧进行分析并输出

同时输出到文本

```
2020-3-13 17:21:32, 50-5b-c2-cd-3d-0d, 192. 168. 68. 165, 54-a3
2020-3-13 17:21:32, 54-a3-1b-31-00-e4, 220. 194. 108. 56, 50-5b
2020-3-13 17:21:32, 50-5b-c2-cd-3d-0d, 192. 168. 68. 165, 54-a3
第1分钟
收到总数据量为: 12142
收到的多播数据量为: 0
收到的广播数据量为: 5566
发送数据量为: 17350
2020-3-13 17:21:32, 50-5b-c2-cd-3d-0d, 192. 168. 68. 165, 01-00
2020-3-13 17:21:33, 50-5b-c2-cd-3d-0d, 192. 168. 68. 165, 54-a3
2020-3-13 17:21:33, 58-00-c2-34-60-00, 192. 168. 68. 150, 01-00
```

record.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

第1分钟

收到总数据量为: 12142

收到的多播数据量为: 0

收到的广播数据量为: 5566

发送数据量为: 17350

2

```
物理地址: 58-00-e3-34-60-09,发送到此地址: 0 从此地址接受: 15  
物理地址: 33-33-ff-ed-d2-c5,发送到此地址: 86 从此地址接受: 0  
物理地址: 54-a3-1b-31-00-e4,发送到此地址: 275 从此地址接受:  
物理地址: 01-00-5e-7f-ff-fa,发送到此地址: 46 从此地址接受: 0 此
```

对不同物理地址进行统计

址接受: 15362 此地址的流量未达到阈值

址接受: 0 此地址的流量未达到阈值

址接受: 459 此地址的流量未达到阈值

址接受: 0 此地址的流量未达到阈值

检测是否超过阈值

4 实验总结

基本了解 winpcap 的一些函数及其作用, 对于以太网帧格式有了一个更深刻的认识, 对于 mac 地址和 ip 地址以及子网掩码等知识有了一个更加明显的理解。难点是获取本机的 MAC 地址, 因此查询了 winpcap 的帮助文档, 发现有对于获取 mac 地址的描述, 进行学习