厦門大學

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 3 班

姓　　名 饶龙宇

学　　号 24320182203256

实验时间 2020 年 3 月 22 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）

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

编程环境：Windows10 Visual Studio 2019

编程语言：C++

3 实验结果

```
1.  \Device\NPF_{4D45C982-404C-46C1-9C92-0161BF53A91C}  (Realtek PCIe GBE Family Controller)
2.  \Device\NPF_{5F9EDE4B-D81D-4BA2-8B7E-15E8EF78A660}  (Microsoft)
3.  \Device\NPF_{11D61CF6-92DA-46D8-9415-1C6D1C3E4D5C}  (Oracle)
4.  \Device\NPF_{12C3FE26-6E7A-4EE5-9F3B-8D152F18D536}  (VMware Virtual Ethernet Adapter)
5.  \Device\NPF_{18D48D7D-F630-4E23-AF50-E01BD0D158F5}  (TAP-Windows Adapter V9)
6.  \Device\NPF_{A58A2AAF-78AB-4A79-8D5B-B341659D31B6}  (Microsoft)
7.  \Device\NPF_{C101CE9A-D941-4D32-8E53-6A352C463710}  (VMware Virtual Ethernet Adapter)
8.  \Device\NPF_{9723E580-9B1A-4AE6-8364-836A8C41B86E}  (Microsoft)
Enter the interface number (1-8):8

listening on Microsoft...
Warning:Traffic over 1 MB!
```

1.流量超过给定阈值(1MB)告警

	A	B	C	D	E	F	G
1	date	time	srcMAC	srcIP	destMAC	destIP	len
2	2020/3/22	16:46:00	50-BD-5F-62-D5-EE	120-232-195-217	74-70-FD-37-EF-C4	192-168-0-108	105
3	2020/3/22	16:46:00	50-BD-5F-62-D5-EE	120-232-195-217	74-70-FD-37-EF-C4	192-168-0-108	124
4	2020/3/22	16:46:00	50-BD-5F-62-D5-EE	120-232-195-217	74-70-FD-37-EF-C4	192-168-0-108	1166
5	2020/3/22	16:46:00	50-BD-5F-62-D5-EE	120-232-195-217	74-70-FD-37-EF-C4	192-168-0-108	161
6	2020/3/22	16:46:00	50-BD-5F-62-D5-EE	120-232-195-217	74-70-FD-37-EF-C4	192-168-0-108	118
7	2020/3/22	16:46:00	50-BD-5F-62-D5-EE	120-232-195-217	74-70-FD-37-EF-C4	192-168-0-108	1166
8	2020/3/22	16:46:00	50-BD-5F-62-D5-EE	120-232-195-217	74-70-FD-37-EF-C4	192-168-0-108	109
9	2020/3/22	16:46:00	50-BD-5F-62-D5-EE	120-232-195-217	74-70-FD-37-EF-C4	192-168-0-108	116
10	2020/3/22	16:46:00	50-BD-5F-62-D5-EE	120-232-195-217	74-70-FD-37-EF-C4	192-168-0-108	1166
11	2020/3/22	16:46:00	50-BD-5F-62-D5-EE	120-232-195-217	74-70-FD-37-EF-C4	192-168-0-108	105
12	2020/3/22	16:46:00	50-BD-5F-62-D5-EE	120-232-195-217	74-70-FD-37-EF-C4	192-168-0-108	187
13	2020/3/22	16:46:00	50-BD-5F-62-D5-EE	120-232-195-217	74-70-FD-37-EF-C4	192-168-0-108	1166
14	2020/3/22	16:46:00	50-BD-5F-62-D5-EE	120-232-195-217	74-70-FD-37-EF-C4	192-168-0-108	105
15	2020/3/22	16:46:00	50-BD-5F-62-D5-EE	120-232-195-217	74-70-FD-37-EF-C4	192-168-0-108	115
16	2020/3/22	16:46:00	50-BD-5F-62-D5-EE	120-232-195-217	74-70-FD-37-EF-C4	192-168-0-108	1166
17	2020/3/22	16:46:00	50-BD-5F-62-D5-EE	120-232-195-217	74-70-FD-37-EF-C4	192-168-0-108	117
18	2020/3/22	16:46:00	50-BD-5F-62-D5-EE	120-232-195-217	74-70-FD-37-EF-C4	192-168-0-108	165
19	2020/3/22	16:46:00	50-BD-5F-62-D5-EE	120-232-195-217	74-70-FD-37-EF-C4	192-168-0-108	1166
20	2020/3/22	16:46:00	50-BD-5F-62-D5-EE	120-232-195-217	74-70-FD-37-EF-C4	192-168-0-108	116
21	2020/3/22	16:46:00	50-BD-5F-62-D5-EE	120-232-195-217	74-70-FD-37-EF-C4	192-168-0-108	105
22	2020/3/22	16:46:00	50-BD-5F-62-D5-EE	120-232-195-217	74-70-FD-37-EF-C4	192-168-0-108	1166
23	2020/3/22	16:46:00	50-BD-5F-62-D5-EE	120-232-195-217	74-70-FD-37-EF-C4	192-168-0-108	182

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，形成 CSV 格式的日志。

	A	B	C
1	srcLog		
2			
3	5 seconds		
4	MACaddress	IPaddress	Len
5	50-BD-5F-62-D5-EE	120-232-195-217	96966
6	74-70-FD-37-EF-C4	192-168-0-108	1747
7			
8	5 seconds		
9	MACaddress	IPaddress	Len
10	50-BD-5F-62-D5-EE	120-232-195-217	204892
11	74-70-FD-37-EF-C4	192-168-0-108	2403
12			
13	5 seconds		
14	MACaddress	IPaddress	Len
15	50-BD-5F-62-D5-EE	120-232-195-217	248272
16	74-70-FD-37-EF-C4	192-168-0-108	1768
17	50-BD-5F-62-D5-EE	183-232-93-26	291
18			
19	5 seconds		
20	MACaddress	IPaddress	Len
21	50-BD-5F-62-D5-EE	120-232-195-217	220883
22	74-70-FD-37-EF-C4	192-168-0-108	2572
23	50-BD-5F-62-D5-EE	183-232-93-26	258

每隔一段时间（5 秒），程序统计来自不同 MAC 和 IP 地址的通信数据长度

	A	B	C
1	destLog		
2			
3	5 seconds		
4	MACaddress	IPaddress	Len
5	74-70-FD-37-EF-C4	192-168-0-108	96966
6	50-BD-5F-62-D5-EE	120-232-195-217	1747
7			
8	5 seconds		
9	MACaddress	IPaddress	Len
10	74-70-FD-37-EF-C4	192-168-0-108	204892
11	50-BD-5F-62-D5-EE	120-232-195-217	2403
12			
13	5 seconds		
14	MACaddress	IPaddress	Len
15	74-70-FD-37-EF-C4	192-168-0-108	248563
16	50-BD-5F-62-D5-EE	120-232-195-217	1566
17	50-BD-5F-62-D5-EE	183-232-93-26	202
18			
19	5 seconds		
20	MACaddress	IPaddress	Len
21	74-70-FD-37-EF-C4	192-168-0-108	221141
22	50-BD-5F-62-D5-EE	120-232-195-217	2572
23			
24	5 seconds		
25	MACaddress	IPaddress	Len
26	74-70-FD-37-EF-C4	192-168-0-108	219474
27	50-BD-5F-62-D5-EE	120-232-195-217	1562

每隔一段时间（5 秒），程序统计发至不同 MAC 和 IP 地址的通信数据长度

4 实验总结

通过本次实验，我初步掌握了 winPcap 库的使用。在观看黄老师精心讲解的视频后，对于编程中遇到的问题，我能更准确地寻求搜索引擎的帮助，这个宝贵经验不仅作用于本次实验，还会对我往后的学习生活产生正向影响，让我认识到我需要努力掌握的其实是学习方法。