

# 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 刘菲艳

学    号 24320182203234

实验时间 2020 年 3 月 24 日

2020 年 3 月 24 日

## 1 实验目的

侦听并分析以太网的帧，记录目标与源 MAC 和 IP 地址。

## 2 实验环境

操作系统：Windows

编程语言：C++

## 3 实验结果

1. 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：

1	date	time	srcMAC	srcIP	destMAC	destIP	len
2	2020/3/24	19:30:16	00-CF-C0-18-1D-EA	183-232-93-29	18-1D-EA-192-168-1-3	192-168-1-3	121
3	2020/3/24	19:30:16	00-CF-C0-18-1D-EA	183-232-93-29	18-1D-EA-192-168-1-3	192-168-1-3	97
4	2020/3/24	19:30:16	18-1D-EA-192-168-100-CF-C0	183-232-93-29	00-CF-C0-18-1D-EA	192-168-1-3	97
5	2020/3/24	19:30:16	00-CF-C0-18-1D-EA	183-232-93-29	18-1D-EA-192-168-100-CF-C0	183-232-93-29	185
6	2020/3/24	19:30:16	18-1D-EA-192-168-100-CF-C0	183-232-93-29	00-CF-C0-18-1D-EA	192-168-100-CF-C0	97
7	2020/3/24	19:30:17	AC-35-EE-192-168-101-00-5E	239-255-255-250	AC-35-EE-192-168-101-00-5E	239-255-255-250	345
8	2020/3/24	19:30:17	AC-35-EE-192-168-101-00-5E	239-255-255-250	AC-35-EE-192-168-101-00-5E	239-255-255-250	354
9	2020/3/24	19:30:17	AC-35-EE-192-168-101-00-5E	239-255-255-250	AC-35-EE-192-168-101-00-5E	239-255-255-250	401
10	2020/3/24	19:30:17	AC-35-EE-192-168-101-00-5E	239-255-255-250	AC-35-EE-192-168-101-00-5E	239-255-255-250	399
11	2020/3/24	19:30:17	AC-35-EE-192-168-101-00-5E	239-255-255-250	AC-35-EE-192-168-101-00-5E	239-255-255-250	411
12	2020/3/24	19:30:17	AC-35-EE-192-168-101-00-5E	239-255-255-250	AC-35-EE-192-168-101-00-5E	239-255-255-250	409
13	2020/3/24	19:30:17	AC-35-EE-192-168-101-00-5E	239-255-255-250	AC-35-EE-192-168-101-00-5E	239-255-255-250	379
14	2020/3/24	19:30:17	AC-35-EE-192-168-101-00-5E	239-255-255-250	AC-35-EE-192-168-101-00-5E	239-255-255-250	345
15	2020/3/24	19:30:17	AC-35-EE-192-168-101-00-5E	239-255-255-250	AC-35-EE-192-168-101-00-5E	239-255-255-250	354
16	2020/3/24	19:30:17	AC-35-EE-192-168-101-00-5E	239-255-255-250	AC-35-EE-192-168-101-00-5E	239-255-255-250	401
17	2020/3/24	19:30:17	AC-35-EE-192-168-101-00-5E	239-255-255-250	AC-35-EE-192-168-101-00-5E	239-255-255-250	399
18	2020/3/24	19:30:17	AC-35-EE-192-168-101-00-5E	239-255-255-250	AC-35-EE-192-168-101-00-5E	239-255-255-250	411
19	2020/3/24	19:30:17	AC-35-EE-192-168-101-00-5E	239-255-255-250	AC-35-EE-192-168-101-00-5E	239-255-255-250	409
20	2020/3/24	19:30:17	AC-35-EE-192-168-101-00-5E	239-255-255-250	AC-35-EE-192-168-101-00-5E	239-255-255-250	379
21	2020/3/24	19:30:17	00-CF-C0-18-1D-EA	183-232-93-29	18-1D-EA-192-168-1-3	192-168-1-3	185
22	2020/3/24	19:30:17	00-CF-C0-18-1D-EA	183-232-93-29	18-1D-EA-192-168-1-3	192-168-1-3	97
23	2020/3/24	19:30:17	18-1D-EA-192-168-100-CF-C0	183-232-93-29	00-CF-C0-18-1D-EA	192-168-100-CF-C0	97
24	2020/3/24	19:30:17	18-1D-EA-192-168-100-CF-C0	183-232-93-29	00-CF-C0-18-1D-EA	192-168-100-CF-C0	97

## 2. 每隔 10 秒钟，程序统计来自不同 MAC 和 IP 地址的通信数据长度

srcLog			
10 seconds			
MACaddress	IPaddress	Len	
0-CF-C0-19-FD-F8	183-232-93-29	1965	
18-1D-EA-D7-1A-E	192-168-1-3	1461	
AC-35-EE-89-ED-5	192-168-1-14	21500	
0-CF-C0-19-FD-F8	192-168-1-1	266	
10 seconds			
MACaddress	IPaddress	Len	
18-1D-EA-D7-1A-E	192-168-1-3	1055	
0-CF-C0-19-FD-F8	192-168-1-1	705	
AC-35-EE-89-ED-5	192-168-1-14	21656	
0-CF-C0-19-FD-F8	183-232-93-29	308	
A0-4E-A7-4-63-BD	192-168-1-8	154	
10 seconds			
MACaddress	IPaddress	Len	
AC-35-EE-89-ED-5	192-168-1-14	29535	
18-1D-EA-D7-1A-E	192-168-1-3	2459	
0-CF-C0-19-FD-F8	192-168-1-1	1217	
0-CF-C0-19-FD-F8	183-232-93-29	3299	
2C-6E-85-A0-7A-1C	192-168-1-12	47	
10 seconds			
MACaddress	IPaddress	Len	
0-CF-C0-19-FD-F8	183-232-93-29	3229	
18-1D-EA-D7-1A-E	192-168-1-3	4830	
0-CF-C0-19-FD-F8	192-168-1-1	659	
AC-35-EE-89-ED-5	192-168-1-14	22828	

## 3. 统计发至不同 MAC 和 IP 地址的通信数据长度。

destLog		
10 seconds		
MACAddress	IPaddress	Len
0-CF-C0-19-FD-F8	183-232-93-29	956
1-0-5E-7F-FF-FA	239-255-255-250	16533
18-1D-EA-D7-1A-E	192-168-1-3	1486
18-1D-EA-D7-1A-E	224-0-0-251	3984
FF-FF-FF-FF-FF-FF	192-168-1-255	3984
FF-FF-FF-FF-FF-FF	255-255-255-255	47
10 seconds		
MACAddress	IPaddress	Len
1-0-5E-7F-FF-FA	239-255-255-250	17367
18-1D-EA-D7-1A-E	192-168-1-3	121
18-1D-EA-D7-1A-E	224-0-0-251	2656
FF-FF-FF-FF-FF-FF	192-168-1-255	2656
0-CF-C0-19-FD-F8	192-168-1-1	110
10 seconds		
MACAddress	IPaddress	Len
18-1D-EA-D7-1A-E	224-0-0-251	3494
FF-FF-FF-FF-FF-FF	192-168-1-255	3984
0-CF-C0-19-FD-F8	192-168-1-1	3318
18-1D-EA-D7-1A-E	192-168-1-3	10900
1-0-5E-7F-FF-FA	239-255-255-250	16188
0-CF-C0-19-FD-F8	221-181-72-119	2240
0-CF-C0-19-FD-F8	183-232-93-29	558

## 4 实验总结

通过使用 winpcap, wireshark 等, 对以太网的帧有了更深刻的了解。