

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 刘明成

学 号 24320182203236

实验时间 2020 年 3 月 21 日

2020 年 3 月 24 日

1 实验目的

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。

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)

2015-03-14 13:05:16,60-36-DD-7D-D5-21,192.168.33.1,60-36-DD-7D-D5-72,192.168.33.2,1536

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。(未能完成)

2 实验环境

实验机: Windows10 x64 位

软件: Visual Studio 2019 (WinPCAP 库)

编程语言: C

3 实验结果

```
G:\Study\WinPCAP\WpdPack\Examples-pcap\Debug\x86\UDPDump.exe
1. \Device\NPF_{0E231877-E7C4-454B-91EC-02CD442DAF1C} (VMware Virtual Ethernet Adapter)
2. \Device\NPF_{E6C75C11-2BF2-4A3D-84F2-93165E461223} (Microsoft)
3. \Device\NPF_{E7A86BD9-611F-4C74-8A86-DF5B9305AFB5} (Microsoft)
4. \Device\NPF_{9CD4E6A5-3CC8-472E-B49D-6C97A7CAA64E} (VMware Virtual Ethernet Adapter)
5. \Device\NPF_{D68AEA2E-B885-400F-826F-E97D2D98A707} (Netease UU TAP-Win32 Adapter V9.21)
6. \Device\NPF_{90631479-F21D-475B-AEAB-A12D86C4B8C2} (Realtek Ethernet Controller)
Enter the interface number (1-6):6

listening on Realtek Ethernet Controller...
2020/03/24 21:12:24, 111.30.159.66, 4c ed fb 2b 7e 87 , 192.168.1.62, 70 89 cc e2 2c bc , 129
2020/03/24 21:12:24, 192.168.1.164, ff ff ff ff ff ff , 192.168.1.255, 60 d2 1c 49 70 2c , 158
2020/03/24 21:12:27, 192.168.1.62, 70 89 cc e2 2c bc , 203.208.40.40, 4c ed fb 2b 7e 87 , 1392, 流量超过阈值!
2020/03/24 21:12:27, 203.208.40.40, 4c ed fb 2b 7e 87 , 192.168.1.62, 70 89 cc e2 2c bc , 1392, 流量超过阈值!
2020/03/24 21:12:27, 192.168.1.62, 70 89 cc e2 2c bc , 203.208.40.40, 4c ed fb 2b 7e 87 , 81
2020/03/24 21:12:27, 192.168.1.62, 70 89 cc e2 2c bc , 203.208.40.40, 4c ed fb 2b 7e 87 , 70
2020/03/24 21:12:28, 203.208.40.40, 4c ed fb 2b 7e 87 , 192.168.1.62, 70 89 cc e2 2c bc , 70
2020/03/24 21:12:28, 192.168.1.62, 70 89 cc e2 2c bc , 203.208.40.40, 4c ed fb 2b 7e 87 , 766, 流量超过阈值!
2020/03/24 21:12:28, 192.168.1.62, 70 89 cc e2 2c bc , 192.168.1.1, 4c ed fb 2b 7e 87 , 85
2020/03/24 21:12:28, 192.168.1.62, 70 89 cc e2 2c bc , 192.168.1.1, 4c ed fb 2b 7e 87 , 85
2020/03/24 21:12:28, 192.168.1.62, 70 89 cc e2 2c bc , 192.168.1.1, 4c ed fb 2b 7e 87 , 79
2020/03/24 21:12:28, 192.168.1.62, 70 89 cc e2 2c bc , 192.168.1.1, 4c ed fb 2b 7e 87 , 79
2020/03/24 21:12:28, 192.168.1.62, 70 89 cc e2 2c bc , 192.168.1.1, 4c ed fb 2b 7e 87 , 78
2020/03/24 21:12:28, 192.168.1.62, 70 89 cc e2 2c bc , 192.168.1.1, 4c ed fb 2b 7e 87 , 78
2020/03/24 21:12:28, 203.208.40.40, 4c ed fb 2b 7e 87 , 192.168.1.62, 70 89 cc e2 2c bc , 445
2020/03/24 21:12:28, 192.168.1.62, 70 89 cc e2 2c bc , 203.208.40.40, 4c ed fb 2b 7e 87 , 70
2020/03/24 21:12:28, 192.168.1.62, 70 89 cc e2 2c bc , 192.168.1.1, 4c ed fb 2b 7e 87 , 77
2020/03/24 21:12:28, 192.168.1.62, 70 89 cc e2 2c bc , 192.168.1.1, 4c ed fb 2b 7e 87 , 77
2020/03/24 21:12:28, 192.168.1.1, 4c ed fb 2b 7e 87 , 192.168.1.62, 70 89 cc e2 2c bc , 85
2020/03/24 21:12:28, 192.168.1.1, 4c ed fb 2b 7e 87 , 192.168.1.62, 70 89 cc e2 2c bc , 101
```

4 实验总结

学会了如何使用 WinPCAP 库侦听并分析网络上数据流的 IP 地址以及 MAC 地址等，了解了一些有关 Wireshark 以及 Omnipcap 等软件的知识。