信息学院软件工程系

《计算机网络》实验报告

题　　目 实验三 基于 PCAP 库侦听并分析网络流量

班　　级 软件工程 2019 级 3 班

姓　　名 王伟龙

学　　号 22920192204287

实验时间 2021 年 3 月 31 日

1、 实验目的

通过完成实验，理解数据链路层、网络层、传输层和应用层的基本原理。掌握用 Wireshark 观察网络流量并辅助网络侦听相关的编程；掌握用 Libpcap 或 WinPcap 库侦听并处理以太网帧和 IP 报文的方法；熟悉以太网帧、IP 报文、TCP 段和 FTP 命令的格式概念，掌握 TCP 协议的基本机制；熟悉帧头部或 IP 报文头部各字段的含义。熟悉 TCP 段和 FTP 数据协议的概念，熟悉段头部各字段和 FTP 控制命令的指令和数据的含义

1 实验环境

Windows10

2 实验结果

```
Frame 1: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface \Device\NPF_{5F1E0E48-1B5E-49BD-BCEB-2F7FAFAA08BB}, id 0
  Interface id: 0 (\Device\NPF_{5F1E0E48-1B5E-49BD-BCEB-2F7FAFAA08BB})
  Encapsulation type: Ethernet (1)
  Arrival Time: Jun  6, 2021 18:34:09.413453000 中国标准时间
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1622975649.413453000 seconds
  [Time delta from previous captured frame: 0.000000000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 0.000000000 seconds]
  Frame Number: 1
  Frame Length: 174 bytes (1392 bits)
  Capture Length: 174 bytes (1392 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ipv6:udp:mdns]
  [Coloring Rule Name: UDP]
  [Coloring Rule String: udp]
Ethernet II, Src: 52:39:2e:5d:78:51 (52:39:2e:5d:78:51), Dst: IntelCor_e5:e3:86 (90:78:41:e5:e3:86)
  Destination: IntelCor_e5:e3:86 (90:78:41:e5:e3:86)
  Source: 52:39:2e:5d:78:51 (52:39:2e:5d:78:51)
  Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: fe80::14c6:f767:1e52:78c2, Dst: ff02::fb
  0110 .... = Version: 6
  .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... .... .... 0000 0000 0111 0000 0000 = Flow Label: 0x00700
  Payload Length: 120
  Next Header: UDP (17)
  Hop Limit: 255
  Source Address: fe80::14c6:f767:1e52:78c2
  Destination Address: ff02::fb
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
  Source Port: 5353
  Destination Port: 5353
  Length: 120
  Checksum: 0x8c8a [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  [Timestamps]
  UDP payload (112 bytes)
Multicast Domain Name System (query)
  Transaction ID: 0x0000
  Flags: 0x0000 Standard query
  Questions: 3
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 1
  Queries
  Additional records
```

从上往下依次为物理层，数据链路层，网络层，传输层的相关信息

```
Flags: 0x002 (SYN)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...0 .... = Acknowledgment: Not set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
  > .... .... ..1. = Syn: Set
    .... .... ...0 = Fin: Not set
    [TCP Flags: ··········S·]
  Window: 65535
  [Calculated window size: 65535]
  Checksum: 0xd090 [unverified]
```

Tcp 第一次握手

```
Flags: 0x011 (FIN, ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
  > .... .... ...1 = Fin: Set
    [TCP Flags: ·····A···F]
  Window: 515
  [Calculated window size: 515]
  [Window size scaling factor: -1 (unknown)]
```

第二次握手

```
0101 .... = Header Length: 20 bytes (5)
Flags: 0x011 (FIN, ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
  > .... .... ...1 = Fin: Set
    [TCP Flags: ·····A···F]
  Window: 1024
  [Calculated window size: 262144]
  [Window size scaling factor: 256]
  Checksum: 0x822a [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
> [SEQ/ACK analysis]
```

第三次握手

2	0.788435	192.168.1.105	14.215.177.39	TCP	54 61828 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
4	3.195109	192.168.1.105	14.215.177.39	TCP	54 [TCP Retransmission] 61828 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
14	7.617080	192.168.1.105	14.215.177.39	TCP	54 61826 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15	8.005430	192.168.1.105	14.215.177.39	TCP	54 [TCP Retransmission] 61828 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0

客户端断开链接，四次挥手

```
2020/03/22 14:51:00,44-F9-71-30-CA-AC,117: 92: 86:164,38-BA-F8-8D-ED-A7,192:168:  0:105,138
2020/03/22 14:51:00,38-BA-F8-8D-ED-A7,192:168:  0:105,44-F9-71-30-CA-AC,117: 92: 86:164,106
2020/03/22 14:51:00,44-F9-71-30-CA-AC,117: 25: 72: 80,38-BA-F8-8D-ED-A7,192:168:  0:105,58
2020/03/22 14:51:00,38-BA-F8-8D-ED-A7,192:168:  0:105,44-F9-71-30-CA-AC,192:168:  1:  9,138
2020/03/22 14:51:00,44-F9-71-30-CA-AC,123:168:156:196,38-BA-F8-8D-ED-A7,192:168:  0:105,58
2020/03/22 14:51:00,44-F9-71-30-CA-AC,182: 47:127:  5,38-BA-F8-8D-ED-A7,192:168:  0:105,58
2020/03/22 14:51:00,38-BA-F8-8D-ED-A7,192:168:  0:105,44-F9-71-30-CA-AC,111:112:244:185,138
```

文件输出日志

```
统计来自不同 MAC 和 IP 地址的通信数据长度:
MAC地址:50-FA-84-60-8F-C4, IP地址: 61:151:180:170, 通信数据长度:857
MAC地址:74-70-FD-39-79-A7, IP地址:192:168:  1:107, 通信数据长度:7589
MAC地址:FF-FF-FF-FF-FF-FF, IP地址:192:168:  1:255, 通信数据长度:276
MAC地址:01-00-5E-00-00-FB, IP地址:224:  0:  0:251, 通信数据长度:294
MAC地址:01-00-5E-00-00-FC, IP地址:224:  0:  0:252, 通信数据长度:128
MAC地址:50-FA-84-60-8F-C4, IP地址:101:198:198:198, 通信数据长度:182
MAC地址:50-FA-84-60-8F-C4, IP地址:114:114:114:114, 通信数据长度:182
MAC地址:50-FA-84-60-8F-C4, IP地址: 59: 36:120:122, 通信数据长度:125


统计发至不同 MAC 和 IP 地址的通信数据长度:
MAC地址:74-70-FD-39-79-A7, IP地址:192:168:  1:107, 通信数据长度:1346
MAC地址:50-FA-84-60-8F-C4, IP地址: 61:151:180:170, 通信数据长度:6401
MAC地址:70-66-55-98-0B-FF, IP地址:192:168:  1:106, 通信数据长度:544
MAC地址:50-FA-84-60-8F-C4, IP地址:101:198:198:198, 通信数据长度:645
MAC地址:50-FA-84-60-8F-C4, IP地址:114:114:114:114, 通信数据长度:543
MAC地址:52-39-2E-5D-78-51, IP地址:192:168:  1:100, 通信数据长度:154
```

统计长度

```
74:70:fd:39:79:a7 10.30.51.22          c4:ca:d9:3c:d7:5c 121.192.180.66        FTP     Request: USER student
c4:ca:d9:3c:d7:5c 121.192.180.66       74:70:fd:39:79:a7 10.30.51.22           FTP     Response: 331 User name okay, need password.
74:70:fd:39:79:a7 10.30.51.22          c4:ca:d9:3c:d7:5c 121.192.180.66        FTP     Request: PASS 111
c4:ca:d9:3c:d7:5c 121.192.180.66       74:70:fd:39:79:a7 10.30.51.22           FTP     Response: 530 Not logged in.
```

检测 ftp，错误输入

```
74:70:fd:39:79:a7 10.30.51.22          c4:ca:d9:3c:d7:5c 121.192.180.66        FTP     Request: USER student
c4:ca:d9:3c:d7:5c 121.192.180.66       74:70:fd:39:79:a7 10.30.51.22           FTP     Response: 331 User name okay, need password.
74:70:fd:39:79:a7 10.30.51.22          c4:ca:d9:3c:d7:5c 121.192.180.66        FTP     Request: PASS software
c4:ca:d9:3c:d7:5c 121.192.180.66       74:70:fd:39:79:a7 10.30.51.22           FTP     Response: 230 User logged in, proceed.
```

检测 ftp，正确输入

3 实验总结

通过这次实验学习了如何使用 WinPCAP 库监听网卡的数据流、统计流量、统计数据长度以及如何用 Wireshark 测试监听程序，此外，也更加了解数据包的格式及属性，为下次实验打下基础。