

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 2019 级 1 班

姓 名 陈栋

学 号 22920192204171

实验时间 2021 年 3 月 19 日

2021 年 3 月 19 日

填写说明

- 1、本文件为 Word 模板文件，建议使用 Microsoft Word 2019 打开，在可填写的区域中如实填写；
- 2、填表时，勿破坏排版，勿修改字体字号，打印成 PDF 文件提交；
- 3、文件总大小尽量控制在 1MB 以下，勿超过 5MB；
- 4、应将材料清单上传在代码托管平台上；
- 5、在学期最后一节课前按要求打包发送至 cni21@qq.com。

1 实验目的

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

2 实验环境

Window10 \c 语言\java

3 实验结果

1、自己创建 ftp，传输数据到 ftp 上，观察 tcp 报文机制：

1	0.000000	121.192.171.172	10.30.74.63	TCP	66 50515 → 58230 [SYN] Seq=0 Win=65535 Len=0 MSS=1386 WS=256 SACK
2	0.000253	10.30.74.63	121.192.171.172	TCP	66 58230 → 50515 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
3	0.003500	121.192.171.172	10.30.74.63	TCP	60 50515 → 58230 [ACK] Seq=1 Ack=1 Win=262144 Len=0
4	0.003501	121.192.171.172	10.30.74.63	FTP	69 Request: STOR test.txt
5	0.004659	10.30.74.63	121.192.171.172	FTP	108 Response: 125 Data connection already open; Transfer starting.
6	0.007767	121.192.171.172	10.30.74.63	TCP	60 50510 → 21 [ACK] Seq=16 Ack=55 Win=1023 Len=0
7	0.007769	121.192.171.172	10.30.74.63	TCP	70 50515 → 58230 [PSH, ACK] Seq=1 Ack=1 Win=262144 Len=16
8	0.008145	121.192.171.172	10.30.74.63	TCP	60 50515 → 58230 [FIN, ACK] Seq=17 Ack=1 Win=262144 Len=0
9	0.008213	10.30.74.63	121.192.171.172	TCP	54 58230 → 50515 [ACK] Seq=1 Ack=18 Win=131584 Len=0
10	0.008647	10.30.74.63	121.192.171.172	TCP	54 58230 → 50515 [FIN, ACK] Seq=1 Ack=18 Win=131584 Len=0
11	0.008933	10.30.74.63	121.192.171.172	FTP	78 Response: 226 Transfer complete.

通过学校实验室机房，向本机搭建的 ftp 上传文件，学校机房（客户端）端口号以 121 开头，本机（服务器）端口以 10 开头

1.1tcp 三次握手：

第一次握手: 建立连接时, 客户端发送 syn 包(syn=1)到服务器, 并进入 syn_sent 状态, 等待服务确认;

1 0.000000	121.192.171.172	10.30.74.63	TCP	66 50515 → 58230 [SYN] Seq=0 Win=65535 Len=0 MSS=1386 WS=256 SACK_PERM=1
------------	-----------------	-------------	-----	--

第二次握手: 服务器收到 syn 包, 必须确认客户的 SYN (ack=j+1), 同时自己也发送一个 SYN 包 (syn=k), 即 SYN+ACK 包, 此时服务器进入 SYN_RECV 状态;

2 0.000253	10.30.74.63	121.192.171.172	TCP	66 58230 → 50515 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
------------	-------------	-----------------	-----	---

第三次握手: 客户端收到服务器的 SYN+ACK 包, 向服务器发送确认包 ACK(ack=k+1), 此包发送完毕, 客户端和服务器进入 ESTABLISHED (TCP 连接成功) 状态, 完成三次握手程序监听该报文

3 0.003500	121.192.171.172	10.30.74.63	TCP	60 50515 → 58230 [ACK] Seq=1 Ack=1 Win=262144 Len=0
------------	-----------------	-------------	-----	---

1.2 可靠传输

请求传送:

4 0.003501	121.192.171.172	10.30.74.63	FTP	69 Request: STOR test.txt
5 0.004659	10.30.74.63	121.192.171.172	FTP	108 Response: 125 Data connection already open; Transfer starting.

停等协议: 客户端传送一个报文后, 会受到一个确认传送确认, 然后再进行下一步传送。

6 0.007767	121.192.171.172	10.30.74.63	TCP	60 50510 → 21 [ACK] Seq=16 Ack=55 Win=1023 Len=0
7 0.007769	121.192.171.172	10.30.74.63	TCP	70 50515 → 58230 [PSH, ACK] Seq=1 Ack=1 Win=262144 Len=16

56 2.437174	192.168.1.106	192.168.1.103	FTP-DA..	1514 FTP Data: 1460 bytes (PASV) (STOR 22920192203947_关伟健_第十二周作业.docx)
57 2.437174	192.168.1.106	192.168.1.103	FTP-DA..	1514 FTP Data: 1460 bytes (PASV) (STOR 22920192203947_关伟健_第十二周作业.docx)
58 2.437176	192.168.1.106	192.168.1.103	FTP-DA..	1230 FTP Data: 1176 bytes (PASV) (STOR 22920192203947_关伟健_第十二周作业.docx)
59 2.437176	192.168.1.106	192.168.1.103	FTP-DA..	1514 FTP Data: 1460 bytes (PASV) (STOR 22920192203947_关伟健_第十二周作业.docx)
60 2.437177	192.168.1.106	192.168.1.103	FTP-DA..	1514 FTP Data: 1460 bytes (PASV) (STOR 22920192203947_关伟健_第十二周作业.docx)
61 2.437177	192.168.1.106	192.168.1.103	FTP-DA..	1230 FTP Data: 1176 bytes (PASV) (STOR 22920192203947_关伟健_第十二周作业.docx)
62 2.437177	192.168.1.106	192.168.1.103	FTP-DA..	1514 FTP Data: 1460 bytes (PASV) (STOR 22920192203947_关伟健_第十二周作业.docx)
63 2.437178	192.168.1.106	192.168.1.103	FTP-DA..	1514 FTP Data: 1460 bytes (PASV) (STOR 22920192203947_关伟健_第十二周作业.docx)
64 2.437178	192.168.1.106	192.168.1.103	FTP-DA..	1230 FTP Data: 1176 bytes (PASV) (STOR 22920192203947_关伟健_第十二周作业.docx)
65 2.437179	192.168.1.106	192.168.1.103	FTP-DA..	1514 FTP Data: 1460 bytes (PASV) (STOR 22920192203947_关伟健_第十二周作业.docx)
66 2.437293	192.168.1.103	192.168.1.106	TCP	54 54801 → 53061 [ACK] Seq=1 Ack=13749 Win=131328 Len=0
67 2.441375	192.168.1.106	192.168.1.103	FTP-DA..	1514 FTP Data: 1460 bytes (PASV) (STOR 22920192203947_关伟健_第十二周作业.docx)
68 2.441376	192.168.1.106	192.168.1.103	FTP-DA..	1514 FTP Data: 1460 bytes (PASV) (STOR 22920192203947_关伟健_第十二周作业.docx)
69 2.441377	192.168.1.106	192.168.1.103	FTP-DA..	1514 FTP Data: 1460 bytes (PASV) (STOR 22920192203947_关伟健_第十二周作业.docx)
70 2.441378	192.168.1.106	192.168.1.103	FTP-DA..	1514 FTP Data: 1460 bytes (PASV) (STOR 22920192203947_关伟健_第十二周作业.docx)
71 2.441460	192.168.1.103	192.168.1.106	TCP	54 54801 → 53061 [ACK] Seq=1 Ack=19589 Win=131328 Len=0

窗口机制:

报文没有捕捉到, 出现报文丢失

1290 3.050974	192.168.1.106	192.168.1.103	FTP-DA..	1514 [TCP Previous segment not captured] FTP Data: 1460 bytes (PASV)
---------------	---------------	---------------	----------	--

拥塞控制:

重复应答: #前表示报文到哪个序号丢失, #后面是第几次丢失

1311	3.051026	192.168.1.103	192.168.1.106	TCP	66 [TCP Dup ACK 1289#1] 54801 → 53061 [ACK] Seq=1 Ack=1654569 Win=131328 Len=0 SLE=1656029 SRE=1656029
1312	3.051078	192.168.1.103	192.168.1.106	TCP	66 [TCP Dup ACK 1289#2] 54801 → 53061 [ACK] Seq=1 Ack=1654569 Win=131328 Len=0 SLE=1656029 SRE=1656029
1313	3.051098	192.168.1.103	192.168.1.106	TCP	66 [TCP Dup ACK 1289#3] 54801 → 53061 [ACK] Seq=1 Ack=1654569 Win=131328 Len=0 SLE=1656029 SRE=1656029
1314	3.051111	192.168.1.103	192.168.1.106	TCP	66 [TCP Dup ACK 1289#4] 54801 → 53061 [ACK] Seq=1 Ack=1654569 Win=131328 Len=0 SLE=1656029 SRE=1656029
1315	3.051124	192.168.1.103	192.168.1.106	TCP	66 [TCP Dup ACK 1289#5] 54801 → 53061 [ACK] Seq=1 Ack=1654569 Win=131328 Len=0 SLE=1656029 SRE=1656029
1316	3.051135	192.168.1.103	192.168.1.106	TCP	66 [TCP Dup ACK 1289#6] 54801 → 53061 [ACK] Seq=1 Ack=1654569 Win=131328 Len=0 SLE=1656029 SRE=1656029
1317	3.051147	192.168.1.103	192.168.1.106	TCP	66 [TCP Dup ACK 1289#7] 54801 → 53061 [ACK] Seq=1 Ack=1654569 Win=131328 Len=0 SLE=1656029 SRE=1656029
1318	3.051159	192.168.1.103	192.168.1.106	TCP	66 [TCP Dup ACK 1289#8] 54801 → 53061 [ACK] Seq=1 Ack=1654569 Win=131328 Len=0 SLE=1656029 SRE=1656029
1319	3.051171	192.168.1.103	192.168.1.106	TCP	66 [TCP Dup ACK 1289#9] 54801 → 53061 [ACK] Seq=1 Ack=1654569 Win=131328 Len=0 SLE=1656029 SRE=1656029
1320	3.051199	192.168.1.103	192.168.1.106	TCP	66 [TCP Dup ACK 1289#10] 54801 → 53061 [ACK] Seq=1 Ack=1654569 Win=131328 Len=0 SLE=1656029 SRE=1656029
1321	3.051211	192.168.1.103	192.168.1.106	TCP	66 [TCP Dup ACK 1289#11] 54801 → 53061 [ACK] Seq=1 Ack=1654569 Win=131328 Len=0 SLE=1656029 SRE=1656029
1322	3.051222	192.168.1.103	192.168.1.106	TCP	66 [TCP Dup ACK 1289#12] 54801 → 53061 [ACK] Seq=1 Ack=1654569 Win=131328 Len=0 SLE=1656029 SRE=1656029
1323	3.051233	192.168.1.103	192.168.1.106	TCP	66 [TCP Dup ACK 1289#13] 54801 → 53061 [ACK] Seq=1 Ack=1654569 Win=131328 Len=0 SLE=1656029 SRE=1656029
1324	3.051244	192.168.1.103	192.168.1.106	TCP	66 [TCP Dup ACK 1289#14] 54801 → 53061 [ACK] Seq=1 Ack=1654569 Win=131328 Len=0 SLE=1656029 SRE=1656029
1325	3.051255	192.168.1.103	192.168.1.106	TCP	66 [TCP Dup ACK 1289#15] 54801 → 53061 [ACK] Seq=1 Ack=1654569 Win=131328 Len=0 SLE=1656029 SRE=1656029
1326	3.051285	192.168.1.103	192.168.1.106	TCP	66 [TCP Dup ACK 1289#16] 54801 → 53061 [ACK] Seq=1 Ack=1654569 Win=131328 Len=0 SLE=1656029 SRE=1656029
1327	3.051296	192.168.1.103	192.168.1.106	TCP	66 [TCP Dup ACK 1289#17] 54801 → 53061 [ACK] Seq=1 Ack=1654569 Win=131328 Len=0 SLE=1656029 SRE=1656029
1328	3.051307	192.168.1.103	192.168.1.106	TCP	66 [TCP Dup ACK 1289#18] 54801 → 53061 [ACK] Seq=1 Ack=1654569 Win=131328 Len=0 SLE=1656029 SRE=1656029
1329	3.051318	192.168.1.103	192.168.1.106	TCP	66 [TCP Dup ACK 1289#19] 54801 → 53061 [ACK] Seq=1 Ack=1654569 Win=131328 Len=0 SLE=1656029 SRE=1656029
1330	3.051329	192.168.1.103	192.168.1.106	TCP	66 [TCP Dup ACK 1289#20] 54801 → 53061 [ACK] Seq=1 Ack=1654569 Win=131328 Len=0 SLE=1656029 SRE=1656029

1.3 四次挥手

客户端发送一个 FIN, 用来关闭客户端到服务器的数据传送

8	0.008145	121.192.171.172	10.30.74.63	TCP	60 50515 → 58230 [FIN, ACK] Seq=17 Ack=1 Win=262144 Len=0
---	----------	-----------------	-------------	-----	---

服务器受到 FIN 后, 发回一个 ACK

9	0.008213	10.30.74.63	121.192.171.172	TCP	54 58230 → 50515 [ACK] Seq=1 Ack=18 Win=131584 Len=0
---	----------	-------------	-----------------	-----	--

服务器关闭与客户端的连接, 发送一个 FIN 给客户端

10	0.008647	10.30.74.63	121.192.171.172	TCP	54 58230 → 50515 [FIN, ACK] Seq=1 Ack=18 Win=131584 Len=0
----	----------	-------------	-----------------	-----	---

客户端回答 ACK 报文确认

11	0.008933	10.30.74.63	121.192.171.172	FTP	78 Response: 226 Transfer complete.
----	----------	-------------	-----------------	-----	-------------------------------------

使用程序监听到的报文数据:

```

D:\Programs\WpdPack\Examples-pcap\Debug\86\UDPDump.exe
1. \Device\NPF_{5C9AE1DE-1509-44A5-882C-5BE59FC98847} (Sangfor SSL VPN CS Support System VNIC)
2. \Device\NPF_{B0B6F91D-9C35-4C18-9221-A2B44A098330} (Microsoft)
3. \Device\NPF_{C9855670-99C5-4371-88BB-87468BFA194F} (Microsoft)
4. \Device\NPF_{81406919-7889-419C-A649-839CF35F3054} (Microsoft)
Enter the interface number (1-4):4
Listening on Microsoft...

no. 1
23:04:32.46-A4-72-7F-14-21, 192.168.1.106, FF-FF-FF-FF-FF-FF, 192.168.1.255, 92
no. 2
23:04:33, C4-CA-D9-3C-D7-5D, 121.192.171.172, 38-00-25-3B-A4-2F, 10.30.74.63, 66
no. 3
23:04:33, 38-00-25-3B-A4-2F, 10.30.74.63, C4-CA-D9-3C-D7-5D, 121.192.171.172, 66
no. 4
23:04:33, C4-CA-D9-3C-D7-5D, 121.192.171.172, 38-00-25-3B-A4-2F, 10.30.74.63, 60
no. 5
23:04:33, C4-CA-D9-3C-D7-5D, 121.192.171.172, 38-00-25-3B-A4-2F, 10.30.74.63, 69
no. 6
23:04:33, 38-00-25-3B-A4-2F, 10.30.74.63, C4-CA-D9-3C-D7-5D, 121.192.171.172, 108
no. 7
23:04:33, C4-CA-D9-3C-D7-5D, 121.192.171.172, 38-00-25-3B-A4-2F, 10.30.74.63, 60

```

2、报文分析：

2.1 数据层报文：

蓝色：以太网报文头 14 位

红色：IP 报文头 20 位

黄色：TCP 报文头 20 位

0000	38 00 25 3b a4 2f c4 ca d9 3c d7 5d 08 00 45 00	8·%;·/·· ·<·]··E·
0010	00 28 6a d6 40 00 7d 06 19 30 79 c0 ab ac 0a 1e	·(j·@·}· ·0y·····
0020	4a 3f c5 4e 00 15 2f 2c 61 35 7e b6 bc ab 50 10	J?·N··/, a5~····P·
0030	03 ff a0 e4 00 00 00 00 00 00 00 00	··········

2.2 TCP 报文：

源端口号（2 字节）：21 （00 15） 目的端口号（2 字节）：50510（c5 4e）

序号（4 字节）：2125905013 （7e b6 bc 75）

确认序号（4）：79143621 （2f 2c 61 35）

首部长（4）：20

标志位（12）：0x018（50 18）

窗口大小（2）：513

校验和（2）：0x7a1a

紧急指针 (2) 0

```

v Transmission Control Protocol, Src Port: 21, Dst Port: 50510, Seq: 1, Ack: 16, Len: 54
  Source Port: 21
  Destination Port: 50510
  [Stream index: 1]
  [TCP Segment Len: 54]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 2125905013
  [Next Sequence Number: 55 (relative sequence number)]
  Acknowledgment Number: 16 (relative ack number)
  Acknowledgment number (raw): 791437621
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
  Window: 513
  [Calculated window size: 513]
  [Window size scaling factor: -1 (unknown)]
  Checksum: 0x7a1a [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
  TCP payload (54 bytes)

```

3、计算一分钟内的通信长度: (java 计算)

总流量113416	13.75.38.A8: 717
源mac地址流量	117.18.232.A8: 264
38-00-25-3B-A4-2F: 44108	192.168.1.60: 495
60-EE-5C-D0-D3-D0: 69308	40.84.185.A8: 54
源ip地址流量	目的mac地址流量
13.107.5.A8: 54	38-00-25-3B-A4-2F: 69308
23.196.217.A8: 636	60-EE-5C-D0-D3-D0: 44108
192.168.1.4B: 1496	目的ip地址流量
192.168.1.C4: 721	202.89.233.100: 3659
192.168.1.59: 3659	23.196.217.131: 721
202.89.233.A8: 63500	192.168.1.103: 69308
192.168.1.54: 180	117.18.232.200: 462
40.119.211.A8: 66	40.84.185.67: 180
192.168.1.12: 462	13.75.38.7: 1496
192.168.1.DD: 37040	40.119.211.203: 55
111.221.29.A8: 3873	111.221.29.254: 37040
192.168.1.77: 55	113.96.202.106: 495
113.96.202.A8: 144	
13.75.38.A8: 717	

4 观察 FTP 数据

ftp 数据报文是利用 tcp 协议传输的，登陆时所传输的登录信息是放在 tcp 报文的数据中。以 530 开头，表示登录失败，以 230 开头表示登录成功，其中登录信息用户名和密码是分开传送，先认定用户名有效，在认定密码有效。

登录成功的数据报：

TIME	SOURCE	DESTINATION	PROTOCOL	LENGTH	INFO
1 0.000000	192.168.1.103	121.192.180.66	FTP	80	Request: USER student
2 0.006416	192.168.1.103	121.192.180.66	FTP	81	Request: PASS software
3 0.011610	121.192.180.66	192.168.1.103	FTP	96	Response: 230 User logged in, proceed.

登录失败的数据报：

1 0.000000	192.168.1.103	121.192.180.66	FTP	76	Request: USER aaa
2 0.040722	192.168.1.103	121.192.180.66	FTP	76	Request: PASS aaa
3 0.043525	121.192.180.66	192.168.1.103	FTP	86	Response: 530 Not logged in.

```
D:\Programs\WpdPack\Examples-pcap\Debug\x86\UDPdump.exe
2. \Device\NPF_{B6E6E91D-9CC5-4CC8-9231-A2E944AD8389} (Microsoft)
3. \Device\NPF_{C9855670-99C5-4371-88BB-87468BFA194F} (Microsoft)
4. \Device\NPF_{81406919-788F-419C-A6A9-83FCF35F3D54} (Microsoft)
Enter the interface number (1-4):4

listening on Microsoft...

no. 1
21:23:19, 38-00-25-3B-A4-2F, 192.168.1.103, 60-EE-5C-D0-D3-D0, 121.192.180.66, USER aaa
G@巽 L

no. 2
21:23:19, 38-00-25-3B-A4-2F, 192.168.1.103, 60-EE-5C-D0-D3-D0, 121.192.180.66, PASS aaa
G@巽 V

no. 3
21:23:19, 60-EE-5C-D0-D3-D0, 121.192.180.66, 38-00-25-3B-A4-2F, 192.168.1.103, 530 Not logged in.

no. 4
21:23:19, 38-00-25-3B-A4-2F, 192.168.1.103, 60-EE-5C-D0-D3-D0, 121.192.180.66, USER student
G@巽/

no. 5
21:23:19, 38-00-25-3B-A4-2F, 192.168.1.103, 60-EE-5C-D0-D3-D0, 121.192.180.66, PASS software
G@

no. 6
21:23:19, 60-EE-5C-D0-D3-D0, 121.192.180.66, 38-00-25-3B-A4-2F, 192.168.1.103, 230 User logged in,
```

4 实验代码

本次实验的代码已上传于以下代码仓库：[cd888888/network: report \(github.com\)](https://github.com/cd888888/network-report)

5 实验总结

掌握了 tcp 报文格式

掌握了 ftp 登录时的通信过程

掌握了怎么使用 wireshark 观察网络流量，并辅助进行网络监听相关的编程

掌握了使用 winpcap 库监听处理以太网帧和 ip 报文的方法等计算机网络的基础知识和网络编程方法。