

Lab3 Report

WT5

see the file WT5.txt

PT4

I separate the posix interface and the tcp machine code. The former is in the socket.cc and the later is in the tcp.cc. I implement the socket, listen, bind, accept and connect. But I haven't finished the write and read and close because of the lack of time. I will complete this later.

CP7

```
> Frame 15: 228 bytes on wire (1824 bits), 228 bytes captured (1824 bits) on interface cp4-veth1-2, id 0
> Ethernet II, Src: 32:ae:70:8b:5d:30 (32:ae:70:8b:5d:30), Dst: ca:e1:fa:b9:7c:27 (ca:e1:fa:b9:7c:27)
> Internet Protocol Version 4, Src: 10.100.1.1, Dst: 10.100.3.2
< Transmission Control Protocol, Src Port: 12345, Dst Port: 80, Seq: 1, Ack: 1, Len: 174
  Source Port: 12345
  Destination Port: 80
  [Stream index: 0]
  [Conversation completeness: Incomplete (12)]
  [TCP Segment Len: 174]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 1
  [Next Sequence Number: 175 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 0
  0101 .... = Header Length: 20 bytes (5)
  < Flags: 0x018 (PSH, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Accurate ECN: Not set
    .... 0... = Congestion Window Reduced: Not set
    .... .0.. = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...1 = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
0000 ca e1 fa b9 7c 27 32 ae 70 8b 5d 30 08 00 45 00 ...|'2· p·]0··E·
0010 00 d6 00 00 00 00 40 06 00 20 0a 64 01 01 0a 64 .....@· · ·d··d
0020 03 02 30 39 00 50 00 00 00 01 00 00 00 00 50 18 ..09·P·· .....P·
0030 10 00 00 00 00 00 49 6e 20 74 68 65 73 65 20 65 .....In these e
0040 78 61 6d 70 6c 65 73 2c 20 69 6e 65 74 5f 6e 74 xamples, inet_nt
0050 6f 70 20 69 73 20 75 73 65 64 20 74 6f 20 63 6f op is us ed to co
0060 6e 76 65 72 74 20 74 68 65 20 62 69 6e 61 72 79 nvert th e binary
0070 20 72 65 70 72 65 73 65 6e 74 61 74 69 6f 6e 20 represe ntation
0080 6f 66 20 61 6e 20 49 50 20 61 64 64 72 65 73 73 of an IP address
0090 20 69 6e 74 6f 20 61 20 68 75 6d 61 6e 2d 72 65 into a human-re
00a0 61 64 61 62 6c 65 20 73 74 72 69 6e 67 2e 20 54 adable s tring. T
00b0 68 65 20 72 65 73 75 6c 74 69 6e 67 20 73 74 72 he resul ting str
00c0 69 6e 67 20 69 73 20 73 74 6f 72 65 64 20 69 6e ing is s tored in
00d0 20 74 68 65 20 69 70 53 74 72 20 76 61 72 69 61 the ipS tr varia
00e0 62 6c 65 2e ble.
```

The tcp header start from the 35 byte. The first 2 bytes indicates the source port 12345, the later two is the destination 80. Then the four are the sequence number 1. After the four are the acknowledge number 1. Then the data offsets indicates the length of the tcp header. The the flags contains push, SYN,ACK and so on. Then are the window size and checksum.

CP8

I use stop and wait method to address packet loss and poor network condition

use tc-netm to implement a delay and loss rate network. And the send host and receive host code is accordingly in the send.cpp and recv.cpp. The script code is in cp4.txt in checkpoint fold. I attach a screenshot below.

```
vnetUtils > helper > $ cp4.sh
1  #!/bin/bash
2  sudo bash ./execNS cp4-ns1 tshark -i cp4-veth1-2 -c 200 -w ns1.pcap &
3  sudo bash ./execNS cp4-ns4 tshark -i cp4-veth4-3 -c 200 -w ns4.pcap &
4  sudo bash ./execNS cp4-ns1 tc qdisc add dev cp4-veth1-2 root netem delay 200ms loss10%
5  sudo bash ./execNS cp4-ns1 /lab-netstack-premium-master/lab3/send cp4-veth1-2 > 1.txt &
6  sudo bash ./execNS cp4-ns2 /lab-netstack-premium-master/lab3/host cp4-veth2-1 cp4-veth2-3 > 2.txt &
7  sudo bash ./execNS cp4-ns3 /lab-netstack-premium-master/lab3/host cp4-veth3-2 cp4-veth3-4 > 3.txt &
8  sudo bash ./execNS cp4-ns4 /lab-netstack-premium-master/lab3/recv cp4-veth4-3 > 4.txt &
9
```

Here are the wireshark trace in host1(send) and host4(receive)

No.	Time	Source	Destination	Protocol	Length	Info
14	3.157102751	8a:90:c6:f3:7...	4a:95:9b:9a:c1:43	ARP	42	10.100.1.2 is at 8a:90:c6:f3:7c:57
15	9.055051796	10.100.1.1	10.100.3.2	TCP	228	12345 → 80 [PSH, ACK] Seq=1 Ack=1 Win=4096 Len=174
16	13.375102298	10.100.3.2	10.100.1.1	TCP	54	80 → 12345 [ACK] Seq=1 Ack=175 Win=4096 Len=0
17	14.078889590	10.100.1.1	10.100.3.2	TCP	228	[TCP Spurious Retransmission] 12345 → 80 [PSH, ACK]
18	18.494113592	10.100.3.2	10.100.1.1	TCP	54	[TCP Dup ACK 16#1] 80 → 12345 [ACK] Seq=1 Ack=175 Wi
19	19.101922300	10.100.1.1	10.100.3.2	TCP	228	12345 → 80 [PSH, ACK] Seq=175 Ack=1 Win=4096 Len=174
20	23.610103553	10.100.3.2	10.100.1.1	TCP	54	80 → 12345 [ACK] Seq=1 Ack=349 Win=4096 Len=0
21	24.124076803	10.100.1.1	10.100.3.2	TCP	228	[TCP Spurious Retransmission] 12345 → 80 [PSH, ACK]
22	28.733980249	10.100.3.2	10.100.1.1	TCP	54	[TCP Dup ACK 20#1] 80 → 12345 [ACK] Seq=1 Ack=349 Wi
23	29.148983583	10.100.1.1	10.100.3.2	TCP	228	12345 → 80 [PSH, ACK] Seq=349 Ack=1 Win=4096 Len=174
24	33.850086335	10.100.3.2	10.100.1.1	TCP	54	80 → 12345 [ACK] Seq=1 Ack=523 Win=4096 Len=0
25	34.177950377	10.100.1.1	10.100.3.2	TCP	228	[TCP Spurious Retransmission] 12345 → 80 [PSH, ACK]
26	38.976719837	10.100.3.2	10.100.1.1	TCP	54	[TCP Dup ACK 24#1] 80 → 12345 [ACK] Seq=1 Ack=523 Wi
27	39.201938212	10.100.1.1	10.100.3.2	TCP	228	12345 → 80 [PSH, ACK] Seq=523 Ack=1 Win=4096 Len=174
28	44.093706590	10.100.3.2	10.100.1.1	TCP	54	80 → 12345 [ACK] Seq=1 Ack=697 Win=4096 Len=0
29	44.224787298	10.100.1.1	10.100.3.2	TCP	228	[TCP Spurious Retransmission] 12345 → 80 [PSH, ACK]
30	49.210830425	10.100.3.2	10.100.1.1	TCP	54	[TCP Dup ACK 28#1] 80 → 12345 [ACK] Seq=1 Ack=697 Wi
31	49.243789592	10.100.1.1	10.100.3.2	TCP	228	12345 → 80 [PSH, ACK] Seq=697 Ack=1 Win=4096 Len=174
32	54.263666386	10.100.1.1	10.100.3.2	TCP	228	[TCP Retransmission] 12345 → 80 [PSH, ACK] Seq=697 A
33	54.328754011	10.100.3.2	10.100.1.1	TCP	54	80 → 12345 [ACK] Seq=1 Ack=871 Win=4096 Len=0
34	58.425818374	10.100.3.2	10.100.1.1	TCP	54	[TCP Dup ACK 33#1] 80 → 12345 [ACK] Seq=1 Ack=871 Wi
35	59.286885458	10.100.1.1	10.100.3.2	TCP	228	12345 → 80 [PSH, ACK] Seq=871 Ack=1 Win=4096 Len=174
36	63.545098751	10.100.3.2	10.100.1.1	TCP	54	80 → 12345 [ACK] Seq=1 Ack=1045 Win=4096 Len=0
37	64.307692085	10.100.1.1	10.100.3.2	TCP	228	[TCP Spurious Retransmission] 12345 → 80 [PSH, ACK]
38	68.674105962	10.100.3.2	10.100.1.1	TCP	54	[TCP Dup ACK 36#1] 80 → 12345 [ACK] Seq=1 Ack=1045 w
39	69.327830754	10.100.1.1	10.100.3.2	TCP	228	12345 → 80 [PSH, ACK] Seq=1045 Ack=1 Win=4096 Len=17
40	73.788133673	10.100.3.2	10.100.1.1	TCP	54	80 → 12345 [ACK] Seq=1 Ack=1219 Win=4096 Len=0
41	74.355670715	10.100.1.1	10.100.3.2	TCP	228	[TCP Spurious Retransmission] 12345 → 80 [PSH, ACK]

No.	Time	Source	Destination	Protocol	Length	Info
14	3.130965585	b2:c3:29:52:c...	36:0f:2f:be:43:72	ARP	42	10.100.3.1 is at b2:c3:29:52:cc:bb
15	10.296073380	10.100.1.1	10.100.3.2	TCP	228	12345 → 80 [PSH, ACK] Seq=1 Ack=1 Win=4096 Len=174
16	11.318035089	10.100.3.2	10.100.1.1	TCP	54	80 → 12345 [ACK] Seq=1 Ack=175 Win=4096 Len=0
17	15.416992882	10.100.1.1	10.100.3.2	TCP	228	[TCP Spurious Retransmission] 12345 → 80 [PSH, ACK]
18	16.442096716	10.100.3.2	10.100.1.1	TCP	54	[TCP Dup ACK 16#1] 80 → 12345 [ACK] Seq=1 Ack=175 Wi
19	20.534065010	10.100.1.1	10.100.3.2	TCP	228	12345 → 80 [PSH, ACK] Seq=175 Ack=1 Win=4096 Len=174
20	21.558049135	10.100.3.2	10.100.1.1	TCP	54	80 → 12345 [ACK] Seq=1 Ack=349 Win=4096 Len=0
21	25.654081887	10.100.1.1	10.100.3.2	TCP	228	[TCP Spurious Retransmission] 12345 → 80 [PSH, ACK]
22	26.678036679	10.100.3.2	10.100.1.1	TCP	54	[TCP Dup ACK 20#1] 80 → 12345 [ACK] Seq=1 Ack=349 Wi
23	30.773596334	10.100.1.1	10.100.3.2	TCP	228	12345 → 80 [PSH, ACK] Seq=349 Ack=1 Win=4096 Len=174
24	31.804914501	10.100.3.2	10.100.1.1	TCP	54	80 → 12345 [ACK] Seq=1 Ack=523 Win=4096 Len=0
25	35.903946378	10.100.1.1	10.100.3.2	TCP	228	[TCP Spurious Retransmission] 12345 → 80 [PSH, ACK]
26	36.919954212	10.100.3.2	10.100.1.1	TCP	54	[TCP Dup ACK 24#1] 80 → 12345 [ACK] Seq=1 Ack=523 Wi
27	41.015001422	10.100.1.1	10.100.3.2	TCP	228	12345 → 80 [PSH, ACK] Seq=523 Ack=1 Win=4096 Len=174
28	42.038867089	10.100.3.2	10.100.1.1	TCP	54	80 → 12345 [ACK] Seq=1 Ack=697 Win=4096 Len=0
29	46.132948508	10.100.1.1	10.100.3.2	TCP	228	[TCP Spurious Retransmission] 12345 → 80 [PSH, ACK]
30	47.158918633	10.100.3.2	10.100.1.1	TCP	54	[TCP Dup ACK 28#1] 80 → 12345 [ACK] Seq=1 Ack=697 Wi
31	51.258986093	10.100.1.1	10.100.3.2	TCP	228	12345 → 80 [PSH, ACK] Seq=697 Ack=1 Win=4096 Len=174
32	52.278714177	10.100.3.2	10.100.1.1	TCP	54	80 → 12345 [ACK] Seq=1 Ack=871 Win=4096 Len=0
33	55.353938845	10.100.1.1	10.100.3.2	TCP	228	[TCP Spurious Retransmission] 12345 → 80 [PSH, ACK]
34	56.374709346	10.100.3.2	10.100.1.1	TCP	54	[TCP Dup ACK 32#1] 80 → 12345 [ACK] Seq=1 Ack=871 Wi
35	60.473776250	10.100.1.1	10.100.3.2	TCP	228	12345 → 80 [PSH, ACK] Seq=871 Ack=1 Win=4096 Len=174
36	61.499090167	10.100.3.2	10.100.1.1	TCP	54	80 → 12345 [ACK] Seq=1 Ack=1045 Win=4096 Len=0
37	65.589089753	10.100.1.1	10.100.3.2	TCP	228	[TCP Spurious Retransmission] 12345 → 80 [PSH, ACK]
38	66.614094211	10.100.3.2	10.100.1.1	TCP	54	[TCP Dup ACK 36#1] 80 → 12345 [ACK] Seq=1 Ack=1045 W
39	70.717088172	10.100.1.1	10.100.3.2	TCP	228	12345 → 80 [PSH, ACK] Seq=1045 Ack=1 Win=4096 Len=17
40	71.744066881	10.100.3.2	10.100.1.1	TCP	54	80 → 12345 [ACK] Seq=1 Ack=1219 Win=4096 Len=0
41	75.829091716	10.100.1.1	10.100.3.2	TCP	228	[TCP Spurious Retransmission] 12345 → 80 [PSH, ACK]

Frame 1: 46 bytes on wire (368 bits) 46 bytes captured (368 bits) on interface en4-veth4-3 id 0

ns4.pcap Packets: 64 · Displayed: 64 (100.0%) Profile: Default