

ECE 636
COMPUTER NETWORKING LABORATORY

Ayush Kale
31573799
ak2739@njit.edu

Lab 6
TCP Experiments

6.2 Lab Descriptions

6.2.1 Connection Establishment and Termination

Step 1a

Use the SSH program to remotely connect to a host in the lab: “ssh <another host>”

```
ak2739@t3net04:~
```

```
File Edit View Search Terminal Help
```

```
To see your aliases, enter "alias"
```

```
t3net16-41 ~ >: ssh 10.10.201.13
ak2739@10.10.201.13's password:
```

```
t3net16-41 ~ >: ssh 10.10.201.13
ak2739@10.10.201.13's password:
Last login: Mon Oct 17 19:01:42 2022 from t3net16
Starting /afs/cad/u/a/k/ak2739/.bash_profile ... standard AFS bash profile
```

```
=====
==> AFS disk quota in your home directory [ /afs/cad/u/a/k/ak2739 ] :
Volume Name          Quota      Used %Used   Partition
user.ak2739           1000000    292432    29%       38%
```

```
Quota = 1.00 Gbytes
Used = 0.29 Gbytes
Note: "Partition" refers to the percentage use of the disk
that the AFS volume is on.
```

```
To free up disk space, including Firefox & Chrome cache, enter :
clean.home
(/usr/ucs/bin/clean.home)
```

```
Calculating Firefox cache usage ...
Put a file named "NoCalcCache" in your home directory to suppress.
du: cannot access './BACKUP-AFS.ACOUNT/BACKUP-AFS.ACOUNT': No such device
Your current Firefox cache uses : 571 Mbytes
```

```
=====
On host t3net04 :
19:02:50 up 7 days, 5:49, 1 user, load average: 0.00, 0.01, 0.05
```

```
==== Your Kerberos ticket and AFS token status ===
Kerberos : Renew until 10/18/2022 19:02:48, Flags: FRIA Renew until 10/18/2022 19:02:48, Flags: FRA
AFS      : User's (AFS ID 520127) tokens for afs@cad.njit.edu [Expires Oct 18 05:02]
```

```
==== Start Python Information ===
1. The default python is Anaconda Python 3
```

```
2. To instead use Anaconda Python 2 :

echo 'module load python2' > ~/.modules

Then log out / log in
==== End Python Information ===
```

```
[Pictures] ak2739@t3net16:~ ak2739@t3net16:~ ak2739@t3net04:~
```

Used ssh program to remotely connect with another host (10.10.201.13) in the lab.

Step 1b

Use “tcpdump -S host <your host IP address> and not host 128.235 -n-ip1p1” to save, observe, and explain the output at the same time in another console.

Command

```
t3net16-43 6.2.1 >: tcpdump -S host 10.10.226.13 and not host 128.235 -n -i p1p1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on p1p1, link-type EN10MB (Ethernet), capture size 262144 bytes
18:37:08.161385 IP 10.10.226.13.724 > 10.10.226.3.nfs: Flags [.], ack 2087663190, win 1424, options [nop,nop,TS val 624505088 ecr 418007607], length 0
```

Output

```
18:37:13.164828 ARP, Request who-has 10.10.226.13 tell 10.10.226.3, length 46
18:37:13.164871 ARP, Reply 10.10.226.13 is-at b4:96:91:52:6c:6b, length 28
18:37:30.481445 ARP, Request who-has 10.10.226.1 tell 10.10.226.13, length 28
18:37:30.481766 ARP, Reply 10.10.226.1 is-at 78:8a:20:be:0b:af, length 46
18:37:43.707588 ARP, Request who-has 10.10.226.13 tell 10.10.226.1, length 46
18:37:43.707615 ARP, Reply 10.10.226.13 is-at b4:96:91:52:6c:6b, length 28
18:38:08.321144 IP 10.10.226.13.724 > 10.10.226.3.nfs: Flags [.], ack 2087663274, win 1424, options [nop,nop,TS val 624565248 ecr 418067765], length 0
18:38:08.321179 IP 10.10.226.13.724 > 10.10.226.3.nfs: Flags [P.], seq 1057540174:1057540294, ack 2087663274, win 1424, options [nop,nop,TS val 624565248 ecr 418067765], length 120: NFS request xid 2796696705 11
6 setattr fh 0,1/53
18:38:08.321400 IP 10.10.226.3.nfs > 10.10.226.13.724: Flags [.], ack 1057540174, win 1432, options [nop,nop,TS val 418127925 ecr 624505088], length 0
18:38:08.321400 IP 10.10.226.3.nfs > 10.10.226.13.724: Flags [P.], seq 2087663274:2087663358, ack 1057540294, win 1432, options [nop,nop,TS val 418127925 ecr 624565248], length 84: NFS reply xid 2796696705 reply ok 88 setattr NON 1 ids 0/815326306 sz 1616396383
18:38:13.324146 IP 10.10.226.13.724 > 10.10.226.3.nfs: Flags [.], ack 2087663358, win 1424, options [nop,nop,TS val 624565248 ecr 418127925], length 0
18:38:13.324644 ARP, Request who-has 10.10.226.13 tell 10.10.226.3, length 46
18:38:13.324685 ARP, Reply 10.10.226.13 is-at b4:96:91:52:6c:6b, length 28
18:38:21.089149 ARP, Request who-has 10.10.226.1 tell 10.10.226.13, length 28
18:38:21.089456 ARP, Reply 10.10.226.1 is-at 78:8a:20:be:0b:af, length 46
18:39:01.169221 ARP, Request who-has 10.10.226.1 tell 10.10.226.13, length 28
18:39:01.169551 ARP, Reply 10.10.226.1 is-at 78:8a:20:be:0b:af, length 46
^C
22 packets captured
22 packets received by filter
0 packets dropped by kernel
t3net16-44 6.2.1 >: 
```

The output consists of ARP request with the message who-has 10.10.226.13 and of length 46 bytes. ARP reply messages with the message 10.10.226.13 is at b4:96:91:52:6c:6b of length 28 bytes.

There were total of 22 packets captured when the tcpdump was running at the time 10.10.226.13 was connected using the ssh command.

Step 2

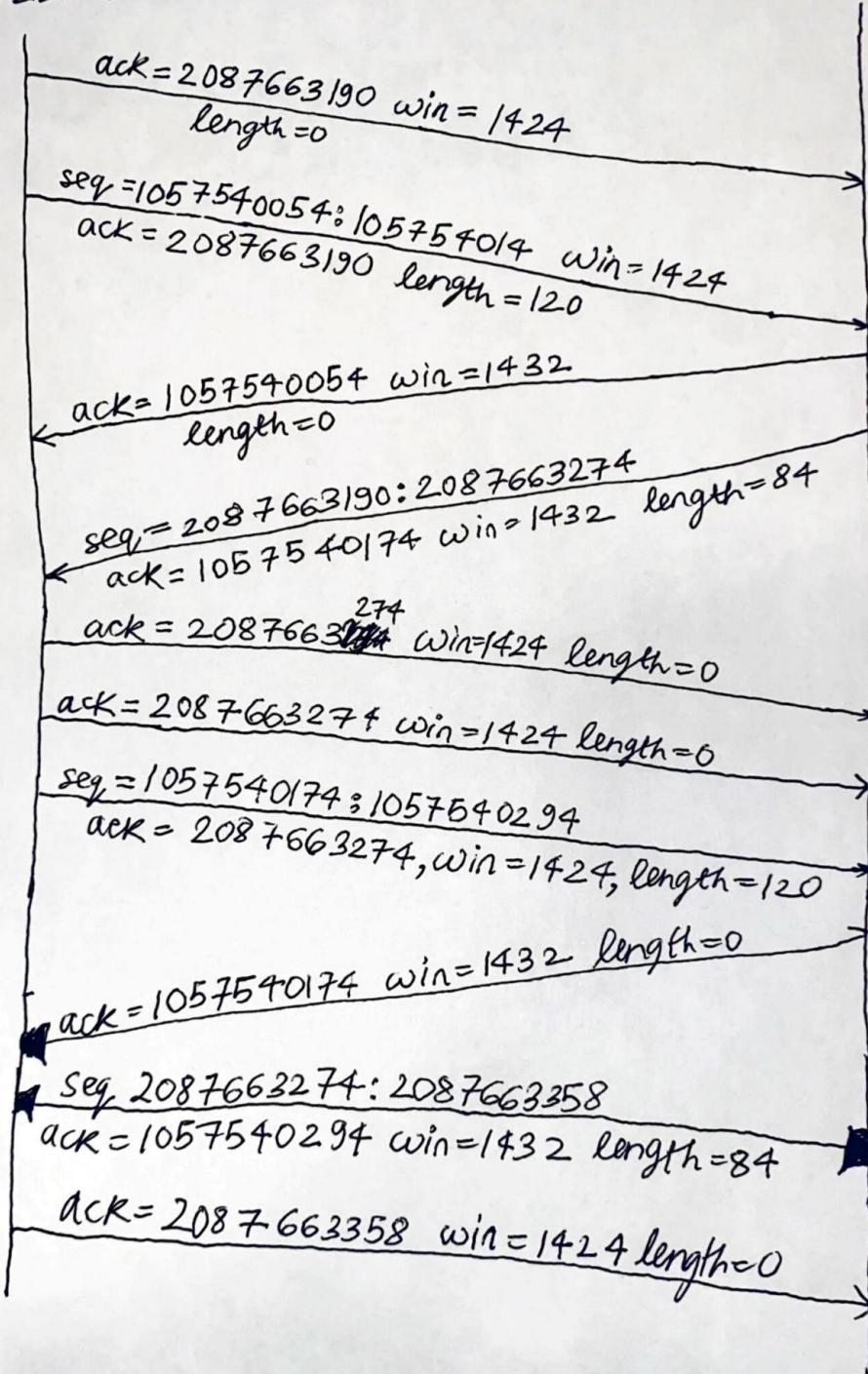
```
t3net04-41 ~ >: hii
bash: hii: command not found...
t3net04-42 ~ >: hi
bash: hi: command not found...
t3net04-43 ~ >: exit
```

Typed any word and pressed exit on the ssh connected terminal.

Step 3: Timeline that shows packet size and demonstrates the data exchange in accordance With the tcp dump.

10.10.226.13.

10.10.226.3.hfs



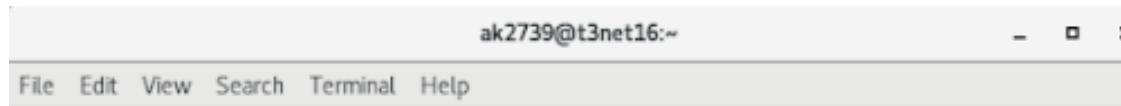
Step 4

The change in the initial sequence number happened from step 1 to step 2.
Earlier the sequence number is 1057540054 and after step 2 the initial sequence

number changed to 1057540174.

b.TCP timeout

```
t3net04-41 ~ >: date
Mon Oct 17 19:13:52 EDT 2022
t3net04-42 ~ >: date
Mon Oct 17 19:16:43 EDT 2022
t3net04-42 ~ >: date
Mon Oct 17 19:17:15 EDT 2022
t3net04-42 ~ >: ssh 10.10.201.233
ssh: connect to host 10.10.201.233 port 22: No route to host
t3net04-43 ~ >: date
Mon Oct 17 19:17:27 EDT 2022
t3net04-44 ~ >: date
Mon Oct 17 19:17:35 EDT 2022
t3net04-44 ~ >: ssh 10.10.201.233
^[[A^[[A^[[Assh: connect to host 10.10.201.233 port 22: No route to host
t3net04-45 ~ >: date
Mon Oct 17 19:17:42 EDT 2022
t3net04-46 ~ >: □
```



The screenshot shows a terminal window with the title bar 'ak2739@t3net16:~'. Below the title bar is a menu bar with options: File, Edit, View, Search, Terminal, and Help. The main area of the terminal contains the command history and output from the previous text block.

To see your aliases, enter "alias"

```
t3net16-41 ~ >: ssh 10.10.201.45
ssh: connect to host 10.10.201.45 port 22: No route to host
t3net16-42 ~ >: ^C
t3net16-42 ~ >: date
Mon Oct 17 19:38:47 EDT 2022
t3net16-43 ~ >: ssh 10.10.201.45
ssh: connect to host 10.10.201.45 port 22: No route to host
t3net16-44 ~ >: date
Mon Oct 17 19:39:02 EDT 2022
t3net16-45 ~ >: □
```

Using the sequence of commands

```
t3net16-42 ~ >: tcpdump -S host 10.10.226.13 and not host 128.235 -n -i plp1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on plp1, link-type EN10MB (Ethernet), capture size 262144 bytes
19:38:45.505883 ARP, Request who-has 10.10.226.13 tell 10.10.226.1, length 46
19:38:45.505923 ARP, Reply 10.10.226.13 is-at b4:96:91:52:6c:6b, length 28
19:38:52.056081 IP 10.10.226.13.37496 > 10.10.201.45.ssh: Flags [S], seq 3968230184, win 29200, options [mss 1460,sackOK,TS val 628208982 ecr 0,nop,wscale 7], length 0
19:38:53.057224 IP 10.10.226.13.37496 > 10.10.201.45.ssh: Flags [S], seq 3968230184, win 29200, options [mss 1460,sackOK,TS val 628209984 ecr 0,nop,wscale 7], length 0
19:38:55.053590 IP 10.10.0.5 > 10.10.226.13: ICMP host 10.10.201.45 unreachable, length 68
19:38:55.053658 IP 10.10.226.13.37496 > 10.10.201.45.ssh: Flags [S], seq 3968230184, win 29200, options [mss 1460,sackOK,TS val 628211980 ecr 0,nop,wscale 7], length 0
19:38:55.053675 IP 10.10.0.5 > 10.10.226.13: ICMP host 10.10.201.45 unreachable, length 68
19:38:55.053759 ARP, Request who-has 10.10.226.1 tell 10.10.226.13, length 28
19:38:55.053759 ARP, Reply 10.10.226.1 is-at 78:8a:20:be:0b:af, length 46
19:38:58.053607 IP 10.10.0.5 > 10.10.226.13: ICMP host 10.10.201.45 unreachable, length 68
19:39:08.353493 IP 10.10.226.13.724 > 10.10.226.3.nfs: Flags [., ack 2087668730, win 1424, options [nop,nop,TS val 628225280 ecr 421727797], length 0
19:39:08.353626 IP 10.10.226.13.724 > 10.10.226.3.nfs: Flags [P.], seq 1057547718:1057547838, ack 2087668730, win 1424, options [nop,nop,TS val 628225280 ecr 421727797], length 120: NFS request xid 3836884097 11
6 getattr fh 0,1/53
19:39:08.353960 IP 10.10.226.3.nfs > 10.10.226.13.724: Flags [., ack 1057547718, win 1432, options [nop,nop,TS val 421787957 ecr 628165121], length 0
19:39:08.353992 IP 10.10.226.3.nfs > 10.10.226.13.724: Flags [P.], seq 2087668814:2087668814, ack 1057547838, win 1432, options [nop,nop,TS val 421787957 ecr 628225280], length 84: NFS reply xid 3836884097 reply ok 80 getattr NON 1 ids 0/815326306 sz 1616396383
19:39:08.354023 IP 10.10.226.13.724 > 10.10.226.3.nfs: Flags [., ack 2087668814, win 1424, options [nop,nop,TS val 628225280 ecr 421787957], length 0
19:39:13.356562 ARP, Request who-has 10.10.226.13 tell 10.10.226.3, length 46
19:39:13.356601 ARP, Reply 10.10.226.13 is-at b4:96:91:52:6c:6b, length 28
^C
17 packets captured
17 packets received by filter
0 packets dropped by kernel
t3net16-42 ~ >: 
```

TCP dump observed. The IP protocol is used to send the ssh requests and the corresponding time stamps are used to calculate the retransmission intervals.

c. TCP connection abort

Using the SSH program to remotely connect to a host with a non-existing port. The following command is used.

```
To see your aliases, enter "alias"

t3net16-41 ~ >: ssh -p2000 10.10.201.33
ssh: connect to host 10.10.201.33 port 2000: No route to host
t3net16-42 ~ >: 
```

To see your aliases, enter "alias"

```
t3net16-41 ~ >: tcpdump -S host 10.10.226.13 and not host 128.235 -n -i plp1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on plp1, link-type EN10MB (Ethernet), capture size 262144 bytes
19:31:44.397615 IP 10.10.226.13.51814 > 10.10.201.33.sieve-filter: Flags [S], seq 971793380, win 29200, options [mss 1460,sackOK,TS val 627781324 ecr 0,nop,wscale 7], length 0
19:31:45.399214 IP 10.10.226.13.51814 > 10.10.201.33.sieve-filter: Flags [S], seq 971793380, win 29200, options [mss 1460,sackOK,TS val 627782326 ecr 0,nop,wscale 7], length 0
19:31:47.401246 IP 10.10.226.13.51814 > 10.10.201.33.sieve-filter: Flags [S], seq 971793380, win 29200, options [mss 1460,sackOK,TS val 627784328 ecr 0,nop,wscale 7], length 0
19:31:47.405884 IP 10.10.0.5 > 10.10.226.13: ICMP host 10.10.201.33 unreachable, length 68
19:31:47.405937 IP 10.10.0.5 > 10.10.226.13: ICMP host 10.10.201.33 unreachable, length 68
19:31:47.405945 IP 10.10.0.5 > 10.10.226.13: ICMP host 10.10.201.33 unreachable, length 68
19:31:52.415547 ARP, Request who-has 10.10.226.13 tell 10.10.226.1, length 46
19:31:52.415581 ARP, Reply 10.10.226.13 is-at b4:96:91:52:6c:6b, length 28
^C
8 packets captured
8 packets received by filter
0 packets dropped by kernel
```

There are 2 segments sent to the address 10.10.201.33 using IP and with options MSS = 1460, sackOK and with length 0.

After this there are unreachable messages (ICMP packets) with length 68.

And ARP request and reply to find the MAC address for the corresponding IP Address

d.TCP connection abort

Step 1 for Host 1 and Step 3 for Host 1

```
t3net11-41 ~ >: sock -L0 10.10.225.13 7777
hello
t3net11-42 ~ >: □
```

Step 2a for Host 1

To see your aliases, enter "alias"

```
t3net11-41 ~ >: sock 10.10.225.13 7788
hello
^C
t3net11-41 ~ >: □
```

Step 2b for Host 1

```
To see your aliases, enter "alias"

t3net11-41 ~ >: tcpdump host 10.10.225.13 and host 10.10.225.12 and not host 128.235 -n -i p1p1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on p1p1, link-type EN10MB (Ethernet), capture size 262144 bytes
19:57:28.623973 IP 10.10.225.12.60078 > 10.10.225.13.7788: Flags [S], seq 1005109244, win 29200, options [mss 1460,sackOK,TS val 602790168 ecr 0,nop,wscale 7], length 0
19:57:28.624466 IP 10.10.225.13.7788 > 10.10.225.12.60078: Flags [S.], seq 2622624259, ack 1005109245, win 28560, options [mss 1440,sackOK,TS val 1217304171 ecr 602790168,nop,wscale 7], length 0
19:57:28.624555 IP 10.10.225.12.60078 > 10.10.225.13.7788: Flags [.], ack 1, win 229, options [nop,nop,TS val 602790169 ecr 1217304171], length 0
19:57:33.637558 ARP, Request who-has 10.10.225.12 tell 10.10.225.13, length 46
19:57:33.637610 ARP, Reply 10.10.225.12 is-at b4:96:91:51:d0:36, length 28
19:57:37.723679 IP 10.10.225.12.60078 > 10.10.225.13.7788: Flags [P.], seq 1:7, ack 1, win 229, options [nop,nop,TS val 602799268 ecr 1217304171], length 6
19:57:37.724293 IP 10.10.225.13.7788 > 10.10.225.12.60078: Flags [.], ack 7, win 224, options [nop,nop,TS val 1217313271 ecr 602799268], length 0
19:57:39.755503 IP 10.10.225.12.60078 > 10.10.225.13.7788: Flags [F.], seq 7, ack 1, win 229, options [nop,nop,TS val 602801300 ecr 1217313271], length 0
19:57:39.756229 IP 10.10.225.13.7788 > 10.10.225.12.60078: Flags [F.], seq 1, ack 8, win 224, options [nop,nop,TS val 1217315303 ecr 602801300], length 0
19:57:39.756280 IP 10.10.225.12.60078 > 10.10.225.13.7788: Flags [.], ack 2, win 229, options [nop,nop,TS val 602801301 ecr 1217315303], length 0
^C
10 packets captured
10 packets received by filter
0 packets dropped by kernel
t3net11-42 ~ >: □
```

The connection has been established on 2 different workstations, one as Host1 and the other performing the role of Host2.

6.2.2 TCP operation

For step 1 both hosts run netstat- an command.

```
t3net04-43 ~ >: netstat -a -n
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp      0      0 0.0.0.0:111              0.0.0.0:*
tcp      0      0 192.168.122.1:53         0.0.0.0:*
tcp      0      0 0.0.0.0:22              0.0.0.0:*
tcp      0      0 127.0.0.1:631            0.0.0.0:*
tcp      0      0 127.0.0.1:25              0.0.0.0:*
tcp      0      0 10.10.201.13:986          10.10.201.3:2049    ESTABLISHED
tcp      0      0 10.10.201.13:47226        128.235.251.10:53   TIME_WAIT
tcp      0      0 10.10.201.13:41576        128.235.251.51:389  ESTABLISHED
tcp      0      0 10.10.201.13:47228        128.235.251.10:53   TIME_WAIT
tcp      0      0 10.10.201.13:47420        10.10.201.12:8899    ESTABLISHED
tcp6     0      0 ::1:111                ::*:*
tcp6     0      0 ::1:22                 ::*:*
tcp6     0      0 ::1:631                ::*:*
tcp6     0      0 ::1:25                 ::*:*
udp      0      0 0.0.0.0:5353           0.0.0.0:*
udp      0      0 0.0.0.0:39028          0.0.0.0:*
udp      0      0 0.0.0.0:7001           0.0.0.0:*
udp      0      0 192.168.122.1:53         0.0.0.0:*
udp      0      0 0.0.0.0:67             0.0.0.0:*
udp      0      0 0.0.0.0:111            0.0.0.0:*
udp      0      0 127.0.0.1:323           0.0.0.0:*
udp6     0      0 ::1:111                ::*:*
udp6     0      0 ::1:323                ::*:*
raw6    0      0 ::1:58                 ::*:*
raw6    0      0 ::1:58                 ::*:*
7
7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type      State       I-Node  Path
unix  2      [ ACC ]     STREAM    LISTENING  9727    /run/systemd/private
unix  2      [ ACC ]     STREAM    LISTENING  22492   /var/lib/sss/pipes/private/sbus-monitor
unix  2      [ ACC ]     STREAM    LISTENING  17045   /var/lib/sss/pipes/private/pam
unix  2      [ ACC ]     STREAM    LISTENING  5103030  @/tmp/dbus-SUJYjjtZzB
unix  2      [ ACC ]     STREAM    LISTENING  5095957  @/tmp/dbus-czKlaiuBwz
```

Step 2

```
t3net04-41 ~ >: sock 10.10.201.12 8899
connect() error: Connection refused
t3net04-42 ~ >: sock 10.10.201.12 8899
```

Step 3

Following the sock command both of the hosts run the netstat -an command again.

```
t3net04-42 ~ >: netstat -a -n
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp      0      0 0.0.0.0:111              0.0.0.0:*
tcp      0      0 192.168.122.1:53         0.0.0.0:*
tcp      0      0 0.0.0.0:22              0.0.0.0:*
tcp      0      0 127.0.0.1:631           0.0.0.0:*
tcp      0      0 127.0.0.1:25           0.0.0.0:*
tcp      0      0 10.10.201.13:986        10.10.201.3:2049    ESTABLISHED
tcp      0      0 10.10.201.13:51144       128.235.251.27:389  ESTABLISHED
tcp      0      0 10.10.201.13:47406       10.10.201.12:8899    ESTABLISHED
tcp6     0      0 ::1:111                ::*:*
tcp6     0      0 ::1:22                 ::*:*
tcp6     0      0 ::1:631                ::*:*
tcp6     0      0 ::1:25                 ::*:*
udp      0      0 0.0.0.0:5353          0.0.0.0:*
udp      0      0 0.0.0.0:39028         0.0.0.0:*
udp      0      0 0.0.0.0:7001          0.0.0.0:*
udp      0      0 192.168.122.1:53         0.0.0.0:*
udp      0      0 0.0.0.0:67             0.0.0.0:*
udp      0      0 0.0.0.0:111            0.0.0.0:*
udp      0      0 127.0.0.1:323          0.0.0.0:*
udp6     0      0 ::1:111                ::*:*
udp6     0      0 ::1:323                ::*:*
raw6     0      0 ::1:58                 ::*:*               7
raw6     0      0 ::1:58                 ::*:*               7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags     Type      State       I-Node  Path
unix  2      [ ACC ]   STREAM    LISTENING  9727    /run/systemd/private
unix  2      [ ACC ]   STREAM    LISTENING  22492   /var/lib/sss/pipes/private/sbus-monitor
unix  2      [ ACC ]   STREAM    LISTENING  17045   /var/lib/sss/pipes/private/pam
```

Step 4

Host 1 runs the sock command with host 2 IP address and the port number 9988.

```
To see your aliases, enter "alias"
```

```
t3net04-41 ~ >: sock 10.10.201.12 9988
```

```
□
```

Step 5

The netstat -an is run by both of the workstations again following the sock command.

The new tcp connection is shown in Established state in the netstat table.

It also shows the Local address and the port number 9988 for the new TCP connection.

```
t3net04-42 ~ >: netstat -a -n
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp      0      0 0.0.0.0:111              0.0.0.0:*
tcp      0      0 192.168.122.1:53         0.0.0.0:*
tcp      0      0 0.0.0.0:22              0.0.0.0:*
tcp      0      0 127.0.0.1:631            0.0.0.0:*
tcp      0      0 127.0.0.1:25              0.0.0.0:*
tcp      0      0 10.10.201.13:986          10.10.201.3:2049    ESTABLISHED
tcp      0      0 10.10.201.13:47410        10.10.201.12:8899    ESTABLISHED
tcp      0      0 10.10.201.13:53404        10.10.201.12:9988    ESTABLISHED
tcp      0      0 10.10.201.13:51144        128.235.251.27:389   ESTABLISHED
tcp6     0      0 ::1:111                  ::*:*
tcp6     0      0 ::1:22                  ::*:*
tcp6     0      0 ::1:631                  ::*:*
tcp6     0      0 ::1:25                  ::*:*
udp      0      0 0.0.0.0:5353            0.0.0.0:*
udp      0      0 0.0.0.0:39028           0.0.0.0:*
udp      0      0 0.0.0.0:7001            0.0.0.0:*
udp      0      0 192.168.122.1:53         0.0.0.0:*
udp      0      0 0.0.0.0:67              0.0.0.0:*
udp      0      0 0.0.0.0:111             0.0.0.0:*
udp      0      0 127.0.0.1:323            0.0.0.0:*
udp6     0      0 ::1:111                  ::*:*
udp6     0      0 ::1:323                  ::*:*
raw6    0      0 ::::58                  ::*:*
raw6    0      0 ::::58                  ::*:*
```

Step 6

Host 1 logs out of the sock connection running with port = 9988 by pressing Control+C

```
To see your aliases, enter "alias"
```

```
t3net04-41 ~ >: sock 10.10.201.12 9988
^C
t3net04-42 ~ >: □
```

Step 7

Both hosts run the “netstat -a -n” command again

It is observed from the netstat -a -n command result below that the connection from Step 6 corresponding to the port number 9988 has a change in state.

The state has been changed to TIME_WAIT as Host 1 removed the connection By using Control+C in step 6.

```
t3net04-42 ~ >: netstat -a -n
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp      0      0 0.0.0.0:111              0.0.0.0:*
tcp      0      0 192.168.122.1:53         0.0.0.0:*
tcp      0      0 0.0.0.0:22              0.0.0.0:*
tcp      0      0 127.0.0.1:631            0.0.0.0:*
tcp      0      0 127.0.0.1:25              0.0.0.0:*
tcp      0      0 10.10.201.13:986          10.10.201.3:2049    ESTABLISHED
tcp      0      0 10.10.201.13:47410         10.10.201.12:8899    ESTABLISHED
tcp      0      0 10.10.201.13:53404         10.10.201.12:9988    TIME_WAIT
tcp      0      0 10.10.201.13:51144         128.235.251.27:389   ESTABLISHED
tcp6     0      0 ::1:111                  ::*:*
tcp6     0      0 ::1:22                   ::*:*
tcp6     0      0 ::1:631                  ::*:*
tcp6     0      0 ::1:25                   ::*:*
udp      0      0 0.0.0.0:5353             0.0.0.0:*
udp      0      0 0.0.0.0:39028            0.0.0.0:*
udp      0      0 0.0.0.0:7001            0.0.0.0:*
udp      0      0 192.168.122.1:53         0.0.0.0:*
udp      0      0 0.0.0.0:67              0.0.0.0:*
udp      0      0 0.0.0.0:111             0.0.0.0:*
udp      0      0 127.0.0.1:323            0.0.0.0:*
udp6     0      0 ::1:111                  ::*:*
udp6     0      0 ::1:323                  ::*:*
raw6    0      0 ::1:58                   ::*:*                7
raw6    0      0 ::1:58                   ::*:*                7

Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type      State     I-Node  Path
unix  2 [ ACC ]     STREAM   LISTENING  9727   /run/systemd/private
unix  2 [ ACC ]     STREAM   LISTENING  22492  /var/lib/sss/pipes/private/sbus-monitor
unix  2 [ ACC ]     STREAM   LISTENING  17045  /var/lib/sss/pipes/private/pam
unix  2 [ ACC ]     STREAM   LISTENING  5103030 @/tmp/dbus-sUJYjjtZzB
unix  2 [ ACC ]     STREAM   LISTENING  5095957 @/tmp/dbus-czKlaiuBwz
unix  2 [ ACC ]     STREAM   LISTENING  5041530 @/tmp/.X11-unix/X0
```

Step 8

Host 1 logouts from another sock connection on the 2nd console by pressing “ctrl” and “D” button at the same time.

```
To see your aliases, enter "alias"

t3net04-41 ~ >: sock 10.10.201.12 8899
connect() error: Connection refused
t3net04-42 ~ >: sock 10.10.201.12 8899
^C
t3net04-42 ~ >: sock 10.10.201.12 8899
connect() error: Connection refused
t3net04-42 ~ >: sock 10.10.201.12 8899
^C
t3net04-42 ~ >: sock 10.10.201.12 8899
t3net04-42 ~ >: █
```

Step 9

Both hosts run the “netstat -a -n” command again.

```
t3net04-43 ~ >: netstat -a -n
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 0.0.0.0:111              0.0.0.0:*
tcp      0      0 192.168.122.1:53          0.0.0.0:*
tcp      0      0 0.0.0.0:22              0.0.0.0:*
tcp      0      0 127.0.0.1:631             0.0.0.0:*
tcp      0      0 127.0.0.1:25              0.0.0.0:*
tcp      0      0 10.10.201.13:986            10.10.201.3:2049        ESTABLISHED
tcp      0      0 10.10.201.13:47410            10.10.201.12:8899        TIME_WAIT
tcp      0      0 10.10.201.13:51144            128.235.251.27:389        ESTABLISHED
tcp6     0      0 ::1:111                  ::*:*
tcp6     0      0 ::1:22                  ::*:*
tcp6     0      0 ::1:631                  ::*:*
tcp6     0      0 ::1:25                  ::*:*
udp      0      0 0.0.0.0:5353             0.0.0.0:*
udp      0      0 0.0.0.0:39028             0.0.0.0:*
udp      0      0 0.0.0.0:7001             0.0.0.0:*
udp      0      0 192.168.122.1:53             0.0.0.0:*
udp      0      0 0.0.0.0:67              0.0.0.0:*
udp      0      0 0.0.0.0:111             0.0.0.0:*
udp      0      0 127.0.0.1:323             0.0.0.0:*
udp6     0      0 ::1:111                  ::*:*
udp6     0      0 ::1:323                  ::*:*
raw6     0      0 ::::58                  ::*:*                7
raw6     0      0 ::::58                  ::*:*                7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type      State      I-Node      Path
unix      2  [ ACC ]      STREAM    LISTENING   9727      /run/systemd/private
```

It can be observed that the connection corresponding to the port number 8899 has the state changed to TIME_WAIT as the connections were closed in Step 8 by Host1.

The waiting times vary slightly but are generally close to one minute.

The various TCP states are established, and they all listen.

The term "established" implies to a successful connection between the server and the system. A port is open when it is listening on the same channel without being connected to a server.

B. Request Queue

My workstation is performing the role of Host 2.

In step 3, within 3s after Step 2b is performed, host 2 presses the command.

```
t3net04-42 ~ >: sock -v 10.10.201.12 9999
connected on 10.10.201.13.36930 to 10.10.201.12.9999
TCP_MAXSEG = 1448
□
```

In step 4, Within 3s after Step 2b is performed, host 2 presses "enter" to run the command.

```
t3net04-41 ~ >: sock -v 10.10.201.12 9999
connected on 10.10.201.13.36932 to 10.10.201.12.9999
TCP_MAXSEG = 1448
```

In Step 5,6,7 : Within 3s after Step 4 is performed, host 2 presses "enter" to run the "sock -v 9999" command on the 4th,5th and 6th console.

```
To see your aliases, enter "alias"
```

```
t3net04-41 ~ >: sock -v 10.10.201.12 9999
connected on 10.10.201.13.36934 to 10.10.201.12.9999
TCP_MAXSEG = 1448
```

```
To see your aliases, enter "alias"
```

```
t3net04-41 ~ >: sock -v 10.10.201.12 9999
connected on 10.10.201.13.36934 to 10.10.201.12.9999
TCP_MAXSEG = 1448
```

```
To see your aliases, enter "alias"
```

```
t3net04-41 ~ >: sock -v 10.10.201.12 9999
connected on 10.10.201.13.36934 to 10.10.201.12.9999
TCP_MAXSEG = 1448
```

Five sock commands are executed within 5 seconds

```
t3net04-41 ~ >: tcpdump host 10.10.201.13 and 10.10.201.12 and not host 128.235 -n -i plpl
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on plpl, link-type EN10MB (Ethernet), capture size 262144 bytes
[...]
19:41:23.224527 IP 10.10.201.13.36934 > 10.10.201.12.distinct: Flags [S], seq 3183789523, win 29200, options [mss 1460,sackOK,TS val 1232601173 ecr 0,nop,wscale 7], length 0
19:41:23.225195 IP 10.10.201.12.distinct > 10.10.201.13.36934: Flags [.], ack 3183789524, win 28960, options [mss 1460,sackOK,TS val 1831520774 ecr 1232601173,nop,wscale 7], length 0
19:41:23.225262 IP 10.10.201.13.36934 > 10.10.201.12.distinct: Flags [.], ack 1, win 229, options [nop,nop,TS val 1232601174 ecr 1831520774], length 0
19:41:24.583998 IP 10.10.201.13.36932 > 10.10.201.12.distinct: Flags [.], seq 1376160115, win 29200, options [mss 1460,sackOK,TS val 1232602532 ecr 0,nop,wscale 7], length 0
19:41:24.584668 IP 10.10.201.12.distinct > 10.10.201.13.36932: Flags [.], seq 2991295325, ack 1376160116, win 28960, options [mss 1460,sackOK,TS val 1831522134 ecr 1232602532,nop,wscale 7], length 0
19:41:24.584732 IP 10.10.201.13.36932 > 10.10.201.12.distinct: Flags [.], ack 1, win 229, options [nop,nop,TS val 1232602533 ecr 1831522134], length 0
19:41:25.334982 IP 10.10.201.13.36934 > 10.10.201.12.distinct: Flags [.], seq 1059284577, win 29200, options [mss 1460,sackOK,TS val 1232603283 ecr 0,nop,wscale 7], length 0
19:41:25.335554 IP 10.10.201.12.distinct > 10.10.201.13.36934: Flags [.], seq 2620615228, ack 1059284578, win 28960, options [mss 1460,sackOK,TS val 1831522885 ecr 1232603283,nop,wscale 7], length 0
19:41:25.335626 IP 10.10.201.13.36934 > 10.10.201.12.distinct: Flags [.], ack 1, win 229, options [nop,nop,TS val 1232603284 ecr 1831522885], length 0
19:41:26.167831 IP 10.10.201.13.36936 > 10.10.201.12.distinct: Flags [.], seq 2271422341, win 29200, options [mss 1460,sackOK,TS val 1232604116 ecr 0,nop,wscale 7], length 0
19:41:26.168389 IP 10.10.201.12.distinct > 10.10.201.13.36936: Flags [.], seq 3704487848, ack 2271422342, win 28960, options [mss 1460,sackOK,TS val 1831523717 ecr 1232604116,nop,wscale 7], length 0
19:41:26.168456 IP 10.10.201.13.36936 > 10.10.201.12.distinct: Flags [.], ack 1, win 229, options [nop,nop,TS val 1232604117 ecr 1831523717], length 0
19:41:26.208795 IP 10.10.201.13.36938 > 10.10.201.12.distinct: Flags [.], seq 3896037190, win 29200, options [mss 1460,sackOK,TS val 1232604756 ecr 0,nop,wscale 7], length 0
19:41:26.807736 IP 10.10.201.12.distinct > 10.10.201.13.36938: Flags [.], seq 3979756866, ack 3896037191, win 28960, options [mss 1460,sackOK,TS val 1831524357 ecr 1232604756,nop,wscale 7], length 0
19:41:26.807829 IP 10.10.201.13.36938 > 10.10.201.12.distinct: Flags [.], ack 1, win 229, options [nop,nop,TS val 1232604756 ecr 1831524357], length 0
19:41:26.807981 IP 10.10.201.12.distinct > 10.10.201.13.36938: Flags [.], seq 3979756866, ack 3896037191, win 28960, options [mss 1460,sackOK,TS val 1831525760 ecr 1232604756,nop,wscale 7], length 0
19:41:28.211066 IP 10.10.201.13.36938 > 10.10.201.12.distinct: Flags [.], ack 1, win 229, options [nop,nop,TS val 1232606160 ecr 1831524357], length 0
19:41:28.242374 ARP, Request who-has 10.10.201.13 tell 10.10.201.12, length 46
19:41:28.242406 ARP, Reply 10.10.201.13 is-at b4:96:91:52:32:2e, length 28
19:41:30.410728 IP 10.10.201.12.distinct > 10.10.201.13.36938: Flags [.], seq 3979756866, ack 3896037191, win 28960, options [mss 1460,sackOK,TS val 1831527960 ecr 1232606160,nop,wscale 7], length 0
19:41:30.410796 IP 10.10.201.13.36938 > 10.10.201.12.distinct: Flags [.], ack 1, win 229, options [nop,nop,TS val 1232608359 ecr 1831524357], length 0
19:41:34.610669 IP 10.10.201.12.distinct > 10.10.201.13.36938: Flags [.], seq 3979756866, ack 3896037191, win 28960, options [mss 1460,sackOK,TS val 1831532160 ecr 1232608359,nop,wscale 7], length 0
19:41:34.610704 IP 10.10.201.13.36938 > 10.10.201.12.distinct: Flags [.], ack 1, win 229, options [nop,nop,TS val 1232612559 ecr 1831524357], length 0
19:41:42.610562 IP 10.10.201.12.distinct > 10.10.201.13.36938: Flags [.], seq 3979756866, ack 3896037191, win 28960, options [mss 1460,sackOK,TS val 1831540160 ecr 1232612559,nop,wscale 7], length 0
19:41:42.610639 IP 10.10.201.13.36938 > 10.10.201.12.distinct: Flags [.], ack 1, win 229, options [nop,nop,TS val 1232620559 ecr 1831524357], length 0
]
```

TCP dump output corresponding to the experiment.

6.2.3 TCP interactive data flow and bulk data flow.

a. TCP interactive data flow

Host 1 observes tcpdump

```
t3net04-41 ~ >: tcpdump host 10.10.201.13 and host 10.10.201.12 and not host 128.235 -n -i plpl
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on plpl, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```

18:47:32.717549 IP 10.10.201.12.ssh > 10.10.201.13.46728: Flags [P.], seq 2850:2910, ack 2666, win 295, options [nop,nop,TS val 1828290266 ecr 1229370615], length 60
18:47:32.717614 IP 10.10.201.13.46728 > 10.10.201.12.ssh: Flags [.], ack 2910, win 291, options [nop,nop,TS val 1229370666 ecr 1828290266], length 0
18:47:32.730953 IP 10.10.201.12.ssh > 10.10.201.13.46728: Flags [P.], seq 2910:3018, ack 2666, win 295, options [nop,nop,TS val 1828290280 ecr 1229370666], length 108
18:47:32.730999 IP 10.10.201.13.46728 > 10.10.201.12.ssh: Flags [.], ack 3018, win 291, options [nop,nop,TS val 1229370680 ecr 1828290280], length 0
18:47:32.834924 IP 10.10.201.12.ssh > 10.10.201.13.46728: Flags [P.], seq 3018:3478, ack 2666, win 295, options [nop,nop,TS val 1828290384 ecr 1229370680], length 460

```

Step 2 Host 1 logins to a remote host (host 2) using SSH

```
t3net03-41 ~ >: ssh 10.10.201.12
ak2739@10.10.201.12's password: 
```

Step 4

Host 1 types “su” and presses the “enter” button.

```

ak2739@t3net03:~ - □ ×
File Edit View Search Terminal Help
18:15:12, Flags: FRA
AFS      : User's (AFS ID 520127) tokens for afs@cad.njit.edu [Expires Nov 8 0
4:15]

==== Start Python Information ====
1. The default python is Anaconda Python 3

2. To instead use Anaconda Python 2 :

echo 'module load python2' > ~/.modules

Then log out / log in
==== End Python Information ===

Loading [ python3.8 java18 firefox/104.0.2 ] modules ...
Currently Loaded Modulefiles:
 1) python3.8          2) java18/18.0.2.1   3) firefox/104.0.2

To see your aliases, enter "alias"

t3net03-41 ~ >: su
Password: 

```

Step 4

Host 1 types his AFS password.

Step 5

Host 1 uses “exit” to exit from host 2.

The entire packet length for each character is 72 packets.

The 72 packets are divided into two steps of 36 each, though.

The enter keypress consumes 40 packets of space.

```

18:16:20.788900 IP 10.10.201.13.43652 > 10.10.201.12.ssh: Flags [.], ack 4481, win 431, options [nop,nop,TS val 591900422 ecr 591898325], length 0
18:16:51.843097 IP 10.10.201.13.43652 > 10.10.201.12.ssh: Flags [P.], seq 1880:1916, ack 4481, win 431, options [nop,nop,TS val 591931476 ecr 591898325], length 36
18:16:51.882943 IP 10.10.201.12.ssh > 10.10.201.13.43652: Flags [.], ack 1916, win 295, options [nop,nop,TS val 591929419 ecr 591931476], length 0
18:16:52.739154 IP 10.10.201.13.43652 > 10.10.201.12.ssh: Flags [P.], seq 1916:1952, ack 4481, win 431, options [nop,nop,TS val 591932372 ecr 591929419], length 36
18:16:52.739737 IP 10.10.201.12.ssh > 10.10.201.13.43652: Flags [.], ack 1952, win 295, options [nop,nop,TS val 591932372 ecr 591932372], length 0
18:16:53.747119 IP 10.10.201.13.43652 > 10.10.201.12.ssh: Flags [P.], seq 1952:1988, ack 4481, win 431, options [nop,nop,TS val 591933388 ecr 59193276], length 36
18:16:53.747731 IP 10.10.201.12.ssh > 10.10.201.13.43652: Flags [.], ack 1988, win 295, options [nop,nop,TS val 591931284 ecr 591933380], length 0

```

b. TCP bulk data flow

```
t3net04-43 ~ >: tcpdump host 10.10.201.13 and host 10.10.201.12 and not host 128.235 -n -i p1p1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on p1p1, link-type EN10MB (Ethernet), capture size 262144 bytes
18:22:41.502488 IP 10.10.201.12.34420 > 10.10.201.13.cbt: Flags [S], seq 1961225178, win 29200, options [mss 1460,sackOK,TS val 592279038 ecr 0,nop,wscale 7], length 0
18:22:41.502584 IP 10.10.201.13 > 10.10.201.12: ICMP host 10.10.201.13 unreachable - admin prohibited, length 68
18:22:46.510403 ARP, Request who-has 10.10.201.12 tell 10.10.201.13, length 28
18:22:46.511007 ARP, Reply 10.10.201.12 is-at b4:96:91:51:cf:14, length 46
18:22:50.874877 IP 10.10.201.12.34422 > 10.10.201.13.cbt: Flags [S], seq 2886697370, win 29200, options [mss 1460,sackOK,TS val 592288410 ecr 0,nop,wscale 7], length 0
18:22:55.888158 ARP, Request who-has 10.10.201.13 tell 10.10.201.12, length 46
18:22:55.888188 ARP, Reply 10.10.201.13 is-at b4:96:91:52:32:2e, length 28
18:23:25.491175 IP 10.10.201.13.39848 > 10.10.201.12.cbt: Flags [S], seq 1278280446, win 29200, options [mss 1460,sackOK,TS val 592325124 ecr 0,nop,wscale 7], length 0
18:23:25.491810 IP 10.10.201.12.cbt > 10.10.201.13.39848: Flags [R.], seq 0, ack 1278280447, win 0, length 0
18:23:30.494526 ARP, Request who-has 10.10.201.12 tell 10.10.201.13, length 28
18:23:30.495135 ARP, Reply 10.10.201.12 is-at b4:96:91:51:cf:14, length 46
18:23:39.091705 IP 10.10.201.13.39850 > 10.10.201.12.cbt: Flags [S], seq 3965120657, win 29200, options [mss 1460,sackOK,TS val 592338725 ecr 0,nop,wscale 7], length 0
18:23:39.092105 IP 10.10.201.12.cbt > 10.10.201.13.39850: Flags [S.], seq 2512217384, ack 3965120658, win 28960, options [mss 1460,sackOK,TS val 592336628 ecr 592338725,nop,wscale 7], length 0
18:23:39.092178 IP 10.10.201.13.39850 > 10.10.201.12.cbt: Flags [S.], ack 1, win 229, options [nop,nop,TS val 592338725 ecr 592336628], length 0
18:23:39.092433 IP 10.10.201.13.39850 > 10.10.201.12.cbt: Flags [P.], seq 1:1025, ack 1, win 229, options [nop,nop,TS val 592338726 ecr 592336628], length 1024
18:23:39.092523 IP 10.10.201.13.39850 > 10.10.201.12.cbt: Flags [S.], seq 1825:2473, ack 1, win 229, options [nop,nop,TS val 592338726 ecr 592336628], length 1448
18:23:39.092572 IP 10.10.201.13.39850 > 10.10.201.12.cbt: Flags [S.], seq 2473:3921, ack 1, win 229, options [nop,nop,TS val 592338726 ecr 592336628], length 1448
18:23:39.092633 IP 10.10.201.13.39850 > 10.10.201.12.cbt: Flags [S.], seq 3921:5369, ack 1, win 229, options [nop,nop,TS val 592338726 ecr 592336628], length 1448
18:23:39.092678 IP 10.10.201.13.39850 > 10.10.201.12.cbt: Flags [S.], seq 5369:6817, ack 1, win 229, options [nop,nop,TS val 592338726 ecr 592336628], length 1448
18:23:39.092691 IP 10.10.201.12.cbt > 10.10.201.13.39850: Flags [S.], ack 1025, win 243, options [nop,nop,TS val 592336629 ecr 592338726], length 0
18:23:39.092750 IP 10.10.201.13.39850 > 10.10.201.12.cbt: Flags [P.], seq 6817:7169, ack 1, win 229, options [nop,nop,TS val 592338726 ecr 592336629], length 352
18:23:39.092763 IP 10.10.201.12.cbt > 10.10.201.13.39850: Flags [S.], ack 3921, win 288, options [nop,nop,TS val 592336629 ecr 592338726], length 0
18:23:39.092915 IP 10.10.201.12.cbt > 10.10.201.13.39850: Flags [S.], ack 6817, win 333, options [nop,nop,TS val 592336629 ecr 592338726], length 0
18:23:39.092944 IP 10.10.201.13.39850 > 10.10.201.12.cbt: Flags [S.], seq 7169:12961, ack 1, win 229, options [nop,nop,TS val 592338726 ecr 592336629], length 5792
18:23:39.093068 IP 10.10.201.12.cbt > 10.10.201.13.39850: Flags [S.], ack 7169, win 356, options [nop,nop,TS val 592336629 ecr 592338726], length 0
18:23:39.093138 IP 10.10.201.13.39850 > 10.10.201.12.cbt: Flags [S.], seq 12961:14409, ack 1, win 229, options [nop,nop,TS val 592338726 ecr 592336629], length 1448
18:23:39.093149 IP 10.10.201.13.39850 > 10.10.201.12.cbt: Flags [P.], seq 14409:18433, ack 1, win 229, options [nop,nop,TS val 592338726 ecr 592336629], length 4024
18:23:39.093213 IP 10.10.201.13.39850 > 10.10.201.12.cbt: Flags [F.], seq 18433:20481, ack 1, win 229, options [nop,nop,TS val 592338726 ecr 592336629], length 2048
18:23:39.093240 IP 10.10.201.12.cbt > 10.10.201.13.39850: Flags [S.], ack 12961, win 446, options [nop,nop,TS val 592336629 ecr 592338726], length 0
18:23:39.093452 IP 10.10.201.12.cbt > 10.10.201.13.39850: Flags [S.], ack 18433, win 532, options [nop,nop,TS val 592336629 ecr 592338726], length 0
18:23:39.093496 IP 10.10.201.12.cbt > 10.10.201.13.39850: Flags [S.], ack 20482, win 564, options [nop,nop,TS val 592336629 ecr 592338726], length 0
18:23:39.093798 IP 10.10.201.12.cbt > 10.10.201.13.39850: Flags [F.], seq 1, ack 20482, win 564, options [nop,nop,TS val 592336630 ecr 592338726], length 0
18:23:39.093843 IP 10.10.201.13.39850 > 10.10.201.12.cbt: Flags [S.], ack 2, win 229, options [nop,nop,TS val 592338727 ecr 592336630], length 0
18:23:44.095900 ARP, Request who-has 10.10.201.13 tell 10.10.201.12, length 46
18:23:44.095928 ARP, Reply 10.10.201.13 is-at b4:96:91:52:32:2e, length 28
```

Step 2

Host 1 runs the “sock -v -i -s 7777” command to serve as a sink server.

```
To see your aliases, enter "alias"
t3net04-41 ~ >: sock -v -i -s 7777
^C
t3net04-42 ~ >: sock -v -i -n20 10.10.201.12 7777
connect() error: Connection refused
t3net04-43 ~ >: sock -v -i -n20 10.10.201.12 7777
connected on 10.10.201.13.39850 to 10.10.201.12.7777
TCP_MAXSEG = 1448
wrote 1024 bytes
t3net04-43 ~ >: □
```

Step 4

```

t3net04-41 ~ >: tcpdump host 10.10.201.13 and host 10.10.201.12 and not host 128.235 -n -i plpl1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on plpl1, link-type EN10MB (Ethernet), capture size 262144 bytes
18:30:24.033341 IP 10.10.201.13.58148 > 10.10.201.12.intervise: Flags [S], seq 3269135257, win 29200, options [mss 1460,sackOK,TS val 592743666 ecr 0,nop,wscale 7], length 0
18:30:24.033982 IP 10.10.201.12.intervise > 10.10.201.13.58148: Flags [S.], seq 2781804279, ack 3269135256, win 28960, options [mss 1460,sackOK,TS val 592741570 ecr 592743666,nop,wscale 7], length 0
18:30:24.034059 IP 10.10.201.13.58148 > 10.10.201.12.intervise: Flags [.], ack 1, win 229, options [nop,nop,TS val 592743667 ecr 592741570], length 0
18:30:24.034324 IP 10.10.201.13.58148 > 10.10.201.12.intervise: Flags [P.], seq 1:1025, ack 1, win 229, options [nop,nop,TS val 592743668 ecr 592741570], length 1024
18:30:24.034409 IP 10.10.201.13.58148 > 10.10.201.12.intervise: Flags [.], seq 1025:2473, ack 1, win 229, options [nop,nop,TS val 592743668 ecr 592741570], length 1448
18:30:24.034460 IP 10.10.201.13.58148 > 10.10.201.12.intervise: Flags [.], seq 2473:3921, ack 1, win 229, options [nop,nop,TS val 592743668 ecr 592741570], length 1448
18:30:24.034514 IP 10.10.201.12.intervise > 10.10.201.13.58148: Flags [.], ack 1025, win 243, options [nop,nop,TS val 592741570 ecr 592743668], length 0
18:30:24.034579 IP 10.10.201.13.58148 > 10.10.201.12.intervise: Flags [P.], seq 3921:5121, ack 1, win 229, options [nop,nop,TS val 592743668 ecr 592741570], length 1200
18:30:24.034651 IP 10.10.201.13.58148 > 10.10.201.12.intervise: Flags [.], seq 5121:6569, ack 1, win 229, options [nop,nop,TS val 592743668 ecr 592741570], length 1448
18:30:24.034741 IP 10.10.201.12.intervise > 10.10.201.13.58148: Flags [.], ack 3921, win 288, options [nop,nop,TS val 592741571 ecr 592743668], length 0
18:30:24.034793 IP 10.10.201.13.58148 > 10.10.201.12.intervise: Flags [.], seq 6569:8017, ack 1, win 229, options [nop,nop,TS val 592743668 ecr 592741571], length 1448
18:30:24.034802 IP 10.10.201.12.intervise > 10.10.201.13.58148: Flags [.], ack 5121, win 311, options [nop,nop,TS val 592741571 ecr 592743668], length 0
18:30:24.034824 IP 10.10.201.13.58148 > 10.10.201.12.intervise: Flags [.], seq 8017:9465, ack 1, win 229, options [nop,nop,TS val 592743668 ecr 592741571], length 1448
18:30:24.034826 IP 10.10.201.12.intervise > 10.10.201.13.58148: Flags [.], ack 6569, win 333, options [nop,nop,TS val 592741571 ecr 592743668], length 0
18:30:24.034859 IP 10.10.201.13.58148 > 10.10.201.12.intervise: Flags [P.], seq 9465:10241, ack 1, win 229, options [nop,nop,TS val 592743668 ecr 592741571], length 776
18:30:24.035064 IP 10.10.201.13.58148 > 10.10.201.12.intervise: Flags [.], seq 10241:16033, ack 1, win 229, options [nop,nop,TS val 592743668 ecr 592741571], length 5792
18:30:24.035157 IP 10.10.201.12.intervise > 10.10.201.13.58148: Flags [.], ack 9465, win 378, options [nop,nop,TS val 592741571 ecr 592743668], length 0
18:30:24.035209 IP 10.10.201.13.58148 > 10.10.201.12.intervise: Flags [.], seq 16033:20377, ack 1, win 229, options [nop,nop,TS val 592743668 ecr 592741571], length 4344
18:30:24.035224 IP 10.10.201.12.intervise > 10.10.201.13.58148: Flags [.], ack 10241, win 401, options [nop,nop,TS val 592741571 ecr 592743668], length 0
18:30:24.035236 IP 10.10.201.13.58148 > 10.10.201.12.intervise: Flags [FP.], seq 20377:20481, ack 1, win 229, options [nop,nop,TS val 592743668 ecr 592741571], length 184
18:30:24.035414 IP 10.10.201.12.intervise > 10.10.201.13.58148: Flags [.], ack 16033, win 492, options [nop,nop,TS val 592741571 ecr 592743668], length 0
18:30:24.035613 IP 10.10.201.12.intervise > 10.10.201.13.58148: Flags [.], ack 20482, win 561, options [nop,nop,TS val 592741572 ecr 592743668], length 0
18:30:24.035725 IP 10.10.201.12.intervise > 10.10.201.13.58148: Flags [F.], seq 1, ack 20482, win 561, options [nop,nop,TS val 592741572 ecr 592743668], length 0
18:30:24.035764 IP 10.10.201.13.58148 > 10.10.201.12.intervise: Flags [.], ack 2, win 229, options [nop,nop,TS val 592743669 ecr 592741572], length 0
18:30:29.038394 ARP, Request who-has 10.10.201.12 tell 10.10.201.13, length 28
18:30:29.039045 ARP, Reply 10.10.201.12 is-at b4:96:91:51:cf:14, length 46

```

□

c. Urgent data.

To see your aliases, enter "alias"

```

t3net04-41 ~ >: sock -v -i -n3 -U1 10.10.201.12 5555
connect() error: Connection refused
t3net04-42 ~ >: sock -v -i -n3 -U1 10.10.201.12 5555
connected on 10.10.201.13.51380 to 10.10.201.12.5555
TCP_MAXSEG = 1448
wrote 1 byte of urgent data
wrote 1024 bytes
wrote 1024 bytes
wrote 1024 bytes
t3net04-42 ~ >: sock -v -i -n3 -U1 10.10.201.12 5555
connect() error: Connection refused
t3net04-42 ~ >: sock -v -i -n3 -U1 10.10.201.12 5555
connect() error: Connection refused
t3net04-42 ~ >: sock -v -i -n3 -U1 10.10.201.12 5555
connected on 10.10.201.13.51386 to 10.10.201.12.5555
TCP_MAXSEG = 1448
wrote 1 byte of urgent data
wrote 1024 bytes
wrote 1024 bytes
wrote 1024 bytes
t3net04-42 ~ >: sock -v -i -n3 -U1 10.10.201.12 5555
connected on 10.10.201.13.51390 to 10.10.201.12.5555
TCP_MAXSEG = 1448
wrote 1 byte of urgent data
wrote 1024 bytes
wrote 1024 bytes
wrote 1024 bytes
t3net04-42 ~ >: □

```

d. TCP repacketization

```

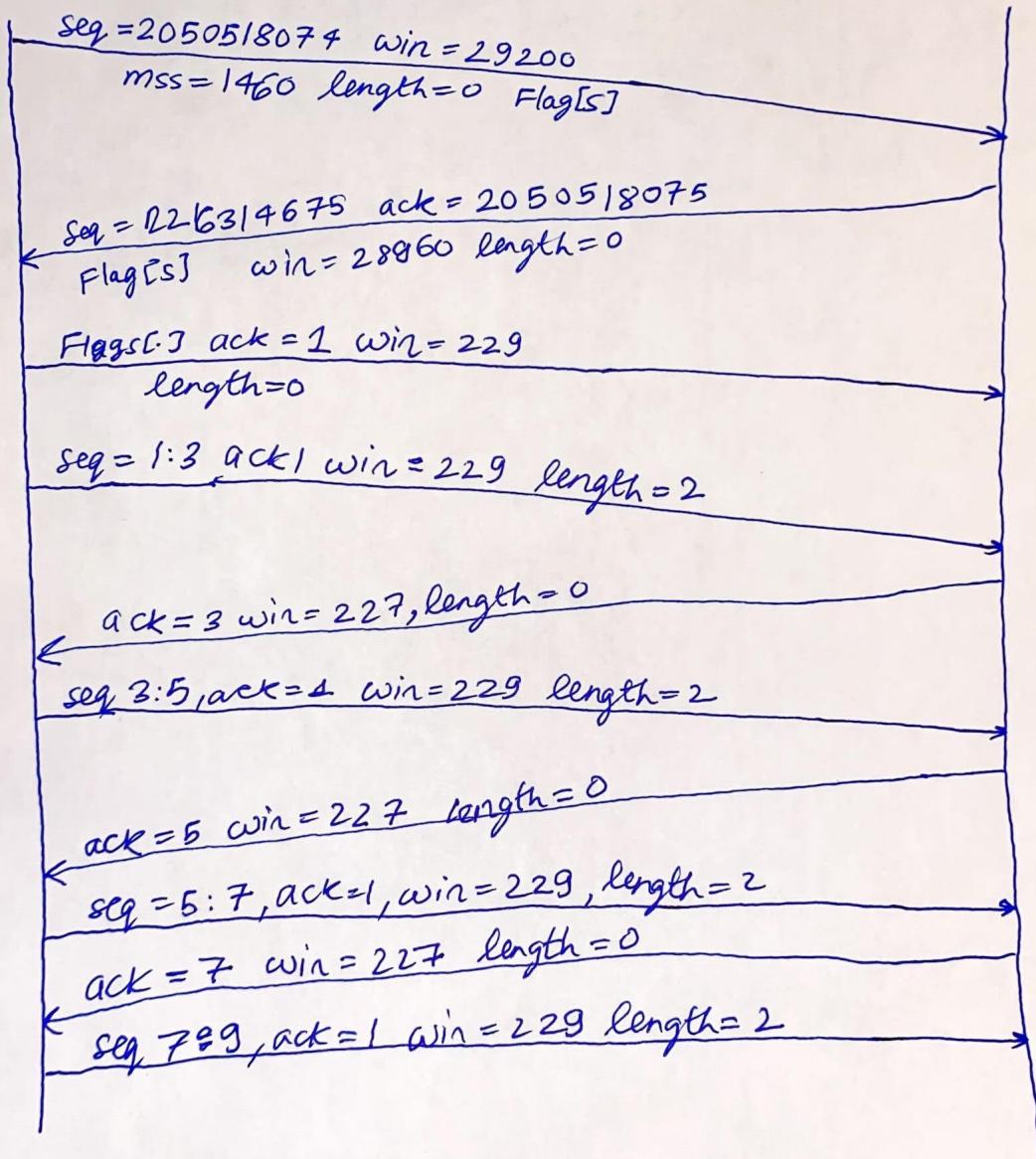
t3net04-41 ~ >: sock -v -i -n3 -U1 10.10.201.12 5555
connect() error: Connection refused
t3net04-42 ~ >: sock -v -i -n3 -U1 10.10.201.12 5555
connected on 10.10.201.13.51380 to 10.10.201.12.5555
TCP_MAXSEG = 1448
wrote 1 byte of urgent data
wrote 1024 bytes
wrote 1024 bytes
wrote 1024 bytes
t3net04-42 ~ >: sock -v -i -n3 -U1 10.10.201.12 5555
connect() error: Connection refused
t3net04-42 ~ >: sock -v -i -n3 -U1 10.10.201.12 5555
connect() error: Connection refused
t3net04-42 ~ >: sock -v -i -n3 -U1 10.10.201.12 5555
connected on 10.10.201.13.51386 to 10.10.201.12.5555
TCP_MAXSEG = 1448
wrote 1 byte of urgent data
wrote 1024 bytes
wrote 1024 bytes
wrote 1024 bytes
t3net04-42 ~ >: sock -v -i -n3 -U1 10.10.201.12 5555
connected on 10.10.201.13.51390 to 10.10.201.12.5555
TCP_MAXSEG = 1448
wrote 1 byte of urgent data
wrote 1024 bytes
wrote 1024 bytes
wrote 1024 bytes
t3net04-42 ~ >: clear
t3net04-43 ~ >: sock 10.10.201.12 9999
1
2
3
4
1
2
3
4
^C
t3net04-44 ~ >: □

t3net04-42 ~ >: clear
t3net04-43 ~ >: tcpdump host 10.10.201.12 and host 10.10.201.13 and not host 128.235 -n -i pip1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on pip1, link-type EN10MB (Ethernet), capture size 262144 bytes
18:51:11.305238 IP 10.10.201.13.54966 > 10.10.201.12.distinct: Flags [S], seq 2050518074, win 29200, options [mss 1460,sackOK,TS val 593990938 ecr 0,nop,wscale 7], length 0
18:51:11.305572 IP 10.10.201.12.distinct > 10.10.201.13.54966: Flags [S.], seq 2216314675, ack 2050518075, win 28960, options [mss 1460,sackOK,TS val 225857 ecr 593990938,nop,wscale 7], length 0
18:51:11.305655 IP 10.10.201.13.54966 > 10.10.201.12.distinct: Flags [.], ack 1, win 229, options [nop,nop,TS val 593990939 ecr 225857], length 0
18:51:16.312535 ARP, Request who-has 10.10.201.13 tell 10.10.201.12, length 46
18:51:16.312586 ARP, Reply 10.10.201.13 is-at b4:96:91:52:32:2e, length 28
18:51:18.998045 IP 10.10.201.12.distinct: Flags [P.], seq 1:3, ack 1, win 229, options [nop,nop,TS val 593998831 ecr 225857], length 2
18:51:18.998374 IP 10.10.201.12.distinct > 10.10.201.13.54966: Flags [.], ack 3, win 227, options [nop,nop,TS val 233550 ecr 593998831], length 0
18:51:28.133899 IP 10.10.201.13.54966 > 10.10.201.12.distinct: Flags [P.], seq 3:5, ack 1, win 229, options [nop,nop,TS val 593999767 ecr 233550], length 2
18:51:28.134480 IP 10.10.201.12.distinct > 10.10.201.13.54966: Flags [.], ack 5, win 227, options [nop,nop,TS val 234686 ecr 593999767], length 0
18:51:23.861445 IP 10.10.201.13.54966 > 10.10.201.12.distinct: Flags [P.], seq 5:7, ack 1, win 229, options [nop,nop,TS val 594003495 ecr 234686], length 2
18:51:23.862059 IP 10.10.201.12.distinct > 10.10.201.13.54966: Flags [.], ack 7, win 227, options [nop,nop,TS val 238413 ecr 594003495], length 0
18:51:25.829977 IP 10.10.201.13.54966 > 10.10.201.12.distinct: Flags [P.], seq 7:9, ack 1, win 229, options [nop,nop,TS val 594005463 ecr 238413], length 2
18:51:25.830574 IP 10.10.201.12.distinct > 10.10.201.13.54966: Flags [.], ack 9, win 227, options [nop,nop,TS val 594005463], length 0
18:52:01.237724 IP 10.10.201.13.54966 > 10.10.201.12.distinct: Flags [P.], seq 9:11, ack 1, win 229, options [nop,nop,TS val 594040871 ecr 240382], length 2
18:52:01.640308 IP 10.10.201.13.54966 > 10.10.201.12.distinct: Flags [P.], seq 9:11, ack 1, win 229, options [nop,nop,TS val 594041872 ecr 240382], length 2
18:52:02.043643 IP 10.10.201.13.54966 > 10.10.201.12.distinct: Flags [P.], seq 9:11, ack 1, win 229, options [nop,nop,TS val 594041274 ecr 240382], length 2
18:52:02.856633 IP 10.10.201.12.distinct > 10.10.201.13.54966: Flags [.], seq 9:11, ack 1, win 229, options [nop,nop,TS val 594042484 ecr 240382], length 2
18:52:04.462634 IP 10.10.201.13.54966 > 10.10.201.12.distinct: Flags [P.], seq 9:11, ack 1, win 229, options [nop,nop,TS val 594044496 ecr 240382], length 2
18:52:06.254499 ARP, Request who-has 10.10.201.12 tell 10.10.201.13, length 28
18:52:07.256447 ARP, Request who-has 10.10.201.12 tell 10.10.201.13, length 28
18:52:07.686380 IP 10.10.201.13.54966 > 10.10.201.12.distinct: Flags [P.], seq 9:11, ack 1, win 229, options [nop,nop,TS val 594047320 ecr 240382], length 2
18:52:08.258618 ARP, Request who-has 10.10.201.12 tell 10.10.201.13, length 28
18:52:14.126549 ARP, Request who-has 10.10.201.12 tell 10.10.201.13, length 28
18:52:14.937824 IP 10.10.201.13.54966 > 10.10.201.12.distinct: Flags [P.], seq 9:11, ack 1, win 229, options [nop,nop,TS val 594053760 ecr 240382], length 2
18:52:14.937268 ARP, Reply 10.10.201.13 is-at b4:96:91:52:32:2e, length 28
18:52:14.937394 IP 10.10.201.12.distinct > 10.10.201.13.54966: Flags [.], ack 11, win 227, options [nop,nop,TS val 289489 ecr 594053760], length 0
18:52:14.937459 IP 10.10.201.13.54966 > 10.10.201.12.distinct: Flags [P.], seq 11:17, ack 1, win 229, options [nop,nop,TS val 594054571 ecr 289489], length 6
18:52:14.937663 IP 10.10.201.12.distinct > 10.10.201.13.54966: Flags [.], ack 17, win 227, options [nop,nop,TS val 289489 ecr 594054571], length 0
18:52:17.909844 IP 10.10.201.13.54966 > 10.10.201.12.distinct: Flags [F.], seq 17, ack 1, win 229, options [nop,nop,TS val 594057543 ecr 289489], length 0
18:52:17.910519 IP 10.10.201.12.distinct > 10.10.201.13.54966: Flags [F.], seq 1, ack 18, win 227, options [nop,nop,TS val 292462 ecr 594057543], length 0
18:52:17.910575 IP 10.10.201.13.54966 > 10.10.201.12.distinct: Flags [.], ack 2, win 229, options [nop,nop,TS val 594057544 ecr 292462], length 0
□

```

10.10.201.13

10.10.201.12



e. TCP segment

To see your aliases, enter "alias"

```
t3net04-41 ~ >: sock -v -i -n1 -wN 10.10.201.12 8899
connected on 10.10.201.13.34994 to 10.10.201.12.8899
TCP_MAXSEG = 1448
Wrote 0 bytes
t3net04-42 ~ >: 
```

```
To see your aliases, enter "alias"
```

```
t3net04-41 ~ >: tcpdump host 10.10.201.13 and host 10.10.201.12 and not host 128.235 -n -i plp1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on plp1, link-type EN10MB (Ethernet), capture size 262144 bytes
18:58:04.969496 IP 10.10.201.13.34994 > 10.10.201.12.ospf-lite: Flags [S], seq 3014100654, win 29200, options [mss 1460,sackOK,TS val 594404603 ecr 0,nop,wscale 7], length 0
18:58:04.970037 IP 10.10.201.12.ospf-lite > 10.10.201.13.34994: Flags [S.], seq 2983004982, ack 3014100655, win 28960, options [mss 1460,sackOK,TS val 639521 ecr 594404603,nop,wscale 7], length 0
18:58:04.970125 IP 10.10.201.13.34994 > 10.10.201.12.ospf-lite: Flags [.], ack 1, win 229, options [nop,nop,TS val 594404603 ecr 639521], length 0
18:58:04.970405 IP 10.10.201.13.34994 > 10.10.201.12.ospf-lite: Flags [F.], seq 1, ack 1, win 229, options [nop,nop,TS val 594404604 ecr 639521], length 0
18:58:04.970717 IP 10.10.201.12.ospf-lite > 10.10.201.13.34994: Flags [F.], seq 1, ack 2, win 227, options [nop,nop,TS val 639522 ecr 594404604], length 0
18:58:04.970782 IP 10.10.201.13.34994 > 10.10.201.12.ospf-lite: Flags [.], ack 2, win 229, options [nop,nop,TS val 594404604 ecr 639522], length 0
18:58:09.976213 ARP, Request who-has 10.10.201.13 tell 10.10.201.12, length 46
18:58:09.976259 ARP, Reply 10.10.201.13 is-at b4:96:91:52:32:2e, length 28
```

No, there is no fragmentation, and 7008 bytes are sent at once. because the network layer does not contain TCP.

f. TCP sliding window and delayed acknowledgment

```
t3net04-43 ~ >: sock -nl -w29200 10.10.201.12 7771
t3net04-43 ~ >: sock -nl -w29200 10.10.201.12 7771
^C
t3net04-44 ~ >: sock -nl -wl1680 10.10.201.12 7771
^C
t3net04-43 ~ >: sock -nl -w29200 10.10.201.12 7771
^C
t3net04-44 ~ >: sock -nl -wl1680 10.10.201.12 7771
^C
t3net04-45 ~ >: sock -nl -wl1680 10.10.201.12 7771
^C

S val 595744464 ecr 1979382], length 0
19:20:29.838599 ARP, Request who-has 10.10.201.12 tell 10.10.201.13, length 28
19:20:29.838865 ARP, Reply 10.10.201.12 is-at b4:96:91:51:cf:14, length 46
19:20:34.681918 IP 10.10.201.13.59668 > 10.10.201.12.7771: Flags [F.], seq 1, ack 1, win 229, options [nop,nop,TS val 595754315 ecr 1979382], length 0
19:20:34.682475 IP 10.10.201.12.7771 > 10.10.201.13.59668: Flags [F.], seq 1, ack 2, win 227, options [nop,nop,TS val 1989234 ecr 595754315], length 0
19:20:34.682498 IP 10.10.201.13.59668 > 10.10.201.12.7771: Flags [.], ack 2, win 229, options [nop,nop,TS val 595754316 ecr 1989234], length 0
19:20:55.214170 IP 10.10.201.13.59670 > 10.10.201.12.7771: Flags [S], seq 1552773319, win 29200, options [mss 1460,sackOK,TS val 595774847 ecr 0,nop,wscale 7], length 0
19:20:55.214831 IP 10.10.201.12.7771 > 10.10.201.13.59670: Flags [S.], seq 3075996369, ack 1552773320, win 28960, options [mss 1460,sackOK,TS val 2009766 ecr 595774847,nop,wscale 7], length 0
19:20:55.214892 IP 10.10.201.13.59670 > 10.10.201.12.7771: Flags [.], ack 1, win 229, options [nop,nop,TS val 595774848 ecr 2009766], length 0
```

The packets are immediately retransmitted when there is a delay in acknowledgement.