

# Comp 8005 Port Forwarder

Mat Siwoski  
Shane Spoor

# Notes:

## Running the application:

To run the application, navigate to the folder that the script was installed to and type:

```
sudo python3 main.py
```

In the event that the file does not run:

```
chmod +x main.py
```

```
chmod +x main.py
```

to ensure that the file can be executed.

## Requirements:

Design and implement a port forwarding server that will forward incoming connection requests to specific ports/services from any IP address, to any user-specified IP address and port. For example, an inbound connection from 192.168.1.5 to port 80 may be forwarded to 192.168.1.25, port 80, or to 192.168.1.25, port 8005.

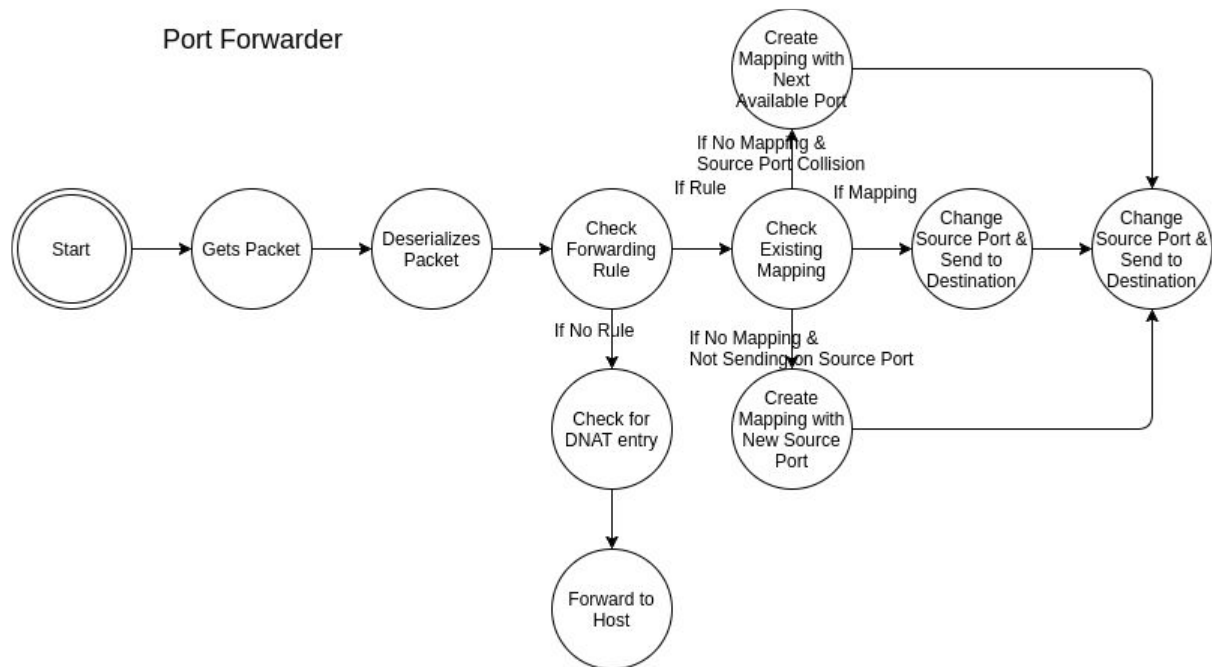
## Constraints:

Your forwarder must provide the following minimum functionality:

- Forward any IP: port pair to any other user-specified IP: port pair.
- The application must support multiple inbound connection requests, as well as simultaneous two-way traffic.
- Only TCP connections will be forwarded by the basic implementation.
- You are required to provide a detailed test case that will document the complete functionality of the port forwarding application. For example, beyond the basic functionality tests you may want to test and see how well your application performs under a heavy load, i.e., heavy throughput from multiple clients.
- Your application will read the IP: port combinations to forward to from a separate configuration file. As always additional work and features will be considered for bonus marks.
- For example, a very useful feature would be to use SSL sockets

# Design:

## Design Diagrams



## Pseudocode:

main.py

main()

Open forwarding rules

While True

Set up connection

If snat entry in snat table

New src port = snat\_table [snat entry]

Else if dnat entry not in dnat table

Dnat table = src ip and src port

Snat table = tcp port

New src port = tcp port

Else

While true

Possible port = random port

Possible dnat = forward ip & port

If not in dnat table

Srcport = possible port

Update dnat/snat table

```
        Forward ip/port = ip/port from rules
        Set up new connection to forward too
    Else
        Destination header = ip/port
        If dnat entry not in table
            Set up destination entry to send back to
```

Ip.py

```
Def __str__
    Print out data
Def get_flags_string
    Print out flags
Def __init__
    Define initial data
```

Tcp.py

```
Def __str__
    Print out data
Def get_flags_string
    Print out flags
Def __init__
    Define initial data
```

# Test Results:

## 1.) Handle Exiting

```
maciu@Maciu: ~/Desktop/School/C8005/Final/COMP8005-Final
maciu@Maciu:~/Desktop/School/C8005/Final/COMP8005-Final$ sudo ./main.py
^C
Exiting
maciu@Maciu:~/Desktop/School/C8005/Final/COMP8005-Final$
```

## 2.) Traffic passing through Port Forwarder

```

    flags: DF
    fragment offset: MF flag not set
    TTL: 64
    protocol: 6
    header checksum: 63768
    source IP: 192.168.0.6
    destination IP: 192.168.0.7
    has options? : no

TCP header contents:
    source port: 22
    destination port: 57462
    sequence number: 3642467590
    ack number: 0
    flags: RST
    data offset: 20
    window size: 0
    checksum: 53203
    urgent pointer: URG flag not set
    has options? False

IP header contents:
    IP version: 4
    header length: 20
    service type: 0
    total len: 40
    identification: 49242
    flags: DF
    fragment offset: MF flag not set
    TTL: 64
    protocol: 6
    header checksum: 63767
    source IP: 192.168.0.6
    destination IP: 192.168.0.7
    has options? : no

```

No.	Time	Source	Destination	Protocol	Length	Info
2654	2017-03-07 19:04:31.674988547	192.168.0.7	192.168.0.9	TCP	230	[TCP Retransmission] 22->57462 [PSH, ACK] Seq=3642467053 Ack=3921491007 Win=34816 Len=164 TSval=2529468
2655	2017-03-07 19:04:31.675112072	192.168.0.7	192.168.0.9	TCP	102	[TCP Retransmission] 22->57462 [PSH, ACK] Seq=3642467217 Ack=3921491007 Win=34816 Len=36 TSval=2529468
2656	2017-03-07 19:04:31.675252811	192.168.0.7	192.168.0.9	TCP	246	[TCP Retransmission] 22->57462 [PSH, ACK] Seq=3642467253 Ack=3921491007 Win=34816 Len=180 TSval=2529468
2657	2017-03-07 19:04:31.675293976	192.168.0.9	192.168.0.7	TCP	66	57462->22 [ACK] Seq=3921491007 Ack=3642467217 Win=40064 Len=0 TSval=2302825 TSecr=2529468
2658	2017-03-07 19:04:31.675304242	192.168.0.9	192.168.0.7	TCP	66	57462->22 [ACK] Seq=3921491007 Ack=3642467253 Win=40064 Len=0 TSval=2302825 TSecr=2529468
2659	2017-03-07 19:04:31.675416777	192.168.0.7	192.168.0.9	TCP	102	[TCP Retransmission] 22->57462 [PSH, ACK] Seq=3642467433 Ack=3921491007 Win=34816 Len=36 TSval=2529468
2660	2017-03-07 19:04:31.675451159	192.168.0.9	192.168.0.7	TCP	66	57462->22 [ACK] Seq=3921491007 Ack=3642467433 Win=42240 Len=0 TSval=2302825 TSecr=2529468
2665	2017-03-07 19:04:31.675635824	192.168.0.9	192.168.0.7	TCP	66	57462->22 [ACK] Seq=3921491007 Ack=3642467469 Win=42240 Len=0 TSval=2302825 TSecr=2529468
2666	2017-03-07 19:04:31.675730963	192.168.0.7	192.168.0.9	TCP	126	[TCP Retransmission] 22->57462 [PSH, ACK] Seq=3642467468 Ack=3921491007 Win=34816 Len=60 TSval=2529468
2669	2017-03-07 19:04:31.675988316	192.168.0.7	192.168.0.9	TCP	126	[TCP Retransmission] 22->57462 [PSH, ACK] Seq=3642467529 Ack=3921491007 Win=34816 Len=60 TSval=2529468
2670	2017-03-07 19:04:31.675956627	192.168.0.9	192.168.0.7	TCP	66	57462->22 [ACK] Seq=3921491007 Ack=3642467529 Win=42240 Len=0 TSval=2302826 TSecr=2529469
2672	2017-03-07 19:04:31.676105838	192.168.0.9	192.168.0.7	TCP	66	57462->22 [ACK] Seq=3921491007 Ack=3642467589 Win=42240 Len=0 TSval=2302826 TSecr=2529469
2747	2017-03-07 19:04:56.242179321	192.168.0.7	192.168.0.9	TCP	66	[TCP Spurious Retransmission] 22->57462 [FIN, ACK] Seq=3642467589 Ack=3921491007 Win=34816 Len=0 TSval=2554035
2748	2017-03-07 19:04:56.242677459	192.168.0.9	192.168.0.7	SSHv2	126	Client: Encrypted packet (len=60)
2749	2017-03-07 19:04:56.242776392	192.168.0.9	192.168.0.7	TCP	66	57462->22 [FIN, ACK] Seq=3921491067 Ack=3642467590 Win=42240 Len=0 TSval=2327392 TSecr=2554035
2750	2017-03-07 19:04:56.242795587	192.168.0.7	192.168.0.9	TCP	54	22->57462 [RST] Seq=3642467590 Win=0 Len=0
2755	2017-03-07 19:04:56.244150918	192.168.0.7	192.168.0.9	TCP	54	22->57462 [RST] Seq=3642467590 Win=0 Len=0
2756	2017-03-07 19:04:56.244536141	192.168.0.7	192.168.0.9	TCP	54	22->57462 [RST] Seq=3642467590 Win=0 Len=0

Frame 2750: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0  
Ethernet II, Src: Dell dc:f3:9b (98:90:96:dc:f3:9b), Dst: Dell d5:84:7b (98:90:96:d5:84:7b)  
Internet Protocol Version 4, Src: 192.168.0.7, Dst: 192.168.0.9  
Transmission Control Protocol, Src Port: 22, Dst Port: 57462, Seq: 3642467590, Len: 0

Source Port: 22  
Destination Port: 57462  
[Stream index: 11]  
[TCP Segment Len: 0]  
Sequence number: 3642467590  
Acknowledgment number: 0  
Header Length: 20 bytes

```

0000  98 90 96 d5 84 7b 98 90  96 dc f3 9b 08 00 45 10  .....E.
0010  00 28 15 cf 40 00 40 06  a3 90 c0 a8 00 07 c0 a8  ...@.@.....
0020  00 09 00 16 e0 76 d9 1b  a5 06 00 00 00 00 50 04  ....V.....P.
0030  00 00 cf d0 00 00

```

### 3.) Multiple hosts connected to Port Forwarder

```
root@datacomm:~/COMP8005-Final
File Edit View Search Terminal Help
destination port: 43432
sequence number: 4236792461
ack number: 2462998738
flags: PSH|ACK
data offset: 32
window size: 249
checksum: 2674
urgent pointer: URG flag not set
has options? True

IP header contents:
  IP version: 4
  header length: 20
  service type: 0
  total len: 52
  identification: 24468
  flags: DF
  fragment offset: MF flag not set
  TTL: 64
  protocol: 6
  header checksum: 22991
  source IP: 192.168.0.9
  destination IP: 192.168.0.7
  has options? : no

TCP header contents:
  source port: 43432
  destination port: 22
  sequence number: 2462998738
  ack number: 4236792961
  flags: ACK
  data offset: 32
  window size: 279
  checksum: 38814
  urgent pointer: URG flag not set
  has options? True

IP header contents:
  IP version: 4
  header length: 20
  service type: 0
  total len: 96
  identification: 7721
  flags: DF
  fragment offset: MF flag not set
  TTL: 64
  protocol: 6
  header checksum: 39697
  source IP: 192.168.0.6
  destination IP: 192.168.0.7
  has options? : no

TCP header contents:
  source port: 22
```

```
root@datacomm:~/COMP8005-Final
File Edit View Search Terminal Help
header length: 20
service type: 16
total len: 112
identification: 1553
flags: DF
fragment offset: MF flag not set
TTL: 64
protocol: 6
header checksum: 45933
source IP: 192.168.0.6
destination IP: 192.168.0.7
has options? : no

TCP header contents:
  source port: 22
  destination port: 52852
  sequence number: 2885577866
  ack number: 849843818
  flags: PSH|ACK
  data offset: 32
  window size: 272
  checksum: 19352
  urgent pointer: URG flag not set
  has options? True

IP header contents:
  IP version: 4
  header length: 20
  service type: 16
  total len: 52
  identification: 11643
  flags: DF
  fragment offset: MF flag not set
  TTL: 64
  protocol: 6
  header checksum: 35901
  source IP: 192.168.0.8
  destination IP: 192.168.0.7
  has options? : no

TCP header contents:
  source port: 52852
  destination port: 22
  sequence number: 849843818
  ack number: 2885577926
  flags: ACK
  data offset: 32
  window size: 279
  checksum: 8624
  urgent pointer: URG flag not set
  has options? True
```

#eno1 [Wireshark 2.2.2 (wireshark-2.2.2)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter:

!8 || !ip.addr == 192.168.0.9 || !ip.addr == 192.168.0.6

Expression...
Clear
Apply
Save

100
100
100
100
100
100
100
100
100
100

No.	Time	Source	Destination	Protocol	Length	Info
494	2017-03-11 11:00:55.893751292	192.168.0.7	192.168.0.9	TCP	60	596 Server: Encrypted packet (len=509)
495	2017-03-11 11:00:55.898352752	192.168.0.9	192.168.0.7	TCP	60	60 43432-22 [ACK] Seq=2462998738 Ack=4236792961 Win=35712 Len=0 TSval=1052981 TSecr=1006825
496	2017-03-11 11:00:55.898759659	192.168.0.7	192.168.0.6	TCP	60	60 43432-22 [ACK] Seq=2462998738 Ack=4236792961 Win=35712 Len=0 TSval=1052981 TSecr=1006825
497	2017-03-11 11:00:55.899044740	192.168.0.6	192.168.0.7	SSHv2	110	Server: Encrypted packet (len=44)
498	2017-03-11 11:00:55.899434444	192.168.0.7	192.168.0.9	SSHv2	110	Server: Encrypted packet (len=44)
499	2017-03-11 11:00:55.899731778	192.168.0.9	192.168.0.7	TCP	60	60 43432-22 [ACK] Seq=2462998738 Ack=4236793005 Win=35712 Len=0 TSval=1052982 TSecr=1006867
500	2017-03-11 11:00:55.899974928	192.168.0.9	192.168.0.7	SSHv2	594	Client: Encrypted packet (len=528)
501	2017-03-11 11:00:55.900054294	192.168.0.7	192.168.0.6	TCP	60	60 43432-22 [ACK] Seq=2462998738 Ack=4236793005 Win=35712 Len=0 TSval=1052982 TSecr=1006867
502	2017-03-11 11:00:55.900367968	192.168.0.7	192.168.0.6	SSHv2	594	Client: Encrypted packet (len=528)
503	2017-03-11 11:00:55.902063234	192.168.0.6	192.168.0.7	SSHv2	174	Server: Encrypted packet (len=108)
504	2017-03-11 11:00:55.902117498	192.168.0.6	192.168.0.7	SSHv2	174	Server: Encrypted packet (len=92)
505	2017-03-11 11:00:55.902387035	192.168.0.7	192.168.0.9	SSHv2	174	Server: Encrypted packet (len=108)
506	2017-03-11 11:00:55.902588085	192.168.0.7	192.168.0.9	SSHv2	158	Server: Encrypted packet (len=92)
507	2017-03-11 11:00:55.902920481	192.168.0.9	192.168.0.7	TCP	60	60 43432-22 [ACK] Seq=2462999266 Ack=4236793205 Win=35712 Len=0 TSval=1052985 TSecr=1006870
508	2017-03-11 11:00:55.903142971	192.168.0.7	192.168.0.6	TCP	60	60 43432-22 [ACK] Seq=2462999266 Ack=4236793205 Win=35712 Len=0 TSval=1052985 TSecr=1006870
509	2017-03-11 11:00:55.905832198	192.168.0.6	192.168.0.7	SSHv2	126	Server: Encrypted packet (len=60)
510	2017-03-11 11:00:55.905869240	192.168.0.6	192.168.0.7	SSHv2	126	Server: Encrypted packet (len=60)
511	2017-03-11 11:00:55.951263873	192.168.0.7	192.168.0.9	SSHv2	126	Server: Encrypted packet (len=60)
512	2017-03-11 11:00:55.951412714	192.168.0.7	192.168.0.9	TCP	60	60 43432-22 [ACK] Seq=2462999266 Ack=4236793325 Win=35712 Len=0 TSval=1053034 TSecr=1006919
513	2017-03-11 11:00:55.951631379	192.168.0.9	192.168.0.7	TCP	60	60 43432-22 [ACK] Seq=2462999266 Ack=4236793325 Win=35712 Len=0 TSval=1053034 TSecr=1006919
514	2017-03-11 11:00:55.951855203	192.168.0.7	192.168.0.6	TCP	74	52052-22 [SYN] Seq=849841472 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2596986 TSecr=0 WS=128
520	2017-03-11 11:00:57.086666815	192.168.0.7	192.168.0.7	TCP	74	52052-22 [SYN] Seq=849841472 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2596986 TSecr=0 WS=128
521	2017-03-11 11:00:57.087251551	192.168.0.6	192.168.0.7	TCP	74	52052-22 [SYN] Seq=849841472 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2596986 TSecr=0 WS=128
522	2017-03-11 11:00:57.887565448	192.168.0.6	192.168.0.7	TCP	74	22-52052 [SYN, ACK] Seq=2885575385 Ack=849841473 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1008855 TSecr=1008855
523	2017-03-11 11:00:57.887995474	192.168.0.7	192.168.0.8	TCP	74	22-52052 [SYN, ACK] Seq=2885575385 Ack=849841473 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1008855 TSecr=1008855
524	2017-03-11 11:00:57.888259663	192.168.0.8	192.168.0.7	TCP	60	60 52052-22 [ACK] Seq=849841473 Ack=2885575386 Win=29312 Len=0 TSval=25

#### 4.) Stress test of Port Forwarder

```
root@datacomm:~/COMP8005-Final
File Edit View Search Terminal Help
sequence number: 2937279067
ack number: 217568833
flags: SYN|ACK
data offset: 40
window size: 28960
checksum: 24390
urgent pointer: URG flag not set
has options? True

IP header contents:
  IP version: 4
  header length: 20
  service type: 0
  total len: 52
  identification: 12944
  flags: DF
  fragment offset: MF flag not set
  TTL: 64
  protocol: 6
  header checksum: 34518
  source IP: 192.168.0.6
  destination IP: 192.168.0.7
  has options? : no

TCP header contents:
  source port: 8005
  destination port: 47778
  sequence number: 3466153903
  ack number: 246243128
  flags: ACK
  data offset: 32
  window size: 243
  checksum: 24174
  urgent pointer: URG flag not set
  has options? True

IP header contents:
  IP version: 4
  header length: 20
  service type: 0
  total len: 60
  identification: 0
  flags: DF
  fragment offset: MF flag not set
  TTL: 64
  protocol: 6
  header checksum: 47454
  source IP: 192.168.0.6
  destination IP: 192.168.0.7
  has options? : no

TCP header contents:
  source port: 8005
```

Capturing from eno1 [Wireshark 2.2.2 [wireshark-2.2.2]]

FileEditViewGoCaptureAnalyzeStatisticsTelephonyToolsInternalsHelp

Filter: !8 | !ip.addr == 192.168.0.9 | !ip.addr == 192.168.0.6

Expression...ClearSave

No.	Time	Source	Destination	Protocol	Length	Info
279097	2017-03-11 11:17:12.67541745	192.168.0.7	192.168.0.8	TCP	70	46822->8085 [PSH, ACK] Seq=131340548 Ack=191092480/ Win=31360 Len=4 TSval=3571692 TSecr=1983591
279098	2017-03-11 11:17:12.673514325	192.168.0.8	192.168.0.7	TCP	68	74180->8085 [ACK] Seq=1607626431 Ack=4267524924 Win=31360 Len=0 TSval=3571692 TSecr=1983643
279099	2017-03-11 11:17:12.673525445	192.168.0.7	192.168.0.8	TCP	68	8005->46820 [FIN, ACK] Seq=1658376088 Ack=2194232869 Win=31104 Len=0 TSval=1983644 TSecr=3571691
279100	2017-03-11 11:17:12.673630549	192.168.0.7	192.168.0.8	TCP	68	46822->8085 [FIN, ACK] Seq=1313405462 Ack=1910924807 Win=31360 Len=0 TSval=3571692 TSecr=1983391
279101	2017-03-11 11:17:12.673641779	192.168.0.8	192.168.0.7	TCP	68	8005->46822 [FIN, ACK] Seq=1010924807 Ack=1313405462 Win=31104 Len=0 TSval=1983644 TSecr=3571692
279102	2017-03-11 11:17:12.673646108	192.168.0.8	192.168.0.7	TCP	68	46820->8085 [ACK] Seq=2194232870 Ack=1658376089 Win=31360 Len=0 TSval=3571693 TSecr=1983643
279103	2017-03-11 11:17:12.673733373	192.168.0.7	192.168.0.8	TCP	68	8005->46820 [ACK] Seq=1658376089 Ack=2194232870 Win=31104 Len=0 TSval=1983643 TSecr=3571691
279104	2017-03-11 11:17:12.673773701	192.168.0.7	192.168.0.8	TCP	68	8005->46822 [ACK] Seq=1910924808 Ack=1313405463 Win=31104 Len=0 TSval=1983644 TSecr=3571692
279105	2017-03-11 11:17:12.673845239	192.168.0.7	192.168.0.8	TCP	74	47922->8085 [SYN] Seq=306746415 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3571692 TSecr=0 WS=128
279106	2017-03-11 11:17:12.673875080	192.168.0.8	192.168.0.7	TCP	70	46820->8085 [PSH, ACK] Seq=248836646 Ack=3018384633 Win=31360 Len=4 TSval=3571693 TSecr=1983392
279107	2017-03-11 11:17:12.673905577	192.168.0.8	192.168.0.7	TCP	68	46820->8085 [FIN, ACK] Seq=3018384633 Ack=3018384633 Win=31360 Len=0 TSval=3571693 TSecr=1983392
279108	2017-03-11 11:17:12.673945953	192.168.0.8	192.168.0.7	TCP	74	47926->8085 [SYN] Seq=2947479500 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3571693 TSecr=0 WS=128
279109	2017-03-11 11:17:12.673952401	192.168.0.7	192.168.0.8	TCP	74	8005->47926 [SYN, ACK] Seq=862407039 Ack=2775635635 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1983139
279110	2017-03-11 11:17:12.674008270	192.168.0.7	192.168.0.8	TCP	74	8005->47922 [SYN, ACK] Seq=2211452306 Ack=3067464416 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1983139
279111	2017-03-11 11:17:12.674063377	192.168.0.7	192.168.0.8	TCP	70	46824->8085 [PSH, ACK] Seq=1466034255 Ack=840965778 Win=31360 Len=4 TSval=3571692 TSecr=1983391
279112	2017-03-11 11:17:12.674159039	192.168.0.8	192.168.0.7	TCP	68	47920->8085 [ACK] Seq=2775635635 Ack=862407040 Win=29312 Len=0 TSval=3571693 TSecr=1983644
279113	2017-03-11 11:17:12.674164309	192.168.0.7	192.168.0.8	TCP	70	47920->8085 [PSH, ACK] Seq=2775635635 Ack=862407040 Win=29312 Len=4 TSval=3571693 TSecr=1983644
279114	2017-03-11 11:17:12.674166246	192.168.0.7	192.168.0.8	TCP	68	46824->8085 [FIN, ACK] Seq=1466034259 Ack=840965778 Win=31360 Len=0 TSval=3571692 TSecr=1983391
279115	2017-03-11 11:17:12.674271545	192.168.0.7	192.168.0.8	TCP	68	8005->46824 [FIN, ACK] Seq=840965778 Ack=1466034259 Win=31104 Len=0 TSval=1983645 TSecr=3571692
279116	2017-03-11 11:17:12.674273013	192.168.0.7	192.168.0.8	TCP	74	47924->8085 [SYN] Seq=996019831 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3571692 TSecr=0 WS=128
279117	2017-03-11 11:17:12.674323117	192.168.0.7	192.168.0.8	TCP	68	8005->46824 [ACK] Seq=840965779 Ack=1466034260 Win=31104 Len=0 TSval=1983645 TSecr=3571692
279118	2017-03-11 11:17:12.674377338	192.168.0.7	192.168.0.8	TCP	68	47018->8085 [ACK] Seq=1607626431 Ack=4267524924 Win=31360 Len=0 TSval=3571692 TSecr=1983643
279119	2017-03-11 11:17:12.674424113	192.168.0.8	192.168.0.7	TCP	74	8005->47924 [SYN, ACK] Seq=3998578312 Ack=996019832 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1983139
279120	2017-03-11 11:17:12.674476913	192.168.0.7	192.168.0.8	TCP	68	8005->46822 [FIN, ACK] Seq=1910924807 Ack=1313405462 Win=31104 Len=0 TSval=1983644 TSecr=3571692
279121	2017-03-11 11:17:12.674579560	192.168.0.7	192.168.0.8	TCP	68	46820->8085 [ACK] Seq=2194232870 Ack=1658376089 Win=31360 Len=0 TSval=3571693 TSecr=1983643
279122	2017-03-11 11:17:12.674628400	192.168.0.7	192.168.0.8	TCP	68	46822->8085 [ACK] Seq=1313405463 Ack=1910924808 Win=31360 Len=0 TSval=3571693 TSecr=1983644

Internet II, Src: Ubiquiti, Seq:6449 (44:49:49:49:49:49), Dst: Dell, dc:e9:22 (98:90:96:dc:e9:22)

Internet Protocol Version 4, Src: 74.125.199.105, Dst: 192.168.0.8

Transmission Control Protocol, Src Port: 443, Dst Port: 42662, Seq: 3483611371, Ack: 7655082475, Len: 60

Secure Sockets Layer

0000 19 00 96 dc e9 22 44 49 67 95 e4 9f 08 05 40 .....D.....E..

0010 00 70 9f 2b 00 00 2b 06 14 72 4a 7d 67 bd c0 a8 .....p.....rj....

0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....N.....

0030 06 53 dd 35 00 00 01 01 08 0a 31 ba 4f c4 00 35 .....5.....1.0.5

0040 94 19 17 03 03 00 37 00 00 00 00 00 00 00 00 .....7.....N....

0050 2a 3e bd 04 c6 62 3b dc 48 cd 69 48 ee 55 .....:..f..LH.KH.U

eno1: live capture in progress...

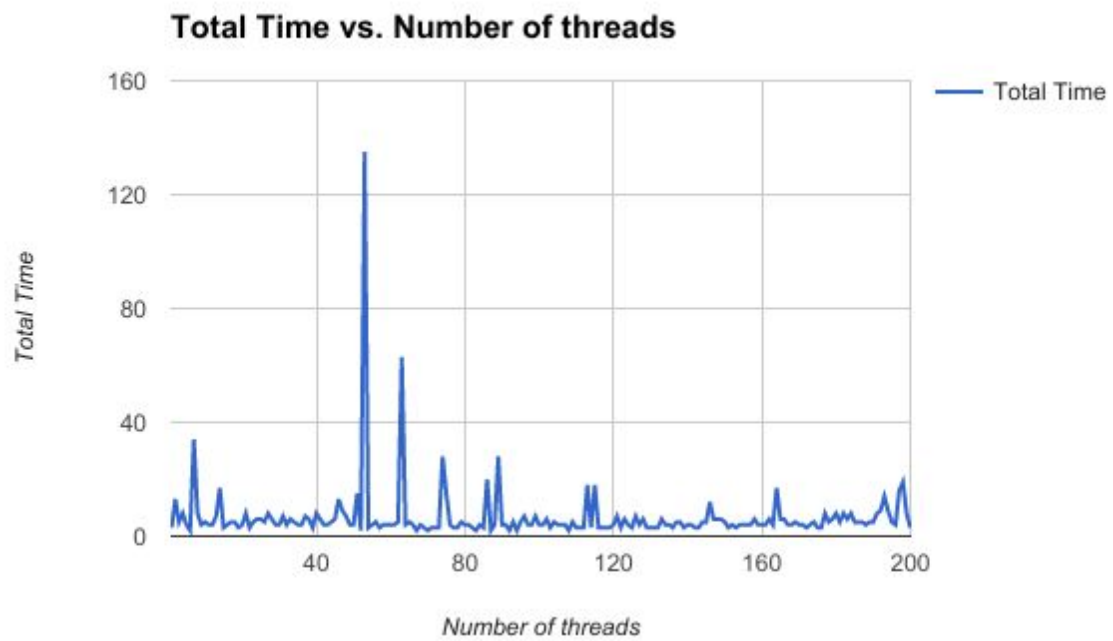
Packets: 41413 / 41413 (100.0%)

Profile: Default

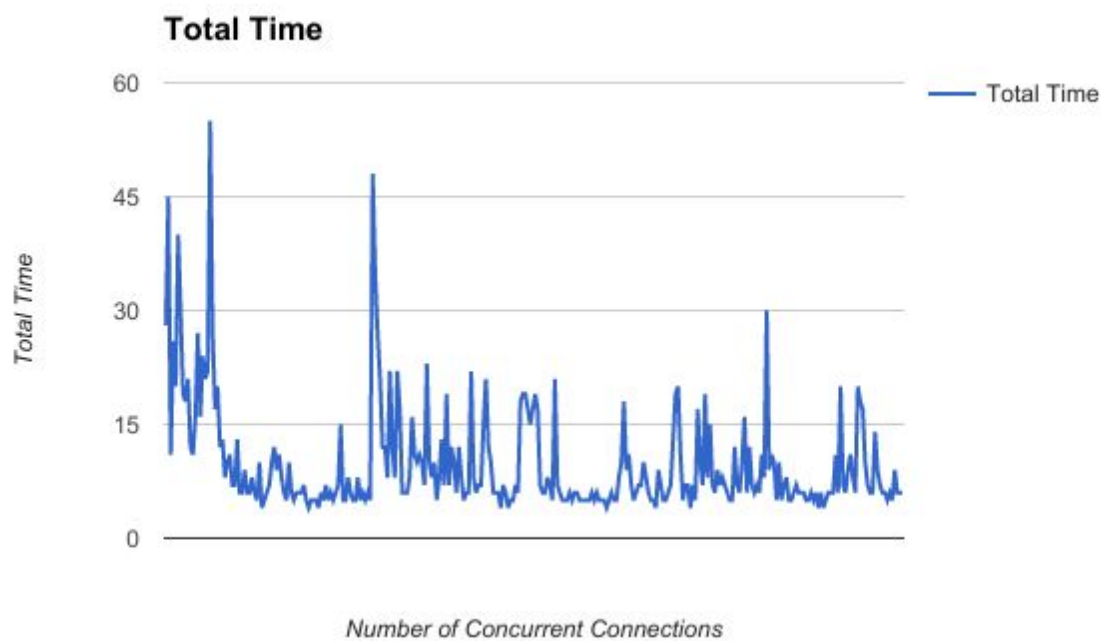


```
root@datacomm:~/COMP8005-Assn2/build/src/server
File Edit View Search Terminal Help
Transfer time: 7us; total bytes transferred: 1032; peer: 192.168.0.7:35760
Transfer time: 7us; total bytes transferred: 1032; peer: 192.168.0.7:35764
Transfer time: 7us; total bytes transferred: 1032; peer: 192.168.0.7:35766
Transfer time: 6us; total bytes transferred: 1032; peer: 192.168.0.7:35768
Transfer time: 6us; total bytes transferred: 1032; peer: 192.168.0.7:35794
Transfer time: 6us; total bytes transferred: 1032; peer: 192.168.0.7:35808
Transfer time: 7us; total bytes transferred: 1032; peer: 192.168.0.7:35848
Transfer time: 6us; total bytes transferred: 1032; peer: 192.168.0.7:35850
Transfer time: 8us; total bytes transferred: 1032; peer: 192.168.0.7:35852
Transfer time: 6us; total bytes transferred: 1032; peer: 192.168.0.7:35856
Transfer time: 7us; total bytes transferred: 1032; peer: 192.168.0.7:35904
Transfer time: 7us; total bytes transferred: 1032; peer: 192.168.0.7:35908
Transfer time: 7us; total bytes transferred: 1032; peer: 192.168.0.7:35910
Transfer time: 6us; total bytes transferred: 1032; peer: 192.168.0.7:35912
Transfer time: 7us; total bytes transferred: 1032; peer: 192.168.0.7:35938
Transfer time: 5us; total bytes transferred: 1032; peer: 192.168.0.7:35940
Transfer time: 7us; total bytes transferred: 1032; peer: 192.168.0.7:35942
Transfer time: 4us; total bytes transferred: 1032; peer: 192.168.0.7:35944
Transfer time: 7us; total bytes transferred: 1032; peer: 192.168.0.7:35946
Transfer time: 7us; total bytes transferred: 1032; peer: 192.168.0.7:35992
Transfer time: 6us; total bytes transferred: 1032; peer: 192.168.0.7:35994
Transfer time: 8us; total bytes transferred: 1032; peer: 192.168.0.7:35996
Transfer time: 21us; total bytes transferred: 1032; peer: 192.168.0.7:35998
Transfer time: 9us; total bytes transferred: 1032; peer: 192.168.0.7:36000
Transfer time: 6us; total bytes transferred: 1032; peer: 192.168.0.7:36004
Transfer time: 7us; total bytes transferred: 1032; peer: 192.168.0.7:36020
Transfer time: 8us; total bytes transferred: 1032; peer: 192.168.0.7:36022
Transfer time: 5us; total bytes transferred: 1032; peer: 192.168.0.7:36040
Transfer time: 6us; total bytes transferred: 1032; peer: 192.168.0.7:36062
Transfer time: 6us; total bytes transferred: 1032; peer: 192.168.0.7:36072
Transfer time: 10us; total bytes transferred: 1032; peer: 192.168.0.7:36080
Transfer time: 7us; total bytes transferred: 1032; peer: 192.168.0.7:36082
Transfer time: 6us; total bytes transferred: 1032; peer: 192.168.0.7:36108
Transfer time: 16us; total bytes transferred: 1032; peer: 192.168.0.7:36112
Transfer time: 16us; total bytes transferred: 1032; peer: 192.168.0.7:36114
Transfer time: 9us; total bytes transferred: 1032; peer: 192.168.0.7:36116
Transfer time: 5us; total bytes transferred: 1032; peer: 192.168.0.7:36128
Transfer time: 17us; total bytes transferred: 1032; peer: 192.168.0.7:36186
Transfer time: 6us; total bytes transferred: 1032; peer: 192.168.0.7:36190
Transfer time: 7us; total bytes transferred: 1032; peer: 192.168.0.7:36192
Transfer time: 9us; total bytes transferred: 1032; peer: 192.168.0.7:36196
Transfer time: 7us; total bytes transferred: 1032; peer: 192.168.0.7:36200
Transfer time: 6us; total bytes transferred: 1032; peer: 192.168.0.7:36202
Transfer time: 5us; total bytes transferred: 1032; peer: 192.168.0.7:36222
Transfer time: 9us; total bytes transferred: 1032; peer: 192.168.0.7:36224
Transfer time: 6us; total bytes transferred: 1032; peer: 192.168.0.7:36226
Transfer time: 5us; total bytes transferred: 1032; peer: 192.168.0.7:36228
Transfer time: 6us; total bytes transferred: 1032; peer: 192.168.0.7:36230
Transfer time: 7us; total bytes transferred: 1032; peer: 192.168.0.7:36232
Transfer time: 6us; total bytes transferred: 1032; peer: 192.168.0.7:36236
Transfer time: 11us; total bytes transferred: 1032; peer: 192.168.0.7:36268
Transfer time: 7us; total bytes transferred: 1032; peer: 192.168.0.7:36342
Transfer time: 12us; total bytes transferred: 1032; peer: 192.168.0.7:36346
Transfer time: 8us; total bytes transferred: 1032; peer: 192.168.0.7:36426
```

Epoll result with no port forwarder



Epoll result with port forwarder



## 5.) Nat Collision

The image shows a terminal window and a Wireshark packet capture. The terminal window, titled 'root@datacomm:~/COMP8005-Final', displays the details of three network packets. The first packet is an IP packet with source IP 192.168.0.9 and destination IP 192.168.0.7. The second packet is a TCP packet with source port 41978 and destination port 22. The third packet is an IP packet with source IP 192.168.0.9 and destination IP 192.168.0.7. The Wireshark window, titled 'Capturing from eno1 [Wireshark 2.2.2 (wireshark-2.2.2)]', shows a list of captured packets. The filter is set to 'ip.addr == 192.168.0.9 || ip.addr == 192.168.0.6'. The packet list shows a series of packets from 192.168.0.9 to 192.168.0.7. The packet details pane shows the selected packet (No. 188) as a TCP packet with source port 41978 and destination port 22. The packet bytes pane shows the raw data of the packet.

```
File Edit View Search Terminal Help

Choosing a random source port to resolve NAT collision
Port chosen: 49936
IP header contents:
  IP version: 4
  header length: 20
  service type: 0
  total len: 40
  identification: 35984
  flags:
  fragment offset: MF flag not set
  TTL: 64
  protocol: 6
  header checksum: 27871
  source IP: 192.168.0.9
  destination IP: 192.168.0.7
  has options? : no

TCP header contents:
  source port: 41978
  destination port: 22
  sequence number: 1667089999
  ack number: 128834164
  flags: SYN
  data offset: 20
  window size: 512
  checksum: 36636
  urgent pointer: URG flag not set
  has options? False

IP header contents:
  IP version: 4
  header length: 20
  service type: 0
  total len: 44
  identification: 0
  flags: DF
  fragment offset: MF flag not set
  TTL: 64
  protocol: 6
  header checksum: 47470
  source IP: 192.168.0.6
  destination IP: 192.168.0.7
  has options? : no

TCP header contents:
  source port: 22
  destination port: 49936
  sequence number: 1667090000
  ack number: 1667090000
  flags: SYN|ACK
  data offset: 24
  window size: 29200
  checksum: 48663

Capturing from eno1 [Wireshark 2.2.2 (wireshark-2.2.2)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ip.addr == 192.168.0.9 || ip.addr == 192.168.0.6 Expression... Clear Apply Save

No. Time Source Destination Protocol Length Info
82 2017-03-11 11:57:00.059211553 192.168.0.6 192.168.0.7 TCP 60 41978->22 [ACK] Seq=2817201303 Ack=4236422883 Win=35712 Len=0 TSval=5959879 TSecr=4371788
83 2017-03-11 11:57:00.059602958 192.168.0.7 192.168.0.6 TCP 66 41978->22 [ACK] Seq=2817201365 Ack=4236422883 Win=35712 Len=0 TSval=5959879 TSecr=4371788
84 2017-03-11 11:57:00.059895080 192.168.0.6 192.168.0.7 SSHv2 110 Server: Encrypted packet (len=44)
85 2017-03-11 11:57:00.060260393 192.168.0.7 192.168.0.8 SSHv2 110 Server: Encrypted packet (len=44)
86 2017-03-11 11:57:00.060519300 192.168.0.8 192.168.0.7 TCP 66 41978->22 [ACK] Seq=2817201365 Ack=4236422927 Win=35712 Len=0 TSval=5959880 TSecr=4371831
87 2017-03-11 11:57:00.060626634 192.168.0.8 192.168.0.7 SSHv2 594 Client: Encrypted packet (len=528)
88 2017-03-11 11:57:00.060914821 192.168.0.7 192.168.0.6 TCP 66 41978->22 [ACK] Seq=2817201365 Ack=4236422927 Win=35712 Len=0 TSval=5959880 TSecr=4371831
89 2017-03-11 11:57:00.061240658 192.168.0.7 192.168.0.6 SSHv2 594 Client: Encrypted packet (len=528)
90 2017-03-11 11:57:00.062861686 192.168.0.6 192.168.0.7 SSHv2 174 Server: Encrypted packet (len=168)
91 2017-03-11 11:57:00.062874257 192.168.0.6 192.168.0.7 SSHv2 158 Server: Encrypted packet (len=92)
92 2017-03-11 11:57:00.063178926 192.168.0.7 192.168.0.8 SSHv2 174 Server: Encrypted packet (len=168)
93 2017-03-11 11:57:00.063448081 192.168.0.7 192.168.0.8 SSHv2 158 Server: Encrypted packet (len=92)
94 2017-03-11 11:57:00.063749525 192.168.0.8 192.168.0.7 TCP 66 41978->22 [ACK] Seq=2817201893 Ack=4236423127 Win=35712 Len=0 TSval=5959883 TSecr=4371834
95 2017-03-11 11:57:00.064038814 192.168.0.7 192.168.0.6 TCP 66 41978->22 [ACK] Seq=2817201893 Ack=4236423127 Win=35712 Len=0 TSval=5959883 TSecr=4371834
96 2017-03-11 11:57:00.063314321 192.168.0.6 192.168.0.7 SSHv2 126 Server: Encrypted packet (len=60)
97 2017-03-11 11:57:00.063460971 192.168.0.6 192.168.0.7 SSHv2 126 Server: Encrypted packet (len=60)
98 2017-03-11 11:57:00.063659673 192.168.0.7 192.168.0.8 SSHv2 126 Server: Encrypted packet (len=60)
99 2017-03-11 11:57:00.063857954 192.168.0.7 192.168.0.8 SSHv2 126 Server: Encrypted packet (len=60)
100 2017-03-11 11:57:00.064086784 192.168.0.8 192.168.0.7 TCP 66 41978->22 [ACK] Seq=2817201893 Ack=4236423247 Win=35712 Len=0 TSval=5959923 TSecr=4371874
101 2017-03-11 11:57:00.064330829 192.168.0.7 192.168.0.6 TCP 66 41978->22 [ACK] Seq=2817201893 Ack=4236423247 Win=35712 Len=0 TSval=5959923 TSecr=4371874
102 2017-03-11 11:57:00.064943734 192.168.0.6 192.168.0.7 SSH 118 Server: Encrypted packet (len=44)
176 2017-03-11 11:57:18.134821491 192.168.0.9 192.168.0.7 TCP 60 41978->22 [SYN] Seq=1667089999 Win=512 Len=0
177 2017-03-11 11:57:18.136316209 192.168.0.7 192.168.0.6 TCP 54 49936->22 [SYN] Seq=1667089999 Win=512 Len=0
178 2017-03-11 11:57:18.136657083 192.168.0.6 192.168.0.7 TCP 60 22->49936 [SYN, ACK] Seq=2351656336 Ack=1667089999 Win=29200 Len=0 MSS=1460
179 2017-03-11 11:57:18.137681999 192.168.0.7 192.168.0.9 TCP 58 22->41978 [SYN, ACK] Seq=2351656336 Ack=1667089999 Win=29200 Len=0 MSS=1460
188 2017-03-11 11:57:18.137962117 192.168.0.9 192.168.0.7 TCP 60 41978->22 [RST] Seq=1667089999 Win=0 Len=0

Ethernet II, Src: Dell_dc:e9:22 (98:90:96:dc:e9:22), Dst: Dell_dc:f3:9b (98:90:96:dc:f3:9b)
Internet Protocol Version 4, Src: 192.168.0.8, Dst: 192.168.0.7
Transmission Control Protocol, Src Port: 41976, Dst Port: 22, Seq: 3956140748, Ack: 3928617584, Len: 36
SSH Protocol

0000 98 90 96 dc f3 9b 98 90 96 dc e9 22 08 00 45 10 .....E.
0010 00 58 df 13 40 00 40 06 da 1c c0 a8 00 08 c0 a8 .X.@.@.
0020 00 07 a3 f8 00 16 eb cd ea cc ea 29 f2 70 80 18 .....p.
0030 01 17 5e 11 00 00 01 01 08 0a 00 5a 08 00 00 42 .....Z..B
0040 0f b3 1e 2c 23 33 d3 d5 68 f1 79 eb ea 68 2a 58 ...#3..h.y.hX
0050 32 62 73 af 7c 1f 38 86 2d 6f 2d 18 46 ea 54 f8 2bs|.8.-o...T.

eno1: <live capture in progress> ... Packets: 379 - Displayed: 82 (21.6%) Profile: Default
```

## 6.) Forward to different port

```
root@datacomm:~/COMP8005-Final
File Edit View Search Terminal Help

IP header contents:
  IP version: 4
  header length: 20
  service type: 16
  total len: 112
  identification: 1607
  flags: DF
  fragment offset: MF flag not set
  TTL: 64
  protocol: 6
  header checksum: 45779
  source IP: 192.168.0.6
  destination IP: 192.168.0.7
  has options? : no

TCP header contents:
  source port: 22
  destination port: 51430
  sequence number: 3917849429
  ack number: 2634281110
  flags: PSH|ACK
  data offset: 32
  window size: 272
  checksum: 50976
  urgent pointer: URG flag not set
  has options? True

IP header contents:
  IP version: 4
  header length: 20
  service type: 16
  total len: 52
  identification: 32221
  flags: DF
  fragment offset: MF flag not set
  TTL: 64
  protocol: 6
  header checksum: 15223
  source IP: 192.168.0.8
  destination IP: 192.168.0.7
  has options? : no

TCP header contents:
  source port: 51430
  destination port: 55
  sequence number: 3634281110
  ack number: 3917849369
  flags: ACK
  data offset: 32
  window size: 296
  checksum: 34982
  urgent pointer: URG flag not set
  has options? True
```