بسم الله الرحمن الرحیم

In the name of Allah

# TCP and Its Applications[1]

## Laboratory Manual


University of Tehran
School of Electrical and Computer Engineering

دانشگاه تهران

دانشکده‌ی مهندسی برق و کامپیوتر


## Computer Network Lab

## آزمایشگاه شبکه‌های کامپیوتری


Dr. Ahmad Khonsari
دکتر احمد خونساری
a_khonsari@ut.ac.ir

Amir Haji Ali Khamseh'i
امیر حاجی‌علی‌خمسه‌ء
khamse@ut.ac.ir

Muhammad Borhani
محمد برهانی
m.borhani@ut.ac.ir

AmirAhmad Khordadi
امیراحمد خردادی
a.a.khordadi@ut.ac.ir

Sina Kashipazha
سینا کاشی‌پزها
sina_kashipazha@ut.ac.ir

Hadi Safari
هادی صفری
hadi.safari@ut.ac.ir



November 14, 2019

۲۳ آبان ۱۳۹۸


[1] S. Panwar, S. Mao, J.-dong Ryoo, and Y. Li, "TCP study," in TCP/IP Essentials: A Lab-Based Approach, Cambridge: Cambridge University Press, 2004, pp. 111–133.

# Part I

# Exercises on TCP Connection Control

Like previous lab, connect two host with one hub together (Figure 5.0).

## 1 Telnet terminal

While `tcpdump -S host your-host and remote-host` is running, execute: `telnet remote-host date`. Save the tcpdump output.

### Report

1. Explain TCP connection establishment and termination using the tcpdump output.
2. What were the announced MSS values for the two hosts?
3. What happens if there is an intermediate network that has an MTU less than the MSS of each host? See if the `DF` flag was set in tcpdump output. You can change interface `MTU` with `sudo ifconfig $ETH mtu 1400`

## 2 TCP vs UDP Connection Establishment

While `tcpdump -nx host your-host and remote-host` is running, use `socket` [1] to send a UDP datagram to *h2*:

```
socket -u -s remote-host 8888
```

Save the `tcpdump` or `wireshark` output for your lab report.
Restart the above `tcpdump` command, execute `socket` in the TCP mode:

```
socket -i -n1 host 8888
```

Save the `tcpdump` output for your lab report.

### Report

1. Explain what happened in both the UDP and TCP cases. When a client requests a non-existing server, how do UDP and TCP handle this request, respectively?

# Part II

# Exercise on TCP Interactive Data Flow

## 3 Interactive Data Flow

While `tcpdump` is capturing the traffic between your machine and a remote machine, issue following commands:

```
tcpdump -nv (or run wireshark)
telnet host
```

After logging in to the host, type `date` and press the Enter key.

[1] Basic command is `sock`. Use alternative `socket` (linked to `sock`).

Now, in order to generate data faster than the round-trip time of a single byte to be sent and echoed, type any sequence of keys in the `telnet` window very rapidly.[2]

Save the `tcpdump` output for your lab report.

### Report

Answer the following questions, based upon the `tcpdump` output saved in the above exercise.

1. What is a delayed acknowledgement? What is it used for?
2. Can you see any delayed acknowledgements in your `tcpdump` output?

   If yes, explain the reason. Mark some of the lines with delayed acknowledgements, and submit the `tcpdump` output with your report.

   Explain how the delayed ACK timer operates from your `tcpdump` output.

   If you don't see any delayed acknowledgements, explain the reason why none was observed.
3. What is the *Nagle*[3] algorithm used for?

   From your `tcpdump` output, can you tell whether the Nagle algorithm is enabled or not? Give the reason for your answer.

   From your `tcpdump` output for when you typed very rapidly, can you see any segment that contains more than one character going from your workstation to the remote machine?

# Part III
# Exercise on TCP Bulk Data Flow

## 4 IP Segment

While tcpdump is running and capturing the packets between your machine and a remote machine, on the remote machine, which acts as the server, execute:

```
socket -i -s 7777
```

Then, on your machine, which acts as the client, execute:

```
socket -i -n16 remote-host 7777
```

Do the same experiment three times.

Save all the `tcpdump` outputs for your lab report.

### Report

1. Using one of three `tcpdump` outputs, explain the operation of TCP in terms of data segments and their acknowledgements. Does the number of data segments differ from that of their acknowledgements?

   Compare all the `tcpdump` outputs you saved. Discuss any differences among them, in terms of data segments and their acknowledgements.
2. From the `tcpdump` output, how many different TCP flags can you see? Enumerate the flags and explain their meanings.

   How many different TCP options can you see? Explain their meanings.

[2] For example hold "A" key or write "qwertyuiop" in `telnet` window.
[3] Nagle Algorithm is a means of improving the efficiency of TCP/IP networks by reducing the number of packets that need to be sent over the network.

# Part IV
# Exercises on TCP Timers and Retransmission

## 5 Keepalive parameter

Execute `sysctl -A | grep keepalive` to display the default values of the TCP kernel parameters that are related to the TCP keepalive timer.

### Report

1. What is the default value of the TCP keepalive timer?
2. What is the maximum number of TCP keepalive probes a host can send?

## 6 TCP Retransmission

While `tcpdump` is running to capture the packets between your host and a remote host, start a `socket` server on the remote host,

```
socket -s 8888
```

Then, execute the following command on your host,

- add link delay in simulator[4]
- `socket -i -n200` ***host*** `8888`

While the sender is injecting data segments into the network, disconnect the cable connecting the sender to the hub for about ten seconds.

After observing several retransmissions, reconnect the cable:

```
ip link set eth0 down or ifconfig eth0 down
```

after seconds...

```
ip link set eth0 up or ifconfig eth0 up
```

When all the data segments are sent, save the `tcpdump` output for the lab report.

### Report

1. Submit the `tcpdump` output saved in this exercise.
2. From the `tcpdump` output, identify when the cable was disconnected.
3. Describe how the retransmission timer changes after sending each retransmitted packet, during the period when the cable was disconnected.
4. Explain how the number of data segments that the sender transmits at once (before getting an ACK) changes after the connection is reestablished.[5].

[4] In GNS3, `right click` on link, select `Packet Filter` and set link `delay` to *10 ms*
[5] TCP Window visualizer

# Part V
# Other Exercises

## 7 Fragmentation

While `tcpdump src host your-host` is running, execute the following command, which is similar to the command we used to find out the maximum size of a UDP datagram in previous lab session (Chapter 5 of reference book),

```
socket -i -n1 -w n remote-host echo
```

Let $n$ be larger than the maximum UDP datagram size we found in previous lab session.

As an example, you may use $n = 70080$.

### Report

1. Did you observe any IP fragmentation?
2. If IP fragmentation did not occur this time, how do you explain this compared to what you observed in previous lab session for UDP packets?

## 8 Linux TCP/IP Kernel Parameter

Study the manual page of `/sbin/sysctl` . Examine the default values of some TCP/IP configuration parameters that you might be interested in. Examine the configuration files in the `/proc/sys/net/ipv4` directory.

### Report

1. Explain what is `sysctl` command for?
2. Explain two arbitrary TCP/IP configuration parameters. What is their default values?
3. Name two arbitrary file in the `/proc/sys/net/ipv4` directory. What is their content?