Hands-on-4: TCP

First of all, merry Dongzhi Festival to you all!

Read the following hands-on. Do as instructed, and submit your solutions **in English or Chinese**. Upload your answers to Canvas in a `.pdf` file. Due is 2021-12-28 23:59.

In this hands-on you will understand how TCP works using `tcpdump`. To begin with, download the tcpdump log from here. For this trace, we used a program that transmits a file from a machine called *DongDong* to a machine called *BingBing* over a TCP connection. We ran the *tcpdump* tool on the sender, DongDong, to log both the departing data packets and the received acknowledgments (ACKs). The file `tcpdump.dat` is a binary file that contains a log of all the TCP packets for the above TCP connection. The file is not human-readable. To parse the file, you can use `tcpdump` by running:

```
> tcpdump -r tcpdump.dat > outfile.txt
```

The output file has several lines listing packets sent from DongDong to BingBing, and the ACKs from BingBing to DongDong:

```
00:34:41.474225 IP dongdong.sjtu.edu.cn.39675 > bingbing.sjtu.edu.cn.5001: Flags [.], seq
1473:2921, ack 1, win 115, options [nop,nop,TS val 282136474 ecr 282202089], length 1448
```

Denotes a packet sent from DongDong to BingBing. The timestamp `00:34:41.474225` indicates the time at which the packet was transmitted by DongDong.

TCP uses sequence numbers to keep track of how much data it has sent. We often associated one sequence number with each packet. In reality, there is one sequence number per *byte of data*. The above packet has a sequence number `1473:2921`, which contains all bytes from byte `#1473` to byte `#2920` (`= 2921 - 1`) in the stream, which is a total of `1448` bytes.

Once BingBing receives the packet, assuming that it has received all previous packets as well, it sends an acknowledgment (ACK):

```
00:34:41.482047 IP bingbing.sjtu.edu.cn.5001 > dongdong.sjtu.edu.cn.39675: Flags [.], ack
2921, win 159, options [nop,nop,TS val 282202095 ecr 282136474], length 0
```

ACK here reflects the corresponding packet's sequence number for demonstration purposes. In reality, the ACK reflects the next byte the receiver expects. The above ACK indicates that BingBing has received all bytes from byte `#0` to byte `#2920`. The next byte BingBing expects is byte `#2921`. The timestamp `00:34:41.482047`, denotes when the ACK was received by DongDong.

Note: There may be minor variations in the format of the output of tcpdump depending on the version of tcpdump on your machine.

Q1: What are the IP addresses and TCP ports of BingBing and DongDong?

Q2: How many KB were transferred during this TCP session and how long did it last?

Q3: What is the throughput (in KB/s) of this TCP flow between DongDong and BingBing?

Q4: What is the round-trip time (RTT) between DongDong and BingBing?