In this assignment you will understand how TCP works using tcpdump.

In your home directory you will find a file named **tcpdump.dat**.

For this trace, we used a program that transmits a file from a machine called ***willow*** to a machine called ***maple*** over a TCP connection. We ran the **tcpdump** tool on the sender, willow, to log both the departing data packets and the received acknowledgments (ACKs).

The file **tcpdump.dat** is a binary file which contains a log of all the TCP packets for the above TCP connection. The file is not human-readable. To access the log file in a human-readable format, run:

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

Now open outfile.txt on your preferred text editor. The output has several lines listing packets sent from willow to maple, and the ACKs from maple to willow. For example:

```
00:34:41.474225 IP willow.csail.mit.edu.39675 > maple.csail.mit.edu.5001: Flags [.], seq 1473:2921,
ack 1, win 115, options [nop,nop,TS val 282136474 ecr 282202089], length 1448
```

Denotes a packet sent from willow to maple. The time stamp 00:34:41.474225 denotes the time at which the packet was transmitted by willow.

TCP uses sequence numbers to keep track of how much data it has sent. For teaching purposes, we often associated one sequence number with each packet (packet 1, packet 2, etc.). In reality, there is one sequence number per *byte of data*. The above packet has a sequence number 1473:2921, indicating that it contains all bytes from byte #1473 to byte #2920 (= 2921 - 1) in the stream, which is a total of 1448 bytes.

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

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

```
00:34:41.482047 IP maple.csail.mit.edu.5001 > willow.csail.mit.edu.39675: Flags [.], ack 2921, win
159, options [nop,nop,TS val 282202095 ecr 282136474], length 0
```

Again, for teaching purposes, we typically talk about an ACK reflecting the corresponding packet's sequence number. In reality, the ACK reflects the next byte that the receiver expects. The above ACK indicates that maple has received all bytes from byte #0 to byte #2920. The next byte that maple expects is byte #2921. The time stamp 00:34:41.482047, denotes the time at which the ACK was received by willow.

Question 1: What are the IP addresses of maple and willow on this network? (Hint: Check the man page of tcpdump to discover how you can obtain the IP addresses)

Question 2: A TCP connection runs not just between two machines, but between two specific *ports* on those machines. What ports are used in the connection between willow and maple?

This tool needs to be loaded in a new browser window

Load Understanding tcpdump in a new window