BITS, Pilani - Hyderabad Campus

CS F303 (Computer Networks)

Second Semester 2022-23

Lab Sheet 5

1. Understanding TCP packets
   a) Open wireshark and start a capture on the **lo** interface on your machine
   b) Run the TCP server and client programs from **Lab Sheet 3**
   c) Apply a display filter for TCP traffic from/to the port you are running the server on
   d) For the above
      i. Identify the TCP SYN packet sent by the client to the server. How would you identify if a given TCP packet is a SYN packet?
         1. What is the sequence number?
         2. What are the source and destination ports?
         3. What is the TCP window size in the packet? What does it mean?

      ii. Identify the TCP SYNACK packet sent by the server to the client. How would you identify if a given TCP packet is a SYNACK packet?
         1. What is the sequence number?
         2. What is the ACK number? Verify that the ACK number is in accordance with the Sequence number in the part above.
         3. What are the source and destination ports?
         4. What is the TCP window size in the packet? What does it mean?

      iii. Identify the TCP ACK sent by the client to the server.
         1. What is the sequence number of the packet?
         2. What is the ACK number? Verify that the ACK number is in accordance with the Sequence number in the part above.

      iv. Run the TCP server/client programs to transfer a file over the network and capture the packets on wireshark. Use this big file: https://drive.google.com/file/d/1Lh8-xGv1fRN4dDUrFEbCg2NasWV6LRRT/view?usp=share_link
         1. Observe the TCP SYN/SYNACK/ACK packets and answer the questions in the parts above

2. In the server (recipient of file), set the SIZE macro to 1. In essence, you are reading 1 byte from the socket in each recv() call.
    1. Trace the TCP Window Full Messages. What do they mean?
    2. Trace the TCP ZeroWindow Messages. What do they mean?
    3. Trace the TCP Window Update messages. What do they mean?