CSE 421 **ID: ____________**

Transport Layer Protocols (TCP) Examination Lab

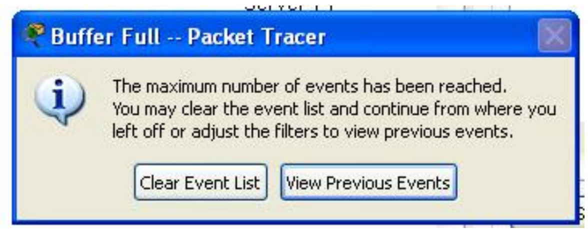
Objectives:

Capture traffic and observe the PDUS for TCP when a HTTP request is made.
.

Task 1: Observe TCP traffic exchange between a client and server.

Step 1 – Run the simulation and capture the traffic.

- Enter **Simulation** mode.
- Check that your Event List Filters shows only **HTTP** and **TCP**.
- Click on the PC1. Open the **Web Browser** from the **Desktop**.
- Enter **www.bracu.ac.bd** into the browser. Clicking on **Go** will initiate a web server request. Minimize the Web Client configuration window.
- A TCP packet appears in the **Event List**, as we will only focus on TCP the DNS and ARP packets are not shown.
- Click the **Auto Capture / Play** button to run the simulation and capture events.
- Sit tight and observe the packets flowing through the network.



Buffer Full -- Packet Tracer

The maximum number of events has been reached. You may clear the event list and continue from where you left off or adjust the filters to view previous events.

- When the above message appears Click “View Previous Events".
- Click on PC1. The web browser displays a web page appears.

Step 2 – Examine the following captured traffic.

Our objective in this lab is only to observe TCP traffic.

	Last Device	At Device	Type
1.	PC1	Switch 0	TCP
2.	Local Web Server	Switch 1	TCP
3.	PC1	Switch 0	HTTP
4.	Local Web Server	Switch 1	HTTP
5.	PC1 (after HTTP response)	Switch 0	TCP
6.	Local Web Server	Switch 1	TCP
7.	PC1	Switch 0	TCP

- As before find the following packets given in the table above in the **Event List**, and click on the colored square in the **Info** column.

- When you click on the Info square for a packet in the event list the **PDU Information** window opens. If you click on these layers, the algorithm used by the device (in this case, the PC) is displayed. View what is going on at each layer.

For packet 1::

Click onto “Inbound PDU details” tab. Scroll down and observe the TCP header. A.

What is this TCP segment created by PC1 for? How do you know what is it for?

_______Here TCP segment has been created for Three Way Handshake process with the server. Here we can see both sequence and acknowledgement value are 0. So, we can say it is the first step of three-way handshake.____

____

____

B. What control flags are visible?

000010 which is sync
request.____

C. What are the sequence and acknowledgement numbers?

____________Both sequence and acknowledgement numbers are
0.____

For packet 2:

Click onto “Inbound PDU details” tab. Scroll down and observe the TCP header.

A. Why is this TCP segment created by the Local Web Server?

___________For sending data the TCP segment created by the Local Web Server.
Now TCP segments can be exchanged between the client and server. TCP uses sequence numbers to verify the correct delivery and ordering of TCP
segments.____

____

____

B. What control flags are visible?

010010

____

C. Why is the acknowledgement number “ 1”?

As it is the second phase of Three way handshaking and server needs to have the next data from user which is supposed to sequence number
1.____

____

For packet 3:

This HTTP PDU is actually the third packet of the “Three Way Handshake” process, along with the HTTP request.

A. Explain why control flags **ACK(Acknowledgement)** and **PSH (Push)** are visible in the TCP header?

________We use control flags ACK to ensure that the server has received the previous data that was sent. So ACK visible here means the server received all the previous data. PSH indicates that the data should be pushed up to the receiving application immediately.
As here data has been pushed immediately rather than waiting so PSH is visible.____

____

For packet 5:

After PC1 receives the HTTP response from the Local Web Server, it again sends a TCP packet to the Local Web server why?

To terminate the TCP connection
____

____

Click onto “Inbound PDU details” tab. Scroll down and observe the TCP header.

A. What control flags are visible?

__________ 010001____

B. Why the sequence number is 104 and acknowledge number 254? Note this packet is created after PC1 receives the HTTP response from the server.

_______Acknowledge number 254 means total 254 bytes of data has been received. It means user has sent data till sequence number 103 and the next sequence number is 104. Here, The sequence number is used to establish a connection, while the acknowledgment number informs us about the package that needs to be synchronised with the rest of the data
____

____

____

____

For packet 6:

Click onto “Inbound PDU details” tab. Scroll down and observe the TCP header.

What is this packet sent from the webserver to PC1 for?

________As the PC1 sends a TCP packet to terminate the TCP connection. The local web server that sends a TCP packet to confirm if the user really wants to terminate the TCP connection. So the packet is sent for confirmation of terminating the TCP connection.
____

____

What control flags are visible?

_________010000____

Why the sequence number is 254?

________It means user has sent data till sequence number 253 and the next sequence number is 254.
____

____