CSE 421 **ID: 23341124**

Transport Layer Protocols (TCP) Examination Lab

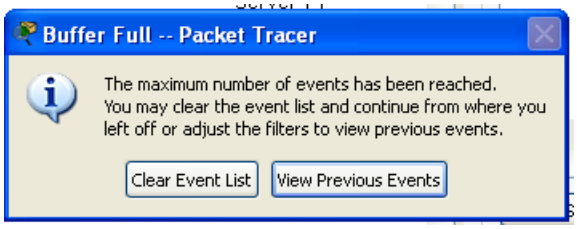
Objectives:

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.



- 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?

PC1 created this to open TCP connection. The sequence and acknowledge no. is 0 so it is requesting the server side.

B. What control flags are visible?

SYN flag is visible

C. What are the sequence and acknowledgement numbers?

sequence number is 0 and acknowledgment number is 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?

It shows that local server knows the request for TCP connection

B. What control flags are visible?

ACK and SYN flags are visible.

C. Why is the acknowledgement number “ 1”?

ACK number 1 means that server has acknowledgment about request for TCP connection.

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?

ACK is visible because PC1 has TCP packet sent by server and PSH is visible because PC1 wants the content

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 close the connection.

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

A. What control flags are visible?

ACK and FIN flags are visible.

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.

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?

To close connection of the TCP by PC1

What control flags are visible?

ACK and FIN are visible

Why the sequence number is 254?