CSE 421 **ID:** 19101532

Transport Layer Protocols (TCP) Examination Lab

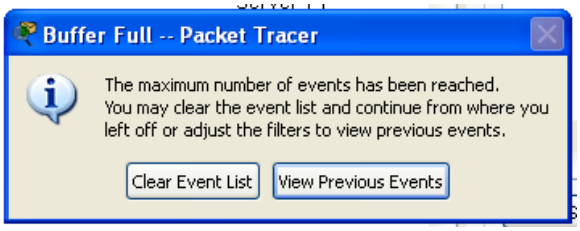
Objectives:

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?

This TCP segment created by PC1 to establish/sync connection by three way handshaking.

It is to sync because, only the sync flag value is 1 in the segment.

B. What control flags are visible?

SYN control flags are visible.

C. What are the sequence and acknowledgement numbers?

sequence number is 0 and acknowledgement 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?

This TCP segment is sent by the server as an acknowledgement of the previous TCP

sync request sent by PC1. This is in the 2nd step of three way handshaking.

B. What control flags are visible?

SYN and ACK control flags are visible.

C. Why is the acknowledgement number “ 1”?

The acknowledge number is 1 because the receiver expects to receive the next byte whose sequence

number will be 1. It also depicts that the receiver has data till acknowledge number 1(excluding).

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?

As it is the third step of three way handshaking, after getting the acknowledgement from the server,

it sends the HTTP request with enable push that means the data should be sent now.

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?

After getting the response from the server, PC1 needs to close the TCP connection that was opened before requesting the server for the webpage. So, it again sends TCP packet to close the connection.

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

A. What control flags are visible?

FIN flag is 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.

The acknowledge number of previous HTTP packet sent by the server was 104 and so the sequence number is 104 which means previous 103 bytes are acknowledged by the server. Now the HTTP packet data content size is 151 bytes. After adding previous acknowledged data with it, we get 103+151=254 bytes. That's why acknowledge number is 254.

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?

It's a response TCP packet where the server has acknowledged the request TCP packet for closing the connection.

What control flags are visible?

FIN flag is visible.

Why the sequence number is 254?

The sequence number is 254 because the previous packets acknowledge number was 254 which was sent by the server to PC1.