CSE 421 **ID:** 19101189

Transport Layer Protocols (TCP) Examination Lab

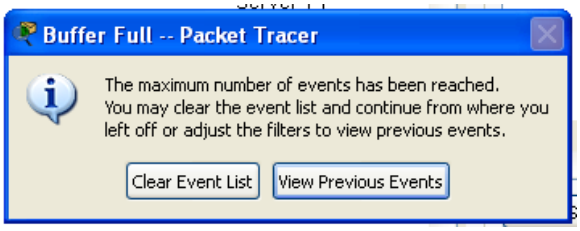
Objectives:

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 is created by PC1 to open a TCP connection to the local server so that PC1 can send HTTP request through it.

It is known via SYN flag value , here it it 1.

B. What control flags are visible?

The SYN (synchronization) flag is visible.

C. What are the sequence and acknowledgement numbers?

Sequence number = 0 and acknowledgement number = 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 created by the local server to uphold that the server acknowledge the request to open a TCP connection by PC1 and also the server want to open a TCP connection with PC1.

B. What control flags are visible?

The ACK (acknowledgement) and the SYN (synchronization) flags are visible.

C. Why is the acknowledgement number “ 1”?

The acknowledgement number is 1 because the local web server has received the byte with sequence number 0 and it is waiting for the next sequence of byte that is 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?

The ACK flag is visible because PC1 has acknowledged the TCP connection that is the server want to establish. And the PSH flag is visible cause PC1 want to push data via HTTP request to the application layer.

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?

For closing the TCP connection.

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

A. What control flags are visible?

The ACK (acknowledgement) flag and the FIN (finished) flag.

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.

Sequence number is 104 as the first byte of the new packet from PC1 has this sequence.

And the acknowledge number is 254 as PC1 expecting byte number 254 from the web 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?

This packet is sent from the web server for the acknowledgement of the closing the TCP connection

that was requested by PC1 as well as the TCP closing request by the server to the PC1.

What control flags are visible?

The ACK (acknowledgement) flag and the FIN (finished) flag.

Why the sequence number is 254?

Because this is the sequence of the last segment sent by the web server , which is PC1 expecting.