CSE 421 **ID:** 19301257

Transport Layer Protocols (TCP) Examination Lab

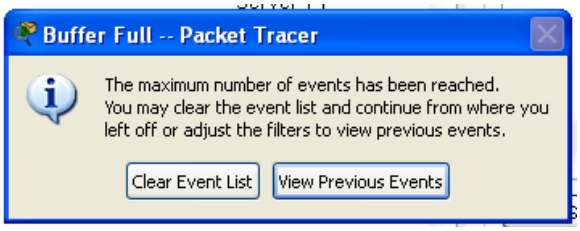
Objectives:

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?

When PC1 initiates a connection with the server via three-way handshake, it does so by generating a TCP Segment. Control bitssegment is part of the TCP header. As PC1 has set the synchronization bit (the packet's final bit) to 1, it is attempting to establish a connection with the server.

B. What control flags are visible?

Synchronization control flag

C. What are the sequence and acknowledgement numbers?

Sequence 0 in Packet 1 with Acknowledgement 0 sent.

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?

The local web server generates this TCP segment to confirm the successful completion of the three-way handshake.

B. What control flags are visible?

ACK, SYN

C. Why is the acknowledgement number “ 1”?

The first computer (PC1) has received byte 0 and is waiting for byte 1 to continue the conversation.

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 PC1 is acknowledging data received from the server, the ACK bit is 1, and the PSH bit is 1, the server should start processing the data that PC1 is preparing to send immediately.

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?

This link has been broken.

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

A. What control flags are visible?

ACK,FIN

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 105 is observed, rather than Sequence Number 104. This means that an HTTP packet/data of size 104 bytes has been received, and the connection has been closed due to a Sequence Number 105 signal. With acknowledgement number 254, PC1 knows to look out for the 254th byte in the following transmission.

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?

Verification of Disconnection or Closure.

What control flags are visible?

ACK,FIN

Why the sequence number is 254?

A confirmation number of 254 indicated that PC1 had successfully received data up to byte 253. The current expected data byte is 254, making Packet 5's sequence number 254.