CSE 421 **ID:** 20101347

Transport Layer Protocols (TCP) Examination Lab

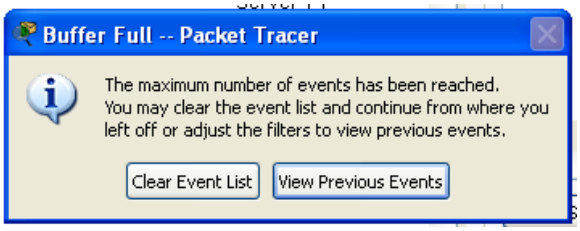
Objectives:

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 has been made for laying out an association with the Server. We know this by glancing at the Control Pieces/Banners section of the TCP Header. We can see that the SYN bit (Ob00000010) has been set. That implies it is making an association with the Server.

B. What control flags are visible?

The synchronization (SYN- Ob00000010) control flag is visible.

C. What are the sequence and acknowledgement numbers?

SEQUENCE NUMBER: 0 : 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 fundamentally the Second packet of the three-way handshake process. This TCP section fundamentally recognizes that the Client is attempting to make an association with the Server, and consequently, the Server sends an ACK in addition to the SYN bundle back to the Client to begin the association.

B. What control flags are visible?

The ACK(Acknowledgment) and SYN(Synchronization) bits of the Control Flags are visible.

C. Why is the acknowledgement number “ 1”?

The Acknowledgment number is 1 because the Server has gotten the principal byte from PC1 and thus hopes to get Portions beginning from byte 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?

ACK digit is 1 since the Client (PC1) is telling the Server about the affirmation of the recently gotten information, and the PSH cycle being 1 shows that the information which will be sent by PC1 needs to quickly be handled and shipped off the upper 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?

This TCP segment is for closing the connection which was created before .

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

A. What control flags are visible?

The ACK(Acknowledgement : 0b00010001) bit and FIN(Final: 0b00010001) bit of the control 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.

The sequence number is 105 here because the Server, while sending the HTTP Reaction, shared with PC1 that it had gotten 104 bytes of information and hoped to get information from byte number 105. The acknowledgment number 254 implies that PC1 had gotten bytes till 253, and it hopes to get bytes beginning from 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?

This packet transported off PC1 is essentially the second packet of the three-way handshake for closing the affiliation. It is basically seeing whether it makes sure about the affiliation being closed or not

What control flags are visible?

The ACK (Acknowledgement: 0b00010001) and FIN (Final: 0b00010001) bits of the Control flags are visible.

Why the sequence number is 254?

This is because, in the past packet, it got an affirmation number of 254, which fundamentally implied that PC1 had gotten information till the 253rd byte and hopes to get information from the 254th byte. In this way, it begins it first-byte number from 254 and subsequently specifies it in the Grouping Number.