CSE 421 **ID:** 19301261

Transport Layer Protocols (TCP) Examination Lab

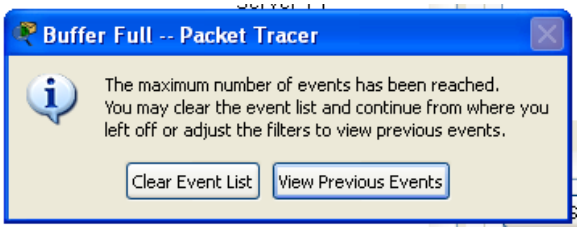
Objectives:

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 established this TCP segment in order to perform three-way handshaking and establish a connection. For synchronization purposes, the segment has simply a single sync flag with a value of 1.

B. What control flags are visible?

SYN Control flags

C. What are the sequence and acknowledgement numbers?

Both the acknowledgment and sequence numbers are 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?

In response to PC1's prior TCP sync request, the server sends the following TCP segment. The second step of a three-way handshake consists of this.

B. What control flags are visible?

SYN & ACK control flags

C. Why is the acknowledgement number “ 1”?

The reason the acknowledge number is 1 is because the receiver anticipates receiving the following byte, which will also have a sequence number of 1. Additionally, it demonstrates that the recipient possesses data up until acknowledgement 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?

Because this is the third step of the three-way handshake, after it has received the acknowledgement from the server, it will send the HTTP request with enable push, which indicates that the data should be transferred 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?

PC1 is required to terminate the TCP connection that was opened before to sending a request to the server for the website after it has received a response from the server. Therefore, it sends another TCP packet in order to terminate the connection.

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

A. What control flags are visible?

FIN control 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.

Since the preceding HTTP packet delivered by the server had an acknowledgement number of 104, the sequence number of 104 indicates that the server has acknowledged the previous 103 bytes. The current data size of an HTTP packet is 151 bytes. Adding this to the previously acknowledged data gives a total of 254 bytes (103 + 151). Due to this fact, the acknowledgement 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, which indicates that the server has acknowledged the request TCP packet for ending the connection.

What control flags are visible?

FIN control flag.

Why the sequence number is 254?

Because the server acknowledged PC1's previous packet with acknowledgement number 254, the sequence number is 254.