CSE 421 **ID: 19301151**

Transport Layer Protocols (TCP) Examination Lab

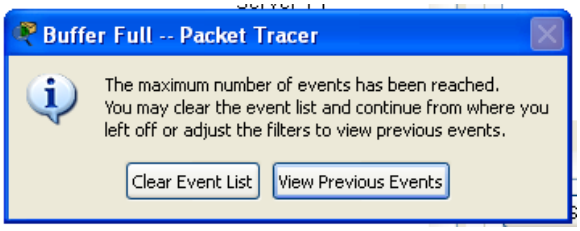
Objectives:

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 for sending a SYN single to the server. And we can indentify it via looking at FLAGS options of TCP tab. As it's 2nd last bit is 1, it is for SYN signal.

B. What control flags are visible?

All control flags are visible here, but only SYN flag is turned on in this packet.

C. What are the sequence and acknowledgement numbers?

Sequence number is 0 and the acknowledgement number is also 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 segmnet is created by the Local Web Server in reply to the 1st packet given by the PC1 side. Now this TCPsegment is created by the Local Web Server to let know the PC1 that it is also ready to create a secure connection with PC1. In short, it giving the PC1 a acknowlegment that it is ready to receive HTTP request from PC1.

B. What control flags are visible?

SYN and ACK flags are visible for packet 2.

C. Why is the acknowledgement number “ 1”?

As the Server acknowledging the request from PC1 in this state, that's why the acknowledgement number is 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?

As we know The PSH flag is used to request immediate delivery of data to the receiving application layer without delay or buffering. and the ACK flag is used to acknowledge the receipt of data segments in TCP. For packect 3 these two are open because PC1 is need a immediate delivery of data from the server.

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 PC1 receives the HTTP response from the local web server, it again sends a TCP packet to the local web server to close the TCP connection.

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

A. What control flags are visible?

Only ACK and FIN 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.

Here sequence number is 104 means the clint PC1 has sends a data up to 104 byte. And via sendingacknowledgement number 254 it means now it wants data from that range. i.e. it it reecives the data upto 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?

TCP close packet send to PC1 to let the PC1 knows it got the FIN signle from it and the server is also all set to close the connection, that's why it sends both the ACK and FIN signle together. Where ACK for it got the close signal form PC1 and FIN for it also ready to close the connection.

What control flags are visible?

ACK and FIN control flags are visible.

Why the sequence number is 254?

The sequence number 254 means the server sends the data to the client from 254 byte.