

Transport Layer Protocols (TCP) Examination Lab

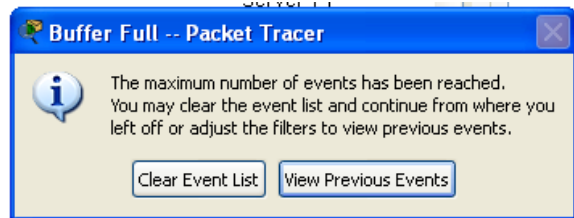
Objectives:

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?

Ans : The TCP segment created by PC1 is for the 3-way handshaking with the server which is to establish a reliable communication with the server. It is in the first phase of the handshake process with the local web server which the sequence and acknowledgement number is 0.

B. What control flags are visible?

Ans : SYN (synchronize) flag is visible.

C. What are the sequence and acknowledgement numbers?

Ans : Sequence no- 0 and Acknowledgement number is 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?

Ans : The TCP segment was created by the Local Web server in response to the SYN request of PC1.

B. What control flags are visible?

Ans : SYN (synchronization) flag and the ACK (Acknowledgement) flag is visible.

C. Why is the acknowledgement number “ 1”?

Ans : Because the local web server acknowledged the request so it turn ACK flag to 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?

Ans : The ACK flag is visible because the request was successfully received and the PSH flag is visible to tell the server to back the HTTP to PC1.

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?

Ans : Because it tells that PC1 has received the HTTP packet and it wants to terminate the connection.

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

A. What control flags are visible?

Ans : The ACK (Acknowledgement) flag and FIN (Finish) flag is 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.

Ans : The sequence number is 104 because there are a total of 104 packets transferred and the acknowledge number is 254 due to the FIN flag.

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?

Ans : It is to determine ~~whether to terminate the connection or not.~~

What control flags are visible?

Ans : The ACK flag and FIN flag is visible.

Why the sequence number is 254?

Ans : Since a total of 254 packets has been transferred the sequence number is 254.