CSE 421 **ID:** 20101065

Transport Layer Protocols (TCP) Examination Lab

Objectives:

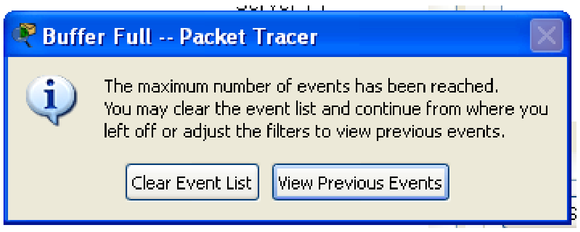
Capture traffic and observe the PDUS for TCP when a HTTP request is made.

.

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 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.



Buffer Full -- Packet Tracer

The maximum number of events has been reached. You may clear the event list and continue from where you left off or adjust the filters to view previous events.

- 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?

The TCP Segment is created by the PC-1 to establish the connection of PC-1 and the server using the three-way handshake. The second last bit of control flag is 1 to define that the synchronization is enabled.

B. What control flags are visible?

SYN Control Flag is visible

C. What are the sequence and acknowledgement numbers?

Sequence Number is 0 and 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 is created as the acknowledgement of the three way handshake process.

B. What control flags are visible?

SYN and ACK control flags are visible.

C. Why is the acknowledgement number “ 1”?

It indicates that it is now expecting byte number 1 as it has received the previous one.

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 bit is visible as the acknowledgement of the received data. On the other hand, PSH means that the sent data of PC 1 needs to process 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?

A TCP Close request is required to close the connection.

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.

Acknowledge number 254 means PC-1 is expecting the 254th bit now.

The sequence number 104 means it has received HTTP packet of 104 bytes and the next 105 is the connection close.

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?

Connection close confirmation.

What control flags are visible?

FIN and ACK

Why the sequence number is 254?

The sequence number 254 means that it has received until byte number 253 and the next expecting byte is 254.