CSE 421 ID: 20101381

Transport Layer Protocols (TCP) Examination Lab

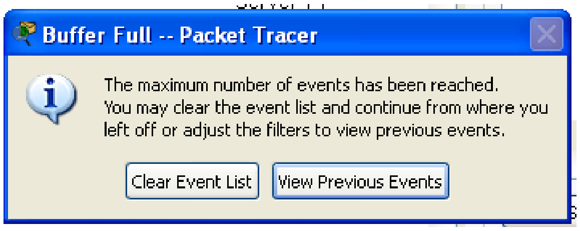
Objectives:

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.



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?

This TCP segment has been created for establishing a connection with the Server. We know this by looking at the Control Bits/Flags segment of the TCP Header. We can see that the SYN bit has been set. That means it is creating a connection with the Server.

B. What control flags are visible?

Only the Synchronization (SYN- 0b00000010) 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 the Second packet of the three way handshake process. That's why it was created by the local web server.

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”?

Because the Server has received the first byte from PC1 and hence expects to receive segments starting 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 bit is 1 since the client PC1 is letting the server know about the acknowledgment of the previously received data and PSH bit being 1 indicates that the data which is going to be sent by PC1 has to immediately been processed and sent to 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 that 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 because while sending the HTTP Response the server indicated PC1 that it had received 104 bytes of data and it expects to receive data from byte number 105. The acknowledgement number being 254 means that PC1 had received bytes till 253, and it expects to receive bytes starting 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 sent to PC1 is actually the second packet of the three way handshake for closing the connection. In fact, it's asking PC1 whether it is sure whether the connection is lost.

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 previous packet, it received an acknowledgment number of 254 that meant PC1 had received data till the byte no. 253, and expects to receive data from the byte no. 254. So, it starts it first byte number from 254 and hence mentions it in the sequence number.