CSE 421 **ID:18301124**

Transport Layer Protocols (TCP) Examination Lab

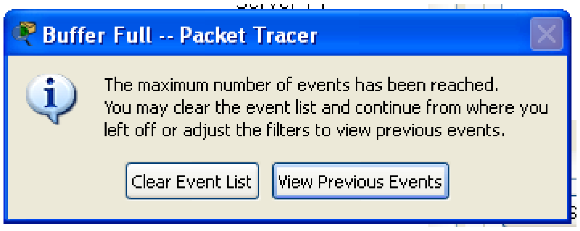
Objectives:

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.



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?

To initialize 3-way hand shake and it can be known by observing sequence and acknowledgment number. As both of these is 0 and SYN bit is enabled these means Three-ways hand-shake.

B. What control flags are visible?

Control flag: 0b00010010

C. What are the sequence and acknowledgement numbers?

Both sequence and acknowledgment 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?

This is the response of the Three-way handshake.

B. What control flags are visible?

Control flag: 0b00010010

C. Why is the acknowledgement number “ 1”?

Acknowledgment number is '1' because, Since it got the first part of handshake as 0. This is the second part of three way handshake and it is acknowledgment from local web server of PC-1's connection request.

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 (Acknowledgment) and PSH (Push) are visible in the TCP header?

ACK indicates that the packet is successfully received. PSH is the request for pushing the data from the server side to the client side without delay no matter the data buffer full or not, the data needs to be sent 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?

To terminate or end TCP connection.

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

A. What control flags are visible?

0b00010001

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 104 because, it detects PC-1 sends 104 bit of data till now.And acknowledgment is 254 because it has received data upto 253 and expecting the 254 th one.

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 packet part for closing TCP connection.

What control flags are visible?

0b00010001

Why the sequence number is 254?

It means it sent 254 th sequence of data