CSE 320 ID: 18301297 Transport Layer Protocols (TCP)

Examination Lab

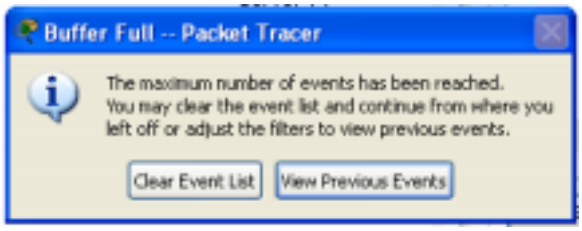
Objectives:

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?

Answer : This TCP segment was created by PC1 to establish a connection with the server. TCP uses a three-way handshake to establish a connection. Before a client attempts to connect with a server, the server must first bind to and listen at a port to open it up for connections

_____

_____

_____

B. What control flags are visible?

Answer: SYN

_____

C. What are the sequence and acknowledgement numbers?

Answer : Acknowledgment:0,Sequence: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?

Answer: For transferring data this TCP segment created by the local webserver.

_____

_____

_____

B. What control flags are visible?

Answer: SYN and ACK

_____

C. Why is the acknowledgement number “ 1”?

Answer: It means the webserver is requesting bit no 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?

Answer : PSH flag used to true for the socket and with that TCP starts pushing the data immediately.
ACK flag used for connection establishment to tell the sender that it received its initial packet.

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?

Answer : HTTP works as a request-response protocol between a client and server.

Example: A client (browser) submits an HTTP request to the server; then the server returns a response to the client. The response contains status information about the request and may also contain the requested content

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

What control flags are visible?

Answer : ACK and 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.

Answer : The sequence number is 104 because the previous acknowledgment number was 104 and the acknowledge number is 254 because now it receives 253 bytes.

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?

Answer : This packet is for connection termination.

What control flags are visible?
Answer : ACK and FIN

Why the sequence number is 254?

Answer : The web server is requesting for 254th data.