

## 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.

|    | <b>Last Device</b>        | <b>At Device</b> | <b>Type</b> |
|----|---------------------------|------------------|-------------|
| 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?

**TCP segment is opened by PC1 to make connection with local server after the SYN flag.**

B. What control flags are visible?

**SYN.**

C. What are the sequence and acknowledgement numbers?

**Both are 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?

**To ask the server if it is ready or not to establish connection.**

B. What control flags are visible?

**SYN and ACK.**

C. Why is the acknowledgement number “1”?

**The sequence of the next segment will be 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 is the prove that the connection got established and PSH is the prove that the data is getting transferred.**

**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?

Confirming termination of connection.

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

A. What control flags are visible?

FIN and ACK.

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 next sequence will be 254 that's why acknowledge number is 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?

To confirm termination and acknowledgment of the very last data.

What control flags are visible?

FIN and ACK

Why the sequence number is 254?

253 segments got delivered by the sender, that's why receiver gave an acknowledgment number of 254.