Application Layer Protocols (HTTP.SMTP/POP)
## Examination Lab

Objectives:

Capture traffic and observe the PDUS for HTTP, SMTP, POP.

Task 1: Observe HTTP traffic exchange between a client and server.

Step 1 – Run the simulation and capture the traffic.

- Enter **Simulation** mode.
- 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.
- Two packets appear in the **Event List**, a DNS request needed to resolve the URL to the IP address of the web server and an ARP request needed to resolve the IP address of the server to its hardware MAC address.
- Click the **Auto Capture / Play** button to run the simulation and capture events.
- Sit tight and observe the packets flowing through the network.
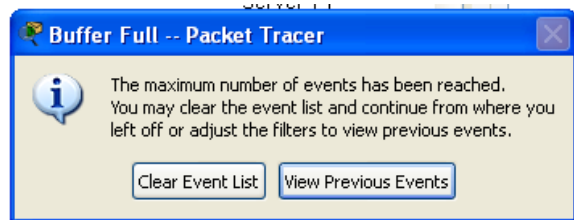
- When the above message appears Click "View Previous Events".
- Click on PC1. The web browser displays a web page appears.

Step 2 – Examine the following captured traffic.

Our objective in this lab is only to observe HTTP traffic.

	Last Device	**At Device**	**Type**
1.	PC1	Switch 0	HTTP
2..	Local Web Server	Switch 1	HTTP

- 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.

- Examine the PDU information for the remaining events in the exchange.

For packet 1::

What kind of HTTP packet is packet no. 1?
Packet no. 1 is HTTP request packet. PC1 is making the HTTP request to local web
server to fetch the website

_____

Click onto "Inbound PDU details" tab. Scroll down at the end, what do you see?
We see HTTP Request Information. Here, Are the details- HTTP Data:Accept-
Language: en-us
Accept: */*
Connection: close
Host: www.bracu.ac.bd

For packet 2:

Click onto "Inbound PDU details" tab. Scroll down at the end, what do you see? What kind of
HTTP packet is this?

_____

The HTTP packet consists of HTTP Response Information. We can see details of HTTP
response information the requested server of www.bracu.ac.bd. Here we can see the HTTP
Response Information details.
HTTP Data:Connection: close
Content-Length: 151
Content-Type: text/html
Server: PT-Server/5.2

Task 2: Observe email traffic exchange between a client and email server using SMTP and POP3.

Step 1 – Run the simulation and capture the traffic.

- On the Event List window click "Reset Simulation" button. All previous packets will disappear.
- At the bottom of the Event List window, there is a filter which filters the protocols that we want to see. Click Edit filters. Another window appears showing different protocols, unclick HTTP and click SMTP and POP3.
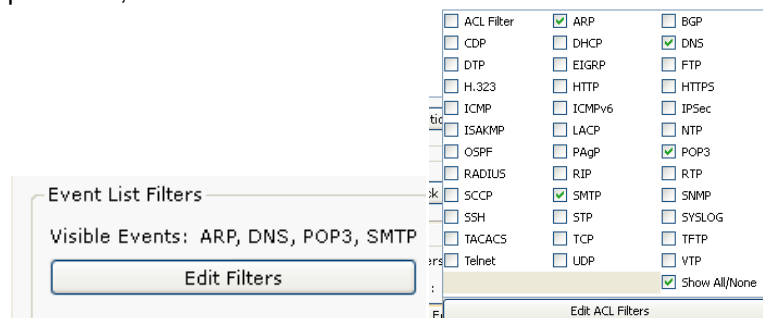
- Click a space anywhere outside the popup window, then it will disappear.
- Your Event List Filter should be as shown below:

Event List Filters

Visible Events: ARP, DNS, POP3, SMTP

[Edit Filters] [Show All]

- Now click on the PC1. Close the web browser window. Open the **Email** from the **Desktop**. A mail browser window will open. Click "compose", another window appears.

Compose Mail

Send   To: sakib@bracu.ac.bd

Subject: Hello|

- Fill the window as shown and press send.
- Minimize the client window .
- Click the **Auto Capture / Play** button to run the simulation and capture events.
- Sit tight and observe the packets flowing through the network.
- This interaction is between the sender client and its email server.

Step 2 – Examine the following captured traffic.

Our objective in this lab is only to observe SMTP traffic.

	Last Device	At Device	Type
3.	PC1	Switch 0	DNS
4.	PC1	Switch 0	SMTP
5.	Bracu Email Server	Switch 1	SMTP

- Find the following packets given in the table above in the **Event List**, and click on the colored square in the **Info** column.
- Examine the PDU information.

For packet 4::

What is the purpose of this DNS packet?

 The purpose of this DNS packet to get the IP Address of BRACU Email Server.
_____

_____

For packet 5& 6::

Explain why SMTP packet was sent to the email server and the server replied with an SMTP packet?

The SMTP Packet was sent by PC1 to BRACU Email server, once it has the IP Address and MAC

Address of BRACU Email Server. This SMTP packet that was sent by PC1 is the mail for the

sakib@bracu.ac.bd . Once server received this SMTP packet then it sends Acknowledgement SMTP

packet to the PC1 which is the confirmation of the sent mail.

3

Step 3 – <u>Run the simulation and capture the traffic for POP.</u>

- On the Event List window click "Reset Simulation" button. All previous packets will disappear.
- Now click on the PC0. Open the **Email** from the **Desktop**. A mail browser window will open. Click "**receive**", minimize the window.
- Click the **Auto Capture / Play** button to run the simulation and capture events.
- Sit tight and observe the packets flowing through the network.
- This interaction is between the sender client and its email server.

Step 2 – <u>Examine the following captured traffic.</u>

Our objective in this lab is only to observe POP traffic.

	Last Device	At Device	Type
6.	PC1	Switch 0	DNS
7.	PC1	Switch 0	POP3
8.	Bracu Email Server	Switch 1	POP3

- Find the following packets given in the table above in the **Event List**, and click on the colored square in the **Info** column.
- Examine the PDU information.

<u>For packet 6::</u>

What is the purpose of this DNS packet?
The Purpose of The DNS packet is to Ask for the IP Address of BRAC DNS server to check whether it has Any mail for the PC0 user.

_____

<u>For packet 7&8::</u>

Explain why POP packet was sent to the email server and the server replied with a POP packet?
The POP packet was sent to the email server is to look for the emails that has been sent to the
_____
user of sakib@bracu.ac.bd email user. The server replied with a POP packet that has all the
_____

latest mails for the receiver PC0 that are currently has the access of sakib@bracu.ac.bd mail address.

-