

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.

(sec)	Last Device	At Device	Type	Info
--	PC1	DNS		
--	PC1	ARP		
	PC1	Switch0	ARP	
	Switch0	PC0	ARP	
	Switch0	Switch1	ARP	

- 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?

HTTP REQUEST

Click onto “Inbound PDU details” tab. Scroll down at the end, what do you see?

I can see some header information such as which language is accepted, connection type - persistent or not and host server name

For packet 2:

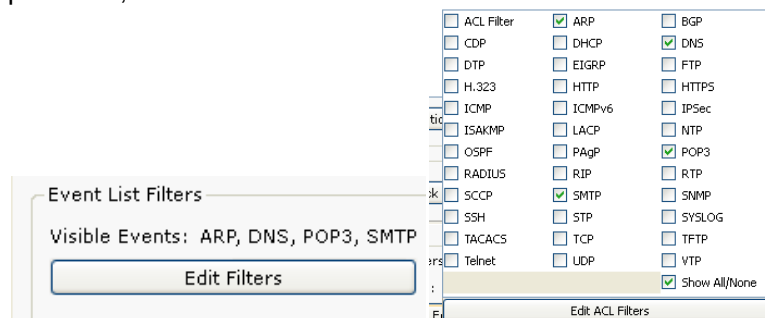
Click onto “Inbound PDU details” tab. Scroll down at the end, what do you see? What kind of HTTP packet is this?

Its an HTTP RESPONSE. Additionally this header has information such as connection type, length of the data in Bytes, content type, Server type (ex-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?

This packet is sent towards the Local DNS server to get the IP address of the email server to PC1 so that it can use the Ip to send the email to the email server.

For packet 5& 6::

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

1. packet PC1 to switch 0 (SMTP): has source IP of the PC1 and destination of the Bracu email server where the email will be stored through this request. We use SMTP request for email storing operation to servers.

2. Bracu Email server then sends back an acknowledgement to the PC1 that the email was received using the SMTP protocol.

Step 3 – Run the simulation and capture the traffic for POP.

- 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 – Examine the following captured traffic.

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.

For packet 6::

What is the purpose of this DNS packet?

The purpose of the DNS packet from PC0 to switch 0 is to get to the local DNS server and get the Ip of the Bracu email server.

For packet 7&8::

Explain why POP packet was sent to the email server and the server replied with a POP packet?

The POP3 was used from PC0 to get the email from server. POP3 is a protocol used for retrieving email from server. One is sent from PC0 to email server to check for email and other to sent back to send the email to PC0.

•