

Application Layer Protocols (HTTP,SMTP/POP)

Examination Lab

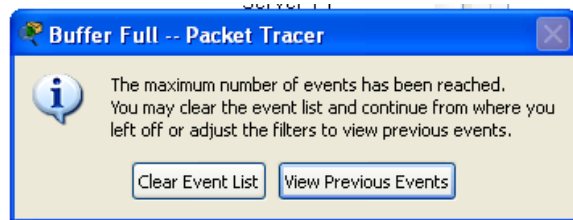
Objectives:

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.



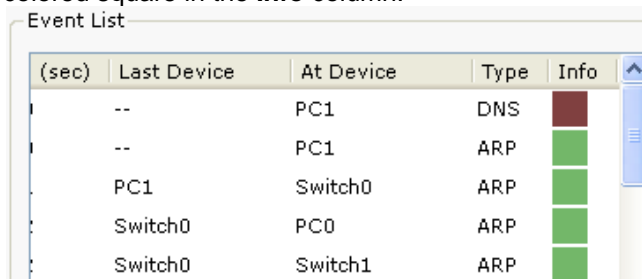
- When the above message appears Click "View Previous Events".
- Click on PC1. The web browser displays a web page appears.

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 1 is an HTTP request packet. It is sent from the client (PC1) to the web server to request access to a web page at www.bracu.ac.bd. The packet contains headers indicating accepted languages, accepted content types, connection instruction, and the host being requested.

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

At the end of the Inbound PDU details, we see the HTTP request details: Accept-Language: en-us, Accept: /, Connection: close, Host: www.bracu.ac.bd

These indicate that the client supports English (US) language, accepts any content type, wishes for the connection be closed after the response, and requests the web page hosted at 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?

At the end of the Inbound PDU details for packet 2, we can see the HTTP response details:

Connection: close, Content-Length: 151, Content-Type: text/html, Server: PT-Server/5.2

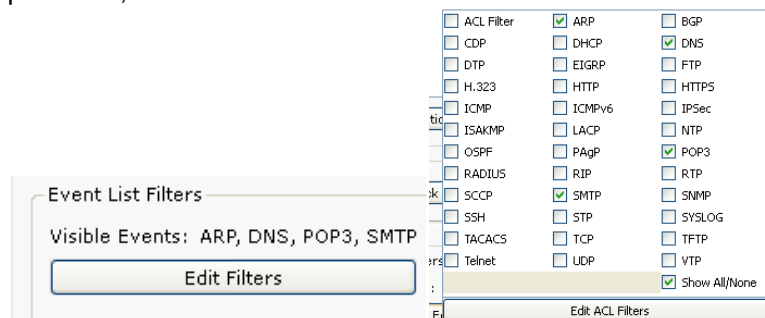
This means the server is replying to the client’s request by sending an HTTP response. The response contains HTML content (151 bytes), specifies that the connection will be closed after transfer, and identifies the server software used

This packet is an HTTP response packet from the web server to the client.

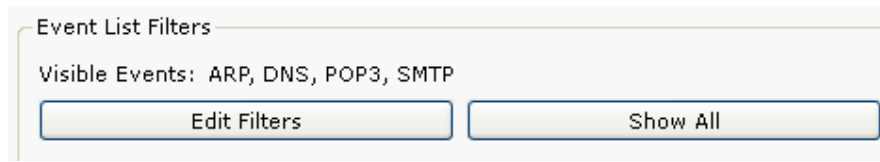
Task 2: Observe email traffic exchange between a client and email server using SMTP and POP3.

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:

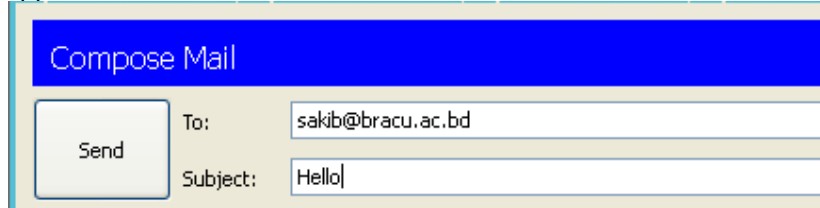


Event List Filters

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 DNS packet is sent from PC1 to the DNS server to resolve the domain name mail.bracu.ac.bd into its corresponding IP address. Without this step, PC1 would not know the correct IP address to contact for sending the email via SMTP. This is a required step before the SMTP session can begin, ensuring the mail is routed to the right server.

For packet 5& 6::

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

PC1 sends an SMTP packet to the email server to initiate the process of delivering an email. This packet carries necessary SMTP commands and the actual email data, starting a communication session with the server. The server responds with its own SMTP packet to acknowledge receipt, provide delivery status, or to continue the SMTP conversation as per the protocol’s operation, ensuring the client knows the outcome or next step in email transmission.

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 DNS packet is used to resolve the domain name mail.bracu.ac.bd to its IP address. This allows the client to identify where to send and retrieve email using POP3. Proper resolution ensures POP3 requests reach the correct mail 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 packet is sent by the client to request email retrieval from the server. The server replies with a POP3 packet, providing the requested email data or response. This exchange enables the client to access and manage emails stored on the server.

•