

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 | PC1 | DNS | Red square |
| -- | PC1 | PC1 | ARP | Green square |
| | PC1 | Switch0 | ARP | Green square |
| | Switch0 | PC0 | ARP | Green square |
| | Switch0 | Switch1 | ARP | Green square |

- 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 a HTTP GET request packet

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

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?

HTTP Data:Connection: close

Content-Length: 151

Content-Type: text/html

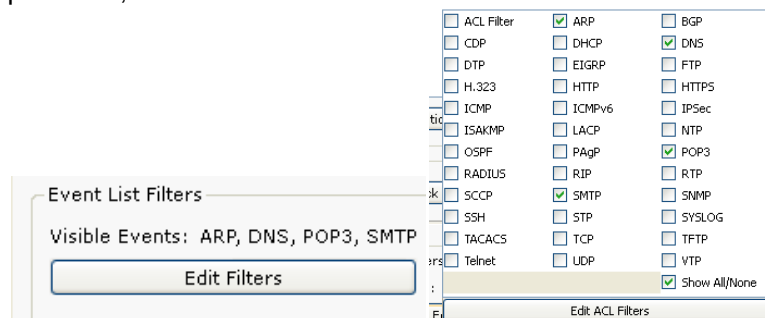
Server: PT-Server/5.2

This is a HTTP response packet which is carrying the requested webpage.

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 DNS packet inquires the IP address of the email server (e.g. mail.bracu.ac.bd) so that the client can communicate with 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?

The SMTP packet was sent to mail email server as it is designed for sending and transferring emails between mail servers and from email clients to email servers. Also, it follows the email protocols and contains email details(sender, recipient, subject, body).

The server replied with the SMTP packet as this protocol replies to the sender with its successful acceptance delivery which ensures that the email is properly transmitted from the sender to the server for further routing.

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 client needs to connect to the mail server to fetch the email by POP3 operation, however the client only has the server's domain name, this DNS packet helps the client to fetch the IP address of the 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 POP packet sent by the client to request the retrieval of incoming emails from the server. To reply to this request, The server send the requested email data to the client. This interaction allows the client to download and view messages stored on the email server.

•