CSE 421 ID: 19101054

Application Layer Protocols (HTTP.SMTP/POP)

Examination Lab

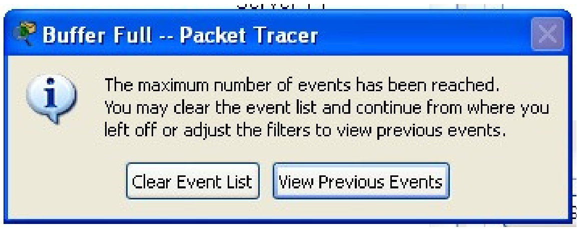
Objectives:

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.



Buffer Full -- Packet Tracer

The maximum number of events has been reached. You may clear the event list and continue from where you left off or adjust the filters to view previous events.

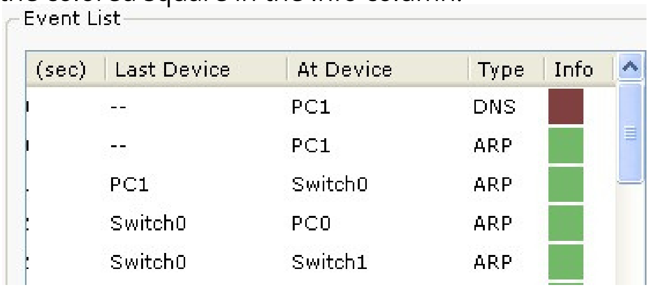
- When the above message appears Click "View Previous Events".
- Click on PC1. The web browser displays a web page appears.

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	HTTP
2..	Local Web Server	0 Switch 1	HTTP

- Find the following packets given in the table above inEvent List , and click on the the colored square in the Info column.



Event List

(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?

Packet no. 1 is a HTTP request.____

____

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

There is an HTTP request from the target host on the "Inbound PDU information" page.
Primarily information about HTTP requests
HTTP Data:Accept-Language: en-us
Accept: */*

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?

Here we can see the details of HTTP response information.______________________
HTTP RESPONSE SECTION HOLDS:
HTTP Data:Connection: close____
Content-Length: 151

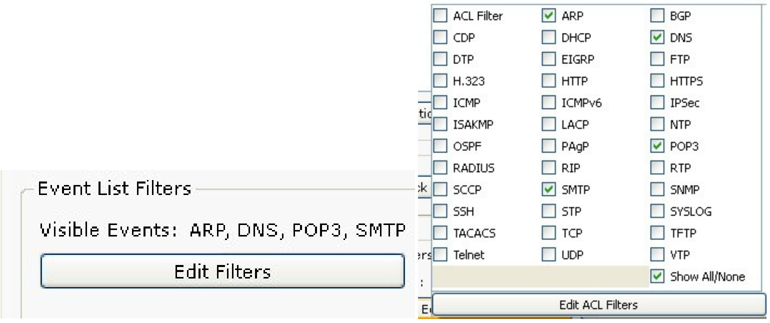
____

____

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.



Event List Filters

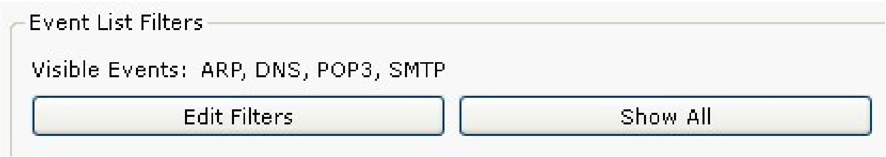
Visible Events: ARP, DNS, POP3, SMTP

Edit Filters

□ ACL Filter	☑ ARP	□ BGP
□ CDP	□ DHCP	☑ DNS
□ DTP	□ EIGRP	□ FTP
□ H.323	□ HTTP	□ HTTPS
□ ICMP	□ ICMPv6	□ IPSec
□ ISAKMP	□ LACP	□ NTP
□ OSPF	□ PAgP	☑ POP3
□ RADIUS	□ RIP	□ RTP
□ SCCP	☑ SMTP	□ SNMP
□ SSH	□ STP	□ SYSLOG
□ TACACS	□ TCP	□ TFTP
□ Telnet	□ UDP	□ VTP
		☑ Show All/None

Edit ACL Filters

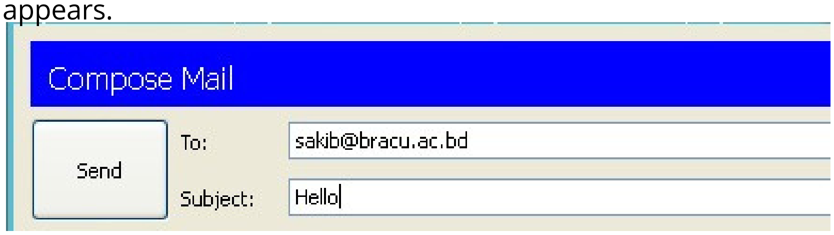
- Click a space anywhere outside the popup window, then it will disappear.
- Your Event List Filter should be as shown below:



Event List Filters

Visible Events: ARP, DNS, POP3, SMTP

- 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

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	DNS
4.	PC1	0	SMTP
5.	Bracu Email Server	Switch 0 Switch 1	SMTP

- Find the following packets given in the table above inEvent List , and click on the 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's purpose is to find the IP address of the 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?

PC1 sent the SMTP packet to the BRACU email server, and after it had the server's IP and MAC, it sent the letter. It sends an acknowledgement SMTP packet to PC1 to verify the mail after receiving the SMTP packet.

____

____

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	DNS
7.	PC1	0	POP3
8.	Bracu Email Server	Switch	POP3

0
Switch
1

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

For packet 6::

What is the purpose of this DNS packet?

This DNS is used to request the IP in order to see if the server has any mail for the user.

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 was sent to the mail server to check for emails that the user had received. The receiver's most recent emails are included in the responded POP package.

——————————————————————————————————————