CSE 421
Lab 2 :Observing DNS and ARP in Packet Tracer

ID 19101038

Introduction:

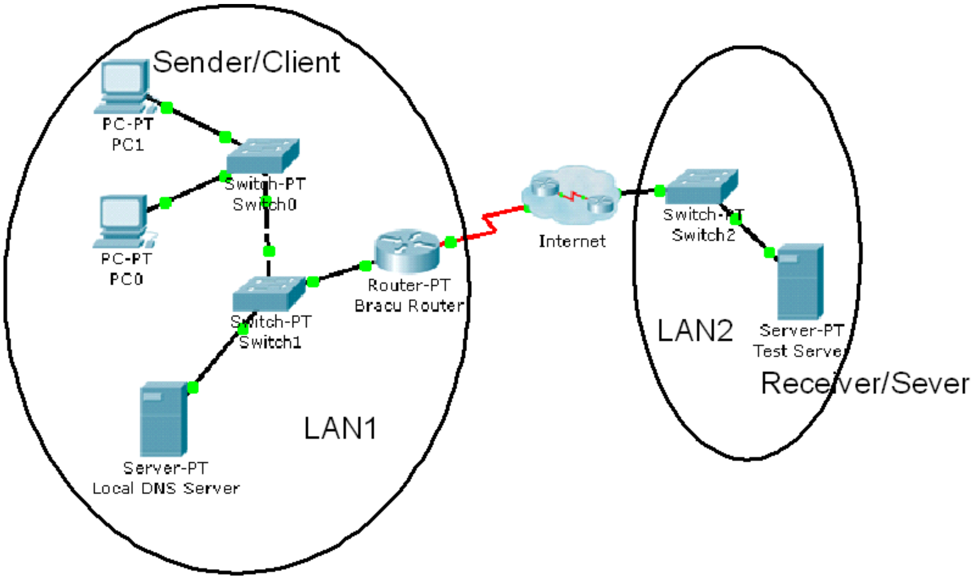
Simulation mode in Packet Tracer captures all network traffic flowing through the entire network . You will observe the packets involved in DNS and ARP process. These two protocols are the helping protocols when a web page is requested using HTTP.

Objectives:

1. Explore how PT uses the OSI Model and TCP/IP Protocols.
   - Creating a Simple PDU (test packet)
   - Switching from Realtime to Simulation Mode

2. Examine a Web Request Packet Processing and Contents
   - Accessing the PDU Information Window, OSI Model View
   - Investigating the layers and addresses in the OSI Model View
   - Animations of packet Flow

Task 1: Observe the network topology shown.

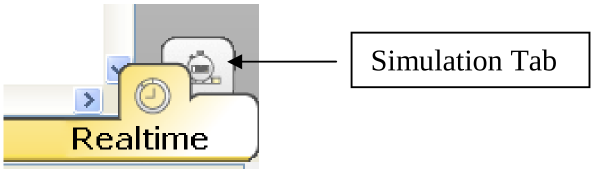


- **PC0**, **PC1** and the **Local DNS server**, **BRACU router** is part of a Local area network. BRACU router connects this LAN to the Internet through an ISP. The **Test server** shown is on another Local area network.
- You will access the web page **www.test.com** which is stored in the Test Web Server through PC1's web browser.
- To access this web page this activity will show you how and what packets are created and how the packets move through the network.
- For this activity we will only focus on DNS and ARP.

Task 1: Capture a web request using a URL from a PC.

Step 1 – Switching from Realtime to Simulation Mode

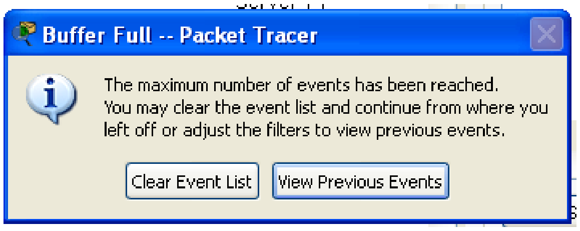
- In the far lower right of the PT interface is the toggle between Realtime and Simulation mode. PT always starts in realtime mode, in which networking protocols operate with realistic timings.



- In simulation mode, you can visually see the flow of packets when you send data from an application. A new window named "**Event List**" will appear. This window will show the packets (PDUs) as colored envelopes.

Step 2 – Run the simulation and capture the traffic.

- Click on the PC1. Click on the **Desktop tab**. Open the **Web Browser** from the **Desktop**.
- Write **www.test.com** into the browser. Clicking on **Go** will initiate a web server request. **Minimize** the PC1 Client window.
- Look at the Event List Window. Two packets appear in the **Event List**, a **DNS request** from **PC1** to the **Local DNS server** needed to resolve the URL "www.test.com" to the IP address of the Test server.
- Before the DNS request can be sent, we need to know the DNS Server's MAC address. So the 2nd PDU is the **ARP request** needed to resolve the IP address of the DNS server to its hardware MAC address.
- Now click the **Auto Capture / Play** button in the Event List Window to run the simulation and capture events.
- Sit tight and observe the packets flowing through the network.



Buffer Full -- Packet Tracer

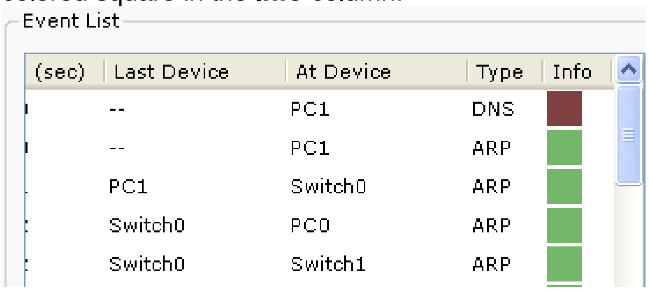
The maximum number of events has been reached. You may clear the event list and continue from where you left off or adjust the filters to view previous events.

- When the above message appears Click "View Previous Events".
- Click on PC1. The web browser will now display a web page.
- Minimize the PC1 window again.

Step 3 – Examine the following captured traffic.

	Last Device	At Device	Type
1.	PC1	Switch 0	ARP
2.	Local DNS Server	Switch 1	ARP
3.	PC1	Switch 0	DNS
4.	Local DNS Server	Switch 1	DNS
5.	--	PC1	HTTP

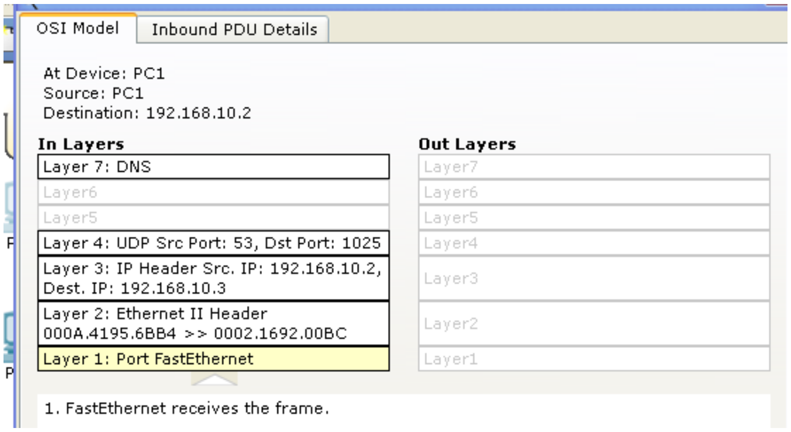
- Find the following packets given in the table above in the **Event List**, and click on the colored square in the **Info** column.



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.



At Device: PC1
Source: PC1
Destination: 192.168.10.2

In Layers	Out Layers
Layer 7: DNS	Layer7
Layer6	Layer6
Layer5	Layer5
Layer 4: UDP Src Port: 53, Dst Port: 1025	Layer4
Layer 3: IP Header Src. IP: 192.168.10.2, Dest. IP: 192.168.10.3	Layer3
Layer 2: Ethernet II Header 000A.4195.6BB4 >> 0002.1692.00BC	Layer2
Layer 1: Port FastEthernet	Layer1

1. FastEthernet receives the frame.

- This windows displays the OSI layers and the information at each layer for each device. (At Device).
- 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.

Packets 1&2 representing ARP packets:

Packet 1 represents the ARP request by PC1. Which devices' MAC addresses are included as source and destination?

SOURCE MAC :0002.1692.00BC TARGET MAC:0000.0000.0000

Why is PC1 sending an ARP packet?

For sending request to the Test Server, PC1 should know the IP and MAC address of the server and in this process DNS server is required and in order to go to DNS server, it also needs MAC address of DNS server thus it requires the ARP packet.

Why was this packet sent to all devices?

ARP broadcasts a request packet to all the hubs and asks if any of the machines are using that particular IP address. If it recognizes the IP address as its own, it sends a reply. To match the IP address of the devices with the IP address from DNS server. If any source device wants to a request to the test server, it have to go through every device until finds the targeted device with the same IP address, other devices will reject the packet.

Packet 2 represents the ARP reply by the Local DNS server. What is the difference in the devices' MAC addresses are included as source and destination?

The difference between devices is that, the source and destination of their MAC Addresses are different. Source device: Local DNS server and Destination device: PC1

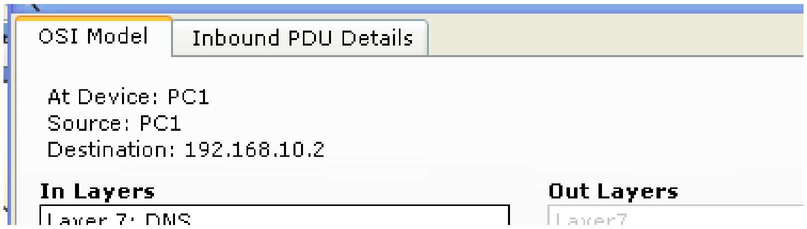
Inbound:	SOURCE MAC :0002.1692.00BC	TARGET MAC:0000.0000.0000
Outbound:	SOURCE MAC :000A.4195.6BB4	TARGET MAC:0002.1692.00BC

Packets 3&4 representing DNS packets:

Packet 3 represents the DNS request made by PC1, why? Which devices' IP addresses are included as source and destination?

Because without DNS request PC1 will not get the IP Address.
Here, Source: PC1 Destination: Local DNS Server

SRC IP:192.168.10.3 DST IP:192.168.10.2



At Device: PC1
Source: PC1
Destination: 192.168.10.2

In Layers
Layer 7: DNS

Out Layers
Layer7

Click onto “Inbound PDU details” tab. Scroll down, you should come across “DNS Query”. What is the purpose of this DNS Query?

DNS query is sent to ask for the IP address associated with a domain name server.

Packet 4 is the reply from the DNS server, what is the difference between Packet 1 and Packet 2 source and destination IP addresses?

For Packet 1, Source IP address is of PC1 and Destination IP address is of Local DNS server.
SOURCE IP :192.168.10.3 & TARGET IP:192.168.10.2
For Packet 2, Source IP address is of Local DNS server and Destination IP address is of PC1
SOURCE IP :192.168.10.2 & TARGET IP:192.168.10.3

For packet 4, click onto “Inbound PDU details” tab. Scroll down, do you see anything different after the DNS query?

From the DNS query we know about the IP address of Test Server then DNS server ask for the MAC address to establish the connection.

Packets 5 is the HTTP request for the web page made by PC1.

Details of this packet will be observed later.