CSE 421
Lab 2 :Observing DNS and ARP in Packet Tracer
ID_____19301151_____

Introduction:

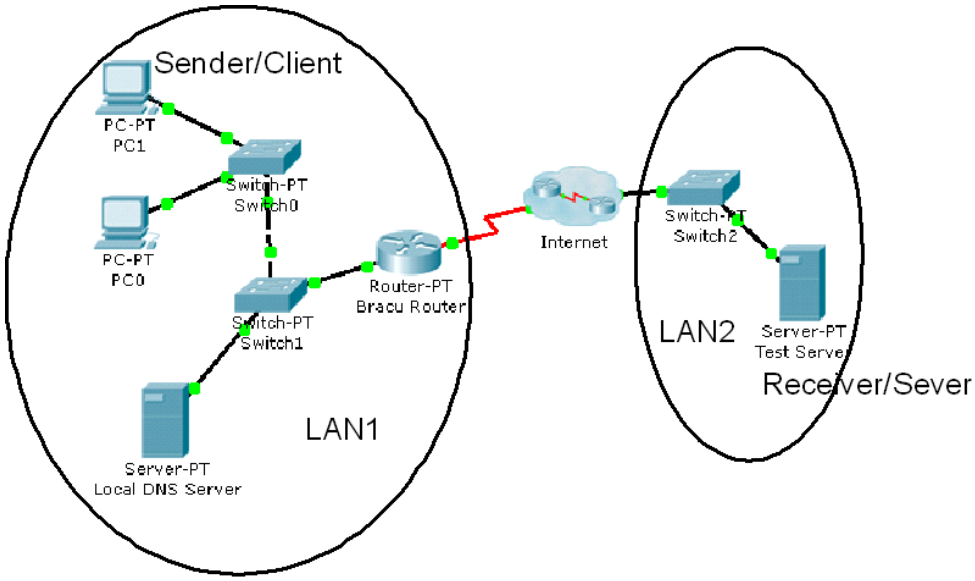
Simulation mode in Packet Tracer captures all network traffic flowing through the entire network . You will observe the packets involved in DNS and ARP process. These two protocols are the helping protocols when a web page is requested using HTTP.

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.

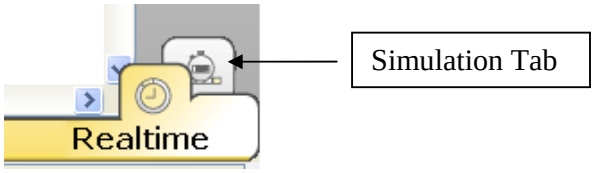


- **PC0**, **PC1** and the **Local DNS server**, **BRACU router** is part of a Local area network. BRACU router connects this LAN to the Internet through an ISP. The **Test server** shown is on another Local area network.
- You will access the web page **www.test.com** which is stored in the Test Web 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

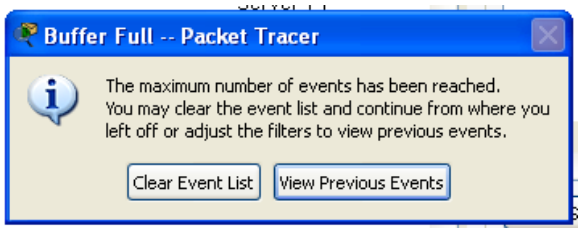
- In the far lower right of the PT interface is the toggle between Realtime and Simulation mode. PT always starts in realtime mode, in which networking protocols operate with realistic timings.



- 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.

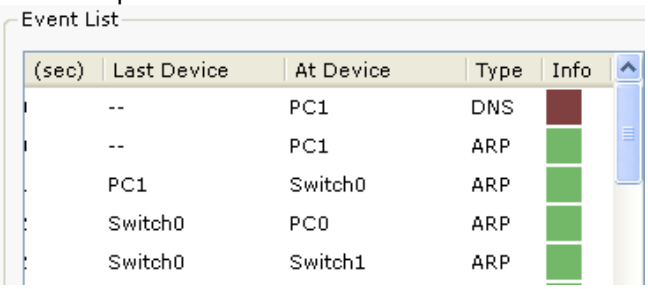


- When the above message appears Click "View Previous Events".
- Click on PC1. The web browser will now display a web page.
- Minimize the PC1 window again.

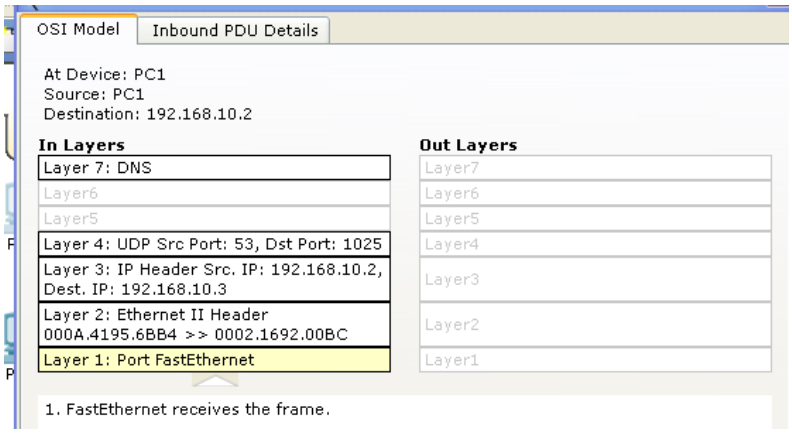
Step 3 – Examine the following captured traffic.

	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.



- When you click on the Info square for a packet in the event list the **PDU information** window opens.



- 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?

As source PC1's MAC address is included which is 0002.1692.00BC, and as destination we use Broadcast here, so we don't have any specific MAC address in this case. And when we usually dobroadcasting the target mac is set to 0000.0000.0000

Why is PC1 sending an ARP packet?

As PC1 is completely new to this network, it doesn't know what is the MAC address of it's Local DNS Server orwhat is the MAC address of it's router. So it sends an ARP packet which find out the Local DNS Server or Routervia broadcasting method which needs send an ARP packet to do so.

Why was this packet sent to all devices?

As ARP packet works in broadcasting method and the PC doesn't have the MAC address ofany specific devices yet. Simply put, our pc doesn't know anyone yet so it send packet to all available devices to figure out a specific devices it looking for. Then all the devices denied the packet of pc except the one the pc was looking for. In this way our pc the figure out it's desire device's MAC address. That's why this packet was sent to all devices.

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?

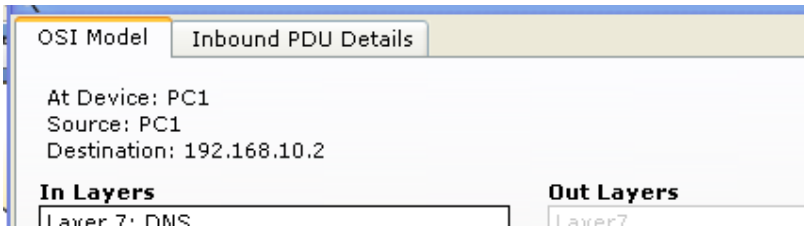
In our Packet 2 we have our source MAC as 000A.4195.6BB4 which is the MAC address of our Local DNSServer. And as destination MAC address we have 0002.1692.00BC which is our PC1. So we can say as source we have a Local DNS Server here and as destination we have a personal computer named PC1.

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?

Via ARP request our PC1 already figured out what is the MAC address of the DNS server of it's local network. And now asit knows what it's local DNS server, it sends the DNS request to figure out a domain name to its corresponding IP address.

As source IP we have 192.168.10.3 what is the IP address of PC1 and as destination we have 192.168.10.2 which is the IP address of Local DNS Server.



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

The purpose of a DNS query is to obtain the IP address associated with a given domain name. DNS queries are essential for translating human-readable domain names into machine-readable IP addresses. The primary purposes of DNS queries are usually... Resolving Domain Names, Local Network Resolution, Internet Access.

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

In packet 1 as source IP we have 192.168.10.3 which is the IP address of PC1, but as we broadcasting here we don't have any specific destination IP here. However we have a target ip though which is the IP: 192.168.10.2 address of Local DNS Server.
Whereas a packet 2 is a reply from the DNS server to the PC1. So, here as sourse we have IP address of Local DNS server which is 192.168.10.2 and as terget ip we have the IP address of PC1, which is 192.168.10.3

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

Yes, In packet 3 there is only a DNS Query present in it's Inbound PDU Details, Whereas in packet 4 we haveDNS Answer present here with resolved IP address, which will be provided to the PC1 ultimately.

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

Details of this packet will be observed later.