মেট্রোপলিটন ইউনিভার্সিটি
Metropolitan University

Department of Computer Science and Engineering

Course Code: CSE312	Credits: 1.5
Course Name: Computer Networks Lab	Faculty: FRS

Lab 02 – DNS and ARP

Introduction:

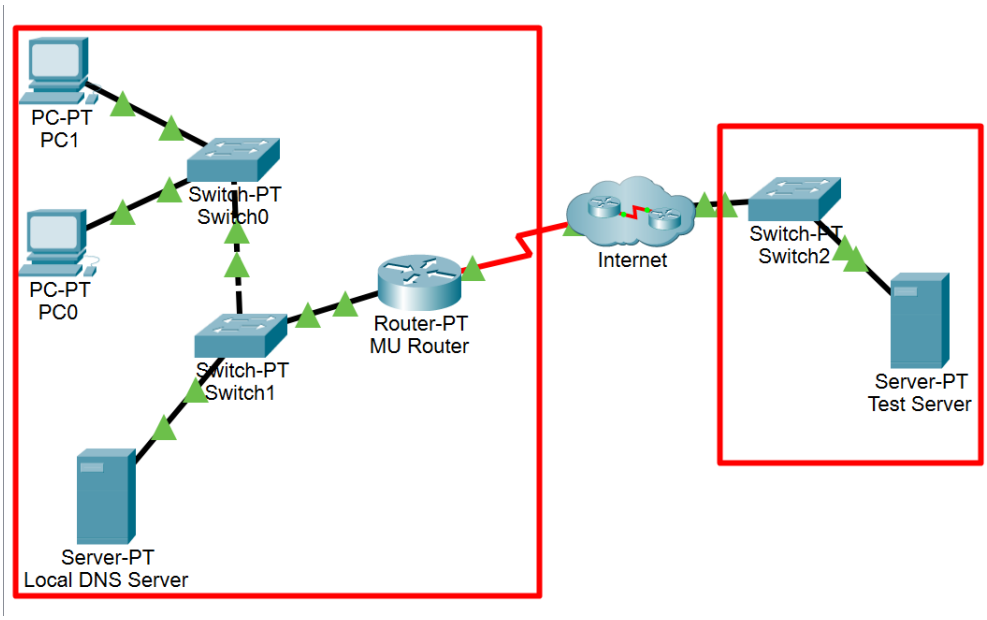
Simulation mode in Packet Tracer captures all network traffic flowing through the entire network. You will observe the packets involved in DNS and ARP process. These two protocols are the helping protocols when a web page is requested using HTTP.

Objectives:

- Explore how PT uses the OSI Model and TCP/IP Protocols.
    a. Creating a Simple PDU (test packet)
    b. Switching from Realtime to Simulation Mode
- Examine a Web Request Packet Processing and Contents
    a. Accessing the PDU Information Window, OSI Model View
    b. Investigating the layers and addresses in the OSI Model View
    c. Animations of packet Flow

Observe the network topology shown

- PC0, PC1 and the Local DNS server, MU router is part of a Local area network. MU 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 through PC1's web browser, which is stored in the Test Web Server.



- 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

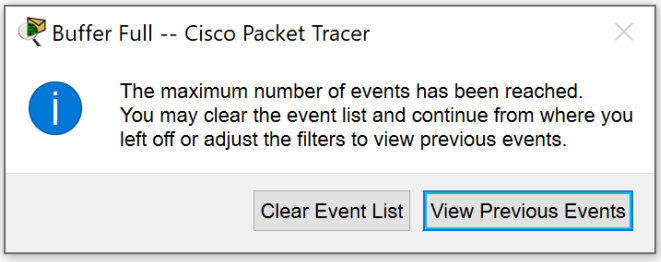
Step 1 – Switching from Realtime to Simulation Mode

- 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.



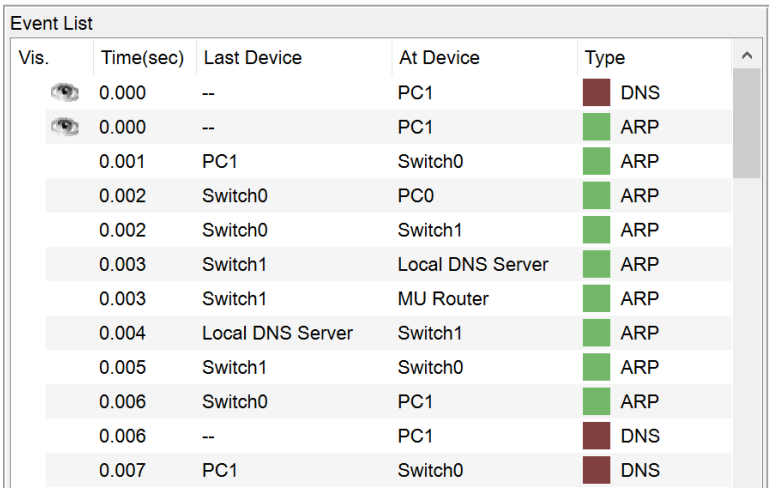
- When the above message appears Click “View Previous Events".
- Click on PC1. The web browser will now display a web page.

- Minimize the PC1 window again.

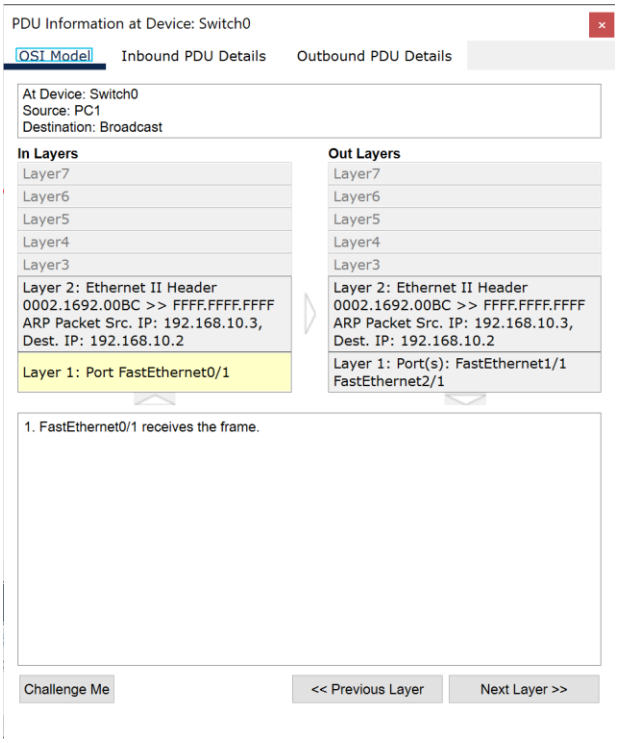
Step 3 – Examine the following captured traffic

Packet	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 window displays the OSI layers and the information at each layer for each 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.



Question & Answer

Packets 1 & 2 representing ARP packets:

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

The source MAC address is 0002.1692.00BC (PC1) and the destination MAC address is FFFF.FFFF.FFFF (broadcast).

Why is PC1 sending an ARP packet?

PC1 sends the ARP packet to find the MAC address of the Local DNS Server (IP: 192.168.10.2) so that it can communicate directly within the local network.

Why was this packet sent to all devices?

The ARP request uses the broadcast address (FFFF.FFFF.FFFF) so that all devices receive it.

Only the device with the matching IP address (the DNS server) replies.

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 the request, the destination MAC is broadcast because PC1 doesn't know the DNS server's MAC yet.

In the reply, the source MAC is 000A.4195.6B84 (DNS server) and the destination MAC is 0002.1692.00BC (PC1).

The main difference is that the request is broadcast and the reply is unicast (sent directly to PC1).

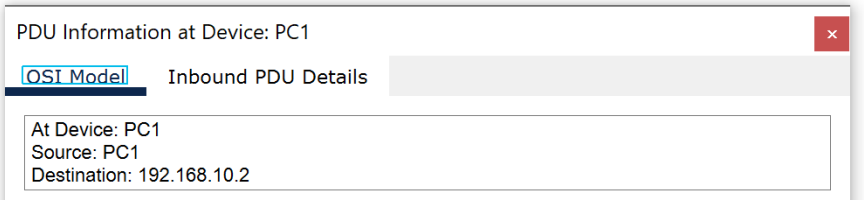
Packets 3 & 4 representing DNS packets:

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

PC1 sends a DNS request to convert the domain name www.test.com into an IP address before accessing the web page for making web communication.

The source IP is 192.168.10.3 (PC1) and

the destination IP is 192.168.10.2 (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 is to ask the DNS server for the IP address of www.test.com

because PC1 only knows the domain name and needs the IP to open the website.

Packet 4 is the reply from the DNS server, what is the difference between Packet 3 and Packet 4 source and destination IP addresses?

In Packet 3, the source is PC1 and the destination is DNS server(request). In Packet 4, the source is DNS server and the destination is PC1(reply).The addresses are simply reversed in the reply.

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

Packet 4 contains the DNS response, which includes the resolved IP address of the Test Web Server. This allows PC1 to send the next HTTP request to load the web page.

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

*Details of this packet will be observed later.