

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:

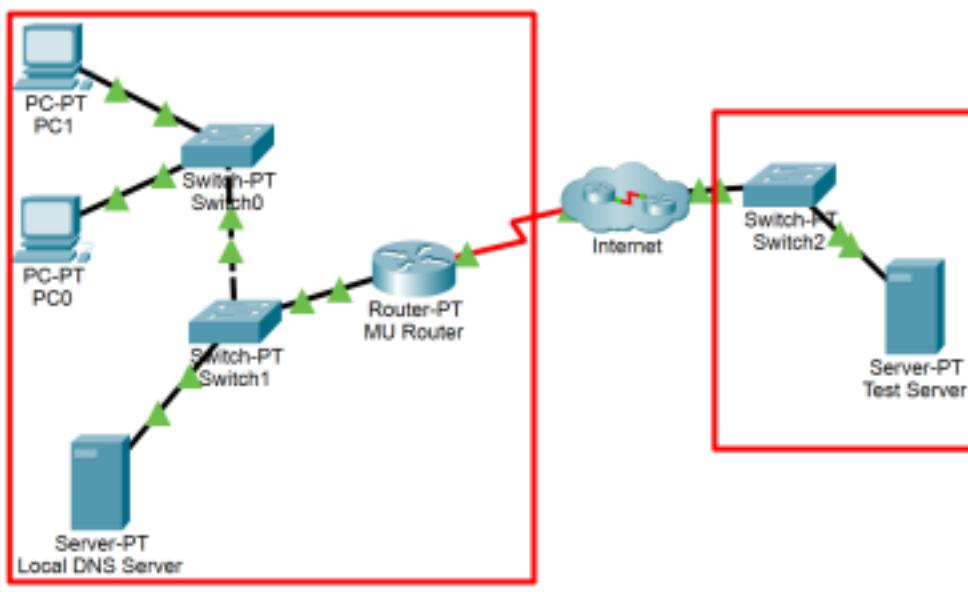
Simulation mode in Packet Tracer captures all network traffic flowing through the entire network. You will observe the packets involved in DNS and ARP process. These two protocols are the helping protocols when a web page is requested using HTTP.

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

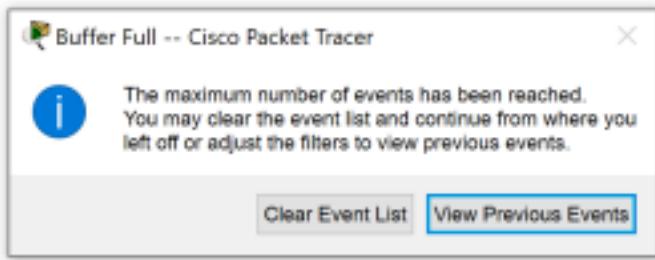
- In the far lower right of the PT interface is the toggle between Realtime and Simulation mode. PT always starts in realtime mode, in which networking protocols operate with realistic timings.
- In simulation mode, you can visually see the flow of packets when you send data from an application. A new 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.

Event List				
Vis.	Time(sec)	Last Device	At Device	Type
0.000	--	PC1		DNS
0.000	--	PC1		ARP
0.001	PC1	Switch0		ARP
0.002	Switch0	PC0		ARP
0.002	Switch0	Switch1		ARP
0.003	Switch1	Local DNS Server		ARP
0.003	Switch1	MU Router		ARP
0.004	Local DNS Server	Switch1		ARP
0.005	Switch1	Switch0		ARP
0.006	Switch0	PC1		ARP
0.006	--	PC1		DNS
0.007	PC1	Switch0		DNS

- 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.

PDU Information at Device: Switch0

OSI Model Inbound PDU Details Outbound PDU Details

All Device: Switch0
Source: PC1
Destination: Broadcast

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3
Layer 2: Ethernet II Header 0002.1692.00BC >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.10.3, Dest. IP: 192.168.10.2	Layer 2: Ethernet II Header 0002.1692.00BC >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.10.3, Dest. IP: 192.168.10.2
Layer 1: Port FastEthernet0/1	Layer 1: Port(s): FastEthernet1/1 FastEthernet2/1

1. FastEthernet0/1 receives the frame.

Challenge Me << Previous Layer Next Layer >>

Question & Answer

1. 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: PC1's MAC address.

Destination MAC: Broadcast (FF:FF:FF:FF:FF:FF).

2. Why is PC1 sending an ARP packet?

To discover the MAC (hardware) address that corresponds to the DNS server's IP address so PC1 can send Ethernet frames to the DNS server on the local LAN.

3. Why was this packet sent to all devices?

Because ARP requests are broadcast on the LAN when the sender lacks the target's MAC. Broadcasting ensures the device that owns the requested IP receives the query and can reply.

4. 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?

Source MAC: Local DNS server's MAC.

Destination MAC: PC1's MAC.

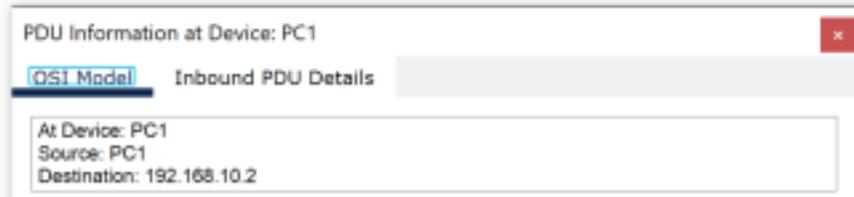
Difference: the reply is unicast (server → PC1) and uses the server's MAC as source rather than a broadcast.

5. 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?

- Why: PC1 needs to resolve www.test.com to an IP address, so it sends a DNS query.
- Source IP: PC1's IP address.
- Destination IP: Local DNS server's IP address (the resolver).

- Additional detail: the DNS query is typically sent over UDP (source ephemeral port >1023 → dest port 53).



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

The DNS Query requests a specific DNS resource record (usually an A record for IPv4) for www.test.com. In short: “What is the IP address of www.test.com?” The DNS Query contains the queried name and query type.

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

They are swapped: Packet 3 had source = PC1 IP, dest = DNS server IP. Packet 4 has source = DNS server IP, dest = PC1 IP.

The reply comes from the DNS server back to PC1

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

Yes. The DNS response contains an Answer section with the resolved IP address(es) for www.test.com (e.g., an A record), plus TTL and record type. Also the response will carry the same DNS transaction ID as the query so the client can match response→query. (You may also see flags showing it's a response and whether it's authoritative.)

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

*Details of this packet will be observed later.