

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

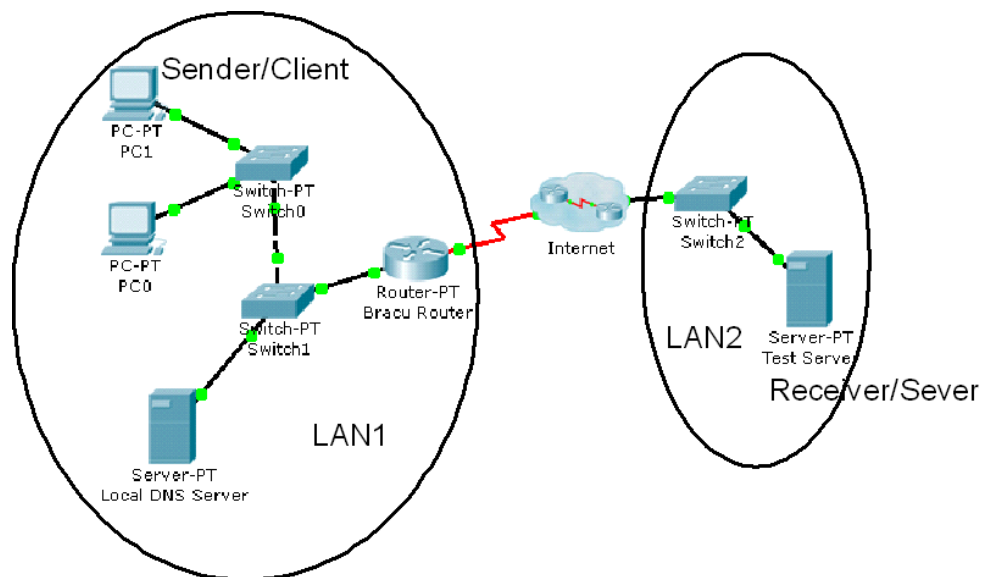
Introduction:

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.

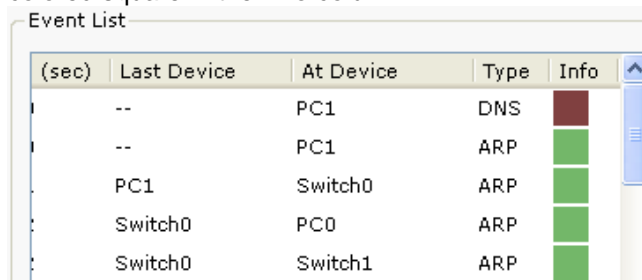


- When the above message appears Click “View Previous Events”.
- Click on PC1. The web browser will now display a web page.
- Minimize the PC1 window again.

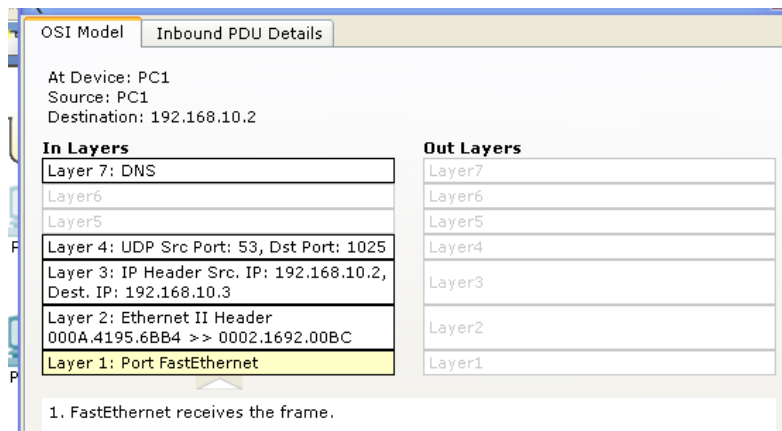
Step 3 – Examine the following captured traffic.

| | 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 window 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?

PC1's MAC address is the source MAC address since it has requested. As it is a broadcasting request for local DNS server's MAC address, the destination MAC address is not defined.

Why is PC1 sending an ARP packet?

To know the IP address of the website, PC1 needs to send request to local DNS server.

Now, PC1 doesn't know the MAC address of DNS server and so it can't request to DNS server.

So, it sends an ARP request to know the MAC address of DNS server.

Why was this packet sent to all devices?

This packet was sent to all devices since it is a broadcasting request. PC1 needs to know the MAC address of the local DNS server, so it sends this to all devices if anyone's IP address matches with the IP address given in the request that device will send its MAC address.

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?

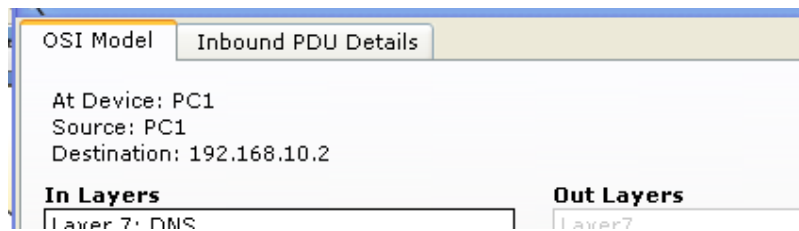
In the ARP reply, source MAC address is local DNS servers' MAC address and the destination MAC address is PC1's MAC address. PC1 didn't know DNS servers' MAC address and so it didn't include the destination MAC but while replying to PC1, DNS server knows the destination host PC1's MAC address.

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?

Packet 3 represents the DNS request made by PC1 because source IP address is PC1's IP address.

Also, PC1 needs to know the IP address of the website. So, it is sending a DNS request to local DNS server. Since it is requesting DNS server, DNS servers IP address is included as destination IP address.



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

The type and class of this DNS query is 1. So, the purpose of this DNS query is to know the IP address of website www.test.com

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

Packet 1's source IP address is PC1's IP address and the destination IP address is DNS servers' IP address but in Packet 2, PC1 becomes the destination and DNS server becomes the source.

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

Yes, DNS answer has been added at the end. DNS server has responded to the DNS query with the IP address of the website in DNS answer.

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

Details of this packet will be observed later.