CSE 421

Lab 2 :Observing DNS and ARP in Packet Tracer

ID: 17301121

**Introduction:**

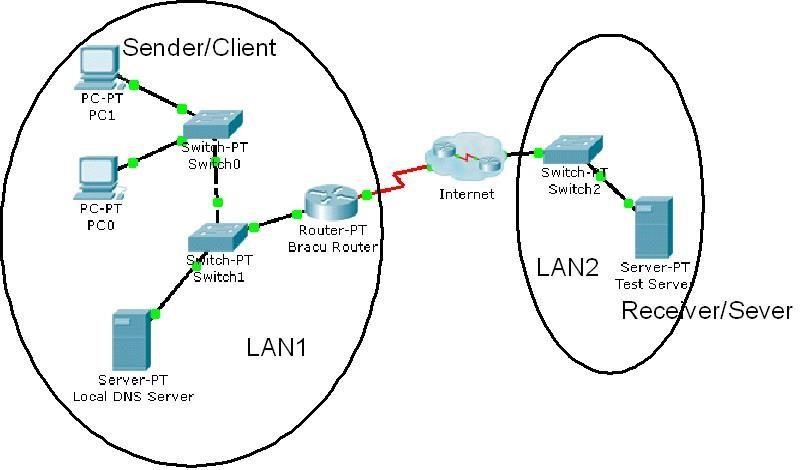
Simulation mode in Packet Tracer captures all network traffic flowing through the entire network . You will observe the packets involved in DNS and ARP process. These two protocols are the helping protocols when a web page is requested using HTTP.

**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

1. 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.

|  |
| --- |
| Simulation Tab |



* + 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.

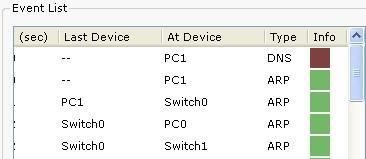


* + When the above message appears Click “View Previous Events".
  + Click on PC1. The web browser will now display a web page.
  + Minimize the PC1 window again.

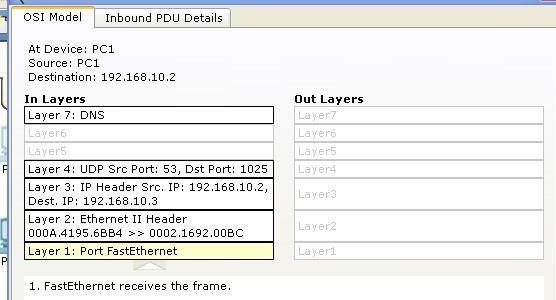
**Step 3 – Examine the following captured traffic.**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **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?

* + Source & destination for packet 1 is included in PC1’s MAC address.

Why is PC1 sending an ARP packet?

* + PC1 is sending an ARP packet because to get the mac address.

Why was this packet sent to all devices?

* + This packet is sent to all devices because it needs to verify IP addresses of all possible devices and it also needs to locate the right device.

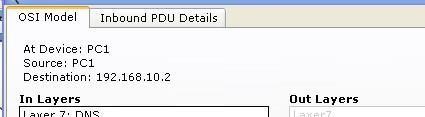
Packet 2 represents the ARP reply by the Local DNS server. What is the difference in the devices’ MAC addresses are included as source and destination?

* + The difference is, PC 1 is the destination & Local DNS server is the source.

***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 it is required to get the IP address of the Test server. Moreover, PC 1’s IP address is the source & Local DNS server’s IP address is the destination.



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

* + They maintain a directory of domain names and translate them to IP address. DNS are basically the Internet’s equivalent to a phone book.

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: the source IP address is PC1 & destination IP address is server.
  + Packet 2: the source IP address is server IP and destination IP is PC1, after getting DNS server’s mac address.

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

* + Yes, I do see changes in the DNS message and the change is occurred in account from 0 to 1**.**

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

Details of this packet will be observed later.