Activity 2

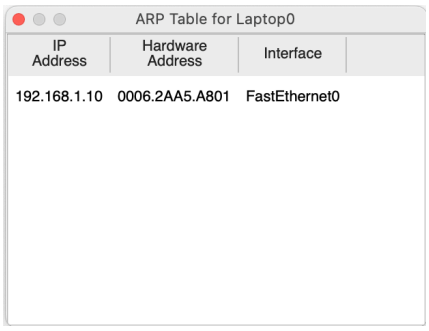
1. As a group, discuss what information Laptop1 in LAN1 requires to connect to PC2 In LAN1.
2. What protocol we can use to get the required information? Discuss the steps involved in getting the required information.
3. Use the simulation mode to check ARP in action by pinging PC2 from Laptop1.
a. What are the types of messages that PC2 generated?
b. Discover the message sequence of ARP and the message content (paying attention to the source IP, destination IP, source MAC address, and destination MAC address).

4. Each device maintains an ARP table. You can check the ARP table of devices using the command prompt and typing "arp -a". Check and compare the arp tables in Laptop 1 and PC2.
5. Check the arp tables of router 1, router 2, PC0, PC1, and Laptop0. Keep notes of the content of each arp table. To show the arp table of a router, "show arp" command can be used in the router's CLI.

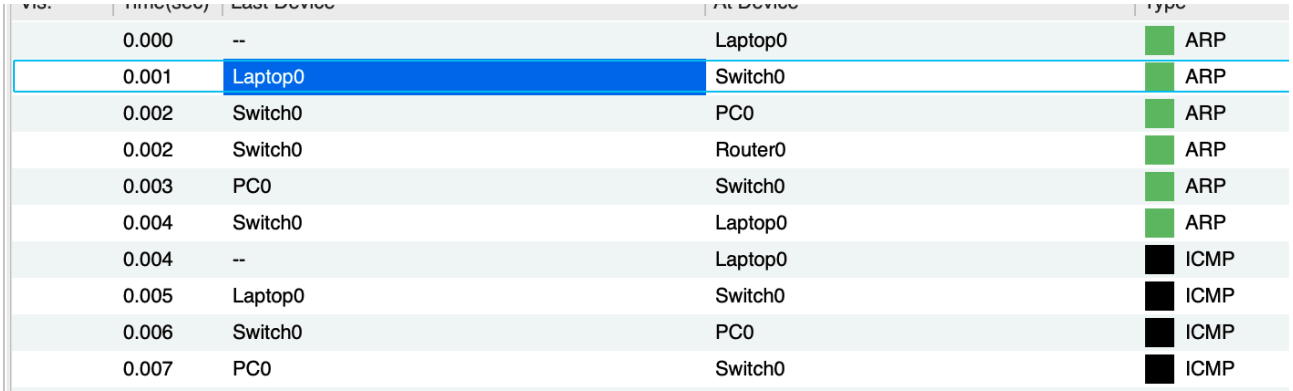
6. Use the simulation mode again. Now, ping PC0 from Laptop1. Discover the arp message sequence and the message content in each link. Once the above steps are completed, ping PC1 from laptop0.
7. Check the arp tables of router 1, router 2, PC0, PC1, and Laptop0.
8. Compare your observations with the observations you recorded in step 5. Discuss your finding with your group members.

1) Laptop1 in LAN1 requires IP addresses, subnet mask, default gateway, DNS server address, and network sharing settings to connect to PC2 in LAN1 on the same network.

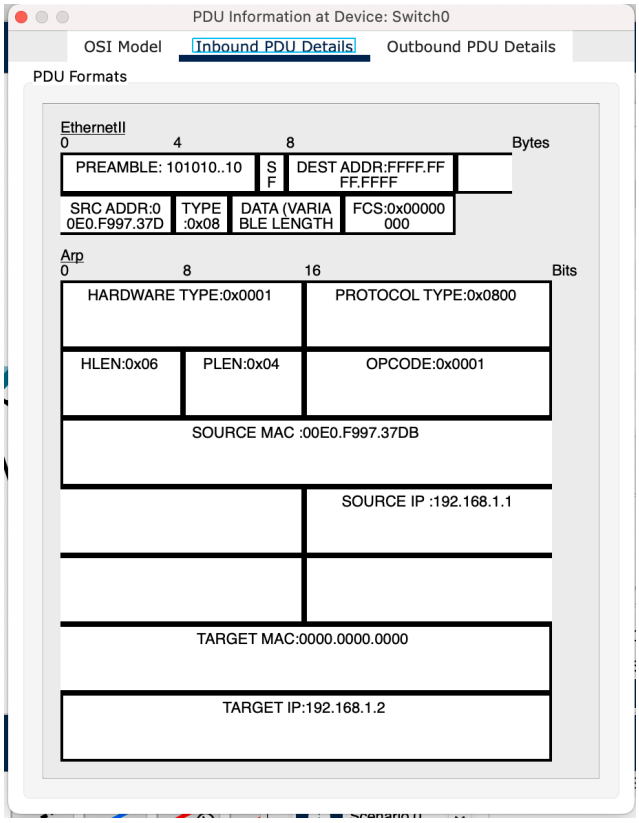
2) To obtain the required information, ARP protocol can be used in the network. After configuring each device, switch, and router, the Ping command is used to check if Laptop1 can communicate with PC2. The ARP command is then used to verify that Laptop1 and PC2 have the correct MAC addresses. The nslookup command is used to ensure that the DNS server address is correctly configured. Here os the screenshot of the ARP table.



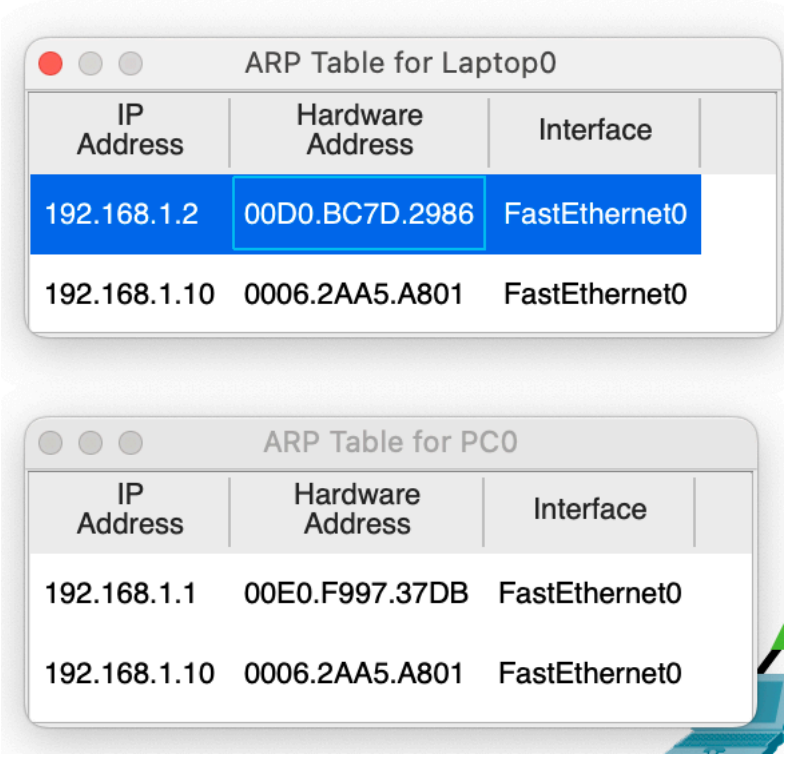
3)
a) There are two type of message being sent, one is ARP and another one is ICMP. As you can see in the figure below first the ARP protocol is transferred then the ICMP protocol is transferred.



b) Here is the information available about the ARP protocol, that includes the information like source MAC address, Source IP, Target IP. As you can see Target MAC is not defined because it is unknown by the sender. First the sender send data to switch, it will transfer the data to the Router which then sends the data back to switch and finally to the PC. After all these the ARP table is updated with the MAC address of each other devices.



4) As you can see in the screenshot, IP address & Mac address of each other devices are stored along with the information about the router.



5) Every device ARP table is empty as we they haven't communicated with any of the other device. Here is the screenshot of one of the device.

```
C:\>arp -a
No ARP Entries Found
C:\>
```

6) After pinging from one device to another, ARP table has been updated with the IP address of the other network gateway.

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=11ms TTL=126
Reply from 192.168.1.1: bytes=32 time=12ms TTL=126
Reply from 192.168.1.1: bytes=32 time=1ms TTL=126
Reply from 192.168.1.1: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 12ms, Average = 6ms

C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.2.10          0004.9a7a.8101        dynamic

C:\>
```

7) The ARP table of other devices has not been updated because they haven't communicated with other devices.

8) Here are the ARP table of every device in the network. We are able to see that the devices which have communicated with the other devices has IP address & Mac address of other devices in the ARP table.