

Evidence of Learning

Activity-1

Que 1. Let's do a small role play to understand the MAC protocol. Assume that your group forms a Wireless LAN (WLAN) that uses Wi-Fi technology (has a wireless access point (AP) and three wireless devices that connect to Wi-Fi AP). One member can be the Wi-Fi AP and other members are the hosts (could be laptops, smart watches, smart phones, etc.). Assume all the devices in the network would like to send packets to Internet simultaneously. For example, when you need to send a packet, you can say "I'm sending a packet". If another group member said the same thing at the same time, then a collision occurred, and both need to retransmit packets.

Your group needs to act as a Wireless LAN and provides a mechanism to enable successful packet transmission. You can illustrate the protocol that you have designed in a timing diagram (Shows in Figure 1). You are not required to replicate the exact protocol used in WiFi. You can design your own protocol based on random access that allows hosts to communicate with WiFi AP with minimal collisions and act fast in case of a packet collision.

Ans. The protocol described is a simple random access protocol that can be used in a wireless LAN with a WiFi AP and multiple hosts. Here is how the protocol would work:

1. Each host chooses a random time slot to transmit a packet to the WiFi AP.
2. If two or more hosts choose the same time slot, a collision occurs and all hosts involved in the collision wait for a random amount of time before attempting to transmit again. This backoff time is selected randomly to avoid multiple hosts selecting the same time slot again.
3. Once a host successfully delivers a packet to the WiFi AP, it waits for an acknowledgement (ACK) from the AP to confirm that the packet has been received. If the ACK is not received within a certain timeout period, the host assumes that the packet was not successfully delivered and retransmits the packet.
4. Upon receiving a packet from a host, the WiFi AP sends an ACK back to the host to confirm that the packet has been successfully received. If the AP does not receive the packet or detects an error in the packet, it does not send an ACK, and the host retransmits the packet.

Using this protocol, multiple hosts can transmit packets to the WiFi AP with minimal collisions and reliable packet delivery.

Que 2. Once you have completed the above activity, discuss the following question with your group members.

- What is the medium access control (MAC) protocol that can be used in WiFi?

Ans. The medium access control (MAC) protocol used in WiFi is called the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol. It is a protocol that helps to avoid collisions between devices that want to transmit data over the same wireless channel.

In the CSMA/CA protocol, devices wait for a clear channel before transmitting their data. They first listen for a period of time to make sure that no other device is transmitting. If the channel is clear, the device can start transmitting its data. If the channel is busy, the device will wait for a random amount of time before listening again.

In addition to avoiding collisions, the CSMA/CA protocol also uses an acknowledgement mechanism to ensure that data packets are received correctly. When a device receives a data packet, it sends an acknowledgement packet back to the sender to confirm that the data was received. The CSMA/CA protocol helps to ensure that data is transmitted reliably and efficiently in WiFi networks.

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 is the screenshot of the ARP table.

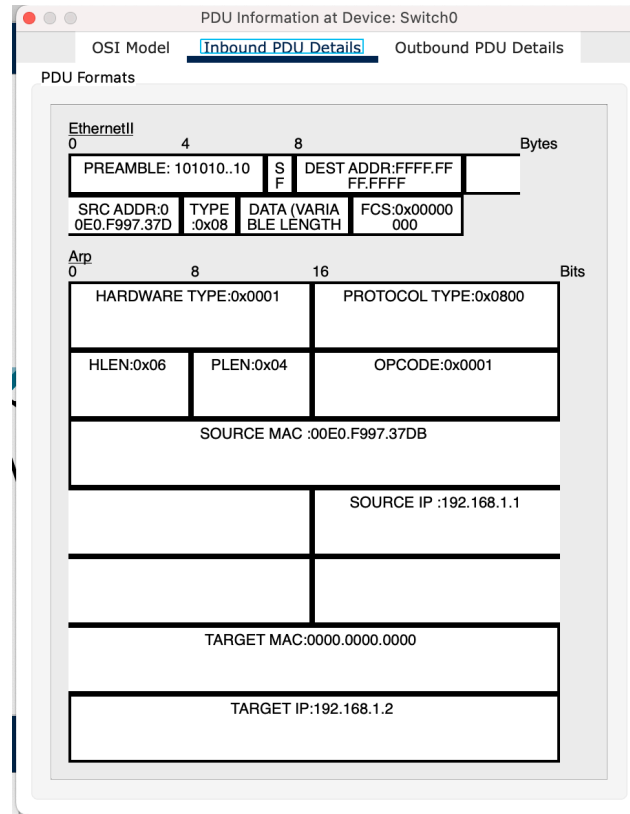
IP Address	Hardware Address	Interface
192.168.1.10	0006.2AA5.A801	FastEthernet0

3)

No.	Time(sec)	Host Device	At Device	Type
0.000	--		Laptop0	ARP
0.001	Laptop0	Switch0		ARP
0.002	Switch0	PC0		ARP
0.002	Switch0	Router0		ARP
0.003	PC0	Switch0		ARP
0.004	Switch0	Laptop0		ARP
0.004	--	Laptop0		ICMP
0.005	Laptop0	Switch0		ICMP
0.006	Switch0	PC0		ICMP
0.007	PC0	Switch0		ICMP

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.

IP Address	Hardware Address	Interface
192.168.1.2	00D0.BC7D.2986	FastEthernet0
192.168.1.10	0006.2AA5.A801	FastEthernet0

IP Address	Hardware Address	Interface
192.168.1.1	00E0.F997.37DB	FastEthernet0
192.168.1.10	0006.2AA5.A801	FastEthernet0

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

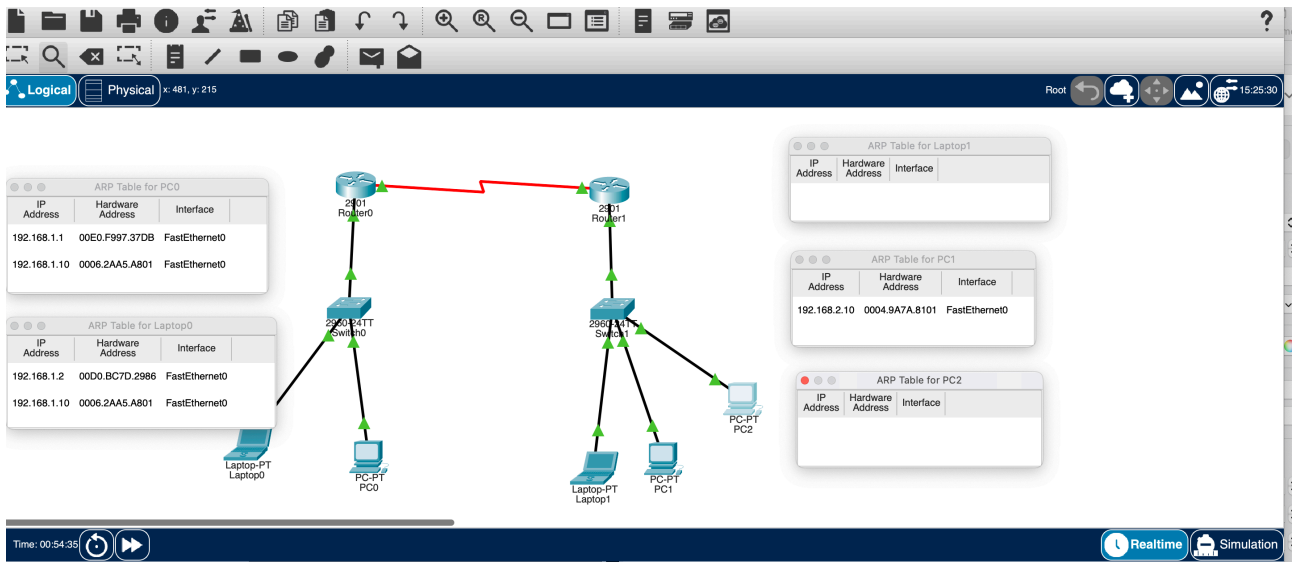
C:\>arp -a

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.

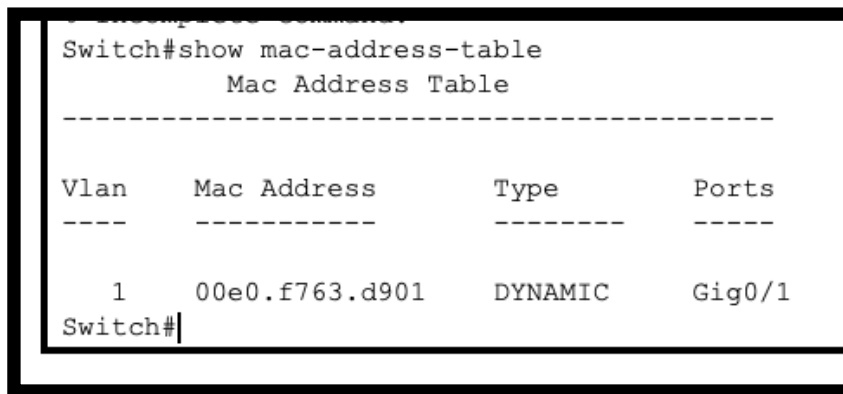
8) Here are the ARP table of every device in the network. We are able to see that the devices which have communicated with the other devices has IP address & Mac address of other devices in the ARP table.



Activity - 3

1. After you configured the devices using static IP configuration,
 - a) Record the MAC addresses of PCs/laptops/servers and Ethernet Ports of Switches.
 - b) Record the arp table in PCs and laptops.
 - c) Check the MAC address table of the switch. In switch's CLI, you can type the following command to show the MAC address table.
 - d) Record your observations. If there are any records in the MAC table, explain your observation.
 - e) Now, ping from PC1 and PC2 to Laptop0 and Laptop 1, respectively.
 - f) Check the MAC address table of the switch. Explain your observations.
 - g) Click on the "magnifying glass" icon and bring that on top of the switch. Click on the switch and select "MAC table". Resize the MAC address table and keep the table visible.
 - h) Ping laptop2 from PC0 and check the changes in the MAC table. Explain your observation.
 - i) Check the arp tables in all the PCs and laptops.

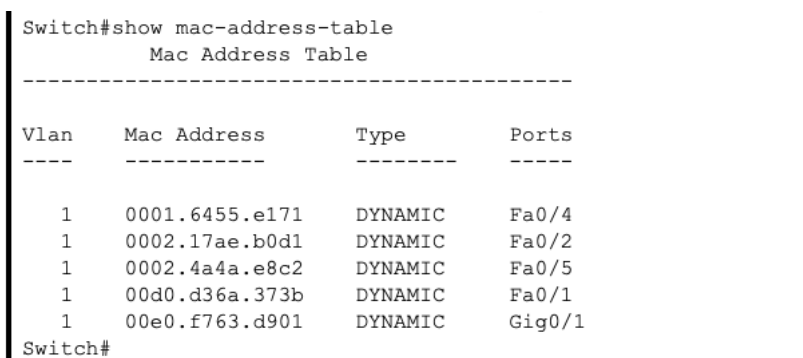
Ans. c) Here is the screenshot of MAC-address-table



```
Switch#show mac-address-table
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
1       00e0.f763.d901   DYNAMIC   Gig0/1
Switch#
```

d) It displays the Mac Address of a device that is connected to the Router on Gig0/1 port. This displays that the Router learns on its own about the Mac address of the devices that are connected to it.

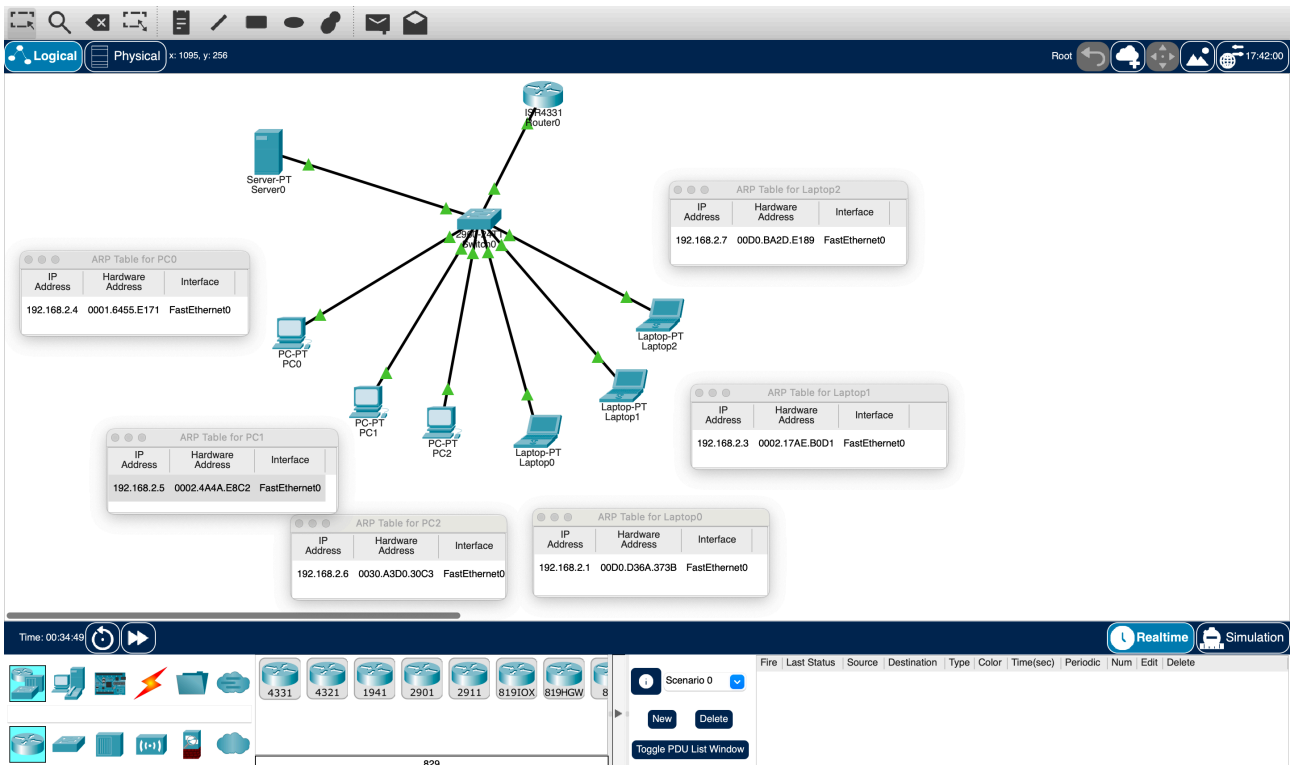
E, f) Here is the screenshot of MAC-address-table



```
Switch#show mac-address-table
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
1       0001.6455.e171   DYNAMIC   Fa0/4
1       0002.17ae.b0d1   DYNAMIC   Fa0/2
1       0002.4a4a.e8c2   DYNAMIC   Fa0/5
1       00d0.d36a.373b   DYNAMIC   Fa0/1
1       00e0.f763.d901   DYNAMIC   Gig0/1
Switch#
```

After pinging from one device to another each Mac addresses are stored in the MAC-address-table along with their Type and Ports.

G)



In each device ARP table, IP addresses and Mac address are stored to maps MAC addresses to IP addresses for efficient communication in a network, improving data transmission speeds.

h) The ARP table will change when we ping from one device to another, the Mac address of that device which we are communicating with will be stored in the ARP table for efficient communication in the future.

2. Clear the mac address table from the switch. You can do this by using “clear mac-address-table” command in CLI of the switch.

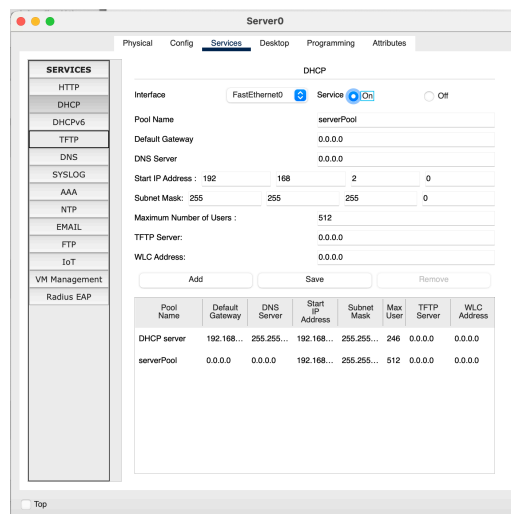
a. Configure server as a DHCP server and use DHCP to obtain IP address for all PCs and laptops.

b. Check the arp table of PCs and laptops. Compare you observation with what you have recorded in 1.b).

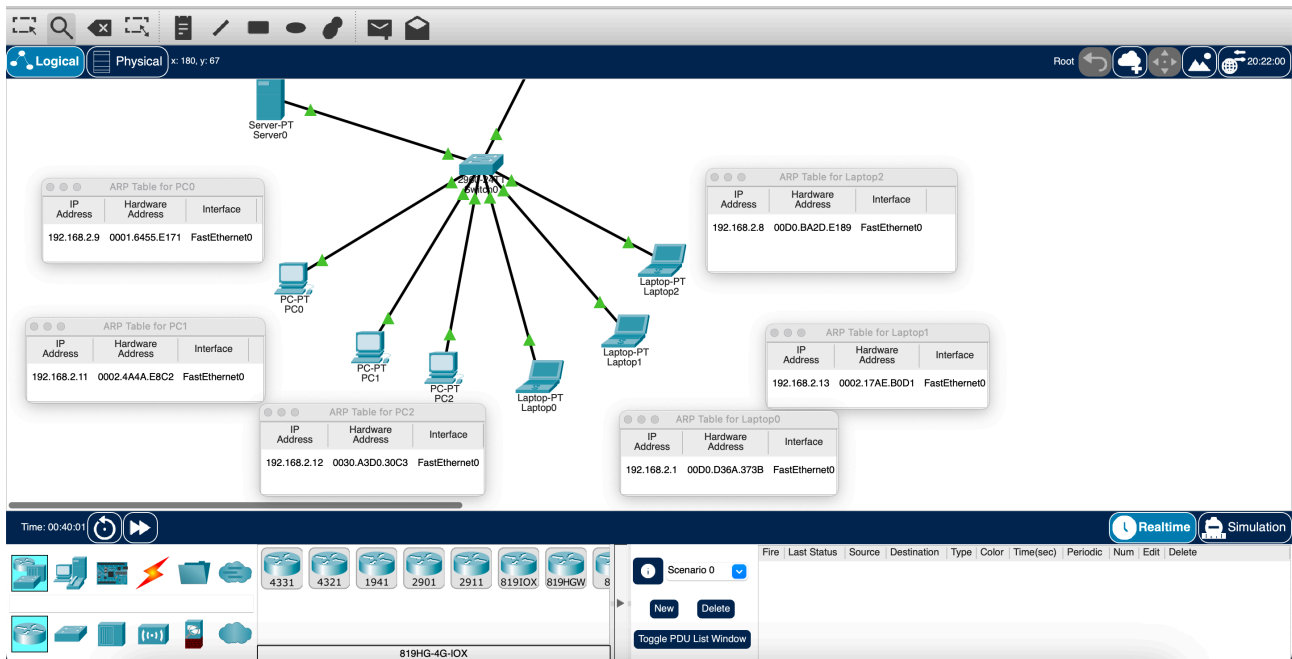
c. Check the Mac table of the switch. Compare and explain you observation with what you have recorded in 1.c)

Ans.

a) Here are the configuration for the DHCP server



B, c) We have set up the DHCP configuration for each device and checked the ARP table of each device after pinging. Here are the ARP table of each device after the pinging from one device to another.



The IP addresses are different after setting up the DHCP server. Here are the Mac address of each device on switch after the DHCP server.

```
Switch>enable
Switch#show mac-address-table
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
1       0001.6455.e171    DYNAMIC Fa0/4
1       0002.17ae.b0d1    DYNAMIC Fa0/2
1       0002.4a4a.e8c2    DYNAMIC Fa0/5
1       0030.a3d0.30c3    DYNAMIC Fa0/6
1       00d0.ba2d.e189    DYNAMIC Fa0/3
1       00d0.d36a.373b    DYNAMIC Fa0/1
1       00e0.f763.d901    DYNAMIC Gig0/1
Switch#
```