SIT202: Computer Networks and Communication
Leaning Evidence for Active Class Task 9

Name: Kenisha Corera
Student ID: C23020001

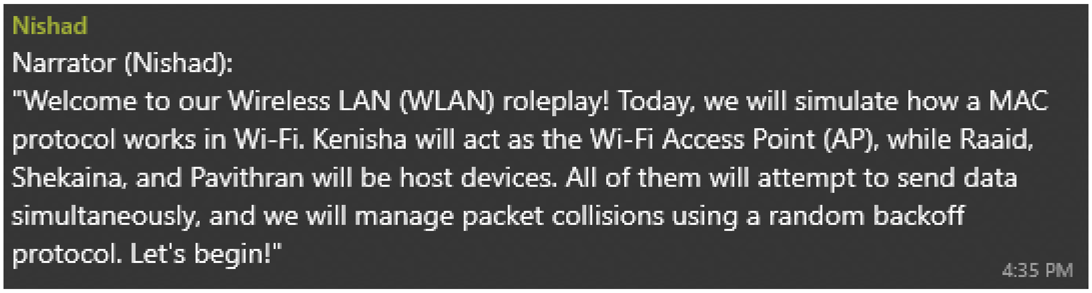
Members in this group activity task:

Nishad – C23110001
Kenisha – C23020001
Shekaina – C23110002
Raaid – C23020004
Pavithran – C22060015

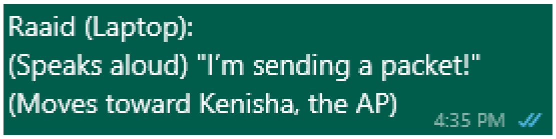
Activity 1

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.

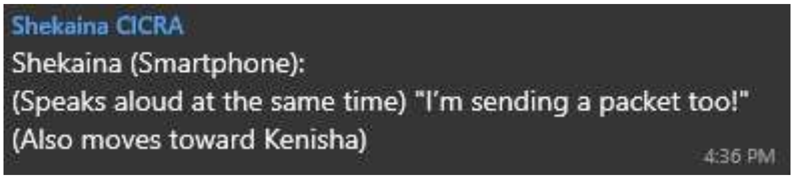
   Your group needs to act as a Wireless LAN and provides a mechanism to enable successful packet transmission. You can illustrate the protocol that you have designed in a timing diagram (Shows in Figure 1). You are not required to replicate the exact protocol used in Wi-Fi. You can design your own protocol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



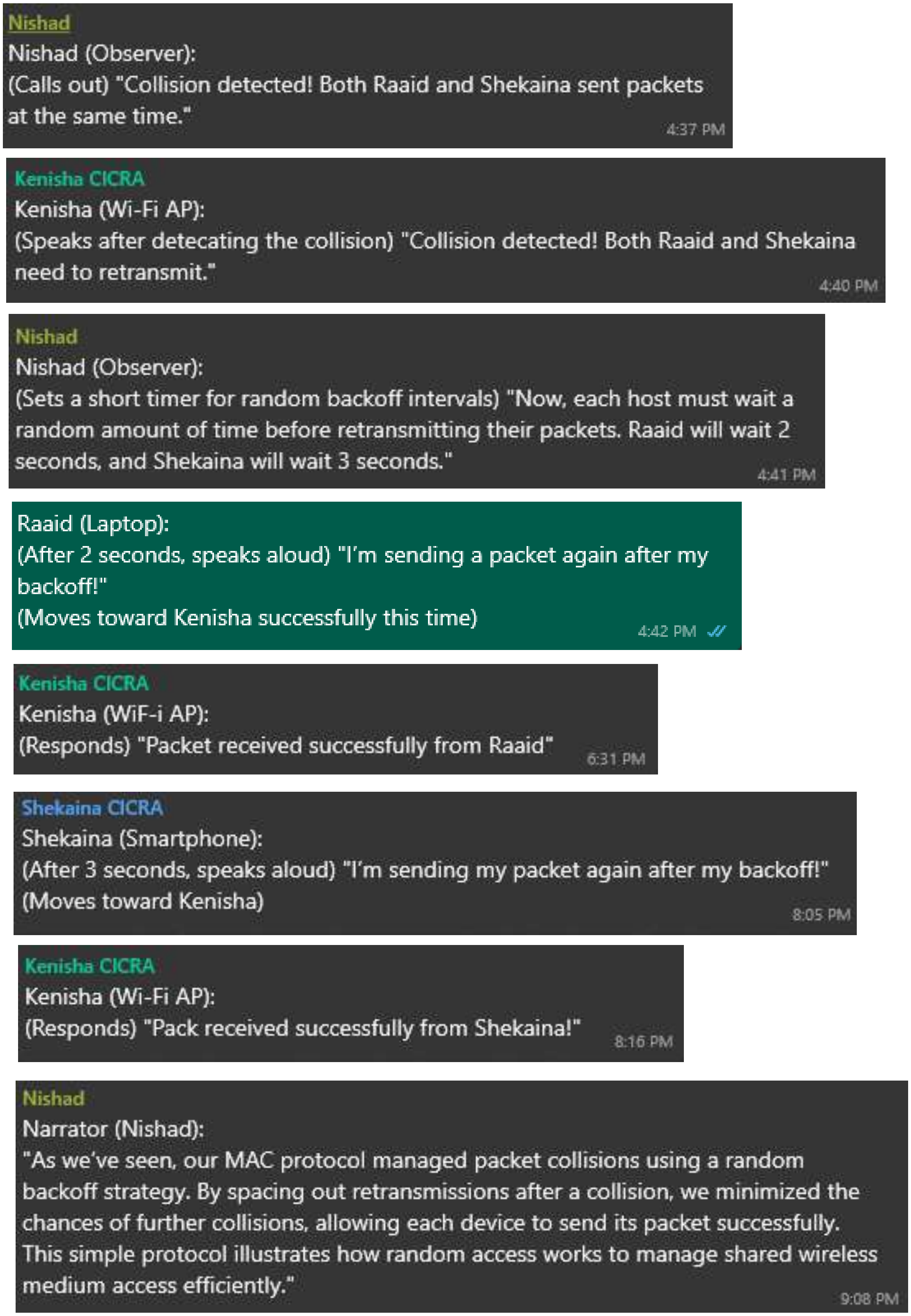
Nishad
Narrator (Nishad):
"Welcome to our Wireless LAN (WLAN) roleplay! Today, we will simulate how a MAC protocol works in Wi-Fi. Kenisha will act as the Wi-Fi Access Point (AP), while Raaid, Shekaina, and Pavithran will be host devices. All of them will attempt to send data simultaneously, and we will manage packet collisions using a random backoff protocol. Let's begin!"
4:35 PM



Raaid (Laptop):
(Speaks aloud) "I’m sending a packet!"
(Moves toward Kenisha, the AP)
4:35 PM



Shekaina CICRA
Shekaina (Smartphone):
(Speaks aloud at the same time) "I’m sending a packet too!"
(Also moves toward Kenisha)
4:36 PM



Nishad
Nishad (Observer):
(Calls out) "Collision detected! Both Raaid and Shekaina sent packets at the same time."
4:37 PM

Kenisha CICRA
Kenisha (Wi-Fi AP):
(Speaks after detecating the collision) "Collision detected! Both Raaid and Shekaina need to retransmit."
4:40 PM

Nishad
Nishad (Observer):
(Sets a short timer for random backoff intervals) "Now, each host must wait a random amount of time before retransmitting their packets. Raaid will wait 2 seconds, and Shekaina will wait 3 seconds."
4:41 PM

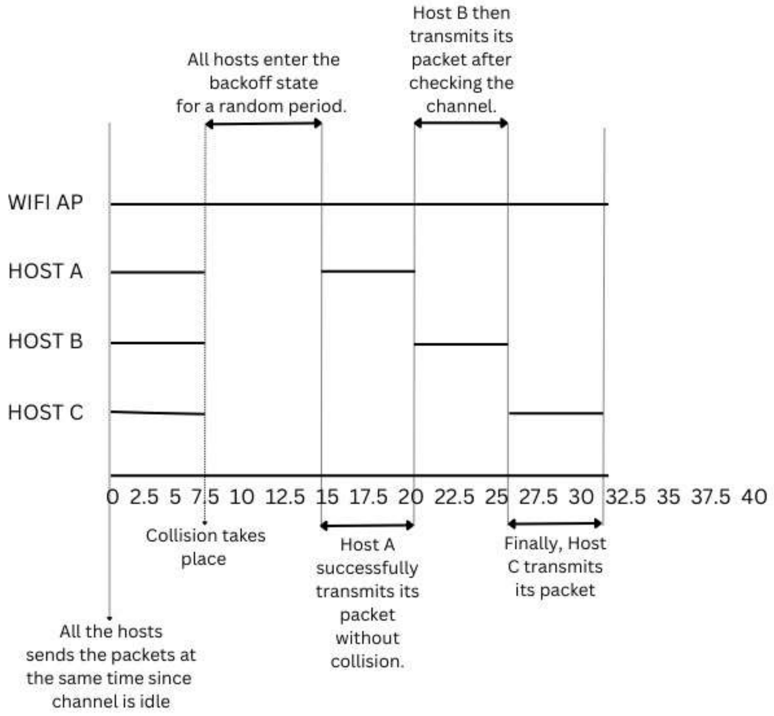
Raaid (Laptop):
(After 2 seconds, speaks aloud) "I'm sending a packet again after my backoff!"
(Moves toward Kenisha successfully this time)
4:42 PM ✓✓

Kenisha CICRA
Kenisha (WiF-i AP):
(Responds) "Packet received successfully from Raaid"
6:31 PM

Shekaina CICRA
Shekaina (Smartphone):
(After 3 seconds, speaks aloud) "I'm sending my packet again after my backoff!"
(Moves toward Kenisha)
8:05 PM

Kenisha CICRA
Kenisha (Wi-Fi AP):
(Responds) "Pack received successfully from Shekaina!"
8:16 PM

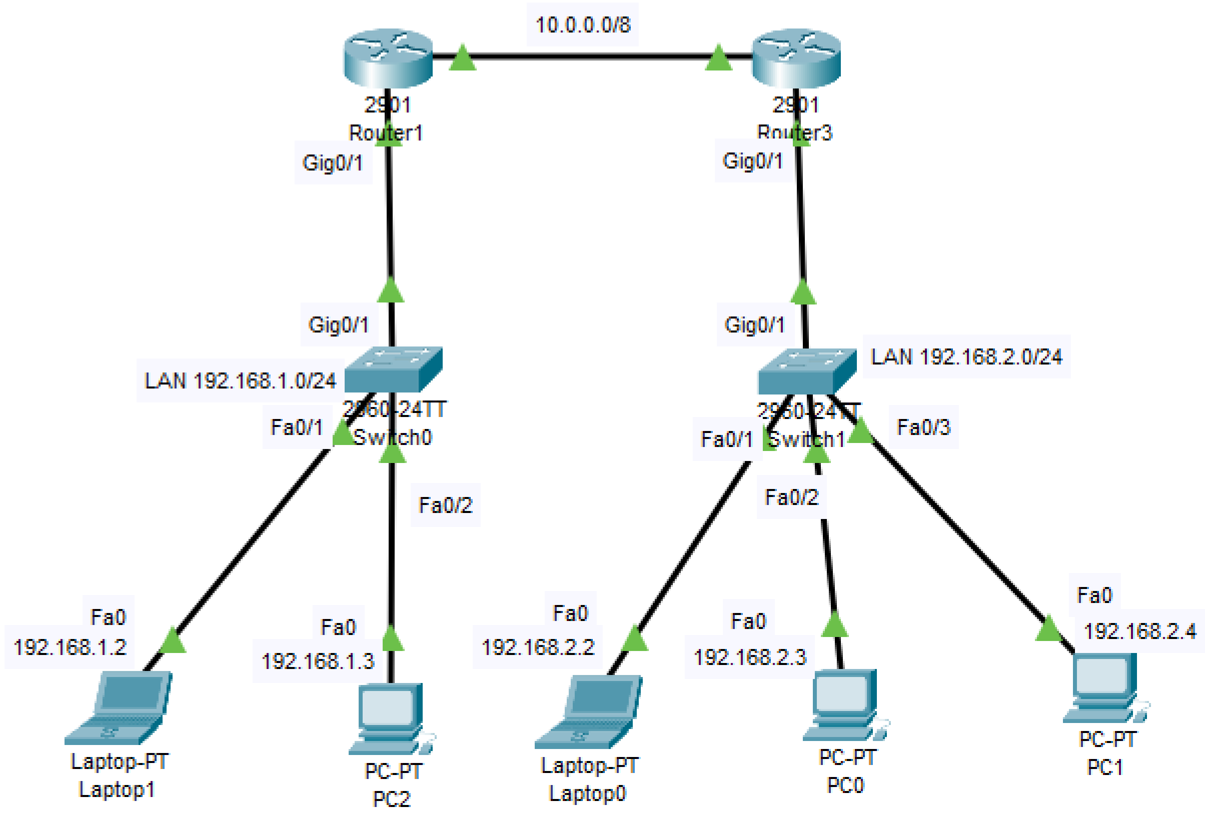
Nishad
Narrator (Nishad):
"As we've seen, our MAC protocol managed packet collisions using a random backoff strategy. By spacing out retransmissions after a collision, we minimized the chances of further collisions, allowing each device to send its packet successfully. This simple protocol illustrates how random access works to manage shared wireless medium access efficiently."
9:08 PM


Host B then transmits its packet after checking the channel.
All hosts enter the backoff state for a random period.
WIFI AP
HOST A
HOST B
HOST C
0 2.5 5 7.5 10 12.5 15 17.5 20 22.5 25 27.5 30 32.5 35 37.5 40
Collision takes place
Host A successfully transmits its packet without collision.
Finally, Host C transmits its packet
All the hosts sends the packets at the same time since channel is idle

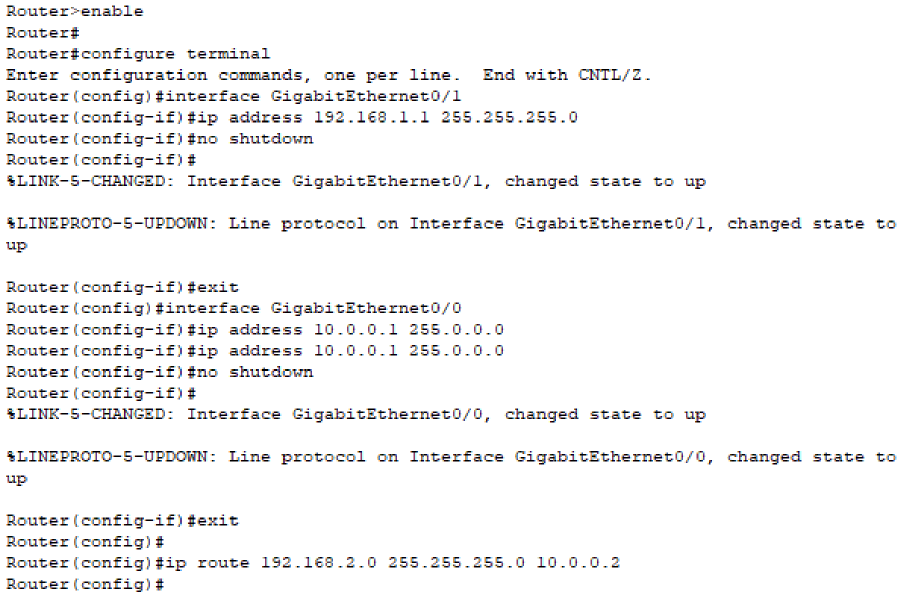
2. Once you have completed the above activity, discuss the following question with your group members.
   - What is the medium access control (MAC) protocol that can be used in WiFi?

The MAC Address protocol used in Wi-Fi is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). this protocol mechanism helps WIFI devices share the wireless medium efferently therefore reducing the chances of data collision and improving overall performance.

Activity 2

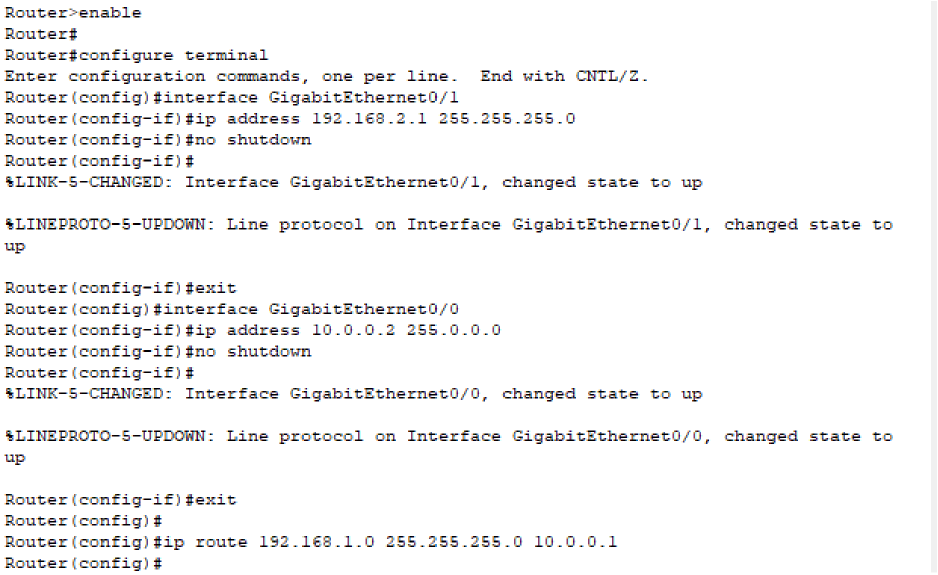


Implement the above network in Cisco Packet Tracer. You can use static IP configuration to configure hosts and router interfaces. Make sure to take screenshots of your findings as you need to include those in the task submissions.



```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to
up

Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to
up

Router(config-if)#exit
Router(config)#
Router(config)#ip route 192.168.2.0 255.255.255.0 10.0.0.2
Router(config)#
```

Router1 Configuration



```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to
up

Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 10.0.0.2 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to
up

Router(config-if)#exit
Router(config)#
Router(config)#ip route 192.168.1.0 255.255.255.0 10.0.0.1
Router(config)#
```

Router3 Configuration

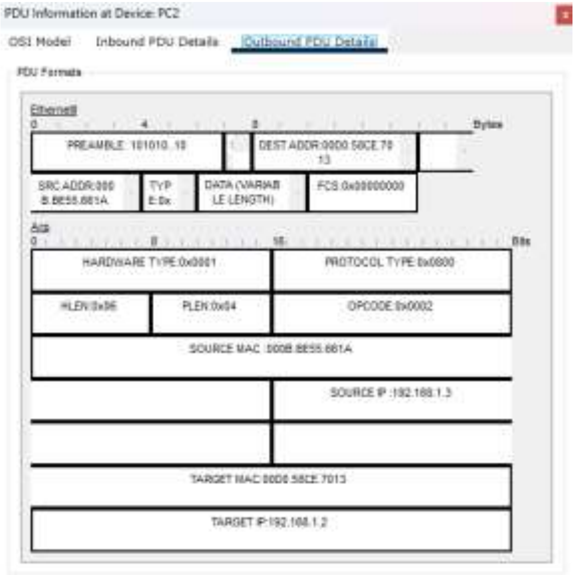
1. As a group, discuss what information Laptop1 in LAN1 requires to connect to PC2 In LAN1.

    - Laptop1 needs the IP address and MAC address of PC2 to communicate with it.

2. What protocol we can use to get the required information? Discuss the steps involved in getting the required information.

    - We can use Address Resolution Protocol (ARP) protocol where an end device sends a broadcast message asking for an IP address of another end device which is wants to communicate with, then the destination end device replies with its IP address and MAC address and the source end device saves it on its ARP table.

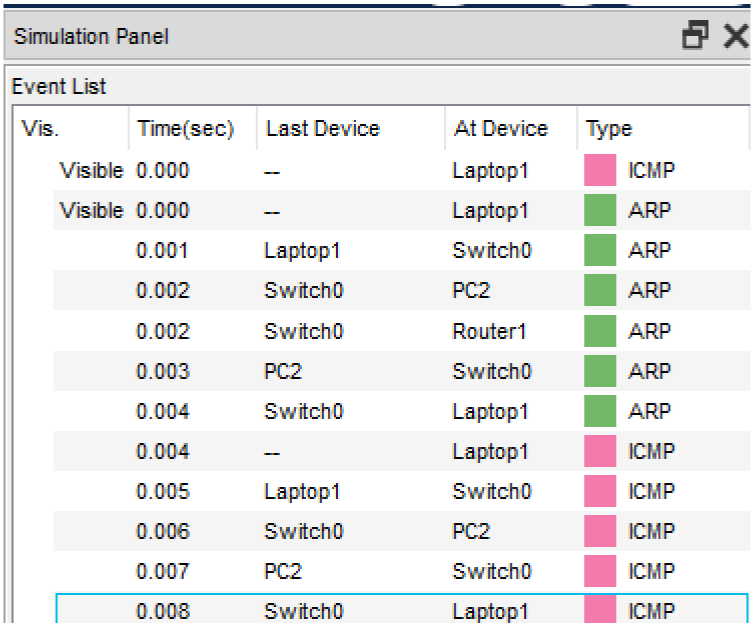
3. Use the simulation mode to check ARP in action by pinging PC2 from Laptop1.
    a. What are the types of messages that PC2 generated?



PREAMBLE: 101010...10
DEST ADDR:0000.58CE.70
13
SRC ADDR:000
B.BE55.661A
TYP
E:0x
DATA (VARIAB
LE LENGTH)
FCS:0x00000000

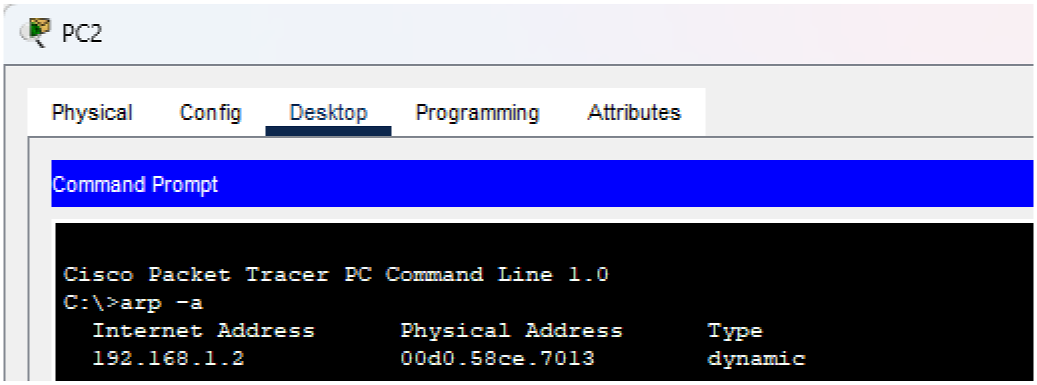
HARDWARE TYPE:0x0001
PROTOCOL TYPE:0x0800
HLEN:0x06
PLEN:0x04
OPCODE:0x0002
SOURCE MAC :000B.BE55.661A
SOURCE IP :192.168.1.3
TARGET MAC:0000.58CE.7013
TARGET IP:192.168.1.2

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).



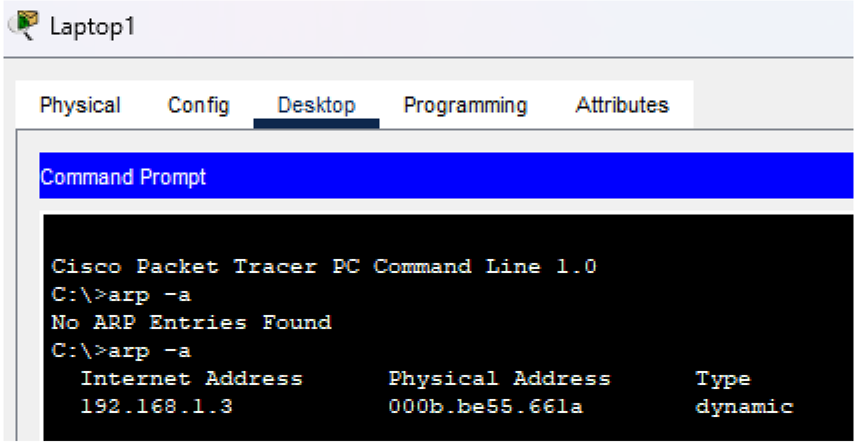
Vis.	Time(sec)	Last Device	At Device	Type
Visible	0.000	--	Laptop1	🟥 ICMP
Visible	0.000	--	Laptop1	🟩 ARP
	0.001	Laptop1	Switch0	🟩 ARP
	0.002	Switch0	PC2	🟩 ARP
	0.002	Switch0	Router1	🟩 ARP
	0.003	PC2	Switch0	🟩 ARP
	0.004	Switch0	Laptop1	🟩 ARP
	0.004	--	Laptop1	🟥 ICMP
	0.005	Laptop1	Switch0	🟥 ICMP
	0.006	Switch0	PC2	🟥 ICMP
	0.007	PC2	Switch0	🟥 ICMP
	0.008	Switch0	Laptop1	🟥 ICMP

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.



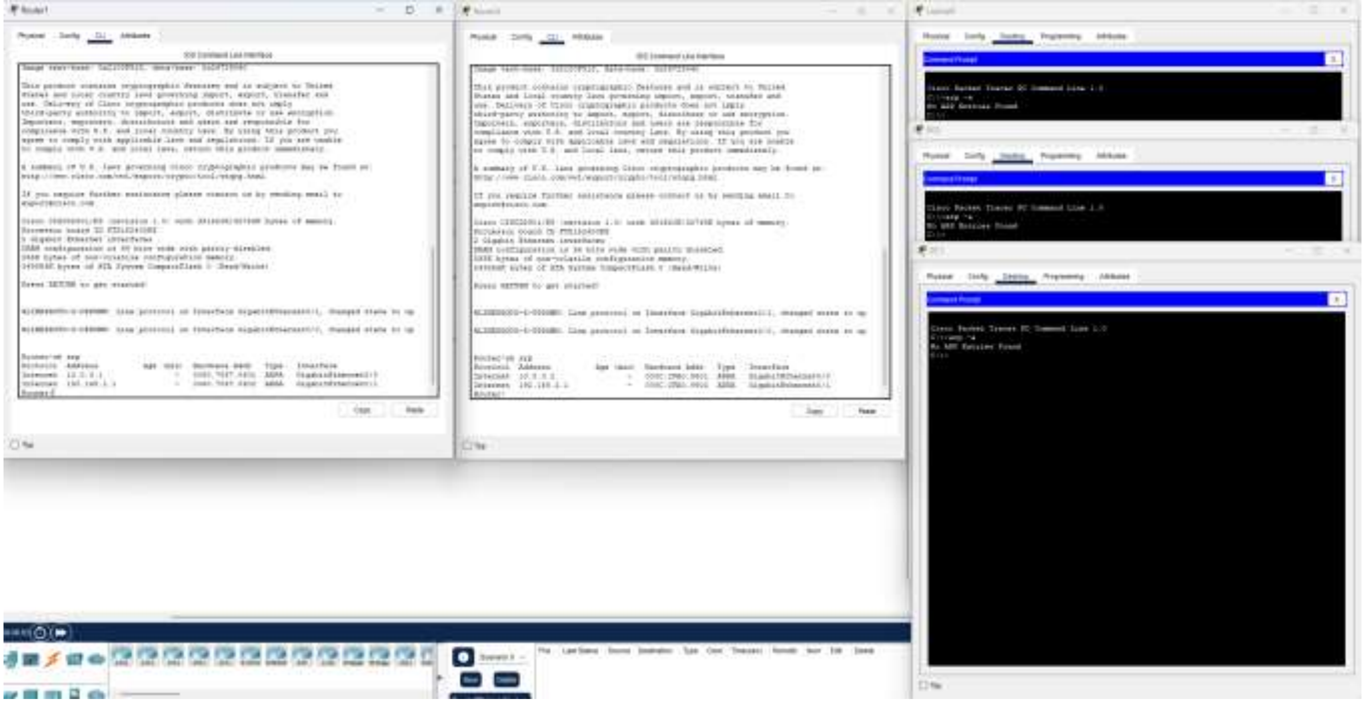
```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.2           00d0.58ce.7013        dynamic
```

PC2's ARP table contains the IP and MAC address of Laptop1 and as seen below Laptop1's ARP table holds the IP and MAC addresses of PC2



```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.3           000b.be55.661a        dynamic
```

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.



```
[illegible]

Router#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.0.0.1                -   [illegible]     ARPA   GigabitEthernet0/1
Internet  192.168.1.1             -   [illegible]     ARPA   GigabitEthernet0/0
Router#
```

```
[illegible]

Router#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.0.0.2                -   [illegible]     ARPA   GigabitEthernet0/0
Internet  192.168.2.1             -   [illegible]     ARPA   GigabitEthernet0/1
Router#
```

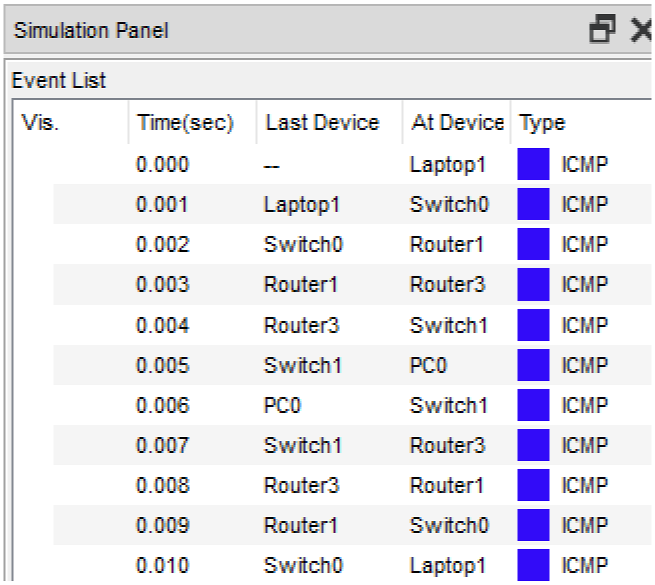
```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>
```

Currently both router only have the IP and MAC addresses of their connection to the switch and the other router and the end devices do not have anh entries in their ARP table.

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.

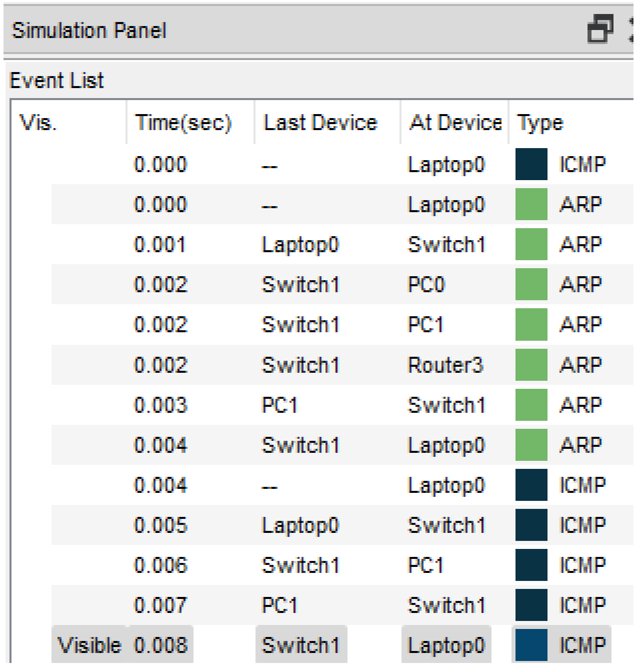


Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	Laptop1	■ ICMP
	0.001	Laptop1	Switch0	■ ICMP
	0.002	Switch0	Router1	■ ICMP
	0.003	Router1	Router3	■ ICMP
	0.004	Router3	Switch1	■ ICMP
	0.005	Switch1	PC0	■ ICMP
	0.006	PC0	Switch1	■ ICMP
	0.007	Switch1	Router3	■ ICMP
	0.008	Router3	Router1	■ ICMP
	0.009	Router1	Switch0	■ ICMP
	0.010	Switch0	Laptop1	■ ICMP

ICMP, sequence once the ARP request was replied between Laptop0 and PC0



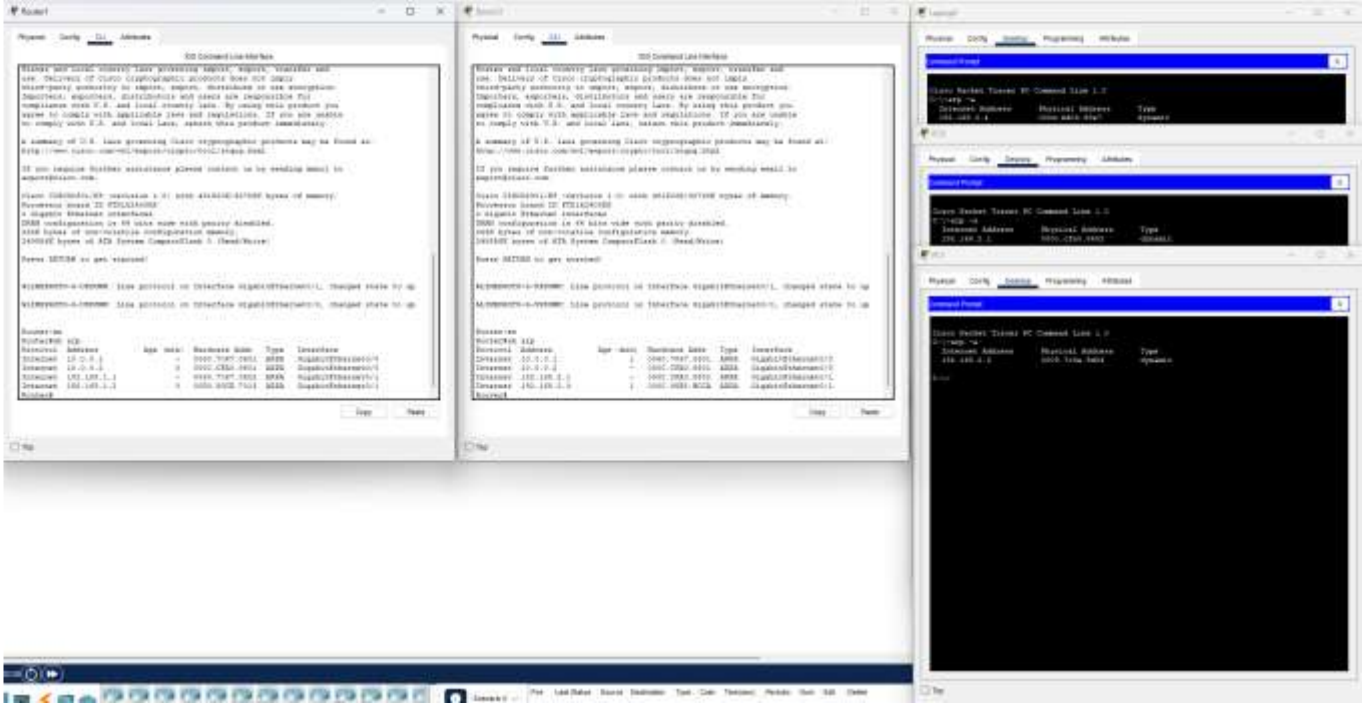
Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	Laptop0	■ ICMP
	0.000	--	Laptop0	🟩 ARP
	0.001	Laptop0	Switch1	🟩 ARP
	0.002	Switch1	PC0	🟩 ARP
	0.002	Switch1	PC1	🟩 ARP
	0.002	Switch1	Router3	🟩 ARP
	0.003	PC1	Switch1	🟩 ARP
	0.004	Switch1	Laptop0	🟩 ARP
	0.004	--	Laptop0	■ ICMP
	0.005	Laptop0	Switch1	■ ICMP
	0.006	Switch1	PC1	■ ICMP
	0.007	PC1	Switch1	■ ICMP
Visible	0.008	Switch1	Laptop0	■ ICMP

Successful ARP sequence leading to the aftermath ICMP sequence as well between Laptop0 and PC1

7. Check the arp tables of router 1, router 2, PC0, PC1, and Laptop0.



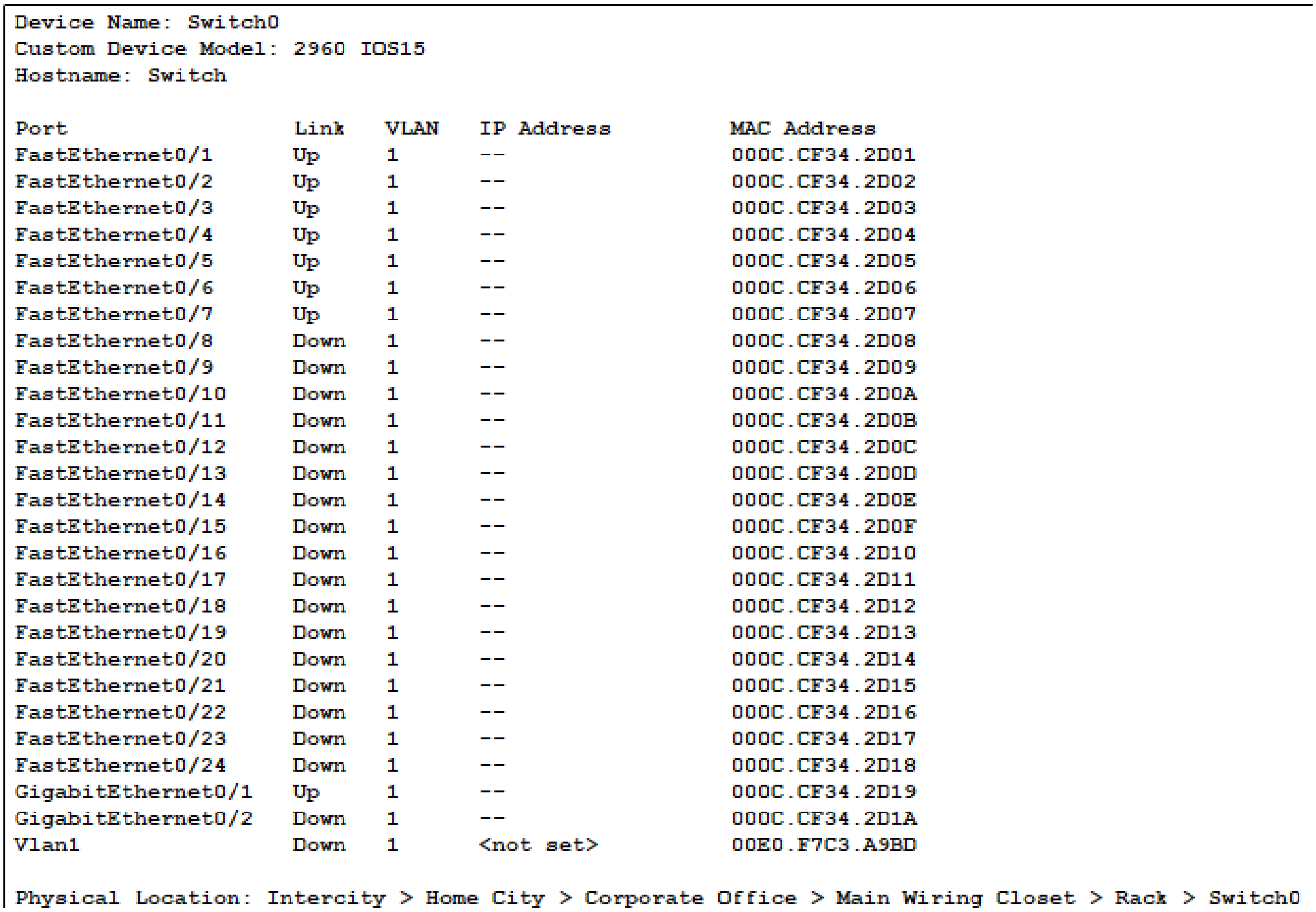
Updated ARP tables

8. Compare your observations with the observations you recorded in step 5. Discuss your finding with your group members.
   - We can see that the reason both routers and all end devices in the 192.168.2.0 subnet have updated their ARP tables is because by sending ARP request to send a ping any end device, be it in your own subnet or not if there is a reply, you will get the receivers IP and MAC address as you can see in the diagrams above.

Activity 3

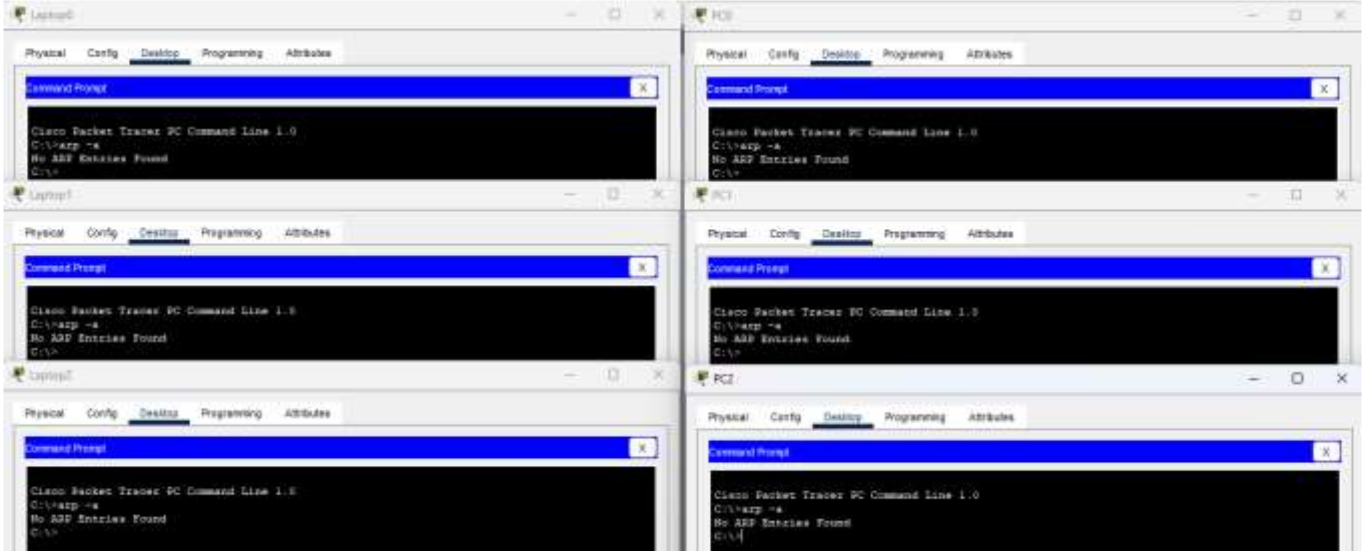
For this activity, you need to build and configure the following topology using a Cisco 2960 Switch.

1. After you configured the devices using static IP configuration,
   a. Record the MAC addresses of PCs/laptops/servers and Ethernet Ports of Switches.



```
Device Name: Switch0
Custom Device Model: 2960 IOS15
Hostname: Switch

Port                  Link   VLAN  IP Address          MAC Address
FastEthernet0/1       Up     1     --                  000C.CF34.2D01
FastEthernet0/2       Up     1     --                  000C.CF34.2D02
FastEthernet0/3       Up     1     --                  000C.CF34.2D03
FastEthernet0/4       Up     1     --                  000C.CF34.2D04
FastEthernet0/5       Up     1     --                  000C.CF34.2D05
FastEthernet0/6       Up     1     --                  000C.CF34.2D06
FastEthernet0/7       Up     1     --                  000C.CF34.2D07
FastEthernet0/8       Down   1     --                  000C.CF34.2D08
FastEthernet0/9       Down   1     --                  000C.CF34.2D09
FastEthernet0/10      Down   1     --                  000C.CF34.2D0A
FastEthernet0/11      Down   1     --                  000C.CF34.2D0B
FastEthernet0/12      Down   1     --                  000C.CF34.2D0C
FastEthernet0/13      Down   1     --                  000C.CF34.2D0D
FastEthernet0/14      Down   1     --                  000C.CF34.2D0E
FastEthernet0/15      Down   1     --                  000C.CF34.2D0F
FastEthernet0/16      Down   1     --                  000C.CF34.2D10
FastEthernet0/17      Down   1     --                  000C.CF34.2D11
FastEthernet0/18      Down   1     --                  000C.CF34.2D12
FastEthernet0/19      Down   1     --                  000C.CF34.2D13
FastEthernet0/20      Down   1     --                  000C.CF34.2D14
FastEthernet0/21      Down   1     --                  000C.CF34.2D15
FastEthernet0/22      Down   1     --                  000C.CF34.2D16
FastEthernet0/23      Down   1     --                  000C.CF34.2D17
FastEthernet0/24      Down   1     --                  000C.CF34.2D18
GigabitEthernet0/1    Up     1     --                  000C.CF34.2D19
GigabitEthernet0/2    Down   1     --                  000C.CF34.2D1A
Vlan1                 Down   1     <not set>           00E0.F7C3.A9BD

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Switch0
```

b. Record the arp table in PCs and laptops.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>
```

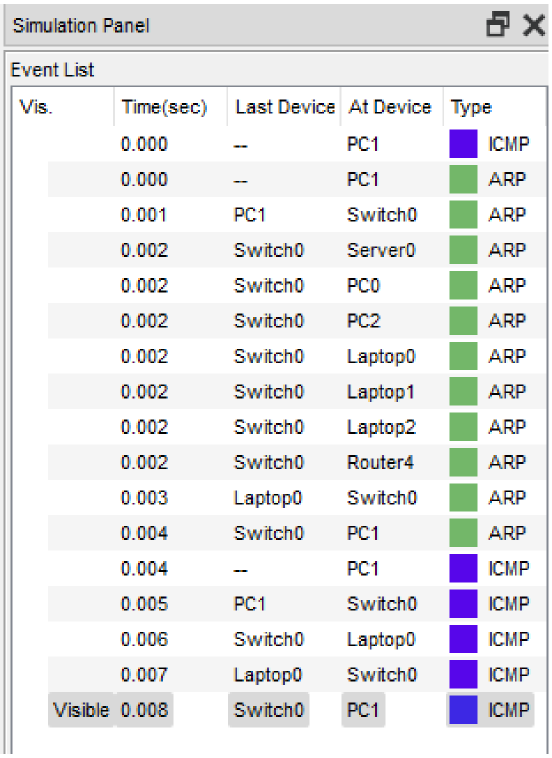
c. Check the MAC address table of the switch. In switch's CLI, you can type the following command to show the MAC address table.

```
Switch>en
Switch#sh mac-add
Switch#sh mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0060.3e69.9001    DYNAMIC     Gig0/1
Switch#
```

d. Record your observations. If there are any records in the MAC table, explain your observation.

- The switch currently only has the router's MAC Address since the router is connected with its gig ethernet port to the switch's gig ethernet port thus letting the switch to record the routers mac addresses with the port its connected to.

e. Now, ping from PC1 and PC2 to Laptop0 and Laptop 1, respectively.

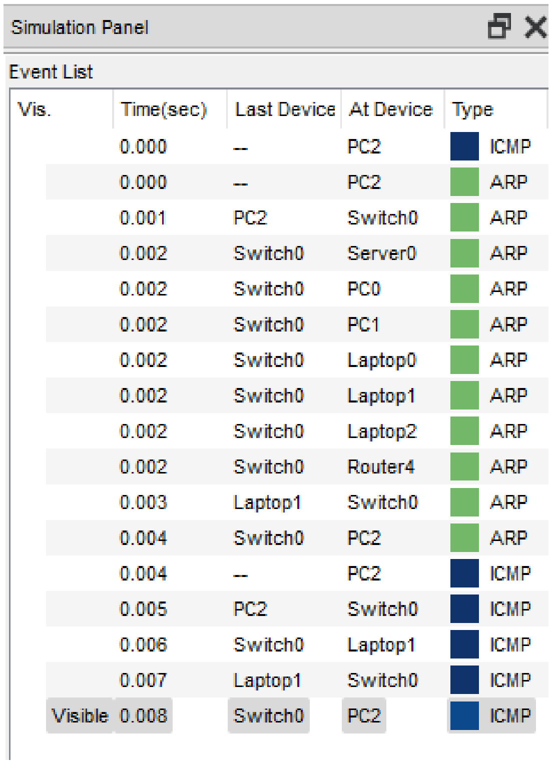


Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC1	🟪 ICMP
	0.000	--	PC1	🟩 ARP
	0.001	PC1	Switch0	🟩 ARP
	0.002	Switch0	Server0	🟩 ARP
	0.002	Switch0	PC0	🟩 ARP
	0.002	Switch0	PC2	🟩 ARP
	0.002	Switch0	Laptop0	🟩 ARP
	0.002	Switch0	Laptop1	🟩 ARP
	0.002	Switch0	Laptop2	🟩 ARP
	0.002	Switch0	Router4	🟩 ARP
	0.003	Laptop0	Switch0	🟩 ARP
	0.004	Switch0	PC1	🟩 ARP
	0.004	--	PC1	🟪 ICMP
	0.005	PC1	Switch0	🟪 ICMP
	0.006	Switch0	Laptop0	🟪 ICMP
	0.007	Laptop0	Switch0	🟪 ICMP
Visible	0.008	Switch0	PC1	🟦 ICMP

Pinging from PC1 to Laptop0 successfully



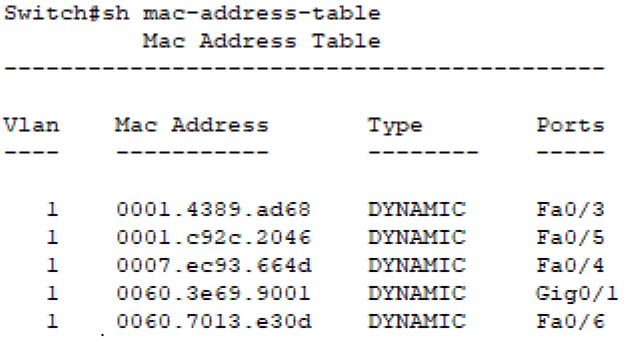
Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC2	🟦 ICMP
	0.000	--	PC2	🟩 ARP
	0.001	PC2	Switch0	🟩 ARP
	0.002	Switch0	Server0	🟩 ARP
	0.002	Switch0	PC0	🟩 ARP
	0.002	Switch0	PC1	🟩 ARP
	0.002	Switch0	Laptop0	🟩 ARP
	0.002	Switch0	Laptop1	🟩 ARP
	0.002	Switch0	Laptop2	🟩 ARP
	0.002	Switch0	Router4	🟩 ARP
	0.003	Laptop1	Switch0	🟩 ARP
	0.004	Switch0	PC2	🟩 ARP
	0.004	--	PC2	🟦 ICMP
	0.005	PC2	Switch0	🟦 ICMP
	0.006	Switch0	Laptop1	🟦 ICMP
	0.007	Laptop1	Switch0	🟦 ICMP
Visible	0.008	Switch0	PC2	🟦 ICMP

Pinging from PC2 to Laptop1 successfully

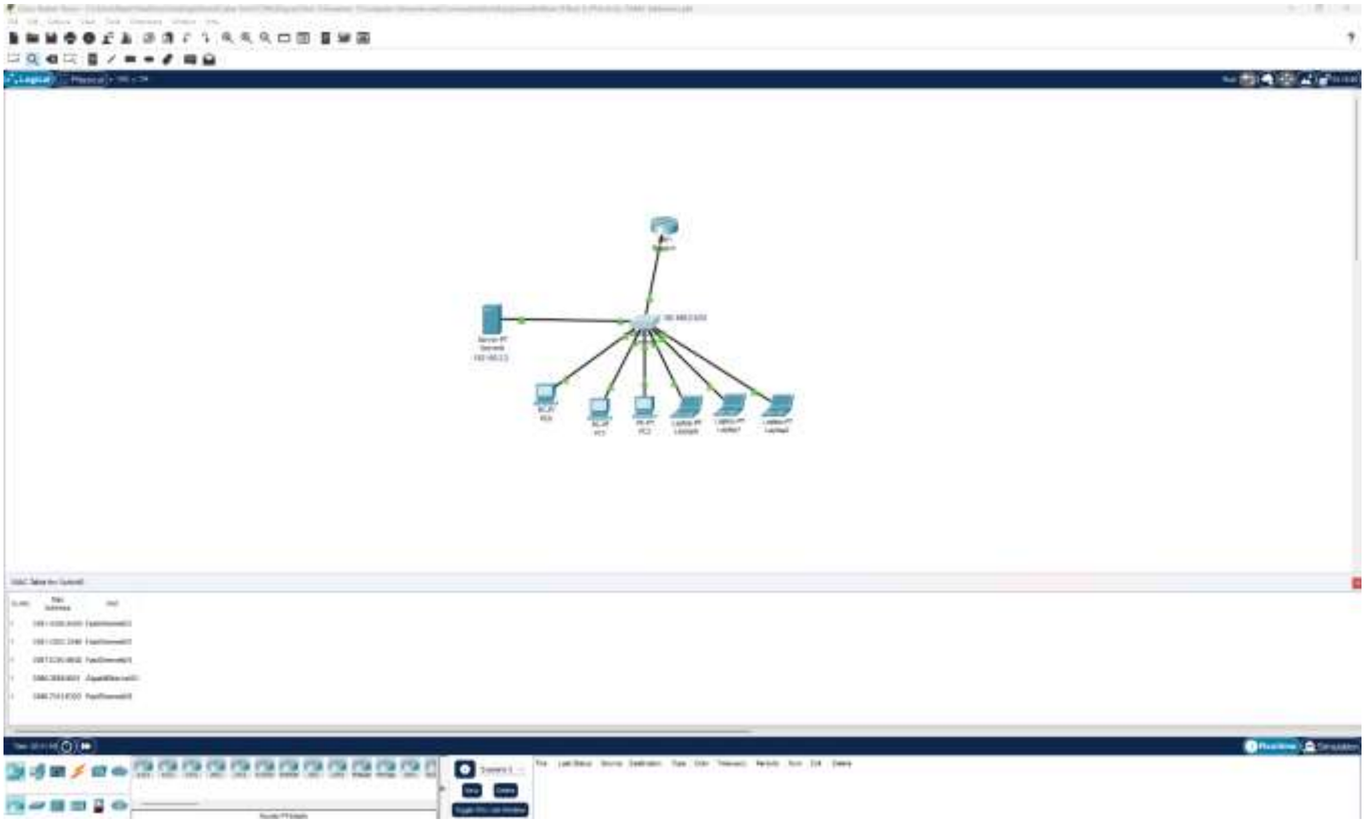
f. Check the MAC address table of the switch. Explain your observations.



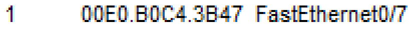
```
Switch#sh mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.4389.ad68    DYNAMIC     Fa0/3
   1    0001.c92c.2046    DYNAMIC     Fa0/5
   1    0007.ec93.664d    DYNAMIC     Fa0/4
   1    0060.3e69.9001    DYNAMIC     Gig0/1
   1    0060.7013.e30d    DYNAMIC     Fa0/6
```

After the ARP request and reply. The MAC Address table has been enlarged with the details of ARP packets sent by end devices being recorded as they arrived at the switch.

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.



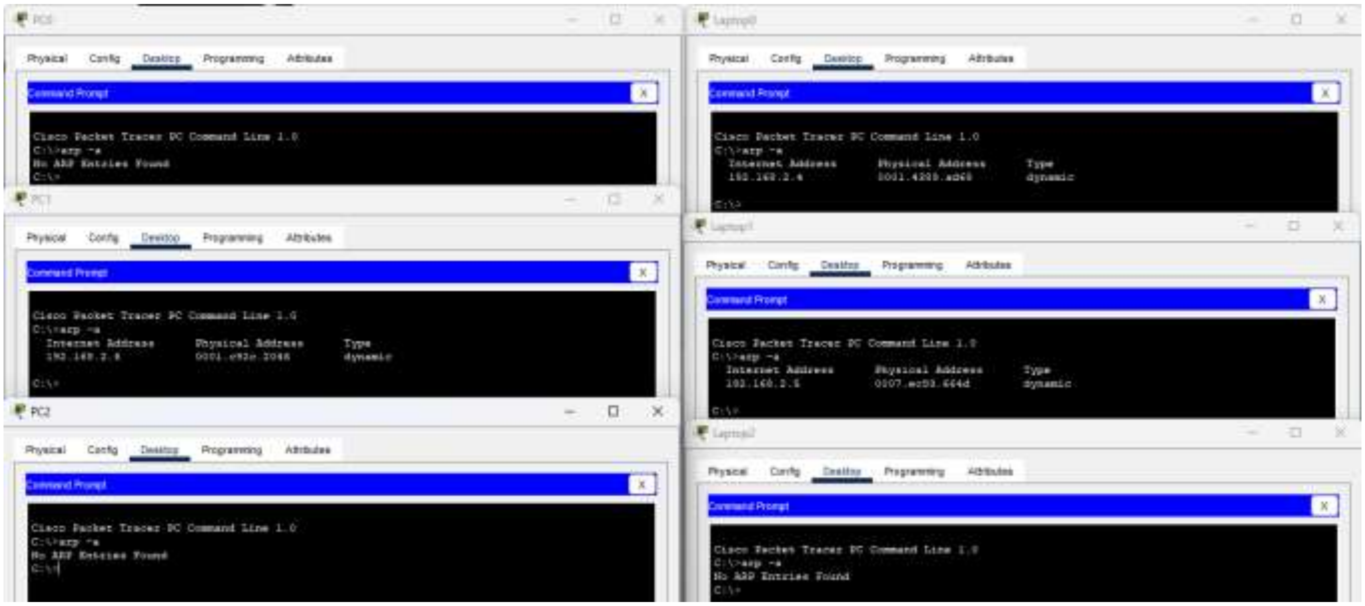
h. Ping laptop2 from PC0 and check the changes in the MAC table. Explain your observation.



```
1        00E0.B0C4.3B47  FastEthernet0/7
```

- A new MAC Address entry has been added after the Pinging Laptop2 from PC0. Since they hadn’t communicated before, PC0 sent out an ARP broadcast request and Laptop2 replied by sending its MAC Address and the switch recorded it

i. Check the arp tables in all the PCs and laptops.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.2.4           0001.4288.ad68        dynamic

C:\>
```

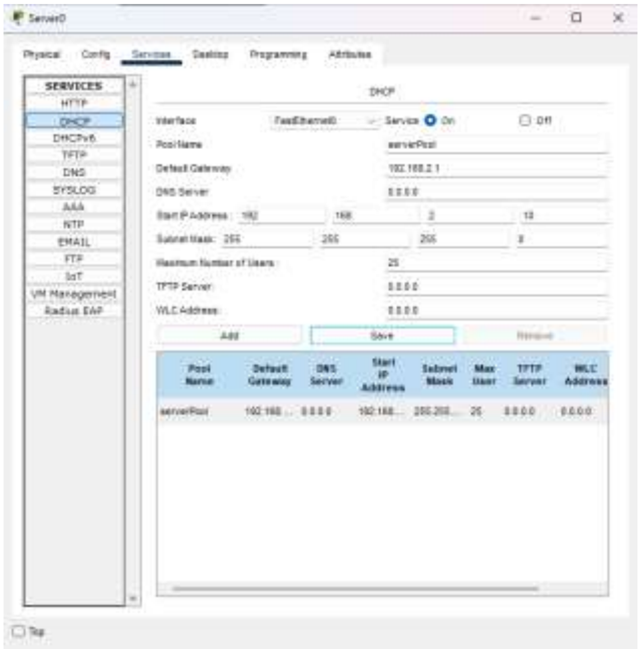
```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.2.8           0001.c92c.2048        dynamic

C:\>
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.2.5           0007.ec93.664d        dynamic

C:\>
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>
```

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.



Interface FastEthernet0 Service ● On ○ Off

Pool Name: serverPool

Default Gateway: 192.168.2.1

DNS Server: 0.0.0.0

Start IP Address: 192 168 2 10

Subnet Mask: 255 255 255 0

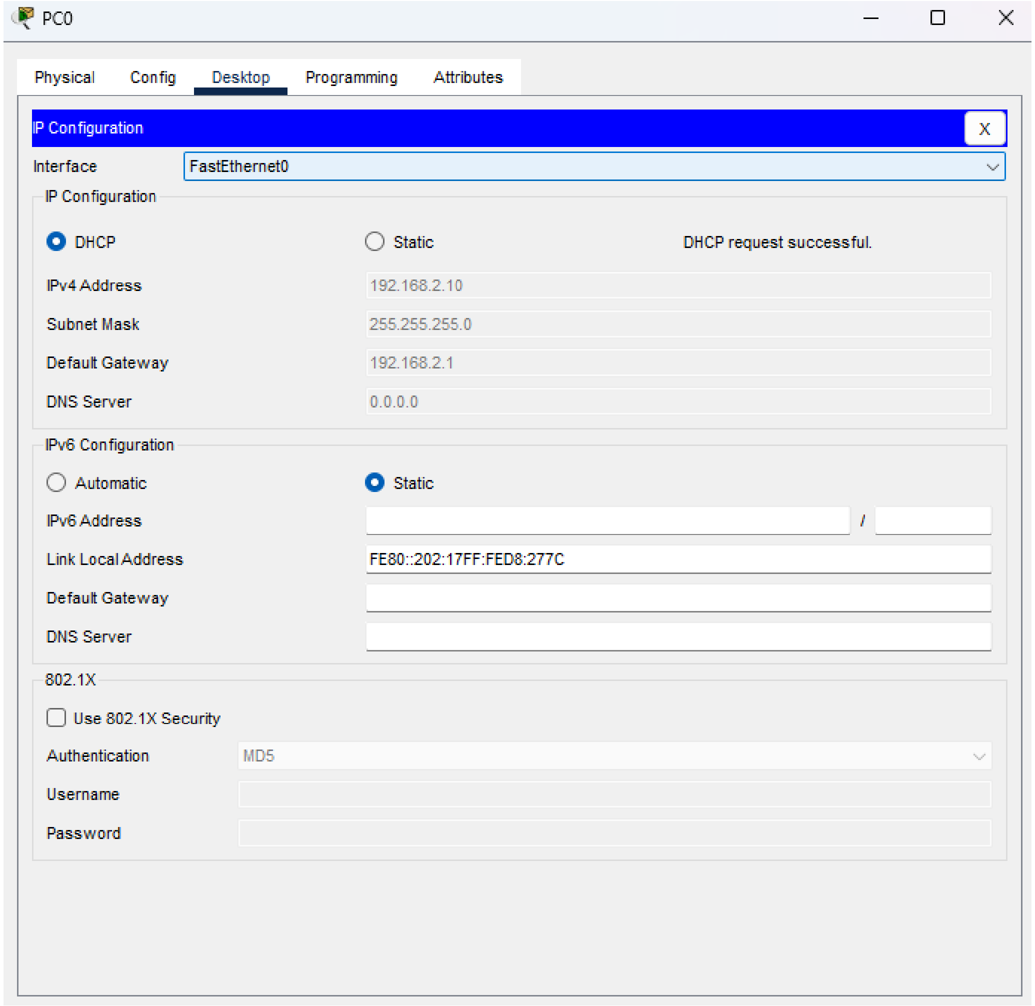
Maximum Number of Users: 25

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168....	0.0.0.0	192.168....	255.255....	25	0.0.0.0	0.0.0.0

Configuring server by adding a DHCP pool



IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address: 192.168.2.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::202:17FF:FED8:277C

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

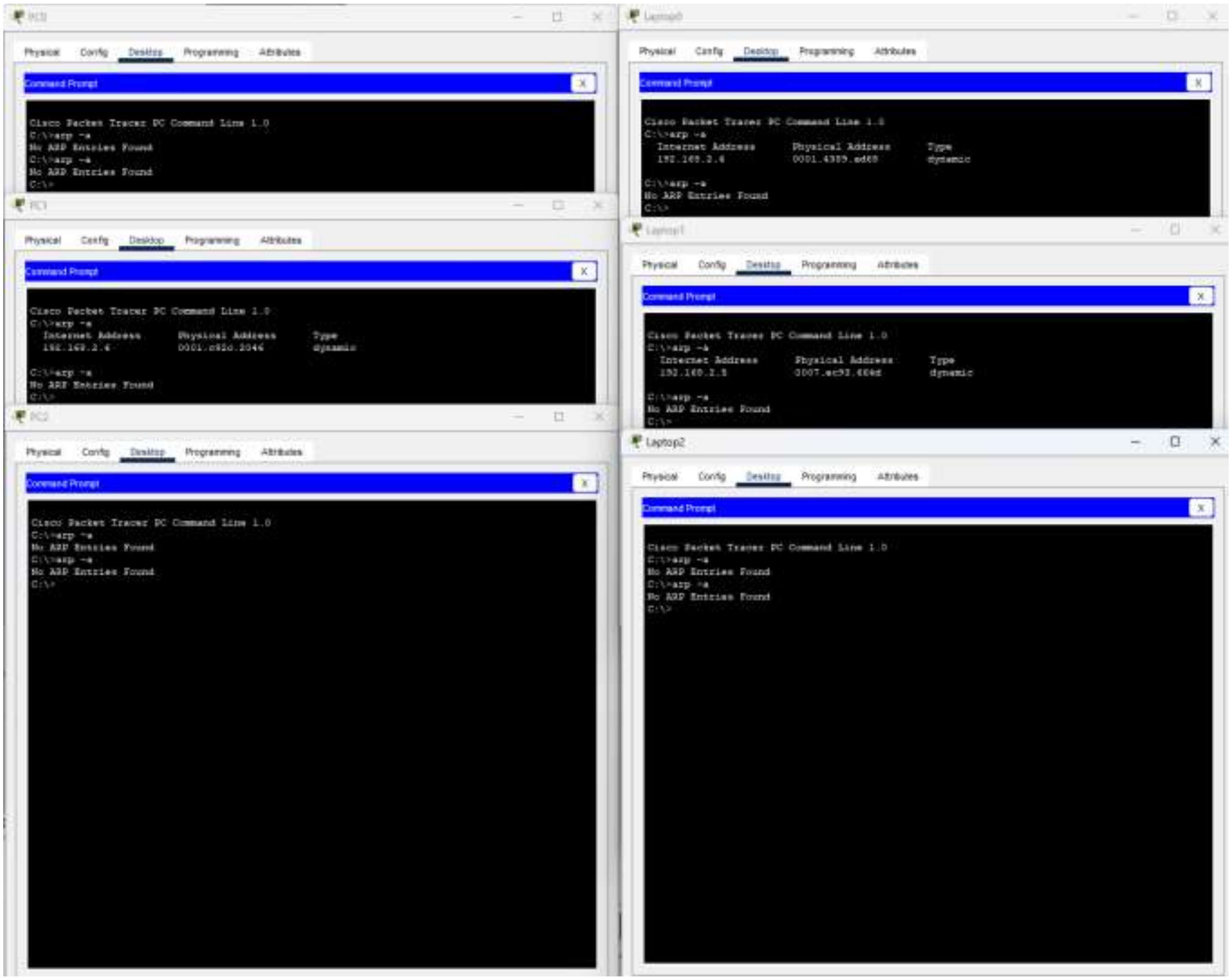
Authentication: MD5

Username:

Password:

Setting IP Configuration in end devices to DHCP as seen in PC0

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



```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>arp -a
No ARP Entries Found
C:\>
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.2.4           0001.c82c.2046        dynamic

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

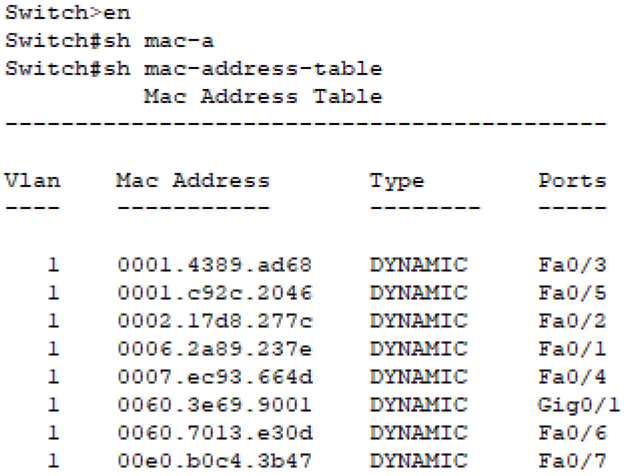
```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>arp -a
No ARP Entries Found
C:\>
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.2.6           0001.4389.ad68        dynamic

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

```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.2.5           0007.ec92.6d4d        dynamic

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

```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>arp -a
No ARP Entries Found
C:\>
```

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



```
Switch>en
Switch#sh mac-a
Switch#sh mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.4389.ad68    DYNAMIC     Fa0/3
   1    0001.c92c.2046    DYNAMIC     Fa0/5
   1    0002.17d8.277c    DYNAMIC     Fa0/2
   1    0006.2a89.237e    DYNAMIC     Fa0/1
   1    0007.ec93.664d    DYNAMIC     Fa0/4
   1    0060.3e69.9001    DYNAMIC     Gig0/1
   1    0060.7013.e30d    DYNAMIC     Fa0/6
   1    00e0.b0c4.3b47    DYNAMIC     Fa0/7
```

The switch automatically records the ARP packets it receives by the end devices who are sending a broadcast message to the server to receive a address from the DHCP server pool.

Above and Beyond Tasks

1. Discuss the security issues associated with ARP identifying the types of attacks (200 – 300 words).

ARP's absence of authentication procedures leaves it open to many security concerns, despite its crucial role in mapping IP addresses to MAC addresses within a network. Now, let's talk about its shortcomings.

ARP Spoofing

ARP spoofing is one of the most popular attacks that take use of ARP vulnerabilities. In order to carry out this attack, a malevolent actor would forge ARP messages and send them into the network, linking their MAC address to the IP address of a victim host or gateway. Consequently, data meant for the authorized device may be intercepted, altered, or blocked by the attacker. This could serve as the basis for a number of attacks, including

1. Man-in-the-Middle – ARP spoofing is used by the attacker in an MITM attack to place himself in the middle of two communicating devices. This gives them the ability to intercept or modify the data being delivered, which can result in data manipulation, information theft, or session hijacking.
2. Denial of Service (DoS) – By associating fictitious MAC addresses with IP addresses through ARP spoofing, an attacker can essentially render the target device unavailable, causing interruptions to the network and a denial of service.
3. Session Hijacking – After employing ARP spoofing to intercept traffic, an attacker can hijack ongoing sessions between two authentic hosts by inserting malicious commands or obtaining private session tokens, like login passwords.