Department of Computer Science and Engineering

Islamic University of Technology (IUT)

A subsidiary organ of OIC

Laboratory Report

CSE 4412 : Data Communication and Networking Lab

Name	**: M M Nazmul Hossain**
Student ID	**: 200042118**
Section	**: 1**
Semester	**: 4th**
Academic Year	**: 2021-2022**
Date of Submission	**: 29.01.2023**
Lab No	**: 4**

Title: Observation of ARP events and lecture on Logical Addressing.

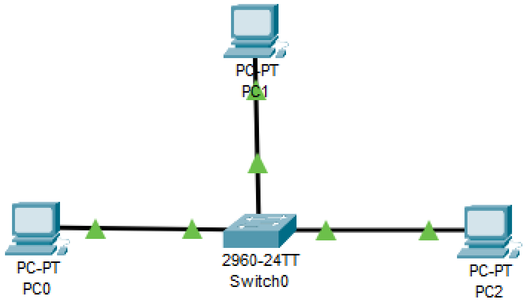
Objective:

1. Understand how the physical address of a node in the same network is found when the source only knows the logical address.
2. Understand the necessity of hierarchical addressing compared to flat addressing.
3. Understand classful addressing of IPv4 Addressing.
4. Understand the subnet mask.

Devices/ Software Used:

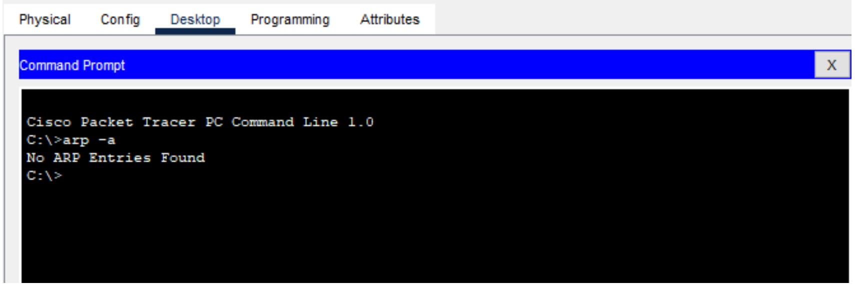
Cisco Packet Tracer: 3 End- User PCs, 1 Switch

Diagram of the experiment:



Experiment Set Up Description:

1. First, set up 3 End-User PCs and join them with copper straight through cable with a Switch.
2. Manually set the IP address of each PC. Let PC0 IP be 192.168.0.1, PC1 be 192.168.0.2, PC2 be 192.168.0.3.
3. Then, check from PC0, we are going to use the command “arp -a” at command line to check the ARP Table. It is found to be empty.

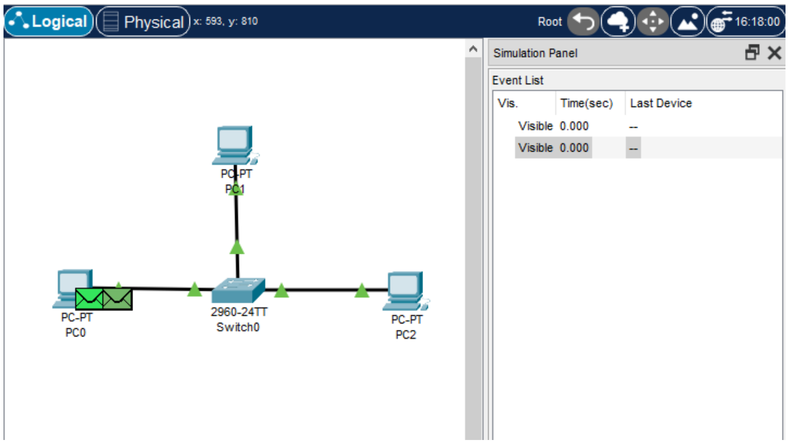


```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>
```

4. Then, send packets from PC0 to PC1 using the command “ping 192.168.0.2” at Simulation Mode keeping only the filters of ARP and ICMP ticked.

Observation:

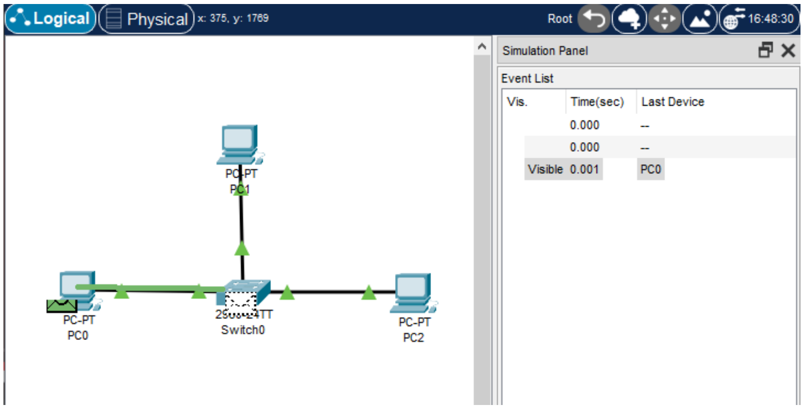
1. It is observed that while pinging, PC0 is sending a different packet at first. The PC1 MAC address and IP address is set as the destination packet address. It is to populate the ARP table.



Simulation Panel

Event List

Vis.	Time(sec)	Last Device
Visible	0.000	--
Visible	0.000	--

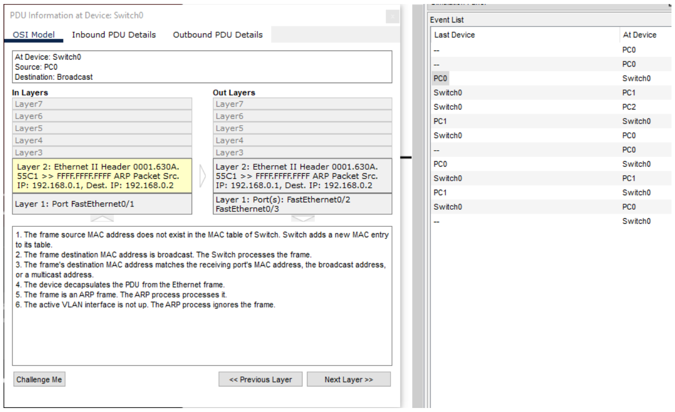


Simulation Panel

Event List

Vis.	Time(sec)	Last Device
	0.000	--
	0.000	--
Visible	0.001	PC0

2. Since the ARP table was not populated, the IP and MAC address didn't match with any entries in the ARP table. The packet broadcasts to all PCs connected to the switch. The broadcast address is FFFF.FFFF.FFFF.FFFF, which means all connected devices except the sender will receive a request.



PDU Information at Device: Switch0

At Device: Switch0
Source: PC0
Destination: Broadcast

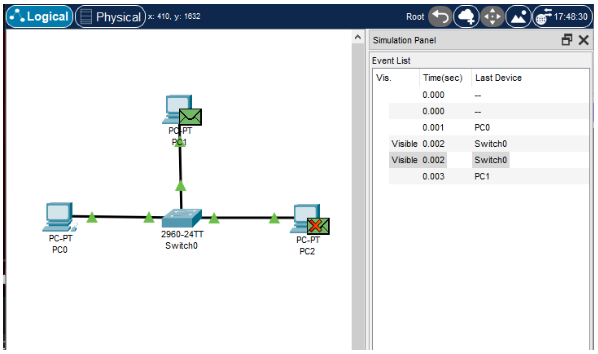
In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3
Layer 2: Ethernet II Header 0001.630A.55C1 >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.0.1, Dest. IP: 192.168.0.2	Layer 2: Ethernet II Header 0001.630A.55C1 >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.0.1, Dest. IP: 192.168.0.2
Layer 1: Port FastEthernet0/1	Layer 1: Port(s): FastEthernet0/2 FastEthernet0/3

1. The frame source MAC address does not exist in the MAC table of Switch. Switch adds a new MAC entry to its table.
2. The frame destination MAC address is broadcast. The Switch processes the frame.
3. The frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address.
4. The device decapsulates the PDU from the Ethernet frame.
5. The frame is an ARP frame. The ARP process processes it.
6. The active VLAN interface is not up. The ARP process ignores the frame.

Event List

Last Device	At Device
--	PC0
--	PC0
PC0	Switch0
Switch0	PC1
Switch0	PC2
PC1	Switch0
Switch0	PC0
--	PC0
PC0	Switch0
Switch0	PC1
PC1	Switch0
Switch0	PC0
--	Switch0

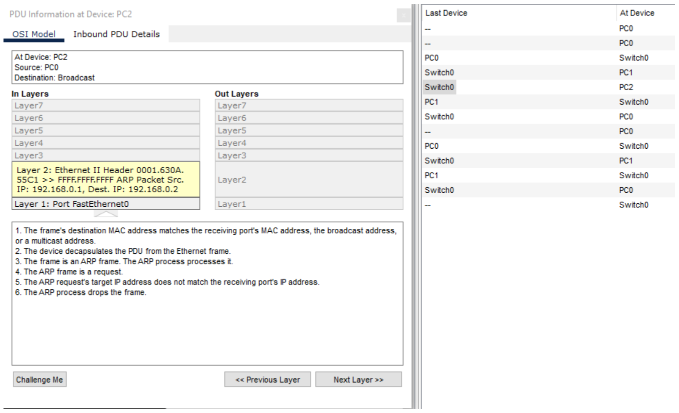
3. The broadcast sends a packet to both PC1 and PC2 since they were the devices which didn't send any request.



Event List

Vis.	Time(sec)	Last Device
	0.000	--
	0.000	--
	0.001	PC0
Visible	0.002	Switch0
Visible	0.002	Switch0
	0.003	PC1

4. At PC2, the request is rejected since the destination IP address don't match.



PDU Information at Device: PC2

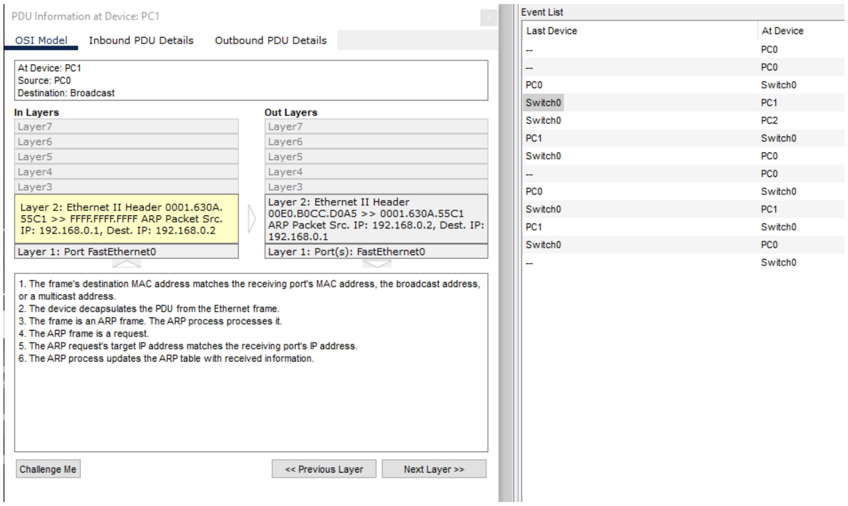
At Device: PC2
Source: PC0
Destination: Broadcast

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3
Layer 2: Ethernet II Header 0001.630A.55C1 >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.0.1, Dest. IP: 192.168.0.2	Layer2
Layer 1: Port FastEthernet0	Layer1

1. The frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address.
2. The device decapsulates the PDU from the Ethernet frame.
3. The frame is an ARP frame. The ARP process processes it.
4. The ARP frame is a request.
5. The ARP request's target IP address does not match the receiving port's IP address.
6. The ARP process drops the frame.

Last Device	At Device
--	PC0
--	PC0
PC0	Switch0
Switch0	PC1
Switch0	PC2
PC1	Switch0
Switch0	PC0
--	PC0
PC0	Switch0
Switch0	PC1
PC1	Switch0
Switch0	PC0
--	Switch0

5. At PC1, the request is received as the Port, IP Address and MAC Address match. PC1 returns a reply. The packet's source is set to the MAC address and IP address for PC0 and the packet destination MAC and IP address is set as the address for PC1.



PDU Information at Device: PC1

At Device: PC1
Source: PC0
Destination: Broadcast

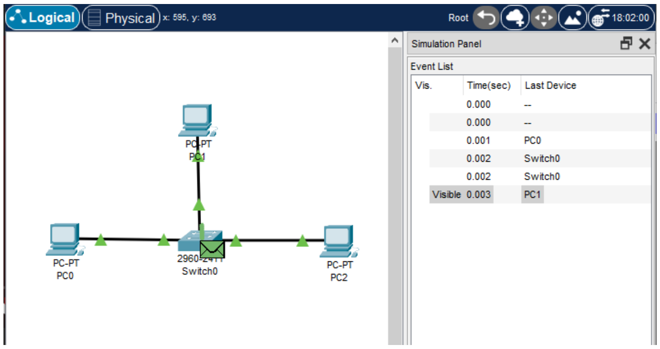
In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3
Layer 2: Ethernet II Header 0001.630A.55C1 >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.0.1, Dest. IP: 192.168.0.2	Layer 2: Ethernet II Header 00E0.B0CC.D0A5 >> 0001.630A.55C1 ARP Packet Src. IP: 192.168.0.2, Dest. IP: 192.168.0.1
Layer 1: Port FastEthernet0	Layer 1: Port(s): FastEthernet0

1. The frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address.
2. The device decapsulates the PDU from the Ethernet frame.
3. The frame is an ARP frame. The ARP process processes it.
4. The ARP frame is a request.
5. The ARP request's target IP address matches the receiving port's IP address.
6. The ARP process updates the ARP table with received information.

Event List

Last Device	At Device
--	PC0
--	PC0
PC0	Switch0
Switch0	PC1
Switch0	PC2
PC1	Switch0
Switch0	PC0
--	PC0
PC0	Switch0
Switch0	PC1
PC1	Switch0
Switch0	PC0
--	Switch0

6. During this time, when the reply reaches the switch0, it sees that the source MAC address doesn't exist in the MAC table of Switch. The switch then adds a new MAC entry. The ARP table is also updated since the frame is an ARP frame.

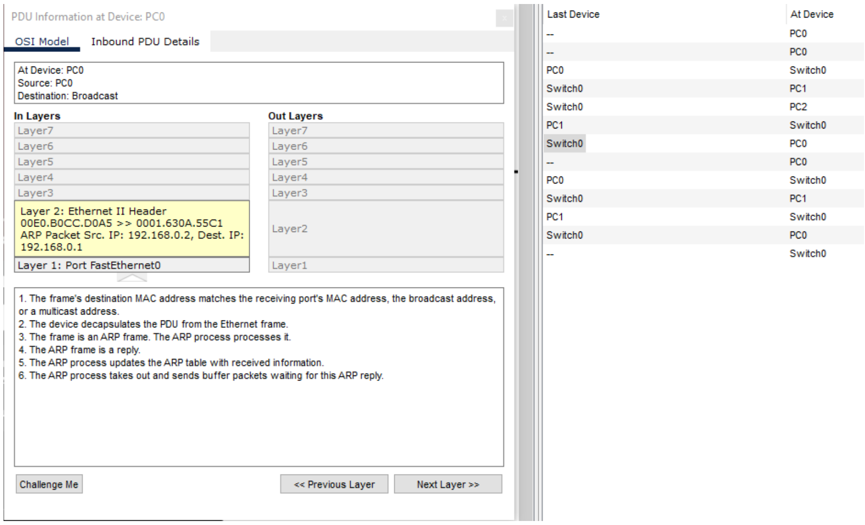


Simulation Panel

Event List

Vis.	Time(sec)	Last Device
	0.000	--
	0.000	--
	0.001	PC0
	0.002	Switch0
	0.002	Switch0
Visible	0.003	PC1

7. The switch sends the ARP reply back to PC0, where it is received. After receiving the mail, the PC finally starts sending an ICMP packet. The packet's source is set to the MAC address and IP address for PC0 and the packet destination MAC and IP address is set as the address for PC1.



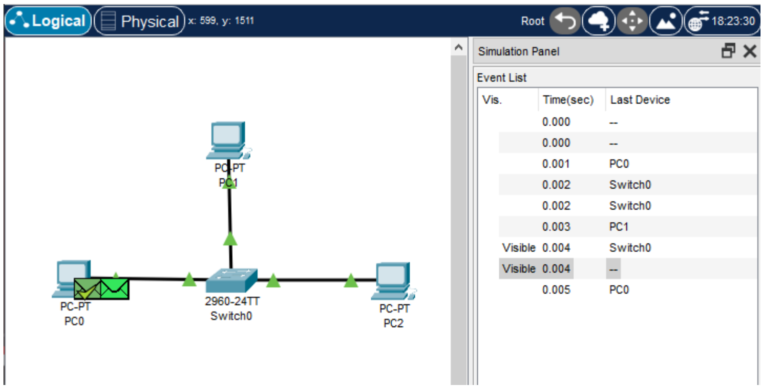
PDU Information at Device: PC0

At Device: PC0
Source: PC0
Destination: Broadcast

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3
Layer 2: Ethernet II Header 00E0.B0CC.D0A5 >> 0001.630A.55C1 ARP Packet Src. IP: 192.168.0.2, Dest. IP: 192.168.0.1	Layer2
Layer 1: Port FastEthernet0	Layer1

1. The frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address.
2. The device decapsulates the PDU from the Ethernet frame.
3. The frame is an ARP frame. The ARP process processes it.
4. The ARP frame is a reply.
5. The ARP process updates the ARP table with received information.
6. The ARP process takes out and sends buffer packets waiting for this ARP reply.

Last Device	At Device
--	PC0
--	PC0
PC0	Switch0
Switch0	PC1
Switch0	PC2
PC1	Switch0
Switch0	PC0
--	PC0
PC0	Switch0
Switch0	PC1
PC1	Switch0
Switch0	PC0
--	Switch0

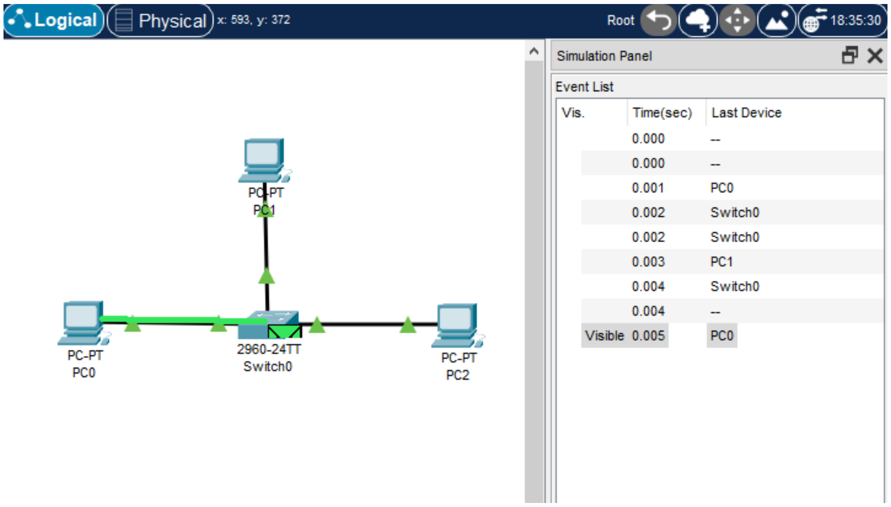


Simulation Panel

Event List

Vis.	Time(sec)	Last Device
	0.000	--
	0.000	--
	0.001	PC0
	0.002	Switch0
	0.002	Switch0
	0.003	PC1
Visible	0.004	Switch0
Visible	0.004	--
	0.005	PC0

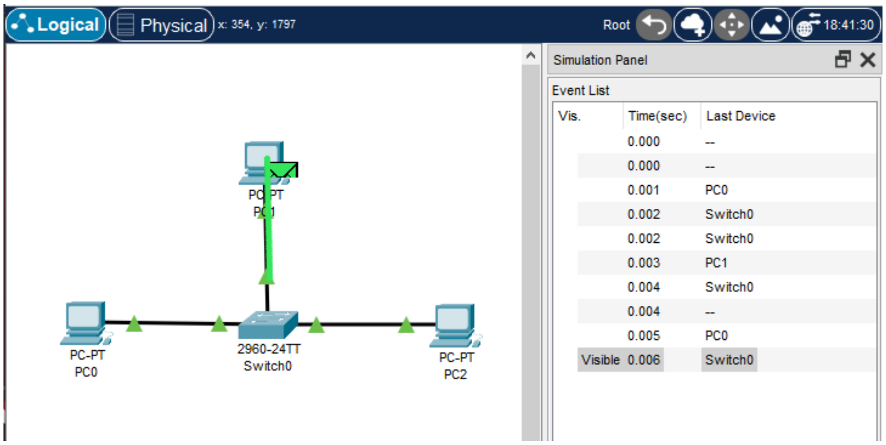
8. The ICMP packet is sent to the Switch and this packet is forwarded directly to PC1 as this time, the destination address is found at the ARP table. The PC1 receives the reply and returns a reply itself. The packet's source is set to the MAC address and IP address for PC1 and the packet destination MAC and IP address is set as the address for PC0. The reply is forwarded directly to PC0.



Simulation Panel

Event List

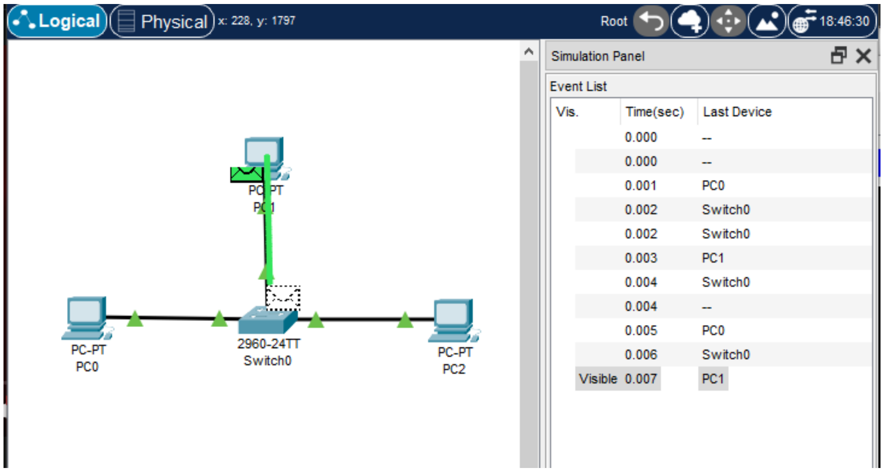
Vis.	Time(sec)	Last Device
	0.000	--
	0.000	--
	0.001	PC0
	0.002	Switch0
	0.002	Switch0
	0.003	PC1
	0.004	Switch0
	0.004	--
Visible	0.005	PC0



Simulation Panel

Event List

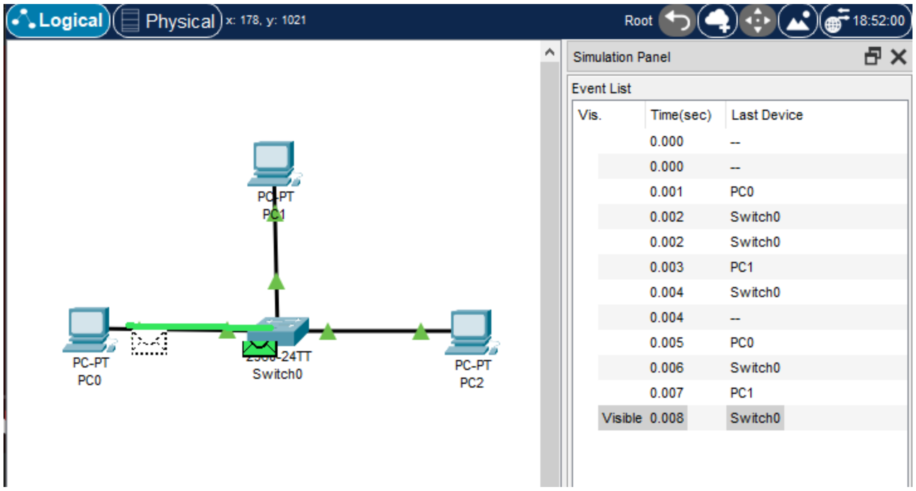
Vis.	Time(sec)	Last Device
	0.000	--
	0.000	--
	0.001	PC0
	0.002	Switch0
	0.002	Switch0
	0.003	PC1
	0.004	Switch0
	0.004	--
	0.005	PC0
Visible	0.006	Switch0



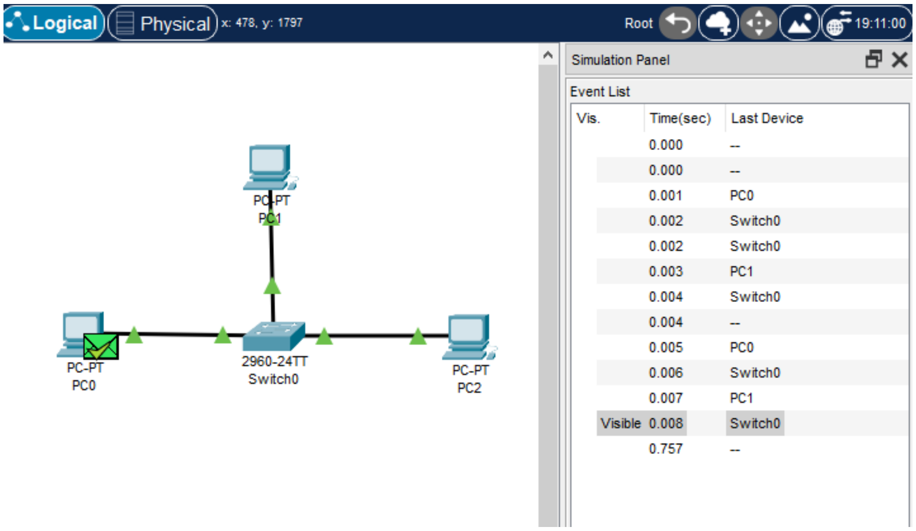
Simulation Panel

Event List

Vis.	Time(sec)	Last Device
	0.000	--
	0.000	--
	0.001	PC0
	0.002	Switch0
	0.002	Switch0
	0.003	PC1
	0.004	Switch0
	0.004	--
	0.005	PC0
	0.006	Switch0
Visible	0.007	PC1

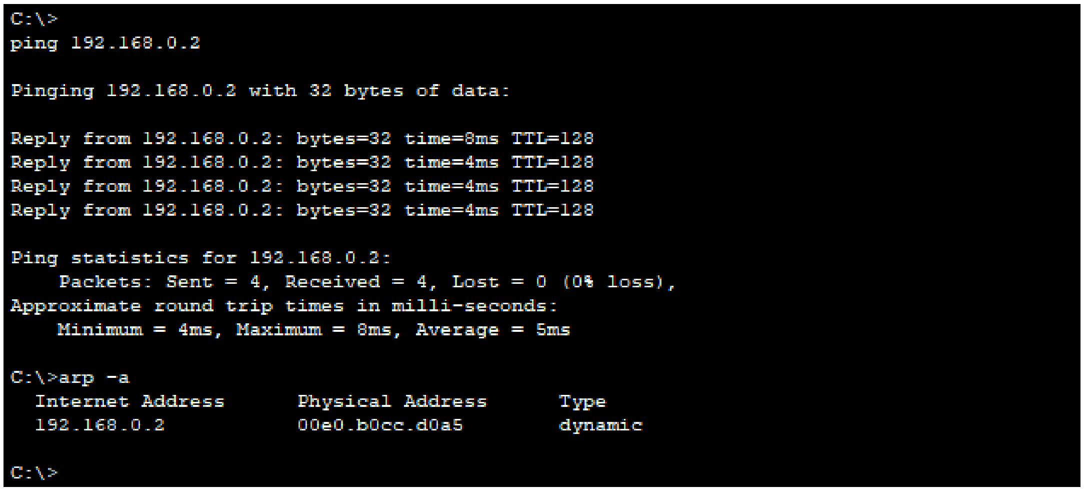


Vis.	Time(sec)	Last Device
	0.000	--
	0.000	--
	0.001	PC0
	0.002	Switch0
	0.002	Switch0
	0.003	PC1
	0.004	Switch0
	0.004	--
	0.005	PC0
	0.006	Switch0
	0.007	PC1
Visible	0.008	Switch0



Vis.	Time(sec)	Last Device
	0.000	--
	0.000	--
	0.001	PC0
	0.002	Switch0
	0.002	Switch0
	0.003	PC1
	0.004	Switch0
	0.004	--
	0.005	PC0
	0.006	Switch0
	0.007	PC1
Visible	0.008	Switch0
	0.757	--

9. PC0 receives the reply. This way, 3 more similar packets are sent. After the packets are sent, we use the “arp -a” again. This time around, we can see that the ARP table has been populated with the Physical address and IP address of PC1.



```
C:\>
ping 192.168.0.2

Pinging 192.168.0.2 with 32 bytes of data:

Reply from 192.168.0.2: bytes=32 time=8ms TTL=128
Reply from 192.168.0.2: bytes=32 time=4ms TTL=128
Reply from 192.168.0.2: bytes=32 time=4ms TTL=128
Reply from 192.168.0.2: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 8ms, Average = 5ms

C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.0.2           00e0.b0cc.d0a5        dynamic

C:\>
```

Challenges:

- The main challenge I faced during this lab was understanding how the ARP table was being populated.
- Understanding which packet was an ICMP packet and which was ARP packet was a bit difficult as during my experimentation, the setting which showed the type of packet was hidden. During a follow-on experiment, my assumptions were seen to be correct.

Answer the Following Questions

1. What is flat addressing and hierarchical addressing? Why is IPv4 address a hierarchical addressing?

Flat addressing is the type of addressing which doesn't contain any layers. It points to a specific host connected to the network. It can support a huge number of hosts. This type of addressing doesn't change with the change of the environment and doesn't indicate the location. An example for flat addressing would be MAC address. The MAC address for a device remains the same despite the device's location.

Hierarchal addressing the type of addressing which contains layers. An example for Hierarchal addressing would be IP address. IP address can be divided into two layers. The Network ID and the Host ID. For example, if the subnet mask is 255.255.255.0, then for IP address 192.168.0.1, the Network ID would be 192.168.0.X and the Host ID portion would be XXX.XXX.X.1.

2. What are the ranges of IP addresses in class A, B, C?

Class	Ranges
A	0-127(128)
B	128-191(64)
C	192-223(32)

3. What is a subnet mask? How to determine the network address and broadcast address of a network from an IP address and subnet mask? What are the default subnet mask of a class A, B, C network?

Subnet mask is a 32 bit number which can be used to determine which section of the IP address is the Host ID and which is the Network ID.

Using the subnet mask and the IP address, we can determine the Network ID and Host ID by operating bitwise **AND** operation.

IP address	192.168.0.1	11000000.10101000.00000000.00000001
Subnet Mask	255.255.255.0	11111111.11111111.11111111.00000000
Network ID	192.168.0.0	11000000.10101000.00000000.00000000

To determine the broadcast address, the 1s compliment of the subnet mask is determined. This means, the 1s are replaced with 0s and the 0s are replaced with 1s. Bitwise **OR** operation of the IP address and the inverse subnet mask would result in the broadcast Address.

IP address	192.168.0.1	11000000.10101000.00000000.00000001
Inverse Subnet Mask	255.255.255.0	00000000.00000000.00000000.11111111
Broadcast Address	192.168.0.255	11000000.10101000.00000000.11111111

Default Subnet Masks

Class	Subnet Masks
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0