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	**: Mashrur Ahsan**
Student ID	**: 200042115**
Section	**: 1 (SWE)**
Semester	**: Winter (4th)**
Academic Year	**: 2021-22**
Date of Submission	**: 31/01/2023**
Lab No	**: 4**

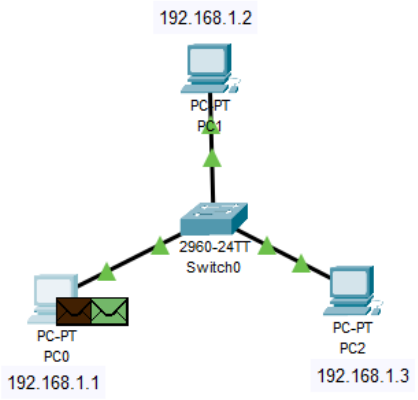
Title: Observation of ARP events and lecture on Logical Addressing.

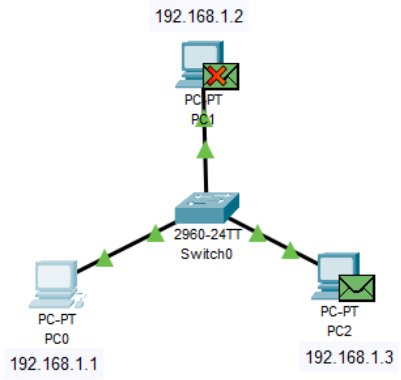
Objective:

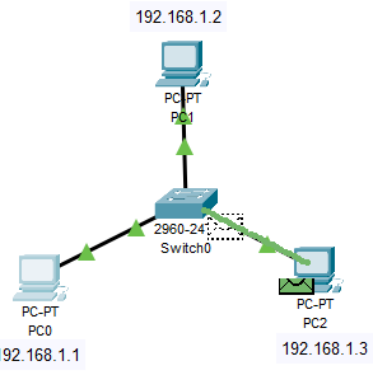
1. Understand how the physical address of a node in the same network is found when the source only knows the logical address.
2. Understand the necessity of hierarchical addressing compared to flat addressing.
3. Understand classful addressing of IPv4 Addressing.
4. Understand the subnet mask.

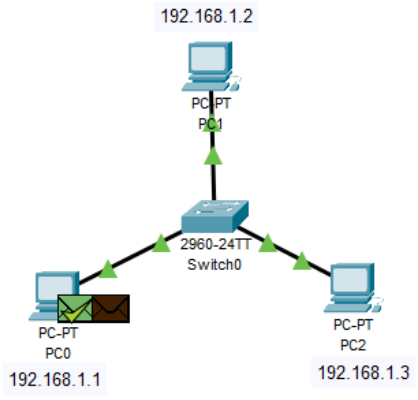
ARP: The Address Resolution protocol (ARP) is a communication protocol used for obtaining the data link layer address (physical address), which is also known as MAC address, with the help of the logical address (IP address). Basically, this protocol is used to get the hardware address (MAC) of a device from an IP address. It's used when a device wants to communicate with some other device on a local network.

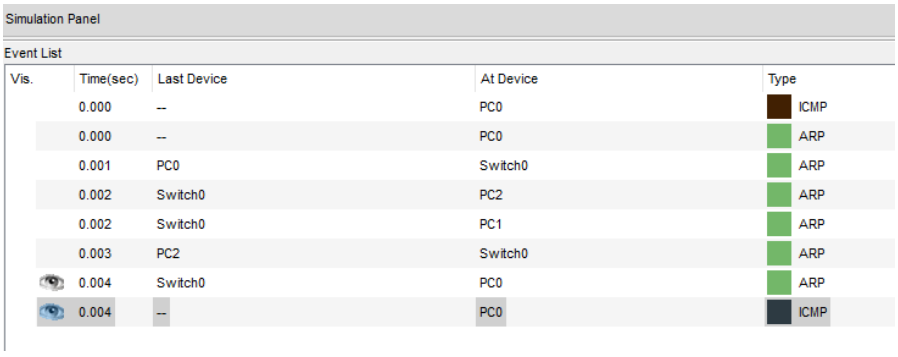
Diagram of the experiment:



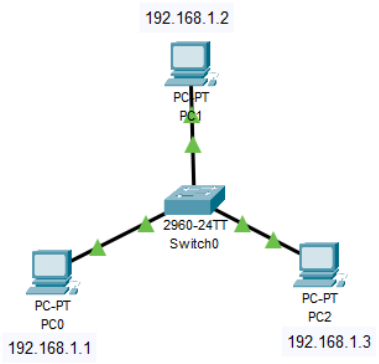








Experiment Set Up Description:



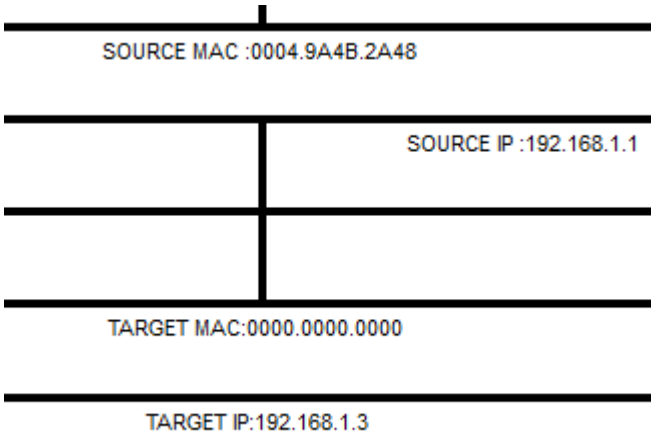
- At first, set up a connection that looks like this:
- Configure the IP addresses as labeled.
- Click on one of the PCs and to the command prompt.
- If we write the command "**arp -a**". It will show that there's no ARP entries.
  "arp -a" command helps to check the ARP table, whether there's any entries or not.

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

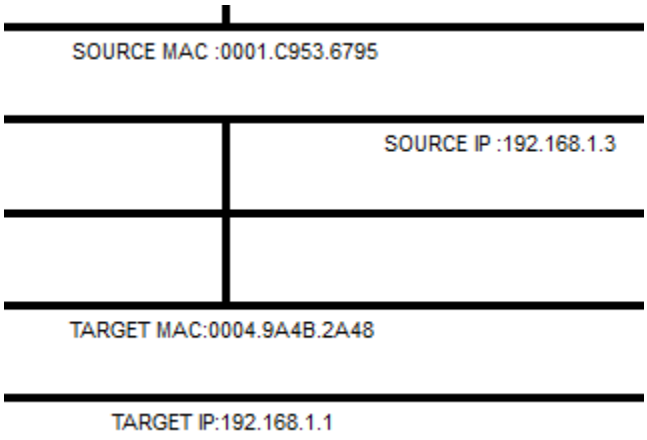
- Now, we have to send a ping request to one of the PCs in the network. Then we have to press ctrl+c.

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:


Ping statistics for 192.168.1.3:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Control-C
^C
C:\>
```

- Now, we have to go to the simulation window and press the Forward button and observe the flow of packet.
- When the packet reaches the switch from the source PC, if we look at the details on the Inbound PDU, then we'll see that we don't know the MAC address of the destination PC yet.



- We need to keep forwarding the simulation. When the packet comes back to the switch from the pinged PC (in this case: 192.168.1.3), we'll see that the Inbound PDU details will have the initial target MAC address.



- Now, if we type "arp -a" in the command prompt, it will the ARP entry that we just did.

```
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.3           0001.c953.6795        dynamic
```

- If we want to clear the ARP cache stored in the ARP table, we can write "**arp -d**" in the command prompt.

And this is how we can find out the MAC address of a PC connected to a local network while only knowing the IP address of it.

Observation:

If the ARP has the IP address of the destination device but doesn't have the MAC address of it. It will send the ARP request packets to the broadcast addresses. For example, let's say device A wants to send a message to device B. But A only knows the IP address of B, not the MAC address. Then A will send an ARP request to B since it knows the IP address of it. B will acknowledge the request and will send it back to A. Now, A will get the MAC address of B and can now send any messages it wants to send.
In conclusion, ARP is the protocol that is used to find the MAC address of the devices whose IP address in known. The ARP commands help us to check or delete the entries available at the end devices.

Challenges:

- Didn't know that we had to press "ctrl+c" after sending the ping request to another PC while being in the simulation window.

Answer the Following Questions

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

Answer: Internetwork address space typically takes one of two forms: hierarchical address space or flat address space. **Hierarchical addressing** organizes the addresses into numerous subgroups or hierarchy. Where higher levels of the hierarchy represent larger groups of devices and lower levels represent individual devices. This type of addressing allows us to manage a large number of addresses with much ease. It also helps us to have an efficient data routing process.
On the other hand, in **flat addressing**, all devices on a network are assigned a unique address, without any hierarchical structure. This enables us to have easy access to devices but it can make managing a large number of addresses much more difficult.

IPv4 addresses can be divided into two parts: the network address and the host address. The first two octets of the address identify the network that the device is connected to. The last two octets identify a specific device within the network.
This scheme allows for more efficient routing of data, as routers can make decisions based on the network portion of the address without having to examine the host portion.
Since the IPv4 addresses are separated into multiple subparts, we can say that IPv4 address follows hierarchical addressing.

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

Answer: Currently there are three classes of TCP/IP networks. Each class uses the 32-bit IP address space differently, providing more or fewer bits for the network part of the address. These classes are class A, class B, and class C.
The values assigned to the first byte of **class A** network numbers fall within the range **0-127**. So Only 127 class A networks can exist.
A class B network number uses 16 bits for the network number and 16 bits for host numbers. The first byte of a **class B** network number is in the range **128-191.**
Class C network numbers use 24 bits for the network number and 8 bits for host numbers. The first byte of a **class C** network number covers the range **192-223**.

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.

Answer: Subnetting is the practice of dividing a network into two or smaller networks. A subnet mask is a 32 bits address that identifies which part of an IP address is the network address and the host address.

To find out the network address and the broadcast address of a network an IP address and subnet mask, we need to follow the following steps:

- Write the IP and the subnet mask in binary form.
- Network address: Perform logical AND operation between the corresponding octets of the IP and the subnet mask. Then convert it to decimal form.
- Broadcast address: Perform logical OR operation between the corresponding octets of the IP and the inverse of the subnet mask. Then convert it to decimal form.

An example:

IP address in decimal notation	192	168	5	50
Binary Equivalent of IP address	11000000	10101000	00000101	00110010
Subnet Mask	11111111	11111111	11111111	11110000
Result of Anding	11000000	10101000	00000101	00110000
Network Address	192	168	5	48

IP address in decimal notation	192	168	5	50
Binary Equivalent of IP address	11000000	10101000	00000101	00110010
Inverse of Subnet Mask	00000000	00000000	00000000	00001111
Result of ORing	11000000	10101000	00000101	00111111
Broadcast Address	192	168	5	63

Class A addresses have a default mask of 255.0.0.0
Class B addresses have a default mask of 255.255.0.0
Class C addresses have a default mask of 255.255.255.0