VANIER COLLEGE – Computer Engineering Technology Winter 2021

Network Fundamentals (247-409-VA)

Leonardo Fusser (1946995)

LABORATORY EXPERIMENT 4

Packet Tracer

NOTE:
To be completed in one lab session of 3 hrs.
To be submitted: Formal lab report, one week later – **at the start** of your respective lab session. This exercise is to be done individually except where specified in the procedure. **Each** student must submit a lab report with original observations and conclusions.

OBJECTIVES:

After performing this experiment, the student will be able to:

1. Develop an understanding of the basic functions of Packet Tracer (PT).
2. Recognize and locate key network components in PT interface.
3. Correctly identify cables for use in network.
4. Create/model a simple network topology.
5. Observe traffic behavior on the network.

PROCEDURE

1. Use the packet tracer file you created in LAB 1. Keep only the basic setup:
    a. 2 generic PCs
    b. 1 generic hub
    c. Click PC0. Select the **Config** tab. Change the PC **Display Name** to PC-A.
    d. Select the **FastEthernet** tab on the left and add the IP address of **192.168.1.1** and subnet mask of **255.255.255.0**. Close the PC-A configuration window.
    e. Click PC1. Repeat similar procedures as in (a) to change the PC Display Name to **PC-B**, IP address of **192.168.1.2** and subnet mask of **255.255.255.0**.

2. Observe the flow of data from PC-A to PC-B by creating network traffic
    a. Switch to **Simulation** mode by selecting the tab that is partially hidden behind the **Realtime** tab in the bottom right-hand corner. The tab has the icon of a stopwatch on it.
    b. Click the **Edit Filters** button in the **Edit List Filters** area. Clicking the **Edit Filters** button will create a pop-up window. In the pop-up window, click the **Show All/None** box to deselect every filter. Select just the **ARP** and **ICMP** filters.
    c. Select a **Simple PDU** by clicking the closed envelope on the right vertical toolbar. Move your cursor to the display area of your screen. Click **PC-A** to establish the source. Move your cursor to **PC-B** and click to establish the destination.

Perform some search and study, and briefly explain what is the purpose of ICMP and ARP protocols.

ICMP: The Internet Control Message Protocol (ICMP) is a supporting protocol in the Internet protocol suite. It is used by network devices, including routers, to send error messages and operational information indicating success or failure when communicating with another IP address, for example, an error is indicated when a requested service is not available or that a host or router could not be reached.

https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol

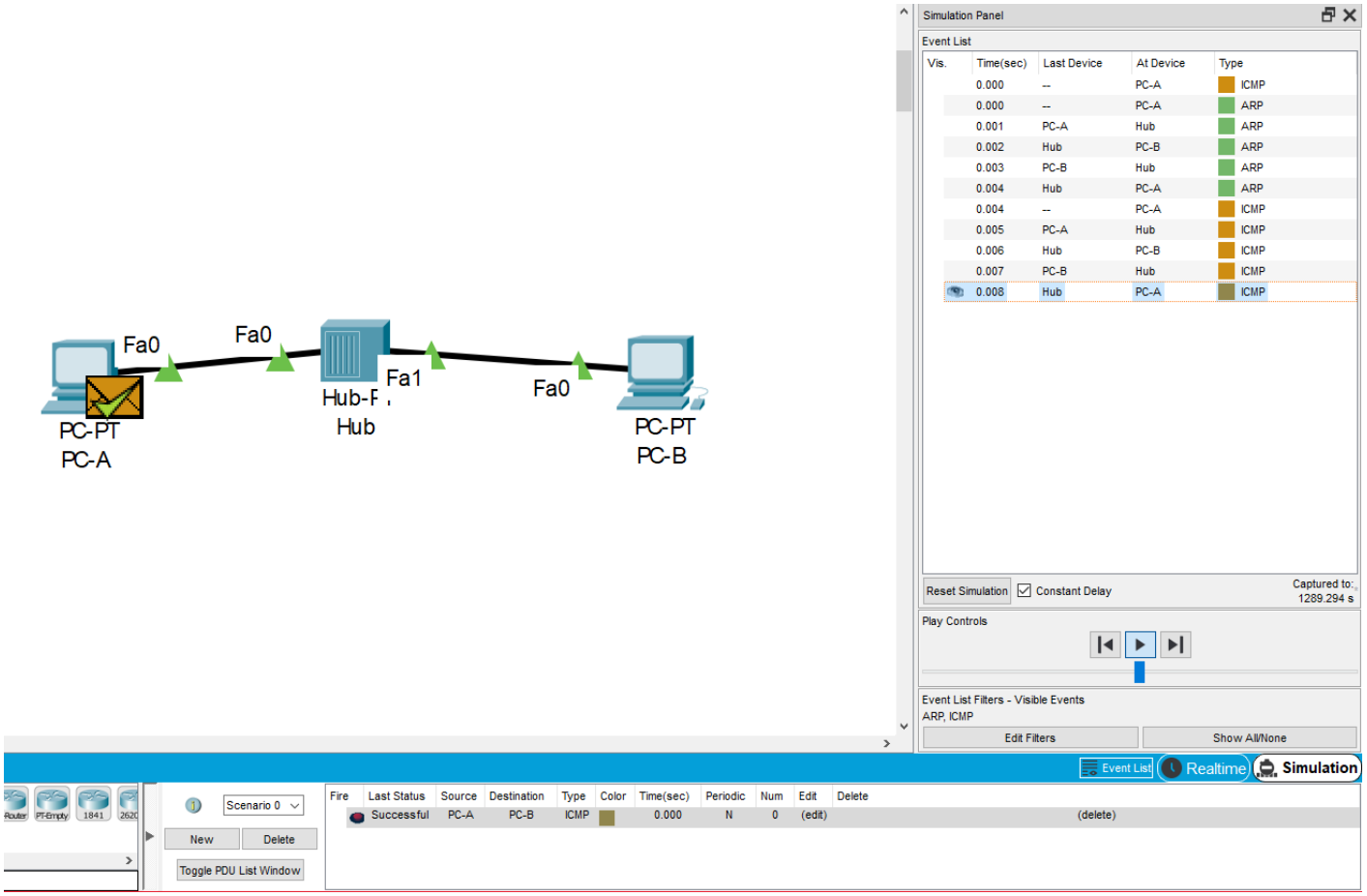
ARP: The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address. This mapping is a critical function in the Internet protocol suite.

https://en.wikipedia.org/wiki/Address_Resolution_Protocol

***Notice that two envelopes are now positioned beside PC-A. One envelope is ICMP, while the other is ARP. The Event List in the Simulation Panel will identify exactly which envelope represents ICMP and which represents ARP*.

d. Select **Auto Capture / Play** from the **Play Controls** area of the Simulation Panel. Below the **Auto Capture / Play** button is a horizontal bar, with a vertical button that controls the speed of the simulation. Dragging the button to the right will speed up the simulation, while dragging is to the left will slow down the simulation.

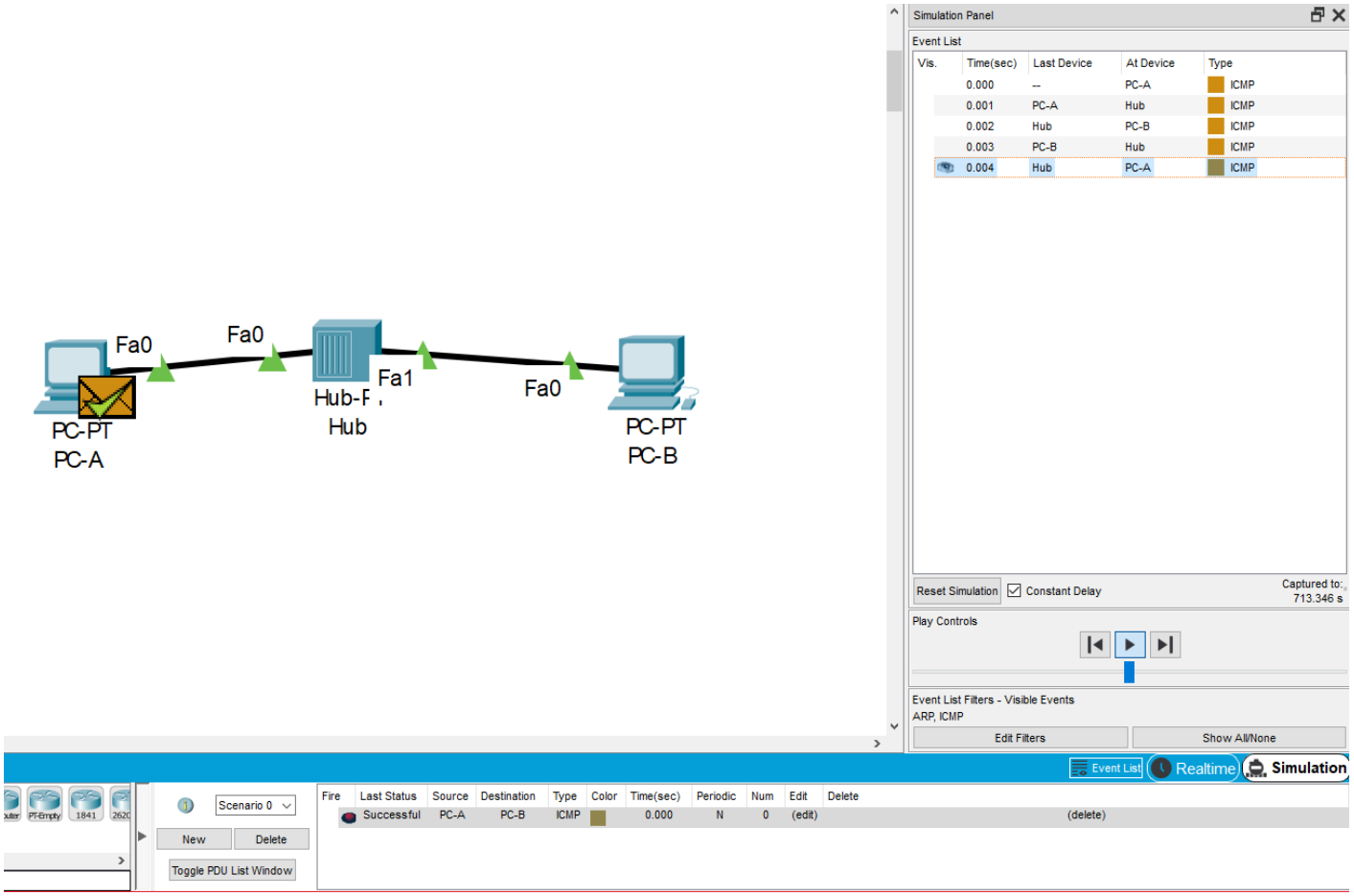
e. The animation will run until a small tick sign appear to indicate the end of successful messaging.



Simple network with two computers shown above. Result from animation shown above.

f. Choose the **Reset Simulation** button in the Simulation Panel. Notice that the ARP envelope is no longer present. This has reset the simulation but has not cleared any configuration changes or dynamic table entries, such as ARP table entries.

g. Choose the **Capture / Forward** button. The ICMP envelope will move from the source to the hub and stop. The **Capture / Forward** button allows you to run the simulation one step at a time. Continue selecting the **Capture / Forward** button until you complete the event.



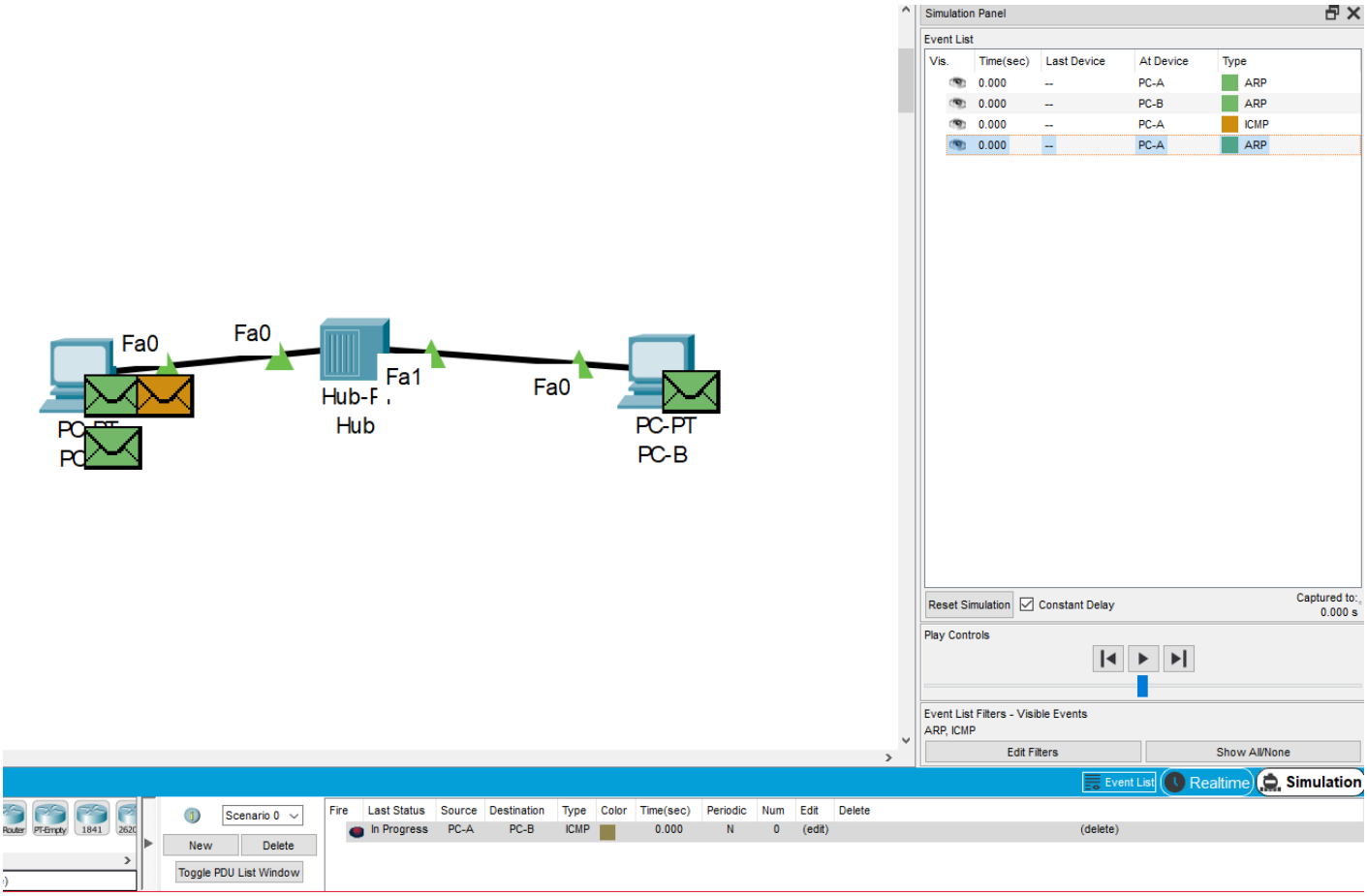
Same network shown from before. Simulation has been reset and ARP is not shown during this animation.

h. Why is ARP request not performed in this step?

The ARP table entries haven't been cleared so an ARP request is not needed (the IPv4 address is still mapped to the MAC address of the destination PC). When an ICMP request (ping request) is sent out for the second time (after resetting the animation), it knows where to go exactly to get a response (it knows exactly where the destination PC is). When the ARP table is cleared, an ARP request will be performed (see next screenshot).

i. Choose **the Power Cycle Devices** button on the bottom left, above the device icons.

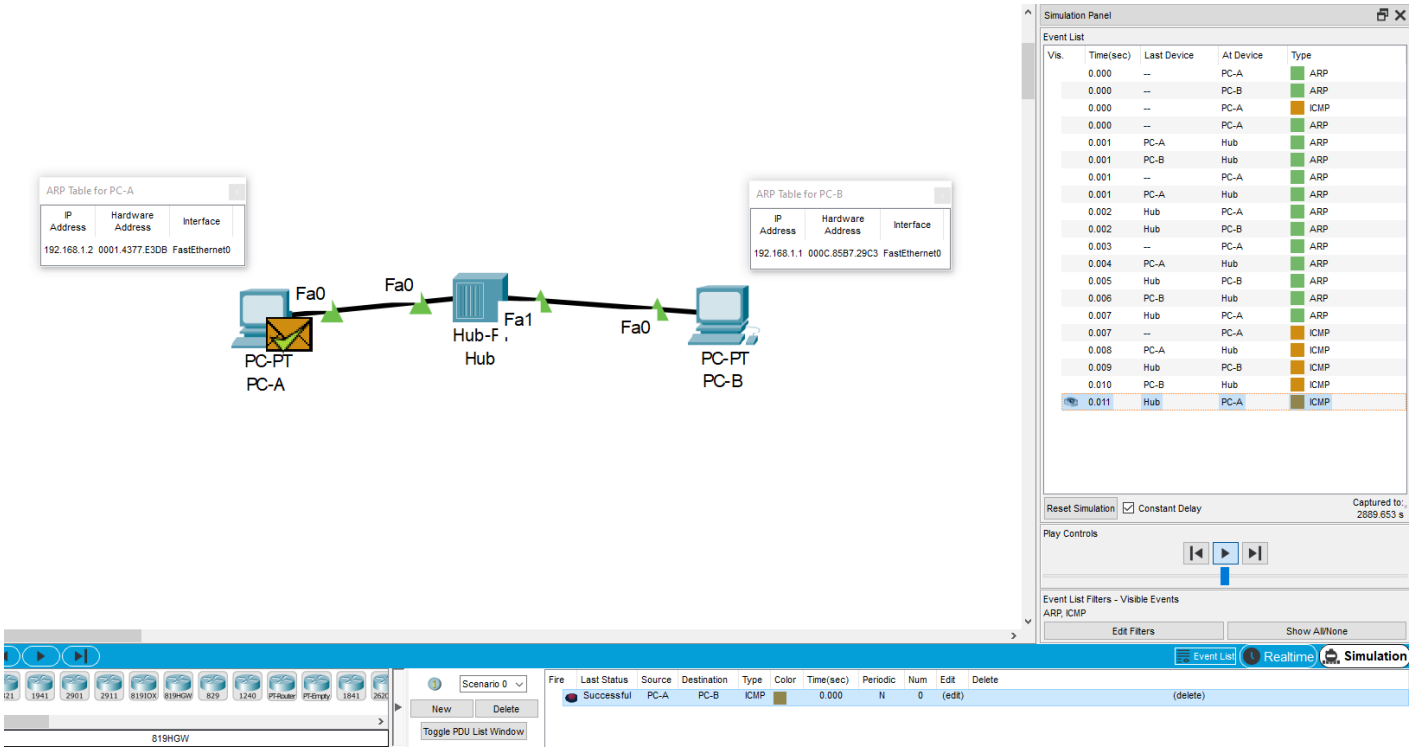
j. An error message will appear asking you to confirm reset. Choose Yes. Now both the ICMP and ARP envelops are present again. The Reset Network button will clear any configuration changes not saved and will clear all dynamic table entries, such as the ARP and MAC table entries.



Same network as before. Devices power-cycled causing ARP table to be cleared (it is volatile). An ARP request is performed again as shown above (the green envelope).

3. View ARP Tables on each PC
   a. Choose the **Auto Capture / Play** button to repopulate the ARP table on the PCs.
   b. Select the magnifying glass on the right vertical tool bar.

c. Click **PC-A** and select **ARP table**. What can you have observed from the ARP table? View the ARP tables for PC-B and record your observation.



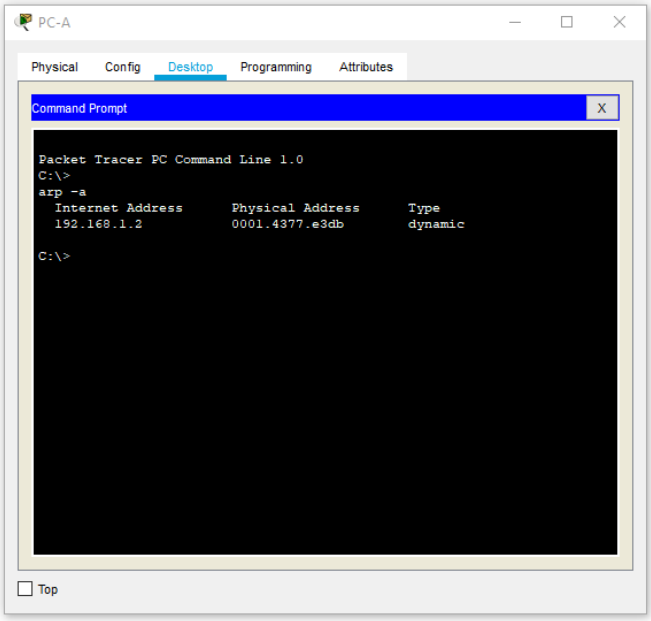
Same network as before. ARP tables from both computers shown above. Each computer has mappings for one another (PC-A has mappings for PC-B and PC-B has mappings for PC-A). Each one has their IP address associated with their respective MAC addresses (PC-A IPv4 address matched to PC-A MAC address and PC-B IPv4 address matched to PC-B MAC address).

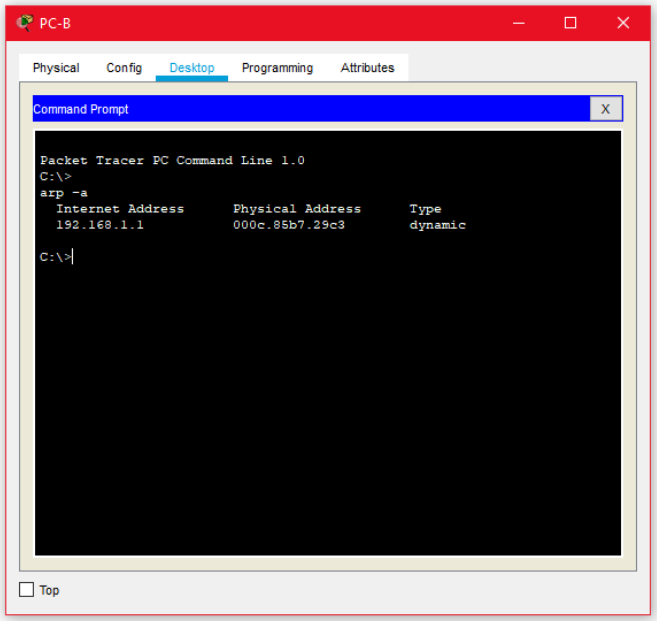
d. Click the **Select Tool** on the right vertical tool bar.

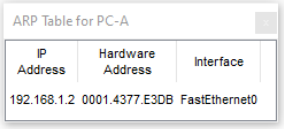
e. Click **PC-A** and select the **Desktop** tab.

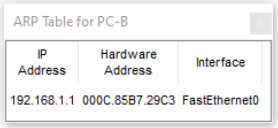
f. Select the **Command Prompt** and type the command arp -a and press enter to view the ARP table from the desktop view. Record your result and explain your observation.

g. Examine the ARP table for **PC-B**.









ARP tables from both PCs shown above. Since the network hasn't been reset or power-cycled, ARP table entries are still intact (same as previous screenshot). Only difference is instead of using inspect tool in PT, ARP tables are being shown using PT command prompt (on PC desktop) from using arp -a command.