Lab 3: Capture/Analyse Local Communication Process

# Things that you will need to know or learn:

* Identify and understand the different layers of addressing necessary to a successful communication.
* Understand the local communication process.
* The general purpose and format of an ARP message.
* Understand the information provided in the Wireshark Details Pane for the purpose of extracting addressing information as well as being able to map protocols to their OSI or TCP/IP network model layers.
* Connecting to a web server via a non-default application port. (PT)
* Determining your network adapter’s MAC address.

# What you need to submit and when:

* Complete the in-lab part of the lab and submit the results on BrightSpace before the due time.
* Complete the “Lab 3 Post-lab” quiz before the due time

# Required Equipment/Software:

* Previous PT Lab 2
* Wireshark and PT installed and working (done in Lab 01)
* Lab documents downloaded to your laptop

# References and Resources:

• Lab 02 resources

• Section chapter 3 (except cisco equipment configuration) and Chapter 3

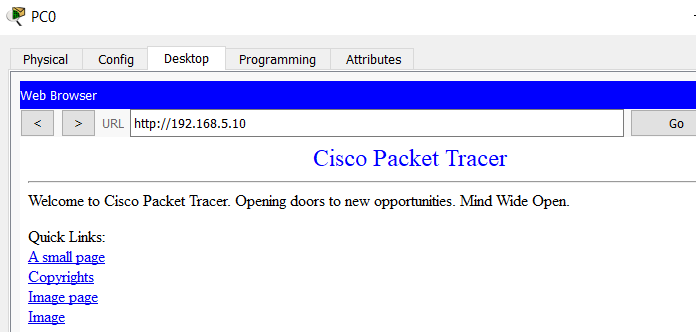
# Task 1: Communication with a Web server in the local network (HTTP protocol) (2 mark)

1. Open the previous PT (Packet Tracer- **Lab 2**).

Make sure **PC0** can ping **server0,** with the right IP address, otherwise this part will not work

When you open the PT, by default, you are in **Realtime** mode.

1. Now click on **PC0** and **Desktop** and then **Web Browser** tab
2. In the URL box type <http://192.168.5.10> (web server IP address), click **Go**



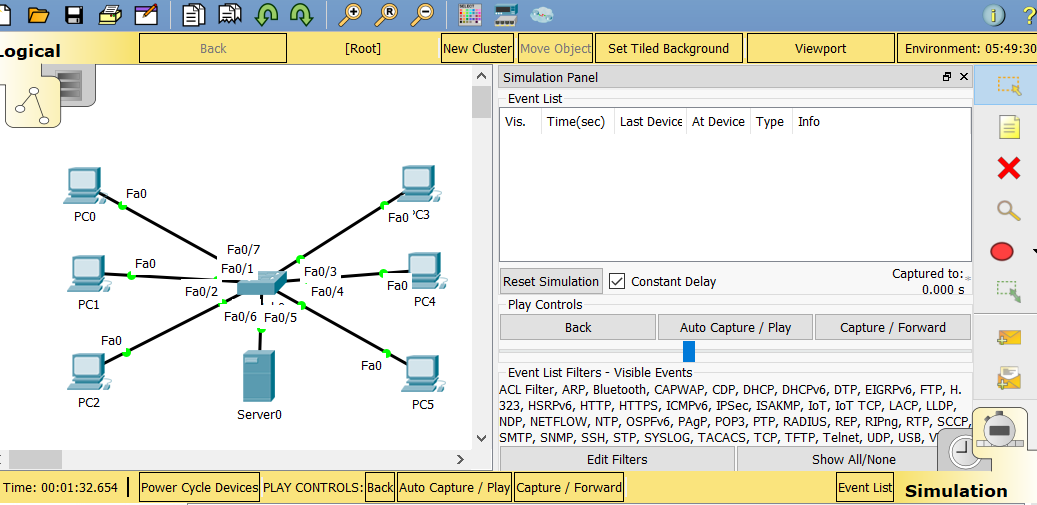
You see an **HTTP** web page opens from the **server0** (blue).

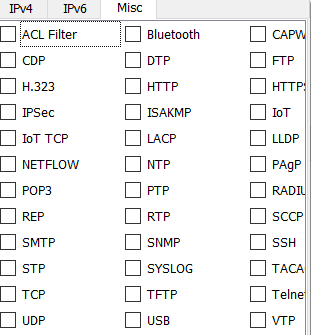
You are connected to a Web server and requested a

web page (Welcome Cisco Packet racer).

1. Minimize the **PC0** screen for now.
2. In PT, change **Realtime** mode to **Simulation** mode, by clicking on the **simulation** icon



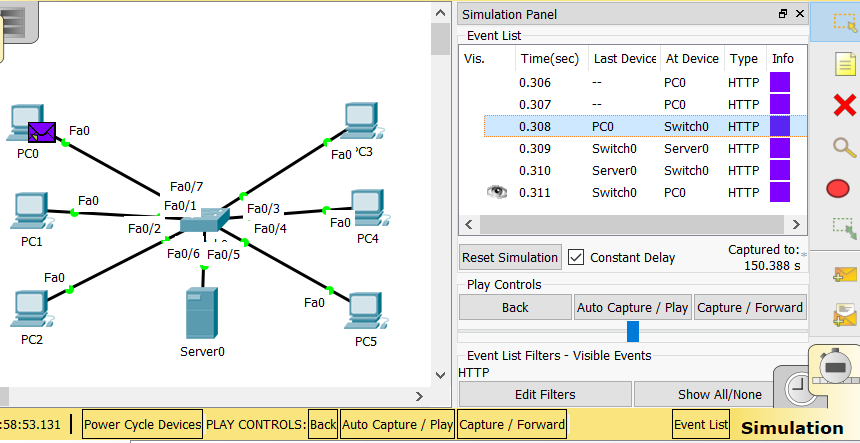




1. In **simulation** mode click on **Edit Filters** and then on the **Misc** tab
2. You will see many protocols with check marks. Make sure they are **unchecked** except **HTTP**.
3. Still in simulation mode, open **PC0** page again (web browser page), click on **Go** to capture the **HTTP** packets

in simulation mode. Make sure to click on the **Capture/Forward** tab to capture

the PDU. To stop capturing PDU, just click on **Capture/Forward** again.



1. Now click on **PC0, Switch 0 PDU** to see inside a packet

**Questions:**

Which layer of OSI model show the MAC address?

**Data link**

What is the Ethernet Header?

**It’s the ethernet frame.**

What protocol did you capture?

**HTTP**

This protocol used by which layer of the OSI model?

**Application**

What is the SRC (PC0) and DES IP (Server0) address?

**SRC – 192.168.5.6**

**DES –192.168.5.10**

What is the destination port?

**192.168.5.10**

Save to a file named: **lab3\_PT\_task1.pkt**

# Task 2: Accessing Local Resources (your laptop) (2 mark)

In this task, you will capture the network traffic between a web client and a web server, each running on the same network segment.

***Do not proceed*** until all previous tasks have succeeded!

1. On your laptop, start the **WS**. Make sure you capture traffic on the **correct interface**! Refer back to lab 2 if you are not sure or do not remember how to do this!

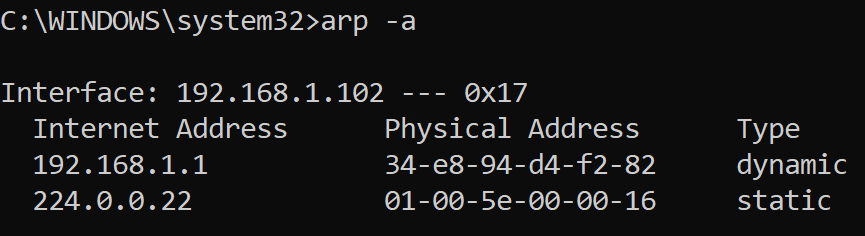
To ensure you are capturing on the correct interface, ping the default gateway and verify the frames are being captured in Wireshark.

1. Delete the ARP cache.

On your laptop, **run CMD as Administrator**.

From the Command Prompt, enter the following command: **arp –a**

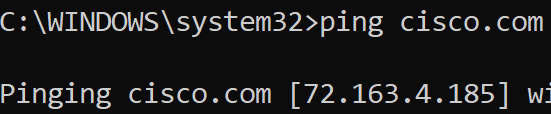
If there are some **arp** cache in the memory, then you have to delete them.



To delete the **Arp cache** in the Windows CMD prompt, just type **arp -d \***

You must make sure that no errors resulted from the execution of the command!

1. In the CMD prompt screen, type ***ping cisco.com*** and press **enter**. The DNS on the Cisco server would resolve the URL **cisco.com** to an IP address. (72.163.4.185)

Now you have an IP address for **Cisco** server.

1. Open a web browser in your laptop.
2. Enter the following URL in the browser’s address bar: http://*a.b.c.d*

replace a.b.c.d with the **web server’s** IP address (72.163.4.185).

**Do not proceed** to the next step until the web page successfully displays in the web browser.

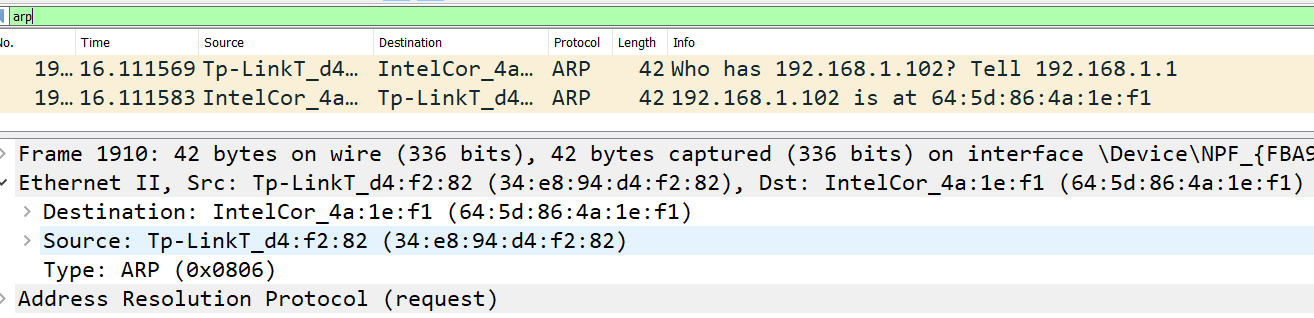
1. Stop the Wireshark. **Save** the captures to a file named: **lab3\_WS\_task2.pcapng**

# Task 3: Validate Wireshark Capture (2 mark)

In this task, you will ensure that task 2 capture contains all the required frames.

1. Filter by **arp** and look for a captured frame having the following in the info column:

ARP (Address Resolution Protocol)



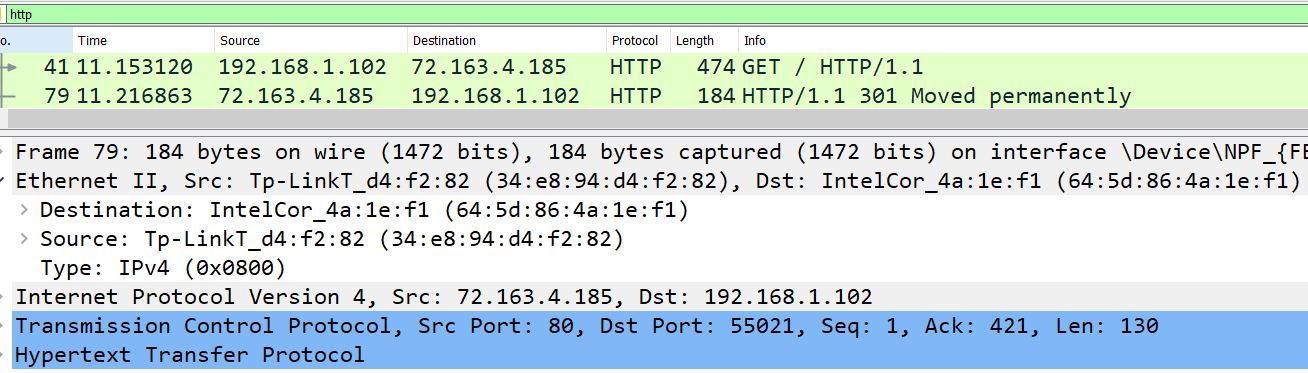
Who has **192.168.0.1**? Tell **192.168.0.27**

**192.168.0.1** is the ***default gateway’s IP address***

**192.168.0.27** is the ***client’s IP address***

1. Filter by **http** and look for two captured frames having the following characteristics:

HTTP (Hyper Text Transfer Protocol)



**First Frame - Client Request**

GET / HTTP/1.1 in the info column

where **77.234.44.196** in the source column (**client IP)**

**192.168.0.90** in the **destination** column (server IP)

**Second Frame - Server Response**

HTTP/1.1 304 Not modified OR

HTTP/1.1 200 OK in the info column

where **77.234.44.196** in the destination column (client IP)

**192.168.0.90** in the source column (server IP)

Take a screen capture of the filtered packets and save to a file named: **lab3\_ws\_task3**

# Task 4: Local Communication Analysis (4 mark)

In Wireshark, select the frame that encapsulates the client’s **request** and examine the message’s **PDU** details in the **Details** Pane to answer the following questions.

1. What is the layer 7 protocol? **Application**

2. What is the Layer 4 protocol? **Transport**

3. What is the Layer 3 protocol? **Network**

4. What is the Layer 2 protocol? **Data Link**

5. What is the frame’s destination MAC address?

**0BAE061E:7AEC-4E98-96F7-613C224E7F24**

6. This destination’s MAC address belongs to which device? **NPF**

7. What is the destination IP address?

**77.234.44.196**

8. This IP address belongs to which device? **The client or the cisco website I am trying to reach.**

9. What is the destination port? **80**

10.This destination port belongs to which application? **Cisco.com**

# Task 05: Submission

Submit the saved files from the previous tasks and this Word file to the drop box inside the folder “lab 03” on BrightSpace.