

Lab 3: Capture/Analyze 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 **LAN** 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.
- Determining your network adapter's MAC address.

What you need to submit and when:

- Complete the in-lab part of the lab and demo the results to your lab instructor before the end of your lab period (refer to the instructions below).
- This lab is done in pairs, yet **each student must individually complete and submit their own answer sheet.**
- Complete the "Lab 3 Post-Lab" quiz by the due date. This part is to be completed individually.

Required Equipment/Software:

- Network cables and Linksys Router from the instructor
- Wireshark installed and working (done in Lab 1)
- Lab documents and the Webserver application downloaded to your laptop
- Lab is done in pairs, each student requires a laptop that has an Ethernet (RJ45) port (or USB-Ethernet adapter).

References and Resources:

- Lab 2 reference document(s)

Task 0: Preparation

- 0.1 Find a partner to work with.
- 0.2 Confirm you have downloaded the following from BB “Labs - > Lab 03” to your computer:
 - Lab 3 – In-Lab Activities.pdf” (this document)
 - Lab 3 answer sheet.txt
 - Webserver – to install the Web Server
- 0.3 **Disable** the Wireless Network Interface of your Laptop computer.
Your only connection to the network must be via the Ethernet (wired) interface.
- 0.4 **Disable** any other network interface (e.g. Bluetooth, VMNet, etc.)

If you have done this correctly, the output of the command **ipconfig** should only list your Ethernet adapter NIC and no other NIC(s).

- 0.5 Do not start until you have completed ALL steps in this task.

Task 1: Build Network with Linksys Router

In this task you will build and test a network which consists of three physical devices: your laptop, your partner's laptop and a Linksys router. Do not start task 1 until you have completed all Task 0 steps.

You are working in teams of two, yet each students must individually complete and submit their own work.

- 1.1 **Team:** Obtain one Linksys router - one per team, power adapter and the required cables
- 1.2 **Team:** Power on your Linksys router and wait until the router's green power indicator led is on steadily before proceeding to the next step.
- 1.3 **Team:** Reset the router back to factory defaults.
- 1.4 Ensure your Laptop's Ethernet network adapter is configured to obtain the IPv4 address automatically.
- 1.5 Using the correct cable connect your laptop's Ethernet network adapter to any of your Linksys router's switch's Ethernet ports. Your laptop will attempt to obtain an IPv4 address from your Linksys's DHCP server. Please be patient as this process may take up to 60 seconds.
- 1.6 The green light corresponding to the Linksys's Ethernet port you connected to should be on and occasionally flashing. This is an indication that there is network activity on the particular port.
- 1.7 Open the command prompt and use the correct command to view your laptop's IP configuration. Use the information to complete the IPv4 Information step in your answer sheet.
- 1.8 Complete the Default Gateway step in your answer sheet.
- 1.9 Compare your Default gateway address value you have with your partner's. Are the Default Gateway addresses the same? Why? Answer in your answer sheet.
- 1.10 Ensure that you can successfully ping your network's default gateway address. You should see 4 TTLs (0 packets lost)

Task 2: Install and Test Web Server

In this task you will assign roles to each laptop. You will need one laptop to play the role of **Client** and the other the role of **Server**.

Any laptop that meets the BYOD hardware and software requirements should be able to run the server.

Note for server: If you are running your MS Windows OS inside a Virtual Machine, you will further need to ensure that your VM machines networking is set to "bridge" instead of NAT.

The other laptop will play the role of client. No special software is required on this laptop.

Note: Some of the instructions below are for **Server Only** or **Client Only**.

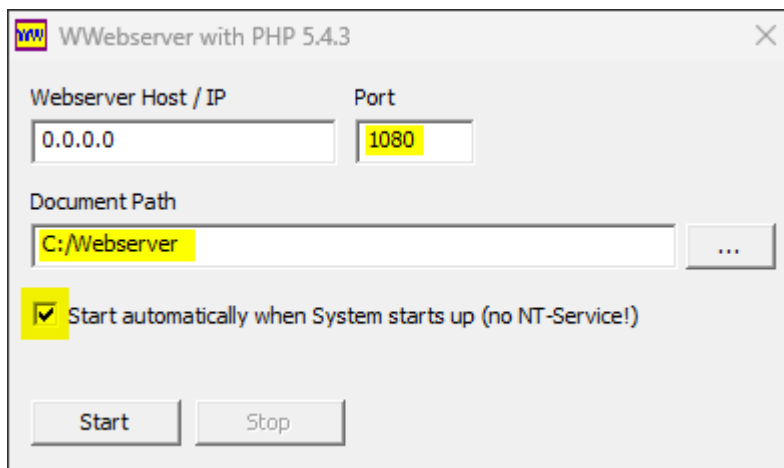
Read all instructions regardless of your role to be able to understand and answer questions about this lab later.

2.1 **Server Only:** install the Webserver software by extracting the zip file.

We recommend to extract it to the **C:** folder. A sub-folder (**C:\wwebserver**) with all the files will be placed in there, you don't need to create another sub-folder for the extracted files.

2.2 **Server Only:** Disable any firewall software.

2.3 **Server Only:** Enter the **wwebserver** folder. Locate and run the **wwebserver.exe** application as administrator. The following window will appear, with some default values.



2.4 **Server Only:** Make the following 3 (highlighted) changes:

- Modify the Port number to **8088**
- Change the **document path** to the folder where **wwebserver.exe** is in (e.g. to **C:\wwebserver**) by typing or by clicking the browse button (...)
- **Uncheck** the box "Start automatically when System starts up"

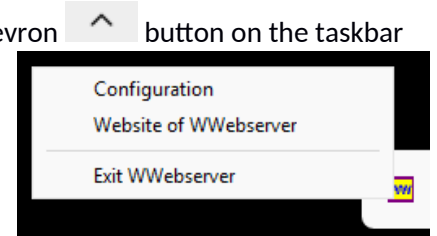
Verify that the 3 items above were correctly modified.

Notes:

- The **0.0.0.0** value in the Webserver Host/IP field has the web server listen to web client requests on all IP addresses assigned to the laptop running the web server software.
- The port **8088** value indicates that the web server is listening for client requests on that port number. The standard port is port 80 for non-secure web communication (HTTP) and port 443 for secure communications (HTTPS).

Click **Start** to start the web server.

IMPORTANT: if you are closing the web server window with the **X** button, it DOES NOT stop the server from running. It only closes the web server window. To find the web server window, click the chevron button on the taskbar and right click on the web server's application icon if you need to re-configure or exit. Sometimes stopping the web server doesn't work. If you made a mistake in the configuration, you may need to exit using the context menu and start it over.



2.5 Server Only:

Start the web browser and use private/incognito browsing (we want to prevent caching).

Type in the following in the web browser's address bar:

http://a.b.c.d:port

but replace **a.b.c.d** and **port** with your IP address and the port number used by the web server.

A web page that displays the client and server IP address values should appear. This is an indication that your web server is working.

Think: Are the shown IP addresses the same? Why?

2.6 Client Only:

Start the web browser in private/incognito browsing (we want to prevent caching).

Type in the following in the web browser's address bar:

http://a.b.c.d:port

but replace **a.b.c.d** and **port** with your the IP address of your partner (server) address and use a port number of **8088**.

A web page that displays the client and server IP addresses values should appear. This is an indication that your web server is working.

2.7 **DO NOT proceed** until the web pages successfully displays on both the client and server laptops:

If 2.5 succeeded but 2.6 failed, then verify the URL used at the client, and that the firewall on the web server laptop has been disabled (Note that ideally a firewall rule would be added to allow connections to the web server application. For now we just temporarily disable the firewall on the server)

Note that if the server is running Windows in a VM: be sure it uses Bridging instead of NAT.

Task 3: Accessing Local Resources

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!

- 3.1 On both laptops, start a Wireshark capture. Make sure you capture traffic on the correct (Ethernet) interface (Check the interface's IP address on Wireshark and see lab 2 reference documents for more information)
- 3.2 **Client Only:** close all the tabs of the web browser.
- 3.3 On both laptops, **start the command prompt as Administrator**.

We will now delete the ARP cache. Enter the following command:

```
arp -d *
```

This command will be important for later coursework, quizzes, and tests. Take note of it in your course notebook. Note the spaces, they are important!

Make sure that no errors resulted from the execution of the command. If you get an error about requiring elevation, start over this step and read the instructions carefully.

Note: some Windows versions do not recognize the command above and require you to instead use: **netsh interface IP delete arpcache**

- 3.4 **Client Only:**

Make sure you followed step 3.2!

Start the web browser in private/incognito browsing. Connect to the web server using the address: **http://a.b.c.d:port** but replace the IP address with the partner's IP address use port number 8088. The same page with the client and server IP should show.

- 3.5 **Both Client and Server:**

Stop the capture on Wireshark and save the capture. You will need to verify it in the next task.

Task 4: Validate the Wireshark Capture

In this task you will ensure that the task 3 capture contains all required frames, by using the Wireshark filter feature with two protocol filters: **arp** and **http**. Note that the protocol names are in lowercase.

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

Who has a.b.c.d? Tell w.x.y.z

in the info column where:

a.b.c.d is the web server's IP address

w.x.y.z is the client's IP address

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

First Frame (The client's request) has the following in the info column:

GET / HTTP/1.1

and the other fields for that frame are:

The "source" column has the client's IP

The "destination" column has the server's IP

Second Frame (The server's response) has the following in the info column:

HTTP/1.1 200 OK OR

HTTP/1.1 304 Not modified

and the other fields for that frame are:

The "source" column has the server's IP

The "destination" column has the client's IP

4.3 You must repeat task 3 if any of the results do not meet the requirements.

4.4 Show your lab instructor the frames.

- Once your capture was verified, continues the rest of the lab individually using your saved capture.
- Carefully pack and return the router, router power supply and any cables.

Task 5: Local Communication Analysis

5.1 In Wireshark, select the frame that encapsulates **the client's request** (identified in 4.2) and examine the message's PDU details in the Details Pane.

Answer the questions in your answer sheet.

Refer to slide 31 of Module 3 (week 2's lecture) as needed.

- A) What is the layer 7 protocol?
- B) What is the Layer 4 protocol?
- C) What is the Layer 3 protocol?
- D) What is the Layer 2 protocol?
- E) What is the frame's destination MAC address?
 - E.I) This destination's MAC address belongs to which device?
- F) What is the destination IP address?
 - F.I) This IP address belongs to which device?
- G) What is the destination port?
 - G.I) This destination port belongs to which application?

Task 6: Challenge Question

In this lab the client and the server were on the same network segment.

Assume that the client and web server are connected to different network segments.

Assume that the web server IP is: 192.168.0.50 and its MAC is: 00:50:03:00:33:00

What would be the layer 2 destination MAC address, the layer 3 IP address and the layer 4 destination port of the message as it leaves the client laptop? Use the knowledge you learned in class to answer.

- Submit the file **Lab3-answer-sheet.txt** after filling the required answers, by the deadline.
- Once you have understanding of the lab process and the answer above, complete the post-lab 3 quiz by the deadline.

Task 7: Cleanup and Other Tasks

- 7.1 Re-enable your firewall
- 7.2 Re-enable your Wireless Network and confirm you are able to access the College network.