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.
- 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 part is to be completed **with a partner**.
- Complete the "Lab 3 Post-Lab" activity before the end of Sunday (Sep.22). 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 01)
- Lab documents downloaded to your laptop
- Webserver.exe downloaded to your laptop
- Two laptops

References and Resources:

- Lab 02 resources
- Chapter 2 Section 2.3 (except cisco equipment configuration) and Chapter 3

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:

0.2.1 “CST8108 Lab 03 – In-Lab Activies.pdf” (this document)

0.2.2 Webserver.exe – 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.)

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. Remember you are working in teams of two.

1.1 Obtain a Linksys router (one per team), power adapter and the required cables from your instructor.

1.2 Power on your Linksys router and wait until the router’s green power indicator led is on steadily before proceeding to the next step. Note that during boot up, router reset and firmware upgrades, the power indicator light flashes slowly. Consult the reference documentation for an explanation of meaning of other power indicator states.

1.3 Reset the router back to factory defaults.

1.4 Ensure your Laptop’s Ethernet network adapter is configured to obtain its IPv4 address automatically via Dynamic Host Configuration Protocol (DHCP). (Ref: “How to IP in Windows 7”) Repeat for your partner’s laptop.

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 Ensure that the green light corresponding to the Linksys’s Ethernet port you connected into is flashing. This is an indication that there is network activity on the particular port.

1.7 At the windows command prompt, type **ipconfig /all.** Locate in the ipconfig output and note in the space below, the IPv4 address and subnet mask that has been assigned to your and your partner’s Ethernet network adapter by the Linksys’s DHCP server. Also note the MAC (physical) addresses of your Network adapters.

Your IPv4 address: _______._______._______._______

Subnet Mask: _______._______._______._______

Your partner’s IPv4 address: _______._______._______._______

Subnet Mask: _______._______._______._______

Your MAC address: _____:_____:_____:_____:_____:_____

Your partner’s MAC address: _____:_____:_____:_____:_____:_____

1.8 Locate in the ipconfig output and note in the space below, the Default Gateway address:
Default Gateway: ______.______.______.______

1.9 Compare your Default gateway address value with that your partner has. Are they the same? Why?
You will verify basic connectivity (layer 3) to your Ethernet network by ensuring you can successfully ping your network's default gateway address. At the windows command prompt, type the following command:

ping a.b.c.d where a.b.c.d is the default gateway address you noted in 1.7.

A successful ping will look similar to this:

```
Pinging 192.168.1.25 with 32 bytes of data:

Reply from 192.168.1.25: bytes=32 time<1ms TTL=255
Reply from 192.168.1.25: bytes=32 time<1ms TTL=255
Reply from 192.168.1.25: bytes=32 time<1ms TTL=255
Reply from 192.168.1.25: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.15.1:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 3ms, Maximum = 9ms, Average = 5ms
```

1.10 Show your instructor the ping result

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 on which the web server software will run.

Either laptop should be able to play the role of server, assuming they both meet the BYOD hardware and software requirements. Note that 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 and NOT NAT.

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

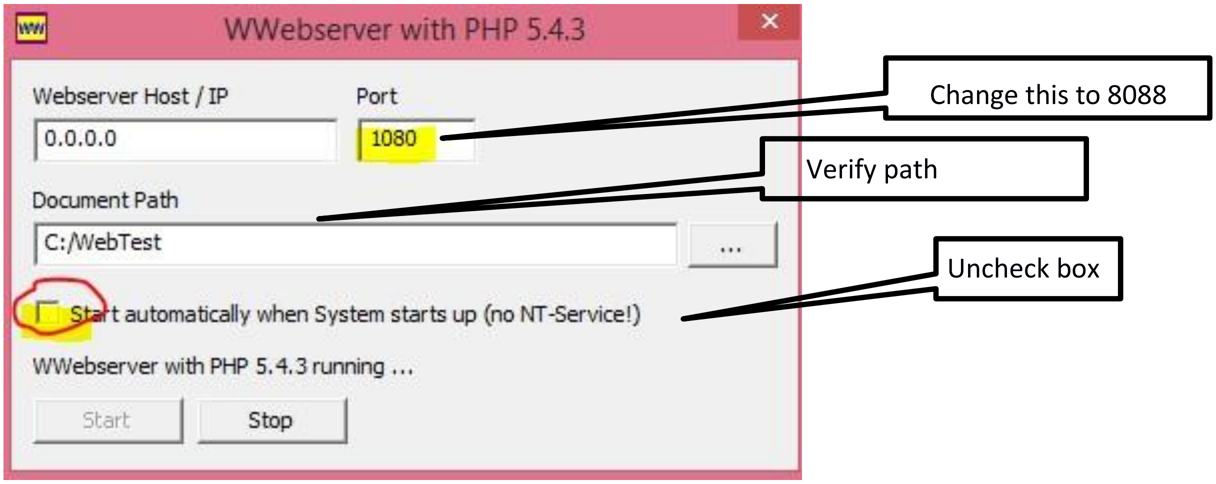
2.1 On the ***laptop you have assigned to be the web server***, install the Webserver software by running the Webserver.exe file (the file you downloaded in task 0). You will be prompted for the extraction location. Extract to a new folder location or to an existing folder location that is empty.

2.2 Disable any firewalls running on the server laptop.

2.3 Navigate to the location you extracted the files in 2.1. Run the wwebser.exe as administrator. The following window will appear. Uncheck the box "Start automatically when System starts up (No NT-Server!)".

2.4 Modify the Port value from 1080 to 8088.

Click Start to start the web server.



WWebserver with PHP 5.4.3

Webserver Host / IP: 0.0.0.0

Port: 1080

Document Path: C:/WebTest

☐ Start automatically when System starts up (no NT-Service!)

WWebserver with PHP 5.4.3 running ...

Change this to 8088

Verify path

Uncheck box

The 0.0.0.0 value in the Webserver Host/IP field indicates that the web server listens for 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 port 8088. Note that the standard port is port 80 for non-secure communication and port 443 for secure communications.

2.5 Connect to web server ***from web browser running on web server laptop***

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

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

replace a.b.c.d:port with the web server's IP address and port number.

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

2.6 Connect to web server ***from web browser running on client laptop***

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

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

replace a.b.c.d:port with the web server's IP address and port number.

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

DO NOT proceed until the web page successfully displays on both client and server laptops.

If 2.5 succeeded but 2.6 failed, then make sure the firewall on the web server laptop has been disabled. This is not the preferred solution but will do until such time that you have learned how to create firewall rules. You also want to make sure bridged networking is enabled if your web server is installed on a Windows OS running inside a VM.

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 interface! Refer back to lab 02 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.

3.2 On the client's laptop, close all the tabs of the web browser.

3.3 Delete the ARP cache.

On both laptops, **run CMD as Administrator**.

From the Command Prompt windows, enter the following command:

```
arp  -d  *
```

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

Note: some Windows versions require you to instead use: **netsh interface IP delete arpcache**

3.4 On the client laptop, open a web browser.

Enter the following URL in the browser's address bar:

http://*a.b.c.d:port* replace a.b.c.d:port with the web server's IP address

and port number.

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

3.5 Stop the Wireshark capture on both client and server. Save the captures.

Task 4: Validate Wireshark Capture

In this task you will ensure that the task 3 capture contains all required frames.

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

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 - Client Request

GET / HTTP/1.1 in the info column where

w.x.y.z in the source column (client IP)

a.b.c.d 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

w.x.y.z in the destination column (client IP)

a.b.c.d in the source column (server IP)

4.3 You must repeat task 3 if either of 4.1 or 4.2 results do not meet the requirements.

4.4 Show your lab instructor the frames.

Task 5: Local Communication Analysis

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

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?

_____:_____:_____:_____:_____:_____

i. This destination's MAC address belongs to which device? ____________________

f. What is the destination IP address?

_____._____._____._____

i. This IP address belongs to which device? ________________________

g. What is the destination port? ____________

i. This destination port belongs to which application? ________________

Task 6: Challenge Question

Assume that the client and web server are connected to different network segments. What would be the layer 2 destination MAC address, the layer 3 IP address and the layer 4 destination port of the message has it leaves the client laptop? Use the knowledge you learned in class to answer and assume the web server IP is: 192.168.0.50 and its MAC is: 00:50:03:00:33:00

Submit the file Lab3-answer-sheet.txt after filling the required answers.

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.

7.3 You will need answers to the above questions to complete the post-lab test.

7.4 Return the borrowed equipment and cables to your instructor.