Lab 4: Capture/Analyze Remote Communication Process

What you will do:

- Using the skills and knowledge acquired in lab 02 and 03, you will build, configure and test a Wired (Ethernet) network consisting of fours nodes: two end devices (laptop) and two intermediary devices (Linksys router).
- Connect to a Web server on a non-default application port.
- Capture and analyze the remote communication process where both sender and receiver are on different network segments.
- Reset a Linksys router to factory settings
- Implement basic router configuration:
  - Connect to router's management web page
  - Configure a static IP on Internet interface
  - Modify the router's IP address
  - Disable Network Address Translation (NAT)
  - Allow anonymous Internet requests

Things that you will need to know or learn:

- Everything that you learned in lab 01, 02 and 03 you will need to complete this lab.
- Identify and understand the different layers of addressing necessary to a successful communication.
- Understand the remote communication process.
- The general purpose and format of an ARP message.
- Writing simple Wireshark expressions to filter frames
- 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.
- Determining your default gateway's IP and MAC address.

What you need to submit and when:

- Complete the in-lab part of the lab including instructor signoffs before the end of your lab period (refer to the instructions below). This part is to be completed **with a partner**.
- Complete the "Lab 4 Post-lab" on Brightspace before the due time. This part is to be completed individually.

Required Equipment:

- Equipment requirements per team:
  - Network cables: two straight-through and one crossover
  - Two Linksys routers and power adapters
  - Wireshark installed and working on both laptops (done in Lab 01)
  - Lab 03 and 04 documents downloaded to your laptop
  - Webserver.zip downloaded to your laptop
  - Two laptops

References and Resources:

- Lab 01, 02 and 03, Lab 4 reference document
- Cisco Module 3

Task 0: Preparations

0.1 Find a partner to work with. You must work in teams of exactly two per team.

0.2 Confirm you have downloaded the following from Brightspace to your computer:

0.2.1 "Lab 04 – In-Lab Activies" (this document) and the Lab 4 Reference document.

0.2.2 "Lab 04 – Network Topology"

0.2.3 Webserver.zip – (you should have it from lab 3 - refer to lab 3 for installation/usage instructions)

0.2.4 Lab04-router1-config – router 1 configuration instructions (see the attached file on Brightspace)

0.2.5 Lab04-router2-config – router 2 configuration instructions (see the attached file on Brightspace)

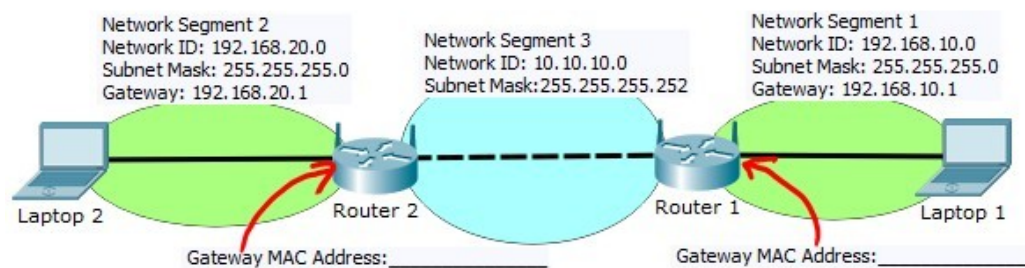0.2.6 Lab04-answer-sheet: this is the file that you are going to submit after filling the answers.

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 Do not continue until you have completed ALL the steps in Task 0.

Task 1: Build, Configure and Test Network

In this task you will build, configure and verify proper operation of the network topology shown below.

Note that the network you are building consists of three separate network segments.

Network Segment 2
Network ID: 192.168.20.0
Subnet Mask: 255.255.255.0
Gateway: 192.168.20.1

Network Segment 3
Network ID: 10.10.10.0
Subnet Mask:255.255.255.252

Network Segment 1
Network ID: 192.168.10.0
Subnet Mask: 255.255.255.0
Gateway: 192.168.10.1

Laptop 2   Router 2   Router 1   Laptop 1

Gateway MAC Address:_____   Gateway MAC Address:_____

Laptop 2
IP Address: 192.168.20.___

MAC Address: _____

Student Name:_____

Role: Web Client or Web Server? _____

Laptop 1
IP Address: 192.168.10.___

MAC Address: _____

Student Name:_____

Role: Web Client or Web Server? _____

Remember you are working with a partner - determine which student using Laptop 1 and Laptop 2 above.

Each student does all the steps below individually with their respective Router (1 or 2).

1. Power up the routers and wait for the power light to be steady on.
2. Reset to factory defaults by pressing (using a pen) the reset switch located at the bottom of the router.
3. Connect your laptop to any to the Linksys Router's switch port using the appropriate cable. (Which cable type?)
4. Connect the routers together via their respective Internet ports using the appropriate cable. (Which cable type?)
5. Confirm basic connectivity by making sure you can successfully ping your default gateway.
6. As shown in the topology diagram, determine which router (1 or 2) your laptop is connected to.
7. Perform the router configuration as per the router configuration document:
   a. Refer to Lab04-router1-config if your laptop is connected to router 1.
   b. Refer to Lab04-router2-config if your laptop is connected to router 2.
8. **Do not continue until all local and remote connectivity tests have succeeded!**
9. Complete the blank details of the diagram above in your answer sheet.

Task 2: Install and Test Web Server

In this task you are preparing the web server for task 3.

1. Assign a **single** laptop to be the web server and on that laptop only install and test the Web Server. Refer to Lab 03 Task 2 for detailed instructions.
2. DO NOT PROCEED UNLESS Lab 03's Tasks 2.5 and 2.6 have succeeded.

Task 3: Remote Communication Process

In this task you will capture the http traffic between a web client and a web server. You are essentially repeating a similar process as in Lab 3, except that the client and server devices are on <u>different</u> network segments.

1. Start a Wireshark capture on both web server and web client.
2. Filter the Wireshark capture by **http**
3. **Client only:** Close all the web browser windows. Start again the web browser in Private/Incognito mode.

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

    http://a.b.c.d:8088

    (replace **a.b.c.d** with the server's IP address)

    Do not proceed to the next step until the web page successfully displays in the web browser.
4. Stop the capture on both client and server.
5. On client and server, locate two captured frames having the following characteristics:

    Client Request
    GET / HTTP/1.1 in the <u>info column</u>
    where:

    > w.x.y.z in the source column is the client IP
    > a.b.c.d in the destination column is the server IP

    Server Response
    HTTP/1.1 200 OK   OR   HTTP/1.1 304 Not modified in the <u>info</u> column
    where:

    > w.x.y.z in the <u>destination</u> column is the client IP

    DEMONSTRATE THE TWO FRAMES TO YOUR PROFESSOR

6. Here is a generic expression that can be used to filter the frame meeting **the client's Request** requirements in 5:

    A) `http && ip.dst == a.b.c.d && ip.src == w.x.y.z`

    where **a.b.c.d** is the web servers IP address

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

    B) Compare the layer 4 addresses (port number) and layer 3 addresses (IP) values for this frame with your partner's. They MUST match.

    Write the filter you used with the actual number in the answer sheet.

7. Compare the <u>layer 2</u> address values with your partner's values and answer the following questions in your answer sheet.

    A)   Are they identical or different?

    B)   Answer the following questions if you answered Different in 7-A:

    i.   Explain why they do not match?

    ii. The destination MAC corresponds to which device?

    iii. The source MAC corresponds to which device?

8. Examine your laptop's ARP table

    A)   In the Command Prompt window, use the correct command to see your laptop's ARP table.

    B)   You should only focus on (and have) table entries under the Interface bearing the IP address assigned to your Ethernet adapter.

    C)   Do you see any entries for your partner's IP or MAC?

    D)   Which entry served to communicate with your partner's laptop?

    Copy and paste the <u>specific ARP Table entry</u> into your answer sheet. No marks are given for copying the entire table.

Submit your completed answer sheet to Brightspace.

Task 4: Demo, Cleanup and Other Tasks

1. Make sure to complete the demo to your professor.
2. Re-enable your firewall.
3. Re-enable your Wireless Network and confirm you are able to access the College network.
4. Carefully pack and return the borrowed equipment.