Lab 4: Capture/Analyse 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 analyse 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 Blackboard before the end of Sunday (Feb.5). This part is to be completed individually.

Required Equipment:

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

Marks:

- 20% of your final mark is for labs done during the course of the semester.

References and Resources:

- Lab 01, 02 and 03
- Cisco Chapter 3

Layer 3 and 2 Addresses

Here are some useful rules to remember about addresses:

- A message's layer 3 (e.g. IP address) and layer 4 port number (e.g. application port) values **do not change** as the message moves from one network to another (there are exceptions but we will not look at these until later in the semester).
    - The destination address value corresponds to the IP address of the device the message is ultimatly intended for.
    - The source address value corresponds to the original message sender's IP.
- The message's layer 2 (e.g. MAC address) address values **change** as the message moves from one network to another. Here are the Layer 2 address values as the frame leaves the sender's device.
    - When sending a message to a local device
        - The frame's destination MAC corresponds to the local device's MAC address.
        - The frame's source MAC corresponds to the sending device's MAC address.
    - When sending a message to a remote device
        - The frame's destination MAC corresponds to your default gateway's MAC address.
        - The source MAC corresponds to the sending devices's MAC address.

Frames are the PDUs we place on the physical media. They are responsible for carrying our messages from one device to another within the boundaries of the same network segment. If the device we wish to communicate with is on another network segment, then, the frame will be addressed and delivered to the default gateway. It is the default gateway (i.e. router) that performs the complex work of moving the message across the network.

Remember that a frame has no life beyond the network segment on which it was created! The router discards the original frame and encapsulates a message in a new frame when it needs to move the message to another network.

Address Resolution Protocol (ARP)

The ARP protocol operates on Wi-Fi and Ethernet networks and provides the mechanism for obtaining the layer 2 addresses necessary to move frames from one device to another within the same network segment. In short, the purpose of the ARP protocol is to resolve IPv4 addresses to MAC addresses.

Here is a brief and simplified description of how ARP works.

- When sending a message to a local device
    - An ARP request seeking to obtain the local devices MAC address is broadcast to all devices on the network segment as the sender
        - The ARP request is of the form:
            - Who has a.b.c.d? Tell w.x.y.z
        - The ARP response is of the form:
            - w.x.y.z is at aa:bb:cc:dd:ee:ff
    - The learned MAC address is used to direct the frame to its destination device.
    - The learned MAC address is cached in the sending device's local ARP memory.
- When sending a message to a remote device
    - Remenber that you direct all remote communications to your router. You let it do the hard work!
    - An ARP request seeking to obtain your default gateway's MAC address is broadcast to all devices on the network segment
    - The learned MAC address is used to direct the frame to your default gatewat device. The default gateway does all the hard work involved in internetwork communcations.
    - The learned MAC address is cached in the sending device's local ARP memory.

Note that an ARP broadcast message does not exist/live beyond the network segment it was created on. That is a router will STOP the spread of an ARP message to other networks! Imagine the traffic that would exist if routers allowed ARPs to spread to all networks!

The **arp –a** command allows you to display the ARP table and hence determine the MAC address of devices your device has communicated with (locally). An ARP table ONLY contains MAC entries of other locally connected devices. You will never see or know the MAC address of remote device – the only MAC you need to know to communicate with remote devices is the default gateway's MAC address. Note that the entries in an ARP table have a time limit; they will be deleted from memory after a configurable amount of time!

The figure below shows the output of running ipconfig and arp –a on a device having IP address 192.168.15.106. By examining the output below we are able to tell that default gateway's MAC address for 192.168.15.106 is: 0c-47-3d-a1-88-82. We can deduct this information by first determining the Default Gateway address from the ipconfig output. We then take this IPv4 address and attempt to find a matching entry in the arp –a output. As there is an entry in the arp –a output for 192.168.15.1, its MAC address is the value that appears under the Physical Address column!

From the output we cannot tell what the MAC address for 192.168.15.106 is. In this particular case we would need to run ipconfig/all in order to obtain the MAC address for 192.168.15.106.

Note that the output below shows multiple interfaces, but as we have learned in class, the interface that provides connectivity with the outside world in this specific configuration is the Ethernet adapter.

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.15.106
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.15.1

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.29.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.227.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{07D56837-C3B9-4EE2-B954-15412F257287}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{1D888087-BE3A-46B1-BFF7-3F00F154E68A}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{ADD13316-AD5F-4A3E-810C-D0074B1FD588}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Yvan>arp -a

Interface: 192.168.15.106 --- 0x3
  Internet Address      Physical Address      Type
  192.168.15.1          0c-47-3d-a1-88-82     dynamic
  192.168.15.2          c0-c1-c0-9f-0f-4f     dynamic
  192.168.15.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.29.1 --- 0x13
  Internet Address      Physical Address      Type
  192.168.29.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.227.1 --- 0x14
  Internet Address      Physical Address      Type
  192.168.227.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

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 BB "Labs - > Lab 04" to your computer:

- 0.2.1 "Lab 04 – In-Lab Activies.pdf" (this document)
- 0.2.2 "Lab 04 – Network Topology"
- 0.2.3 Webserver.exe – to install the Web Server
- 0.2.4 Lab04-router1-config – router 1 configuration instructions
- 0.2.5 Lab04-router2-config – router 2 configuration instructions

0.3 Disable the Wireless Network Interface of your Laptop computer. Your only connection to the network must be via the Ethernet (wired) interface.

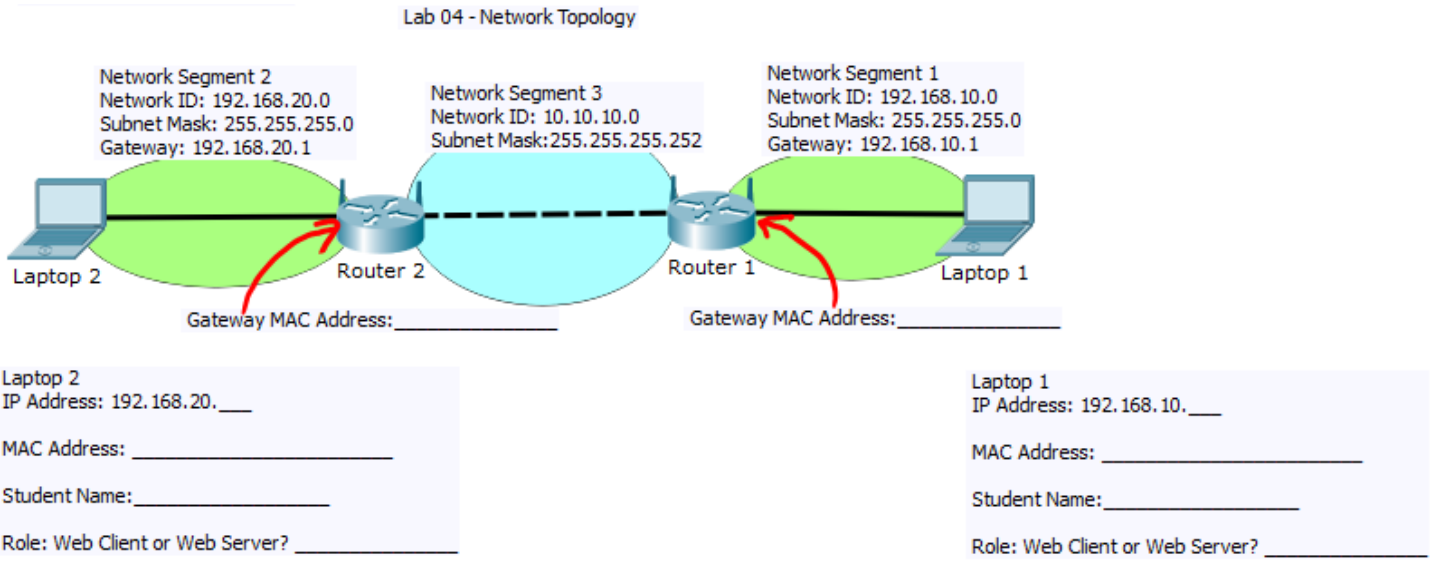
0.4 Do not start until you have completed ALL steps in this task.

Task 1: Build, Configure and Test Network (2 marks)

In this task you will build, configure and verify proper operation of the network topology shown in "Lab 04 – Network Topology". The network you are building consists of three separate network segments: Network segment 1, Network segment 2 and Network segment 3.

Do not start task 1 until you have completed all Task 0 steps. Remember you are working in teams of two.

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.
   a. Keep the reset button depressed until the power light flashes
3. Connect your laptop to any of your Linksys' switch port using the appropriate cable
   a. One laptop per router!
4. Connect the routers together via their respective Internet ports using the appropriate cable
   a. What cable did you use?
5. Confirm basic connectivity by making sure you can successfully ping your default gateway.
6. As shown in the topology diagram, determine who will be router 1 and who will be router 2.
7. Perform the router configuration as per the router configuration document:
   a. Refer to Lab04-router1-config if you are router 1;
   b. Refer to Lab04-router2-config if you are router 2.
8. Do not continue until all local and remote connectivity tests have succeeded!
9. Record your addresses on your paper copy of your topology diagram and demo to your lab instructor.



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 (5 marks)

In this task you will capture the http traffic between a web client and a web server. You are essentially repeating the same task as in Lab03, except that the client and server devices are on different network segments.

1. Start a Wireshark capture on both web server and web client.
2. Filter Wireshark capture by http
3. On the client laptop, open a web browser.

   Enter the following URL in the browser's address bar:
   http://*a.b.c.d*:8088

   replace a.b.c.d with the web server's ip address.

   Do not proceed to the next step until the web page successfully displays in the web browser.
4. Stop and save your capture on both client and server. Save as WS-task3.
5. On client and server, locate two captured frames having the following characteristics:

   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)

   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)

6. **2 marks** - Here is an expression that filters the frame meeting the Client 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. Apply the filter and take a screen capture of the results.
      i. Your screen capture must include both Wireshark's summary and details pane
   c. Compare the layer 4 and layer 3 address values with your partner's. They MUST match.
   d. Save the screen capture.
7. **2 marks** - Compare the layer 2 address values with your partner's values and answer the following questions.
   a. Are they identical or different? _____
   b. Answer the following questions if you answered Different in 7a:
      i. Explain why they do not match?

      ii. The destination MAC corresponds to which device? _____

      iii. The source MAC corresponds to which device? _____

8. **1 marks** - Examine your laptop's ARP table
   a. From a Command Prompt window type in the following command:
      i. arp –a
      ii. The command shows the IP to MAC mappings that have been learned by your laptop.
   b. In particular, you want to focus on the entries that fall 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? _____
      i. Which entry served to communicate with your partner's laptop? Screen capture the arp –a output and highlight the entry that is used for remote communication.

Instructor Signoff_____

Task 4: Demo, Cleanup and Other Tasks

1. Demo your screen capture and answers to your lab instructor.
2. Re-enable your firewall.
3. Re-enable your Wireless Network and confirm you are able to access the College network.
4. Return the borrowed equipment and cables to your instructor.