Lab 4: Capture/Analyse Remote Communication Process

# What you will do:

* Using the skills and knowledge acquired in lab 02 and 03, in Packet Tracer, you will build, configure and test a Wired (Ethernet) network consisting of three network segments.
* Set up a web server.
* Capture and analyse the remote communication process where both sender and receiver are on different network segments.
* Implement basic router configuration:
  + Configure a static IP on each of the router’s interface

# 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.
* Understand the PDU provided in PT simulation mode 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.
* Determining the network adapter’s MAC address.
* Determining the default gateway’s IP and MAC address.

# What you need to submit and when:

* Complete the lab and submit required files to BrightSpace before the due time.
* Complete the “Lab 4 Post-lab” on Brightspace before the due time.

# Required Equipment in PT:

* Equipment requirements:
  + Network cables: straight-through cables
  + One Cisco router (model: 2901), two switches (2960), two servers, one laptop and one PC
  + Lab 04 documents downloaded to your laptop
  + Your laptop

# 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.

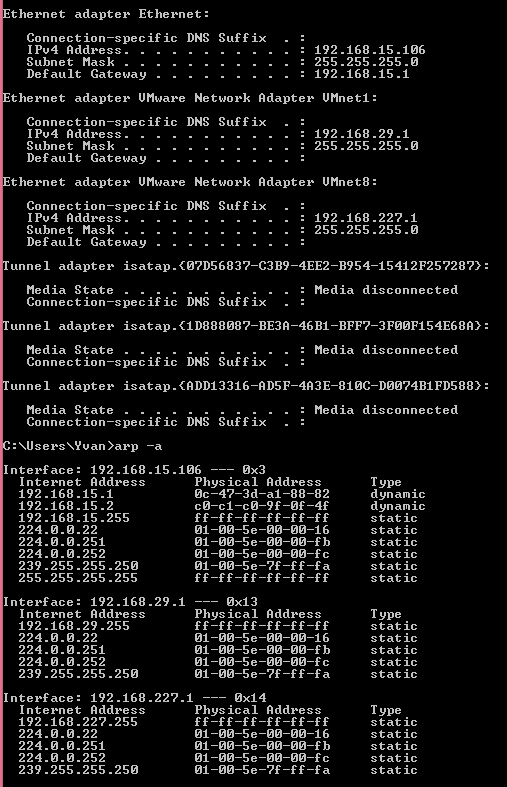
Note that an ARP broadcast message does not exist/live beyond the network segment it was created on. That is a router will STOP the spread of an ARP message to other networks! Imagine the traffic that would exist if routers allowed ARPs to spread to all networks!

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.



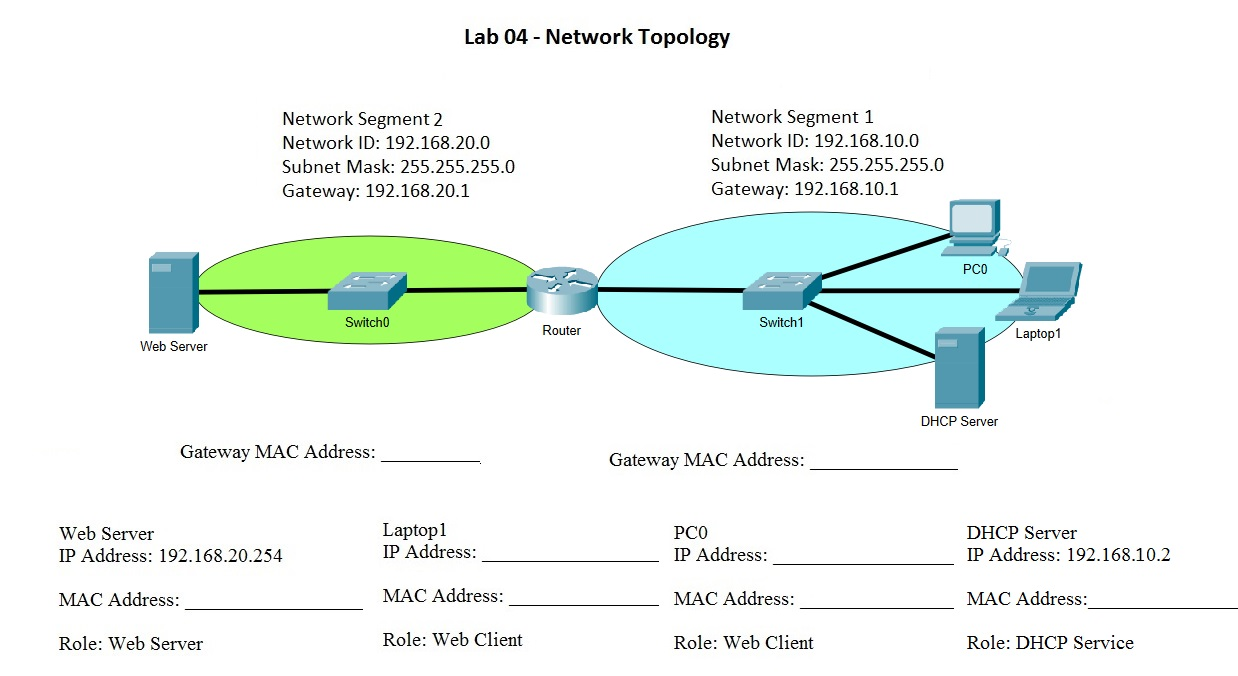
# Task 0: Preparations

* 1. Confirm you have downloaded the following from BS “Labs - > Lab 04” to your computer:
     1. “Lab 04 – In-Lab Activities - online.pdf” (this document)
     2. “Lab 04 – Network Topology – online.jpg”
  2. Do not start until you have downloaded all the files.

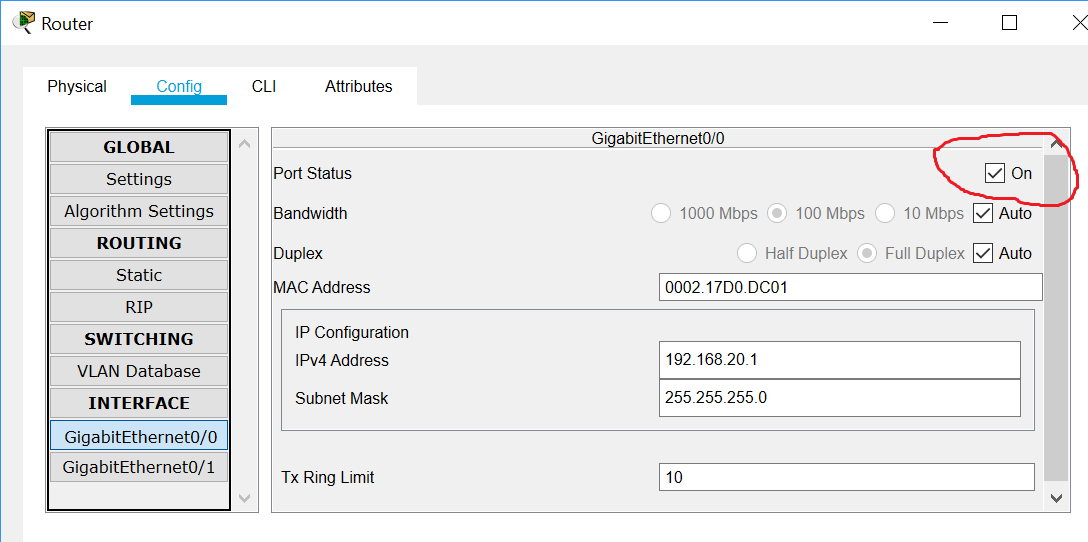
# Task 1: Build, Configure and Test Network

In this task you will build, configure and verify proper operation of the network topology shown in “Lab 04 – Network Topology - online” in PT. The network you are building consists of two separate network segments: Network segment 1 and Network segment 2.

Do not start task 1 until you have completed all Task 0 steps.



1. Connect DHCP Server, Laptop1 and PC0 to any of the ports of Switch1 using the appropriate cable.
   1. What cable did you use? Copper straight through
2. Connect the Web Server, Switch0 and Server Router using the appropriate cable.
3. Connect the router to Switch0 and Switch1.
4. Configure the network interface of all devices by following the table of network topology diagram as below.
5. When you configure the IP address for the router, make sure that the status of the port is up. Click the port status checkbox as showed in the picture.



1. Confirm basic connectivity by making sure you can successfully ping your default gateway.
2. Record your addresses on your network topology for your later data communication analysis.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| Router | GigabitEthernet0/0 | 192.168.20.1 | 255.255.255.0 | N/A |
| GigabitEthernet0/1 | 192.168.10.1 | 255.255.255.0 |
| Web Server | NIC | 192.168.20.254 | 255.255.255.0 | 192.168.20.1 |
| DHCP Server | NIC | 192.168.10.2 | 255.255.255.0 | 192.168.10.1 |
| PC0 | NIC | Dynamic | 255.255.255.0 | 192.168.10.1 |
| Laptop1 | NIC | Dynamic | 255.255.255.0 | 192.168.10.1 |

Network Topology Diagram

# Task 2: Remote Communication Process

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.

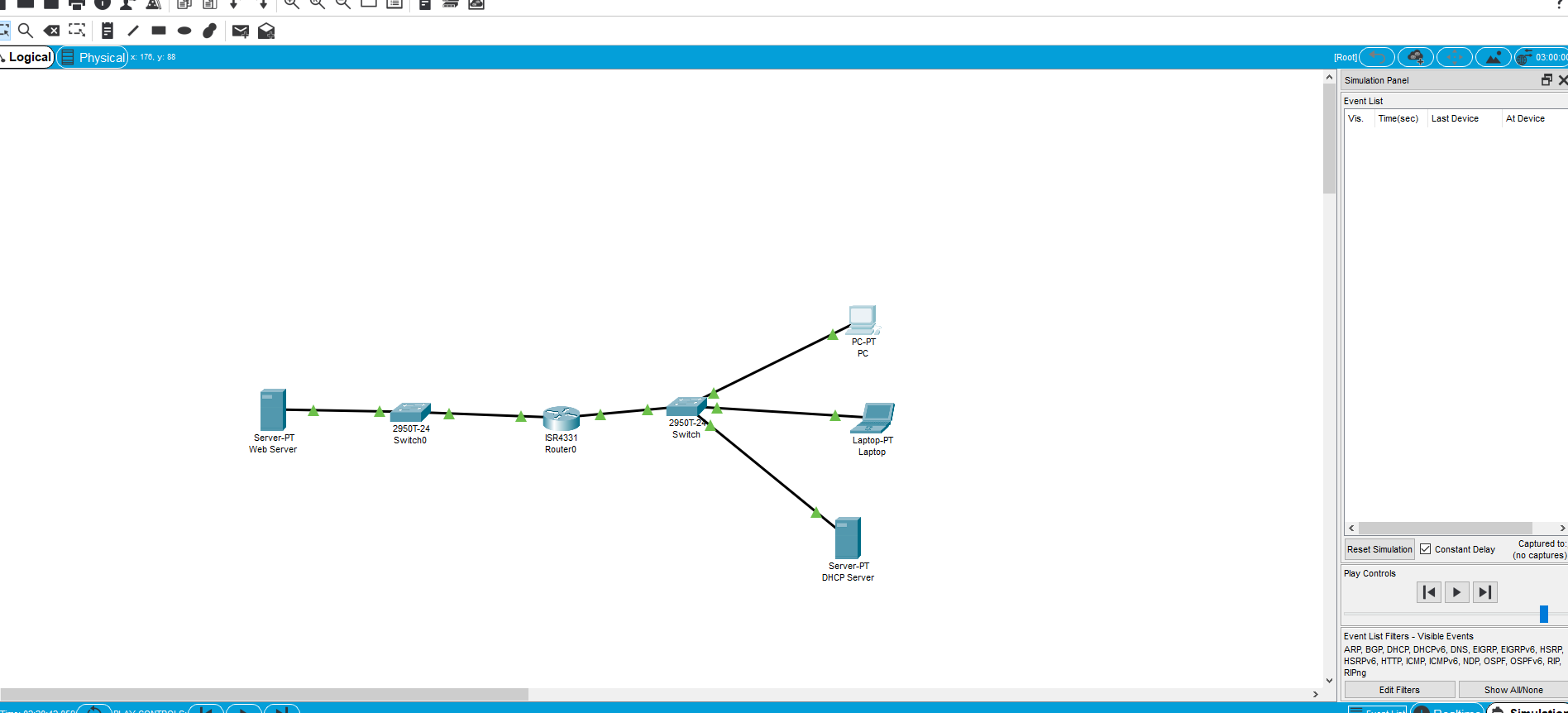
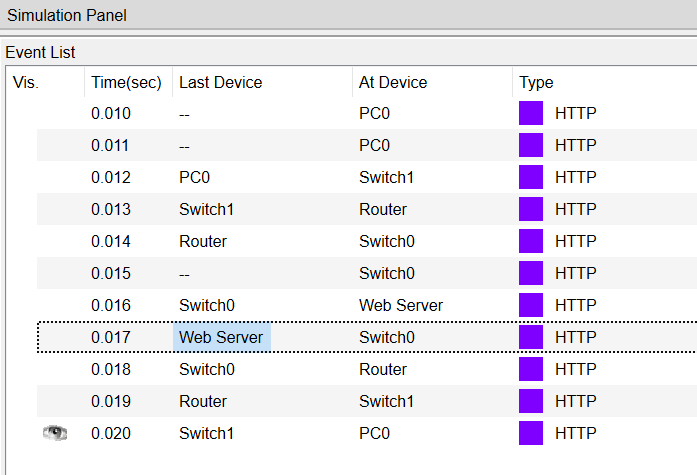
1. In PT, change **Realtime** mode to **Simulation** mode by clicking on the simulation icon. 
2. In simulation mode, click on **Edit Filters** and then on the **Misc** tab.
3. You will see many protocols with check marks. Make sure they are **unchecked** except **HTTP**.
4. On PC0, open a web browser.

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.

Keep the web browser window open, focus back to the PT workplace.

1. Click on the Capture/Forward tab to capture the PDU. To stop capturing PDU, just click on Capture/Forward again.
2. **2 marks -** Take a screen capture including your network topology and the simulation panel and save as Lab4-task2.
3. 
4. On PC0 and Web Server, locate two captured PDU having the following characteristics:

**Client Request (PC0 – Switch1)**

PDU Details:

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

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

**Server Response (Web Server – Switch0)**

PDU Details:

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

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

1. **4 marks** - Compare the layer 2 address values in the two PDU from step 7 and answer the following questions.
   1. Are they identical or different? different
   2. Answer the following questions if you answered Different in 8a:
      1. Explain why they do not match?
      2. The destination MAC in the PDU sent from the client corresponds to which device? Switch1
      3. The source MAC in the PDU sent from the client corresponds to which device? PC0
      4. The destination MAC in the PDU sent from the server corresponds to which device? Web Server
      5. The source MAC in the PDU sent from the server corresponds to which device? Switch0
2. **2 marks** - Examine the ARP table on PC0
   1. Change **Simulation** mode to **Realtime** mode by clicking on the Realtime icon.
   2. From a Command Prompt window of PC0, type in the following command:
      1. ping a.b.c.d

replace a.b.c.d by the IP address of Laptop1

* + 1. ping w.x.y.z

replace w.x.y.z by the IP address of Web Server

* + 1. arp –a
    2. The command shows the IP to MAC mappings that have been learned by PC0.
  1. In particular, you want to focus on the entries that fall under the Interface bearing the IP address assigned to the NIC of PC0.
  2. Do you see any entries for the IP or MAC of the Web Server? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
     1. Which entry served to communicate with the Web Server? Screen capture the arp –a output and highlight the entry that is used for remote communication. **Paste the screen capture below.**

# Task 3: Submission

Submit the saved files from the previous tasks and this Word file to the drop box inside the folder “lab 04” on BrightSpace.