Course:Cloud and Network Security-C1-2026

Cyber Shujaa Program

Week 1 Assignment
Examine TCP/IP and OSI Models in Action

Student Name: Salim Katana Karuku

Student ID: CS-CNS11-26048

Table of Contents

Introduction

This week's assignment was to start installing packet tracer. While I was already familiar with some of the tools introduced, I found the structured approach highly beneficial in reinforcing my understanding. Having previously do networking, I was able to focus more on how data travels from server to pc. This hands-on learning approach is particularly effective in deepening my understanding of how the flow of data from server to PC and how to configure IP address. This experience has laid a strong foundation for exploring more advanced techniques in the coming weeks.

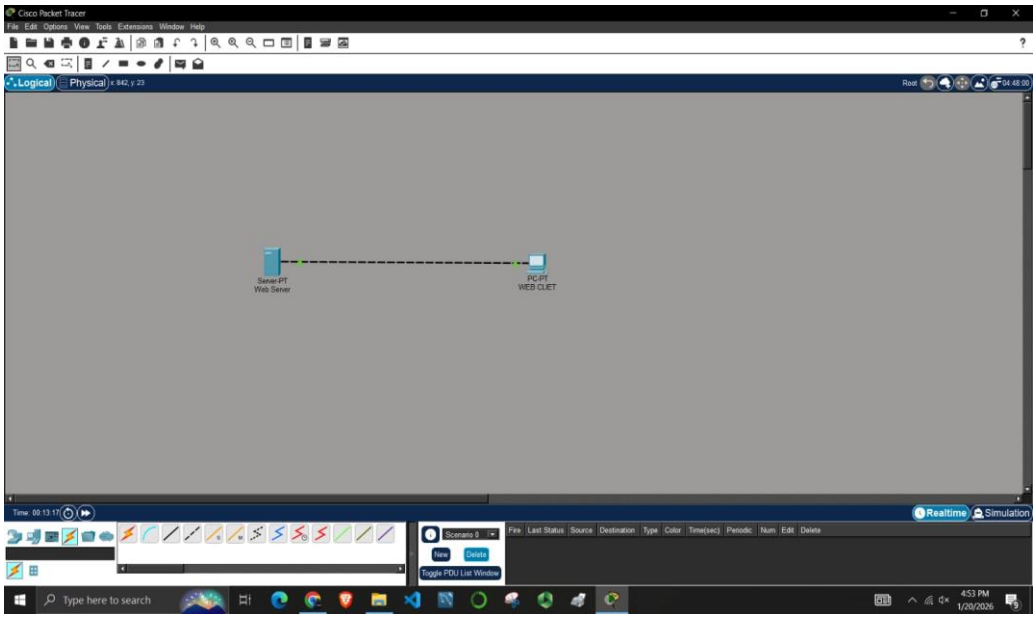
Objectives

The objectives of the assignment were:

1. To visualize data flow,
2. Understand encapsulation/DE capsulation
3. Identify protocols (HTTP, TCP, IP, ETC) and PDUs at each layer
4. Bridging the theoretical models with practical packet behaviour in tools like packet tracer

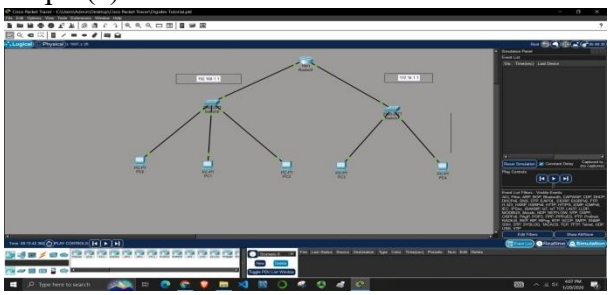
Tasks Completed

SECTION A: Installing Packet Tracer version 8.2



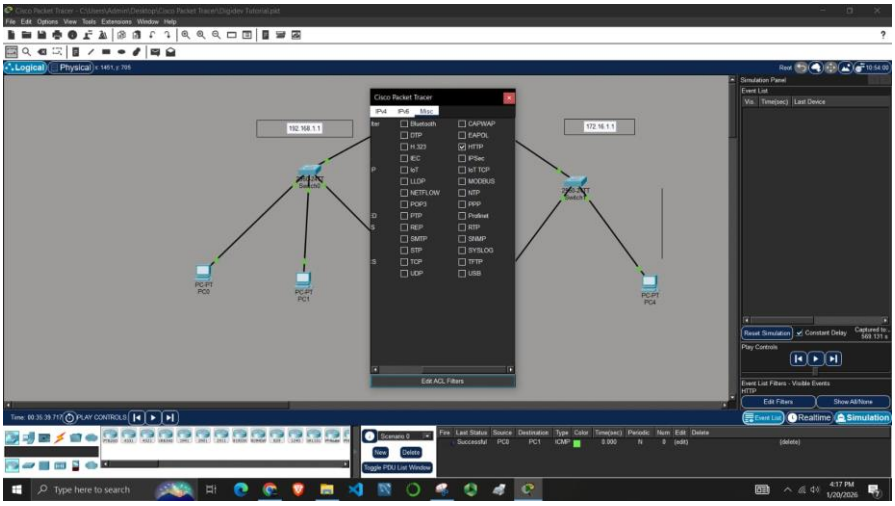
SECTION B: ASSIGNMENT ONE

Step1 (a) Switch from Real time to Simulation mode

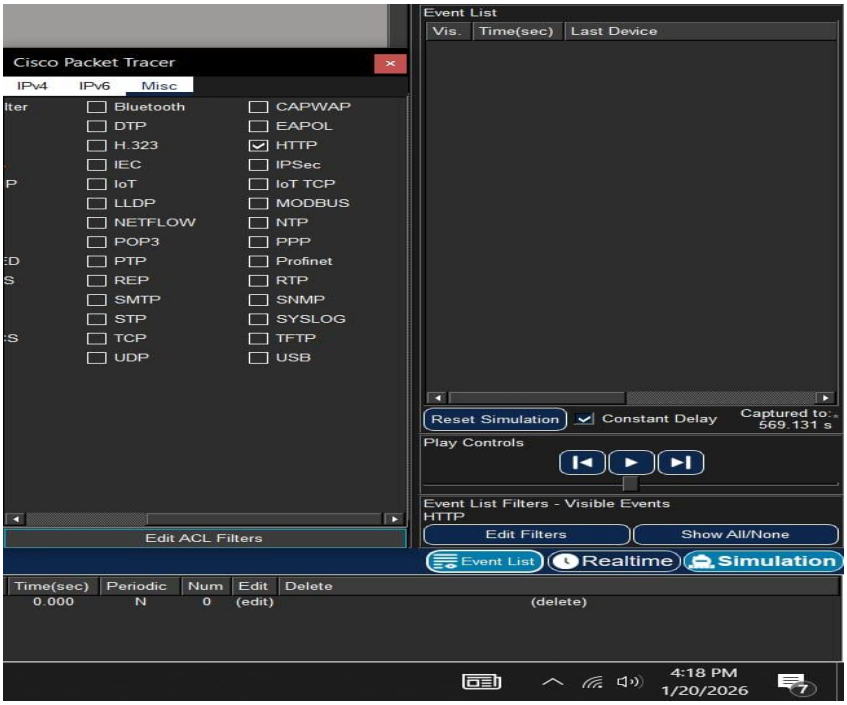


I have switch the real time to simulation mode

Step 1 (b) 1 select HTTP from the Event List Filters

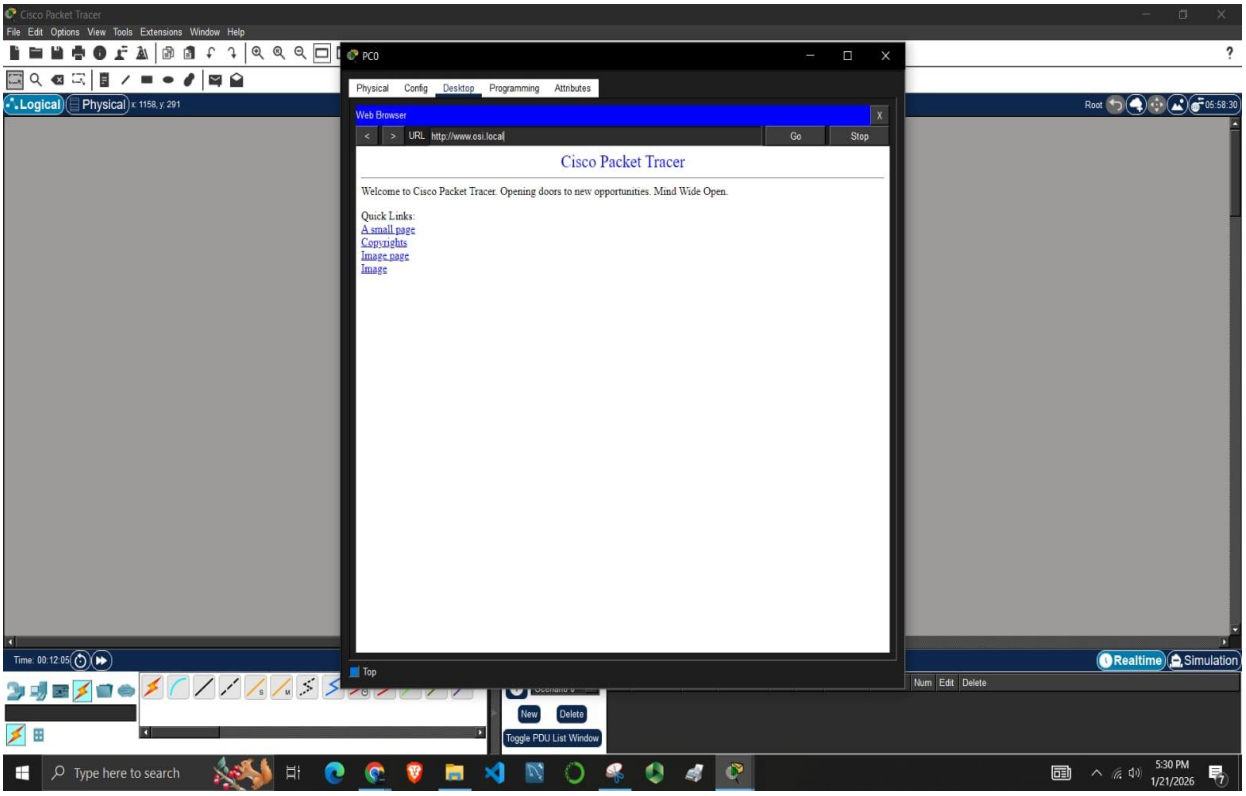


Step 1 (b) 2 : Show All/None until all boxes are cleared

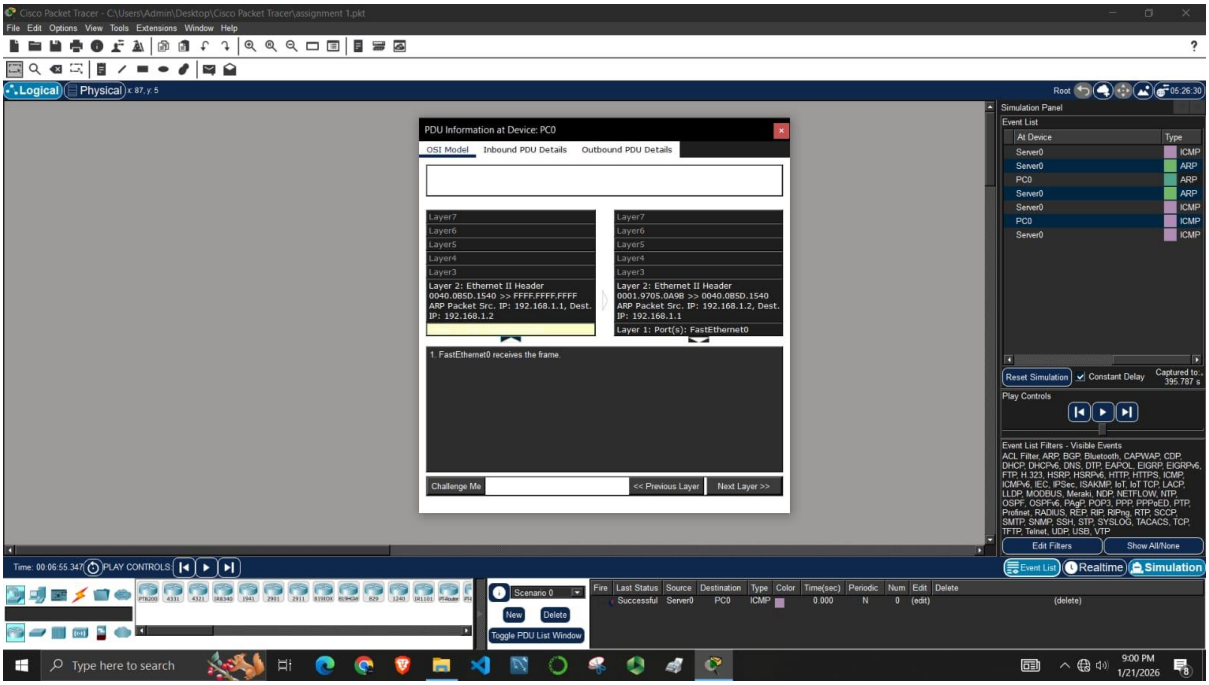


STEP 2: (a, b, c & d) Generate web (HTTP) traffic

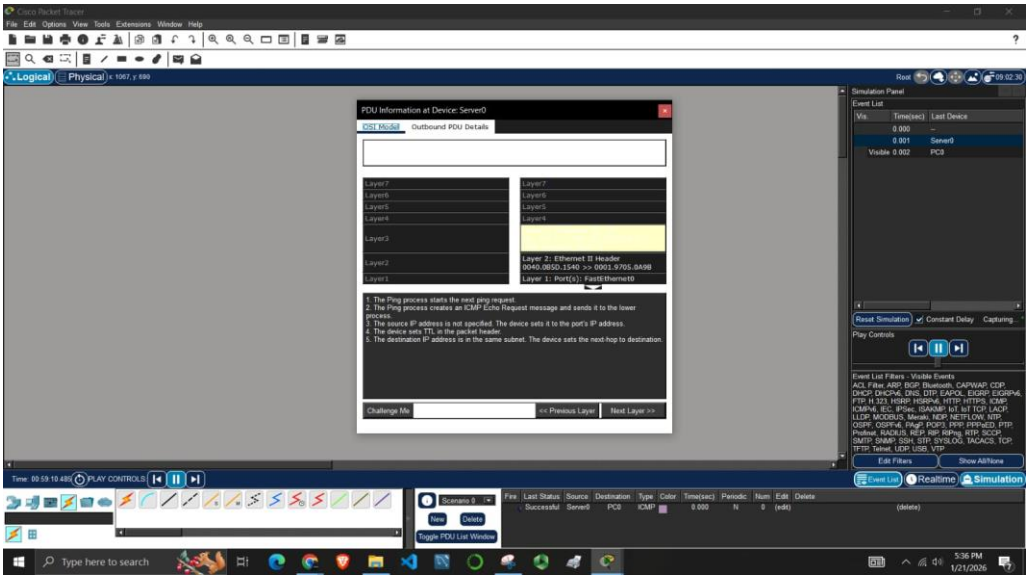
After follow all the steps, then I enter the URL www.osi.local there after I did the capture forward (4) times then it display, welcome to packet tracer opening door to new opportunities mind wide open as shown below



Step: 3(a) Explore the contents of the HTTP packet



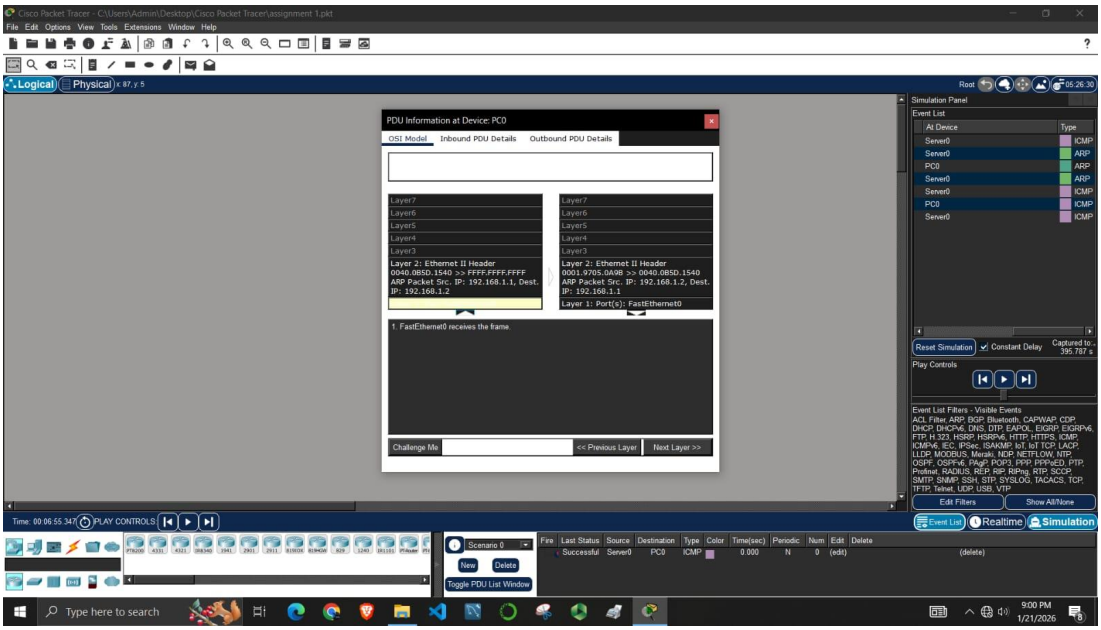
Step 3 (b) OSI Model is selected



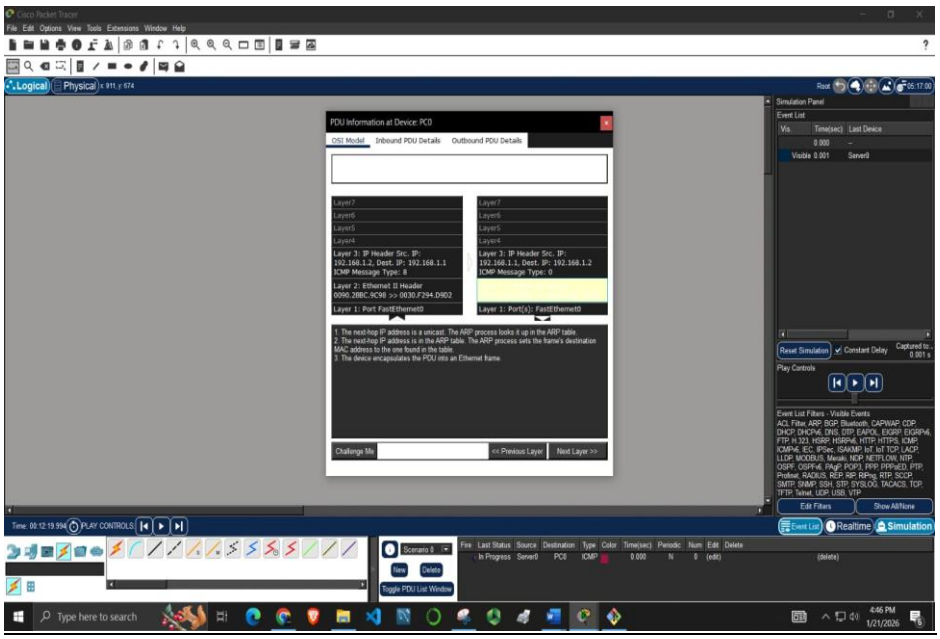
- The Dest. IP value for layer 3
  Dest. IP: 192.168.1.2
  Dest. IP: 192.168.1.1

- Information displayed at layer 2 under the out layer columns are;
  i. The next-hop IP address is uncast. The APR process looks it up in the ARP table.
  ii. The next-hop IP address is not in the ARP table. The ARP process tries to send on ARP request for that IP address and buffers this packet

STEP 3: (C) Outbound PDU Details tab

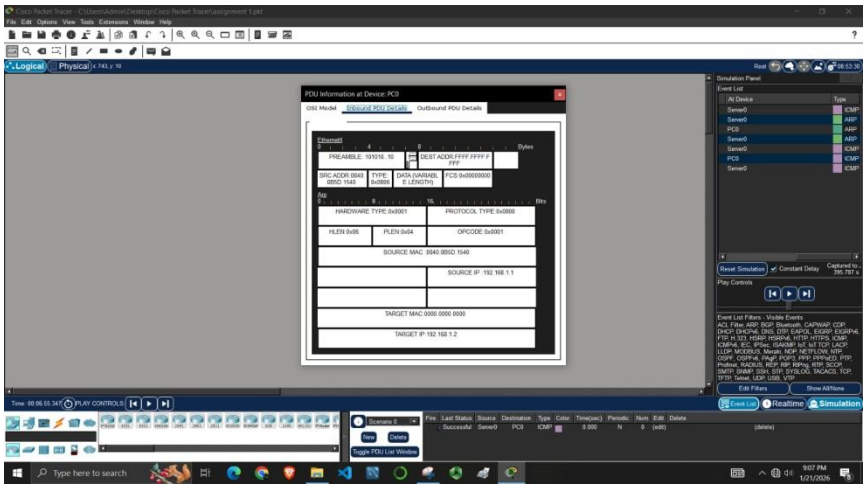


In PDU details, the common information between the TCP section and the TCP section and the OSI model tab are the source port and Destination port, which are associated with the transport layer 4 which is responsible for end to end communication, reliable delivery and segmenting data while TCP handles data at the transport layer (segment PDU) the OSI Model tab visually maps these port numbers to its layer 4, which show the link between the two models

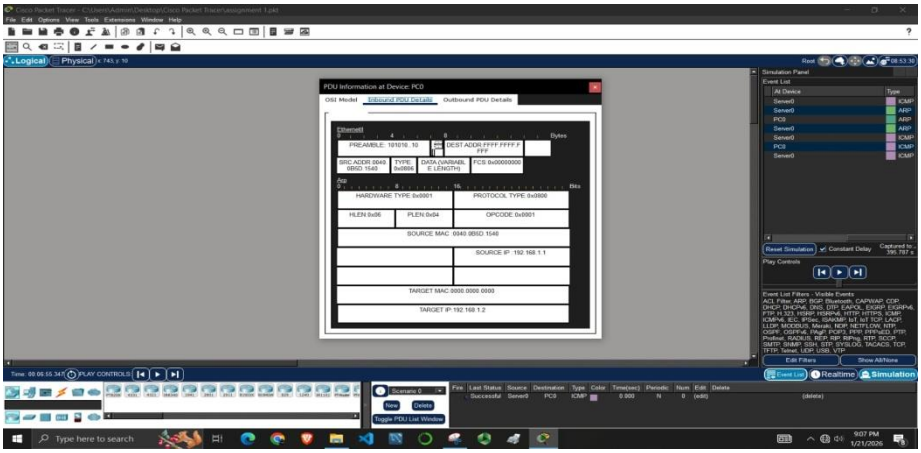


The Host listed under the HTTP refers to the domain name e.g www.osi.local which is representing the destination server hence associates with application layer 7 of the OSI model where we can be able to read and operate

Step 3 (d) Coloured square box under the event list

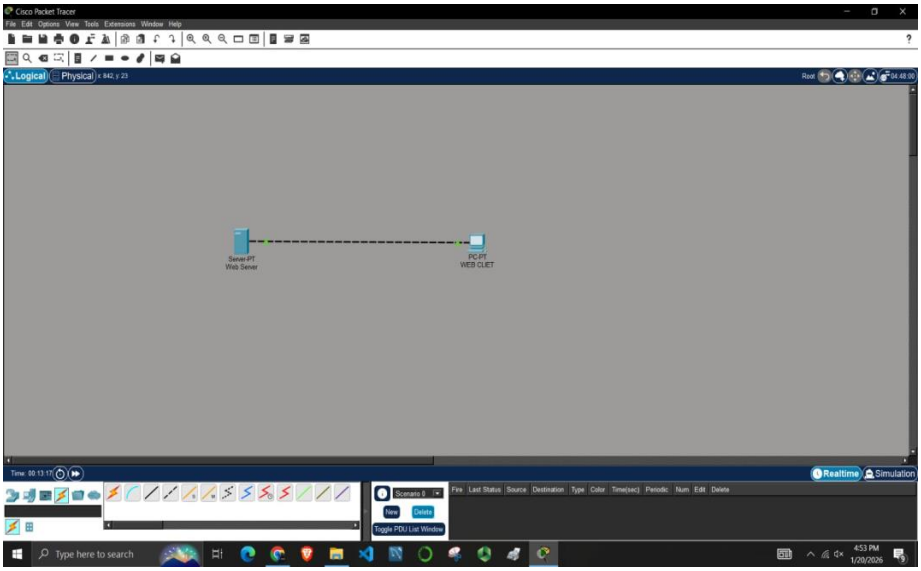


Step 3 :(e) Comparing the information displayed in the in layers column with the out layers column



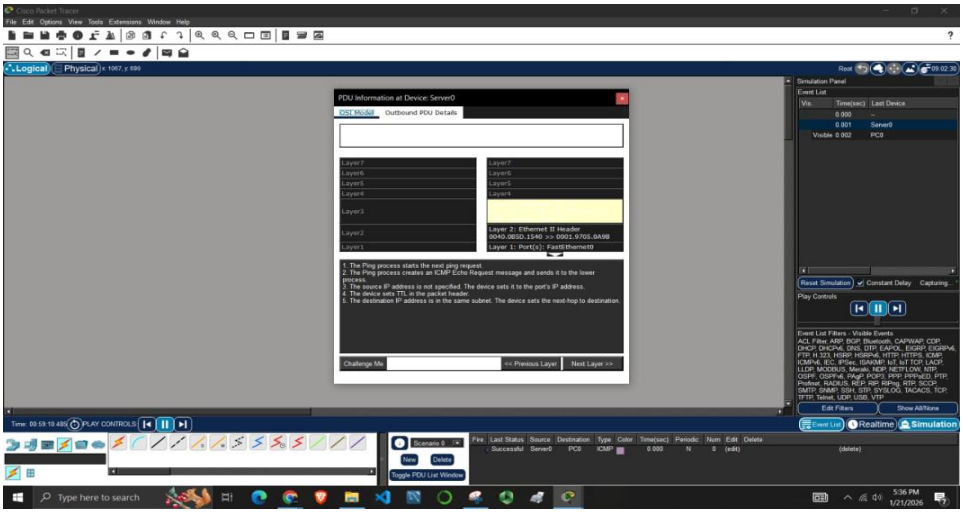
The differences are In Layers show the building up of the request packet while Out Layer show the unwrapping of the response packet as it is being prepared for transmission back to the client, with data moving from lower to higher layers in the Out Layers view.

Step 3 (F) inbound and outbound PDU Details tab.

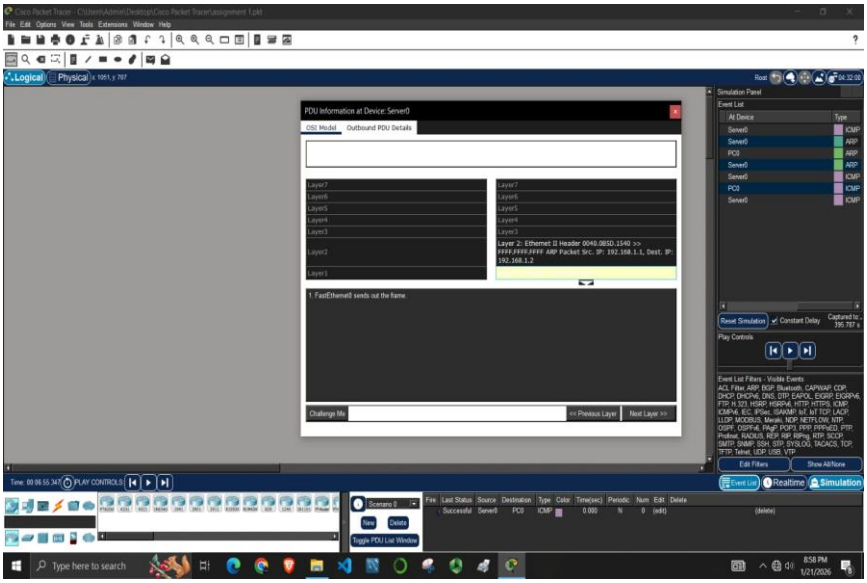


.
This involves the scrolling through layers such as Ethernet11,IP, TCP/HTTP to let as see the source or destination addresses and data, noting how addresses swap for return traffic and identifying key data like the http/1.1 200 ok message on the outbound side or if it is successful.

Step 3 (g) The last coloured square box
It shows only two tabs inbound show the data arriving while the which is the final reply due to the HTTP response there is only just a data to receive



PART 2: Display Elements of the TCP/IP Protocal Suite
Step 1: (a) view Addictional Events

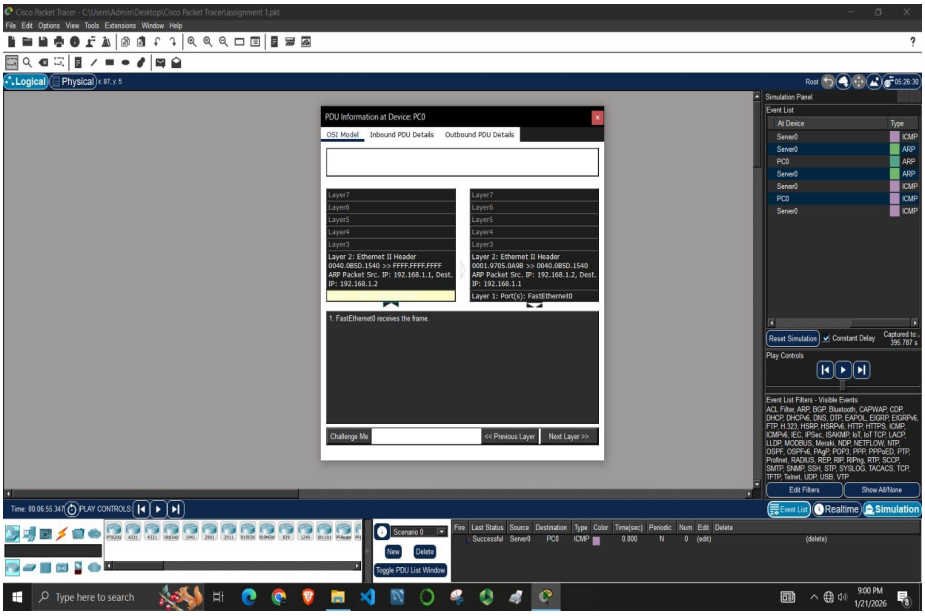


Step 1: (b) The additional events being displayed

a) ARP
b) ICMP
c) ACL filter
d) PPP
e) BGP
f) Bluetooth
g) CAPWAP
h) CDP
i) DHCPv6
j) DNS
k) DTP
l) TCP

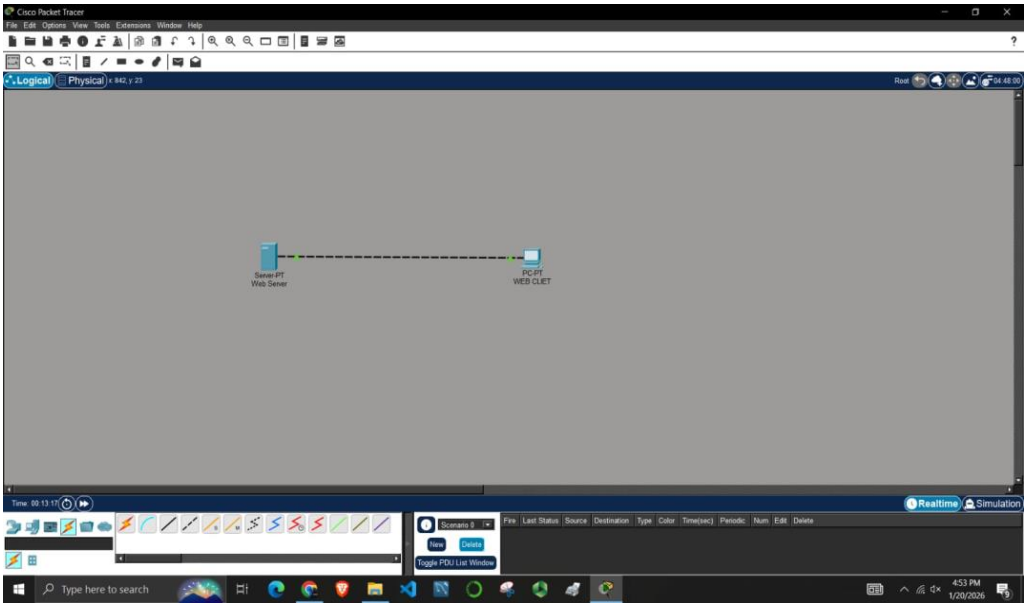
m) IoT
n) IES

Step1: (c) The first DNS event in the Type column



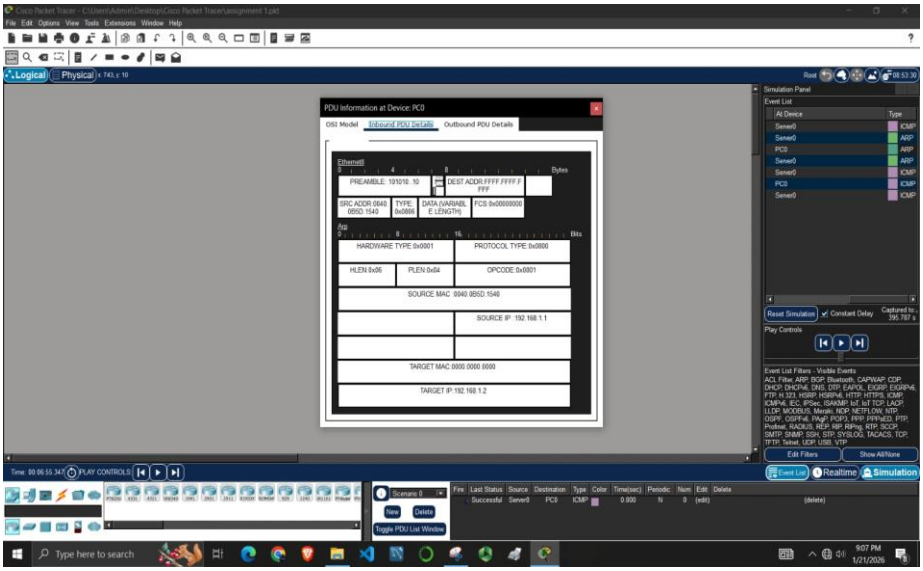
This steps involves observing the encapsulation process where data gets wrapped with headers from each layer e.g application, transport, network, data link as it goes down the OSI stack that's layer 7-1 and de-encapsulation in reverse, with the DNS query starting at Layer 7 that's the application layer and becoming a UDP/TCP segment layer 4 and IP packet Layer 3 and an Ethernet frame Layer 2 before transmission, revealing details like port numbers that's UDP 53 for DNS and IP addresses in the PDU

Step 1: (d) The outbound PDU Details tab



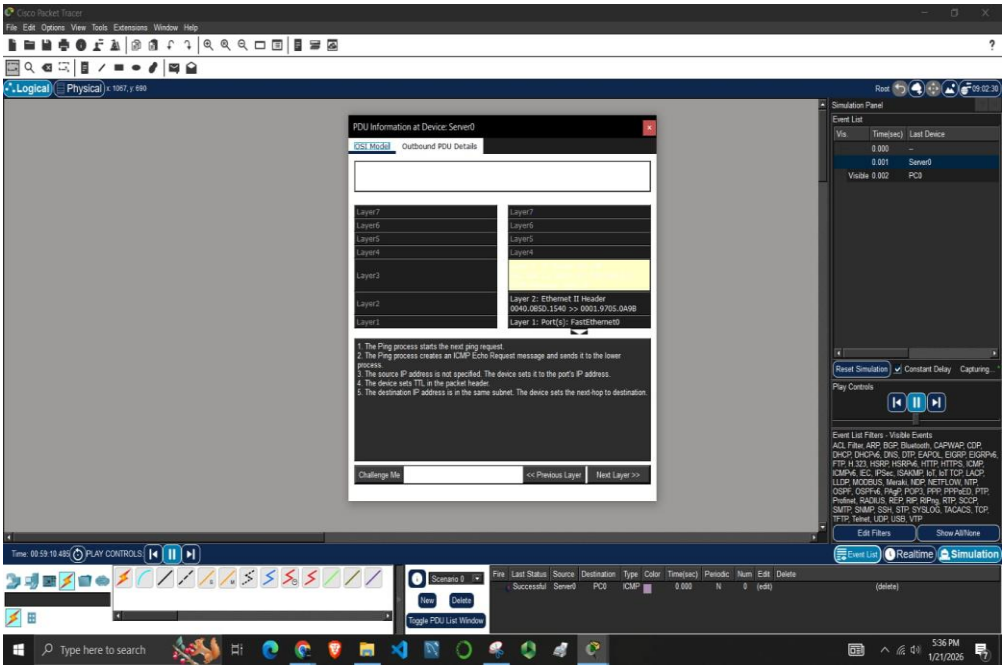
The name which is in the field lists is the fully qualified domain name that the client is trying to resolve which is www.osi.local which I enter in the browser indicating the domain being looked up

Step 1: (e) The last DNS in the coloured



When click the DNS- coloured box the PDU was captured at the web client and the value next to ADDRESS in the DNS ANSWER section of the inbound PDU Details will be the IP Address of the Web Server which it receives the servers IP for the requested domain.

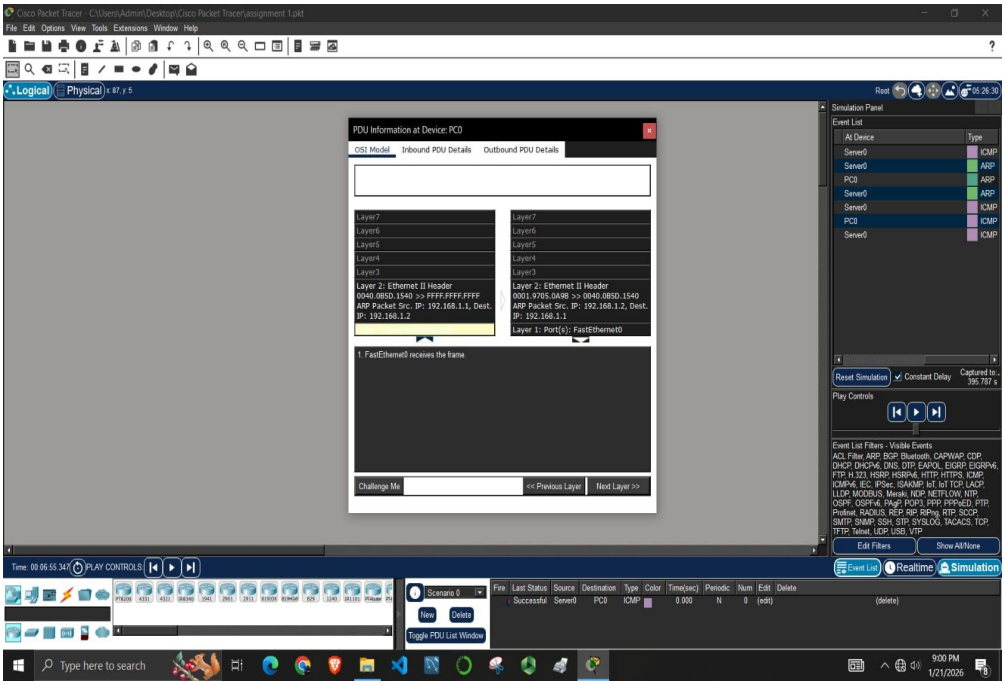
Step 2: (f) The first HTTP event in the list



After finding the first HTTP event and clicking the following TCP events coloured box, then highlighting Layer 4 in the OSI Model tab hence the information under items 4 and 5 in the

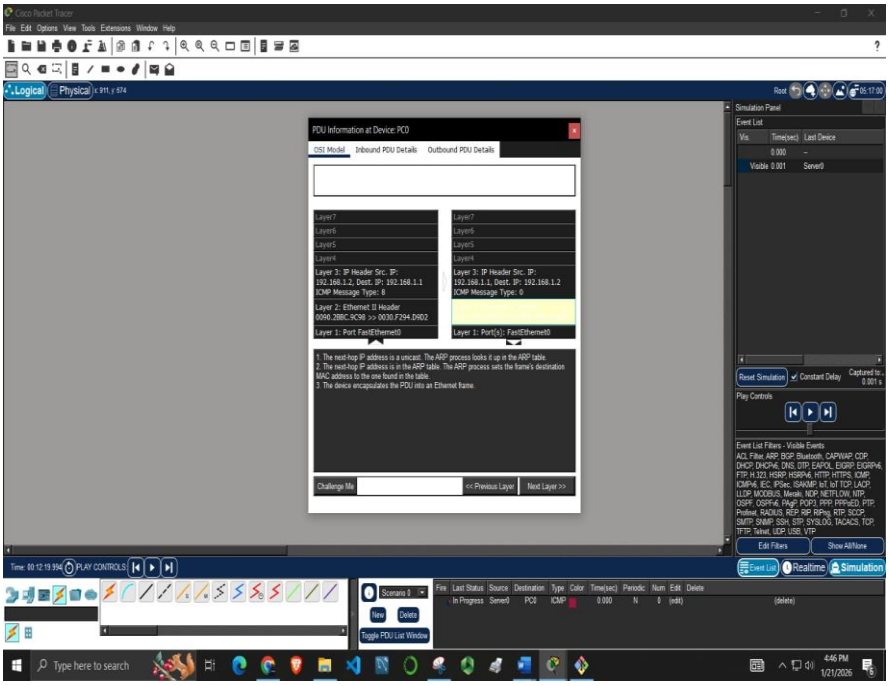
list below in layers and out layers is 4 ,the TCP connection is successful and 5, the device sets the connection state to indicate a successful three-way handshake for communication

Step 2: (g) The last TCP event



This shows purpose is to gracefully terminate the established connection (session) between the client and server. The layers section at Layer 4 would show the FIN flag being set, which indicates the sender wants to close the connection, and the out layers would show the ACK for that FIN which will complete the shutdown process

The Challenge Questions



Based on the information I typically found in a packet tracer simulation and general networking standards, the web server listens on the following ports:
For the web request (HTTP), the server is listening on port 80 while for the DNS request the server is listening on port 53
The transport layer 4 uses these port numbers to direct incoming data to the correct service running on the server. The source port for the client is a dynamically assigned ephemeral port but the destination ports on the server are the standard well known ports for these services

Conclusion

This week I gained a good grounding on the introductory concepts relating to Packet Tracer- investigating the TCP/IP and OSI Model in Action. I am getting a better understanding that I can build on as we work on more advanced concepts in later weeks.