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

RENE OLUOCH

CS-CNS09-25030

Contents

Introduction

As part of my assignment and exploration into computer networking concepts, I undertook a hands-on investigation using Cisco Packet Tracer to deepen my understanding of the **TCP/IP and OSI reference models**. The aim was to observe how data, particularly HTTP and DNS traffic, flows across various layers of these models during real-world network communication. This practical activity not only solidified my theoretical knowledge but also provided an insightful look into how packets are encapsulated, transmitted, and interpreted across devices in a simulated network environment. Through active experimentation and step-by-step packet analysis, I was able to witness key networking principles come to life.

Part 1: Examining HTTP Web Traffic

Step 1: Switching to Simulation Mode

I began by switching from Realtime to Simulation mode in Packet Tracer and filtered events to only display HTTP traffic.
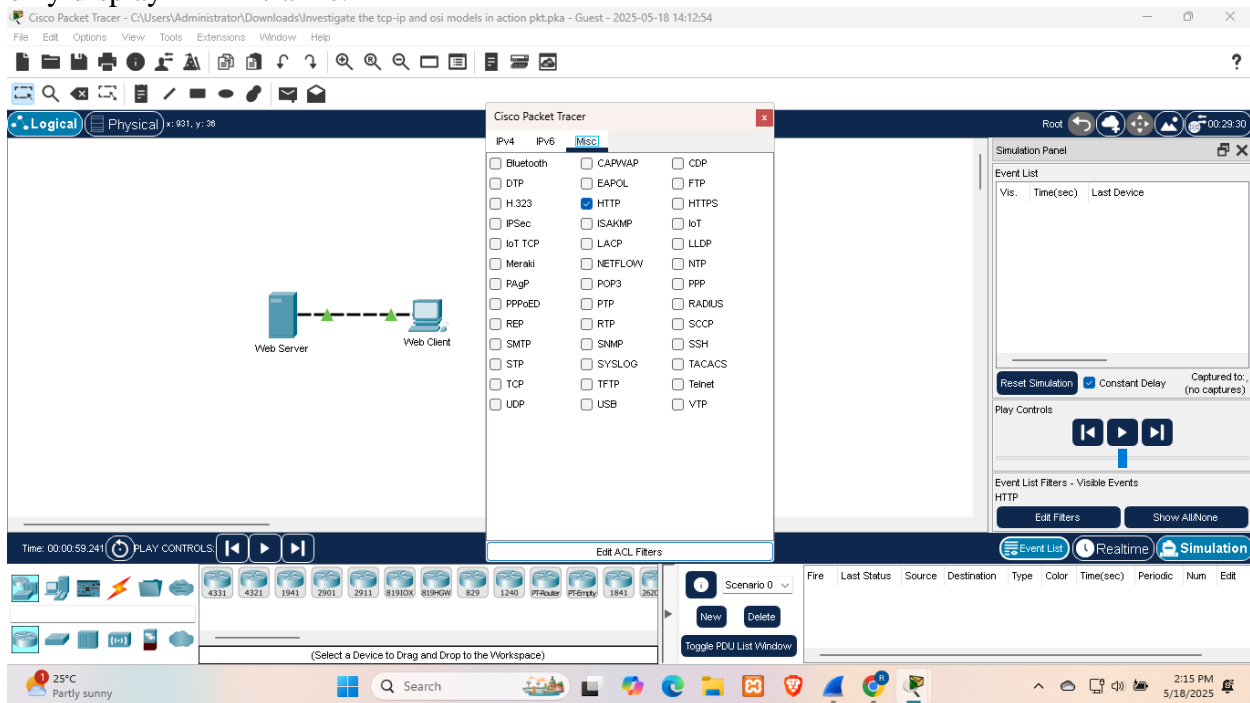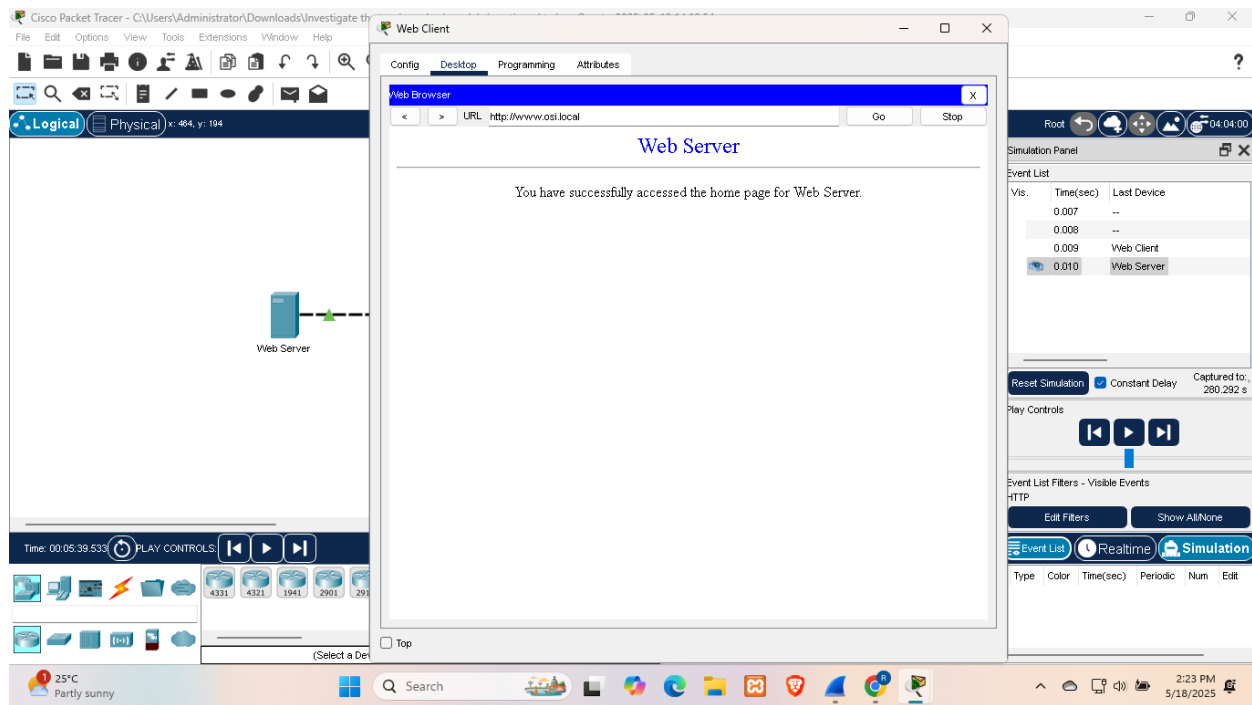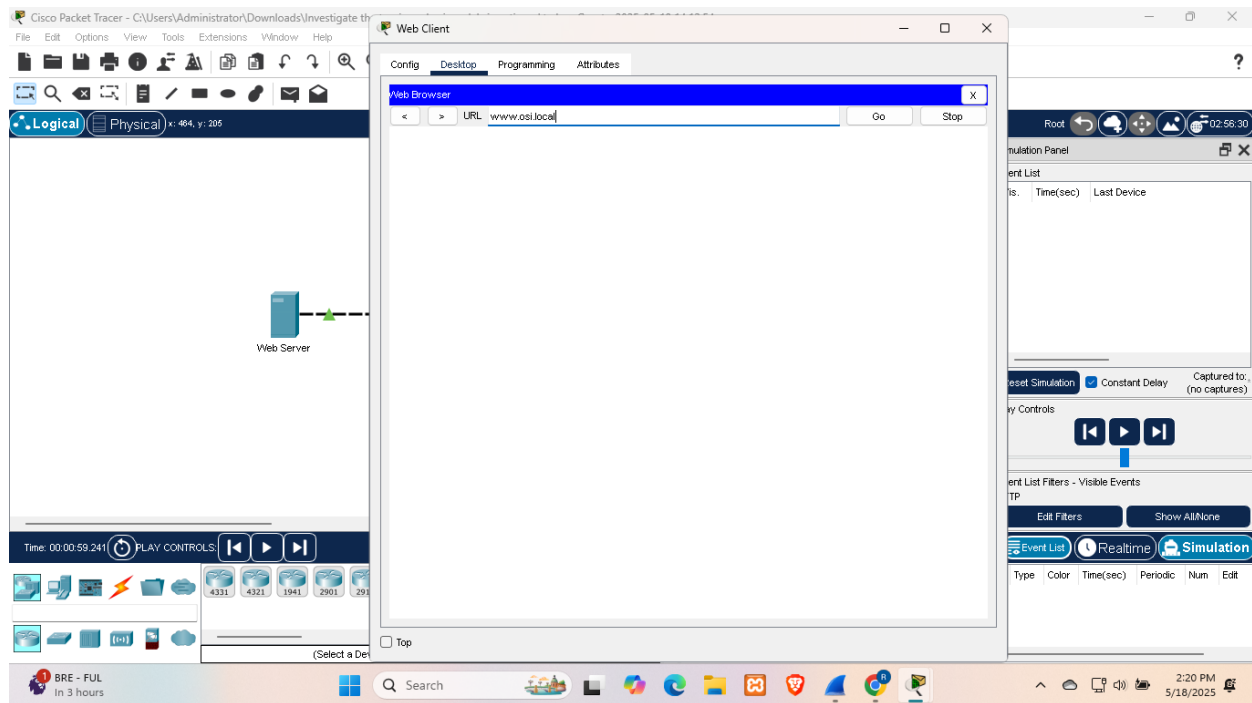

Generating HTTP Traffic

1. I launched the Web Browser on the client PC.
2. Entered the URL: www.osi.local and clicked **Go**.
3. I then clicked **Capture/Forward** four times to simulate and trace the request.

Observation:
After forwarding the events, the web page successfully loaded with the message:
"You have successfully accessed the home page for Web Server."

Analyzing the HTTP Packet

I examined the encapsulated HTTP packet at various OSI layers:

- **Layer 7 (Application Layer):**
  "The HTTP client sends an HTTP request to the server."
- **Layer 4 (Transport Layer – TCP):**
  Destination Port: **80** (standard for HTTP)
- **Layer 3 (Network Layer – IP):**
  Destination IP: **192.168.1.254**
- **Layer 2 (Data Link Layer – Ethernet):**
  An ARP request was made to resolve the MAC address, after which the frame was encapsulated into Ethernet format.

What is the text displayed next to the **Layer 7** label?

The displayed text is "The HTTP client sends an HTTP request to the server."

What information is listed in the numbered steps directly below the In Layers and Out Layers boxes?- The numbered steps under the Out Layers column included

- **Layer 4:** Sent segment info — sequence number 1, ACK number 1, data length 102.
- **Layer 3:** Destination IP is in the same subnet; next-hop is set to destination.
- **Layer 2:**
  1. Next-hop IP is a unicast. ARP process looks it up in the ARP table.
  2. IP is found in ARP table; sets frame's destination MAC address accordingly.
  3. Device encapsulates the PDU into an Ethernet frame.
- **Layer 1:** FastEthernet0 is busy; frame is buffered to be sent later.
  (Note: In Layers column is inactive for this first event.)

The Destination port value is 80

The What is the destination IP address value is 192.168.1.254
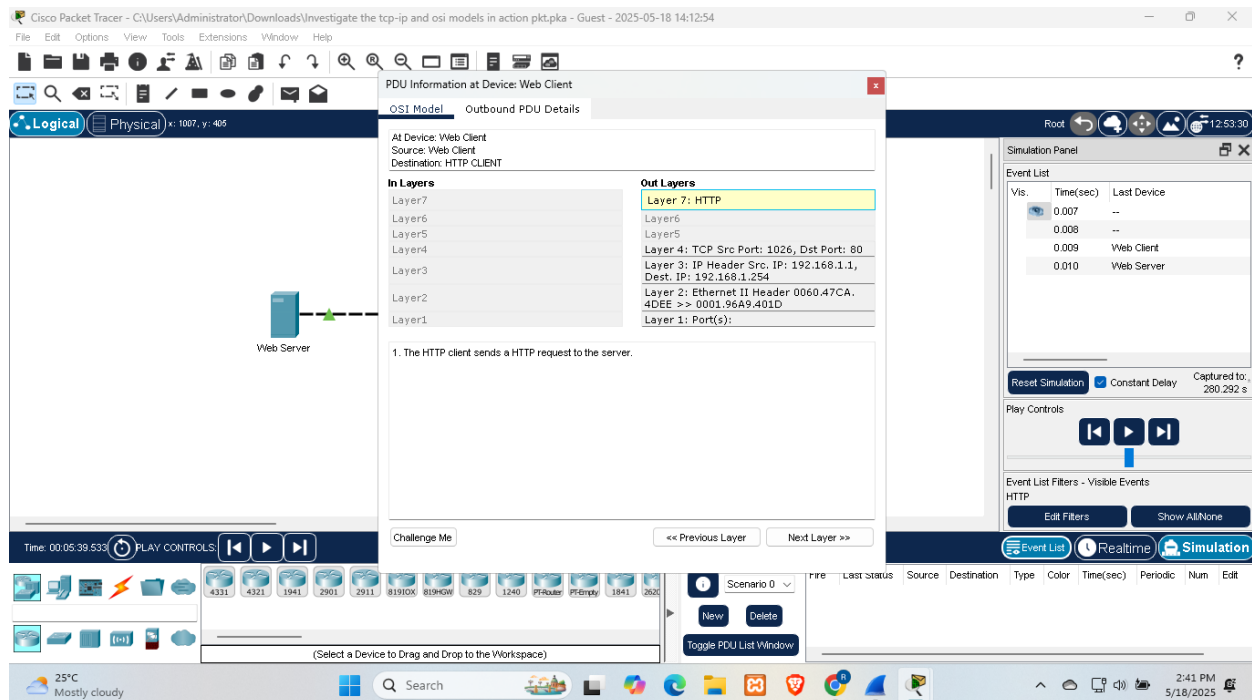
Osi layer details

What information is displayed at this layer?
(Under Layer 2 in the OSI Model tab)

☐ The next-hop IP address is a unicast. The ARP process looks it up in the ARP table.

☐ The next-hop IP address is in the ARP table. The ARP process sets the frame's destination MAC address to the one found in the table.

☐ The device encapsulates the PDU into an Ethernet frame.

Outbound PDU Details:

What is the common information listed under the IP section of the PDU Details compared to the OSI Model tab, and with which layer is it associated?

- The IP section of the PDU Details includes the Source and Destination IP addresses, which is the same as what is shown under Layer 3 of the OSI Model tab.
Associated Layer: Layer 3 (Network Layer)

- **HTTP Section:**
  - Request
  - Host: www.osi.local

What is the **Host** listed under the HTTP section of the PDU Details?
What OSI layer is it associated with?

- Host**:** www.osi.local
Associated OSI Layer**:** Layer 7 (Application Layer)

- **TCP Section:**
 - Source Port: Random high number (e.g., 1026)
  - Destination Port: 80

What is the common information listed under the TCP section of the PDU Details, **and** with which layer is it associated?

- The TCP section includes the Source and Destination Port numbers, matching the information shown under Layer 4 in the OSI Model tab.
Associated Layer: Layer 4 (Transport Layer)

- **IP Section:**
  - Source IP: Client's IP
  - Destination IP: 192.168.1.254
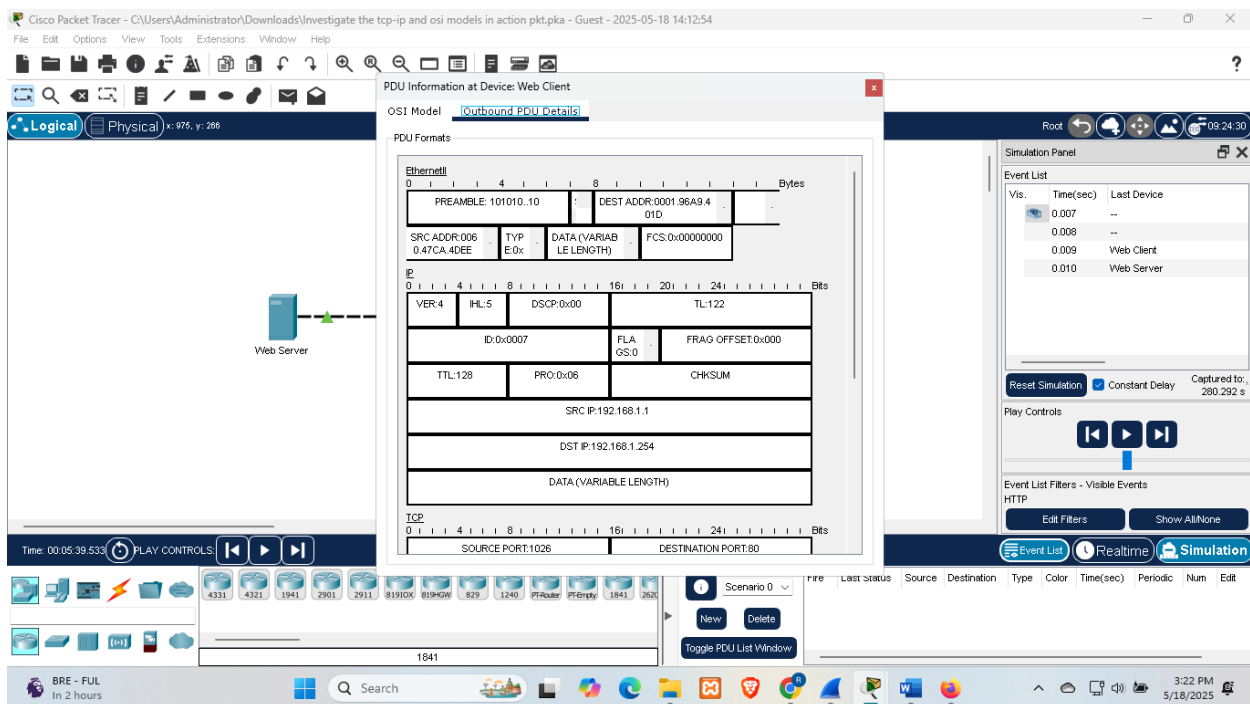
Inbound HTTP Response:

☐ For the outbound HTTP response, the first line is:
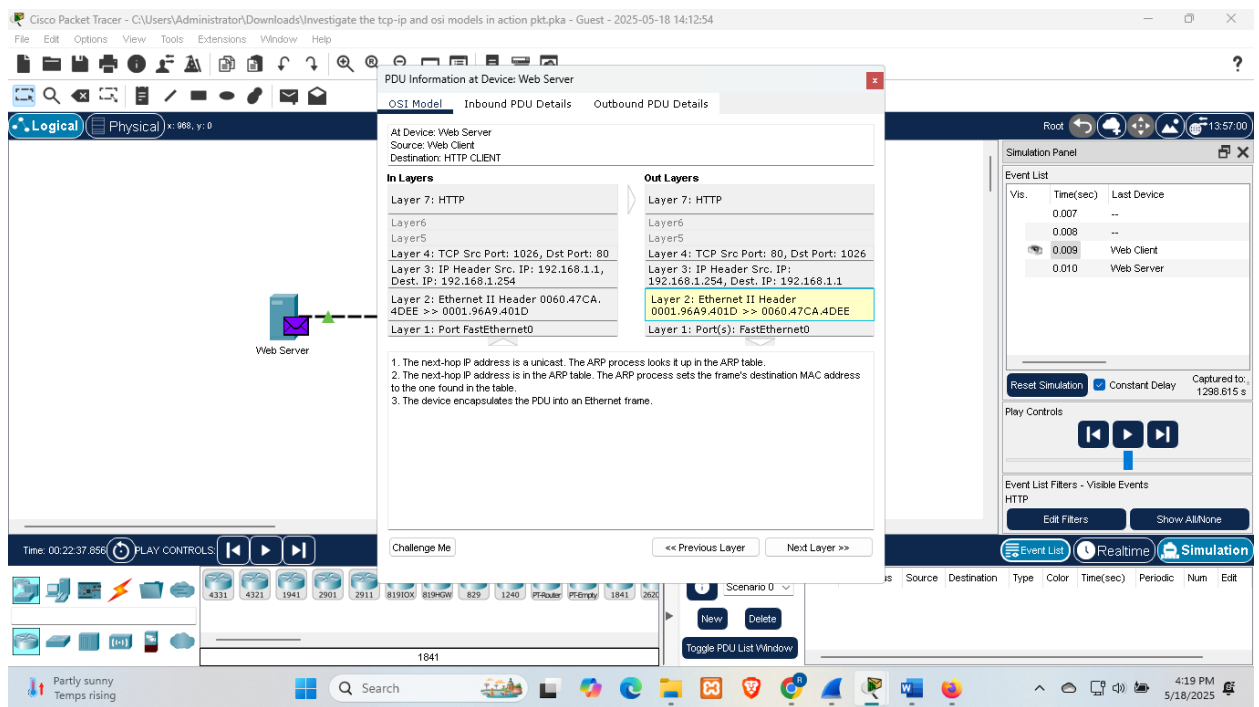HTTP Data: Connection: close Content-Length: 170

☐ For the inbound HTTP request, the first line is:
HTTP Data: Accept-Language: en-us Accept: */*

Key Observation:

- The inbound and outbound layers reflected a reversal of source/destination addresses and

  ports.

Comparing the In Layers and Out Layers columns, what are the major differences?-

The major differences between the In Layers and Out Layers columns are that the Source and Destination Ports, IP Addresses, and Ethernet II headers (MAC addresses) are reversed. This reflects the server responding to the client — reversing the direction of communication.

What is the first line in the HTTP message that displays?-

☐ For the outbound HTTP response, the first line is:
HTTP Data: Connection: close Content-Length: 170

☐ For the inbound HTTP request, the first line is:
HTTP Data: Accept-Language: en-us Accept: */*

How many tabs are displayed with this event, and why?

There is 1 active tab: Inbound PDU Details.

Why?
This is the final event in the HTTP flow, where the server sends the last response to the client.
Only the inbound data is displayed, and the Out Layers are grayed out because there's no further
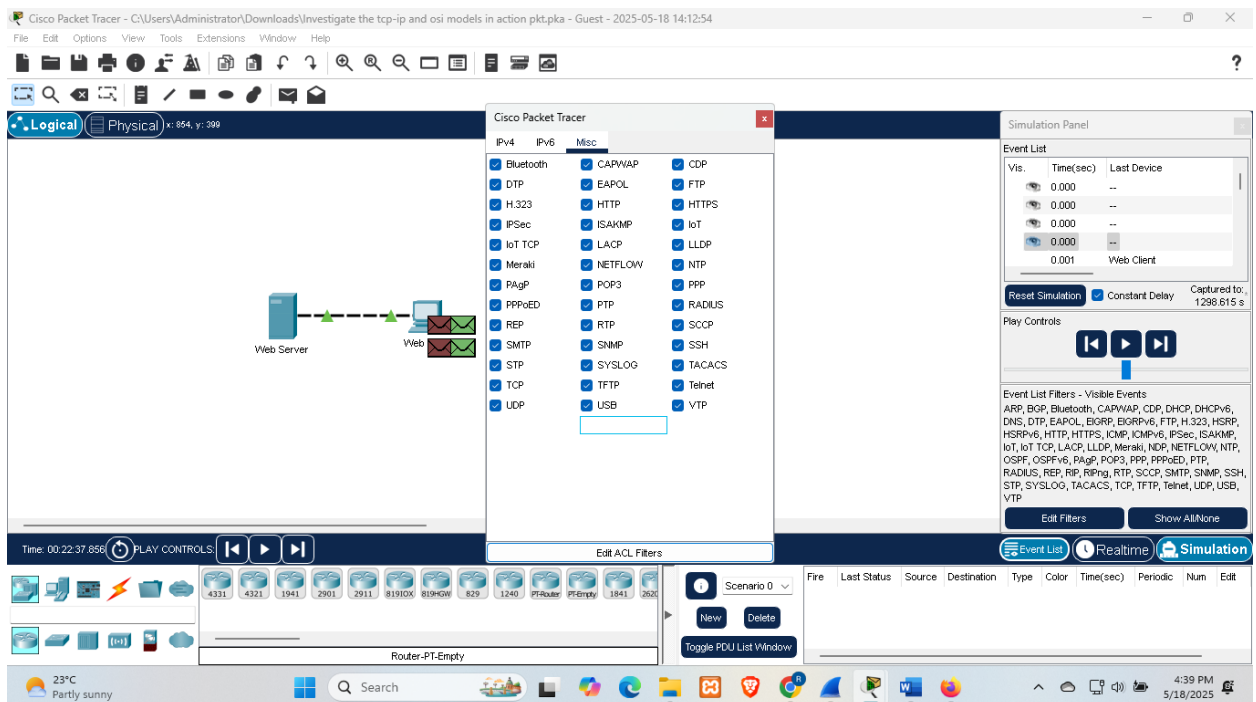encapsulation — the packet has reached its destination.

Part 2: Exploring the TCP/IP Protocol Suite

Step 1: Viewing Additional Protocols

I enabled **"Show All"** in the Event List Filters to expand visibility and noticed additional
protocol activity:

- **DNS** (Domain Name System)
- **ARP** (Address Resolution Protocol)
- **TCP** and many more as in the screenshot below

DNS Analysis

What information is listed in the NAME field of the DNS query

1. The client initiated a DNS query:
    - o **NAME:** www.osi.local
    - o **ADDRESS:** 192.168.1.254 (resolved by the DNS server)

The device that is displayed in the last DNS Info event is the web server

 What is the ADDRESS**:** value in the DNS ANSWER section of the Inbound PDU Details? - 192.168.1.254
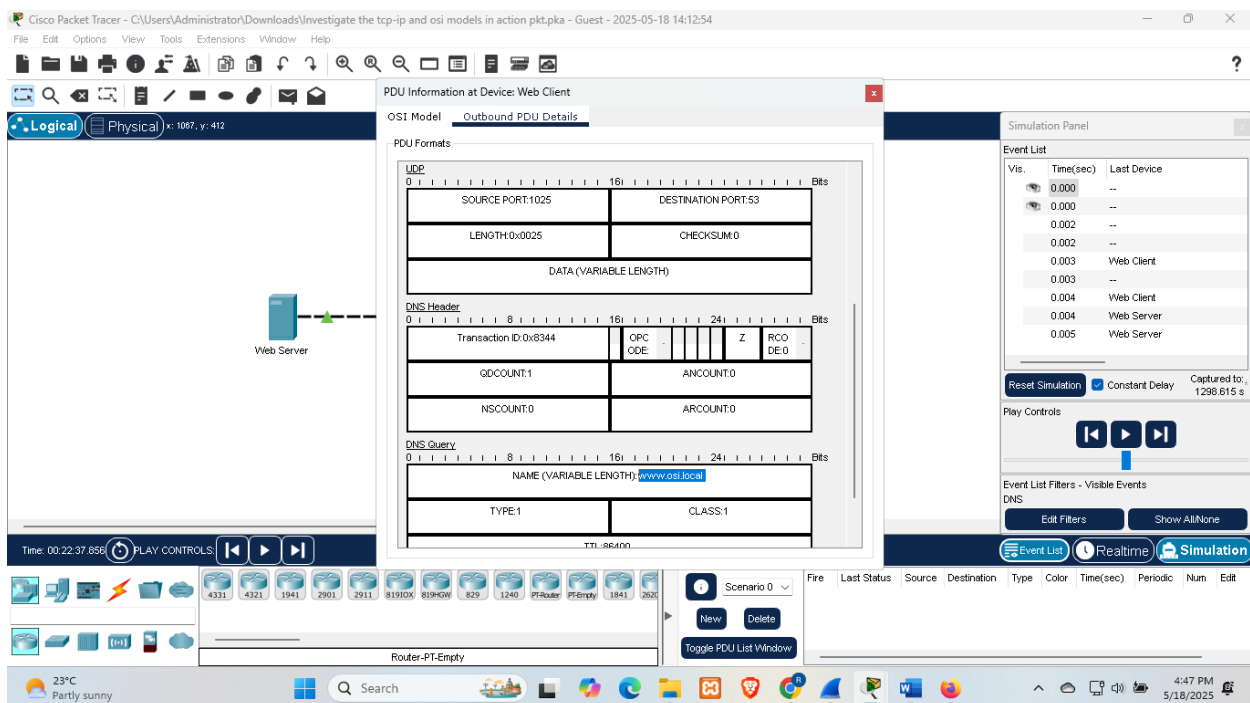
TCP Connection Process

 In the TCP event immediately after the first HTTP event, what is displayed under items 4 and 5 **in** Layer 4 of the OSI Model tab?

The last two lines, which are 4 and5 display;

 4. "The TCP connection is successful."
5. "The device sets the connection state to ESTABLISHED."

What is the purpose of the last TCP event, based on the description under Layer 4 (item 4)

- The purpose of the last TCP event is to terminate the TCP connection. Item 4 states: *"The device sets the connection state to CLOSED."*

This indicates that the TCP session is being properly closed after the communication is complete.
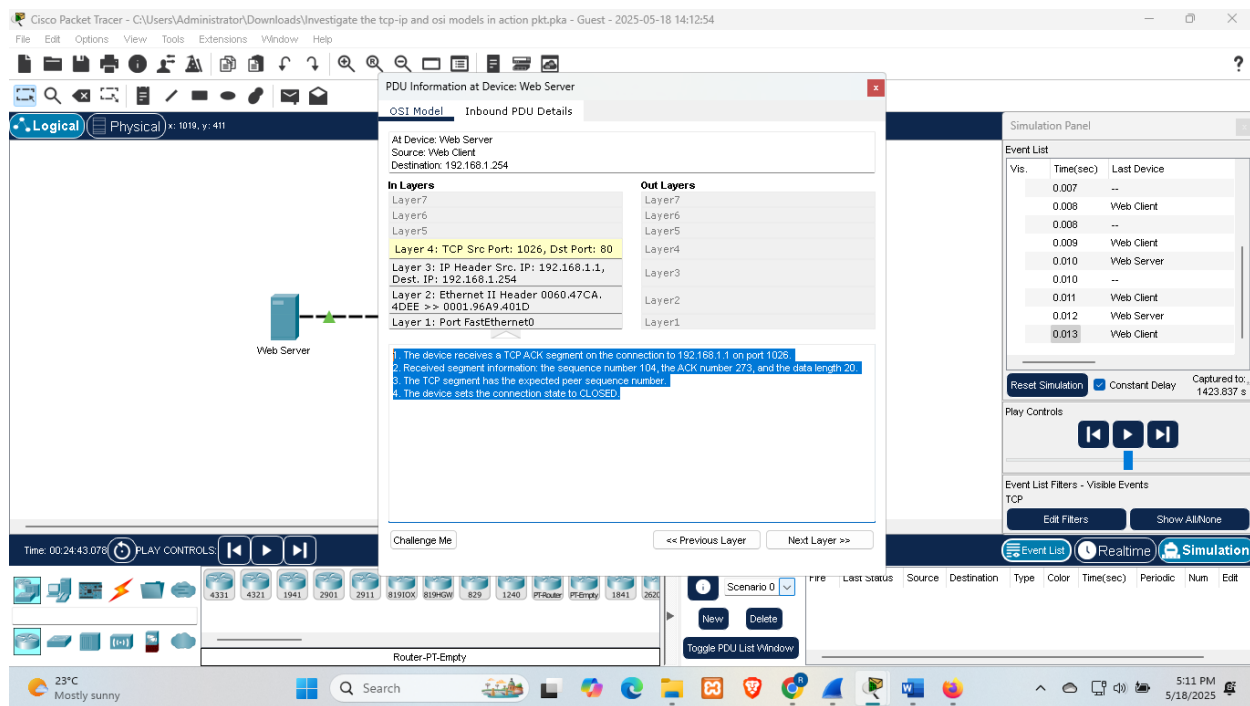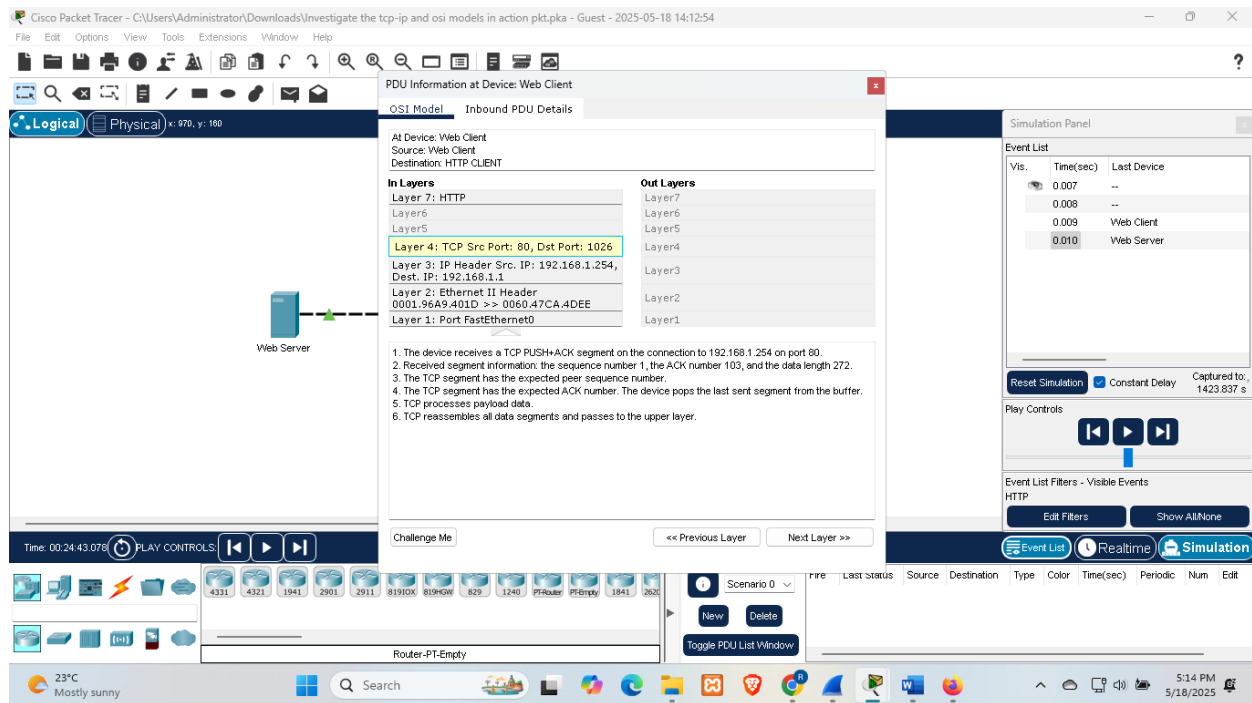

Challenge Questions & Findings

1. **Web Server Listening Ports:**
   o HTTP (Web Traffic): Port 80
   o DNS Requests**:** Port 53

Verification:
I verified that the web server listens via port 80 for web traffics and port 53 for DNS requests by inspecting the Transport Layer (Layer 4) of the OSI Model tab.

Conclusion

This Packet Tracer simulation was an eye-opening experience that allowed me to explore and understand how real-world web traffic and DNS lookups traverse the layered architecture of TCP/IP and OSI models. I observed firsthand how HTTP requests are constructed and transmitted, how the DNS protocol assists in name resolution, and how TCP manages reliable communication through its state transitions.

By breaking down packets at each OSI layer, I was able to clearly see the encapsulation and de-encapsulation processes that are fundamental to networking. These insights reinforced my grasp of critical concepts like port numbers, IP addressing, ARP, and TCP connection states. Ultimately, this lab gave me not just theoretical comprehension but also practical exposure to the inner workings of data communication over networks, an essential step in my journey to becoming proficient in network technologies.