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

Philiphine Cheptanui

CS-CNS09-25161

CyberShujaa

Cloud and Network Security - C2- 2025

Samwel Katana

Wednesday, 21 May 2025, 12:00 AM

Contents

Introduction

In this assignment, I explore how the TCP/IP and OSI Models work. Simulating real-world networking scenarios allowed me to understand how data is encapsulated and transmitted across network layers and how various protocols interact to aid transmission and successful communication. Specifically, I explored and analysed HTTP web traffic using the Simulation mode in Packet Tracer and observed how different protocols interact to facilitate communication. This hands-on activity allowed me to visualize the encapsulation process and the relationship between the OSI and TCP/IP models. In part 1, I examined HTTP traffic by generating a web request from a client to a server. I used Packet Tracer Simulation mode and observed HTTP traffic, analyzed PDU in different OSI layers, and compared Inbound Details and Outbound Details. Key aspects of network traffic observed include the ports, IP addresses, and MAC addresses. Additionally, the activity allowed for an understanding of how HTTP requests and responses are organized in a network environment.

In Part 2, I observe key TCP/IP protocols including DNS, ARP, and TCP. I was able to observe how DNS resolves domain names to IP addresses, how ARP maps IP addresses to MAC addresses, and how TCP manages connection establishment and termination. Overall, I was able to understand and visualize network communication and interpret network traffic, understand how encapsulation works, how protocols interact to communicate with one another, and the layered structure of network communication models.

Discussion

Part 1: Examine HTTP Web Traffic

Part 1 of the activity sought to examine HTTP traffic. In this activity, I generate web traffic and examine HTTP using Packet Tracer (PT) Simulation mode.

D. Click **Capture/Forward** four times. There should be four events in the Event List.

Look at the Web Client web browser page. Did anything change? *Yes. The web client has displayed "You have successfully accessed the home page for Web Server" (Fig. 1)*

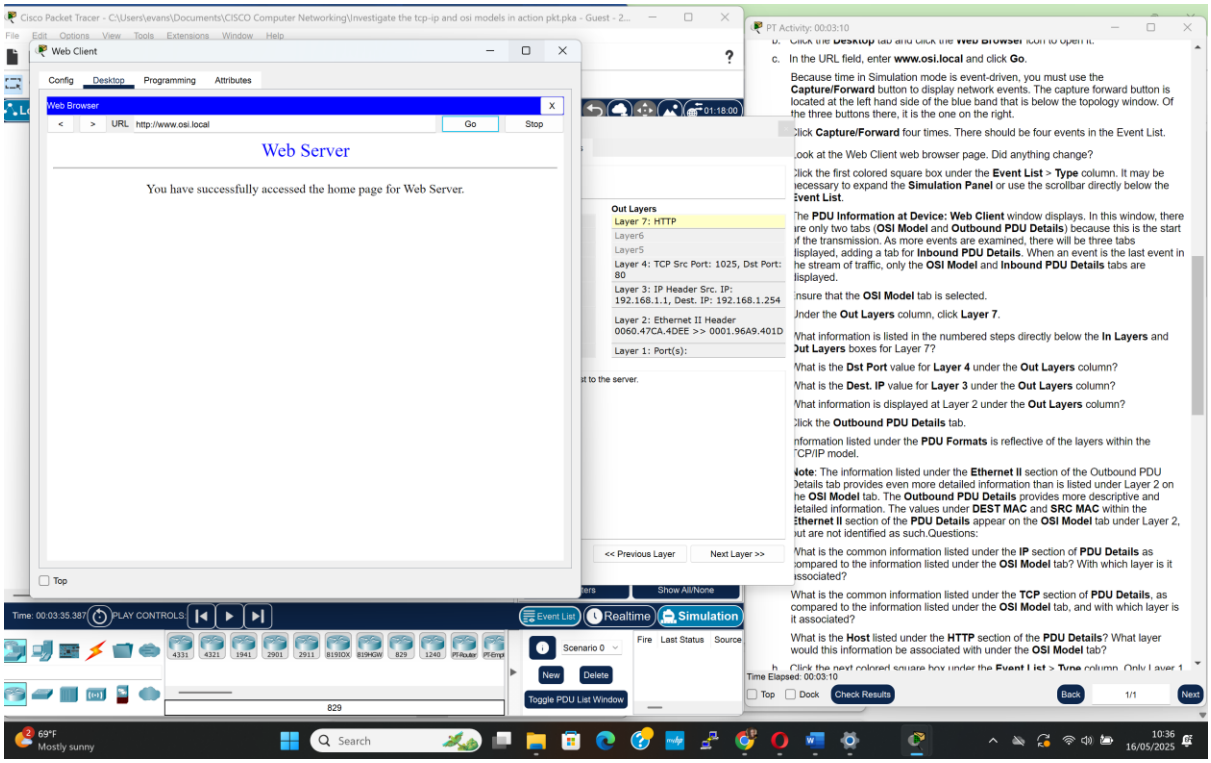

Figure 1. Source: Learner

F. What information is listed in the numbered steps directly below the **In Layers** and **Out Layers** boxes for Layer 7?

The information given for layer 7 under Out Layers is "1. The HTTP client sends an HTTP request to the server." (Fig.2)

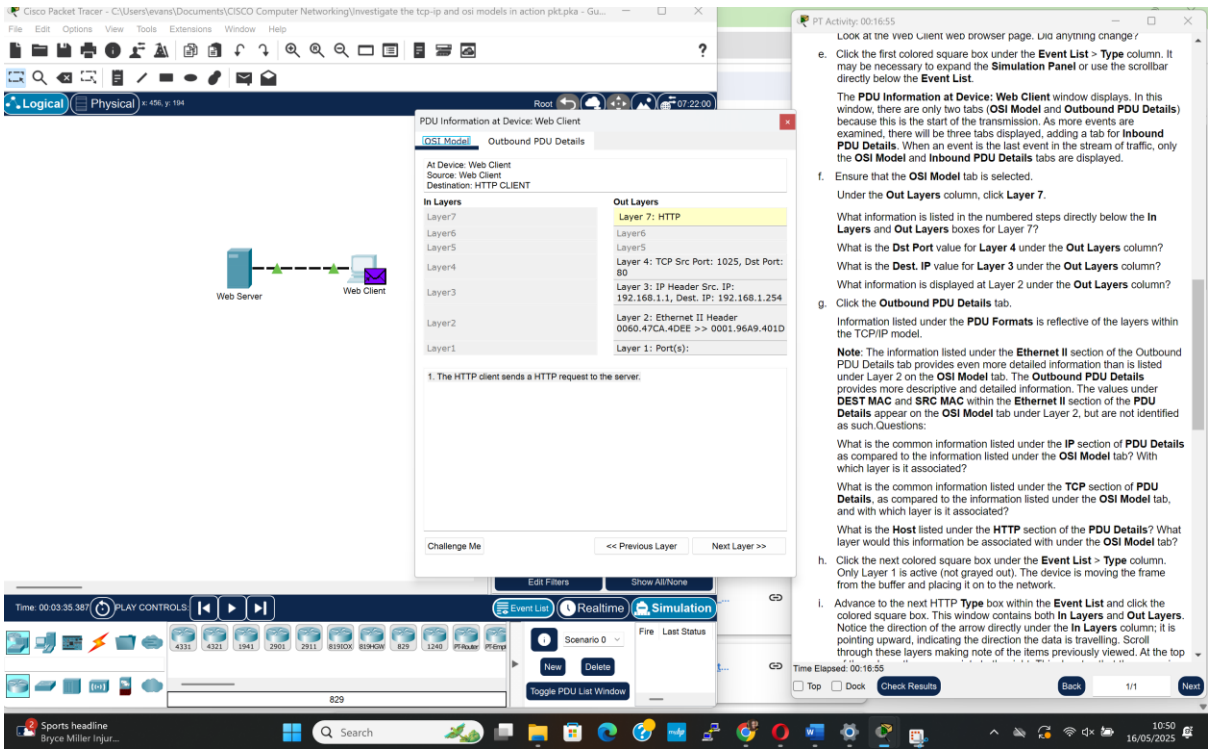

Figure 2. Source: Learner

What is the **Dst Port** value for **Layer 4** under the **Out Layers** column?

The destination port value for layer 4 under the Out Layers is 80 (Fig. 3)

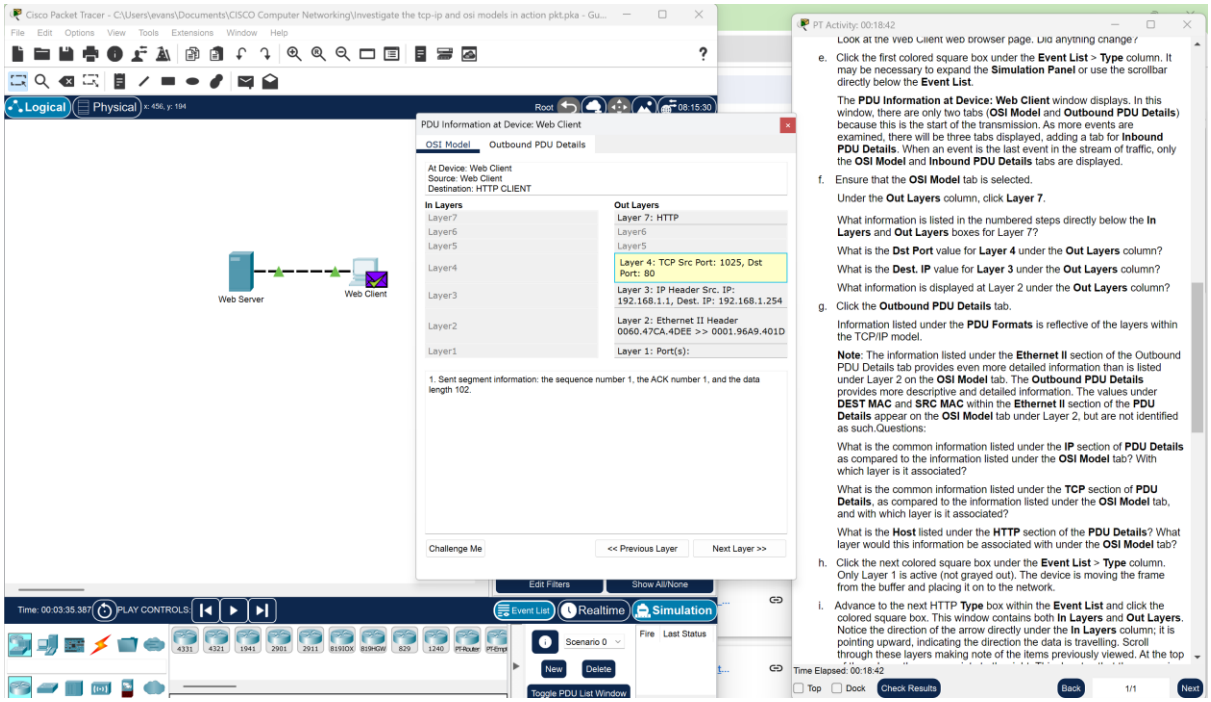

Figure 3. Source: Learner

What is the **Dest. IP** value for **Layer 3** under the **Out Layers** column?

The destination IP value for layer 3 under the Out Layers column is 192.168.1.254 (Fig.4)

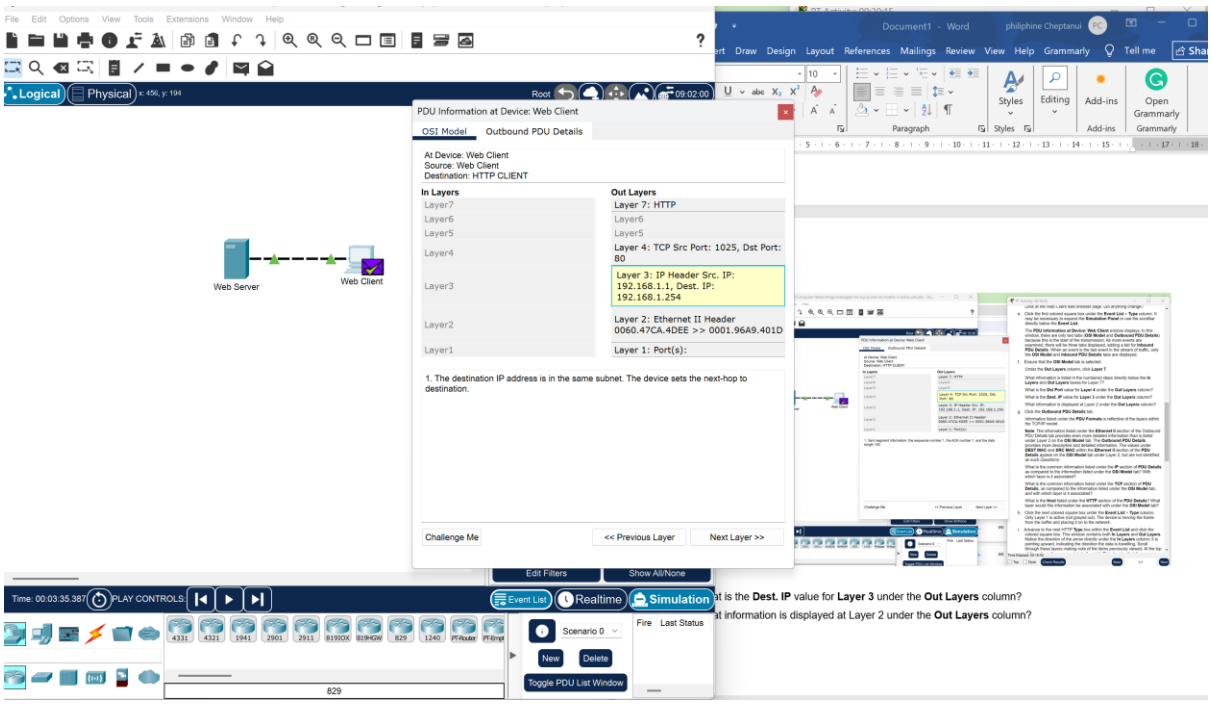

Figure 4. Source: Learner

What information is displayed at Layer 2 under the **Out Layers** column? *(Fig.5)*

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

2. 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.

3. The device encapsulates the PDU into an Ethernet frame.

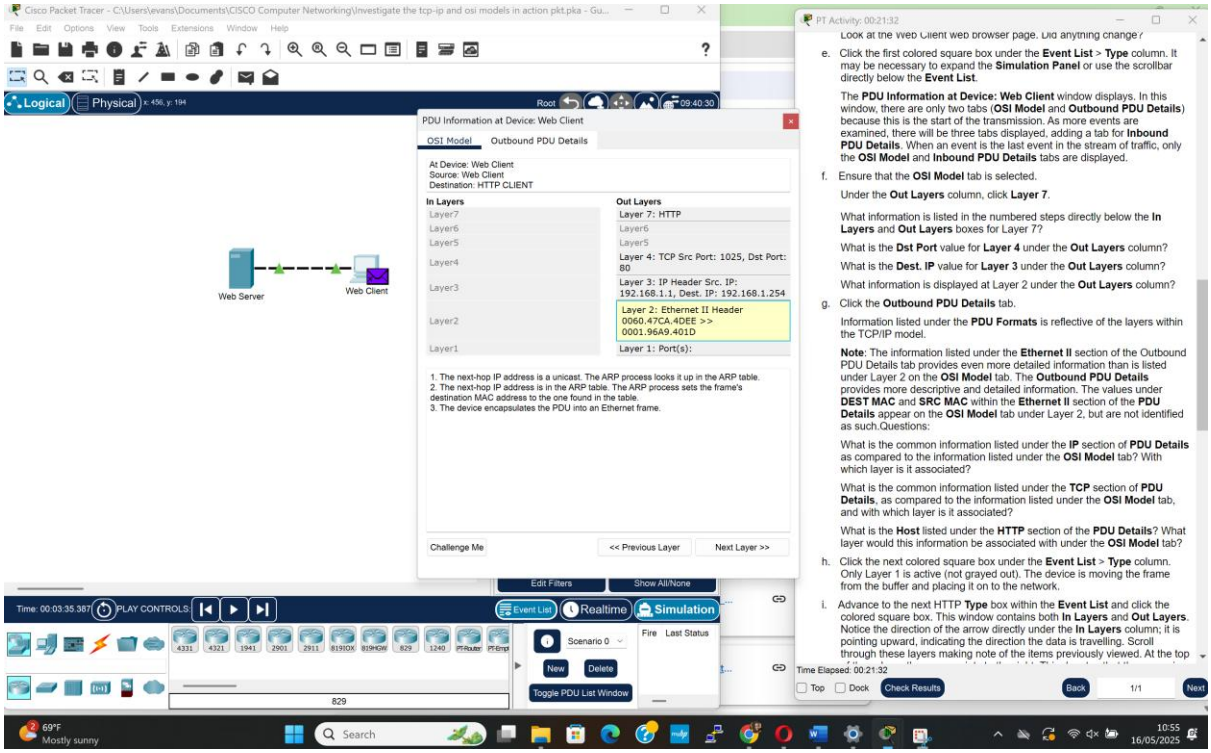

Figure 5. Source: Learner

G. What is the common information listed under the **IP** section of **PDU Details** as compared to the information listed under the **OSI Model** tab? With which layer is it associated?

The common information listed under the IP section of PDU details, as compared to the information listed under the OSI model include IP version (4), IP Header Length (IHL5), time to live total length (TL 122), 16-bit identification (0x0004), flag and fragmentation (splits large messages into IP packets), 13-bit flag offset (0x000), Time to Live (TTL 128 hops), protocol (PRO 0x06), checksum, source IP, destination IP and data to be sent to the receiving node. However, the OSI model only gives source and destination IP addresses. This information is associated with Layer 3 of the OSI model. (Fig.6)

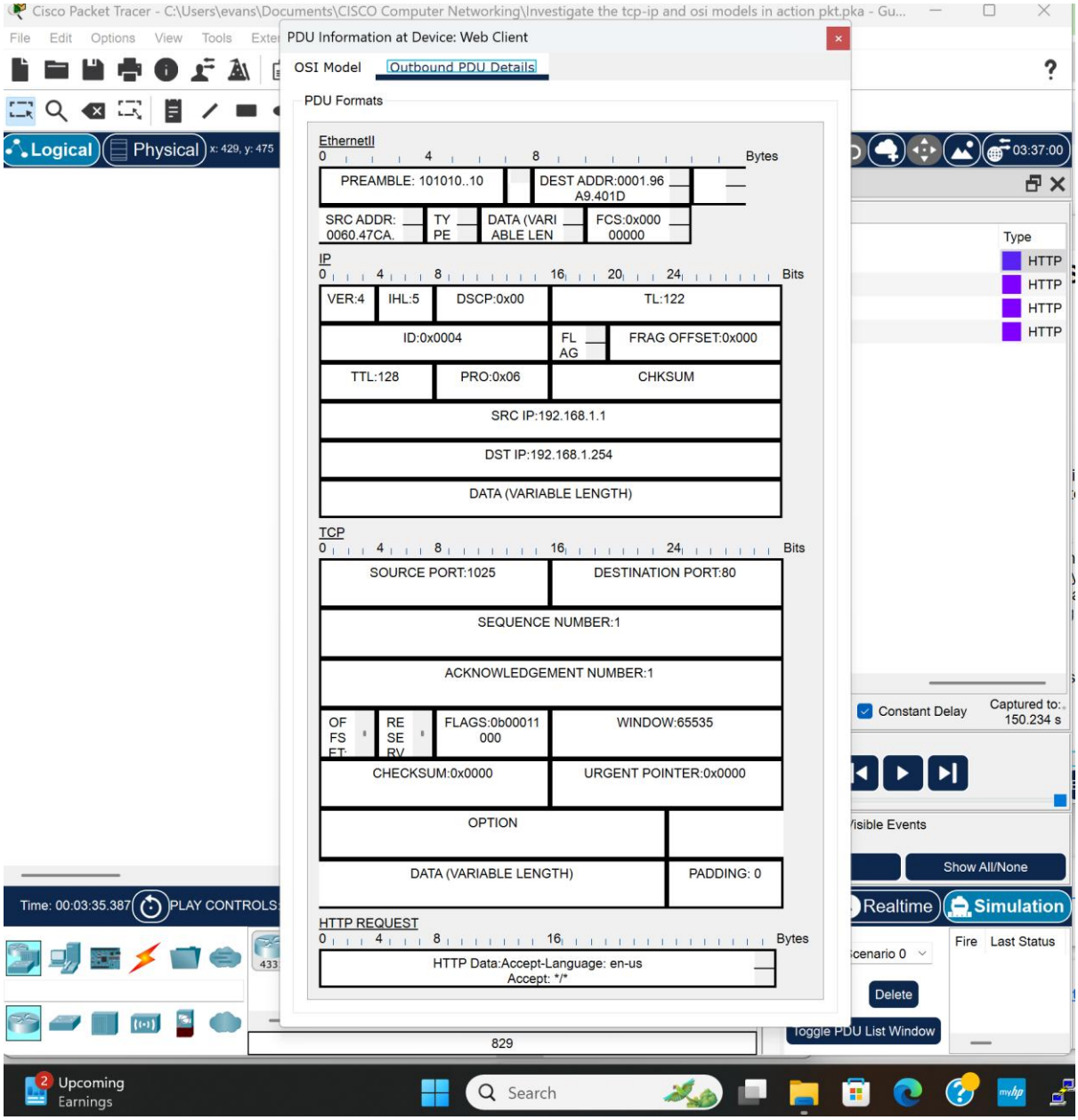

Figure 6. Source: Learner

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

In the Out Layers' TCP section, detailed information about ports is given. They include source and destination ports, sequence number (1), acknowledgement number (1), data offset, reserved bits, control flags (0b00011000), window size (65535), checksum (0x0000), urgent pointer (0x0000), optional data, data to be sent to the receiving node and padding (0). Unlike the TCP model, the OSI model only shows the source port and the destination port. The TCP details are associated with layer 4 of the OSI model. (Fig.7)

What is the **Host** listed under the **HTTP** section of the **PDU Details**? What layer would this information be associated with under the **OSI Model** tab?

The Host listed under the HTTP section of the PDU Details is www.osi.local. This information is associated with layer 7.

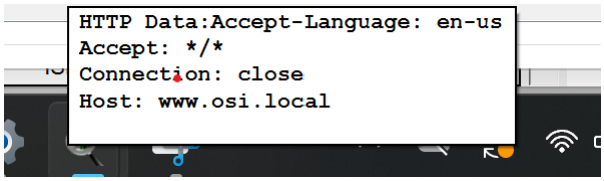

Figure 7. Source: Learner

I. Comparing the information displayed in the **In Layers** column with that of the **Out Layers** column, what are the major differences?

The information in the In Layers is slightly different from the information in the Out Layers. In the In Layers, the destination MAC address is 0060.47CA.4DEE, and is the source MAC address in the Out Layers layer two. This also applies to the In Layers layer 2 source MAC address (0001.96A9.401D), which is the destination MAC in layer 2 of Out Layers. In layer 3, the source IP address (192.168.1.1) and the destination IP address (192.168.1.254) in the In Layers become the destination and source IP addresses in the Out Layers, respectively. This trend also applies to layer four in that the source and destination ports in the In Layers become the destination and source ports in the Out Layers. (Fig.8)

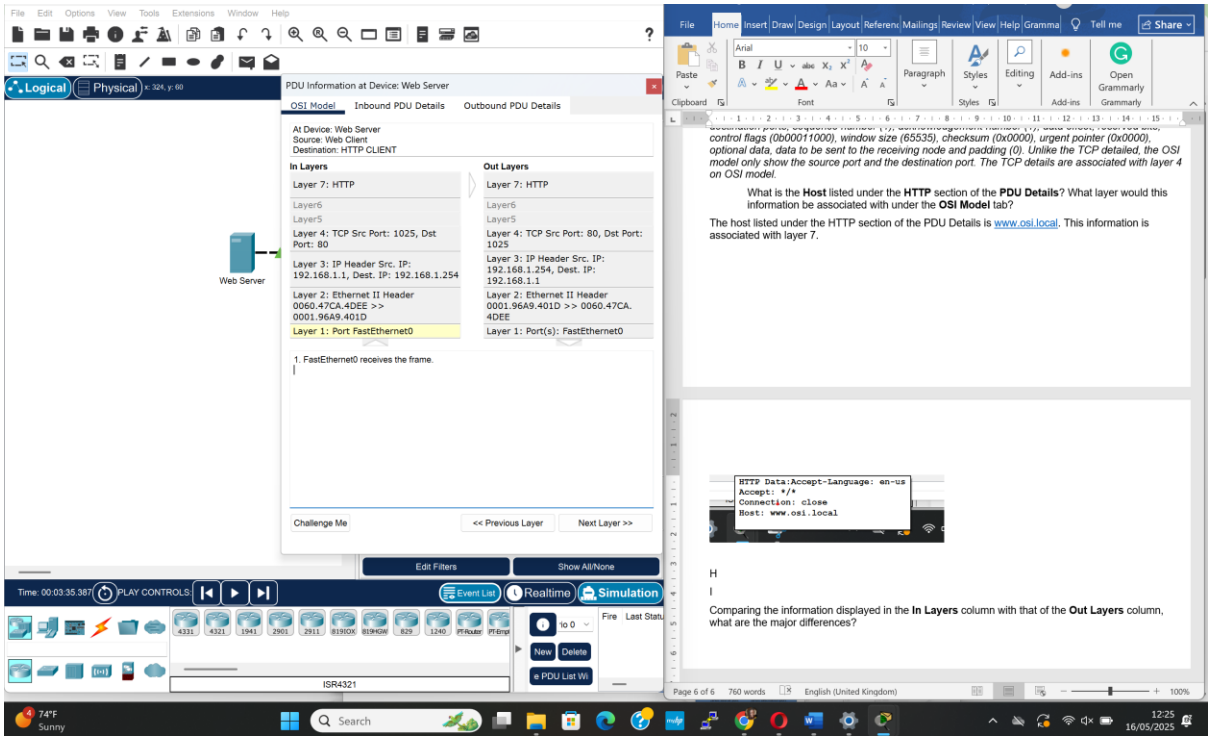

Figure 8. Source: Learner

K. Click the last coloured square box under the **Info** column. How many tabs are displayed with this event? Explain.

The last-coloured square is the last event and has two tabs only, which are the OSI model and the Inbound PDU details. It has two tabs alone because the device is at the endpoint and only receives the PDU. The intermediate events have three tabs – the OSI model, Outbound PDU details, and Inbound PDU details. The first event has the OSI model and the Outbound PDU details because it is at the start of transmission. (Fig.8)

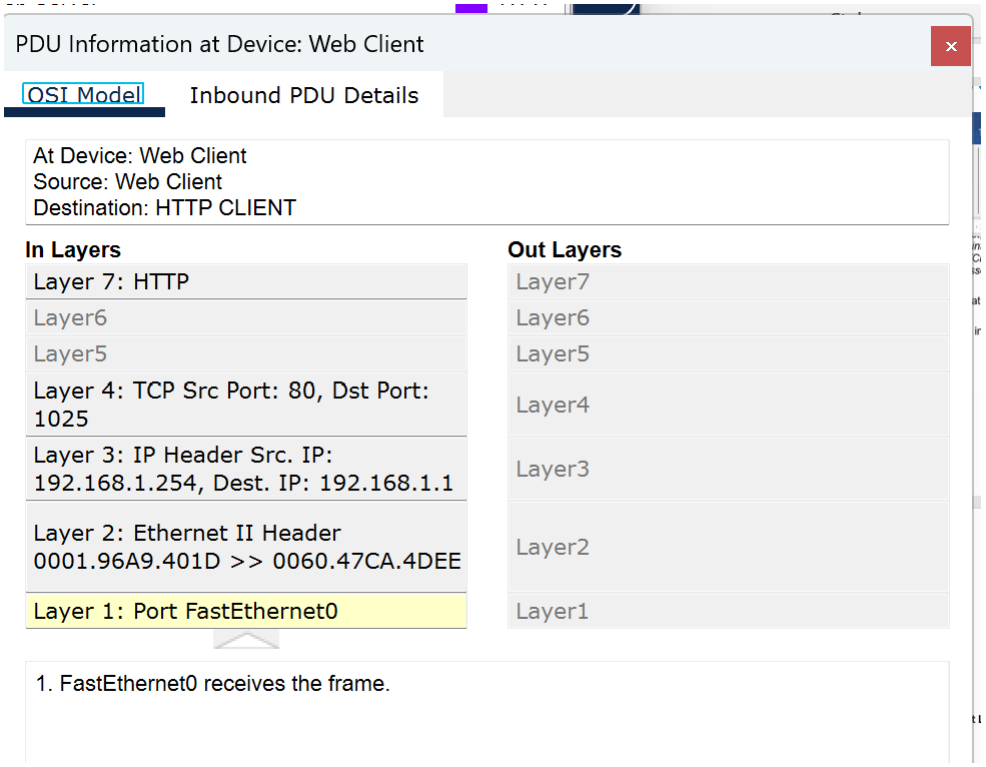

Figure 9. Source: Learner

Part 2: Display Elements of the TCP/IP Protocol Suite

Part 2 of the activity required the learner to use the Packet Tracer Simulation mode to view and examine some of the other protocols comprising of TCP/IP suite.

B. What additional Event Types are displayed?

Several extra entries are displayed. (Fig.10)

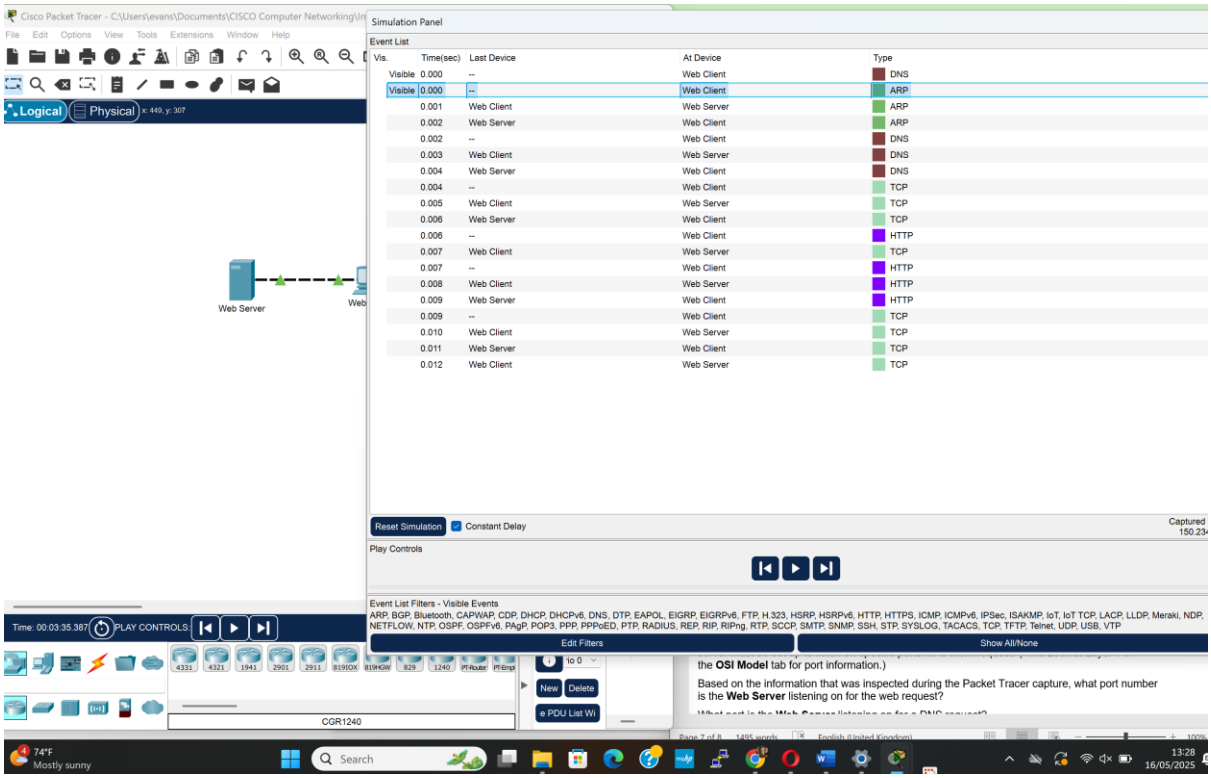

Figure 10. Source: Learner

D. What information is listed in the **NAME** field: in the DNS QUERY section?

www.osi.local (Fig.11)

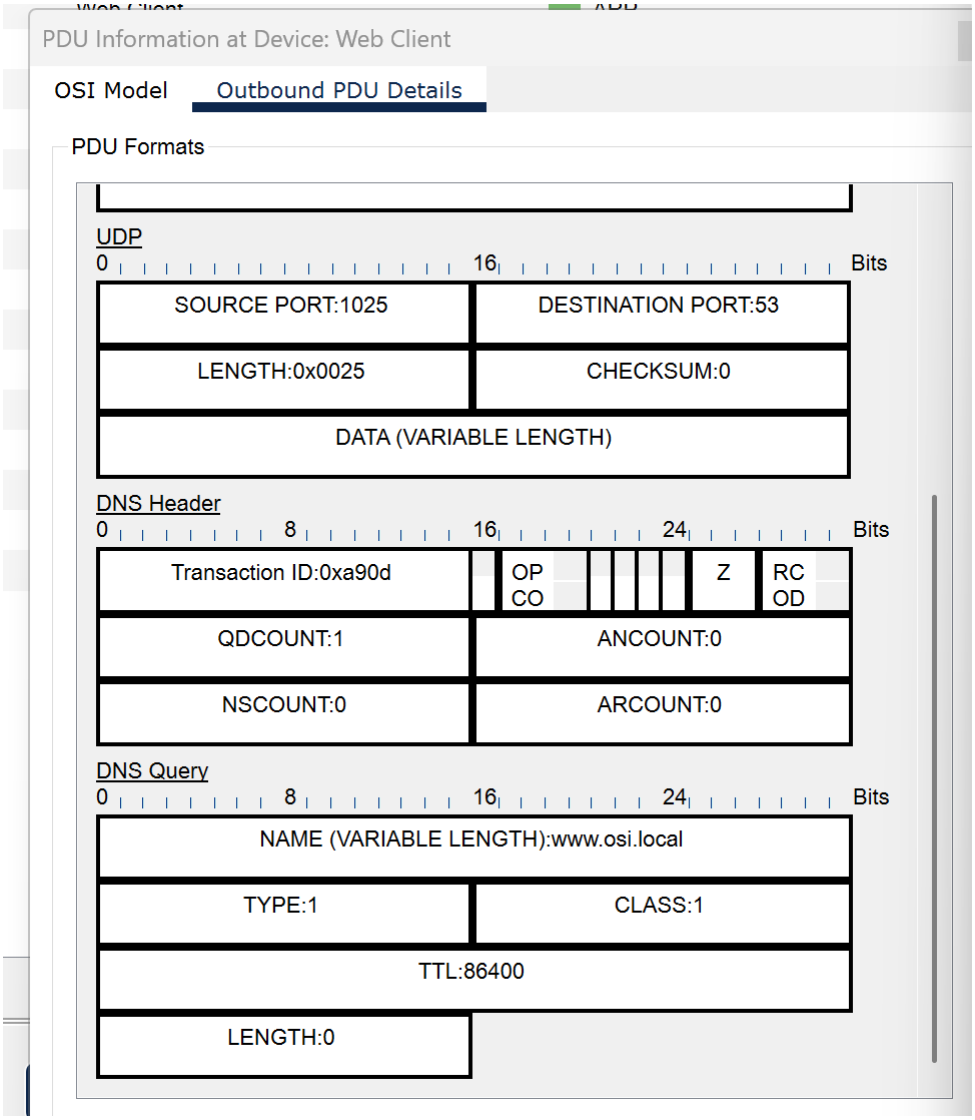

Figure 11. Source: Learner

E. At which device was the PDU captured? *Web client*

What is the value listed next to **ADDRESS**: in the DNS ANSWER section of the **Inbound PDU Details**? *192.168.1.254 (Fig.12)*

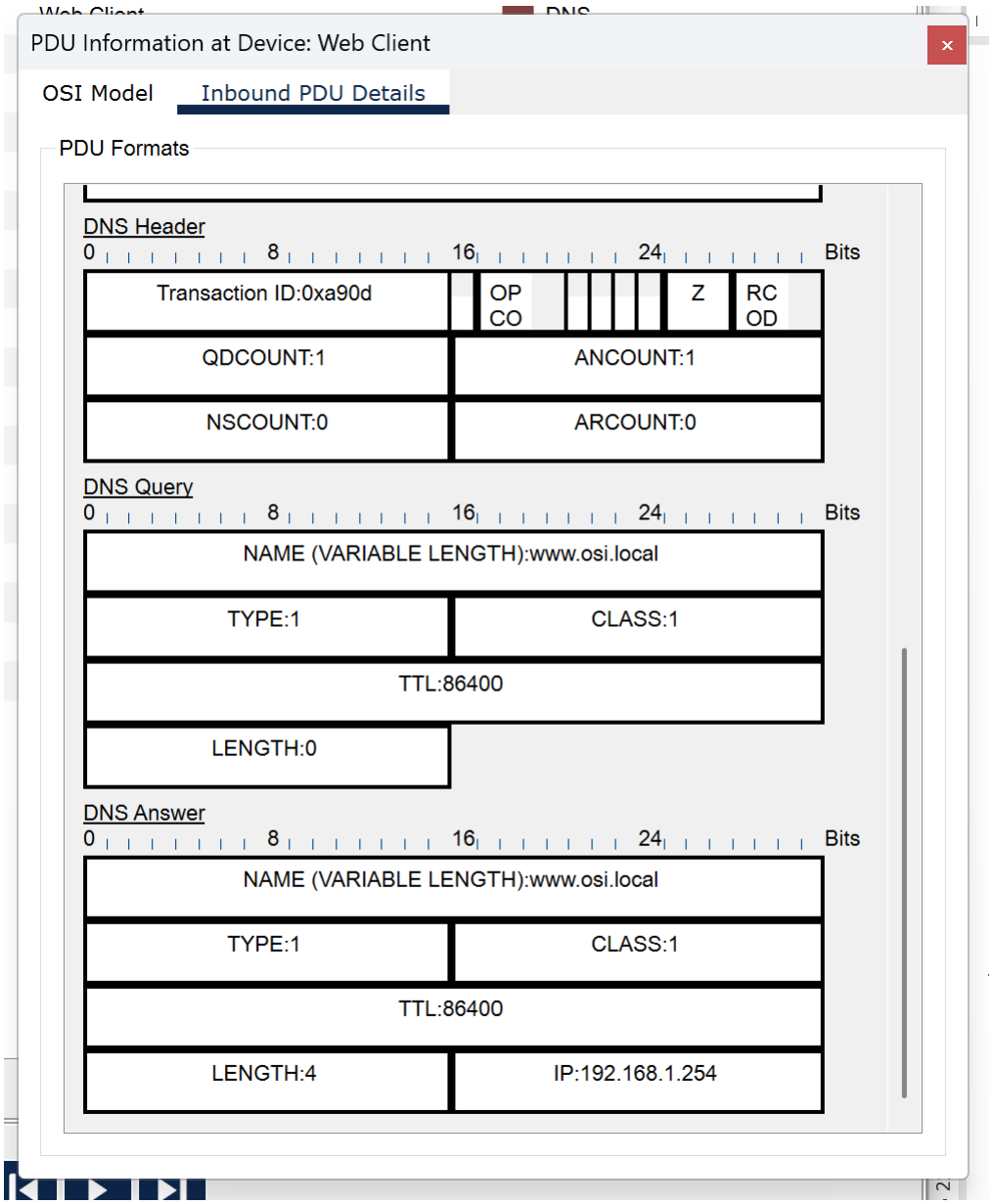

Figure 12. Source: Learner

F. In the numbered list directly below the **In Layers** and **Out Layers**, what is the information displayed under items 4 and 5? *(Fig.13)*

4: The TCP segment request has the expected peer sequence number.

5: The device sets the connection state to ESTABLISHED

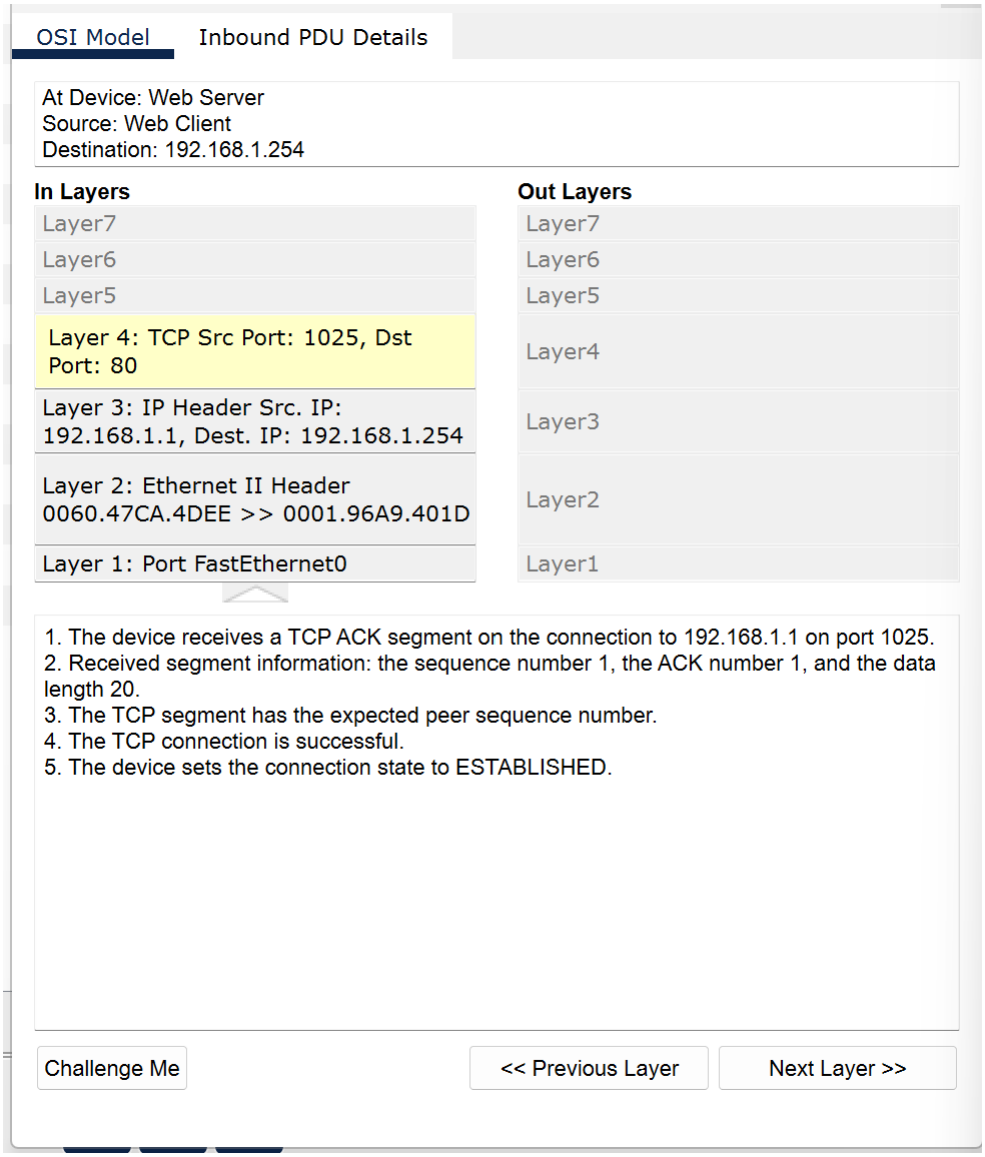

Figure 13. Source: Learner

G. What is the purpose of this event, based on the information provided in the last item in the list (should be item 4)?

This event is the last event that marks the closure of a TCP connection between the device and 192.168.1.1 on port 1025. The last TCP ACK segment confirms the receipt of the last expected data and transitions the connection to CLOSED state to end the session. (Fig.14)

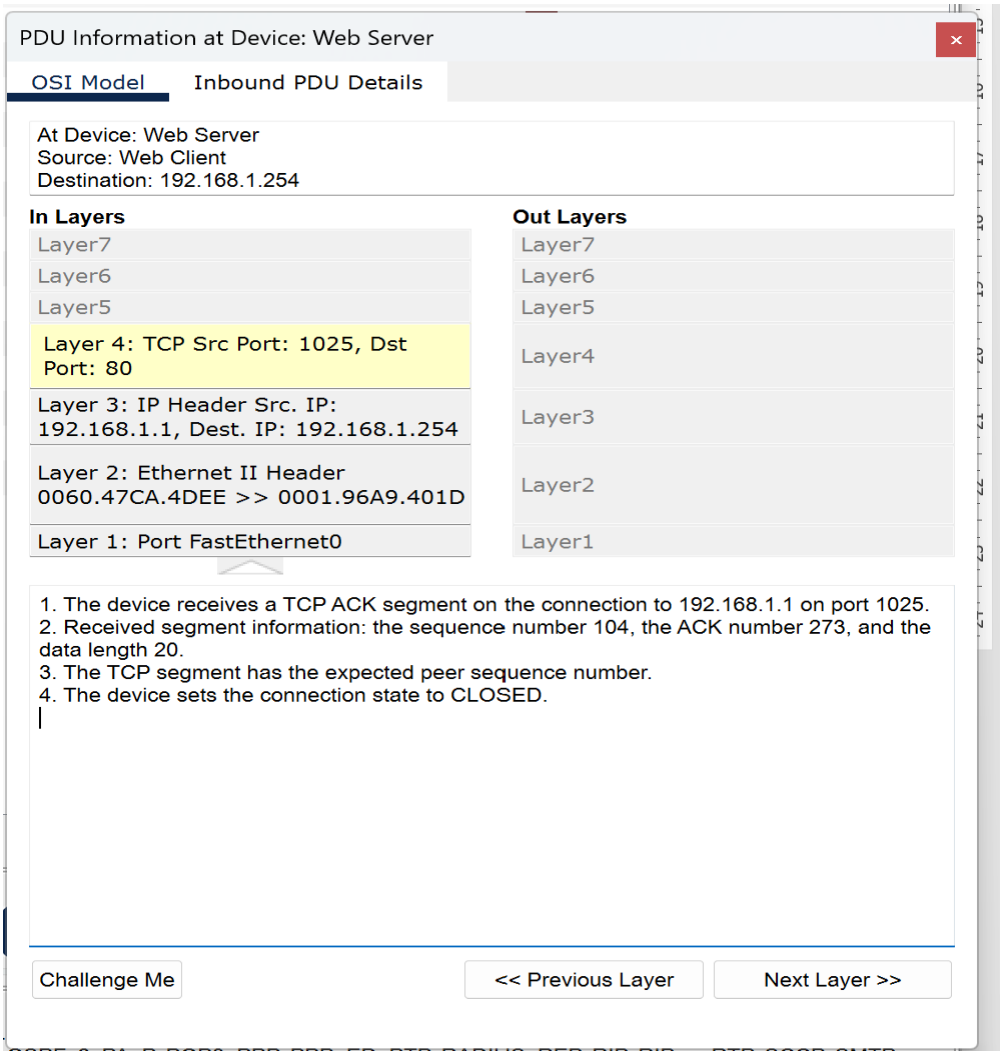

Figure 14. Source: Learner

Challenge Questions

Based on the information that was inspected during the Packet Tracer capture, what port number is the **web server listening to** for the web request?

The web server listens to web requests on port 80. In the attached screenshot, the destination port is set at 80 in layer 4 in the TCP segment of the HTTP request. This is a default port for unencrypted web traffic (La Lau & La Lau, 2021). *(Fig.15)*

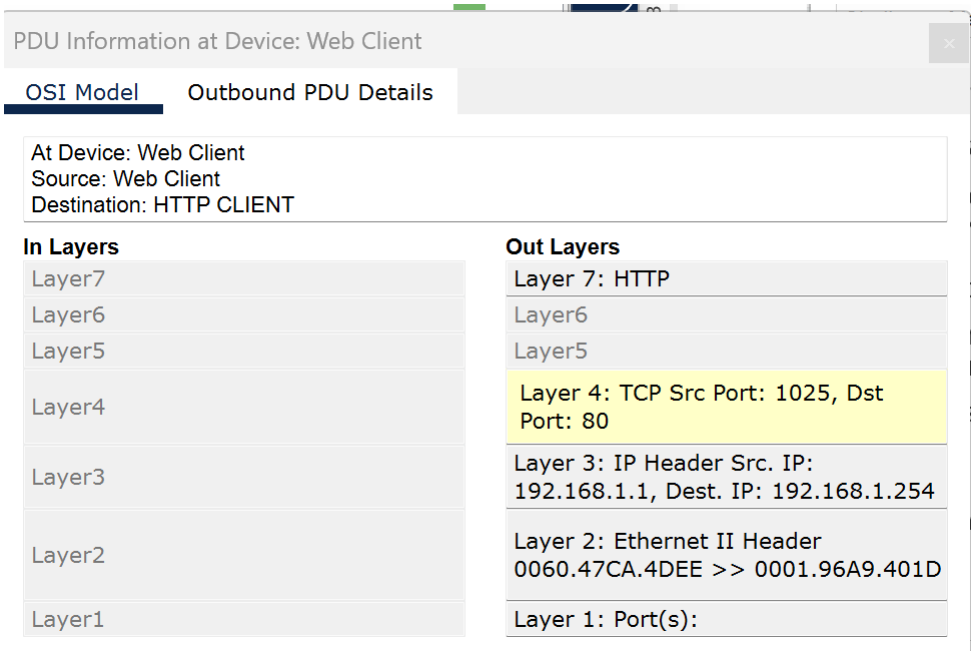

Figure 15. Source: Learner

What port is the **Web Server** listening on for a DNS request?

The web server is listening to the DNS requests on port 53. By default, DNS uses UDP on port 53 to resolve domain names and IP addresses (Zhan et al., 2022). *(Fig.16)*

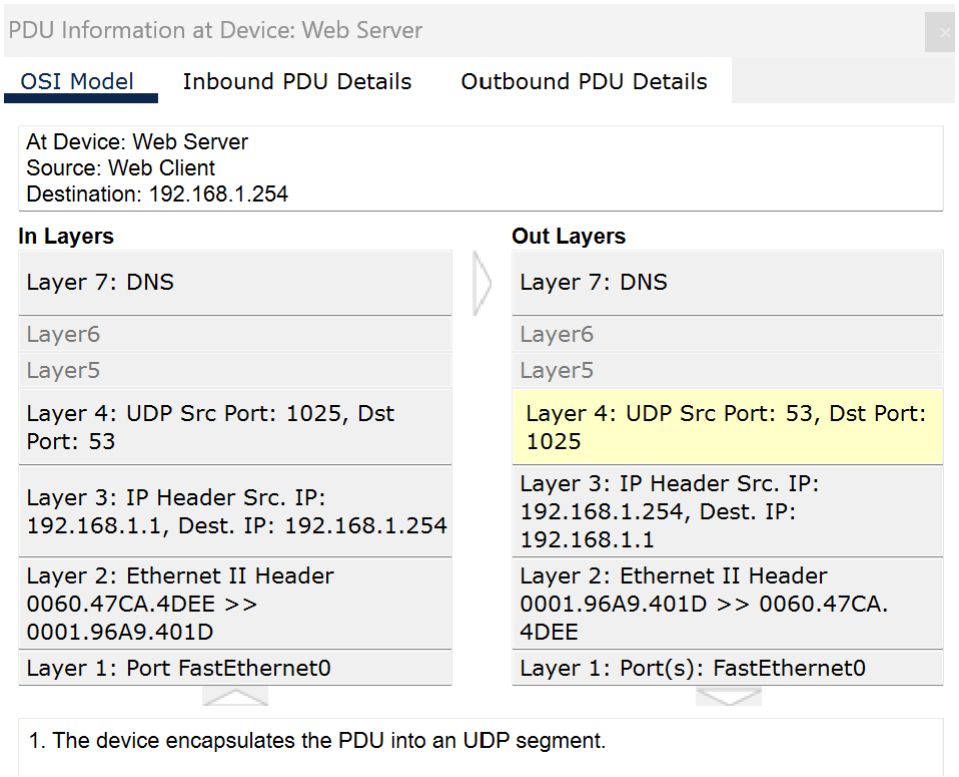

Figure 16. Source: Learner

Conclusion

In this network simulation in Packet Tracer activity, I comprehensively explored network protocols in great detail in two main sections. In Part 1, I analysed HTTP web traffic by observing how data is encapsulated and transmitted throughout the OSI Model layers. I also identified elements like port numbers, IP addresses, and MAC addresses. In Part 2, I observed and learned how the DNS, ARP, and TCP protocols assist the web communication process. Through hands-on activity simulation in Packet Tracer, I verified that the web server listens to HTTP requests on port 80 and listens to DNS requests on port 53. This revelation underscores the importance of port numbers in network services. Overall, this lab activity enhanced my understanding of fundamental networking principles and, through it, I developed crucial skills for analysing and troubleshooting network traffic.

References

La Lau, R., & La Lau, R. (2021). Web Server Part 1: Apache/Nginx Basics. *Practical Internet Server Configuration: Learn to Build a Fully Functional and Well-Secured Enterprise Class Internet Server*, 183-225.

Zhan, M., Li, Y., Yu, G., Li, B., & Wang, W. (2022). Detecting DNS over HTTPS based data exfiltration. *Computer Networks*, *209*, 108919.