Course: Cloud and Network Security - C3 - 2025
Name: Neville Ngothe Iregi
Student No.: CS-CNS10-25054
Date: Tuesday, 16 September 2025

WEEK 1 Assignment 1: Examining TCP/IP and OSI Models in Action

Introduction

Data moving through a network is broken down into smaller pieces and identified so that the pieces can be put back together at the data's destination. Each piece of data is given a specific name(a Protocol Data Unit) and is associated with a specific layer of the **TCP/IP** and **OSI (Open Systems Interconnection) models.**

The **OSI model** is a theoretical internetwork reference model that standardizes network communication functions into seven distinct layers: Application, Presentation, Session, Transport, Network, Data Link, and Physical. It is used for data network design, operation specifications, and troubleshooting.

The **TCP/IP model**, also known as the Internet model, is a modern dominant commercial protocol architecture, powered by the Transmission Control Protocol(TCP) and Internet Protocol(IP). It is a four-layer communication framework for networks that defines how data is packetized, addressed, transmitted, routed, and received. The four layers are Application, Transport, Internet, and Network Access.

This simulated activity in Packet Tracer aims to provide a foundation for understanding the TCP/IP protocol suite and the relationship to the OSI model by allowing one to view the data contents being sent across the network at each layer and visualize the encapsulation process (Process of adding information such as headers containing addressing info that identifies the source and destination hosts to the pieces of data that make up the message).

Objectives

1. Examine HTTP web traffic.
2. Display Elements of the TCP/IP protocol suite.

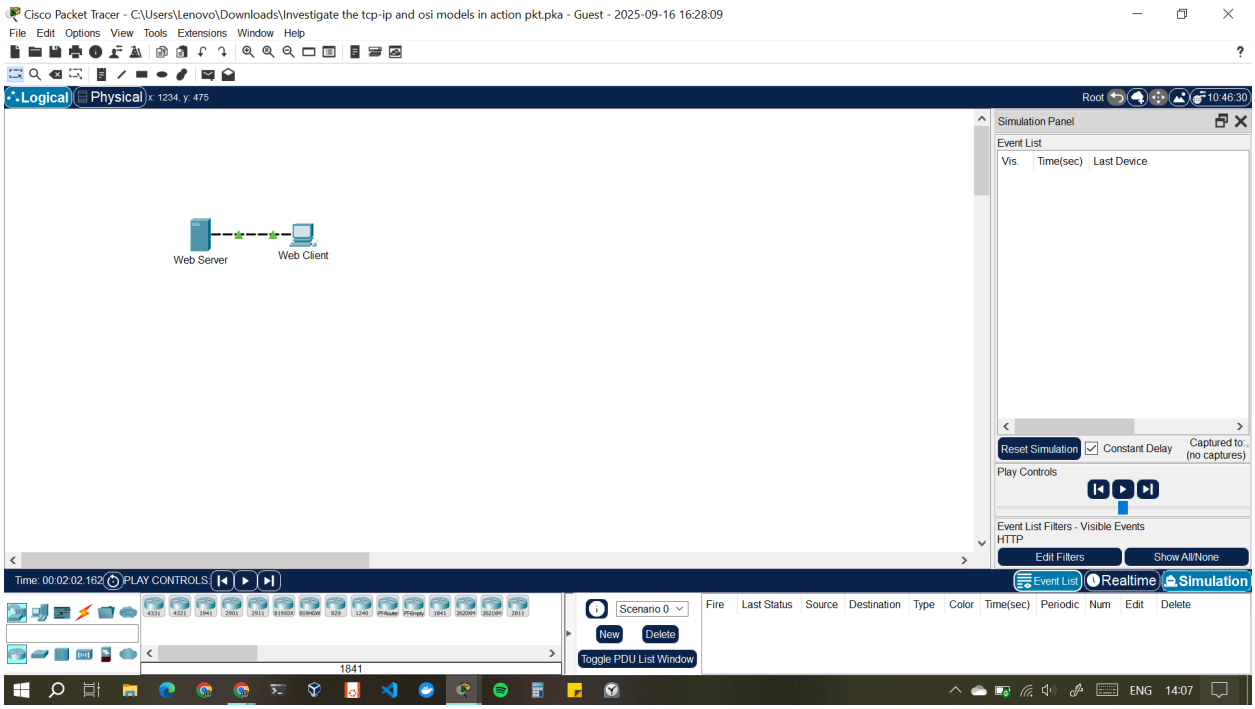
PART 1: Examine HTTP web traffic

In part 1 of this activity, I used Packet Tracer(PT) Simulation mode to generate web traffic and examine the contents of the HTTP packet.

Step 1: Switch from Realtime to Simulation mode.

In the lower right corner of the Packet Tracer interface are buttons that toggle between Realtime and Simulation mode. PT always starts in Realtime mode, in which networking protocols operate with realistic timings. However, a powerful feature of Packet Tracer allows the user to "stop time" by switching to Simulation mode. In Simulation mode, packets are displayed as animated envelopes, time is event driven, and the user can step through networking events.

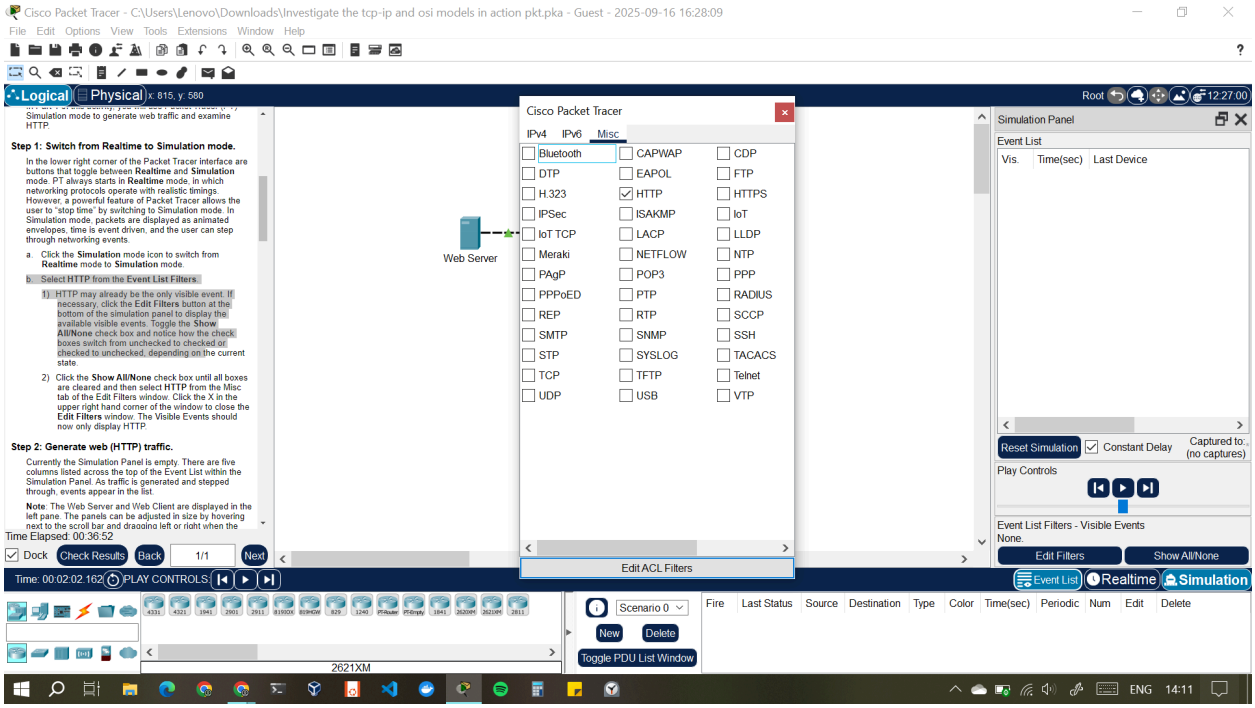
a. Click the Simulation mode icon to switch from Realtime mode to Simulation mode.

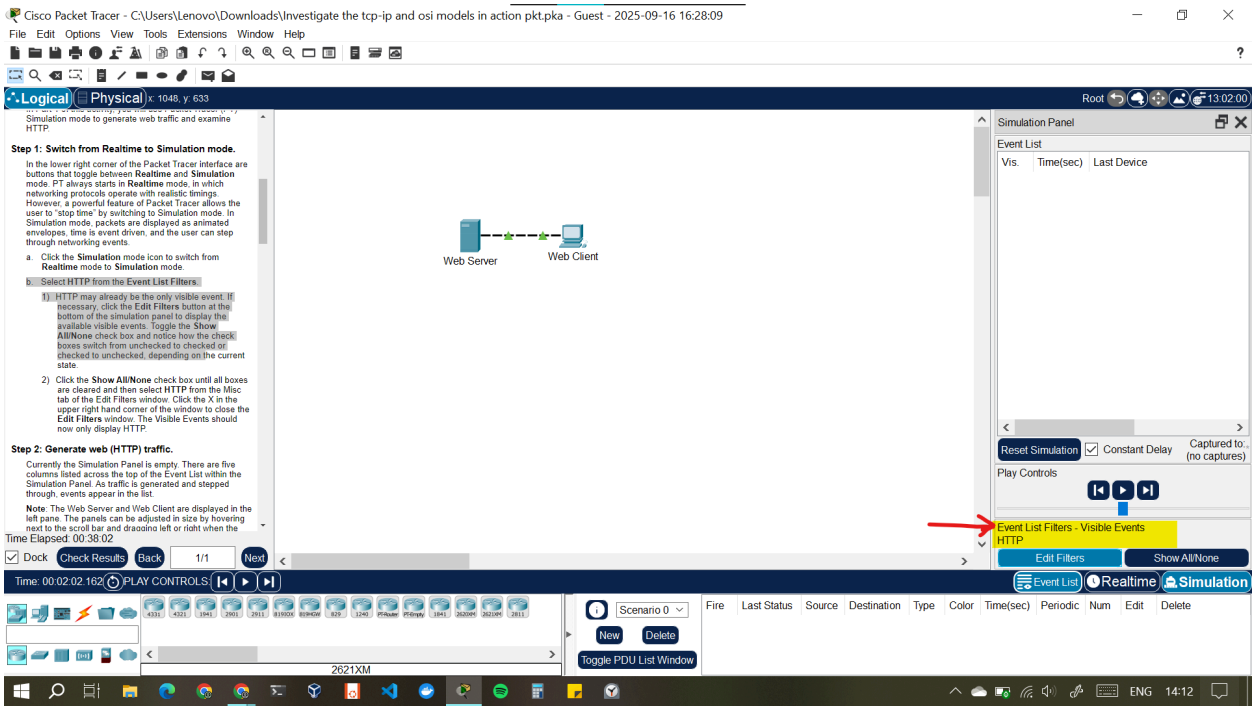


b. Select HTTP from the Event List Filters.

1) HTTP may already be the only visible event. If necessary, click the Edit Filters button at the bottom of the simulation panel to display the available visible events. Toggle the Show All/None check box and notice how the check boxes switch from unchecked to checked or checked to unchecked, depending on the current state.

2) Click the Show All/None check box until all boxes are cleared and then select HTTP from the Misc tab of the Edit Filters window. Click the X in the upper right hand corner of the window to close the Edit Filters window. The Visible Events should now only display HTTP.


Cisco Packet Tracer - C:\Users\Lenovo\Downloads\Investigate the tcp-ip and osi models in action pkt.pka - Guest - 2025-09-16 16:28:09
File Edit Options View Tools Extensions Window Help
Logical Physical x: 815, y: 580
Root 12:27:00
Step 1: Switch from Realtime to Simulation mode.
In the lower right corner of the Packet Tracer interface are buttons that toggle between Realtime and Simulation mode. PT always starts in Realtime mode, in which networking protocols operate with realistic timings. However, a powerful feature of Packet Tracer allows the user to "stop time" by switching to Simulation mode. In Simulation mode, packets are displayed as animated envelopes, time is event driven, and the user can step through networking events.
a. Click the Simulation mode icon to switch from Realtime mode to Simulation mode.
b. Select HTTP from the Event List Filters.
1) HTTP may already be the only visible event. If necessary, click the Edit Filters button at the bottom of the simulation panel to display the available visible events. Toggle the Show All/None check box and notice how the check boxes switch from unchecked to checked or checked to unchecked, depending on the current state.
2) Click the Show All/None check box until all boxes are cleared and then select HTTP from the Misc tab of the Edit Filters window. Click the X in the upper right hand corner of the window to close the Edit Filters window. The Visible Events should now only display HTTP.
Step 2: Generate web (HTTP) traffic.
Currently the Simulation Panel is empty. There are five columns listed across the top of the Event List within the Simulation Panel. As traffic is generated and stepped through, events appear in the list.
Note: The Web Server and Web Client are displayed in the left pane. The panels can be adjusted in size by hovering next to the scroll bar and dragging left or right when the
Time Elapsed: 00:36:52
Dock Check Results Back 1/1 Next
Time: 00:02:02.162 PLAY CONTROLS:
Cisco Packet Tracer
IPv4 IPv6 Misc
Bluetooth DTP H.323 IPSec IoT TCP Meraki PAgP PPPoED REP SMTP STP TCP UDP
CAPWAP EAPOL HTTP ISAKMP LACP NETFLOW POP3 PTP RTP SNMP SYSLOG TFTP USB
CDP FTP HTTPS IoT LLDP NTP PPP RADIUS SCCP SSH TACACS Telnet VTP
Edit ACL Filters
Web Server
Simulation Panel
Event List
Vis. Time(sec) Last Device
Reset Simulation Constant Delay Captured to: (no captures)
Play Controls
Event List Filters - Visible Events
None.
Edit Filters Show All/None
Event List Realtime Simulation
Scenario 0 New Delete Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
2621XM
ENG 14:11

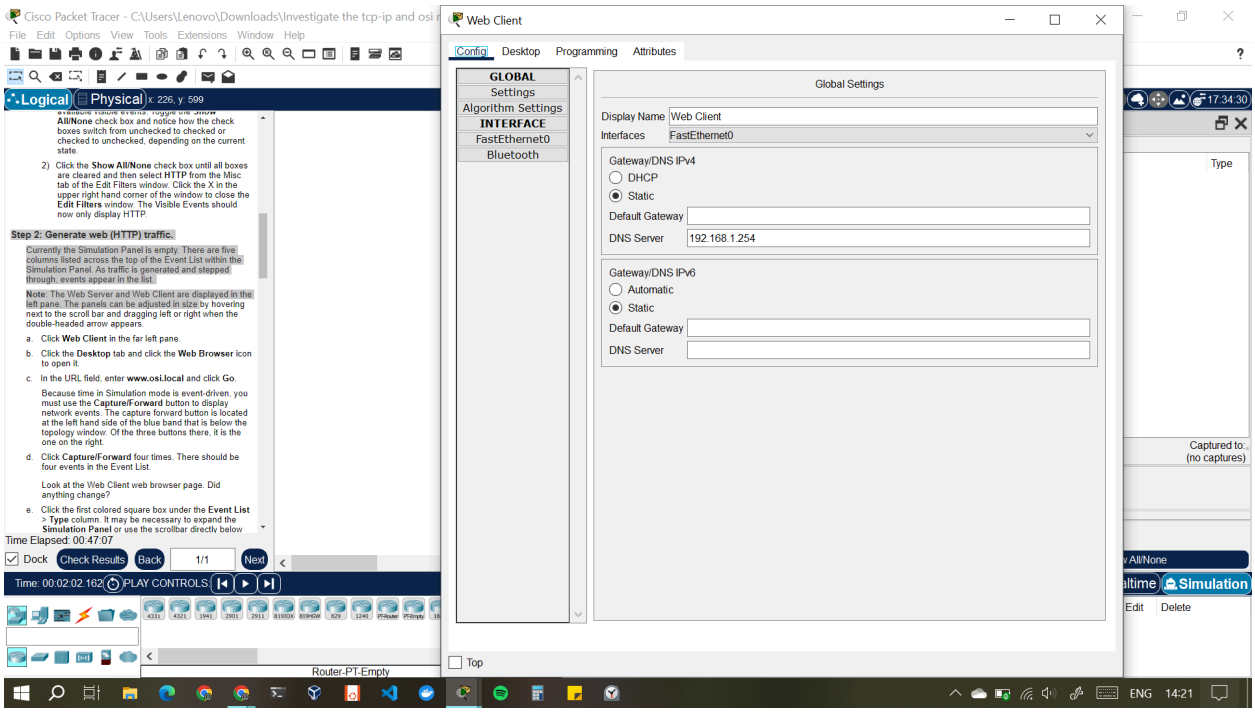

Cisco Packet Tracer - C:\Users\Lenovo\Downloads\Investigate the tcp-ip and osi models in action pkt.pka - Guest - 2025-09-16 16:28:09
File Edit Options View Tools Extensions Window Help
Logical Physical x: 1048, y: 633
Root 13:02:00
Step 1: Switch from Realtime to Simulation mode.
In the lower right corner of the Packet Tracer interface are buttons that toggle between Realtime and Simulation mode. PT always starts in Realtime mode, in which networking protocols operate with realistic timings. However, a powerful feature of Packet Tracer allows the user to "stop time" by switching to Simulation mode. In Simulation mode, packets are displayed as animated envelopes, time is event driven, and the user can step through networking events.
a. Click the Simulation mode icon to switch from Realtime mode to Simulation mode.
b. Select HTTP from the Event List Filters.
1) HTTP may already be the only visible event. If necessary, click the Edit Filters button at the bottom of the simulation panel to display the available visible events. Toggle the Show All/None check box and notice how the check boxes switch from unchecked to checked or checked to unchecked, depending on the current state.
2) Click the Show All/None check box until all boxes are cleared and then select HTTP from the Misc tab of the Edit Filters window. Click the X in the upper right hand corner of the window to close the Edit Filters window. The Visible Events should now only display HTTP.
Step 2: Generate web (HTTP) traffic.
Currently the Simulation Panel is empty. There are five columns listed across the top of the Event List within the Simulation Panel. As traffic is generated and stepped through, events appear in the list.
Note: The Web Server and Web Client are displayed in the left pane. The panels can be adjusted in size by hovering next to the scroll bar and dragging left or right when the
Time Elapsed: 00:38:02
Dock Check Results Back 1/1 Next
Time: 00:02:02.162 PLAY CONTROLS:
Web Server
Web Client
Simulation Panel
Event List
Vis. Time(sec) Last Device
Reset Simulation Constant Delay Captured to: (no captures)
Play Controls
Event List Filters - Visible Events
HTTP
Edit Filters Show All/None
Event List Realtime Simulation
Scenario 0 New Delete Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
2621XM
ENG 14:12

Step 2: Generate web (HTTP) traffic.

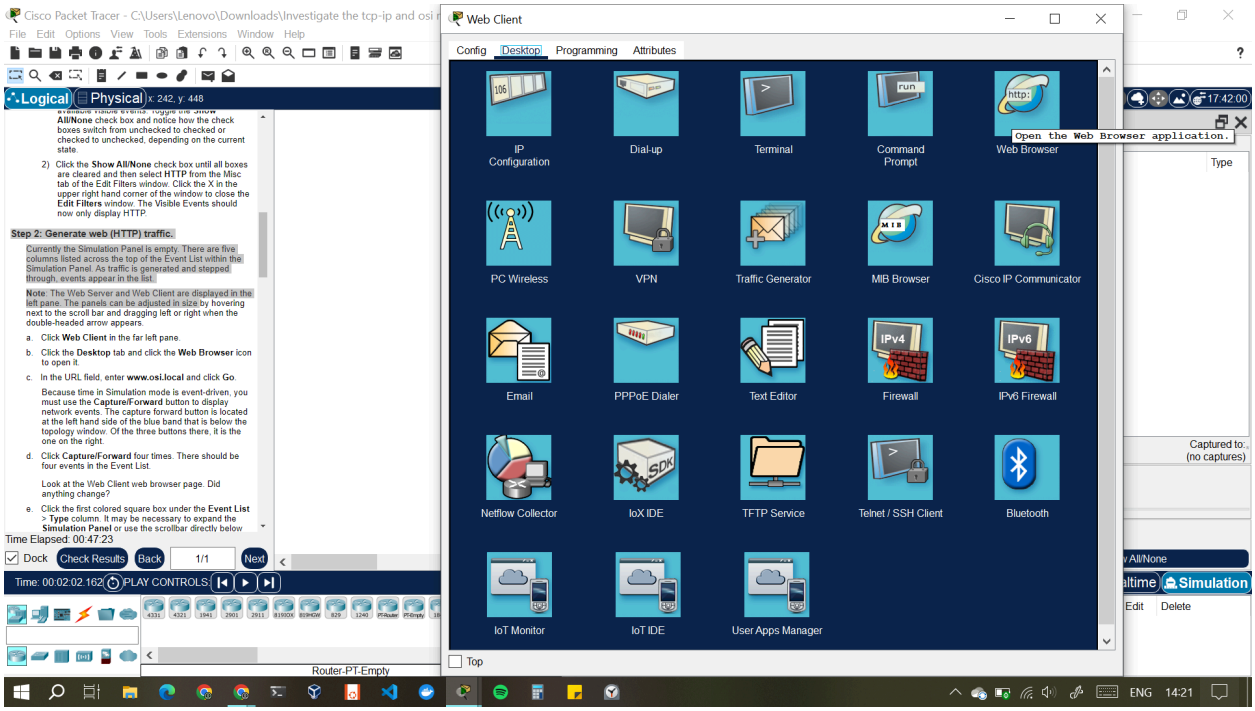
Currently the Simulation Panel is empty. There are five columns listed across the top of the Event List within the Simulation Panel. As traffic is generated and stepped through, events appear in the list.

Note: The Web Server and Web Client are displayed in the left pane. The panels can be adjusted in size by hovering next to the scroll bar and dragging left or right when the double-headed arrow appears.

a. Click Web Client in the far left pane.

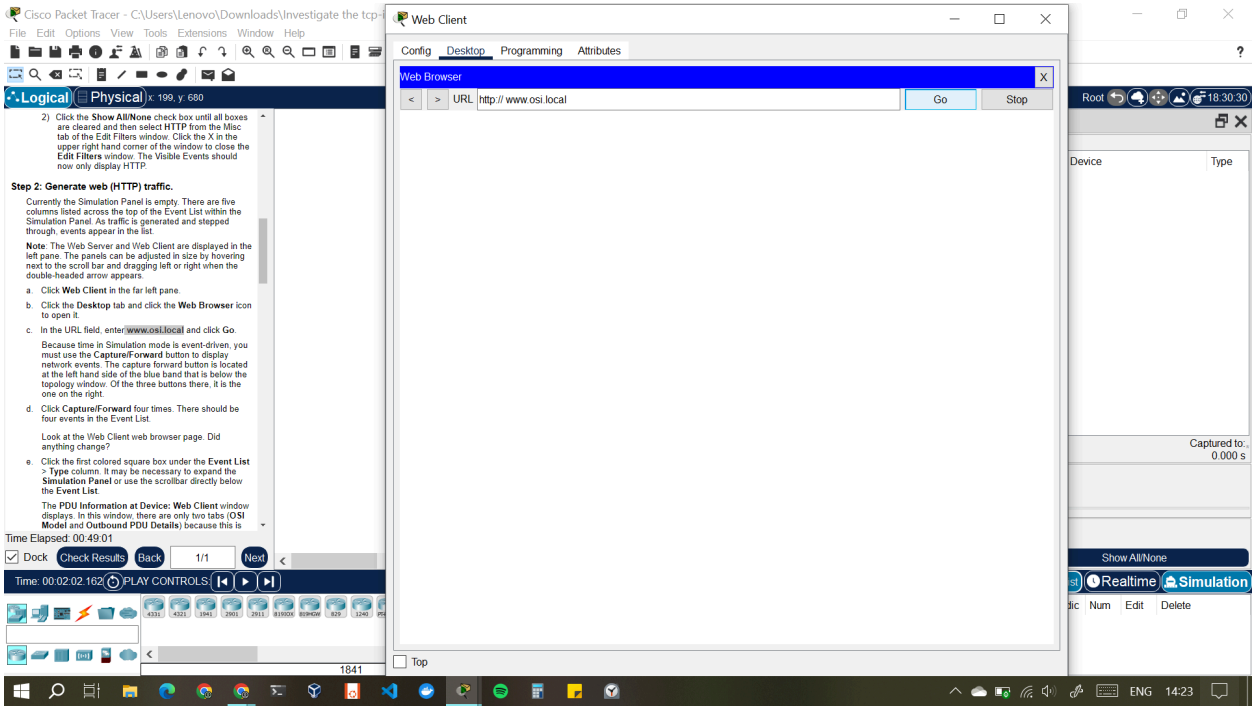


b. Click the Desktop tab and click the Web Browser icon to open it.

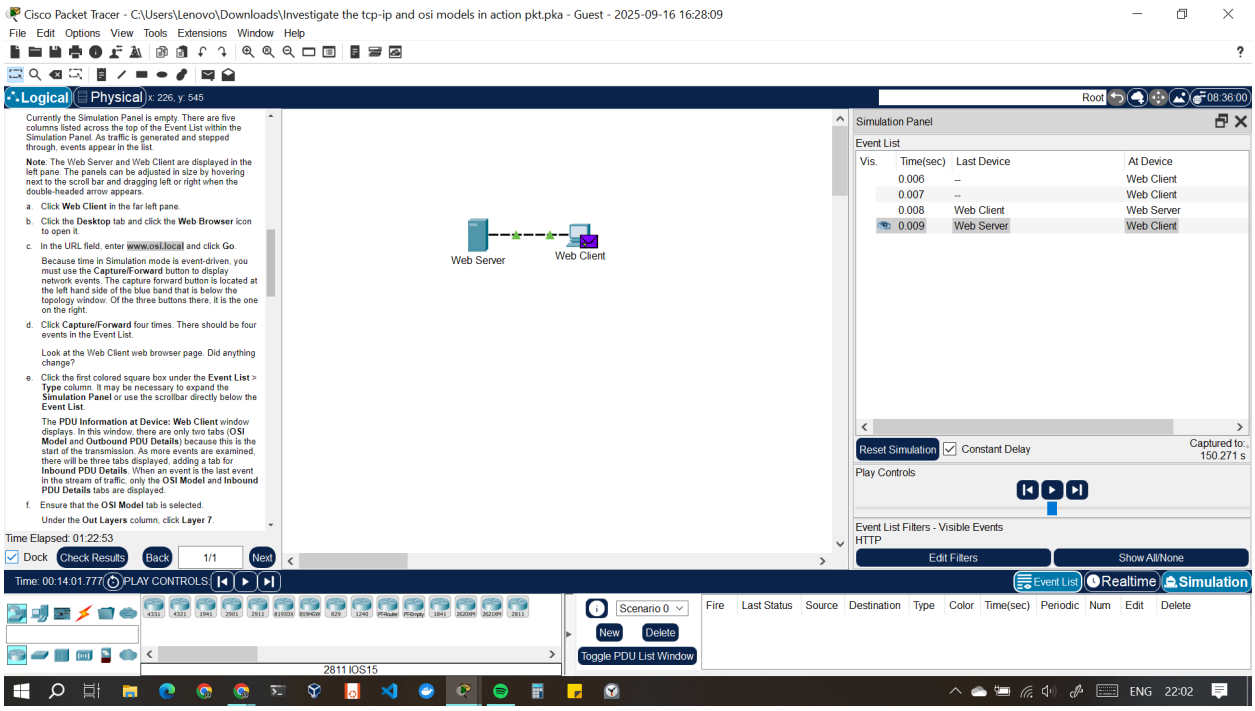


c. In the URL field, enter www.osi.local and click Go.

Because time in Simulation mode is event-driven, you must use the Capture/Forward button to display network events. The capture forward button is located at the left hand side of the blue band that is below the topology window. Of the three buttons there, it is the one on the right.



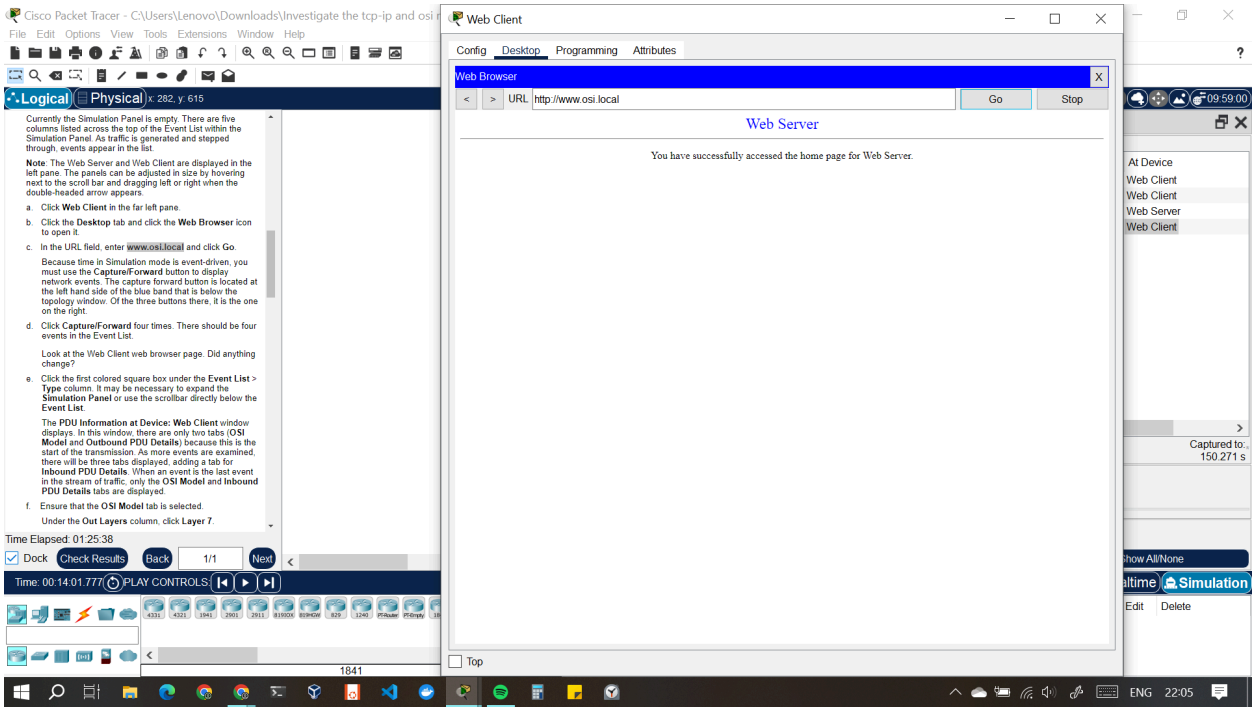
d. Click Capture/Forward four times. There should be four events in the Event List.



Question:

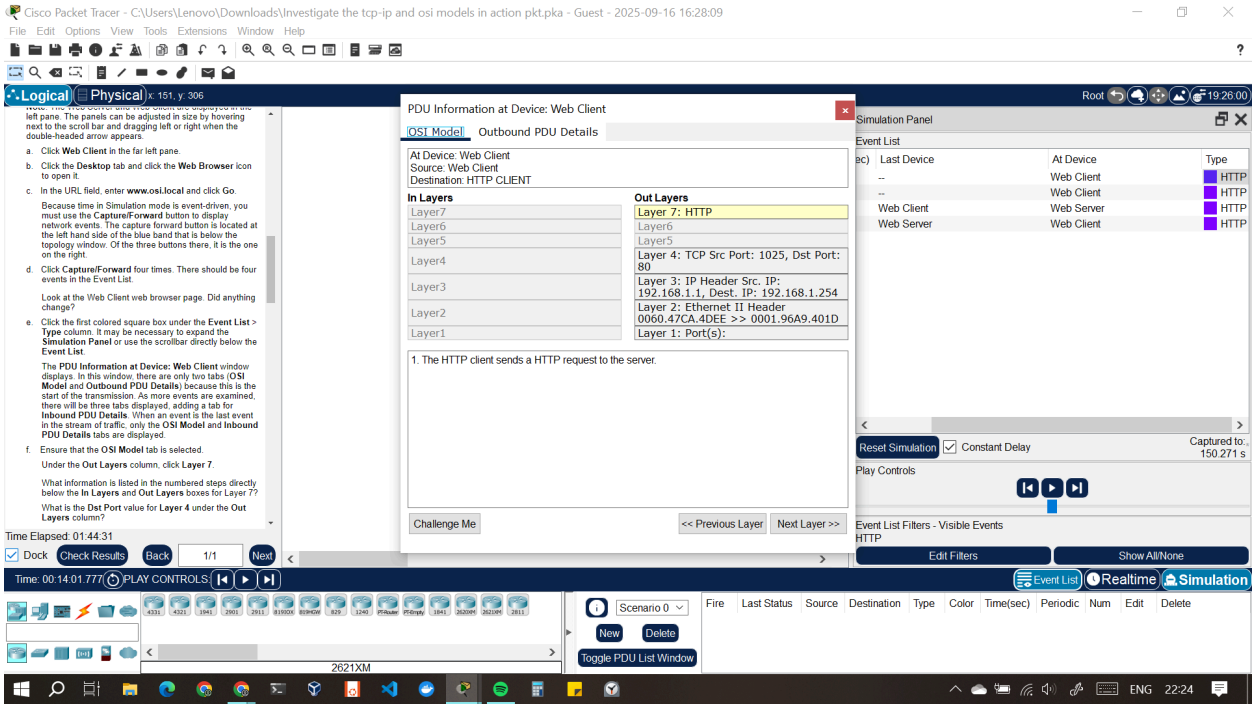
Look at the Web Client web browser page. Did anything change?

Answer: The web browser page changed to show the home page of the web server from the request made.



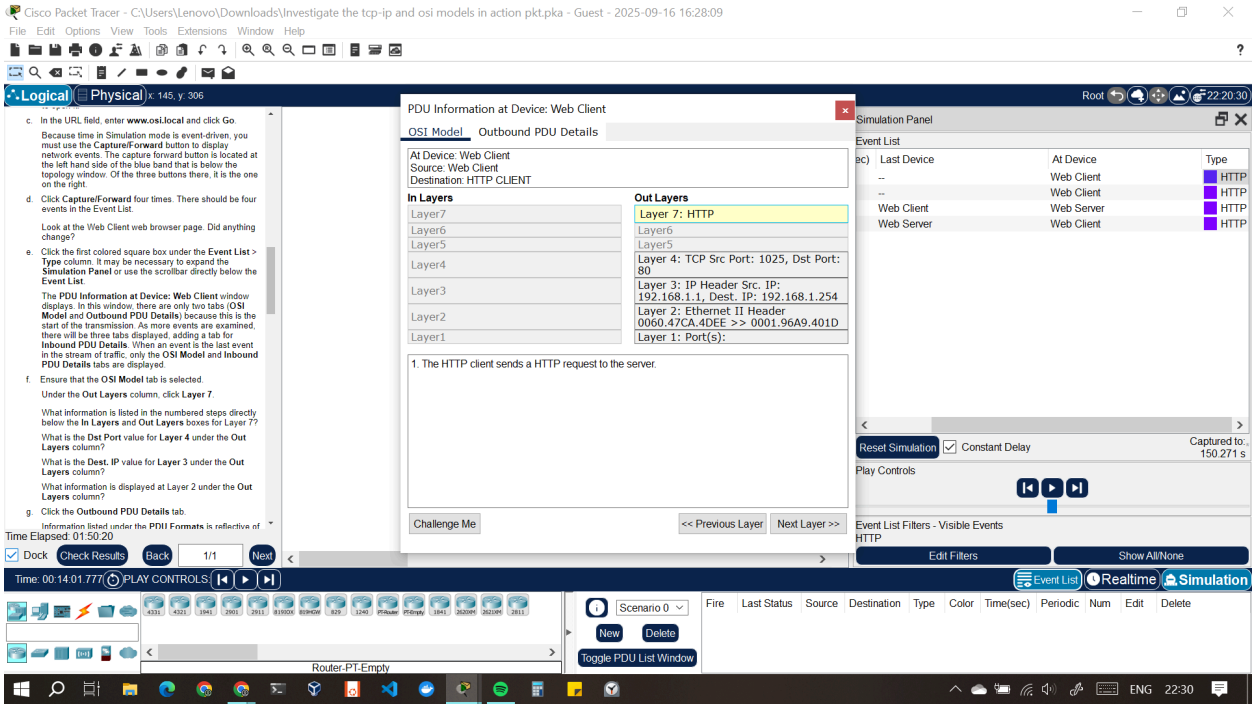
e. Click the first colored square box under the Event List > Type column. It may be necessary to expand the Simulation Panel or use the scrollbar directly below the Event List.

The PDU Information at Device: Web Client window displays. In this window, there are only two tabs (OSI Model and Outbound PDU Details) because this is the start of the transmission. As more events are examined, there will be three tabs displayed, adding a tab for Inbound PDU Details. When an event is the last event in the stream of traffic, only the OSI Model and Inbound PDU Details tabs are displayed.



f. Ensure that the OSI Model tab is selected.

Under the Out Layers column, click Layer 7.



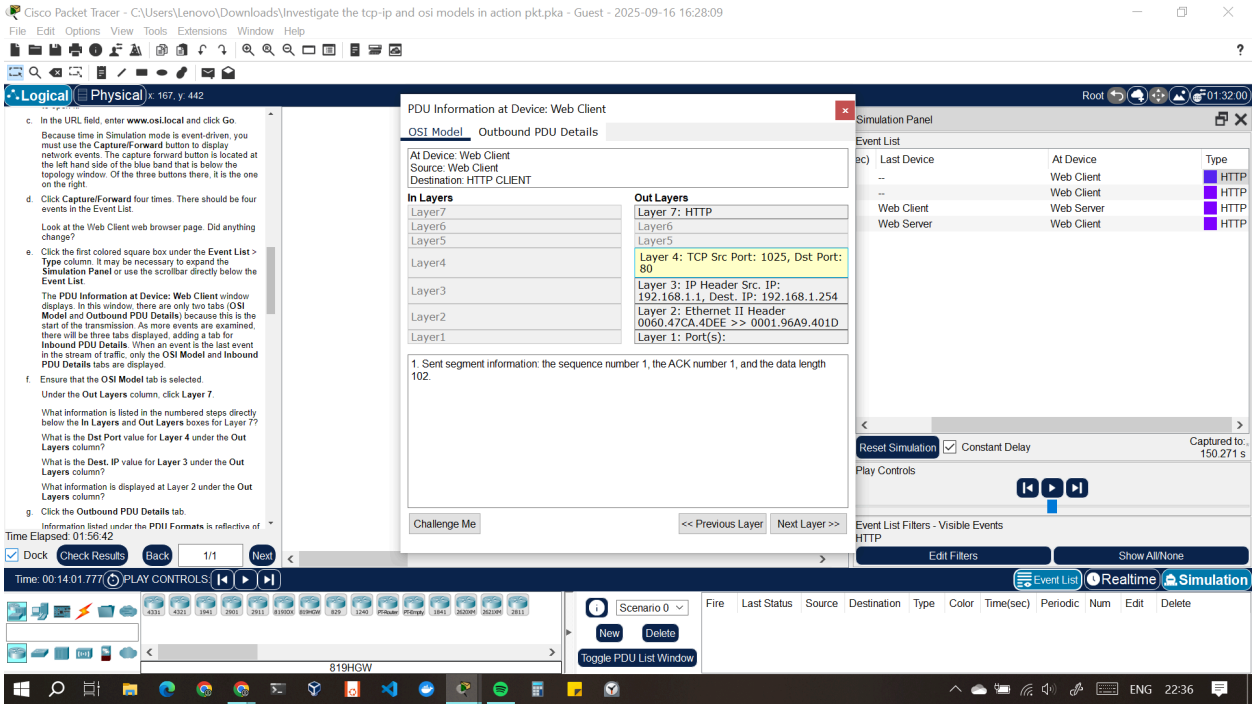
Questions:

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

Answer: 1. The HTTP client sends a HTTP request to the server.

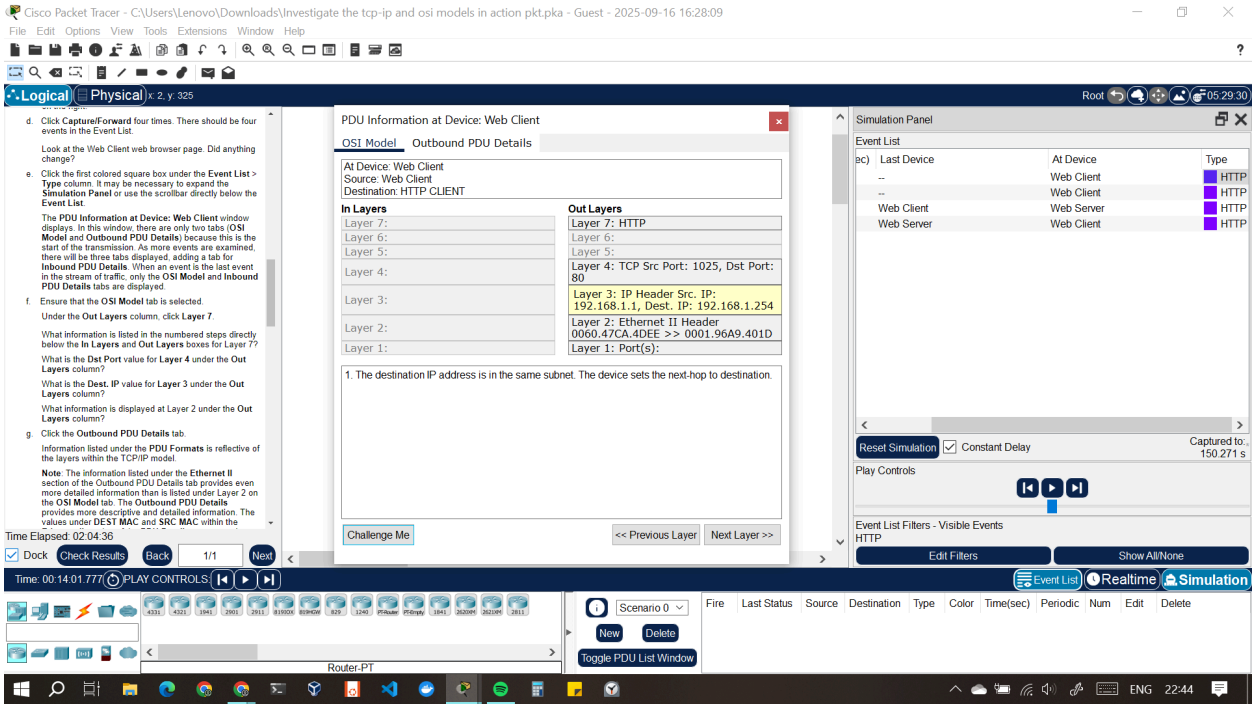
What is the Dst Port value for Layer 4 under the Out Layers column?

Answer: Dst Port value is 80(Port 80 is the default TCP port for the HTTP (Hypertext Transfer Protocol) protocol, used to transmit web pages between web browsers and servers on the World Wide Web.)



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

Answer: Dest. IP is 192.168.1.254

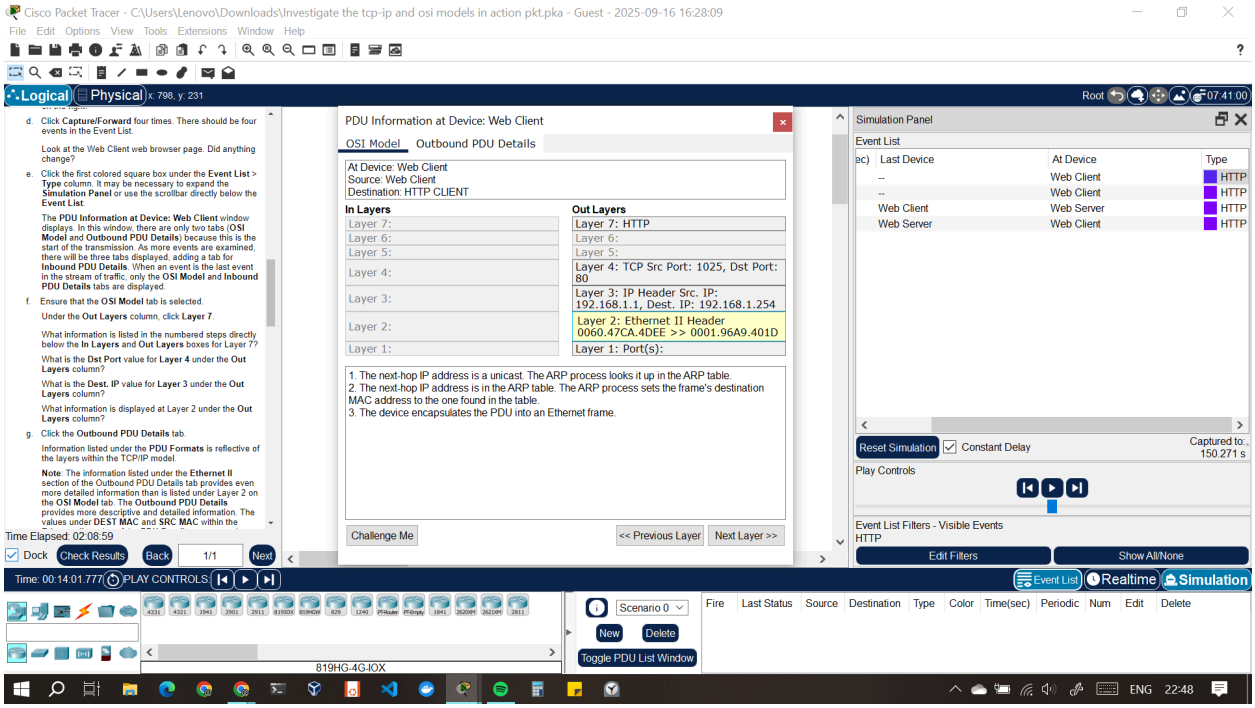


What information is displayed at Layer 2 under the Out Layers column?

Answer: Ethernet II Header 0060.47CA.4DEE >> 0001.96A9.401D

0060.47CA.4DEE - This is the source MAC address

0001.96A9.401D - This is the destination MAC address



g. Click the Outbound PDU Details tab.

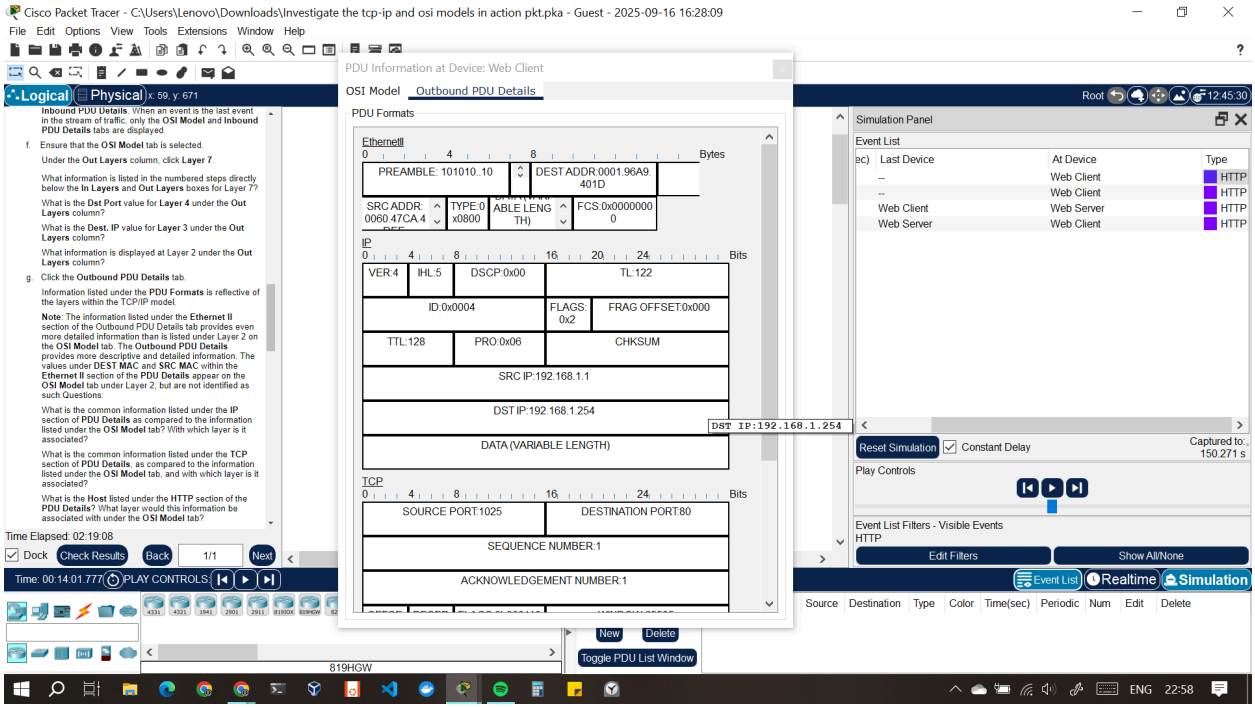
Information listed under the PDU Formats is reflective of the layers within the TCP/IP model.

Note: The information listed under the Ethernet II section of the Outbound PDU Details tab provides even more detailed information than is listed under Layer 2 on the OSI Model tab. The Outbound PDU Details provides more descriptive and detailed information. The values under DEST MAC and SRC MAC within the Ethernet II section of the PDU Details appear on the OSI Model tab under Layer 2, but are not identified as such.

Questions:

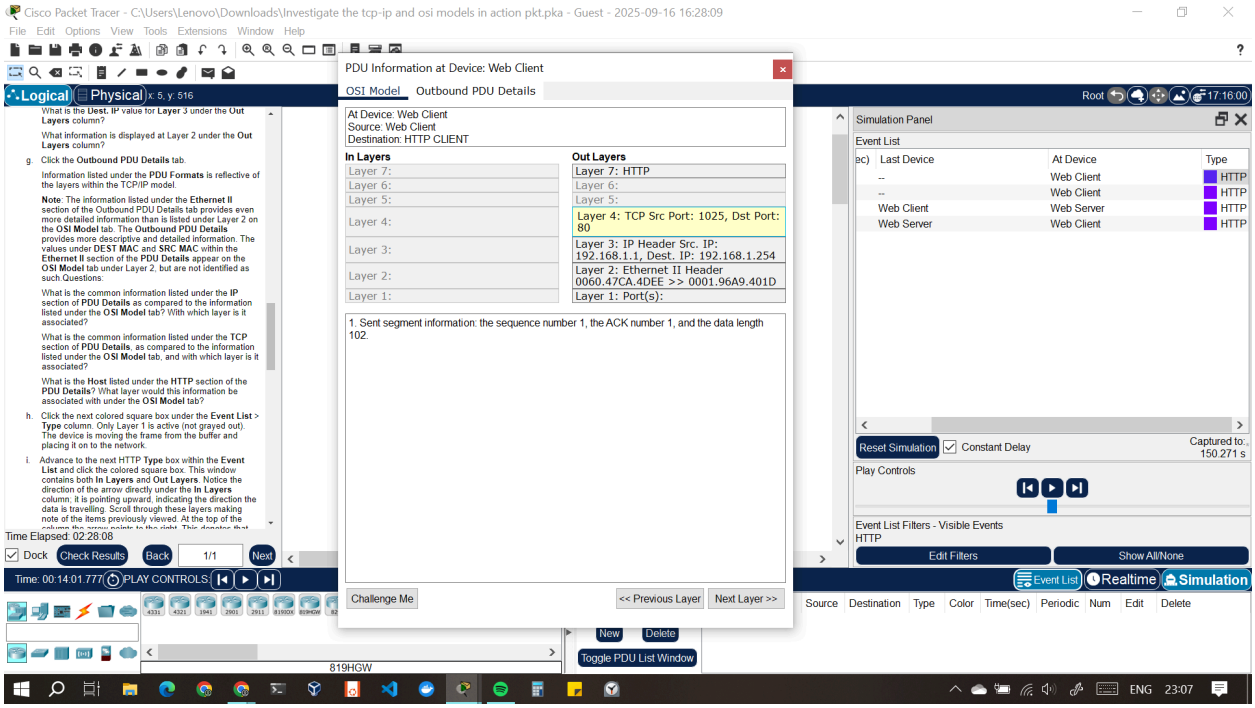
What is the common information listed under the IP section of PDU Details as compared to the information listed under the OSI Model tab? With which layer is it associated?

Answer: The source and destination IP addresses are the common info listed in the PDU details and OSI model tab. It is associated with layer 3(Network layer).



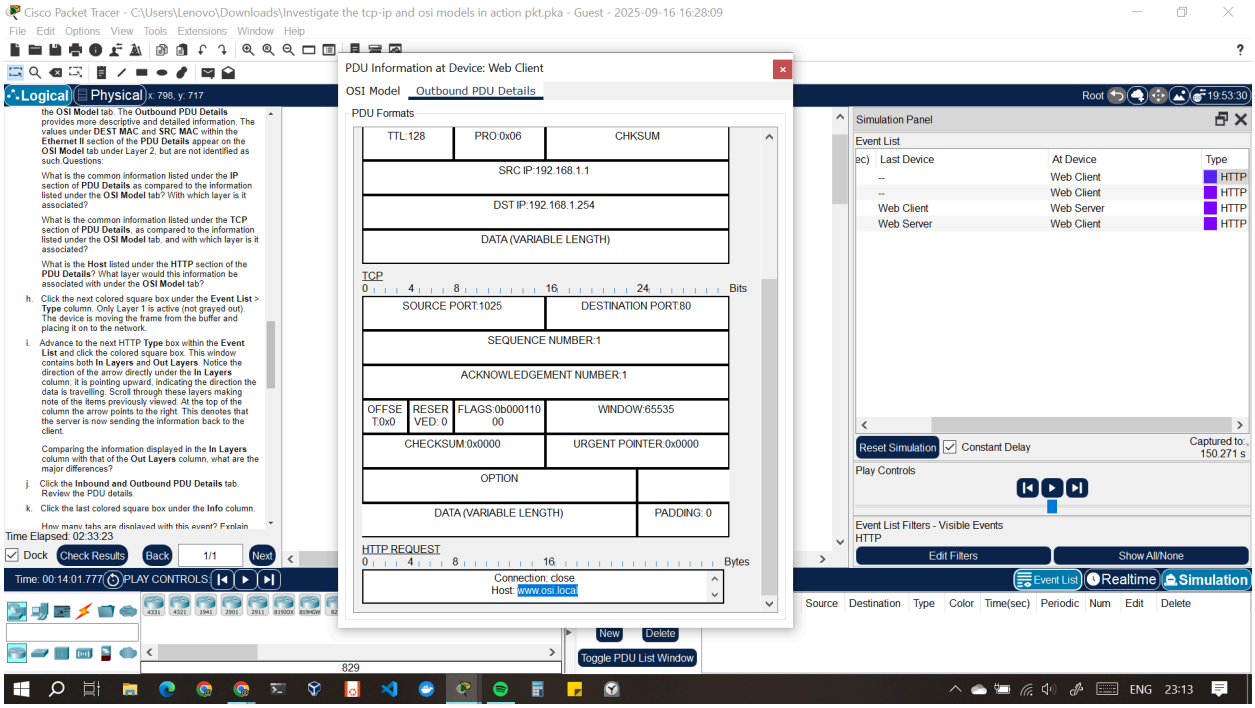
What is the common information listed under the TCP section of PDU Details, as compared to the information listed under the OSI Model tab, and with which layer is it associated?

Answer: The common information is the SOURCE PORT: 1025 and DESTINATION PORT: 80. It is associated with layer 4(Transport layer)

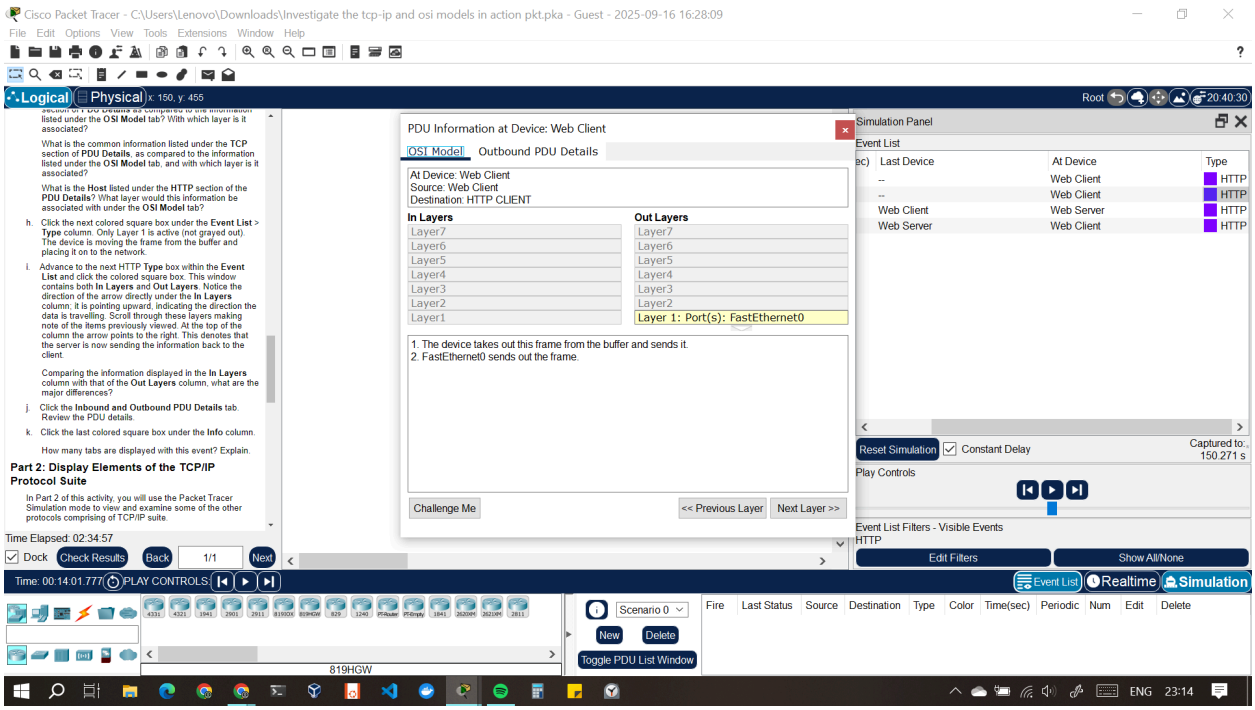


What is the Host listed under the HTTP section of the PDU Details? What layer would this information be associated with under the OSI Model tab?

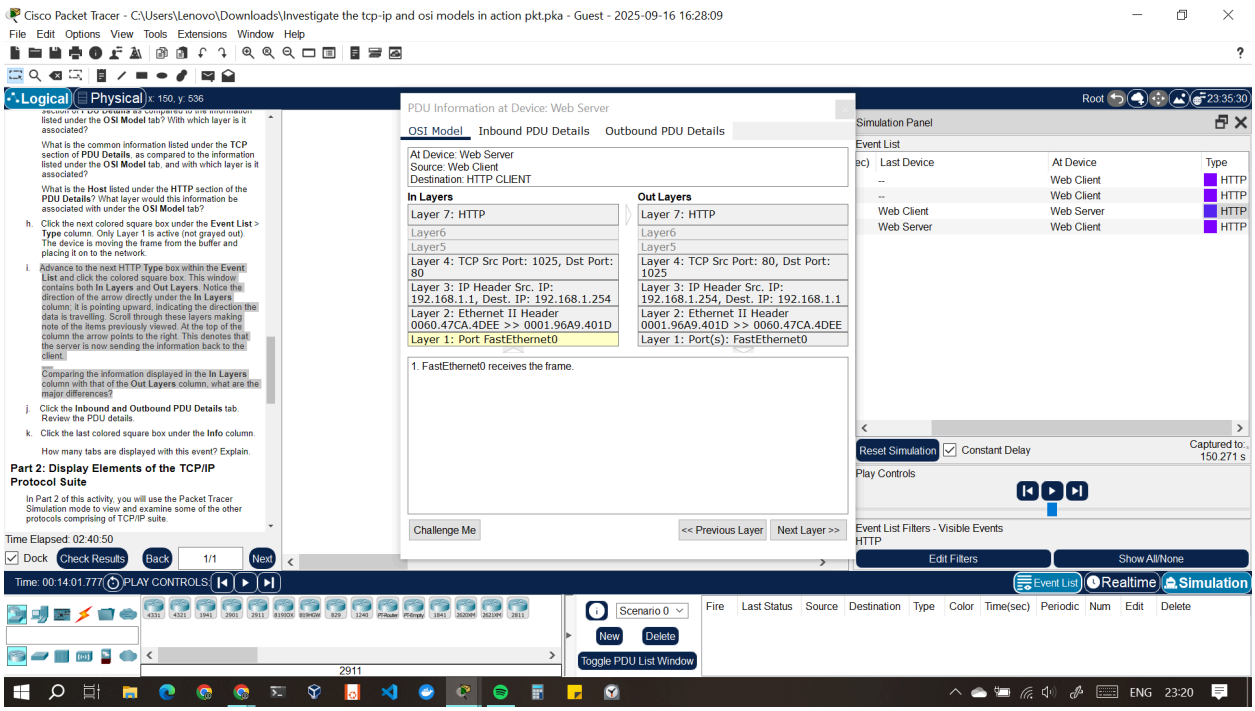
Answer: The Host is www.osi.local. The layer associated with this information under the OSI model is layer 7(Application layer)



h. Click the next colored square box under the Event List > Type column. Only Layer 1 is active (not grayed out). The device is moving the frame from the buffer and placing it on to the network.



i. Advance to the next HTTP Type box within the Event List and click the colored square box. This window contains both In Layers and Out Layers. Notice the direction of the arrow directly under the In Layers column; it is pointing upward, indicating the direction the data is travelling. Scroll through these layers making note of the items previously viewed. At the top of the column the arrow points to the right. This denotes that the server is now sending the information back to the client.



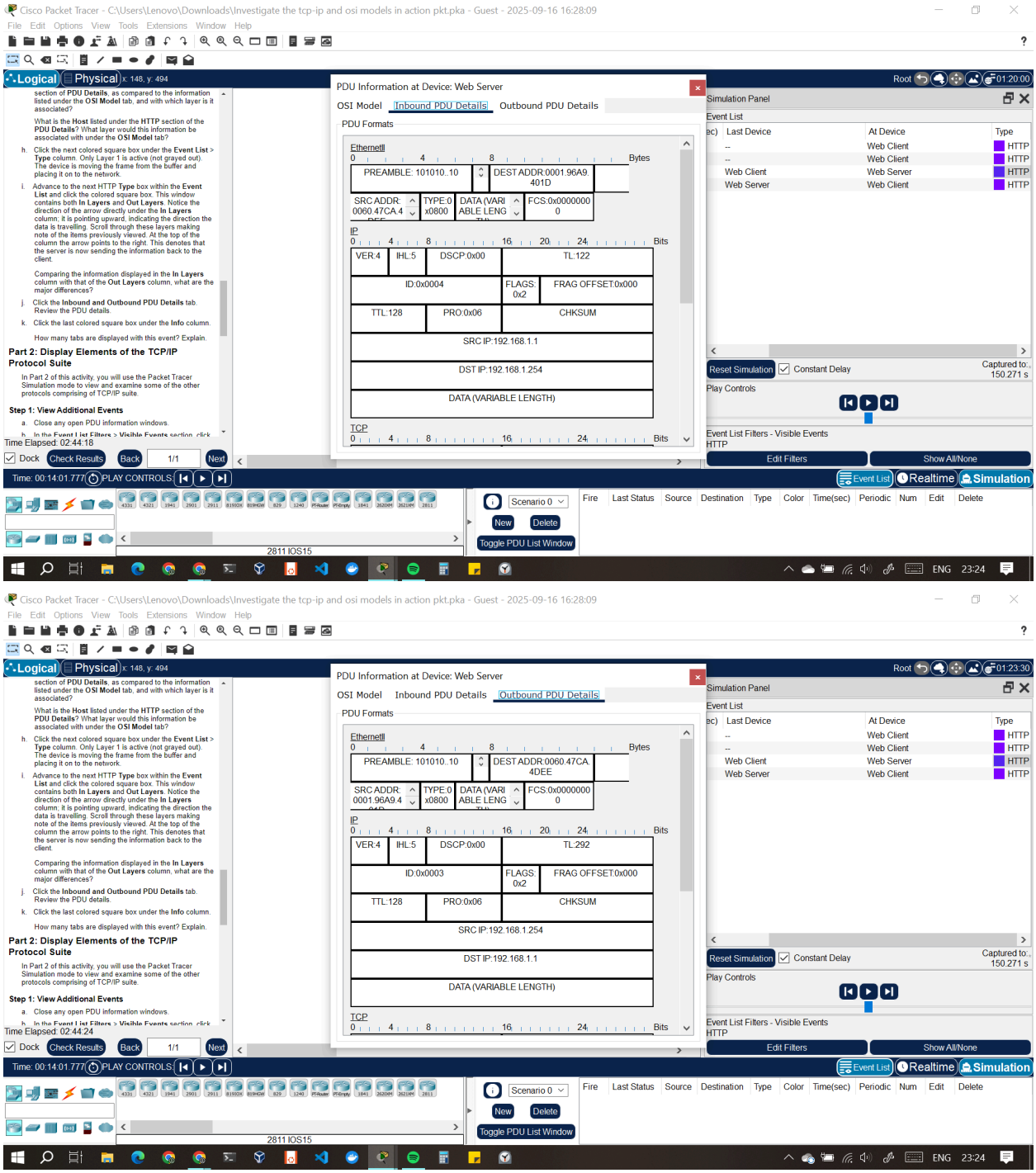
Question:

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

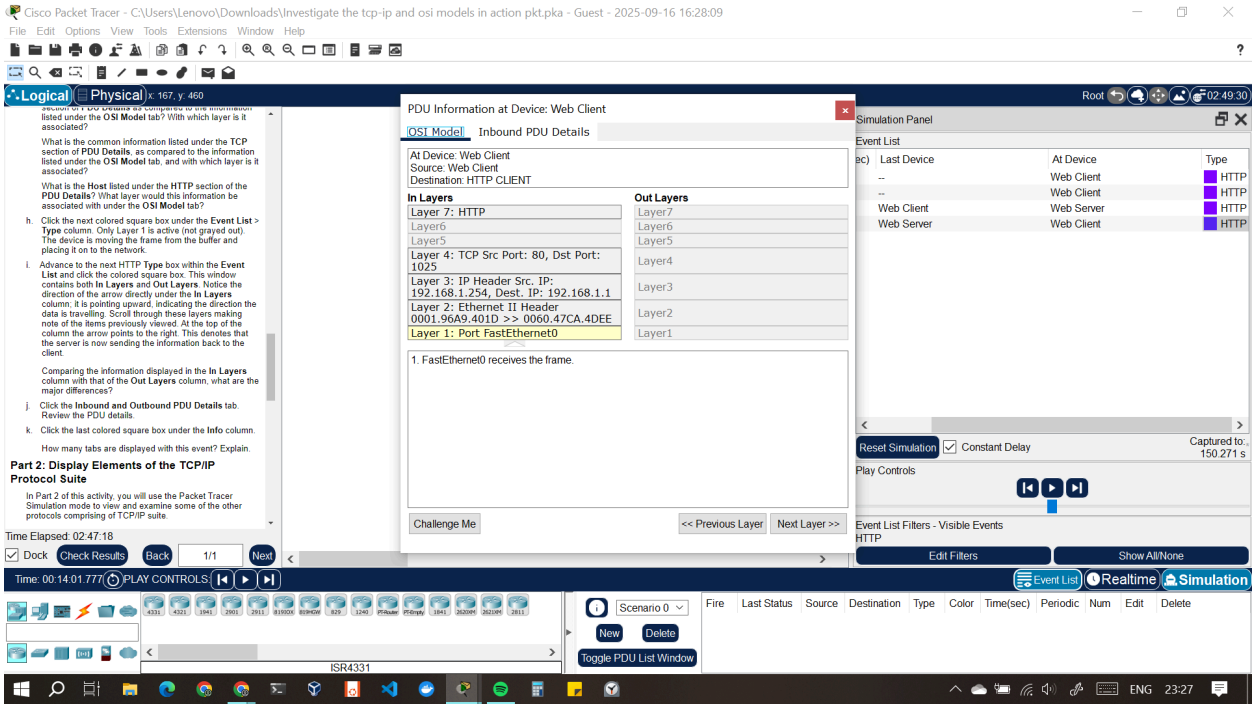
Answer: the differences between the in and out layers

1. **The destination and source MAC addresses are interchanged.**
2. **The source and destination IP addresses are interchanged.**
3. **The source and destination ports are interchanged.**

j. Click the Inbound and Outbound PDU Details tab. Review the PDU details.



k. Click the last colored square box under the Info column.



Question:

How many tabs are displayed with this event? Explain.

Answer: There are 2 tabs displayed in this event: the OSI Model tab and the Inbound PDU Details tab. This is because the web client is at the end of the communication process, only receiving the inbound data (the home page of www.osi.local) from the web server. Since the client is not sending any data at this point, no Outbound PDU Details tab is displayed.

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

In Part 2 of this activity, you will use the Packet Tracer Simulation mode to view and examine some of the other protocols comprising the TCP/IP suite.

Step 1: View Additional Events

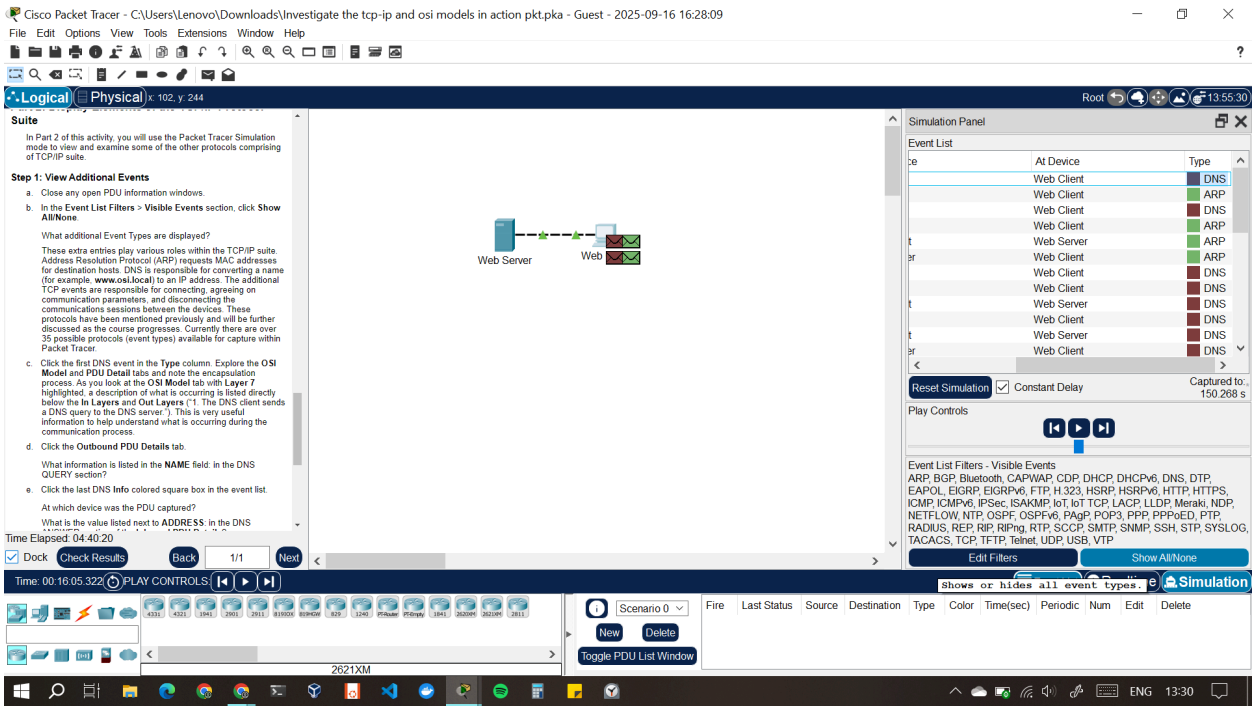
a. Close any open PDU information windows.

b. In the Event List Filters > Visible Events section, click Show All/None.

Question:

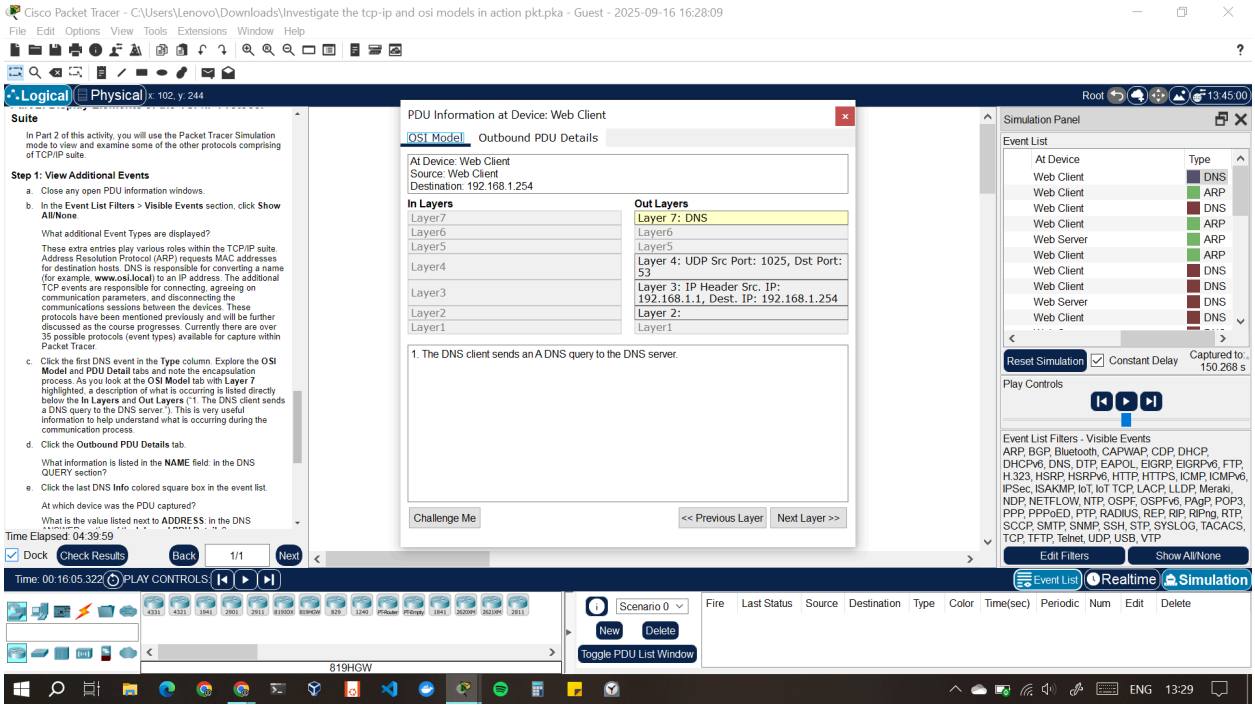
What additional Event Types are displayed?

Answer: ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP



These extra entries play various roles within the TCP/IP suite. Address Resolution Protocol (ARP) requests MAC addresses for destination hosts. DNS is responsible for converting a name (for example, www.osi.local) to an IP address. The additional TCP events are responsible for connecting, agreeing on communication parameters, and disconnecting the communications sessions between the devices. These protocols have been mentioned previously and will be further discussed as the course progresses. Currently there are over 35 possible protocols (event types) available for capture within Packet Tracer.

c. Click the first DNS event in the Type column. Explore the OSI Model and PDU Detail tabs and note the encapsulation process. As you look at the OSI Model tab with Layer 7 highlighted, a description of what is occurring is listed directly below the In Layers and Out Layers ("1. The DNS client sends a DNS query to the DNS server."). This is very useful information to help understand what is occurring during the communication process.

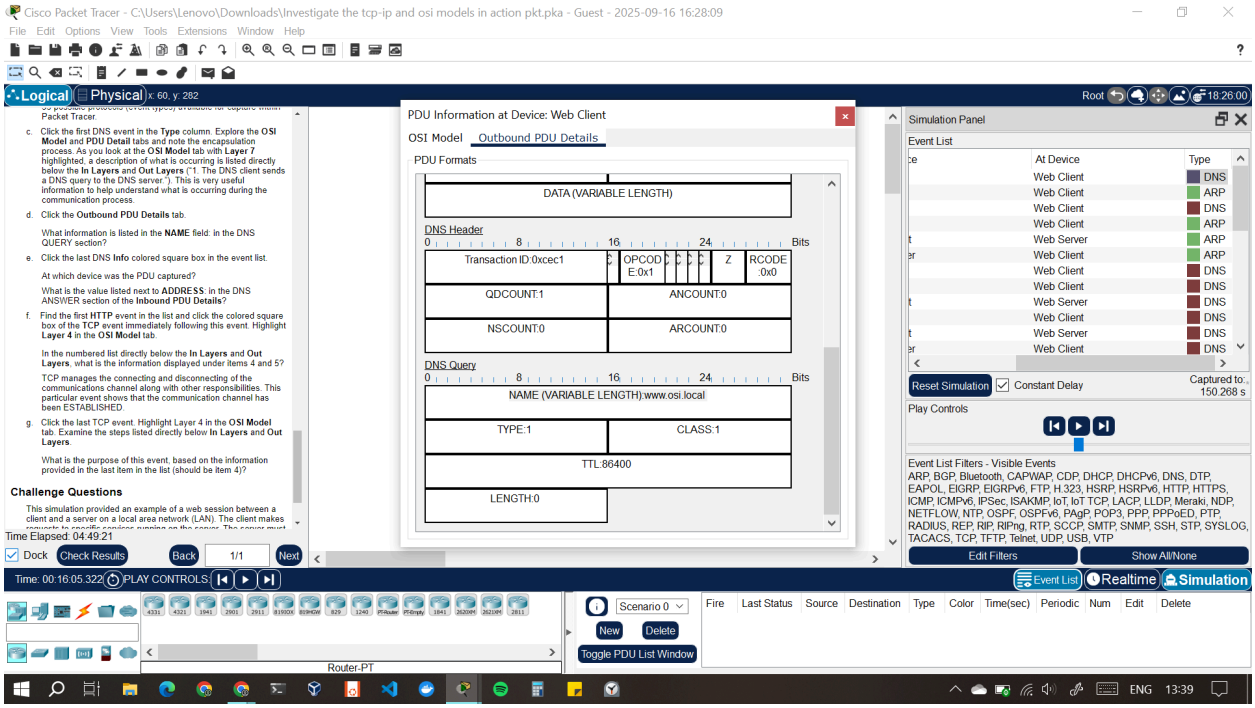


d. Click the Outbound PDU Details tab.

Question:

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

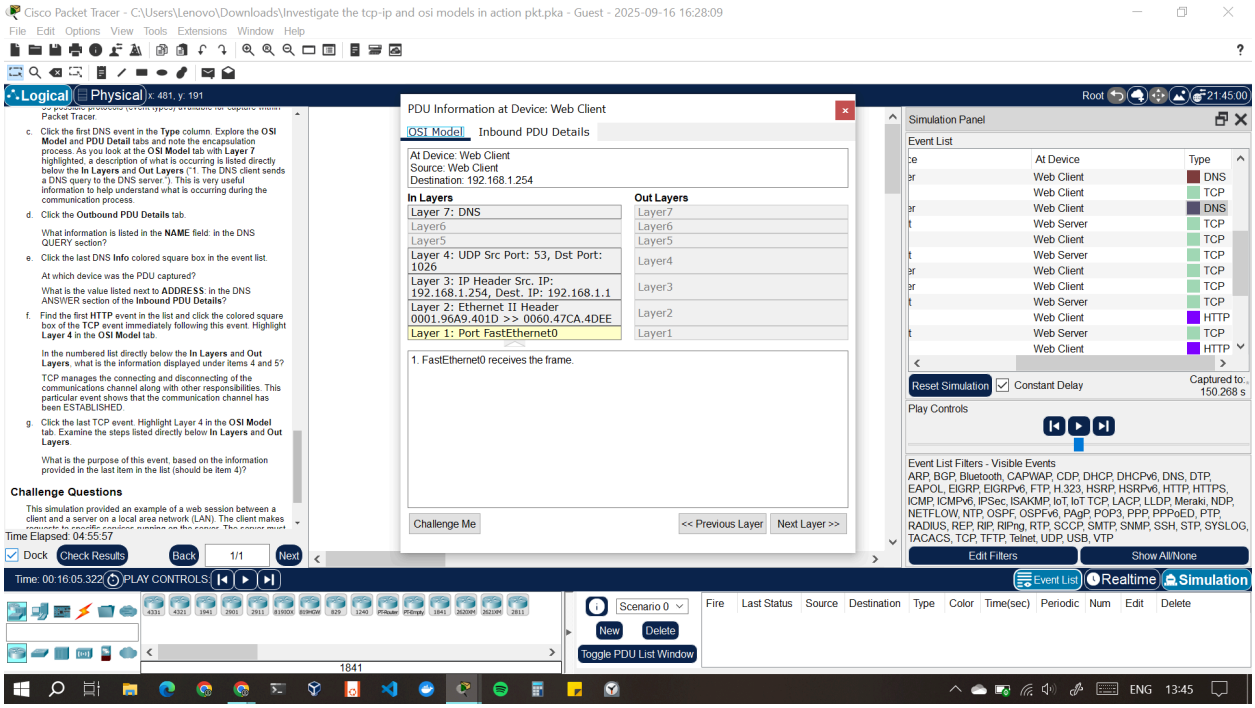
Answer: NAME (VARIABLE LENGTH):www.osi.local



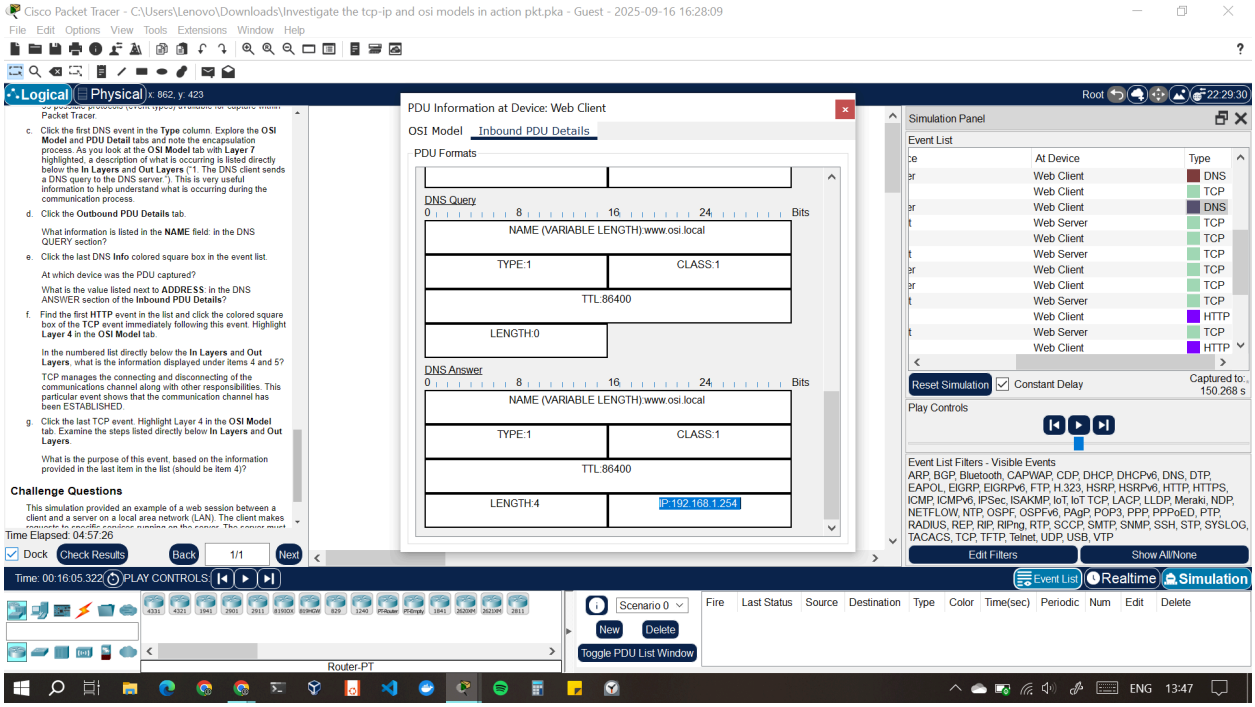
e. Click the last DNS Info colored square box in the event list.

Questions:

At which device was the PDU captured? **Answer: at the Web Client**



What is the value listed next to ADDRESS: in the DNS ANSWER section of the Inbound PDU Details? **Answer: 192.168.1.254 - this is the IP address of the DNS server**

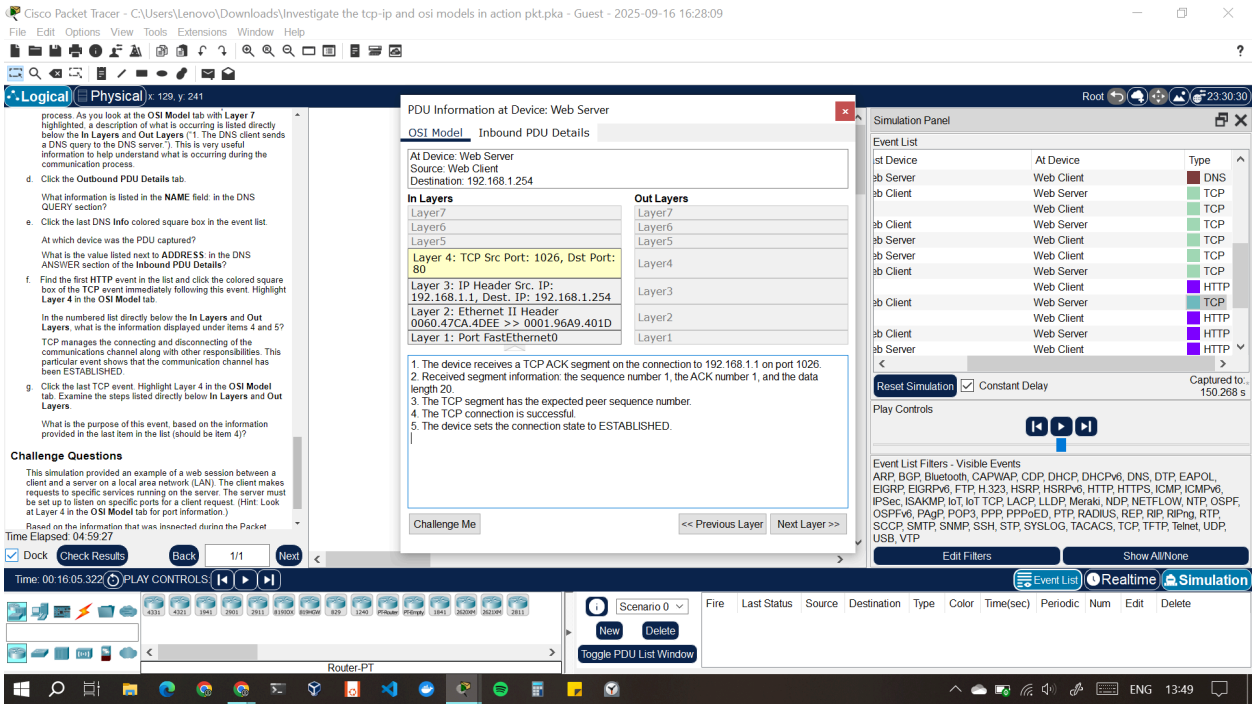


f. Find the first HTTP event in the list and click the colored square box of the TCP event immediately following this event. Highlight Layer 4 in the OSI Model tab.

Question:

In the numbered list directly below the In Layers and Out Layers, what is the information displayed under items 4 and 5? **Answer:**

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



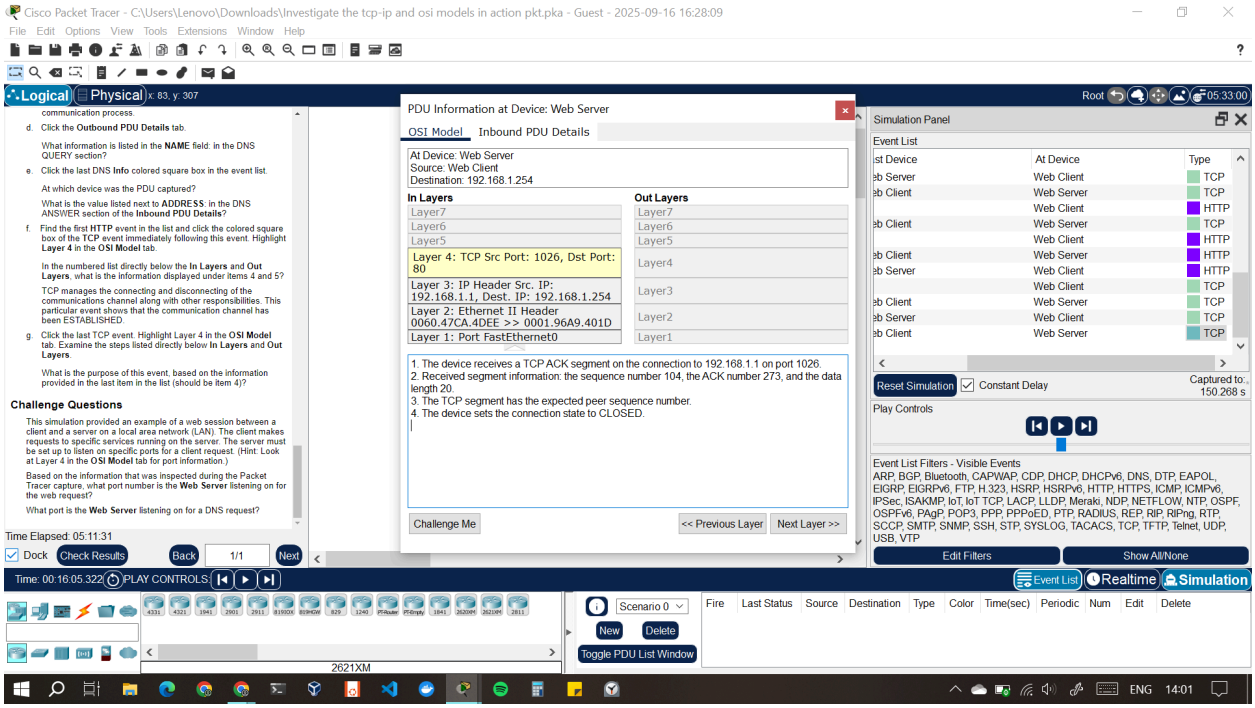
TCP manages the connecting and disconnecting of the communications channel along with other responsibilities. This particular event shows that the communication channel has been ESTABLISHED.

g. Click the last TCP event. Highlight Layer 4 in the OSI Model tab. Examine the steps listed directly below In Layers and Out Layers.

Question:

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

Answer: The device closes the TCP connection communication channel and sets its state to CLOSED.

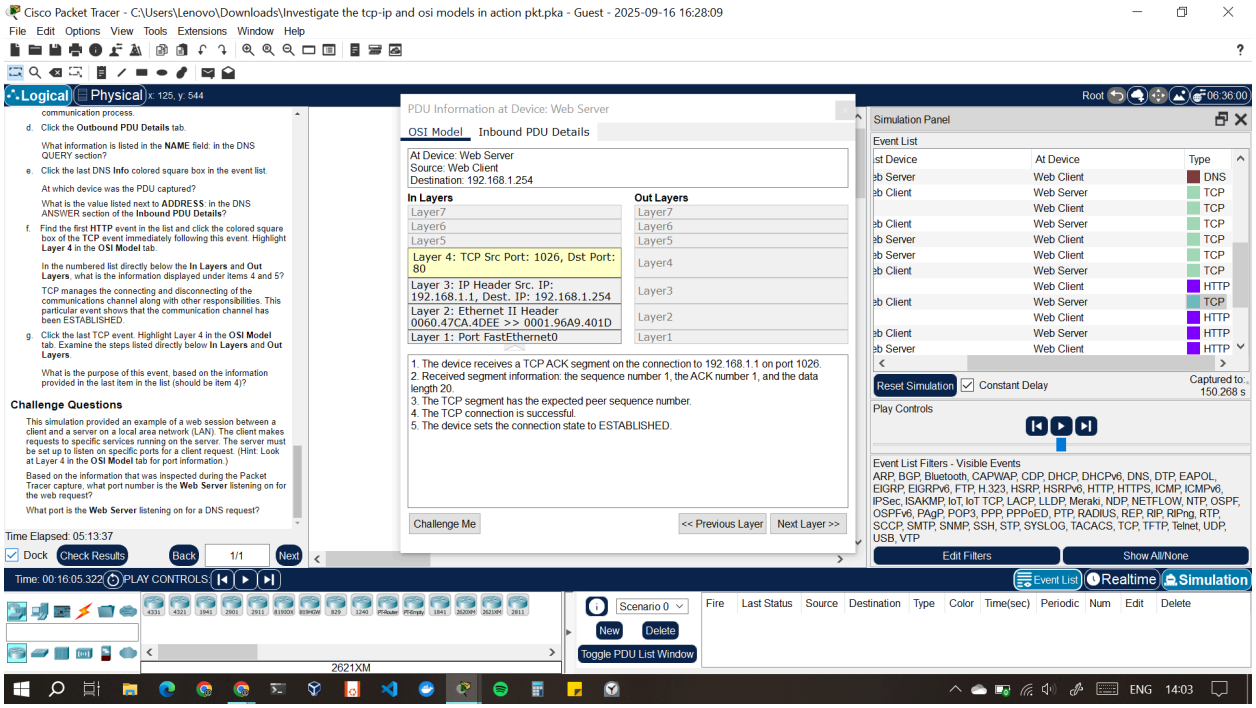


Challenge Questions

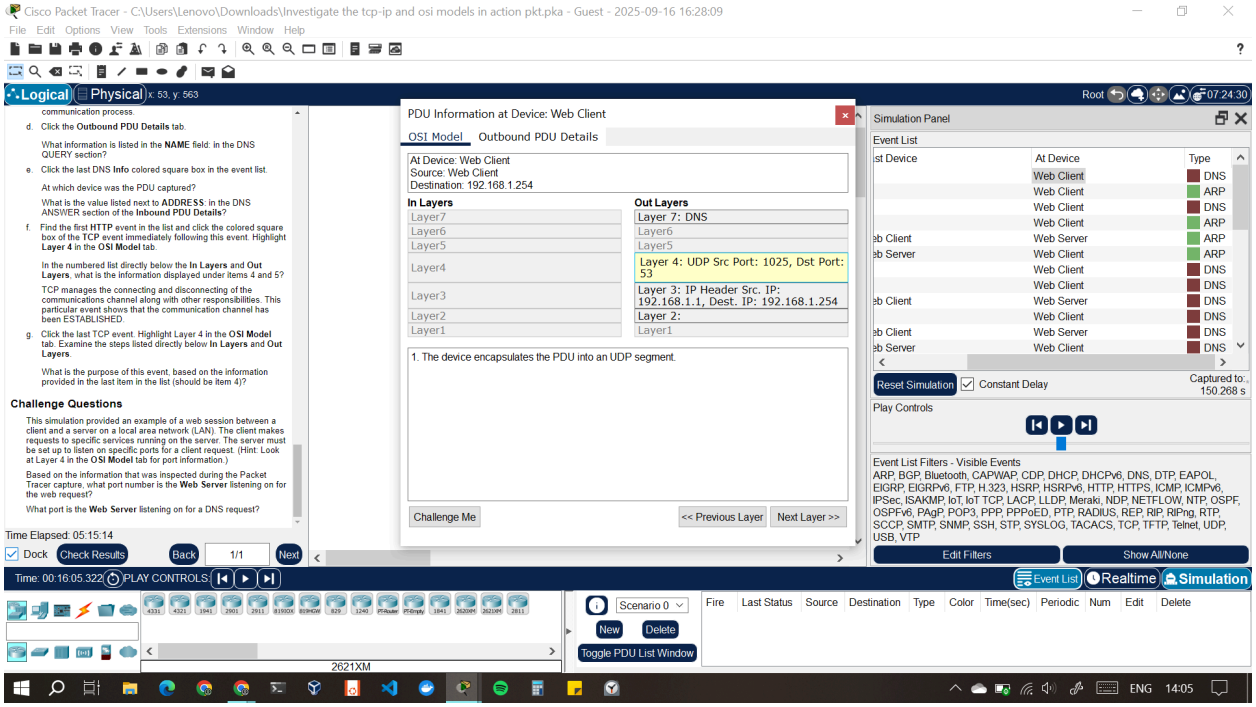
This simulation provided an example of a web session between a client and a server on a local area network (LAN). The client makes requests to specific services running on the server. The server must be set up to listen on specific ports for a client request. (Hint: Look at Layer 4 in the OSI Model tab for port information.)

1. Based on the information that was inspected during the Packet Tracer capture, what port number is the Web Server listening on for the web request?

   Answer: Port number 80



2. What port is the Web Server listening on for a DNS request?
Answer: Port number 53



Conclusion

This activity showed how the OSI and TCP/IP models work together to facilitate communication across the network and how the encapsulation process works. I was able to generate and examine HTTP web traffic, DNS resolution, and how TCP manages connections in detail. Similarly, I was also able to observe the Protocol Data Units(PDUs) at each layer and see how IP addressing, port numbers, and protocol headers allow data to move from a client to a server and back.

Moreover, the activity also helped me understand the difference between outbound and inbound traffic, how to identify different services such as HTTP and DNS by the port numbers, and how TCP manages establishment and closed connections.

Hence, my understanding of the theory of TCP/IP and the OSI model was further enhanced by a practical approach to how protocols work and interact in different layers to ensure web services are delivered across a network.