

**COURSE: CLOUD AND NETORK SECURITY**

**NAME: DENISE SOPHY ONDISO MUTAYI**

**STUDENT NO: CS-CN09-25047**

**EXAMINE TCP/IP AND OSI MODELS IN ACTION WITH  
CISCO PACKET TRACER**

## Table of contents:

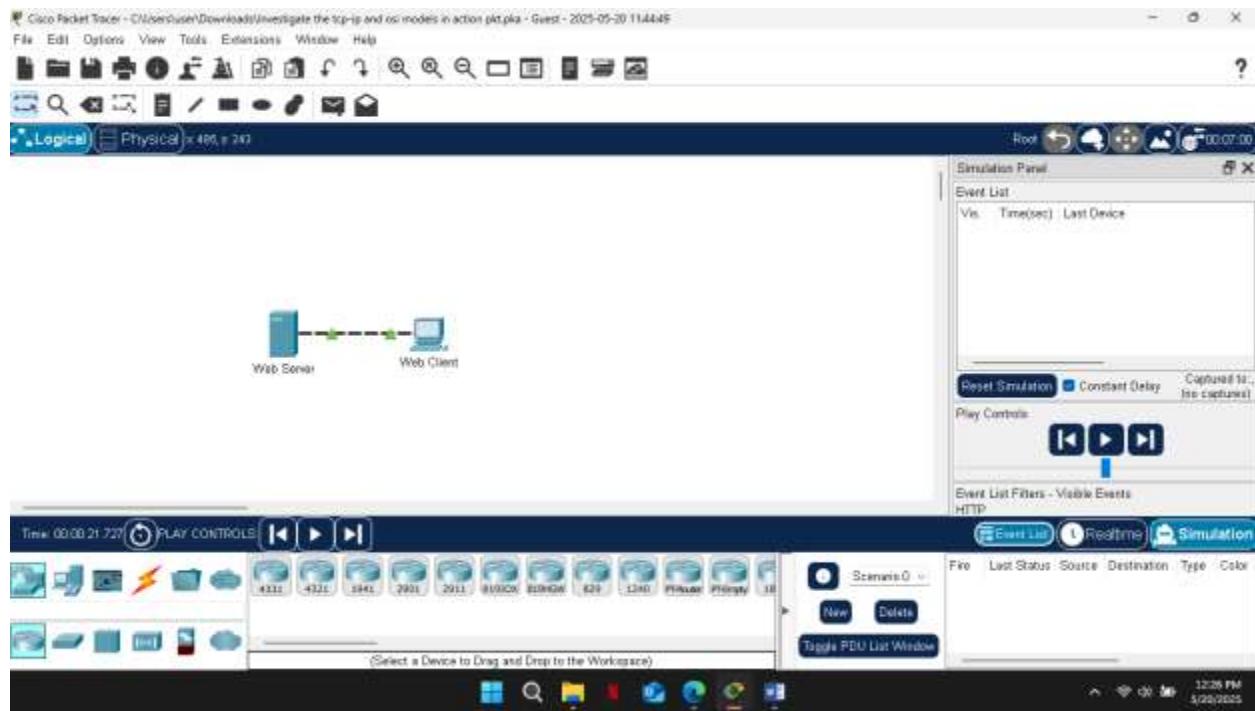
INTRODUCTION .....	4
SWITCH FROM REALTIME TO SIMULATION MODE.....	5
Generate web (HTTP) traffic .....	5
ACCESSING THE WEB.....	6
Questions: .....	6
What information is listed in the numbered steps directly below the In Layers and Out Layers boxes for Layer 7?.....	6
What is the <b>Dst Port</b> value for <b>Layer 4</b> under the <b>Out Layers</b> column? .....	7
What is the <b>Dest. IP</b> value for <b>Layer 3</b> under the <b>Out Layers</b> column? .....	7
What information is displayed at Layer 2 under the <b>Out Layers</b> column?.....	8
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?.....	9
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? ...	9
What is the <b>Host</b> listed under the <b>HTTP</b> section of the <b>PDU Details</b> ? What layer would this information be associated with under the <b>OSI Model</b> tab?.....	10
Comparing the information displayed in the In Layers column with that of the Out Layers column, what are the major differences? .....	11
Question: .....	12
How many tabs are displayed with this event? Explain. ....	12
Display Elements of the TCP/IP Protocol Suite .....	13
Question: .....	13
What information is listed in the <b>NAME</b> field: in the DNS QUERY section? .....	13
Questions: .....	14
At which device was the PDU captured?.....	14
What is the value listed next to <b>ADDRESS</b> : in the DNS ANSWER section of the <b>Inbound PDU Details</b> ?.....	14
In the numbered list directly below the <b>In Layers</b> and <b>Out Layers</b> , what is the information displayed under items 4 and 5?.....	15
Question: .....	16
What is the purpose of this event, based on the information provided in the last item in the list (should be item 4)?.....	16
Challenge Questions .....	17

What port number is the Web Server listening on for the web request? .....	17
What port is the Web Server listening on for a DNS request? .....	17
CONCLUSION.....	18

## **INTRODUCTION**

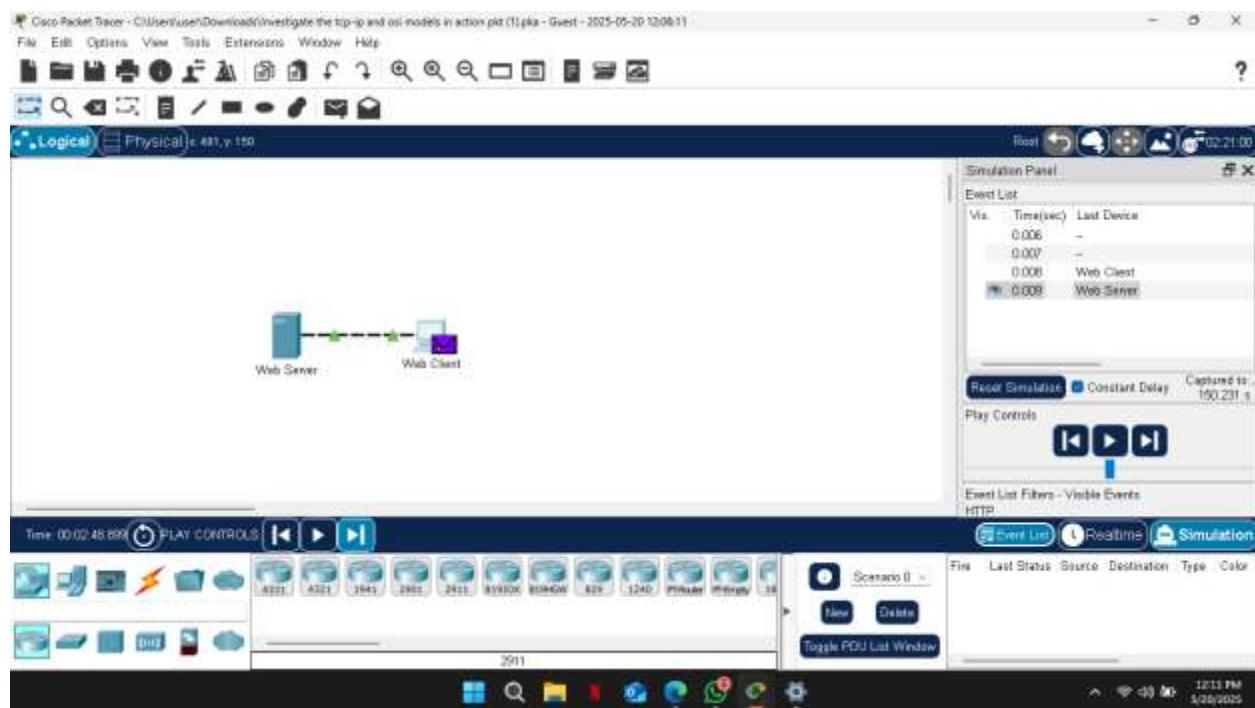
This Packet Tracer simulation was all about digging into how the TCP/IP and OSI models actually work when you request something as simple as a web page. Using the simulation mode in Packet Tracer, I was able to slow down time, watch packets move across the network, and really understand how each layer — from the application layer down to the physical layer — plays its part. By examining protocols like HTTP, DNS, TCP, and ARP, I got a hands-on view of the encapsulation process, how IP addresses and MAC addresses are used, and how devices talk to each other behind the scenes.

## SWITCH FROM REALTIME TO SIMULATION MODE.

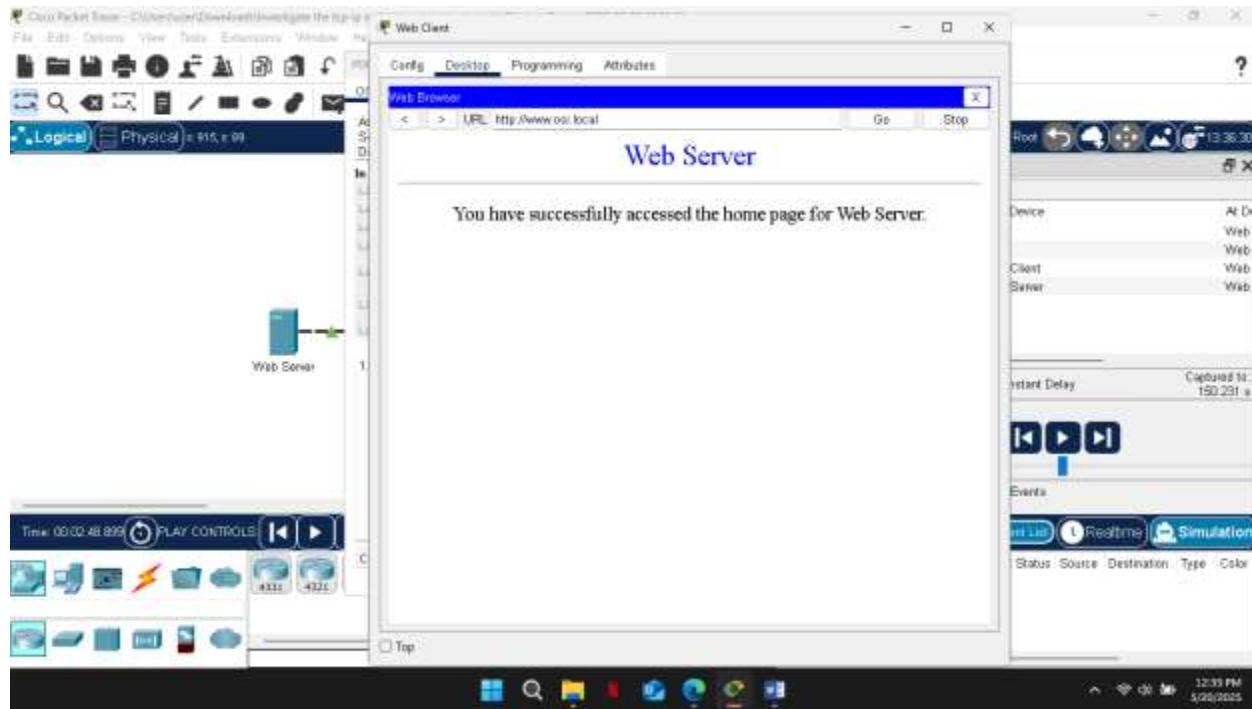


In simulation mode we get to see the *slow motion + pause + step-by-step* mode. I got to watch packets move from one device to another, inspect what's happening in the background.

### Generate web (HTTP) traffic.



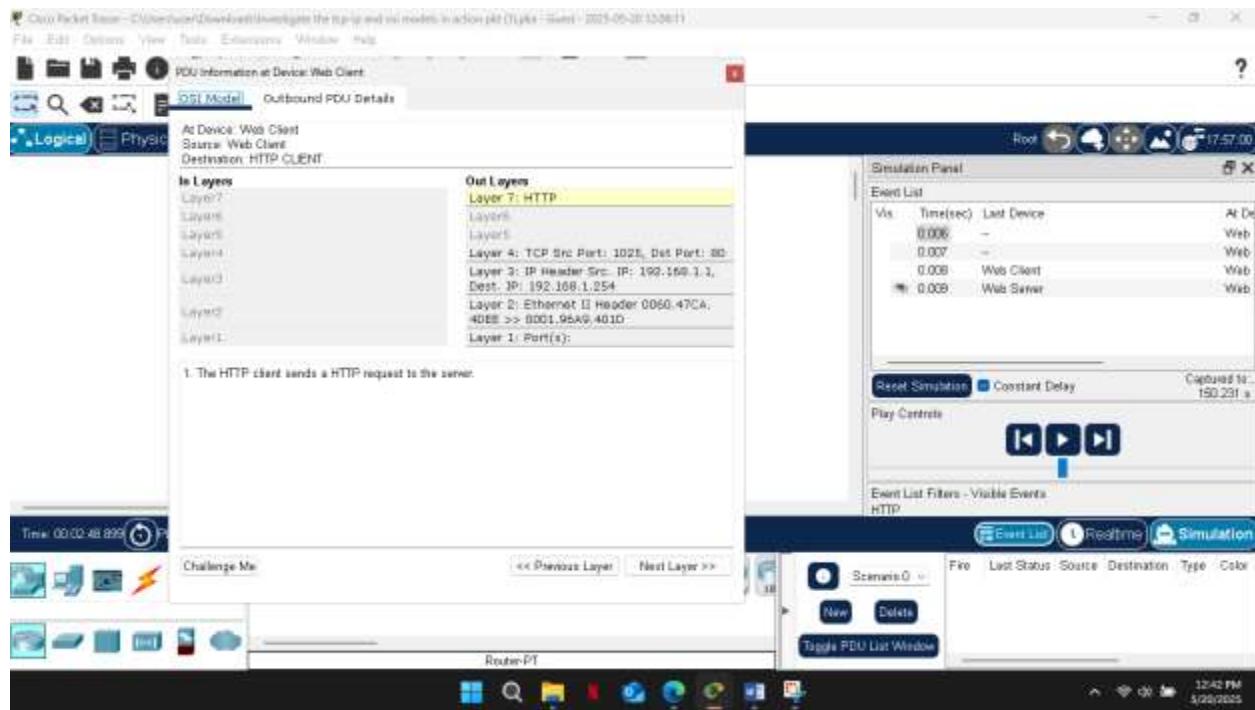
## ACCESSING THE WEB



Questions:

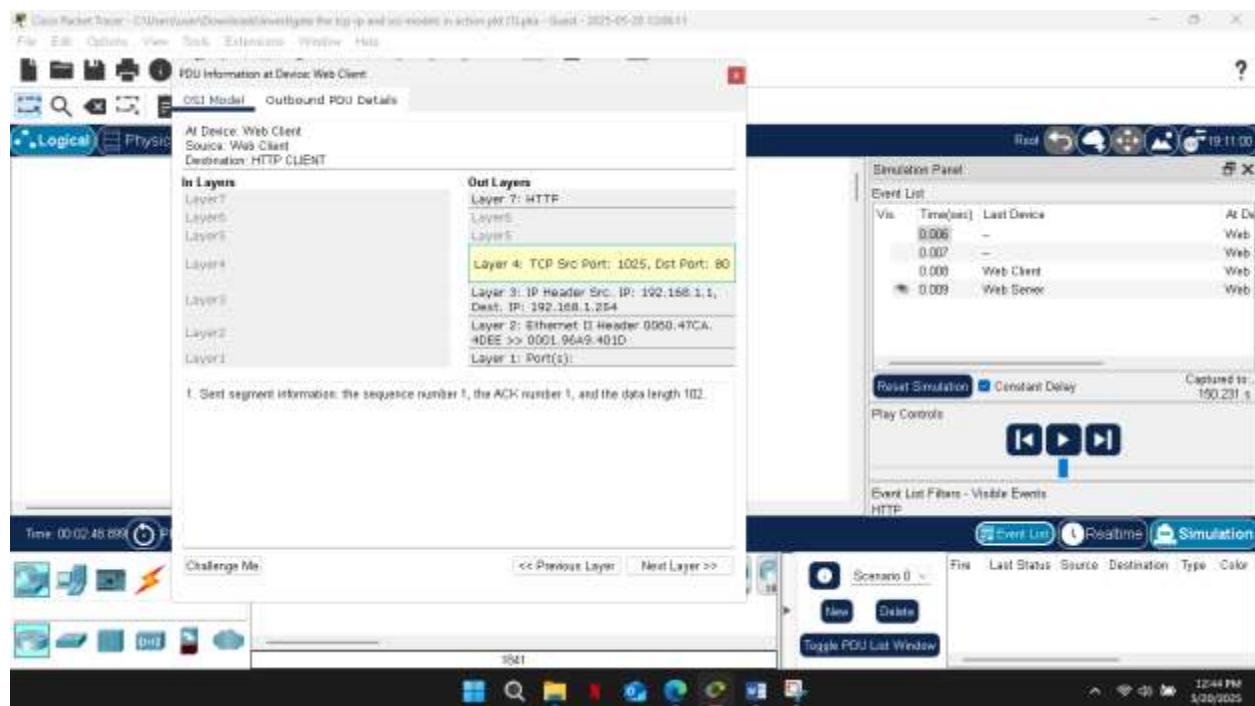
What information is listed in the numbered steps directly below the In Layers and Out Layers boxes for Layer 7?

In layer 7 HTTP is listed and the HTTP client sends a Http request to the server



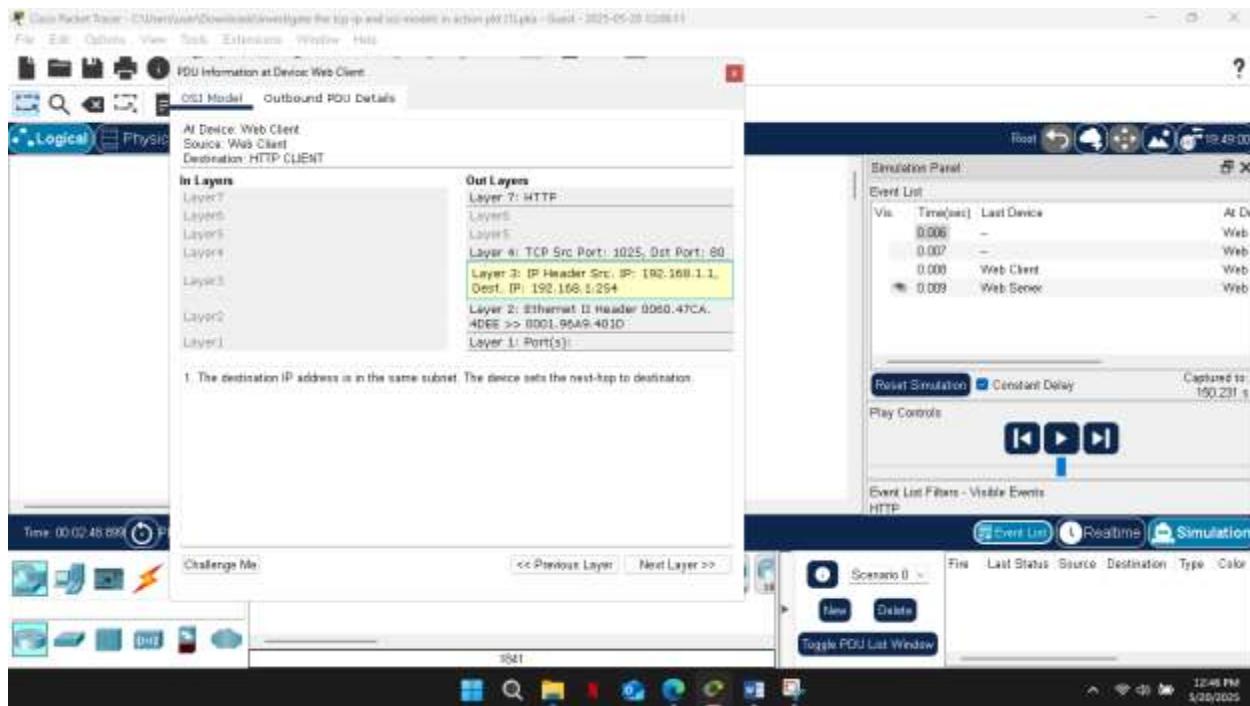
What is the **Dst Port** value for Layer 4 under the **Out Layers** column?

The DST PORT is port 80



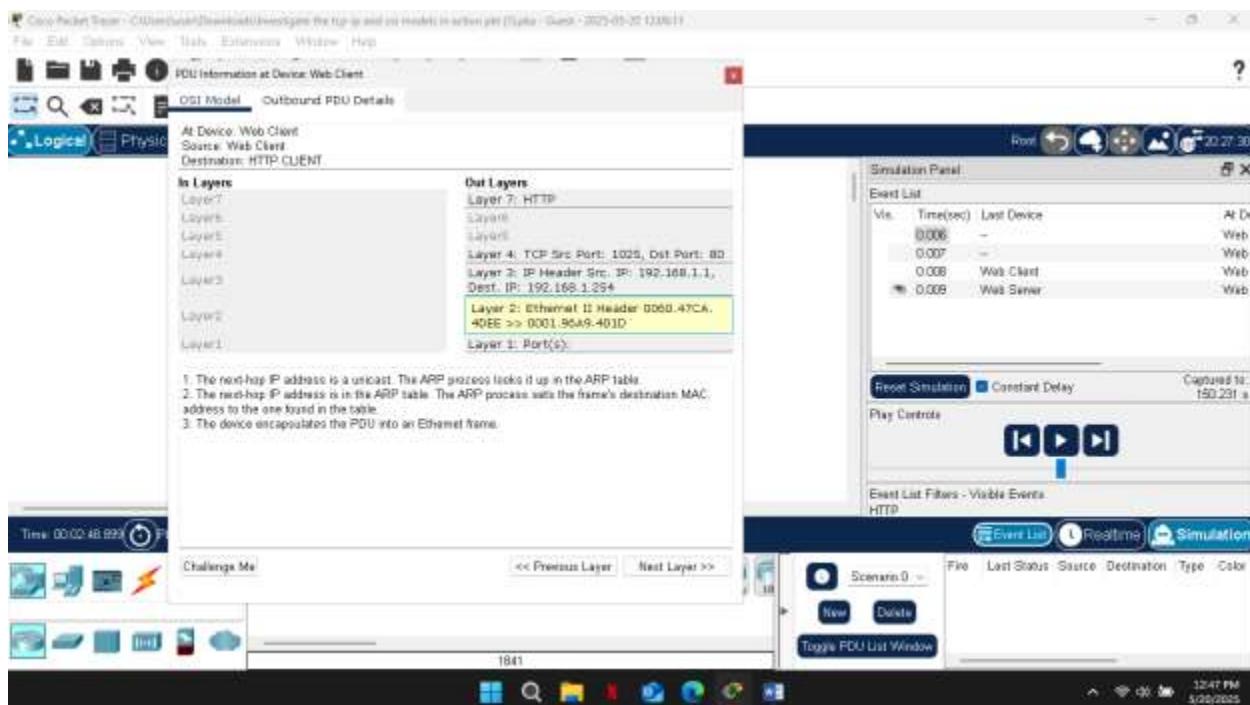
What is the **Dest. IP** value for Layer 3 under the **Out Layers** column?

The Dest IP in layer 3 is 192.168.1.254



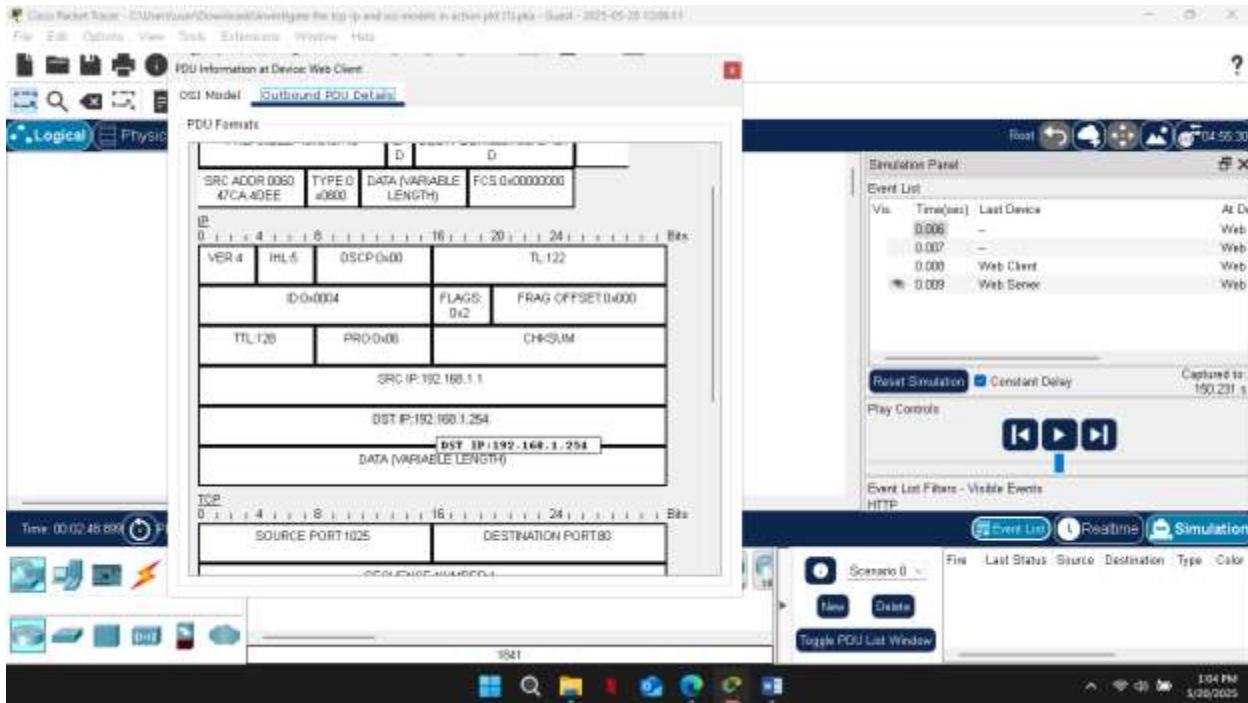
What information is displayed at Layer 2 under the **Out Layers** column?

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.



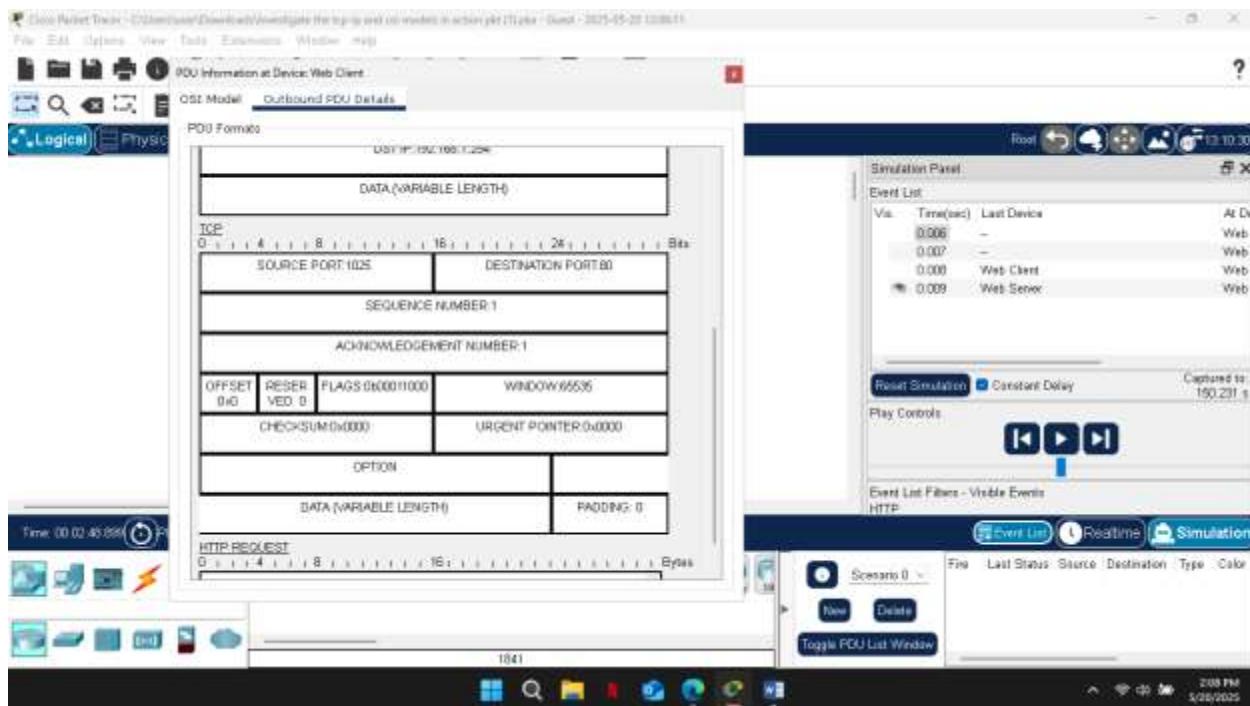
What is the common information listed under the IP section of PDU Details as compared to the information listed under the OSI Model tab? With which layer is it associated?

In both PDU and OSI Model tab the Dest IP:192.168.1.254 is the same, it is associated to the Network layer In the OSI Model tab and in the IP section of it.



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?

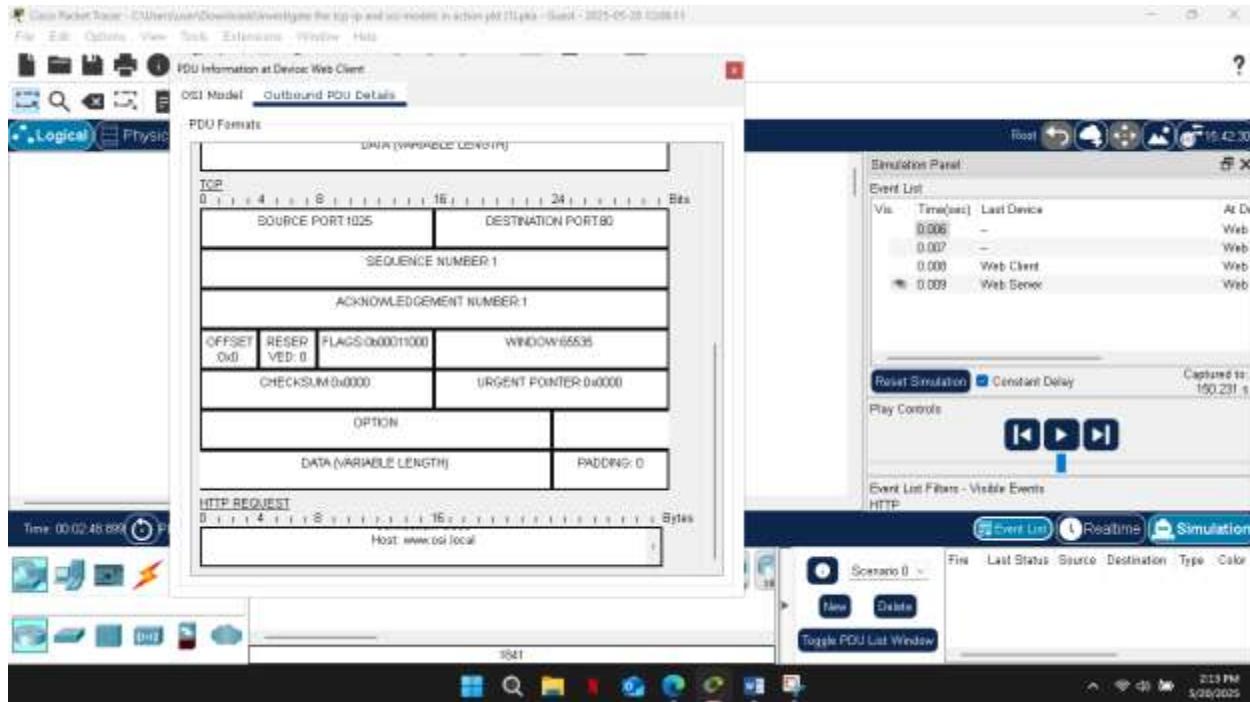
In both PDU and OSI Model tab the DESINATION PORT 80 is the same, it is associated to the Transport layer In the OSI Model tab and in the IP section of it.



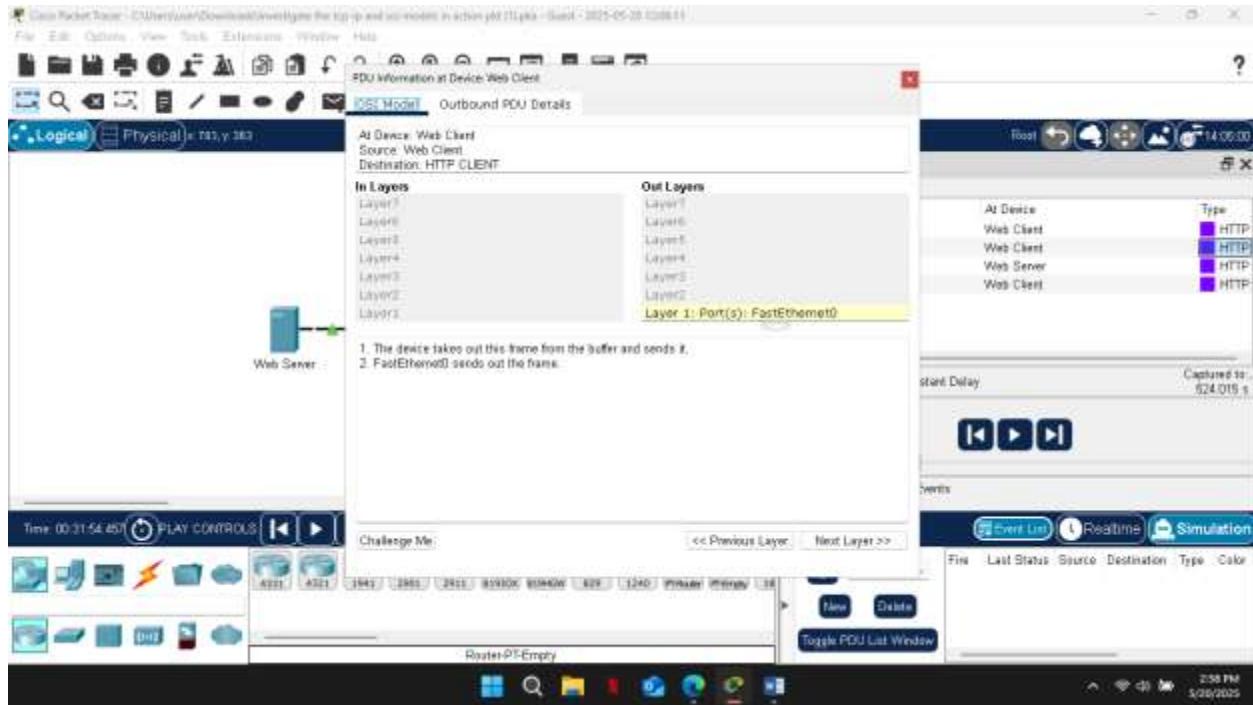
What is the **Host** listed under the **HTTP** section of the **PDU Details**? What layer would this information be associated with under the **OSI Model** tab?

Host: [www.osi.local](http://www.osi.local)

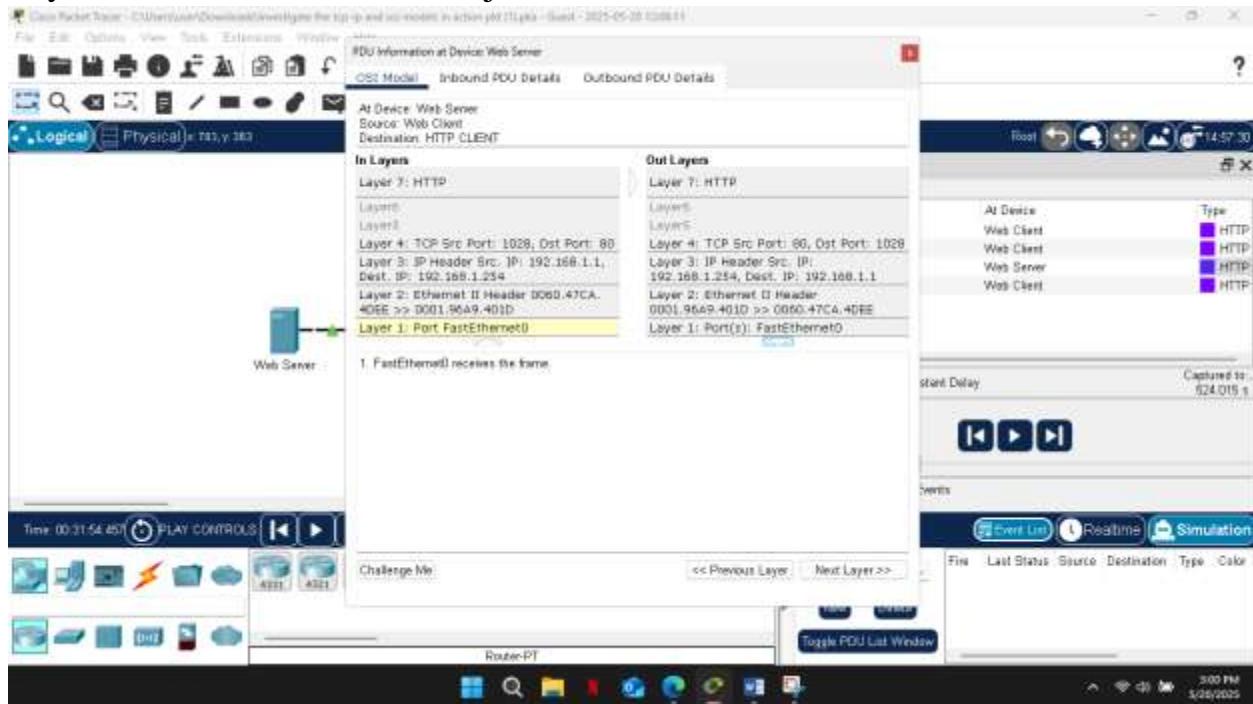
It is part of the application layer in the OSI MODEL it is the human to computer layer where applications can access network services.



Only Layer 1 is active (not grayed out). The device is moving the frame from the buffer and placing it on to the network.



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



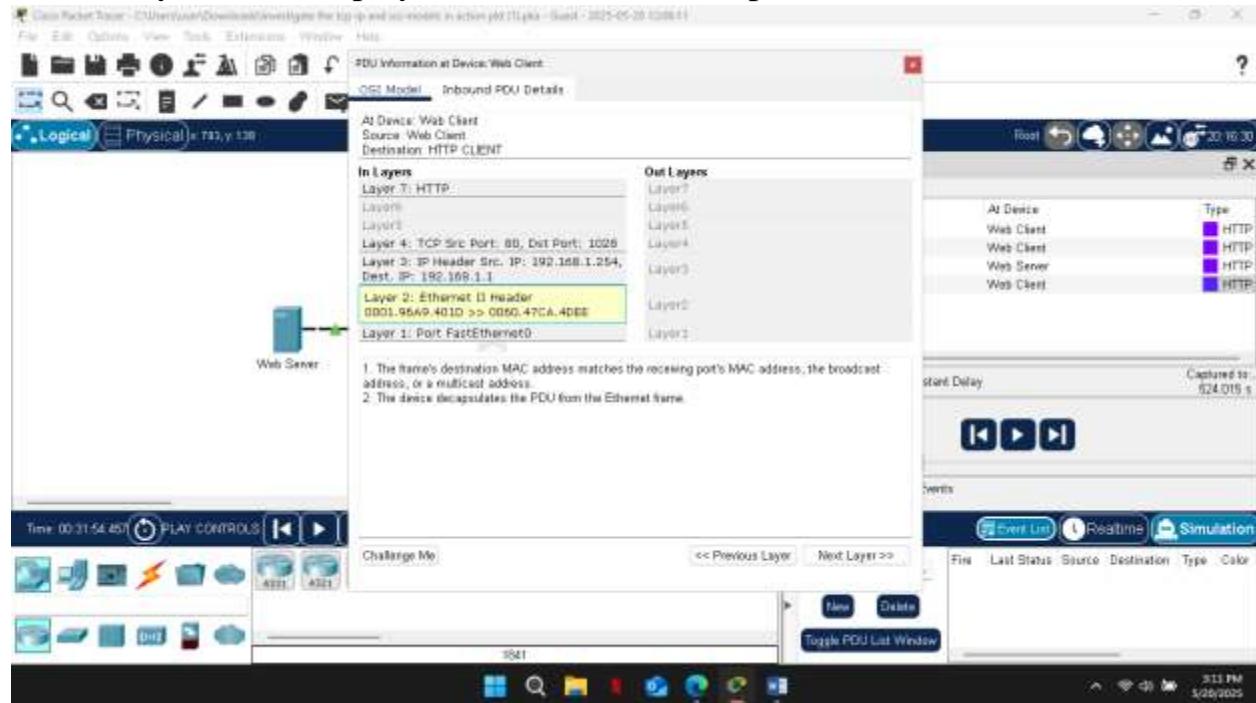
The In Layers represent data entering the Web Server, starting at the Physical Layer up to the Application Layer.

The Out Layers show the response being built from the Application Layer down to the Physical Layer.

The key difference is direction and purpose: one is processing incoming data, the other is constructing outgoing data

Question:

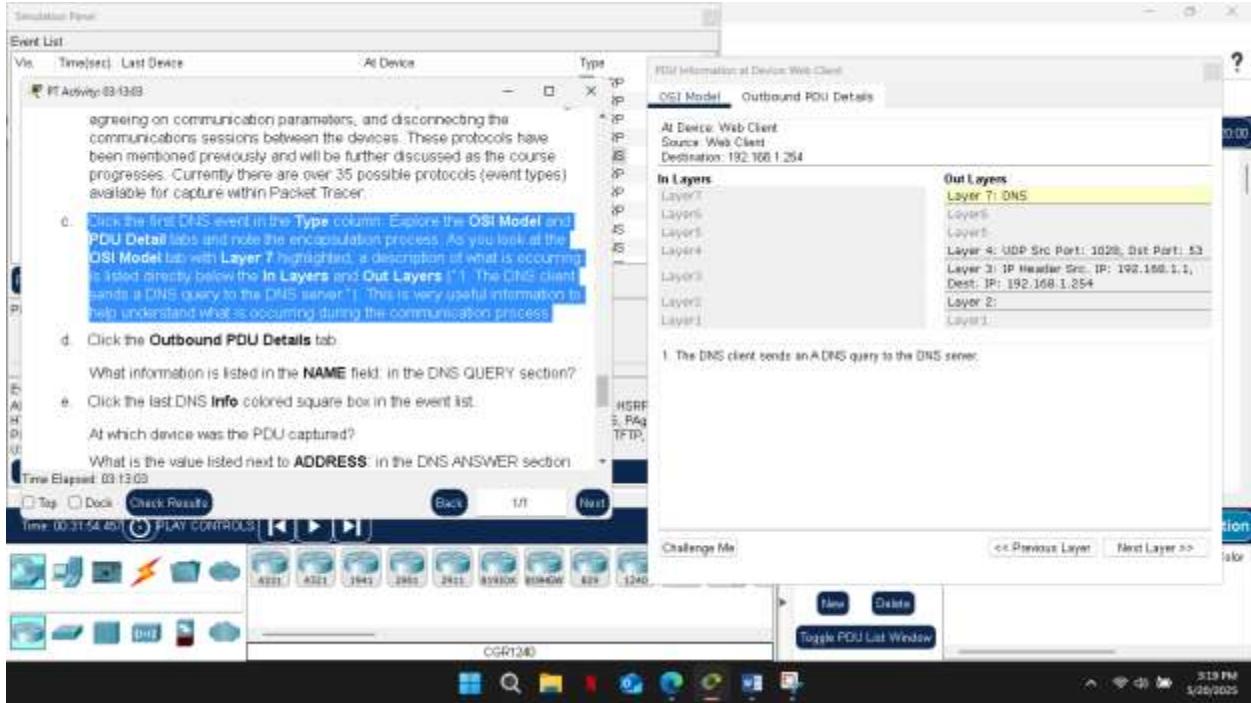
How many tabs are displayed with this event? Explain.



There are two tabs displayed: OSI Model and Inbound PDU Details. This is because the selected event involves the Web Client receiving data (an inbound packet), and thus only the layers and PDU details related to the incoming transmission are shown.

## Display Elements of the TCP/IP Protocol Suite

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.”)

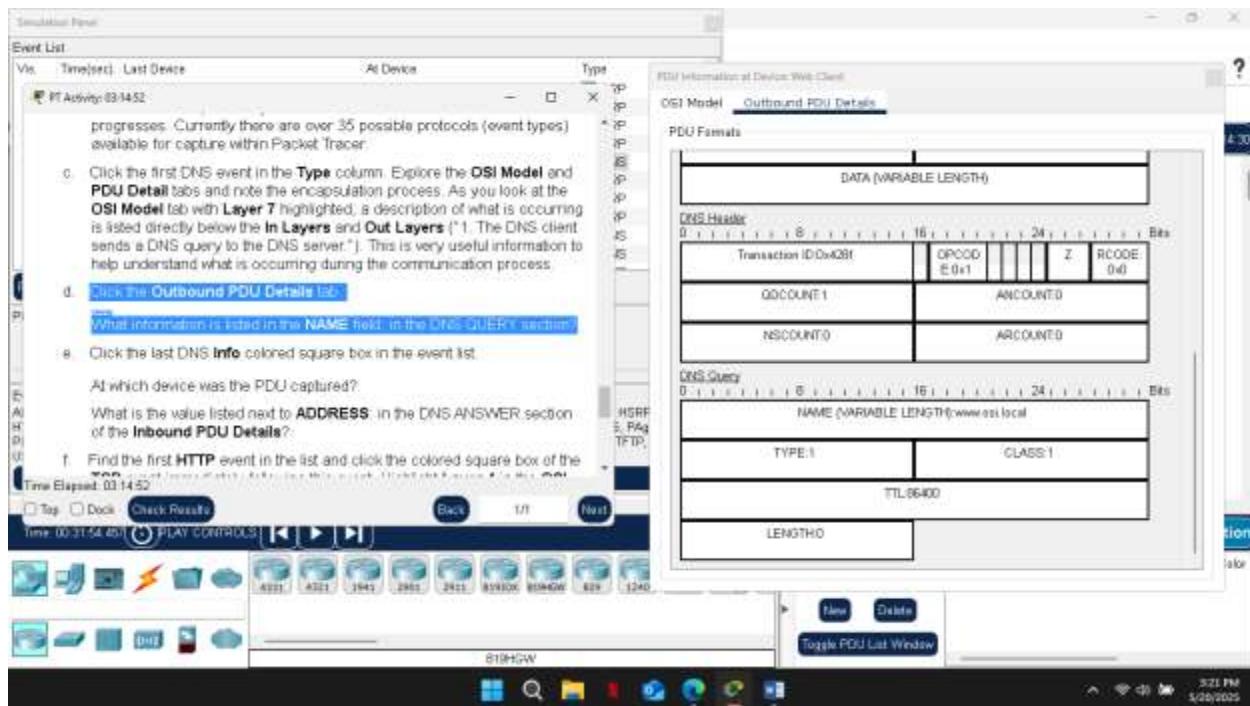


Click the **Outbound PDU Details** tab.

Question:

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

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



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

Questions:

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

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

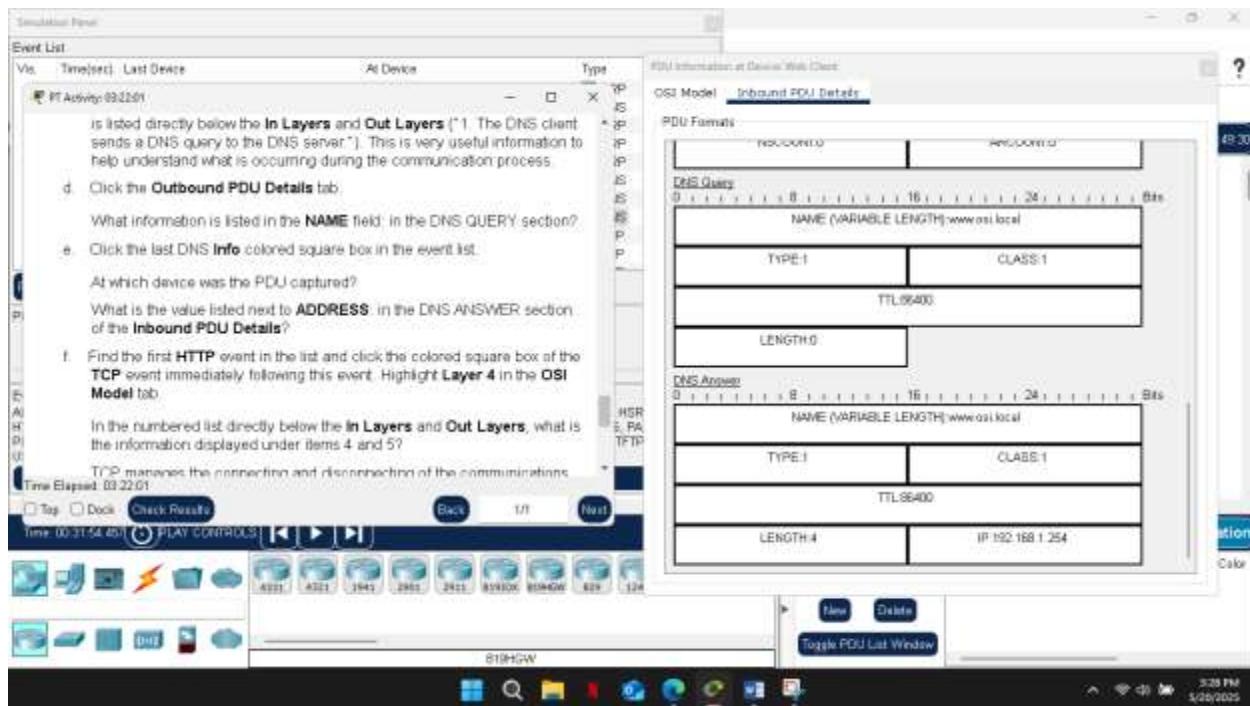
The screenshot shows the WinPcap NetworkMiner interface. The top menu bar includes File, Edit, Tools, Help, and a Simulation tab. The main window has several panes:

- Event List:** A table showing network events with columns: Id, Time(s), Last Device, At Device, and Source/Type. Events listed include various Web Client and Web Server interactions.
- FDU Information at Device: Web Client:** A detailed view of a selected event, showing OSI Model (At Device: Web Client) and Outbound PDU Details (Source: Web Client, Destination: HTTP CLIENT).
- In Layers:** A stack of layers for the selected packet, from Layer 1 (Port) to Layer 7 (HTTP).
- Out Layers:** A stack of layers for the selected packet, from Layer 1 (Port) to Layer 7 (HTTP).
- Play Controls:** Buttons for playing back the capture.
- Event List Filters - Visible Events:** A list of protocols: ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCP6, DNS, DTP, EAPOL, EIGRP, EIGRP6, FTP, HTTPS, ICMP, ICMP6, IPSec, ISAHMP, iSIT, iST, TCP, LACP, LLDP, Mpls, NDR, NETFLOW, NTP, OS PPP, PPPoE, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCR, SMTP, SNMP, SSH, STP, SYSLOG, TAC, USB, VTP.
- Edit Filters** and **Show All** buttons.
- Time: 00:31:54.451** and **PLAY CONTROLS** buttons.
- Challenge Me...** button.
- cc Previous Layer** and **Next Layer >>** buttons.
- New** and **Delete** buttons.
- Toggle PDU List Window** button.

Below it is layer 3

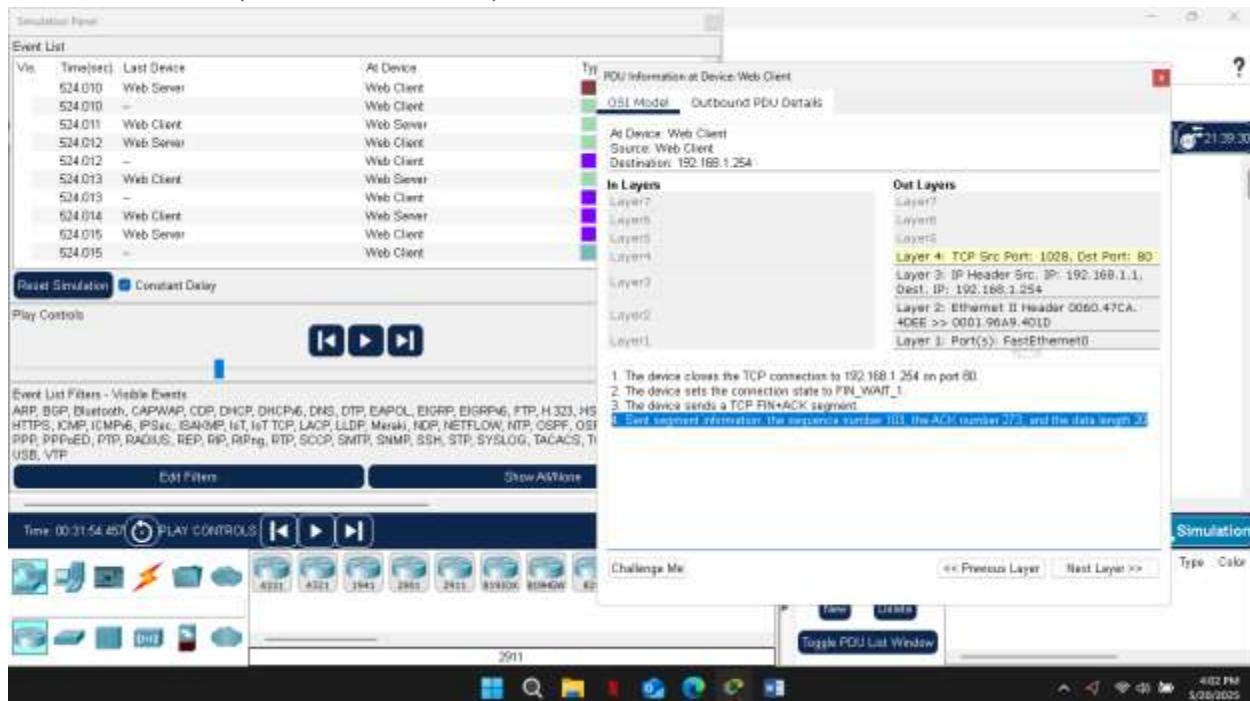
IP header src:IP 192.168.1.1

THE DEST IP : 192.168.1.254



Question:

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



The purpose of this event is to send a segment of application data across an established TCP connection.

- Sequence number 103 shows where this chunk starts in the data stream.
- ACK number 273 confirms the sender received all prior data up to byte 272.
- Data length 20 means 20 bytes of new data are being pushed out.

### Challenge Questions

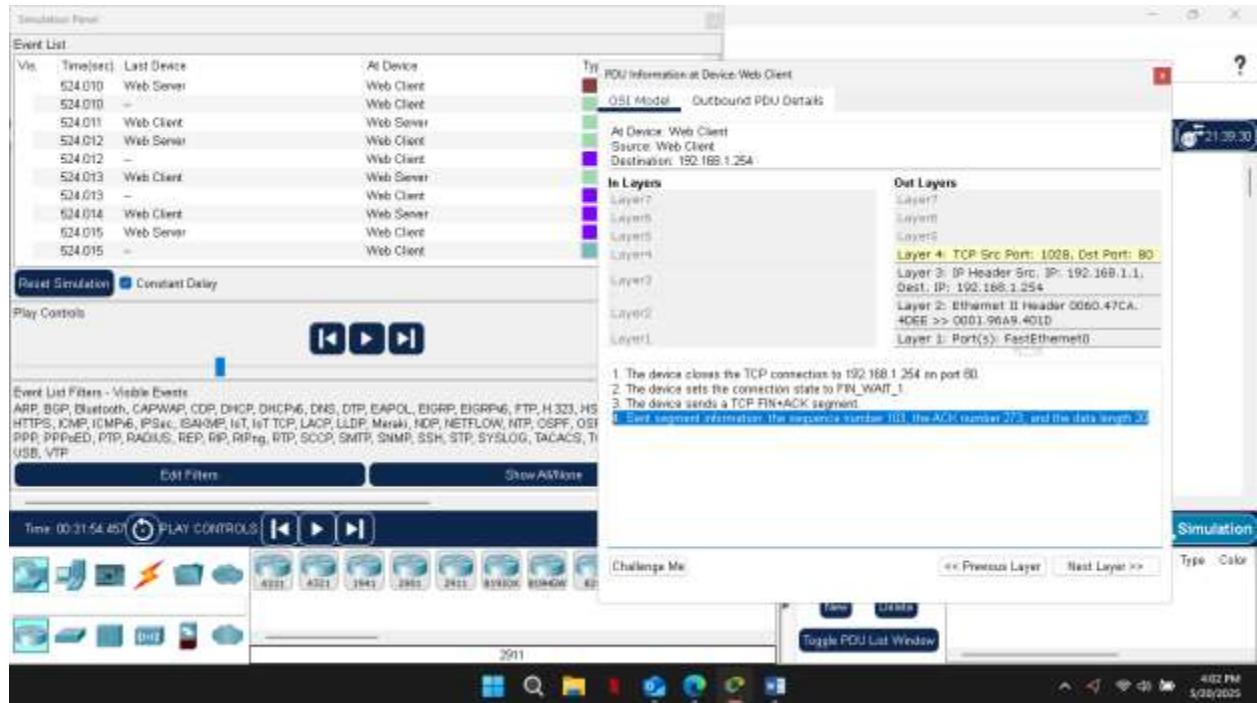
Based on the information that was inspected during the Packet Tracer capture

What port number is the Web Server listening on for the web request?

**Port 80** — the default port for HTTP web traffic.

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

Port 1028- assigned by the client to listen for a dns request.



## CONCLUSION

This simulation provided a detailed walkthrough of a typical client-server interaction within a local area network (LAN), highlighting key layers in the OSI Model that power modern web communication. We traced the journey of DNS queries and HTTP requests as they moved across devices and ports.

Through analysis of the captured PDUs, we identified:

1. The PDU was captured at the Web Client — the initiating device making requests to the server.
2. In the DNS Answer section, we discovered the resolved IP 192.168.1.254 for www.osi.local, meaning the DNS server successfully mapped the domain to a reachable server inside the LAN.
3. By examining Layer 4 (Transport Layer), we confirmed the Web Server listens on port 80 for HTTP traffic — the industry-standard for web services. The client used port 1028 to initiate the request.
4. The TCP event with sequence number 103, ACK number 273, and data length 20 signaled the actual transfer, confirming that the HTTP communication is fully underway. This represents a reliable TCP segment delivering part of the requested web data.