CLOUD AND NETWORK SECURITY REPORT

CHARLES GITHINJI

CS-CNS07-24006

WEEK 1: Assignment 1

PACKET TRACER: Investigate the TCP/IP and OSI Models In Action

INTRODUCTIONS

This lab is aimed at using Packet Tracer to investigate the TCP/IP protocol suite and the OSI model by viewing the data content sent across the network at each layer.

Objectives

- Examine HTTP Web Traffic
- Display Elements of the TCP/IP protocol suite

Background

This simulation activity is intended to provide a foundation for understanding the TCP/IP protocol suite and the relationship to the OSI model. Simulation mode allows you to view the data contents being sent across the network at each layer.

As data moves through the network, it is broken down into smaller pieces and identified so that the pieces can be put back together when they arrive at the destination. Each piece is assigned a specific name (protocol data unit [PDU]) and associated with a specific layer of the TCP/IP and OSI models. Packet Tracer simulation mode enables you to view each of the layers and the associated PDU. The following steps lead the user through the process of requesting a web page from a web server by using the web browser application available on a client PC.

Even though much of the information displayed will be discussed in more detail later, this is an opportunity to explore the functionality of Packet Tracer and be able to visualize the encapsulation process.

Part 1: Examine HTTP Web Traffic

Step 1: Switch from real-time to simulation mode

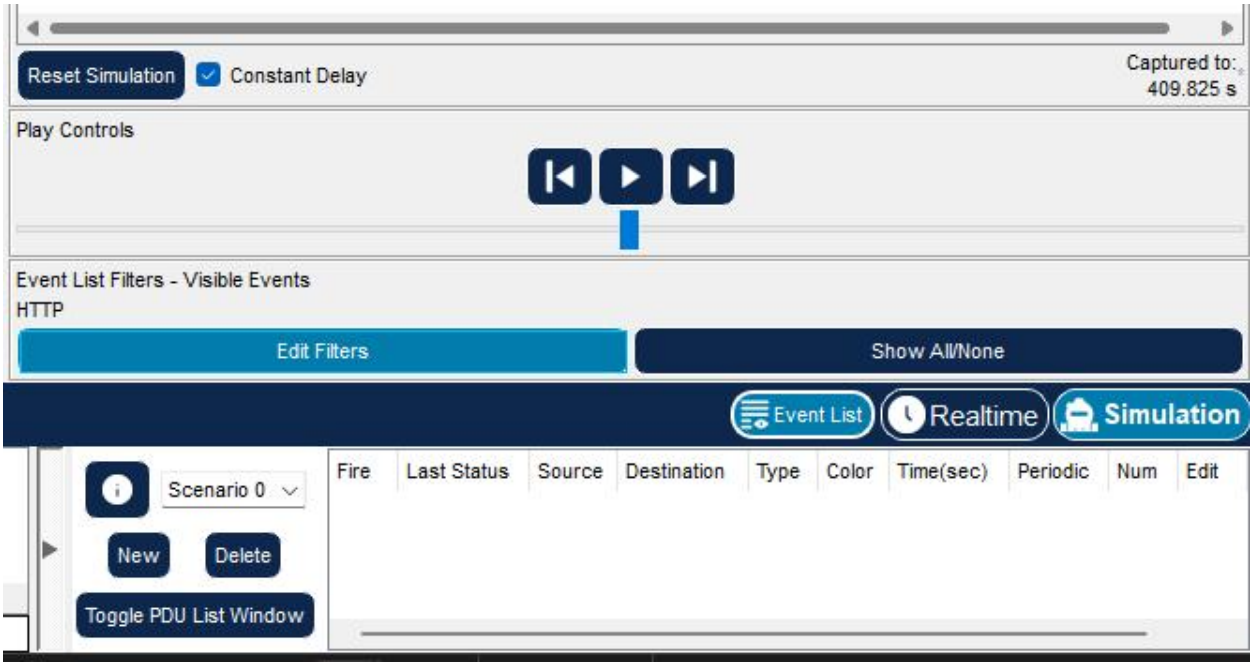
a. Click **the Simulation** mode icon to switch from **Real-time** mode to **Simulation** mode.

b. Select **HTTP** from **the Event list filter**

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 checkboxes 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.

THE FIGURE



Step 2: **Generate web (HTTP) traffic**

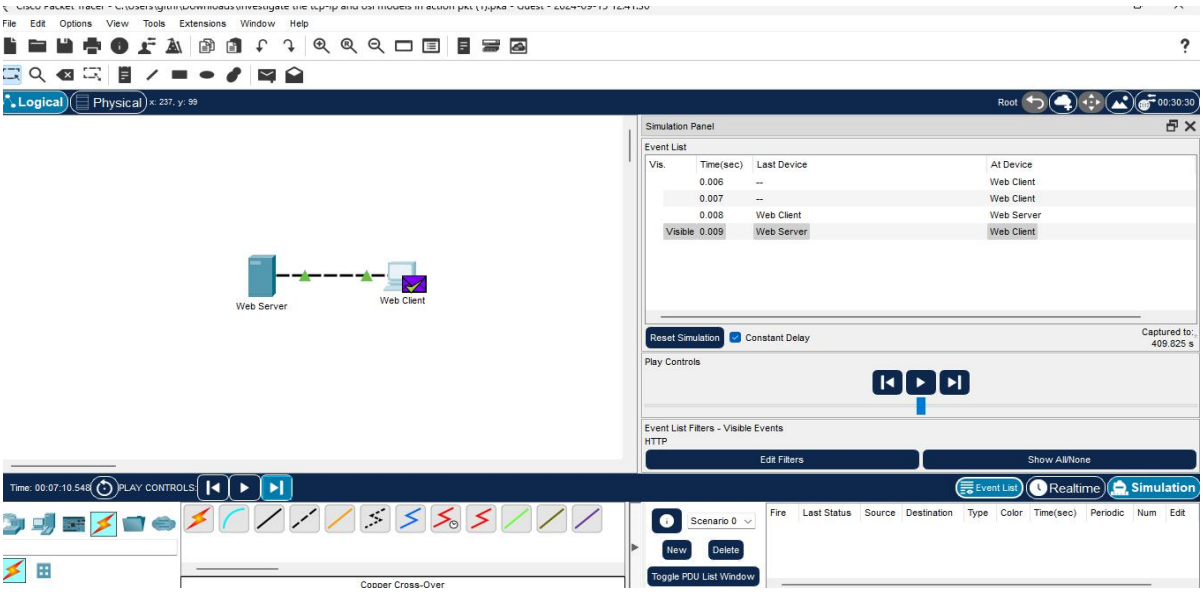
a. Click Web Client in the far left pane

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

d. Click capture/forward four times. There should be four events in the Events List

a. Look at the web client web browser page. Did anything change? ***The web page was returned from the web server***



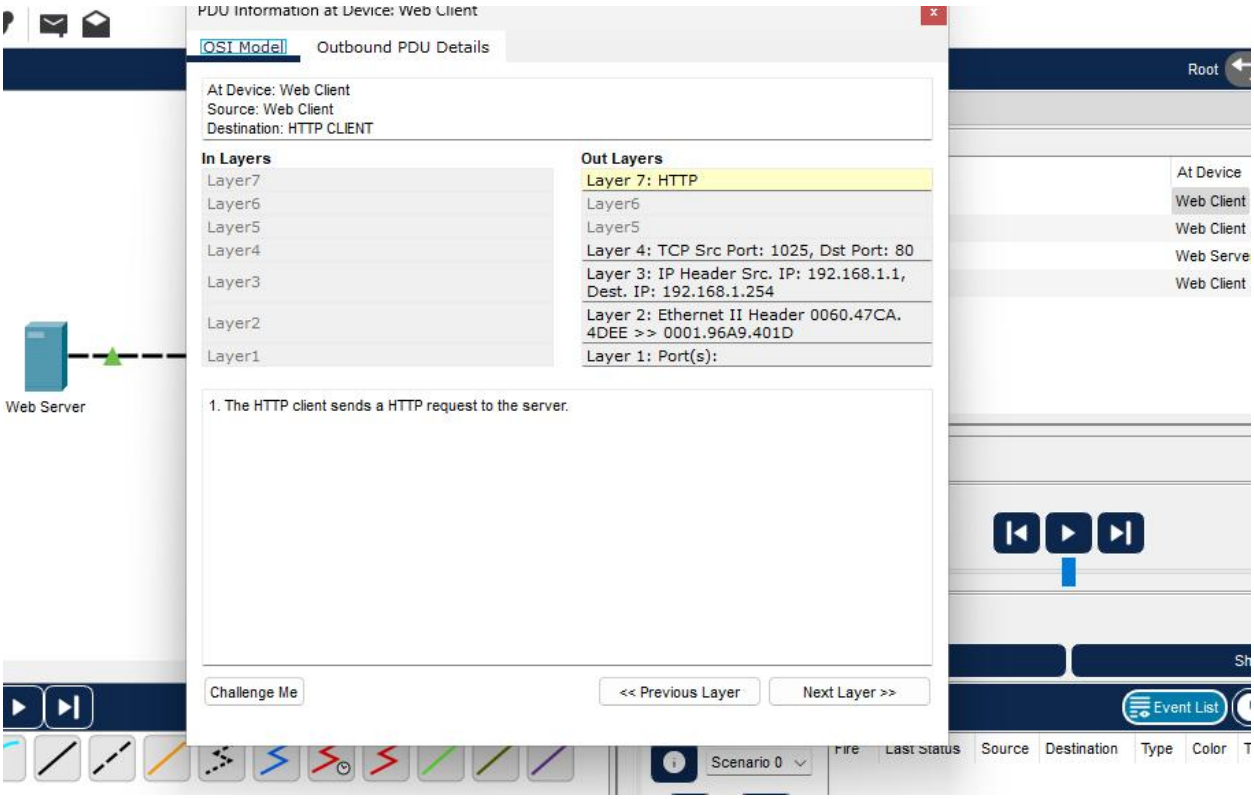
e. Click the first colored square box under the **Event List** > **Type** column. It may be necessary to expand the **Simulation Panel** or use the scrollbar directly below the **Event List**.

f. Ensure that the **OSI Model** tab is selected.

Under the **Out Layers** column, click **Layer 7**

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

The HTTP client sends a HTTP request to the server



What is the **Dst Port** value for **Layer 4** under the **Out Layers** column? *port 80*

What is the **Dest. IP** value for **Layer 3** under the **Out Layers** column? Port 192.168.1.254

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

Layer 2 Ethernet II Header and inbound and outbound MAC addresses.

g. Click the **Outbound PDU Details** tab.
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? *SRC IP AND DST IP AT LAYER 3*

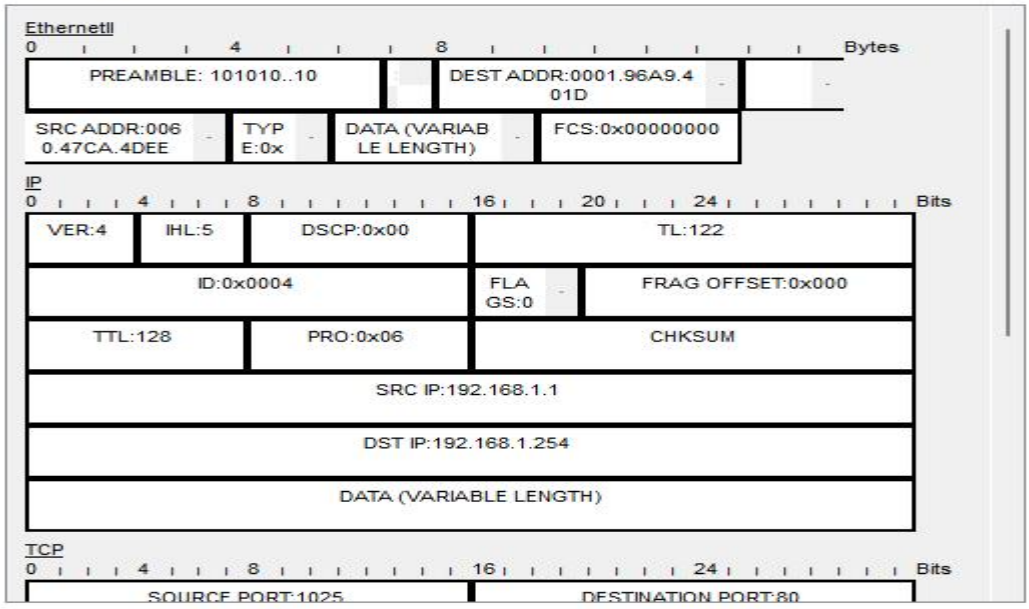
What is the common information listed under the **TCP** section of **PDU Details**, as compared to the information listed under the **OSI Model** tab, and with which layer is it associated? Source port and DST port at layer 4

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?
www.oosi.local , layer 7

PDU Information at Device: Web Client

OSI Model | Outbound PDU Details

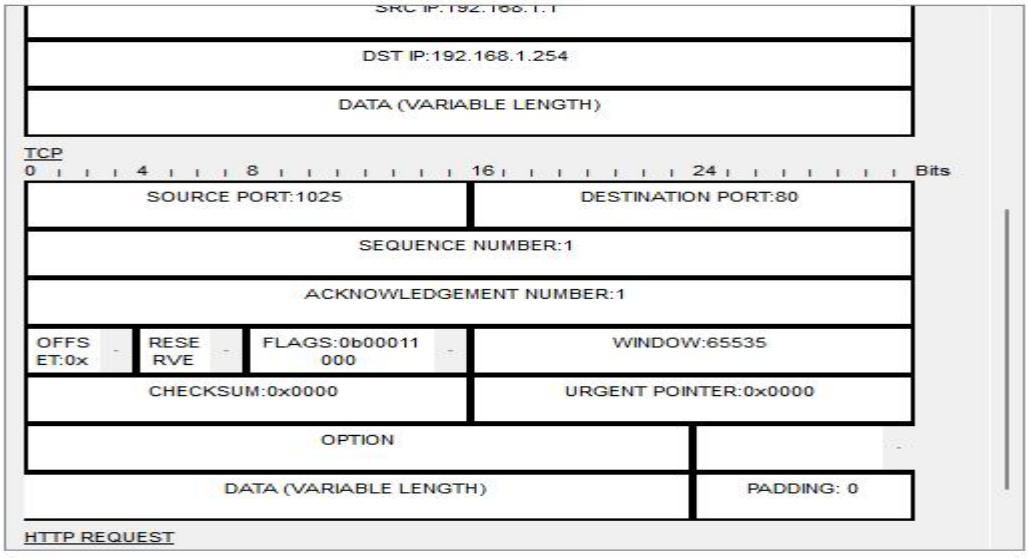
PDU Formats



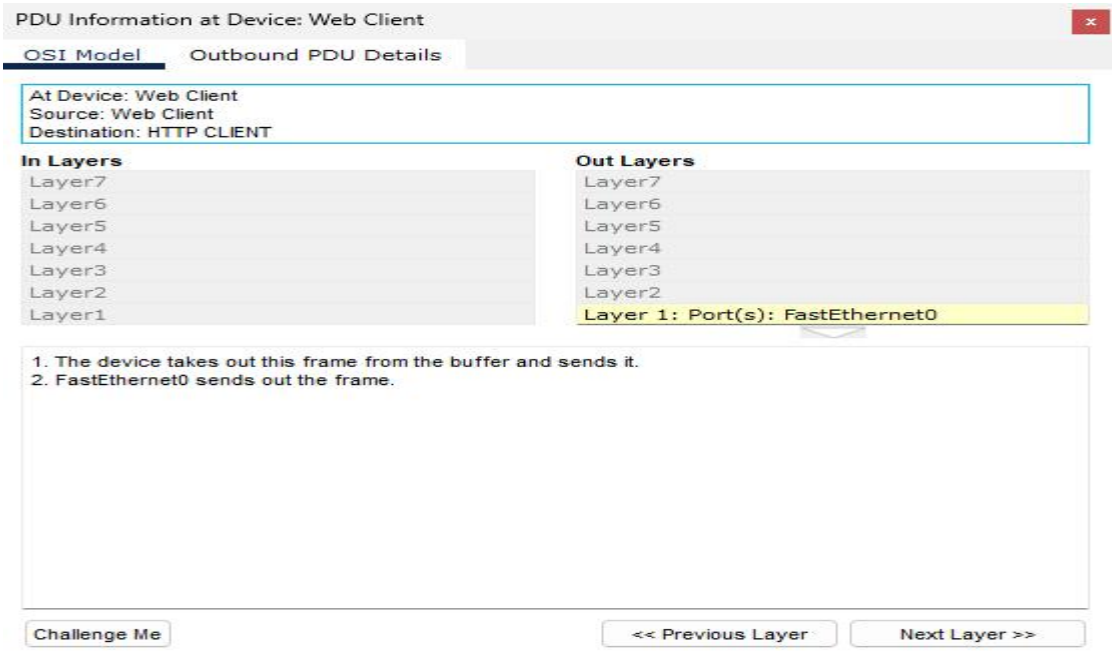
PDU Information at Device: Web Client

OSI Model | Outbound PDU Details

PDU Formats

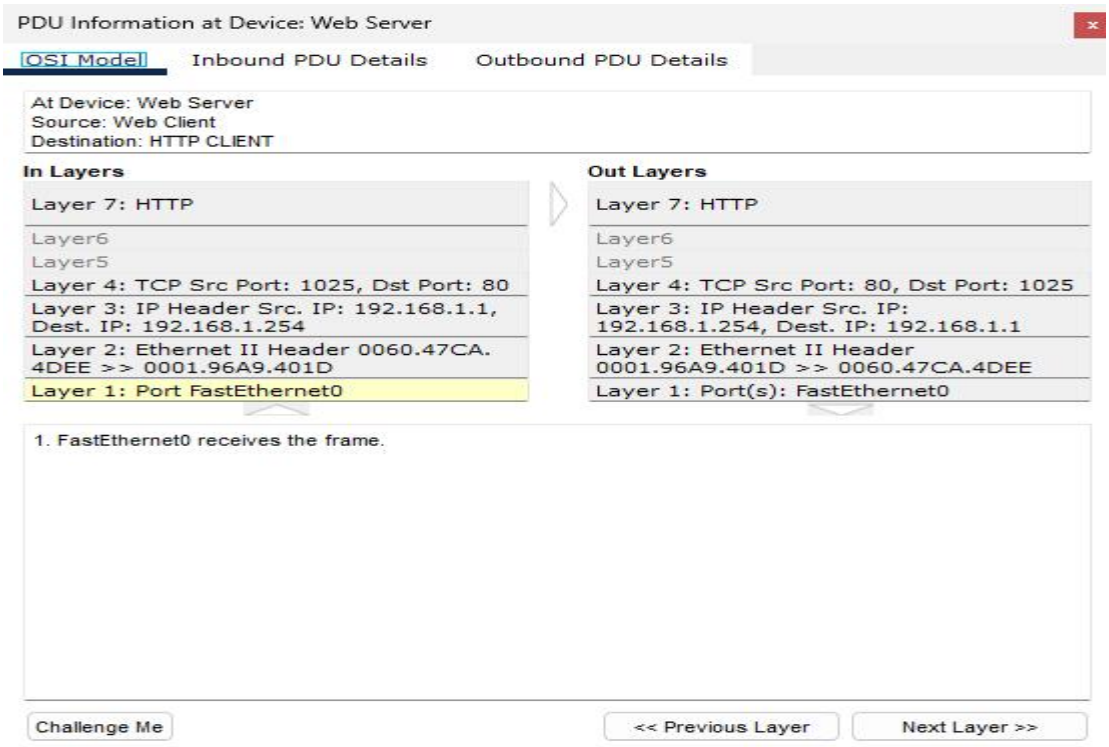


h. Click the next colored square box under the **Event List** > **Type** column. Only Layer 1 is active (not grayed out). The device is moving the frame from the buffer and placing it on to the network

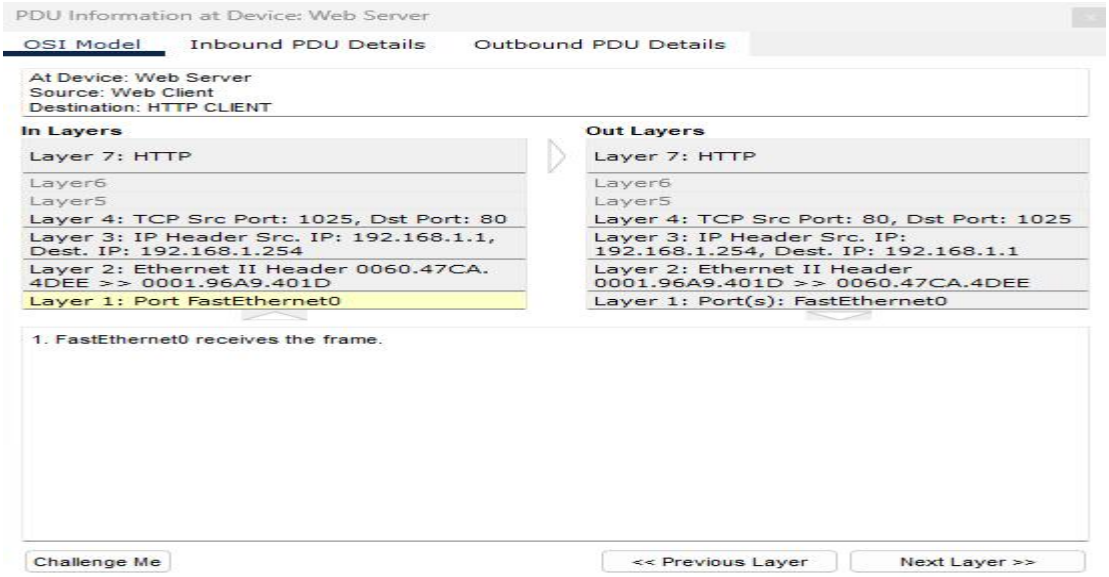


.

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.

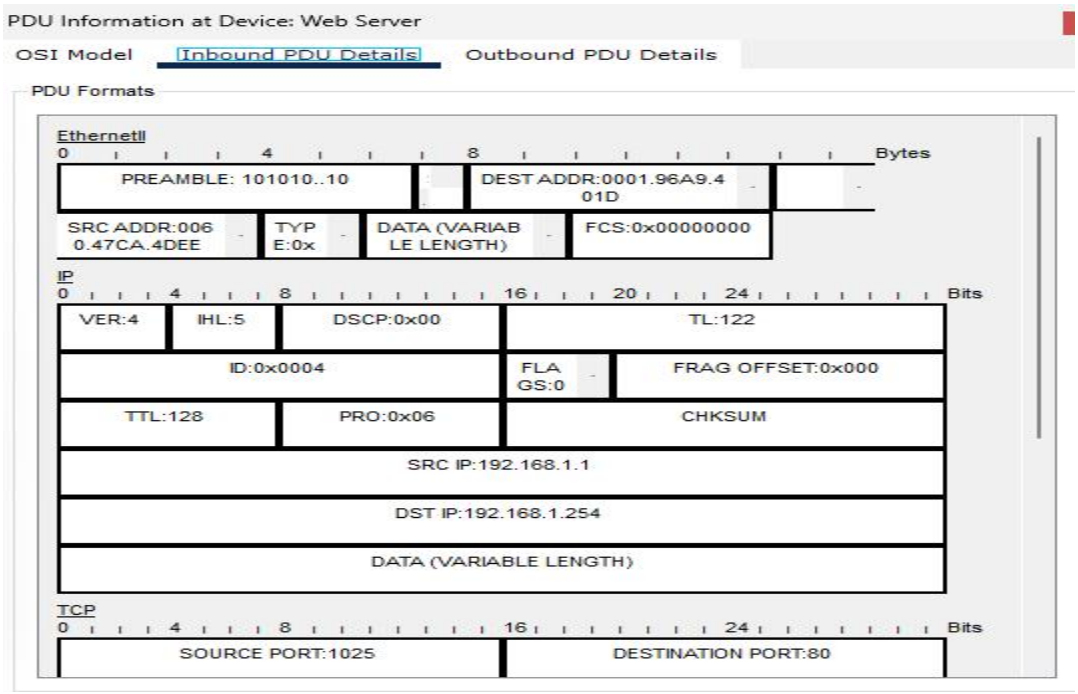


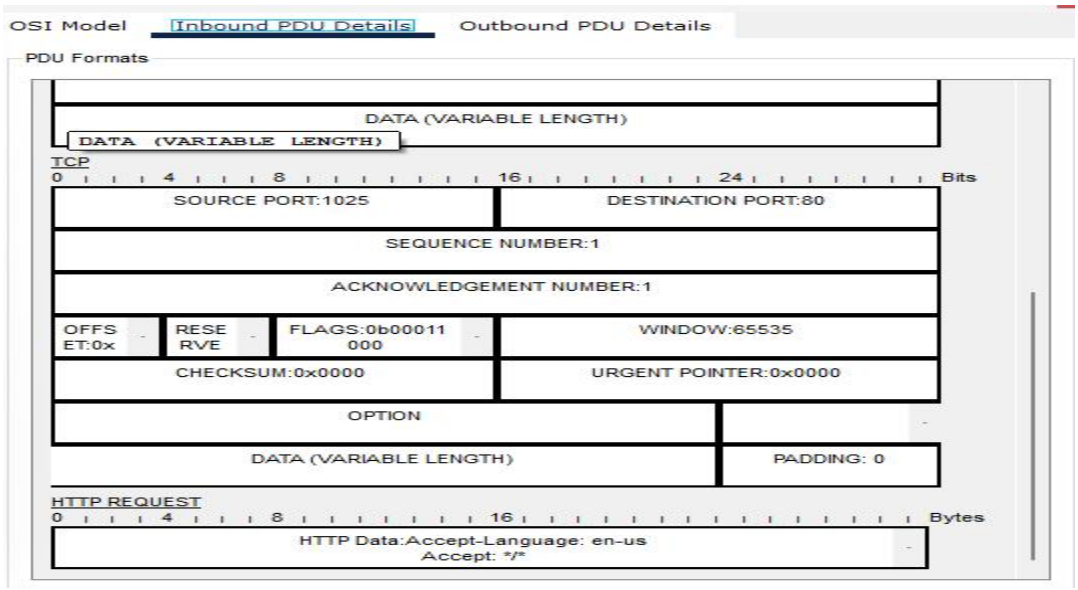
Comparing the information displayed in the **In Layers** column with that of the **Out Layers** column, what are the major differences? The src and Dst, Src and Dst Ips and MAC addresses have been swapped



The main difference is between the source and destination ip address and port

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

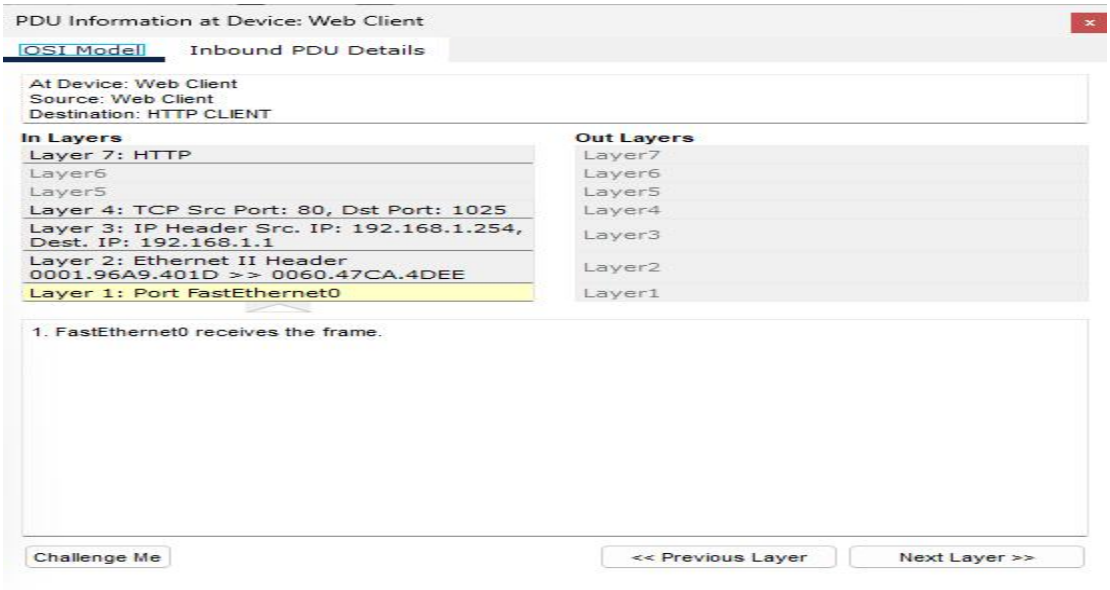




k. Click the last colored square box under the **Info** column.

How many tabs are displayed with this event? Explain.

2, one for the OSI model and the inbound PDU: this is the receiving device



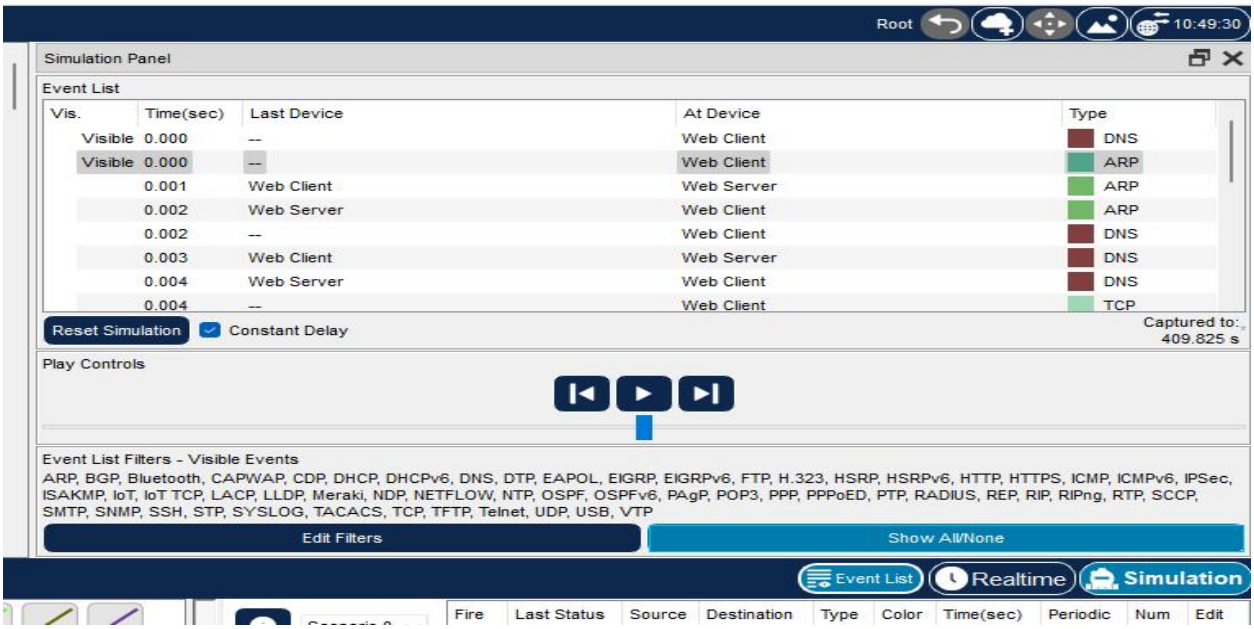
Part 2: Display Elements of the TCP/IP protocol Suite

Step 1: View additional Events

a. Close any open PDU information windows.

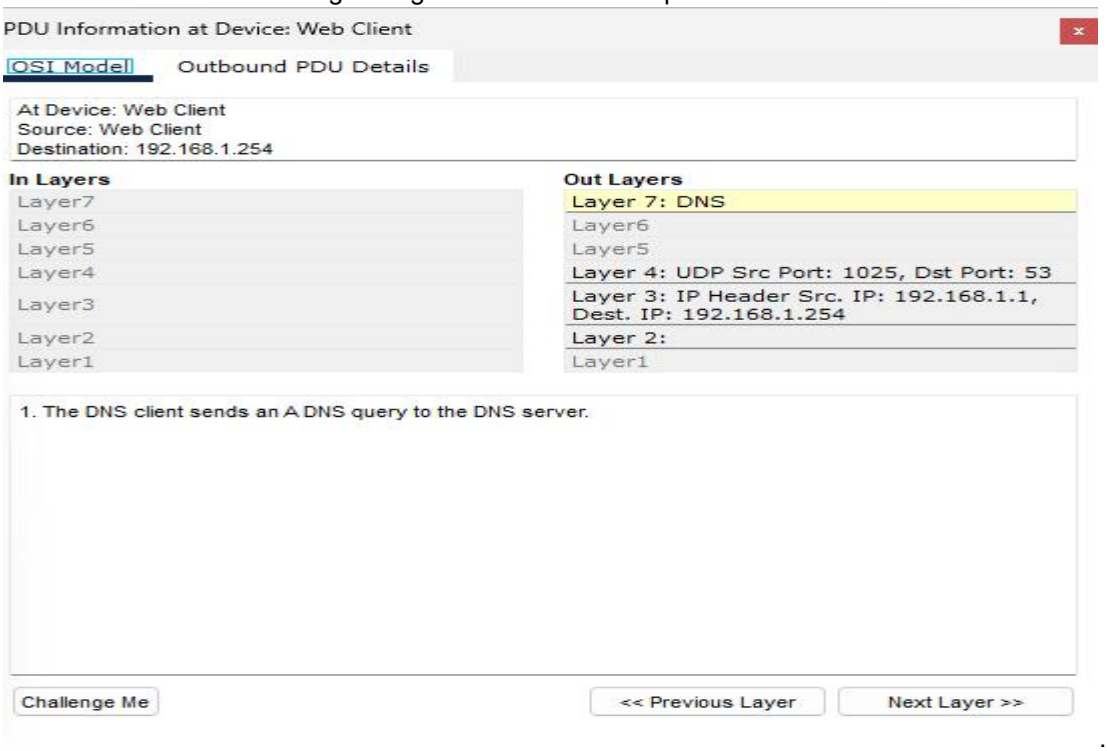
b. In the **Event List Filters** > **Visible Events** section, click **Show All/None**.

What additional Event Types are displayed? ARP,DNS,TCP and HTTP



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



Click the **Outbound PDU Details** tab.

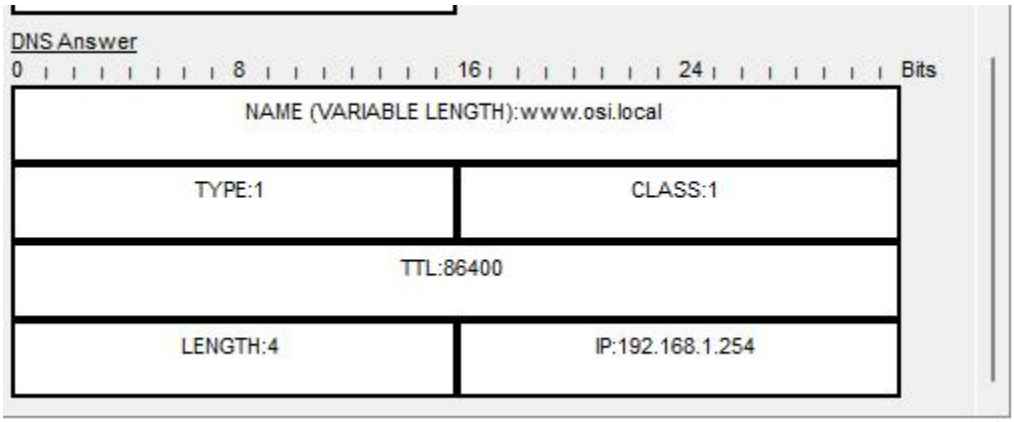
What information is listed in the **NAME** field: in the DNS QUERY section?

www.osi.local

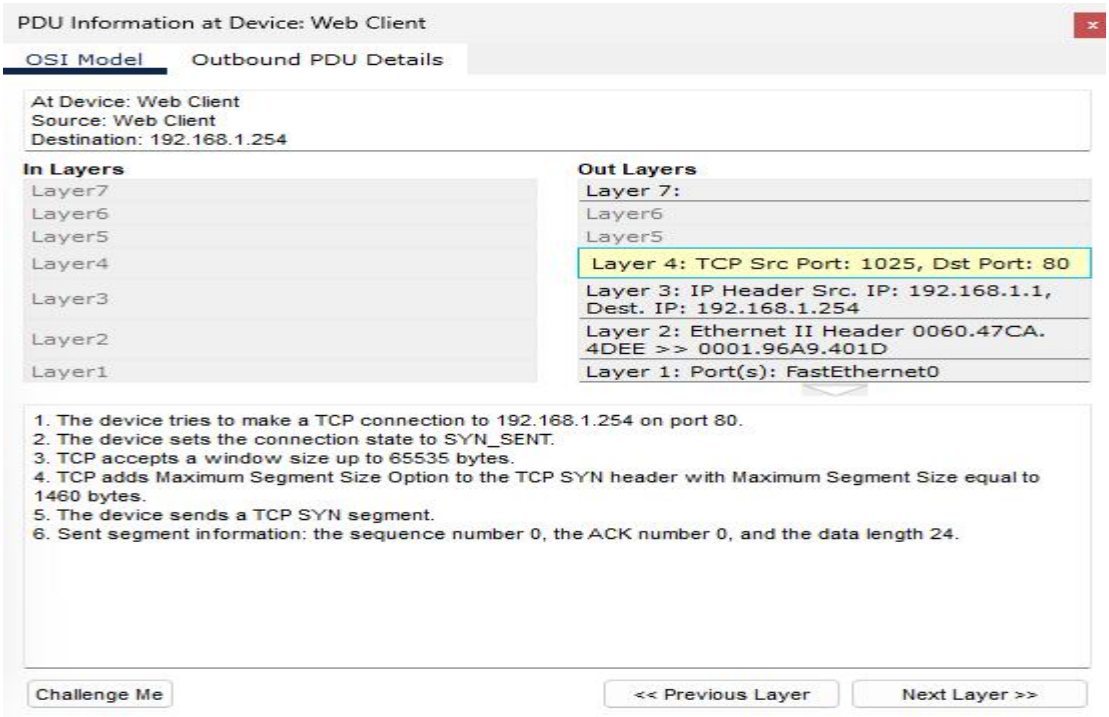
Click the last DNS **Info** colored square box in the event list.

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 ADDRESS OF THE WEB SERVER



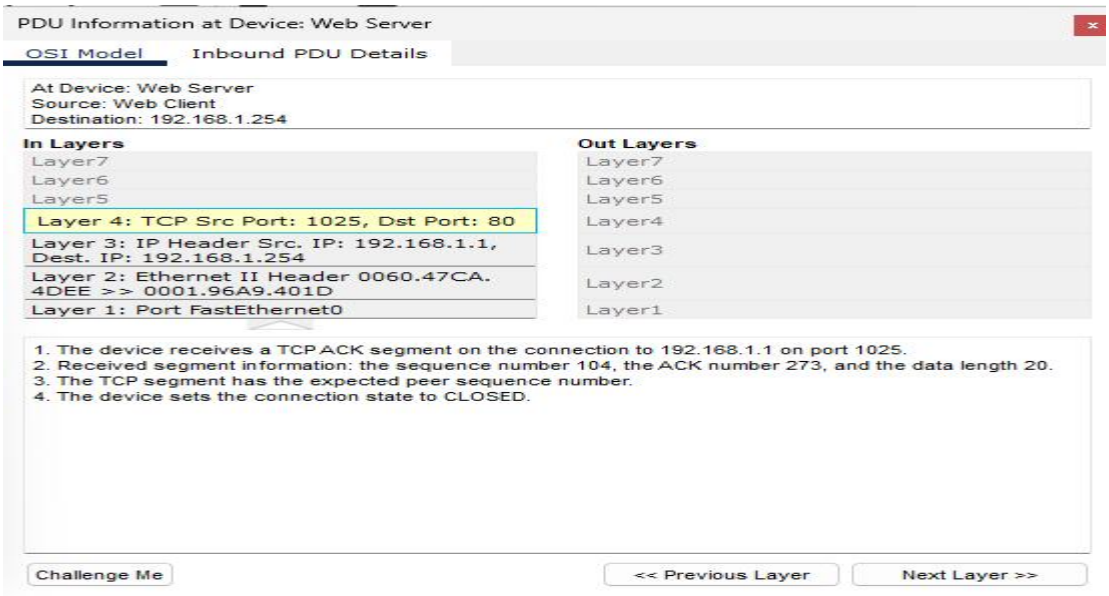
Find the first **HTTP** event in the list and click the colored square box of the **TCP** event immediately following this event. Highlight **Layer 4** in the **OSI Model** tab.



In the numbered list directly below the **In Layers** and **Out Layers**, what is the information displayed under items 4 and 5? 4. The TCPconnection is successful
5.The device sets the connection state to Established

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

What is the purpose of this event, based on the information provided in the last item in the list



CLOSING the connection

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.)

  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?
  The first HTTP PDU being requested by the Web Client shows port 80 under the layer 4 DST port.

  What port is the Web Server listening on for a DNS request?
  The first DNS PDU being requested by the Web Client shows a layer 4 destination of port 53.

Conclusion

I was able to examine the HTTP web traffic using the packet tracer and analyze the traffic well and also the elements of the TCP/IP protocol suite with the relationship to the OSI model.