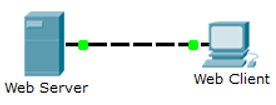
Notes:

1. This document contains the instruction and questions that you need to answer for the Packet Tracer activity named wk3-computer-prac-PKA-c-Investigate-TCPIP-OSI-Models.pka.
2. Make sure you have downloaded and opened the Packet Tracer activity file named wk3-computer-prac-PKA-c-Investigate-TCPIP-OSI-Models.pka.
3. Follow the instruction in this Word document to complete the Packet Tracer activity
4. Type in your answer to EACH question (highlighted) included in this document, immediately after the question in the space provided
5. Save this Word document and submit it as part of your Week 3 Computer Practical submission in Week 3 class (unless permission has been given by your tutor to submit it by the end of day when your week Computer practical class is on)

Packet Tracer - Investigating the TCP/IP and OSI Models in Action

1. Topology



1. Objectives

Part 1: Examine HTTP Web Traffic

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

1. 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 (known as a PDU, or Protocol Data Unit) is assigned a specific name 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.

1. Examine HTTP Web Traffic

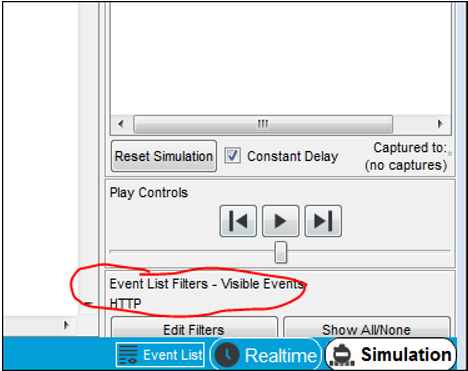
In Part 1 of this activity, you will use Packet Tracer Simulation mode to generate web traffic and examine HTTP.

* 1. Switch from Realtime to Simulation mode.

In the lower right corner of the Packet Tracer interface are tabs to toggle between **Realtime** and **Simulation** mode. Packet Tracer 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.

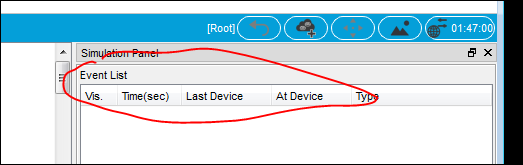
1. Click the **Simulation** mode icon to switch from **Realtime** mode to **Simulation** mode.

**HTTP** should be the only visible event in the **Event List Filters**, as illustrated in the graphic below. If HTTP is NOT the only filter shown, close the pka file and re-open it.



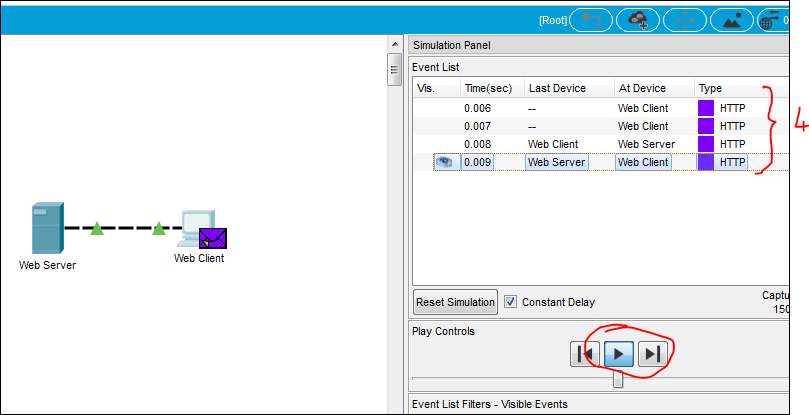
* 1. Generate web (HTTP) traffic.

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. The **Type** column is used to inspect the contents of a particular event.



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

1. Click on the icon **Web Client** in the left pane (refer to the graphic on next page)
2. On the pop-up window, click the **Desktop** tab and click the **Web Browser** icon to open it.
3. In the URL field of the browser, enter **www.osi.local** and click **Go**. Minimise this window, but do not close it.
4. In the simulation panel, click the play button near the bottom of the panel **at least four** times until you see four HTTP events in the Event List, as illustrated in the graphic below. (**Note** that because time in Simulation mode is event-driven, you must use the play button to display network events.)



Look at the Web Client web browser page that you minimised earlier. Did anything change?

Your answer: I am now able to access successfully to the home page for Web Server

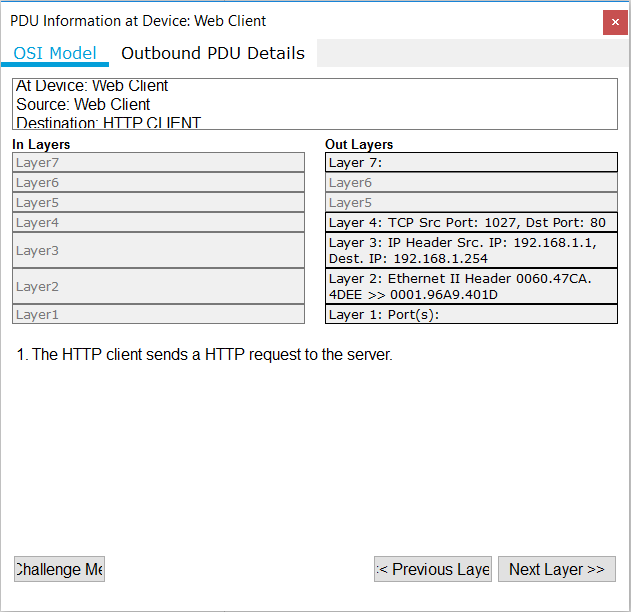
* 1. Explore the contents of the HTTP request and response

1. 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, similar to the one in the graphic below.

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.

Ensure that the OSI Model tab is selected. Under the Out Layers column (the right column), ensure that the Layer 7 row is highlighted/clicked.

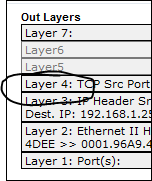


* + - 1. What information is listed in the numbered steps directly below the **In Layers** and **Out Layers** boxes, i.e. the yellow area in the graphic above?

Your answer: sent segment information named as the sequence number, the ACK number and the data length

* + - 1. Click the **Next Layer** button (circled in the graphic above). Layer 4 in the Out Layers box should now be highlighted (as indicated in the graphic below. Note that the highlighting may not be clearly seen). What is the **Dst Port** value listed in the Layer 4 information?

Your answer: 80



* + - 1. Click Next Layer. Layer 3 should be highlighted. What is the **Dest. IP** value?

Your answer: 192.168.1.254

* + - 1. Click Next Layer. What information is displayed at this layer, Layer 2?

Your answer:

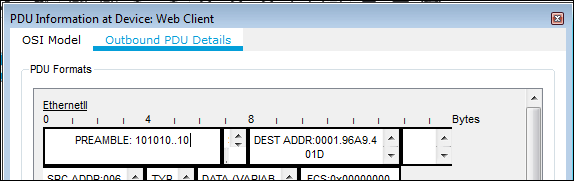
- The next-hop IP address is a unicast. The ARP process looks it up in the ARP table

* The next-hop 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

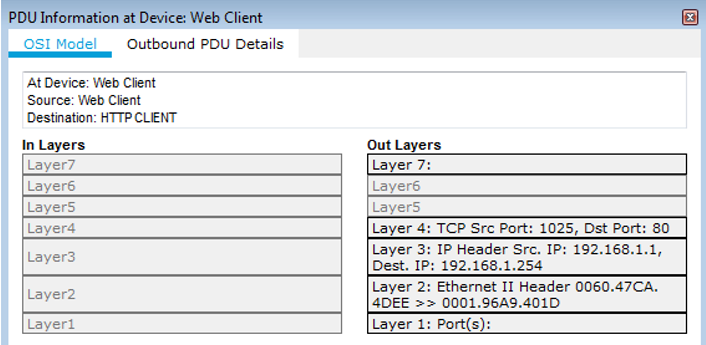
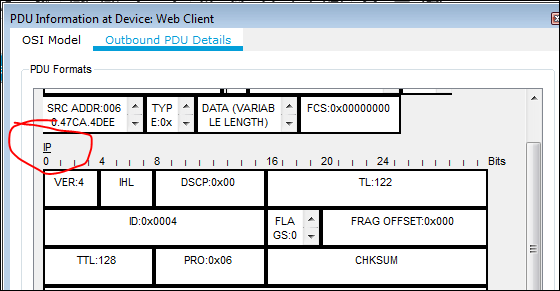
1. Click the Outbound PDU Details tab on the **PDU Information at Device: Web Client** window.

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

**Note**: Refer to the graphic below, the information listed under the **Ethernet II** section (the top section) 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 detailsappear on the **OSI Model** tab under Layer 2, but are not identified as such.



1. Compare the information provided under the OSI Model tab (illustrated in left graphic below), with the PDU details under the Outbound PDU Details tab (illustrated in right graphic below).

* + - 1. What is the common information listed in both the IP section of **PDU Formats** under the Outbound PDU Details tab and under the OSI Model tab?

Your answer: They both have SRC IP and DST IP

* + - 1. With which layer is the common information identified in (i) above associated?

Your answer: Layer 3

* + - 1. What information is listed in both the TCP section of PDU Formats under the Outbound PDU Details tab and the OSI Model tab?

Your answer: SRC PORT and DST PORT

* + - 1. With which layer is the common information identified in (iii) above associated?

Your answer: Layer 4

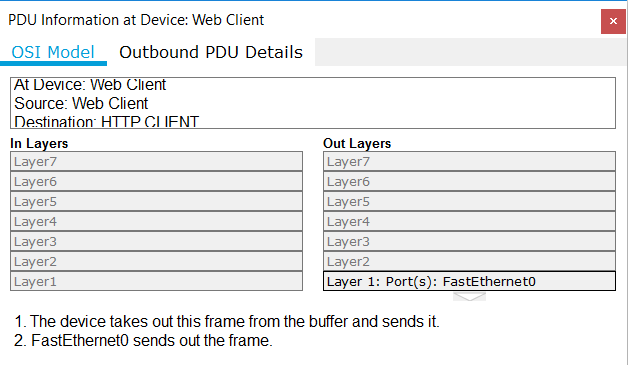
* + - 1. What is the address of the **Host** you find under the HTTP REQUEST section of the PDU Formats? (Need to scroll down to the bottom to see the information)

Your answer: www.osi.local

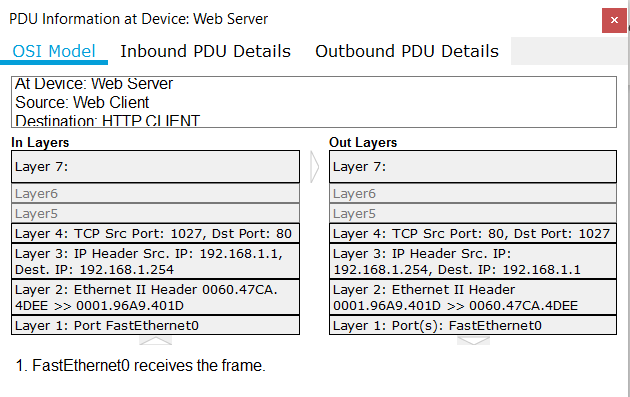
* + - 1. What layer would the information identified in (v) above be associated with under the OSI Model tab?

Your answer: Layer 7

1. 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.



1. Advance to **the next HTTP** Type colored square box (the 3rd one) 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 information is travelling. Scroll/click 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.



Compare the itemised information displayed in the **In Layers** column (left column) with that of the **Out Layers** column (right column), what are the major differences?

Your answer: The In Layers column received information and data through the frame in Layer 1, respectively decapsulated PDU, packet, received and reassemble data segments via layer 2, 3, 4 then passed to the upper layer (Layer 7) that received HTTP request. While, in contrast, the Out Layer reversed the whole process and encapsulated the data then eventually, sent out the frame.

1. Click the **Outbound PDU Details** tab. Scroll down to the **HTTP** section. It no longer says HTTP Request.

What information is written in the HTTP section now ?

Your answer:

HTTP Data:

Connection: close  
Content-Length: 170  
Content-Type: text/html  
Server: PT-Server/5.2

1. Click the last colored square box under the Type column. How many tabs are displayed with this event and why?

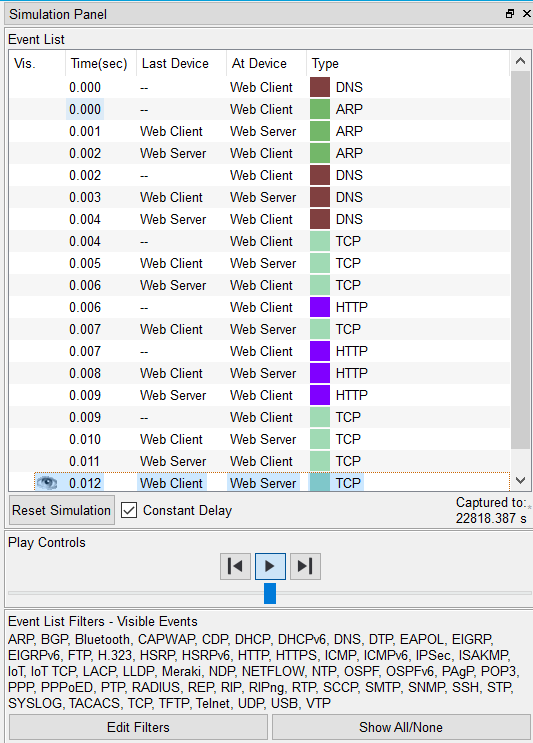
Your answer: 2 tabs. Because this is the final step of the connecting process between web client and web browser which are only information about the decapsulation data and received data from the server.

1. 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 of the TCP/IP suite.

* 1. View Additional Events

1. Close any open PDU Information windows, but no other windows or panels.
2. In the Event List Filters > Visible Events section at the bottom of the Simulation panel, click **Show All (**may need to click **Show All** multiple times until you see multiple events in the Event list, as indicated in the graphic below**)**.



What additional Event Types are displayed in the Type column? (List all those Types that show up as coloured squares except HTTP)

Your answer: DNS, ARP, TCP

These extra entries play various roles within the TCP/IP suite, and two these entries are related to addresses: (**please read the following dot points carefully to gain more from this lab**)

* **ARP (Address Resolution Protocol),** which is used by a device to query other devices on its local network to find out the MAC address of a known IP address. This happens when a device needs to communicate with another device when it only has the IP address of the other device.
* **DNS (Domain Name Service)** is responsible for “converting” a name (for example, **www.osi.local**) to an IP address. This happens when host A only knows host B’s name, but host A needs Host B’s IP address to reach host B. In this case, Host A will contact its DNS server using DNS messages to find out Host B’s IP address by telling the DNS server Host B’s name.

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.

1. **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/clicked, 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. Scroll down to see the DNS section.

What is the **NAME** (to be “converted” by the DNS query) that is shown in the DNS Query section?

Your answer: www.osi.local

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

Which device’s information is shown in the PDU Information window popped up? (You can find the device information either by checking the title of the pop-up window or look at the first line displayed under the OSI Model tab.)

Your answer: Web client

1. Click the **Inbound PDU Details** tab.
2. What is the difference between the DNS Query section and the DNS Answer section?

Your answer: The DNS Answer section has an IP address but the query not. Moreover, the length in this section is 4, instead of 0 in DNS Query section

1. What value is listed next to **IP:** in the DNS ANSWER section of the Inbound PDU Details?

Your answer: 192.168.1.254

1. Find the first HTTP event in the list and click the colored square box of the **TCP** event immediately following this HTTP event.
2. Highlight/click **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?

Your answer:

- The TCP connection is successful.

- 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.

1. Click **the last TCP event**. Highlight/click 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 (should be item 4)?

Your answer: To announce that this is the end of the process and the connection state is set to CLOSED by the device