Lab: Part 2, Investigating the TCP-IP and OSI Models

Name: Natalia Palej

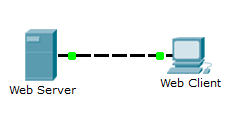
Student ID: A00279259

Course: Software Design with Artificial Intelligence for Cloud Computing

Year: 4

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. Aim / 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 student 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.

The student is required to complete the various blank sections below then upload the completed word document back to Moodle. Please include screenshots from Part 1- step 3 onwards and place then at the end of this document. When completed upload the final document back to Moodle.

1. ~~Examine HTTP Web Traffic~~

~~In Part 1 of this activity, you will use Packet Tracer (PT) 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. 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.~~

* + 1. ~~Click the~~ **~~Simulation~~** ~~mode icon to switch from~~ **~~Realtime~~** ~~mode to~~ **~~Simulation~~** ~~mode.~~
    2. ~~Select~~ **~~HTTP~~** ~~from the~~ **~~Event List Filters~~**~~.~~
       1. ~~HTTP may already be the only visible event. Click~~ **~~Edit Filters~~** ~~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~~**~~. Click anywhere outside of the~~ **~~Edit Filters~~** ~~box to hide it. The Visible Events should now only display HTTP.~~
  1. Generate web (HTTP) traffic.

~~Currently the Simulation Panel is empty. There are six 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~~ **~~Info~~** ~~column is used to inspect the contents of a particular event.~~

**~~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.~~

* + 1. ~~Click~~ **~~Web Client~~** ~~in the far left pane.~~
    2. ~~Click the~~ **~~Desktop~~** ~~tab and click the~~ **~~Web Browser~~** ~~icon to open it.~~
    3. ~~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.~~

* + 1. ~~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?

Page has loaded which displays “Web Server \n You have successfully accessed the home page for Web Server.”

screenshots

* 1. ~~Explore the contents of the HTTP packet.~~
     1. ~~Click the first colored square box under the~~ **~~Event List~~** ~~>~~ **~~Info~~** ~~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.~~

* + 1. ~~Ensure that the~~ **~~OSI Model~~** ~~tab is selected. Under the~~ **~~Out Layers~~** ~~column, ensure that the~~ **~~Layer 7~~** ~~box is highlighted.~~

What is the text displayed next to the **Layer 7** label? Layer 7: HTTP

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

“1. The HTTP client sends a HTTP request to the server.”

* + 1. Click **Next Layer**. Layer 4 should be highlighted. What is the **Dst Port** value? 80
    2. Click **Next Layer**. Layer 3 should be highlighted. What is the **Dest. IP** value? 192.168.1.254
    3. Click **Next Layer**. What information is displayed at this layer?

Layer 2: Ethernet II Header 0060.47CA.4DEE >> 0001.96A9.401D

This layer (Data Link) shows Ethernet II Header, source and destination MAC address.

* + 1. ~~Click the~~ **~~Outbound PDU Details~~** ~~tab.~~

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

**~~Note~~**~~: The information listed under the~~ **~~Ethernet II~~** ~~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 Details~~** ~~appear on the~~ **~~OSI Model~~** ~~tab under Layer 2, but are not identified as such.~~

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 information listed under the IP section shows details about the source and destination IP addresses, and its data length. In comparison to OSI Model tab, we can see more details, such as checksum, data variable length, protocol number. This information is associated with OSI Model Layer 3, which is 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?

The TCP section under PDU Details provides source and destination port numbers, just like the OSI Model tab, along with additional information such as the sequence, ack number or data length. This is Layer 4 Transport Layer in the OSI Model.

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 under HTTP section contains information such as the accepted language (set as “en-us”) and it also specifies that it accepts any media type “\*/\*” which tells us that the client is not restricting the types of responses that it can handle. In other words it accepts content like HTML, images etc. This is Layer 7 Application Layer in the OSI Model.

* + 1. ~~Click the next colored square box under the~~ **~~Event List~~** ~~>~~ **~~Info~~** ~~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.~~
    2. ~~Advance to the next HTTP~~ **~~Info~~** ~~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 information 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 major difference between In and Out Layers column is the source and destination address for IPs, MAC address and Ports at each layer.

In Layers: the MAC address source is 0060.47CA.4DEE, the destination MAC address is 0001.96A9.401D. The source IP is 192.168.1.1 and destination IP is 192.168.1.254. The source port is 1028, destination is 80.

Out Layers are reversed to In Layers. This means that when the request is sent, the server becomes the sender and the client becomes the receiver.

* + 1. ~~Click the~~ **~~Outbound PDU Details~~** ~~tab. Scroll down to the~~ **~~HTTP~~** ~~section.~~

What is the first line in the HTTP message that displays?

HTTP Data: Connection: close

Click the last colored square box under the **Info** column. How many tabs are displayed with this event and why? There are 5 tabs active in the last event in the Event List. These tabs are moving up through the Layer 1 (Physical) -> 2 -> 3 -> 4 -> 7 (Application). Each layer is handling different part of data, and each active layer is processing incoming packet. All rows in Out Layers column is grayed out as the there is no outbound traffic at this point.

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.~~
     2. ~~In the Event List Filters > Visible Events section, click~~ **~~Show All~~**~~.~~

What additional Event Types are displayed?

DNS (converts URL to an IP address), ARP (resolves MAC address), TCP (manages communication) and HTTP which was displayed in previous view

~~These extra entries play various roles within the TCP/IP suite. If the Address Resolution Protocol (ARP) is listed, it searches MAC addresses. 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.~~

* + 1. ~~Click the first DNS event in the~~ **~~Info~~** ~~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.~~
    2. ~~Click the~~ **~~Outbound PDU Details~~** ~~tab.~~ What information is listed in the **NAME**: in the DNS QUERY section?

[www.osi.local](http://www.osi.local), the URL that we have entered in the Web Browser

* + 1. ~~Click the last DNS~~ **~~Info~~** ~~colored square box in the event list.~~ Which device is displayed?

Web Client

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

IP: 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 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 TCP connection is successful

5. The device sets the connection state to ESTAVLISHED

~~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 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)?

The purpose of the last TCP event is to show that the device received TCP Reset segment. It tells us that the connection to 192.168.1.1 on port 1027 has been closed. This results in the connection state to be “CLOSED”, which means that no further communication can happen over this connection.

1. Challenge

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?

Web Server is listening on port number 80 for web request

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

Web Server is listening on default port number 53 for DNS request

1. Suggested Scoring Rubric

|  |  |  |  |
| --- | --- | --- | --- |
| Activity Section | Question Location | Possible Points | Earned Points |
| Part 1: Examine HTTP Web Traffic | Step 2d | 5 |  |
| Step 3b-1 | 5 |  |
| Step 3b-2 | 5 |  |
| Step 3c | 5 |  |
| Step 3d | 5 |  |
| Step 3e | 5 |  |
| Step 3f-1 | 5 |  |
| Step 3f-2 | 5 |  |
| Step 3f-3 | 5 |  |
| Step 3h | 5 |  |
| Step 3i | 5 |  |
| Step 3j | 5 |  |
| **Part 1 Total** | | **60** |  |
| Part 2: Display Elements of the TCP/IP Protocol Suite | Step 1b | 5 |  |
| Step 1d | 5 |  |
| Step 1e-1 | 5 |  |
| Step 1e-2 | 5 |  |
| Step 1f | 5 |  |
| Step 1g | 5 |  |
| **Part 2 Total** | | **30** |  |
| Challenge | 1 | 5 |  |
| 2 | 5 |  |
| **Part 3 Total** | | **10** |  |
| **Total Score** | | **100** |  |

Screenshots

**Part 1 Step 3**

**First event from the Event List PDU Information at Device: Web Client**

The below screenshots show the PDU Information at the Web Client device for the first event in the Event List. The OSI Model tab shows that there are 5 out of 7 active layers. Each layer explains the data flow through that specific layer. The Outbound PDU Details gives extra information about the IP, TCP, HTTP – it shows how the data is encapsulated and prepared for transmission.

**OSI Model – three layers available**

A screenshot of a computer

Description automatically generated

**Outbound PDU Details – IP/TCP/HTTP additional information**

A screenshot of a computer

Description automatically generated

**Second event from the Event List PDU Information at Device: Web Client**

The below screenshot displays information about Layer 1. It means that the device is in a state where it is preparing to send a frame, but no additional information about the data is currently available.

**A screenshot of a computer

Description automatically generated**

**Third event from the Event List PDU Information at Device: Web Client**

The below screenshot shows three different tabs: OSI Model, Inbound PDU Details, and Outbound PDU Details. The active layers are:

* Layer 7 Application
* Layer 4 Transport
* Layer 4 Network
* Layer 2 Data Link
* Layer 1 Physical

When data is traveling through these layers, it means it is actively being processed and transmitted. This indicates that a full cycle of data transmission from the server to the client was achieved.A screenshot of a computer

Description automatically generated

**Part 2 Step 1**

First DNS event (Outbound PDU) in Event List shows the initial DNS query sent from the Web Client to the DNS sever on IP address 192.168.1.254. We can read from the column that the source port is 1025, and the destination port is 53 (for DNS request). The request is encapsulated at OSI Layers displayed below. On the other hand, the last DNS event from Event List (Inbound PDU) shows the response from the DNS server to the Web Client. The response is sent back to the client on port 1027. The query travels through the same OSI Layers which confirms that the client received DNS answer. The only difference is that the First DNS event Layer 1 is grayed out, which means its not active at this point, instead the DNS query is being prepared at this point. The Layer 1 (Physical) becomes active in last DNS event as the device received the DNS response at this point.

**First DNS Info**

A screenshot of a computer

Description automatically generated

**Last DNS Info**

A screenshot of a computer

Description automatically generated

**First Outbound PDU Details for DNS**

A screenshot of a computer

Description automatically generated

**Last Inbound PDU Details for** **DNS**

A screenshot of a computer

Description automatically generated

**First TCP event type right after HTTP type**

In the first TCP event, right after HTTP type. The segment (packet) is travelling upwards through the layers 4 (TCP), 3 (IP), 2 (Ethernet II), 1 (Port FastEthernet0). It shows that the device received TCP packet and is processing it. The segment is received on Physical layer via Ethernet, then in Data Link the header is processed which makes sure it reaches the right device. Network layer (3) checks Header, Source/Destination IP. Then in Layer 4 (Transport) the TCP displays source and destination port numbers. This OSI Model flow confirms that the device successfully received the TCP segment for processing.

A screenshot of a computer

Description automatically generated

**Challenge**

**Web request port number**

A screenshot of a computer

Description automatically generated

**DNS request port number**

A screenshot of a computer

Description automatically generated