**Lab work 2. Issayev Zh. 20B030318**

[**3.5.5 - Packet Tracer - Investigate the TCP/IP and OSI Models in Action**](https://contenthub.netacad.com/itn#3.5.5)

**Part 1: Examine HTTP Web Traffic**

### Step 2: Generate web (HTTP) traffic.

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

Answer: You have successfully accessed the home page for Web Server.

2. 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.”

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

Answer: 80

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

Answer: 192.168.1.254

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

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

6. 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: SRC IP and DST IP at Layer 3

7. 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: SRC PORT and DEST PORT at Layer 4

8. 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: www.osi.local, Layer 7

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

Answer: The Src and Dst Ports, Src and Dst IPs and MAC addresses have been swapped.

10. How many tabs are displayed with this event? Explain.

Answer: Just 2, one for the OSI Model and one for Inbound PDU Details because this is the receiving device.

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

### Step 1: View Additional Events

1. What additional Event Types are displayed?

Answer: Depending on whether any communications has occurred prior to starting the original simulation, there should now be entries for ARP, DNS, TCP and HTTP. It is possible that the ARP entries may not show, depending on what a student may have done prior to going to simulation mode. If the activity is started from scratch all of those will be listed.

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

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

3. At which device was the PDU captured?

Answer: The Web Client

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

Answer: 192.168.1.254 – the address of the Web Server

5. 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.

6. 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.

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

Answer: CLOSING the connection.

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

9.   
What port is the Web Server listening on for a DNS request?

Answer: The first DNS PDU being requested by the Web Client shows a layer 4 destination of port 53.

[**3.7.10 - Lab - Use Wireshark to View Network Traffic**](https://contenthub.netacad.com/itn#3.7.10)

### Part 1: Capture and Analyze Local ICMP Data in Wireshark

#### Step 1: Retrieve your PC interface addresses.

1. Does the source MAC address match your PC interface ?

Answer: Yes

1. Does the destination MAC address in Wireshark match your team member MAC address?

Answer: Yes

1. How is the MAC address of the pinged PC obtained by your PC?

Answer: The MAC address is obtained through an ARP request.

### Step 2:  Examining and analyzing the data from the remote hosts.

1. What is significant about this information?

Answer: The MAC addresses for all three locations are the same.

1. How does this information differ from the local ping information you received in Part 1?

Answer: A ping to a local host returns the MAC address of the PC NIC. A ping to a remote host returns the MAC address of the default gateway LAN interface.

Reflection Question

Why does Wireshark show the actual MAC address of the local hosts, but not the actual MAC address for the remote hosts?

Answer: MAC addresses for remote hosts are not known on the local network, so the MAC address of the default-gateway is used. After the packet reaches the default-gateway router, the Layer 2 information is stripped from the packet and a new Layer 2 header is attached with the destination MAC address of the next hop router.