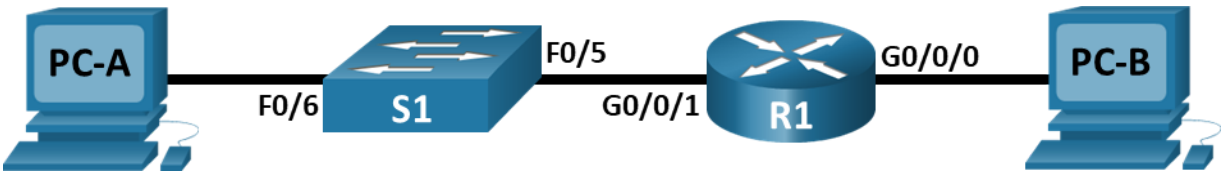
# Lab-2- Investigate the TCP-IP and OSI Models in Action

## Part 1: Build a Switch and Router Network

### Topology




### Addressing Table

| Device | Interface | IP Address / Prefix | Default Gateway |
|---|---|---|---|
| R1 | G0/0/0 | 192.168.0.1 /24 | N/A |
| | | 2001:db8:acad::1/64 | |
| | | fe80::1 | |
| | G0/0/1 | 192.168.1.1 /24 | N/A |
| | | 2001:db8:acad:1::1/64 | |
| | | fe80::1 | |
| S1 | VLAN 1 | 192.168.1.2 /24 | 192.168.1.1 |
| PC-A | NIC | 192.168.1.3 /24 | 192.168.1.1 |
| | | 2001:db8:acad:1::3/64 | fe80::1 |
| PC-B | NIC | 192.168.0.3 /24 | 192.168.0.1 |
| | | 2001:db8:acad::3/64 | fe80::1 |

**Step 1: Assign static IP information to the PC interfaces.**

a. On PC-A, configure the IP address, subnet mask, and default gateway settings.

b. On PC-B, configure the IP address, subnet mask, and default gateway settings.

**Step 2: Configure the router.**

a. Console into the router and enable privileged EXEC mode.

b. Enter configuration mode.

c. Assign the device name to the router.

d. Assign **class** as the privileged EXEC encrypted password.

e. Assign **aait** as the console password and enable login.

f. Assign **aait** as the vty password and enable login.

g. Encrypt the plaintext passwords.

h. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

i. Configure and activate both interfaces on the router.

j. Configure an interface description for each interface indicating which device is connected to it.

k. To enable IPv6 routing, enter the **ipv6 unicast-routing** command.

l. Save the running configuration to the startup configuration file.

### Step 1: Configure the switch.

In this step, you will configure the hostname, the VLAN 1 interface, and its default gateway.

a. Console into the switch and enable privileged EXEC mode.

b. Enter configuration mode.

c. Assign a device name to the switch.

d. Configure and activate the VLAN interface on the switch S1.

e. Configure the default gateway for the switch S1.

f. Save the running configuration to the startup configuration file.

# Part 2: Investigate the TCP/IP and OSI Models in Action

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

### Step 0: Add and configure HTTP Web Server and DNS Server

a. Add a server device to either of the lan and configure the server with IPV4 address.
b. turn on HTTP server
c. create a DNS record to resolve **www.osi.local** to the server's ip address.

### Step 1: Switch from Realtime to Simulation mode.

In the lower right corner of the Packet Tracer interface are buttons that 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.

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

b. Select **HTTP** from the **Event List Filters**.

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 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** 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.

### Step 2: 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.

a. Click **on PCA**.

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**.

Because time in Simulation mode is event-driven, you must use the **Capture/Forward** button to display network events. The capture forward button is located at the left hand side of the blue band that is below the topology window. Of the three buttons there, it is the one on the right.

d. 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? Yes. The web browser was displayed.

### Step 3: Explore the contents of the HTTP packet.

a. 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. 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.

b. 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 an HTTP request.

**Question 1:** What is the **Dst Port** value for **Layer 4** under the **Out Layers** column? 80

**Question 2:** What is the **Dest. IP** value for **Layer 3** under the **Out Layers** column? 192.168.1.254

**Question 3:** What information is displayed at Layer 2 under the **Out Layers** column? Ethernet 2 header and the Mac addresses.

c. Click the **Outbound PDU Details** tab.

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

**Note**: The information listed under the **Ethernet II** section of the Outbound PDU Details tab 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.Questions:

**Question 4:** 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 source IP and the destination IP are associated with layer 2.

**Question 5:** 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 source port and destination port, are at layer 4.

**Question 6:** 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.osi.local

d. 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.

e. 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.

**Question 6:** Comparing the information displayed in the **In Layers** column with that of the **Out Layers** column, what are the major differences? The source and destination ports, IP addresses, and Mac addresses are reversed.

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

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

How many tabs are displayed with this event? Explain. 2 tabs are displayed. 1 is for the OSI Model and the other is for the Inbound PDU details.

## Part 2: 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 TCP/IP 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? DNS, ARP, and TCP.

These extra entries play various roles within the TCP/IP suite. Address Resolution Protocol (ARP) requests MAC addresses for destination hosts. 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.

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.

d. Click the **Outbound PDU Details** tab.

**Question 7:** What information is listed in the **NAME** field: in the DNS QUERY section? www.osi.local

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

**Question 8:** At which device was the PDU captured? at the web client.

**Question 9:** What is the value listed next to **ADDRESS**: in the DNS ANSWER section of the **Inbound PDU Details**? 192.168.1.254

f. 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? Under item 4, "The TCP connection is successful." is displayed.

Under item 5, "The device sets the connection state to established." is displayed.

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.

g. 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)? It is a connection closure.

## 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? 80

**Question 10:** What port is the **Web Server** listening on for a DNS request? 53