

LAB 2

Using Packet Tracer to simulate & analyze UDP & TCP protocol

***** Before you start your lab, please go through Introduction to Packet Tracer (PT Introduction To Packet Tracer.pka) with your lecturer**

2A: TCP Session Establishment and Termination

Introduction:

TCP is a connection-oriented protocol. Before information, such as a web page, can be exchanged, the peers must establish a connection. A connection is established by a three-way handshake where the initial sequence numbers for both peers are sent and acknowledged. When the exchange is complete, the peers exchange TCP segments to terminate the session properly. The previous activity focused on the actual exchange of TCP segments. This activity will focus on connection establishment before the exchange and session termination following the exchange.

***** Open file PT2A Analyzing the Application and Transport Layers.pka**

Task 1: Setup and run the simulation

Step 1. Enter simulation mode

To verify the connection, click on the PC in the logical workplace. Open the **Web Browser** on the **Desktop**. Type **192.168.1.2** into the URL box and click the **Go** button. The web page should appear. Click the **Simulation** tab to enter simulation mode.

Step 2. Set Event List Filters

We want to capture only TCP events. In the **Event List Filters** section, click the **Edit Filters** button. Select only TCP events. TCP events include TCP based application protocols like HTTP and Telnet.

Step 3. Request a web page from the PC

Restore the web browser window. In the **Web Browser**, click the **Go** button to request that the web page be resent. Minimize the simulated browser window.

Step 4. Run the simulation

Click the **Auto Capture / Play** button. The exchange between the PC and the server is animated and the events are added to the **Event List**. These events represent the establishment of the TCP session, the PC's request for web page, the server sending the web page in two segments, the PC acknowledging the web page, and the termination of the TCP session. A dialog box appears indicating there are no more events. Click **OK** to close it.

Task 2: Examine the results

Step 1. Access specific PDUs

In the **Simulation Panel Event List** section, the last column contains a colored box that provides access to detailed information about an event. Click the colored box in the last column for the first event. The **PDU Information** window opens.

Step 2. Examine the contents of the PDU Information Window

In this activity, we will focus only on event information only at Layer 4. The first tab in the **PDU Information** window contains information about the inbound and outbound PDU as it relates to the OSI model. Click the **Layer 4:** boxes for both the inbound and outbound layers and read the content of the box and description in the box below the layers. Pay attention to the type of TCP segment. Click the **Outbound PDU Details** tab. In the TCP segment, note the initial sequence number.

Examine the PDU information for the first four TCP events in the same fashion. These events show the three-way handshake that establishes the session. Note the type of TCP segment and the change in the sequence number.

Examine the PDU information for the TCP events that follow the main HTTP exchange in the same fashion. These events show the session termination. Note the type of TCP segment and the change in the sequence number.

Note that if you use the **Reset Simulation** button in the **Event List** window, you will need to return to the web browser window and press **Go** to make a new request.

2B: Analyzing the Application and Transport Layers

Topology Diagram: Partial topology given; must be completed.

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1-ISP	Fa0/0	192.168.254.253	255.255.255.0	N/A
	S0/0/0	10.10.10.6	255.255.255.252	
R2-Central	Fa0/0	172.16.255.254	255.255.0.0	N/A
	S0/0/0	10.10.10.5	255.255.255.252	
S1-Central	VLAN 1	172.16.254.1	255.255.0.0	172.16.255.254
PC 1A	NIC	172.16.1.1	255.255.0.0	172.16.255.254
PC 1B	NIC	172.16.1.2	255.255.0.0	172.16.255.254
Eagle Server	NIC	192.168.254.254	255.255.255.0	192.168.254.253

Learning Objectives:

- Configure Hosts and Services
- Connect and configure hosts and services on the model of the lab network
- Explore How DNS, UDP, HTTP, and TCP Work Together
- Use simulation mode to visualize the operation of DNS, UDP, HTTP, and TCP on the model of the lab network

Background:

Throughout the course, you will be using a standard lab setup created from actual PCs, servers, routers, and switches to learn networking concepts. At the end of each chapter, you will build increasingly larger parts of this topology in Packet Tracer, and analyze increasingly more complex protocol interactions.

***** Open file PT2B Analyzing the Application and Transport Layers.pka**

Task 1: Repair and Test The Topology

Configure the server with the following settings:

- IP Address 192.168.254.254, Subnet Mask 255.255.255.0, Default Gateway 192.168.254.253.
- Enable DNS in the server. Add "eagle-server.example.com" (without the quotes) in the Name box and server's IP address in the Address box.
- Enable HTTP.
- Connect the Eagle Server to the Fa0/0 port on the R1-ISP router.

PC 1A has lost its IP address information. Configure it with the following settings:

- IP Address 172.16.1.1, Subnet Mask 255.255.0.0, Default Gateway 172.16.255.254, and DNS Server 192.168.254.254.
- Connect PC 1A to the Fa0/1 port of the S1-Central switch.

Verify your work using feedback from the **Check Results** button and the **Assessment Items** tab. Test connectivity, in realtime, by using ADD SIMPLE PDU to test connectivity between PC 1A and the Eagle Server.

Note that when you add a simple PDU, it appears in the PDU List Window as part of "Scenario 0". The first time you issue this one-shot ping message, it will show as **Failed**--this is because of the ARP process which will be explained later. Double clicking the "Fire" button in the PDU List Window, will send this single test ping a second time

Task 2: Explore How DNS, UDP, HTTP, and TCP Work Together

- Switch from Realtime to Simulation Mode.
- Make sure Event Filter is set to display DNS, UDP, HTTP, TCP.
- Open a web browser from the desktop of 1A. Type in the URL eagle-server.example.com, press Enter.
- Use the **Capture / Forward** button in the **Event List** to capture the interaction of DNS, UDP, HTTP and TCP.

You can examine the packet in two ways: by clicking on the packet envelope as it is displayed in the animation, or by clicking on the **Info** column for that packet instance as it is listed in the **Event List**. Play this animation and examine the Packet contents (**PDU Information** Window, **Inbound PDU Details**, **Outbound PDU Details**) for each event in the event list, especially when the packets are at PC 1A or at the Eagle Server.

If you receive a "Buffer Full" message, click the **View Previous Events** button. While the processing of the packets at the switch and the routers may not make sense to you yet, you should be able to see how DNS, UDP, HTTP, and TCP work together by tracing the packets and using the PDU Information window to look "inside" them.

Extra Lookout:

- ✓ Look at the port numbers. Port 53 represents DNS, the application protocol that associates domain names with IP addresses. Port 80 represents HTTP that supports web pages. The other port is generated by the client PC from the range of port numbers greater than 1023.
- ✓ Click the **Outbound PDU Details** tab. In TCP segment, note the initial sequence number. In UDP segments, note the way DNS information is encapsulated in the UDP segment

Reflection:

Can you make a diagram of the sequence of protocol events involved in requesting a web page using a URL? Where might things go wrong?

SUBMISSION:

In group of 2s, capture your activities (ALL the Tasks, Check Results, Assessment Items, Extra Lookout and Reflection) in **Lab 2B** using CamStudio software and submit in e-learning before _____.