Name: Chheang Sovanpanha
Packet Tracer - TCP and UDP Communications

Objectives

Part 1: Generate Network Traffic in Simulation Mode

Part 2: Examine the Functionality of the TCP and UDP Protocols

Background

This simulation activity is intended to provide a foundation for understanding TCP and UDP in detail. Packet Tracer simulation mode provides you the ability to view the state of different PDUs as they travel through the network.

Packet Tracer Simulation mode enables you to view each of the protocols and the associated PDUs. The steps outlined below lead you through the process of requesting network services using various applications that are available on a client PC. You will explore the functionality of the TCP and UDP protocols, multiplexing, and the function of port numbers in determining which local application requested the data or is sending the data. Packet Tracer will not score this activity.

Instructions

Part 1: Generate Network Traffic in Simulation Mode and View Multiplexing

Step 1: Generate traffic to populate Address Resolution Protocol (ARP) tables.

Perform the following task to reduce the amount of network traffic viewed in the simulation.

a. Click **MultiServer** and click the **Desktop** tab > **Command Prompt**.

b. Enter the **ping -n 1 192.168.1.255** command. You are pinging the broadcast address for the client LAN. The command option will send only one ping request rather than the usual four. This will take a few seconds as every device on the network responds to the ping request from MultiServer.

c. Close the **MultiServer** window.

Step 2: Generate web (HTTP) traffic.

a. Switch to Simulation mode.

b. Click **HTTP Client** and open the **Web Browser** from the desktop.

c. In the URL field, enter **192.168.1.254** and click **Go**. Envelopes (PDUs) will appear in the topology window.

d. Minimize, but do not close, the **HTTP Client** configuration window.

Step 3: Generate FTP traffic.

a. Click **FTP Client** and open the **Command Prompt** from the desktop

b. Enter the **ftp 192.168.1.254** command. PDUs will appear in the simulation window.

c. Minimize, but do not close, the **FTP Client** configuration window.

Step 4: Generate DNS traffic.

a. Click DNS Client and open the **Command Prompt**.

b.   Enter the **nslookup multiserver.pt.ptu** command. A PDU will appear in the simulation window.

c.   Minimize, but do not close, the **DNS Client** configuration window.

Step 5: Generate Email traffic.

a.   Click **E-Mail Client** and open the **E Mail** tool from the Desktop.

b.   Click **Compose** and enter the following information:

1)   **To:** user@multiserver.pt.ptu

2)   **Subject:** personalize the subject line

3)   **E-Mail Body:** personalize the Email

c.   Click **Send**.

d.   Minimize, but do not close, the **E-Mail Client** configuration window.

Step 6: Verify that the traffic is generated and ready for simulation.

There should now be PDU entries in the simulation panel for each of the client computers.

Step 7: Examine multiplexing as the traffic crosses the network.

You will now use the **Capture/Forward button** in the Simulation Panel to observe the different protocols travelling on the network.

Note: The **Capture/Forward** button ' **>|** ' is a small arrow pointing to the right with a vertical bar next to it.

a.   Click **Capture/Forward** once. All of the PDUs travel to the switch.

b.   Click **Capture/Forward** six times and watch the PDUs from the different hosts as they travel on the network. Note that only one PDU can cross a wire in each direction at any given time.

What is this called?

It's called multiplex

A variety of PDUs appears in the event list in the Simulation Panel. What is the meaning of the different colors?

The meaning of the different colors is that they represent the different protocols.

Part 2: Examine Functionality of the TCP and UDP Protocols

Step 1: Examine HTTP traffic as the clients communicate with the server.

a.   Click **Reset Simulation**.

b.   Filter the traffic that is currently displayed to only **HTTP** and **TCP** PDUs. To filter the traffic that is currently displayed:

1)   Click **Edit Filters** and toggle the **Show All/None** button.

2)   Select **HTTP** and **TCP**. Click the red "x" in the upper right-hand corner of the Edit Filters box to close it. Visible Events should now display only **HTTP** and **TCP** PDUs.

c.   Open the browser on HTTP Client and enter **192.168.1.254** in the URL field. Click **Go** to connect to the server over HTTP. Minimize the HTTP Client window.

d.   Click **Capture/Forward** until you see a PDU appear for HTTP. Note that the color of the envelope in the topology window matches the color code for the HTTP PDU in the Simulation Panel.

Why did it take so long for the HTTP PDU to appear?

It takes HTTP PDU a long time to appear because TCP must first establish the connection before the HTTP traffic appear.

e. Click the PDU envelope to show the PDU details. Click the **Outbound PDU Details** tab and scroll down to the second to the last section.

What is the section labeled?

TCP

Are these communications considered to be reliable?

Yes, TCP is in use.

Record the **SRC PORT**, **DEST PORT**, **SEQUENCE NUM**, and **ACK NUM** values.

1029, 80, 1, 1

f. Look at the value in the Flags field, which is located next to the Window field. The values to the right of the "b" represent the TCP flags that are set for this stage of the data conversation. Each of the six places corresponds to a flag. The presence of a "1" in any place indicates that the flag is set. More than one flag can be set at a time. The values for the flags are shown below.

Flag Place	6	5	4	3	2	1
Value	URG	ACK	PSH	RST	SYN	FIN

Which TCP flags are set in this PDU?

ACK and PSH

g. Close the PDU and click **Capture/Forward** until a PDU with a checkmark returns to the **HTTP Client**.

h. Click the PDU envelope and select **Inbound PDU Details**.

How are the port and sequence numbers different than before?

The source and destination ports are reversed, and the acknowledgement number is 1. The flags have changed to SYN+ACK.

i. Click the HTTP PDU which **HTTP Client** has prepared to send to **MultiServer**. This is the beginning of the HTTP communication. Click this second PDU envelope and select **Outbound PDU Details**.

What information is now listed in the TCP section? How are the port and sequence numbers different from the previous two PDUs?

The source and destination ports are reversed, both sequence number is 1, the acknowledgement number is 103 (value my vary), and the flags are PSH and ACK.

j. Reset the simulation.

Step 2: Examine FTP traffic as the clients communicate with the server.

a. Open the command prompt on the FTP Client desktop. Initiate an FTP connection by entering **ftp 192.168.1.254**.

b. In the Simulation Panel, change **Edit Filters** to display only **FTP** and **TCP**.

c. Click **Capture/Forward**. Click the second PDU envelope to open it.

Click the **Outbound PDU Details** tab and scroll down to the TCP section.

Are these communications considered to be reliable?

Yes.

d. Record the **SRC PORT**, **DEST PORT**, **SEQUENCE NUM**, and **ACK NUM** values.

What is the value in the flag field?

1025, 21, 0, 0. SYN

e. Close the PDU and click **Capture/Forward** until a PDU returns to the **FTP Client** with a checkmark.

f. Click the PDU envelope and select **Inbound PDU Details**.

How are the port and sequence numbers different than before?

21, 1025, 0, 1. SYN+ACK. The source and destination ports are reversed, and the acknowledgement number is 1.

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

How are the port and sequence numbers different from the previous results?

1025, 21, 1, 1. The source and destination ports are reversed, and both sequence and acknowledgement numbers are 1.

h. Close the PDU and click **Capture/Forward** until a second PDU returns to the **FTP Client**. The PDU is a different color.

i. Open the PDU and select **Inbound PDU Details**. Scroll down past the TCP section.

What is the message from the server?

"Welcome to PT Ftp server"

j. Click Reset Simulation.

Step 3: Examine DNS traffic as the clients communicate with the server.

a. Repeat the steps in Part 1 to create DNS traffic.

b. In the Simulation Panel, change **Edit Filters** to display only **DNS** and **UDP**.

c. Click the PDU envelope to open it.

d. Look at the OSI Model details for the outbound PDU.

What is the Layer 4 protocol?

UDP

Are these communications considered to be reliable?

No

e. Open the Outbound PDU Details tab and find the UDP section of the PDU formats. Record the **SRC PORT** and **DEST PORT** values.

Why are there no sequence and acknowledgement numbers?

1025 (value may vary) and 53. Because UDP does not need to establish a reliable connection.

f. Close the **PDU** and click **Capture/Forward** until a PDU with a check mark returns to the **DNS Client**.

g. Click the PDU envelope and select **Inbound PDU Details**.

How are the port and sequence numbers different than before?

53, 1025. The source and destination ports are reversed.

What is the last section of the **PDU** called? What is the IP address for the name **multiserver.pt.ptu**?

DNS ANSWER, 192.1681.254.

h.   Click Reset Simulation.

Step 4: Examine email traffic as the clients communicate with the server.

a.   Repeat the steps in Part 1 to send an email to **user@multiserver.pt.ptu**.

b.   In the Simulation Panel, change **Edit Filters** to display only **POP3, SMTP** and **TCP**.

c.   Click the first PDU envelope to open it.

d.   Click the **Outbound PDU Details** tab and scroll down to the last section.

What transport layer protocol does email traffic use?

TCP

Are these communications considered to be reliable?

Yes.

e.   Record the **SRC PORT**, **DEST PORT**, **SEQUENCE NUM**, and **ACK NUM** values. What is the flag field value?

1025 (value may vary), 25, 0, 0. SYN

f.   Close the **PDU** and click **Capture/Forward** until a PDU returns to the **E-Mail Client** with a checkmark.

g.   Click the TCP PDU envelope and select **Inbound PDU Details**.

How are the port and sequence numbers different than before?

25, 1025, 0, 1. SYN+ACK. The source and destination ports are reversed, and the acknowledgement number is 1.

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

How are the port and sequence numbers different from the previous two results?

1025, 25, 1, 1. ACK. The source and destination ports are reversed, and both sequence and acknowledgement numbers are 1.

i.   There is a second **PDU** of a different color that **E-Mail Client** has prepared to send to **MultiServer**. This is the beginning of the email communication. Click this second PDU envelope and select **Outbound PDU Details**.

How are the port and sequence numbers different from the previous two **PDU**s?

1025, 25, 1, 1. PSH+ACK. The source and destination ports are reversed, and both sequence and acknowledgement numbers are 1.

What email protocol is associated with TCP port 25? What protocol is associated with TCP port 110?

SMTP. POP3.