Packet Tracer - TCP and UDP Communications Objectives

**Aim:**

The aim of this lab is for the learner to explore in detail, the communication activity of various different traffic types (such as Web (HTTP)) traffic, FTP traffic, DNS traffic and Email).

The network deployment (PT-activity file supplied) incorporates a number of different clients, connected in a star topology to a central switch. 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.

The learner is required to follow the instructions given in this document to complete the simulation, exploring the different states of transmission and complete the questions presented.

Take note of the various protocols used (from the Application layer) and the underlying Transport layer protocol that they use.

Upon completion of this lab exercise, the learner will have gained an understanding of communications between devices using various application protocols and the fundamentals of TCP and UDP as the underlying Transport layer protocols used.

Part 1: Generate Network Traffic in Simulation Mode

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

# Background

~~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

## ~~Generate Network Traffic in Simulation Mode and View Multiplexing~~

### ~~Generate traffic to populate Address Resolution Protocol (ARP) tables.~~

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

* + - 1. ~~Click~~ **~~MultiServer~~** ~~and click the~~ **~~Desktop~~** ~~tab >~~ **~~Command Prompt~~**~~.~~
      2. ~~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.~~
      3. ~~Close the~~ **~~MultiServer~~** ~~window~~.

### ~~Generate web (HTTP) traffic.~~

* + - 1. ~~Switch to Simulation mode.~~
      2. ~~Click~~ **~~HTTP Client~~** ~~and open the~~ **~~Web Browser~~** ~~from the desktop.~~
      3. ~~In the URL field, enter~~ **~~192.168.1.254~~** ~~and click~~ **~~Go~~**~~. Envelopes (PDUs) will appear in the topology window.~~
      4. ~~Minimize, but do not close, the~~ **~~HTTP Client~~** ~~configuration window~~.

### ~~Generate FTP traffic.~~

* + - 1. ~~Click~~ **~~FTP Client~~** ~~and open the~~ **~~Command Prompt~~** ~~from the desktop~~
      2. ~~Enter the~~ **~~ftp 192.168.1.254~~** ~~command. PDUs will appear in the simulation window.~~
      3. ~~Minimize, but do not close, the~~ **~~FTP Client~~** ~~configuration window.~~

### ~~Generate DNS traffic.~~

* + - 1. ~~Click DNS Client and open the~~ **~~Command Prompt~~**~~.~~
      2. ~~Enter the~~ **~~nslookup multiserver.pt.ptu~~** ~~command. A PDU will appear in the simulation window.~~
      3. ~~Minimize, but do not close, the~~ **~~DNS Client~~** ~~configuration window.~~

### ~~Generate Email traffic.~~

* + - 1. ~~Click~~ **~~E-Mail Client~~** ~~and open the~~ **~~E Mail~~** ~~tool from the Desktop.~~
      2. ~~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~~
      3. ~~Click~~ **~~Send~~**~~.~~
      4. ~~Minimize, but do not close, the~~ **~~E-Mail Client~~** ~~configuration window.~~

### ~~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.~~

### ~~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.~~

* + - 1. ~~Click~~ **~~Capture/Forward~~** ~~once. All of the PDUs travel to the switch.~~
      2. ~~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.~~

#### Questions:

**What is this called?**

Answer: Multiplexing

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

Answer: Different colors represent different protocols.  
Brown – DNS   
Light Green – TCP   
Purple – HTTP  
Grey - FTP

## ~~Examine Functionality of the TCP and UDP Protocols~~

### ~~Examine HTTP traffic as the clients communicate with the server.~~

* + - 1. ~~Click~~ **~~Reset Simulation~~**~~.~~
      2. ~~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~~.
      3. ~~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.~~
      4. 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.

#### Question:

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

Answer: It is because connection was being established first, to make sure that the information is sent/received to/from the right device. After information was established, HTTP PDU appeared (purple envelope)

* + - 1. Click the HTTP PDU envelope to show the PDU details. Click the **Outbound PDU Details** tab and scroll down to the second last section.

#### Questions:

**What is the section labeled?**

Answer: TCP

**Are these communications considered to be reliable?**

Answer: Yes, TCP communication is reliable

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

Answer:   
SRC PORT: 1026  
DEST PORT: 80  
SEQ NUM: 1  
ACK NUM: 1

* + - 1. ~~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. (EXPAND THE POP UP WINDOW IS NECESSARY, SO THAT YOU MAY SEE THE FLAG BITS, ALL ON ONE LINE)~~

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

#### Question:

**Which TCP flags are set in this PDU?**

Answer: ACK and PSH here.

* + - 1. ~~Close the PDU and click~~ **~~Capture/Forward~~** ~~until a PDU with a checkmark returns to the~~ **~~HTTP Client~~**~~.~~
      2. ~~Click the PDU envelope and select~~ **~~Inbound PDU Details~~**~~.~~

#### Question:

How are the port and sequence numbers different than before?

Answer:   
Source Port: 80  
Destination Port: 1026  
The source and destination ports have swapped as Server (source) responded to Client (destination). Before Client was the source as it initiated the communication and was sending request to Server.

Type your answers here.

* + - 1. ~~Click the HTTP PDU which~~ **~~HTTP Client~~** ~~has prepared to send to~~ **~~MultiServer~~**~~. This is the beginning of the HTTP communication. Click this second HTTP PDU envelope and select~~ **~~Outbound PDU Details~~**.

#### Question:

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

Answer: The ports are the same, in all three the sequence number is 1 and the ack no is 103. The flags are ACK and PSH (5 and 4)

3rd Last HTTP PDU:  
Source Port: 80  
Destination: 1026   
Sequence No: 1  
Ack No: 103  
  
2nd Last HTTP PDU:  
Source Port: 80  
Destination Port: 1026  
Sequence No: 1  
Ack No: 103  
  
Last HTTP PDU:  
Source Port: 80  
Destination Port: 1026  
Sequence No: 1  
Ack No: 103

* + - 1. ~~Reset the simulation.~~

### ~~Examine FTP traffic as the clients communicate with the server.~~

* + - 1. ~~Open the command prompt on the FTP Client desktop. Initiate an FTP connection by entering~~ **~~ftp 192.168.1.254~~**~~. (place this after c:\> )~~
      2. ~~In the Simulation Panel, change~~ **~~Edit Filters~~** ~~to display only~~ **~~FTP~~** ~~and~~ **~~TCP~~**~~.~~
      3. ~~Click~~ **~~Capture/Forward~~**~~. Click the second PDU envelope to open it. (It’s a TCP PDU)~~

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

#### Question:

**Are these communications considered to be reliable?**

Answer: Yes

* + - 1. **Record the SRC PORT, DEST PORT, SEQUENCE NUM, and ACK NUM values.**

#### Question:

What is the value in the flagfield?

Answer:   
SRC PORT: 1026  
DEST PORT: 21  
SEQ NO: 0  
ACK NO: 0  
FLAGS: 0b000000**1**0 -> SYN (2)

* + - 1. ~~Close the PDU and click~~ **~~Capture/Forward~~** ~~until a PDU returns to the~~ **~~FTP Client~~** ~~with a checkmark.~~
      2. ~~Click the checked PDU envelope and select~~ **~~Inbound PDU Details~~**~~.~~

#### Question:

How are the port and sequence numbers different than before?

Answer: The ports have swapped as the envelope now is coming from Server to FTP Client   
SRC PORT: 21  
DEST PORT: 1026  
SEQ NO: 0  
ACK NO: 1  
FLAGS: 0b000**1**00**1**0 -> SYN (2) + ACK (5)

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

#### Question:

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

Answer: The ports are swapped vs previous result, the sequence number is now 1, ack no remains the same. The flag is only on ACK (5)  
SRC PORT: 1026  
DEST PORT: 21  
SEQ NO: 1  
ACK NO: 1  
FLAGS: 0b000**1**0000 -> ACK (5)

* + - 1. ~~Close the PDU and click~~ **~~Capture/Forward~~** ~~until a second PDU returns to the~~ **~~FTP Client~~**~~. The PDU is a different color and will not have a checked marker attached.~~
      2. ~~Open the PDU and select~~ **~~Inbound PDU Details~~**~~. Scroll down past the TCP section.~~

#### Question:

What is the message from the server? (FTP Response)

Answer:   
“220- Welcome to PT Ftp server  
Username:”~~.~~

* + - 1. ~~Click Reset Simulation.~~

### ~~Examine DNS traffic as the clients communicate with the server.~~

* + - 1. ~~Repeat the steps in Part 1 to create DNS traffic.~~
      2. ~~In the Simulation Panel, change~~ **~~Edit Filters~~** ~~to display only~~ **~~DNS~~** ~~and~~ **~~UDP~~**~~.~~
      3. ~~Click the PDU envelope to open it.~~
      4. ~~Look at the OSI Model details for the outbound PDU.~~

#### Question:

What is the Layer 4 protocol?

Answer: UDP

Are these communications considered to be reliable?

Answer: No, as it does not guarantee packet delivery

Type your answers here.

* + - 1. ~~Open the Outbound PDU Details tab and find the UDP section of the PDU formats. Record the~~ **~~SRC PORT~~** ~~and~~ **~~DEST PORT~~** ~~values.~~

#### Question:

Why are there no sequence and acknowledgement numbers?

Answer: There is no SEQ NO or ACK NO because UDP does not need to establish a reliable connection.  
SRC PORT: 1026  
DEST PORT: 53

Type your answers here.

* + - 1. ~~Close the~~ **~~PDU~~** ~~and click~~ **~~Capture/Forward~~** ~~until a PDU with a check mark returns to the~~ **~~DNS Client~~**~~.~~
      2. ~~Click the PDU envelope and select~~ **~~Inbound PDU Details~~**.

#### Question:

How are the port and sequence numbers different than before?

Answer: The ports are now swapped, source being 53 and dest 1026. There is no sequence number in the PDU Details for DNS or any other header.   
SRC PORT: 53  
DEST PORT: 1026  
SEQ NO: N/A

Type your answers here.

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

Answer: DNS Answer. The IP address: 192.168.1.254

* + - 1. ~~Click Reset Simulation.~~

### ~~Examine email traffic as the clients communicate with the server.~~

* + - 1. ~~Repeat the steps in Part 1 to send an email to~~ **~~user@multiserver.pt.ptu~~**~~.~~
      2. ~~In the Simulation Panel, change~~ **~~Edit Filters~~** ~~to display only~~ **~~POP3, SMTP~~** ~~and~~ **~~TCP~~**~~.~~
      3. ~~Click the first PDU envelope to open it. (a TCP PDU)~~
      4. ~~Click the~~ **~~Outbound PDU Details~~** ~~tab and scroll down to the last section.~~

#### Questions:

**What transport layer protocol does email traffic use?**

Answer: TCP

**Are these communications considered to be reliable?**

Answer: Yes

here.

* + - 1. **Record the SRC PORT, DEST PORT, SEQUENCE NUM, and ACK NUM values.**

What is the flag field value?

Answer:   
SRC PORT: 1027  
DEST PORT: 25  
SEQ NO: 0  
ACK NO: 0  
FLAG: 0b000000**1**0 -> SYN (2)

Type your answers here.

* + - 1. ~~Close the~~ **~~PDU~~** ~~and click~~ **~~Capture/Forward~~** ~~until a PDU returns to the~~ **~~E-Mail Client~~** ~~with a checkmark.~~
      2. ~~Click the TCP PDU envelope and select~~ **~~Inbound PDU Details~~**~~.~~

#### Question:

**How are the port and sequence numbers different than before?**

Answer: The ports have now reversed, sequence number is still 0 and ack number changed to 1.  
SRC PORT: 25  
DEST PORT: 1027  
SEQ NO: 0  
ACK NO: 1  
FLAG: 0b000**1**00**1**0 -> ACK (5) + SYN (2)

here.

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

#### Question:

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

Answer: The port numbers are reversed vs Inbound PDU Details tab, the seq and ack numbers are both at 1 and the flag is only at ack.  
SRC PORT: 1027  
DEST PORT: 25  
SEQ NO: 1  
ACK NO: 1  
FLAG: 0b00**1**0000 -> ACK (5)

* + - 1. 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**.

#### Questions:

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

Answer:   
Difference between previous TCP: The src/dest ports, seq/ack no are the same as previous TCP PDU. The flag has changed, and flag changed from Ack to ACK+PSH.   
  
Difference between second TCP: The ports have reversed, the swq number is now 1 and the ack is still 1. The flag is changed from ACK+SYN to ACK+PSH   
  
SMTP TCP Details:  
SRC PORT: 1027  
DEST PORT: 25  
SEQ NO: 1  
ACK NO: 1  
FLAG: 0b000**11**000 -> ACK (5) + PSH (4)

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

Answer:   
TCP port 25 -> SMTP protocol (transmitting emails)  
TCP port 110 -> POP3 protocol (downloads messaged directly to our device)

.