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 di ferent 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.

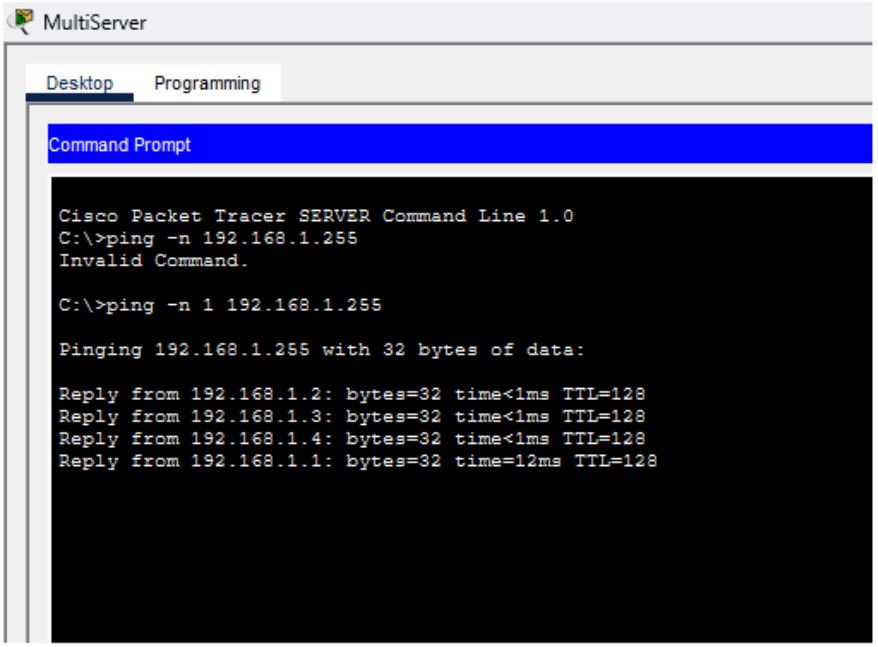
You will explore the functionality of the TCP and UDP protocols, multiplexing, and the function of port numbers in determining which local application requested the data or is sending the data.

Packet Tracer wi l not score this activity.

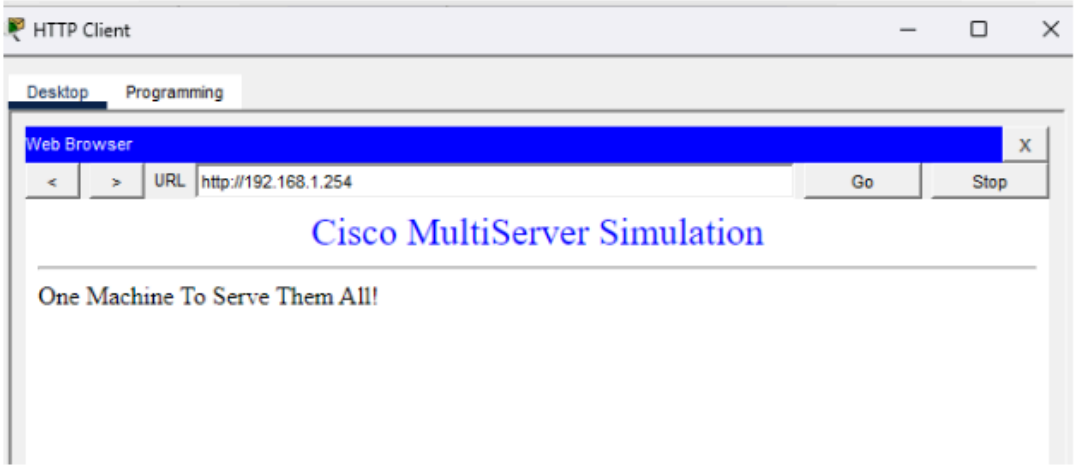
Instructions

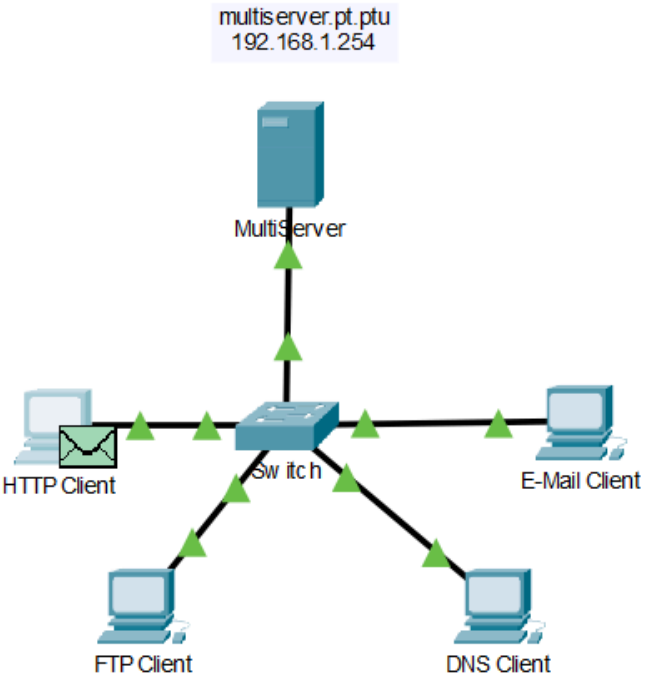
Part 1: Generate Network Traffic in Simulation Mode and View Multiplexing

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

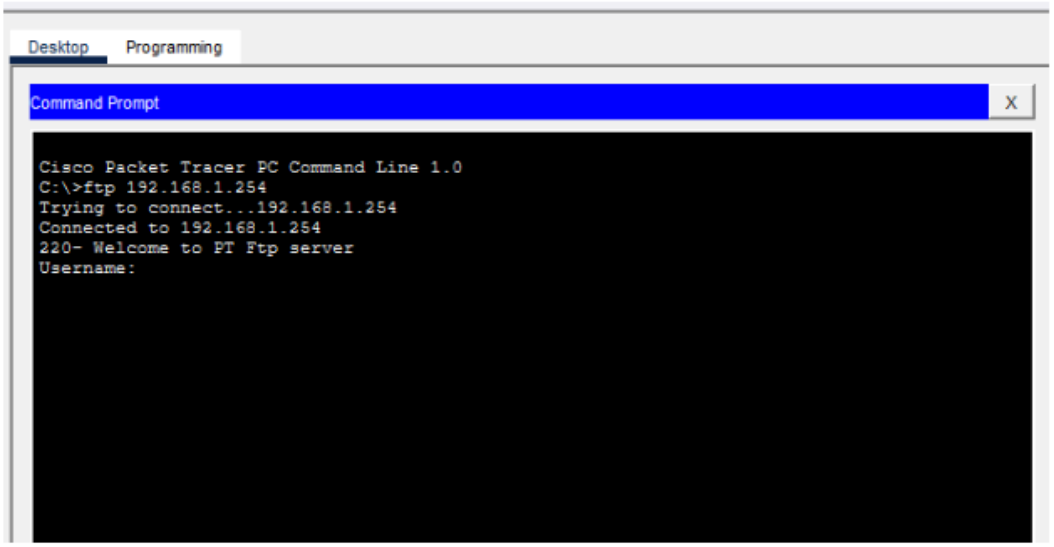


Step 2: Generate web (HTTP) traffic.

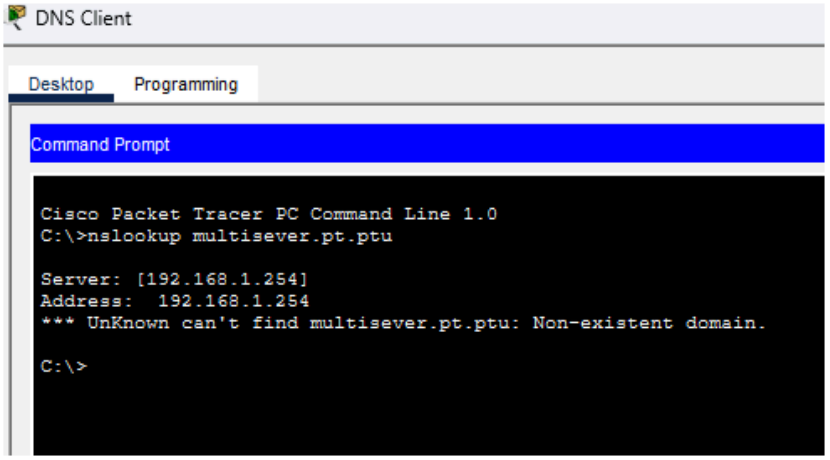




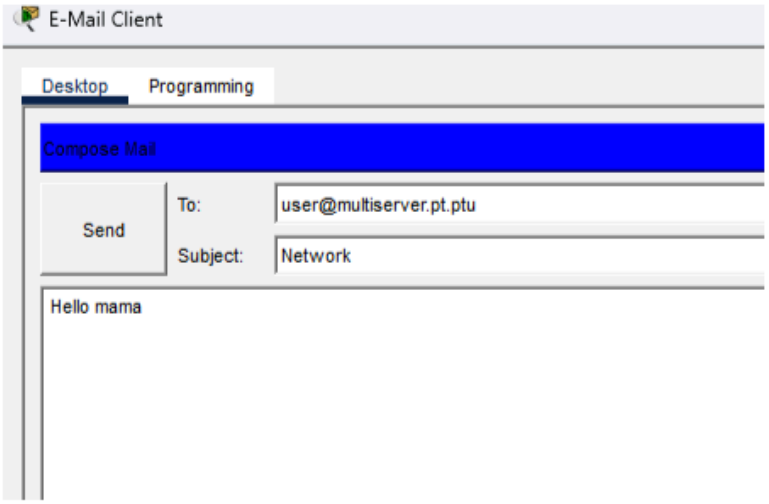
Step 3: Generate FTP traffic.



Step 4: Generate DNS traffic.



Step 5: Generate Email traffic.



1.What is this called?

-เรียกว่า Multiplexing

คือการที่หลายๆโปรโตคอลหรือหลายแอปพลิเคชันส่งข้อมูลผ่านสื่อเดียวกันถูกจัดการด้วย port number ทำให้แยกได้ว่า packet มาจากอะไร

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

-สีที่ต่างกันใช้เพื่อแยกประเภทของโปรโตคอลหรือชนิดของ PDU เช่น สีหนึ่งอาจแทน HTTP

อีกสีแทน TCP อีกสีแทน DNS / UDP หรือ Email / FTP

Part 2: Examine Functionality of the TCP and UDP Protocols

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

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.

Event List

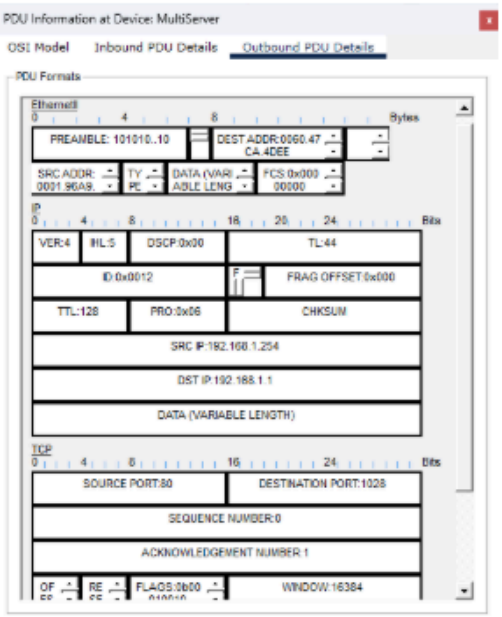
	At Device	Type
	HTTP Client	TCP
	Switch	TCP
	MultiServer	TCP
	Switch	TCP
	HTTP Client	TCP
	HTTP Client	HTTP
	Switch	TCP
	HTTP Client	HTTP
	Switch	HTTP
	MultiServer	TCP

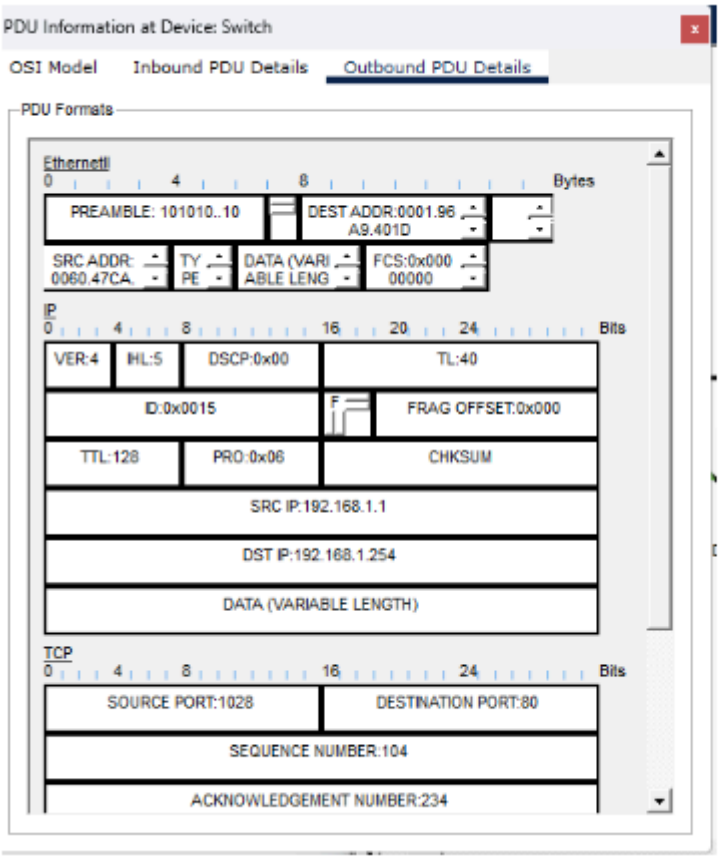
d. Click Capture/Forward until you see a PDU appear for HTTP. Note that the color of the envelope in the
topology window matches the color code for the HTTP PDU in the Simulation Panel.
Question:**Why did it take so long for the HTTP PDU to appear?**

เพราะก่อนที่จะส่งข้อมูล HTTP จริง ๆ ต้องมีขั้นตอน **TCP Three-Way Handshake** ก่อน ได้แก่ SYN

SYN-ACK ACK รวมถึงอาจมี ARP หรือ DNS ที่ต้องทำก่อน ทำให้ใน Simulation ต้องมีหลาย PDU วิ่งก่อน จึงจะเห็น HTTP PDU ปรากฏภายหลัง

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.





-ส่วนนี้จะถูกระบุว่า TCP เพราะ HTTP ใช้ TCP ที่ Transport Layer

Are these communications considered to be reliable?

-Yes, reliable TCP เป็นโปรโตคอลแบบ connection-oriented มีการยืนยันการรับข้อมูล (ACK) และมีการเรียงลำดับ sequence

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

-ค่าตัวเลขตรงนี้ของแต่ละคนอาจไม่เหมือนกันใน Packet Tracer เพราะระบบสุ่ม ephemeral port แต่รูปแบบที่ควรเห็นคือ:

SRC PORT : หมายเลขพอร์ตฝั่ง Client มักเป็นเลขสุ่ม >1023

DEST PORT : 80 HTTP

SEQUENCE NUM : เริ่มต้นมักเป็น 0 หรือ 1

ACK NUM : 0 หรือ 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.

Which TCP flags are set in this PDU?

-SYN -ACK

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.

Question:How are the port and sequence numbers different than before?

-SRC PORT และ DEST PORT สลับกัน

-SEQUENCE NUM และ ACK NUM เปลี่ยนค่า เพื่อยืนยันการรับข้อมูลจาก PDU ก่อนหน้า

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.

Question:What information is now listed in the TCP section? How are the port and sequence numbers differentfrom the previous two PDUs?

-แสดงข้อมูล TCP สำหรับการรับ–ส่งข้อมูลจริง (Data Transfer)

-หมายเลข Sequence Number เพิ่มขึ้น ตามปริมาณข้อมูล

-ACK Number ใช้ยืนยันข้อมูลที่ได้รับแล้ว

-พอร์ตยังคงเดิม (Client ↔ Server) แต่บทบาทผู้ส่ง–ผู้รับเปลี่ยนไป

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.

Question:Are these communications considered to be reliable?

-เชื่อถือได้

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

Question:What is the value in the flag field?

- :0b00010000

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.

Question:How are the port and sequence numbers different than before?

- พอร์ตต้นทางและปลายทางสลับกัน และหมายเลขลำดับและหมายเลขการรับทราบเปลี่ยนแปลงไป เนื่องจากเซิร์ฟเวอร์กำลังตอบกลับและรับทราบเซ็กเมนต์ TCP ก่อนหน้า

g. Click the Outbound PDU Details tab.

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

- พอร์ตต้นทางและปลายทางจะสลับกลับไปยังฝั่งผู้ส่ง ข้อมูลลำดับจะเพิ่มขึ้น และหมายเลขการยืนยันจะได้รับการอัปเดตเพื่อยืนยันว่าได้รับข้อมูลจากเซิร์ฟเวอร์แล้ว

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.

Question:What is the message from the server?

- ใน FTP ส่วนใหญ่ เมื่อ client เชื่อมต่อสำเร็จ ข้อความจาก server ที่จะเห็นหลัง TCP section คือ 220 Service ready for new user

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.

Question:What is the Layer 4 protocol?

- UDP (User Datagram Protocol) เพราะ DNS ใน Packet Tracer ใช้ UDP ที่ Transport Layer

Are these communications considered to be reliable?

-เชื่อถือไม่ได้

เนื่องจาก UDP เป็น connectionless ไม่มี ACK และไม่มีการรับประกันการส่งถึงเหมือน TCP

e. 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?

-เพราะ DNS ใช้ UDP ซึ่งเป็น connectionless protocol

UDP ไม่มีการเรียงลำดับข้อมูลและไม่มีการยืนยันการรับ (ACK) จึงไม่มี sequence number หรือ acknowledgement number

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.

Question:How are the port and sequence numbers different than before?

ตอบ : ตอน Inbound PDU

- SRC PORT กับ DEST PORT จะสลับกัน เมื่อ server ตอบกลับ client
- UDP ไม่มี sequence number อยู่แล้ว จึงไม่มีค่า sequence เปลี่ยนเหมือน TCP

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

ตอบ : ส่วนสุดท้ายของ PDU คือ DNS IP address ของ multiserver.pt.ptu = 192.168.1.254

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.

Questions:What transport layer protocol does email traffic use?

ตอบ : TCP

Are these communications considered to be reliable?

ตอบ : น่าเชื่อถือ เพราะ TCP มี ACK และ sequence number

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

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.
Question:How are the port and sequence numbers different than before?
ตอบ : ตอนเป็น Inbound PDU

- SRC PORT และ DEST PORT สลับกัน (server ตอบกลับ client)
- SEQUENCE และ ACK numbers เปลี่ยนค่า เพื่อยืนยัน segment ก่อนหน้า

h. Click the Outbound PDU Details tab.
Question:How are the port and sequence numbers different from the previous two results?
ตอบ : ใน Outbound PDU รอบใหม่

- พอร์ตกลับมาเป็นฝั่ง client ส่งอีกครั้ง
- Sequence number เพิ่มขึ้น จากเดิม
- ACK number อัปเดตตาม packet ที่เพิ่งรับ

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.

Questions:How are the port and sequence numbers different from the previous two PDUs?
ตอบ : PDU สีใหม่คือเริ่ม session email จริง

- ใช้ port ของโปรโตคอล email
- sequence number เริ่มลำดับใหม่ของ data
- acknowledgement number เปลี่ยนตามการตอบกลับล่าสุด

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

ตอบ : TCP port 25 = SMTP

TCP port 110 = POP3