นาย วัชรพล ดวงกองเงิน 673380290-9

Assignment 4: 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

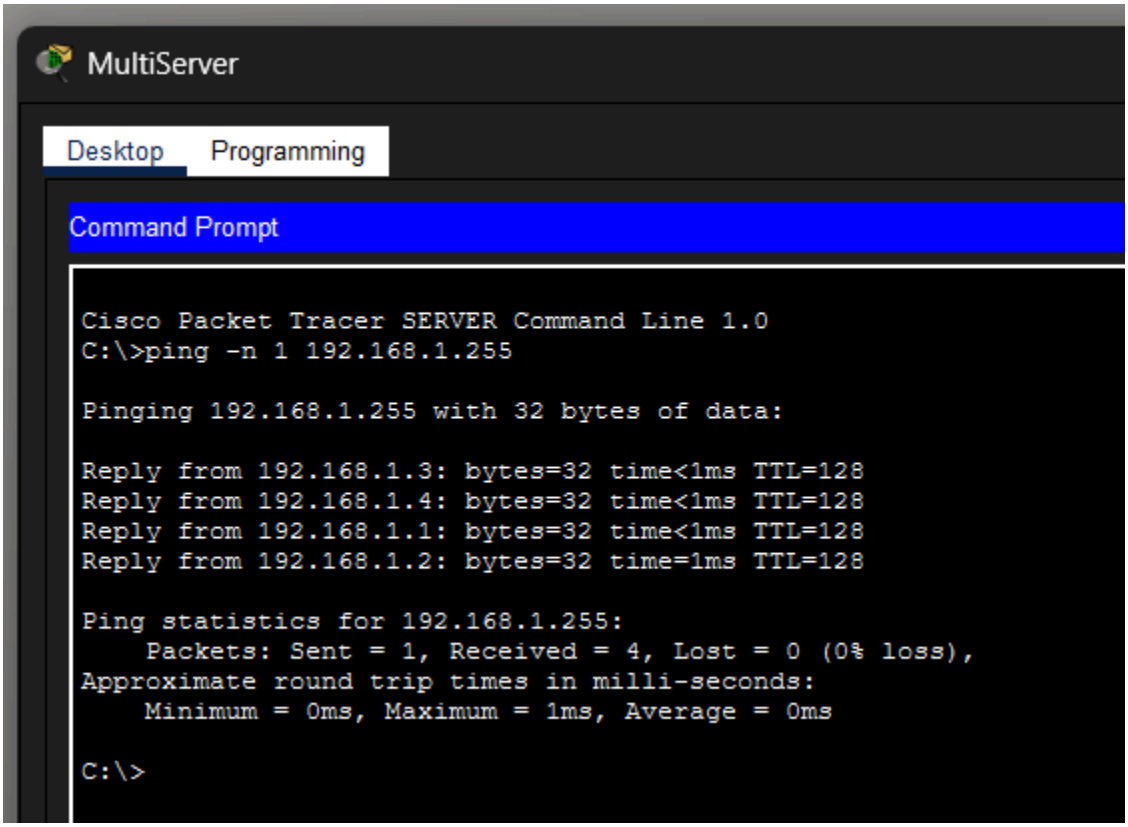
This simulation activity is intended to provide a foundation for understanding TCP and UDP in detail. Packet Tracer simulation mode provides you the ability to view the state of different PDUs as they travel through the network.

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.

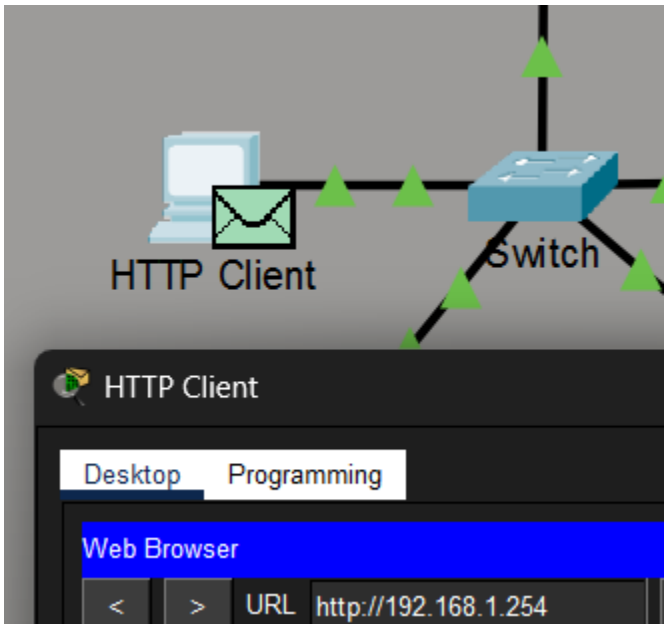
Instructions

Part 1: Generate Network Traffic and View Multiplexing

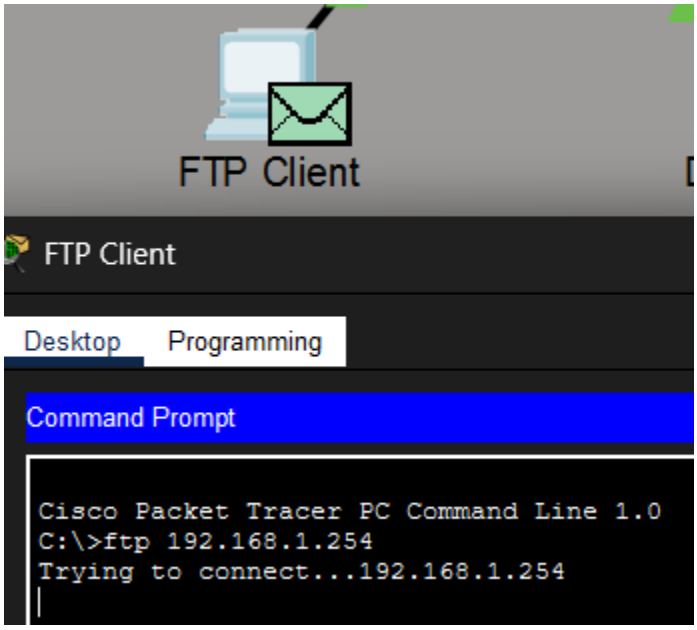
Step 1: Generate traffic to populate ARP tables



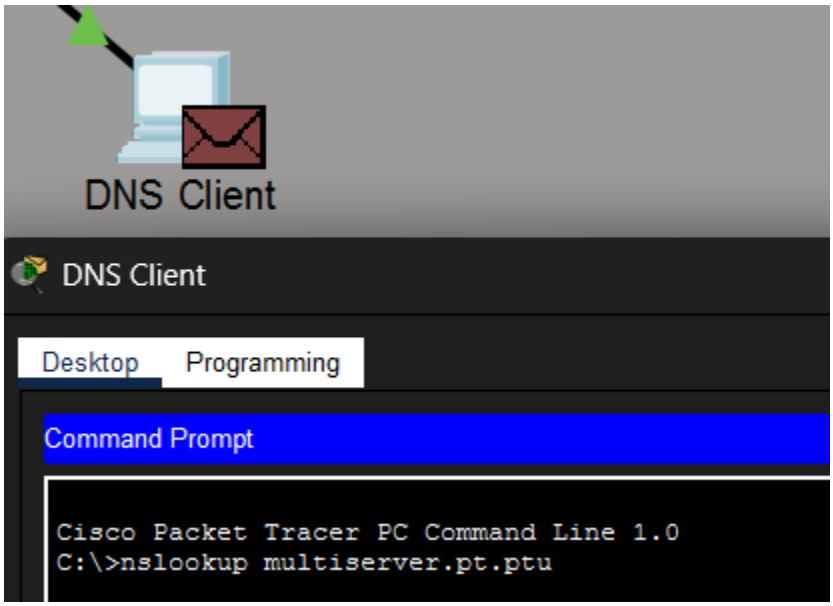
Step 2 : Create web(HTTP) Traffic



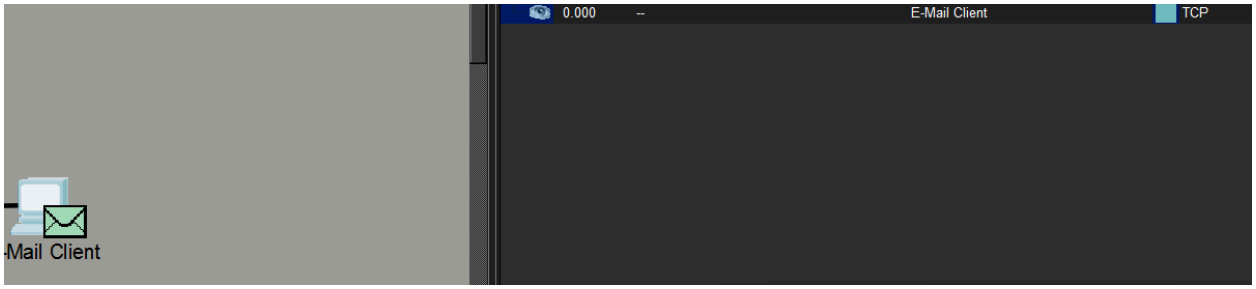
Step 3 : Create FTP Traffic



Step 4 : Create DNS Traffic



Step 5 : Create Email Traffic

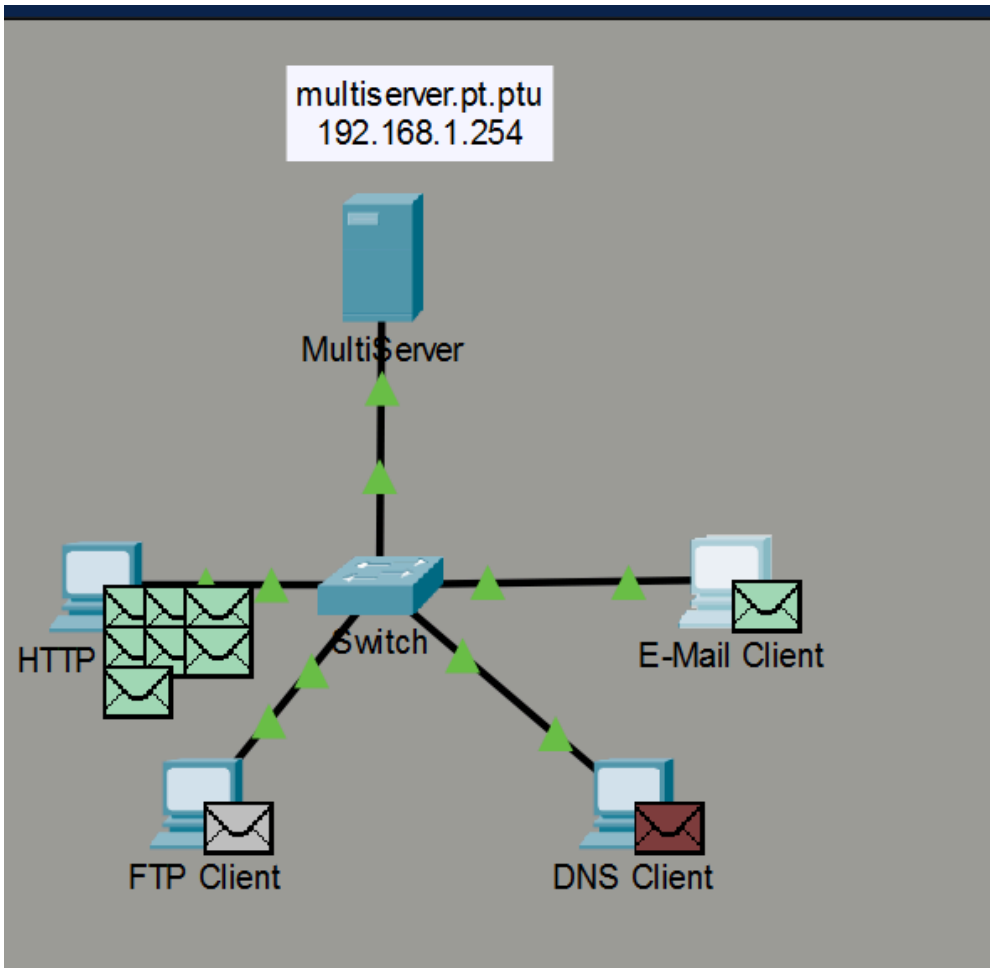


Step 6: Verify that traffic is generated and ready for simulation

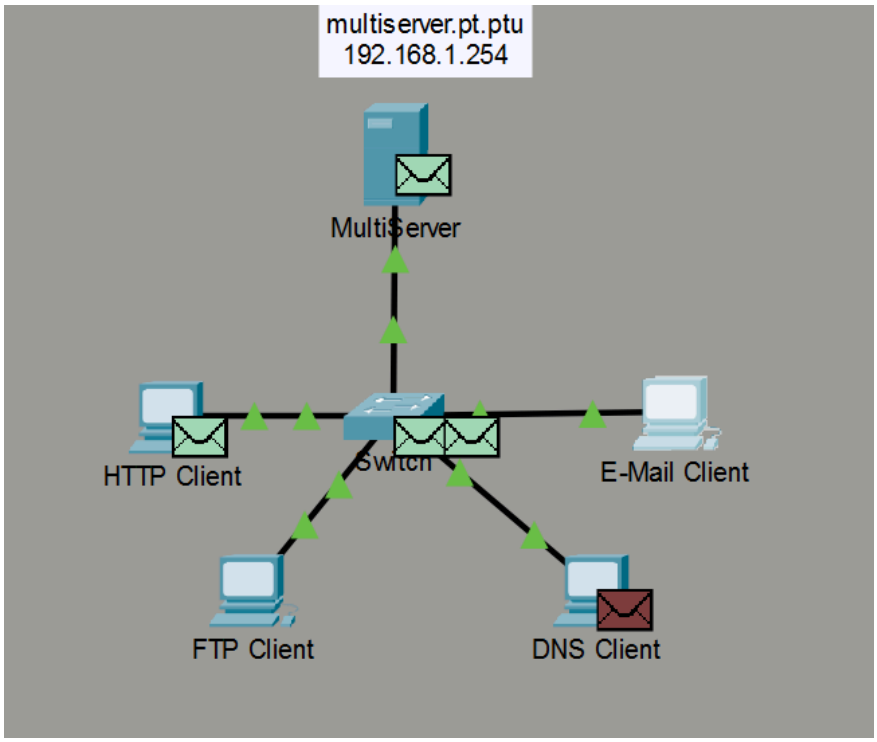
Before start simulation

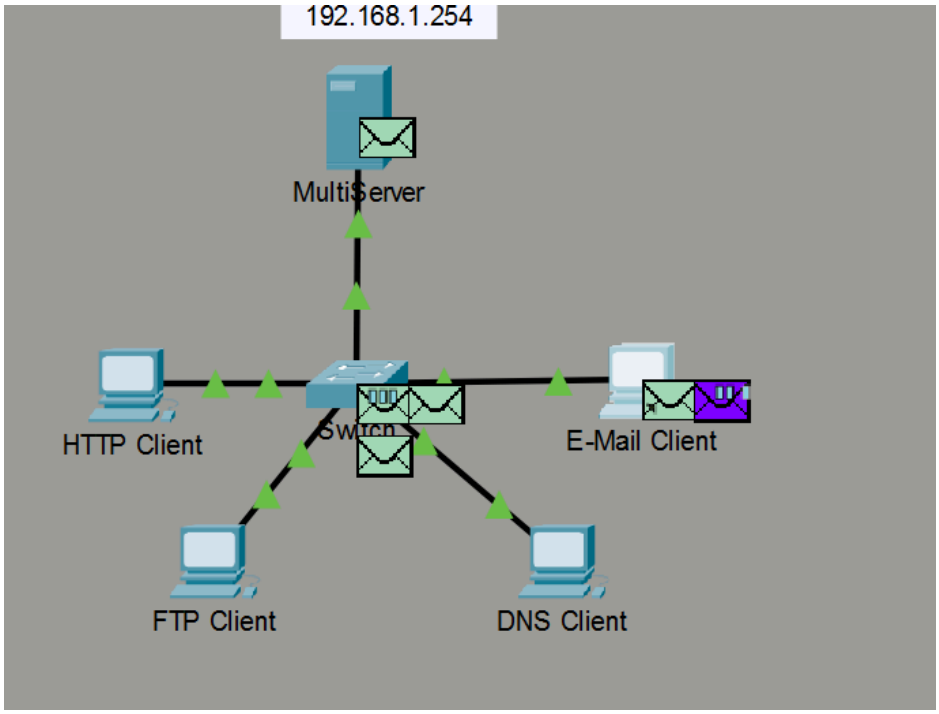
Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	HTTP Client	TCP
	0.000	--	HTTP Client	TCP
	0.000	--	HTTP Client	TCP
	0.000	--	HTTP Client	TCP
	0.000	--	HTTP Client	TCP
	0.000	--	HTTP Client	TCP
	0.000	--	HTTP Client	TCP
	0.000	--	FTP Client	FTP
	0.000	--	DNS Client	DNS
	0.000	--	E-Mail Client	TCP



After pressing 6-7 Capture/forward





Step 7: Examine multiplexing

What is this called?

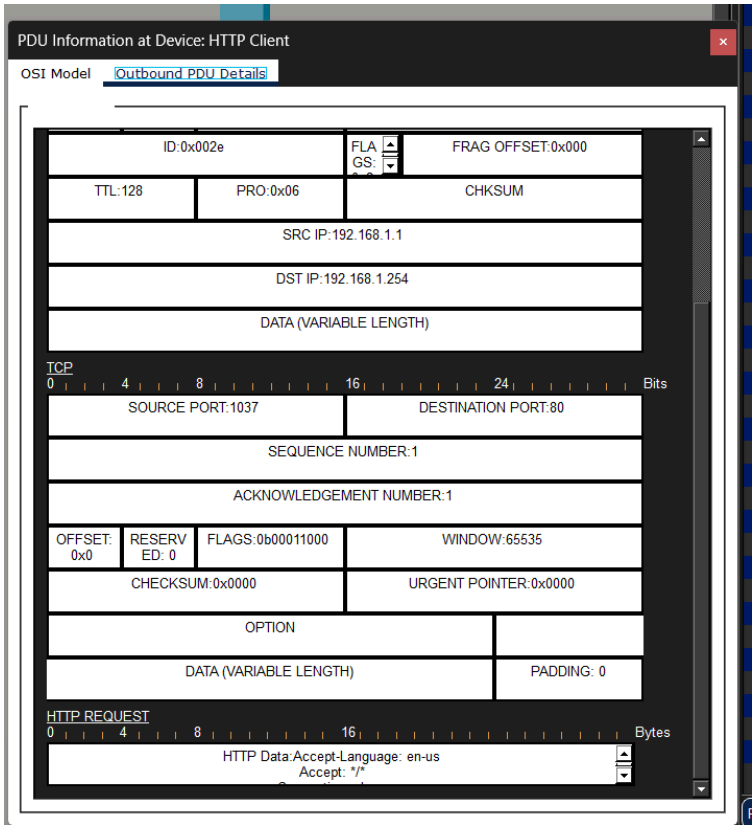
- Multiplexing

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

- สีม่วง เป็น SMTP , HTTP
- สีแดง จะเป็น DNS
- สีมิ้น จะเป็น TCP

Part 2: Examine Functionality of the TCP and UDP Protocols

Step 1: Examine HTTP Traffic (TCP)



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

- เนื่องจาก TCP ต้องสร้างการเชื่อมต่อก่อนส่งข้อมูล โดยใช้กระบวนการ Three-way Handshake (SYN, SYN-ACK, ACK) ทำให้เกิดความล่าช้าเมื่อเทียบกับ UDP

What is the section labeled?

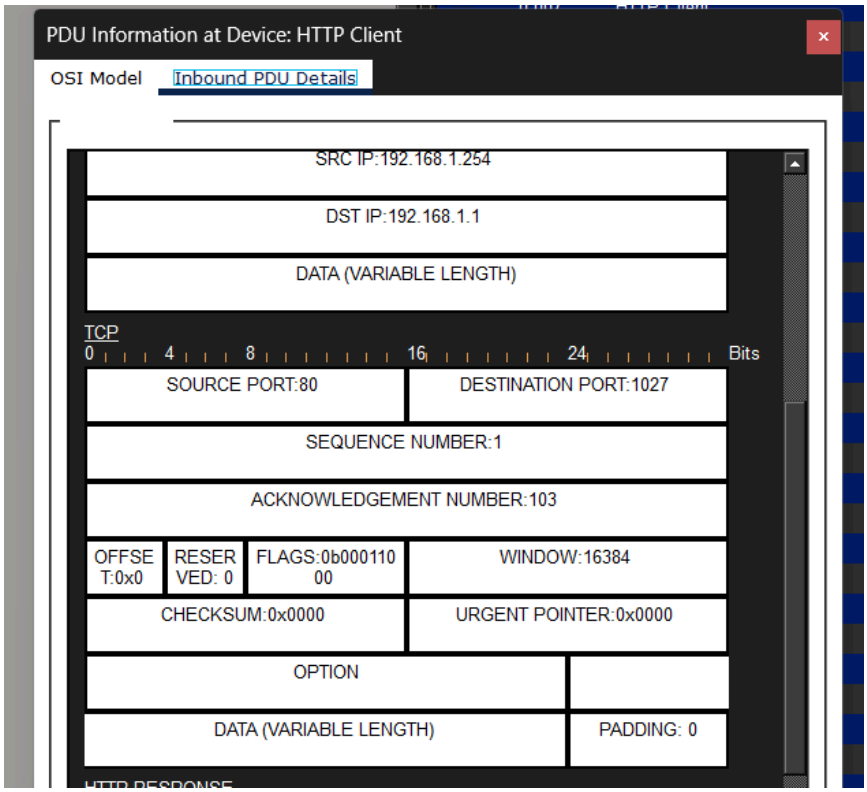
- TCP

Are these communications considered to be reliable?

- เชื่อถือได้เพราะมีการใช้ Sequence Number เพื่อจัดลำดับข้อมูลและ Acknowledgment Number เพื่อยืนยันว่าปลายทางได้รับข้อมูลครบถ้วน

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

- *SRC PORT : **1025**, DEST PORT : **80***
- *SEQUENCE NUM : **1** , ACK NUM : **1***



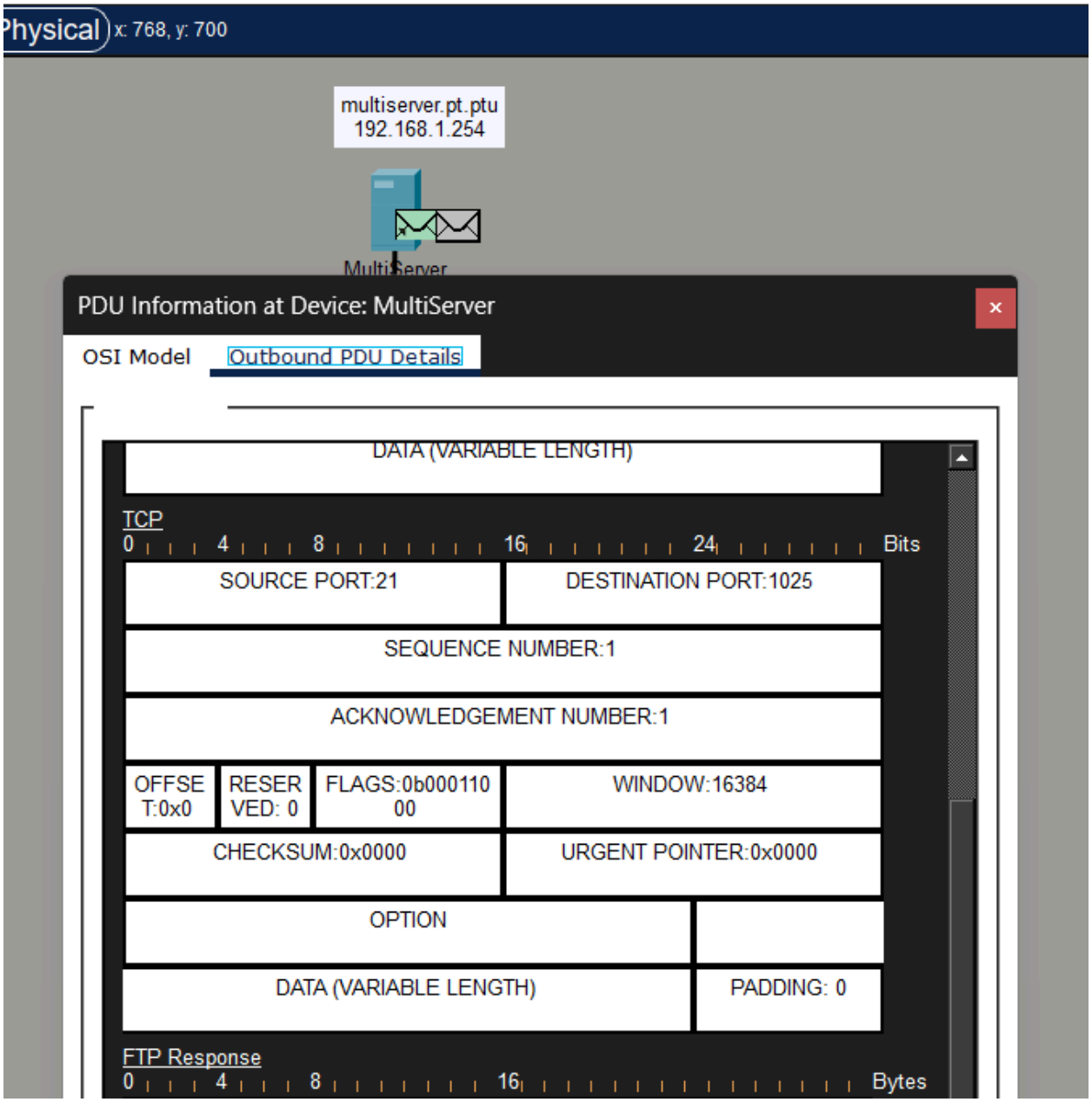
How are the port and sequence numbers different than before?

- เกิดการสลับกัน โดยพอร์ตต้นทางกลายเป็น **80** และปลายทางกลายเป็น **1027**

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

- เลข Acknowledgment Number จะอัปเดตตามจำนวนข้อมูลที่ Server ส่งมาให้ เพื่อยืนยันว่าฝั่งเราได้รับของครบแล้วเช่นกัน

Step 2: Examine FTP Traffic (TCP)



Are these communications considered to be reliable?

- น่าเชื่อถือ เพราะ FTP ต้องการความถูกต้องของไฟล์ 100% จึงต้องใช้ TCP ที่มีระบบตรวจสอบและส่งซ่อมข้อมูลที่หายไป

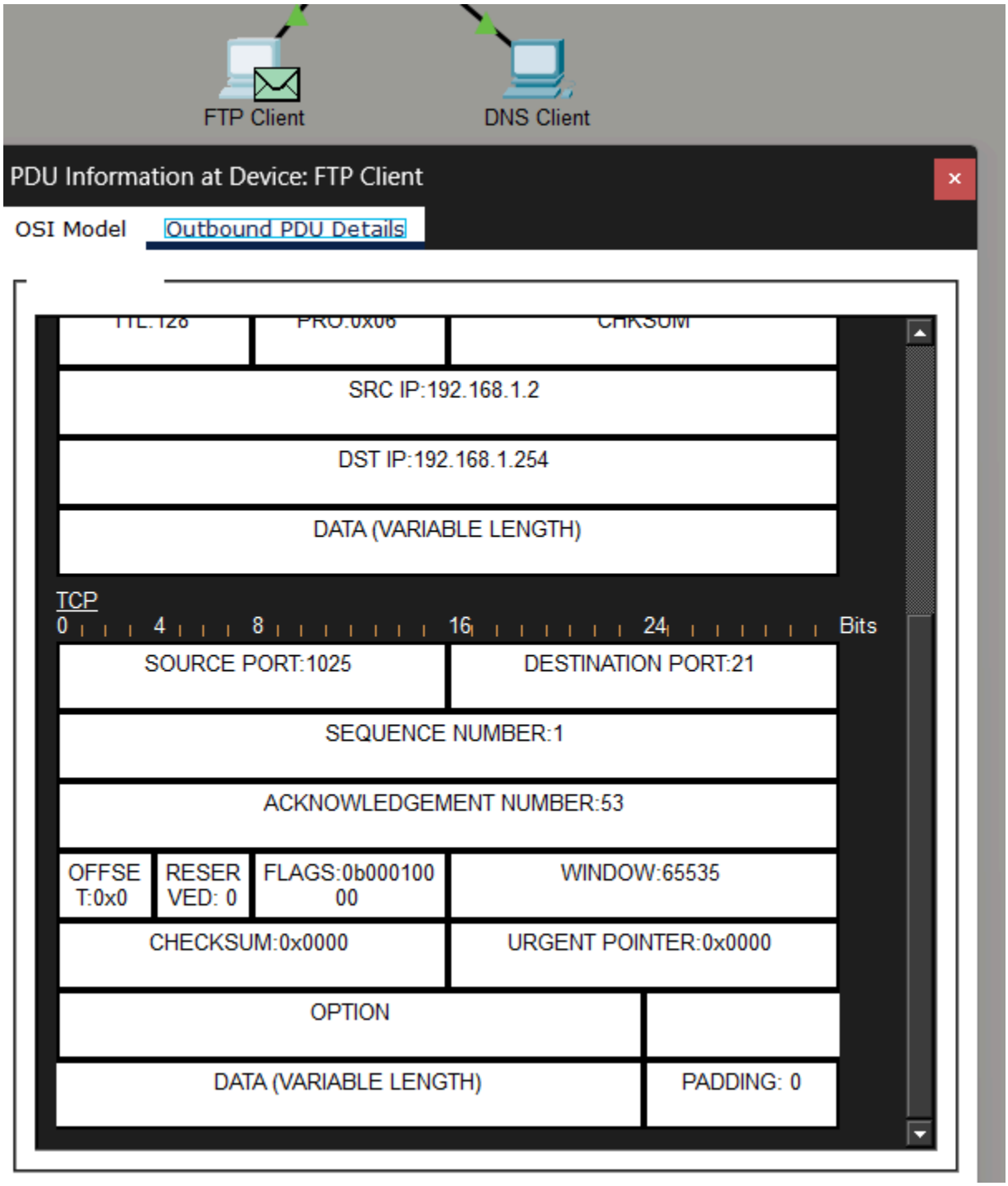
Record the **SRC PORT**, **DEST PORT**, **SEQUENCE NUM**, and **ACK NUM** values.

- SRC PORT: **21**, DEST PORT: **1025**

- SEQUENCE NUM: **1** , ACK NUM: **1**

What is the value in the flag field?

- Flags: 0b00011000



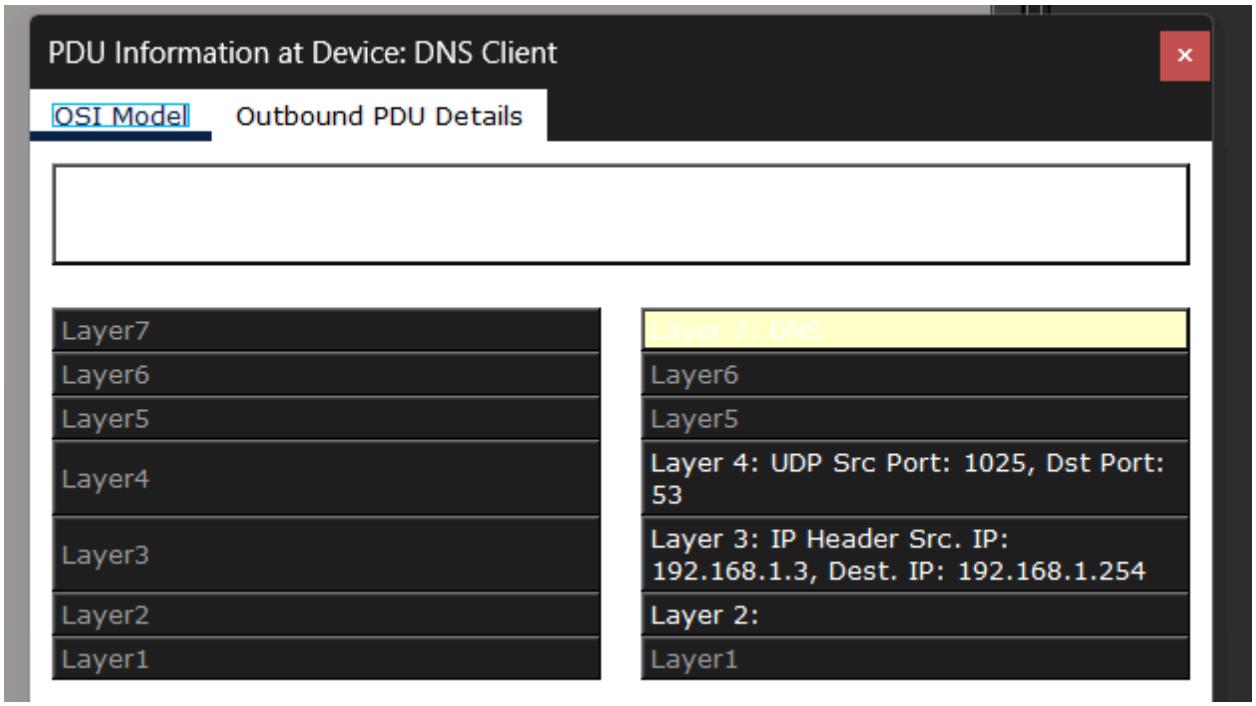
How are the port and sequence numbers different from the previous results?

- Ports: สลับกัน Source: 1025, Dest: 21 เพื่อให้ข้อมูลกลับมาถูกช่องทาง
- Sequence/Ack: ค่า Acknowledgment Number เพิ่มขึ้นจากเดิมเป็น 53

What is the message from the server?

- Sequence Number: จะขยับตามเลขที่ Server ร้องขอมา
- Acknowledgment Number: จะขยับตามสถานะการตอบรับของฝั่ง Server

Step 3: Examine DNS Traffic (UDP)



What is the Layer 4 protocol?

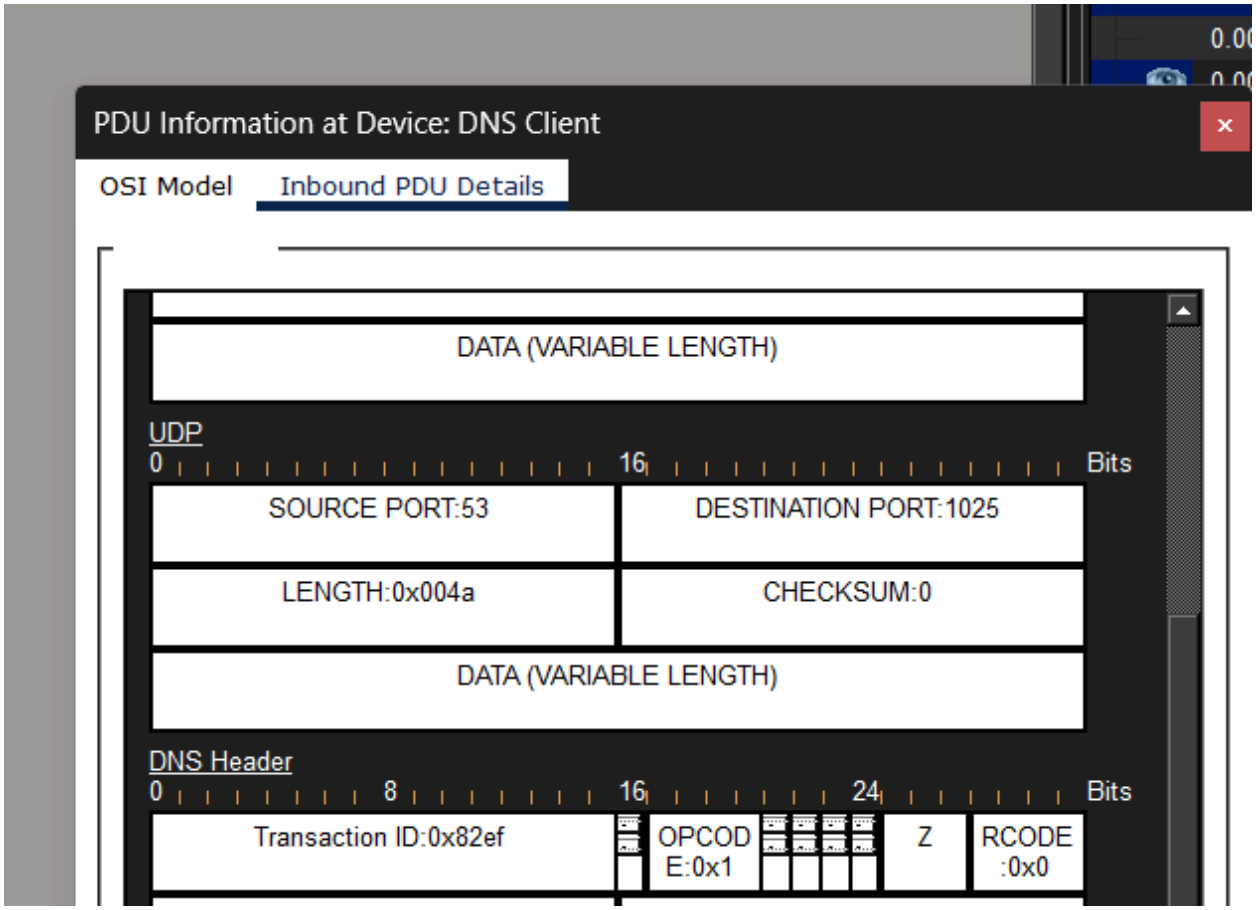
- Layer 4: UDP Src Port: 1025, Dst Port: 53

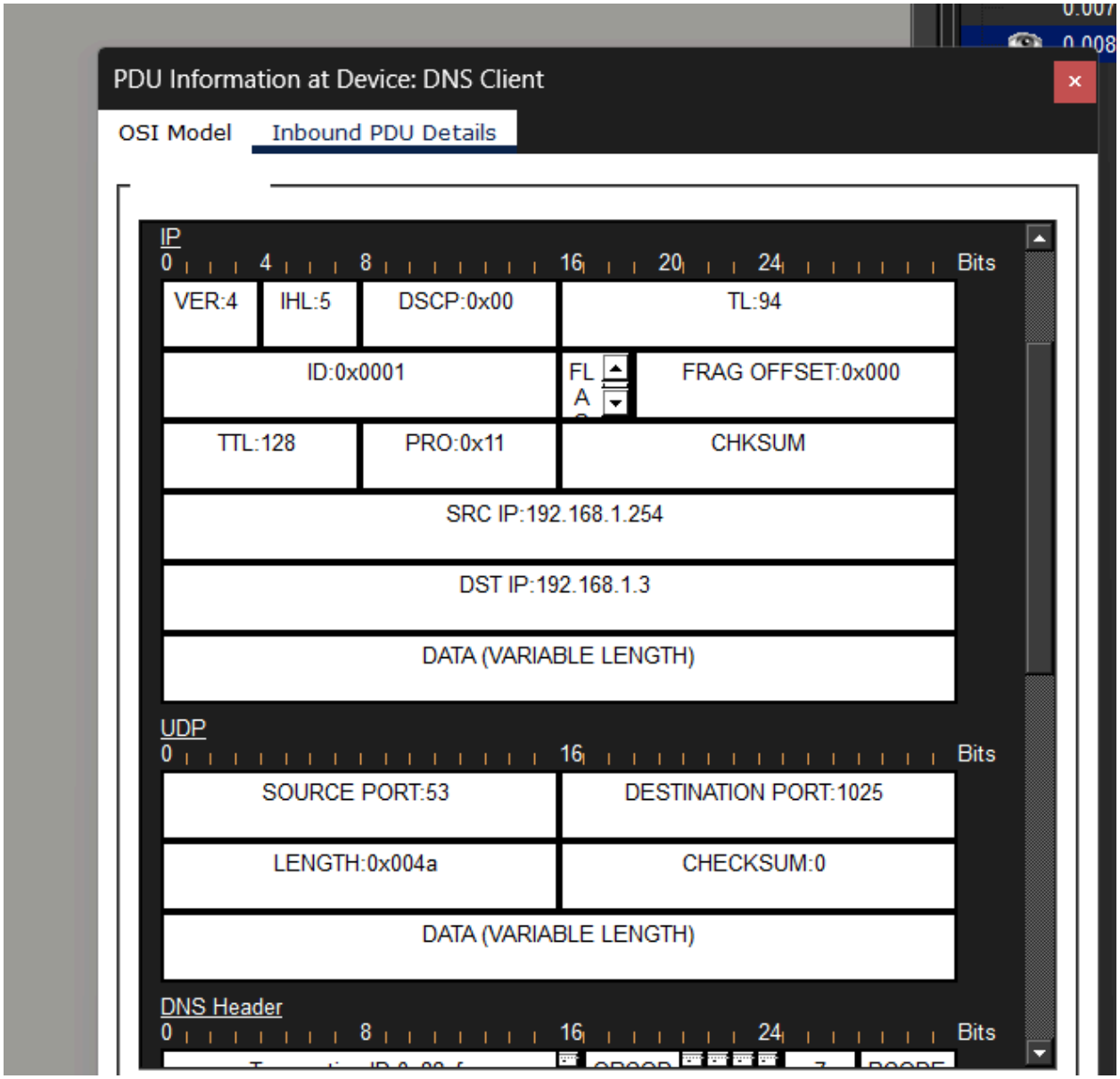
Are these communications considered to be reliable?

- ไม่

Why are there no sequence and acknowledgement numbers?

- เพราะมันคือโปรโตคอลแบบ Connectionless ซึ่งต่างจาก TCP


PDU Information at Device: DNS Client
OSI Model
Inbound PDU Details
DATA (VARIABLE LENGTH)
UDP
0
16
Bits
SOURCE PORT:53
DESTINATION PORT:1025
LENGTH:0x004a
CHECKSUM:0
DATA (VARIABLE LENGTH)
DNS Header
0
8
16
24
Bits
Transaction ID:0x82ef
OPCODE:0x1
Z
RCODE:0x0

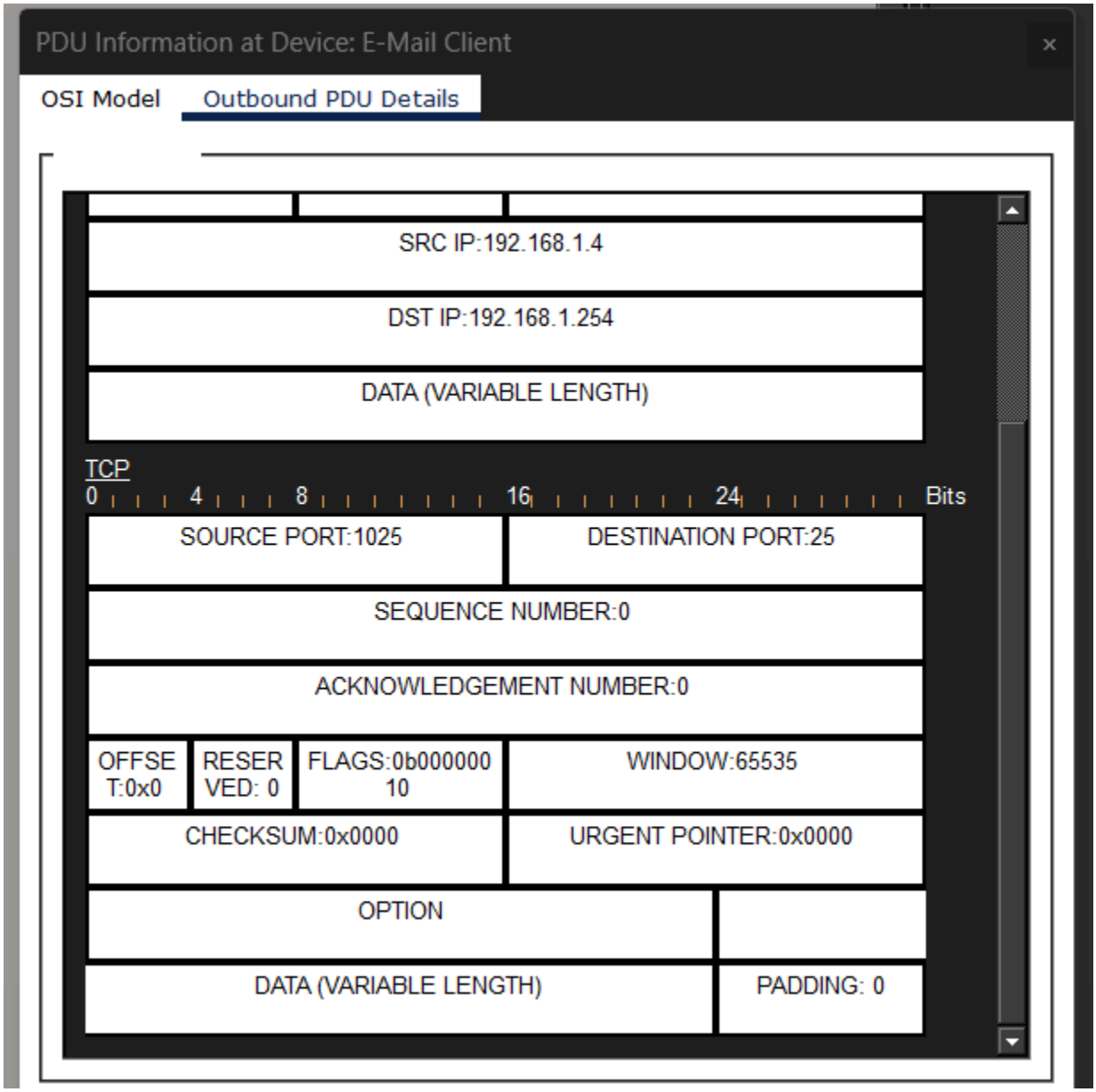


How are the port and sequence numbers different than before?

- Seq number ไม่มีเหมือนเดิม พอร์ตก็เหมือนเดิม

Step 4: Examine Email Traffic (TCP)

c.



What transport layer protocol does email traffic use?

- TCP

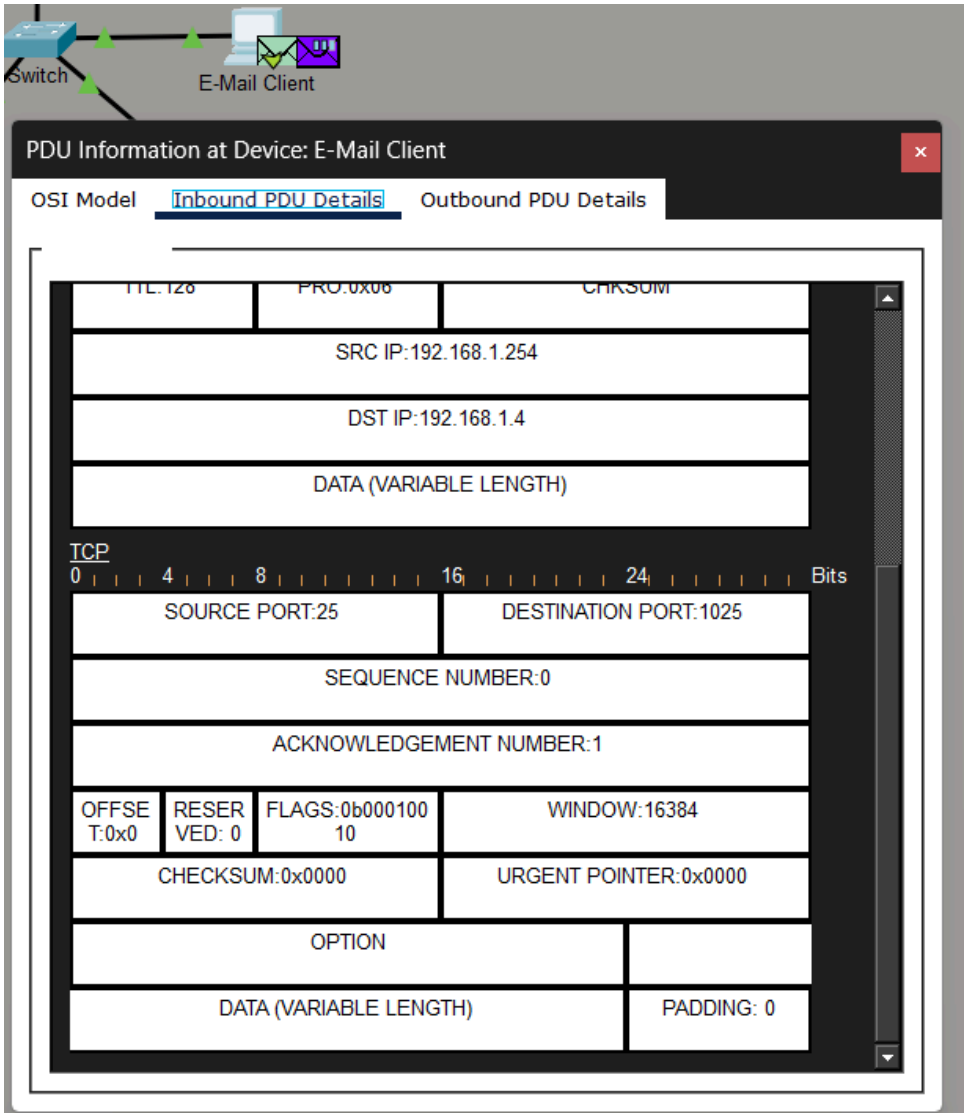
Are these communications considered to be reliable?

- Yes

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

- **SRC PORT:** 1025 **DEST PORT: 25**
  SEQUENCE NUM: 0 **ACK NUM:** 0 , flag SYN

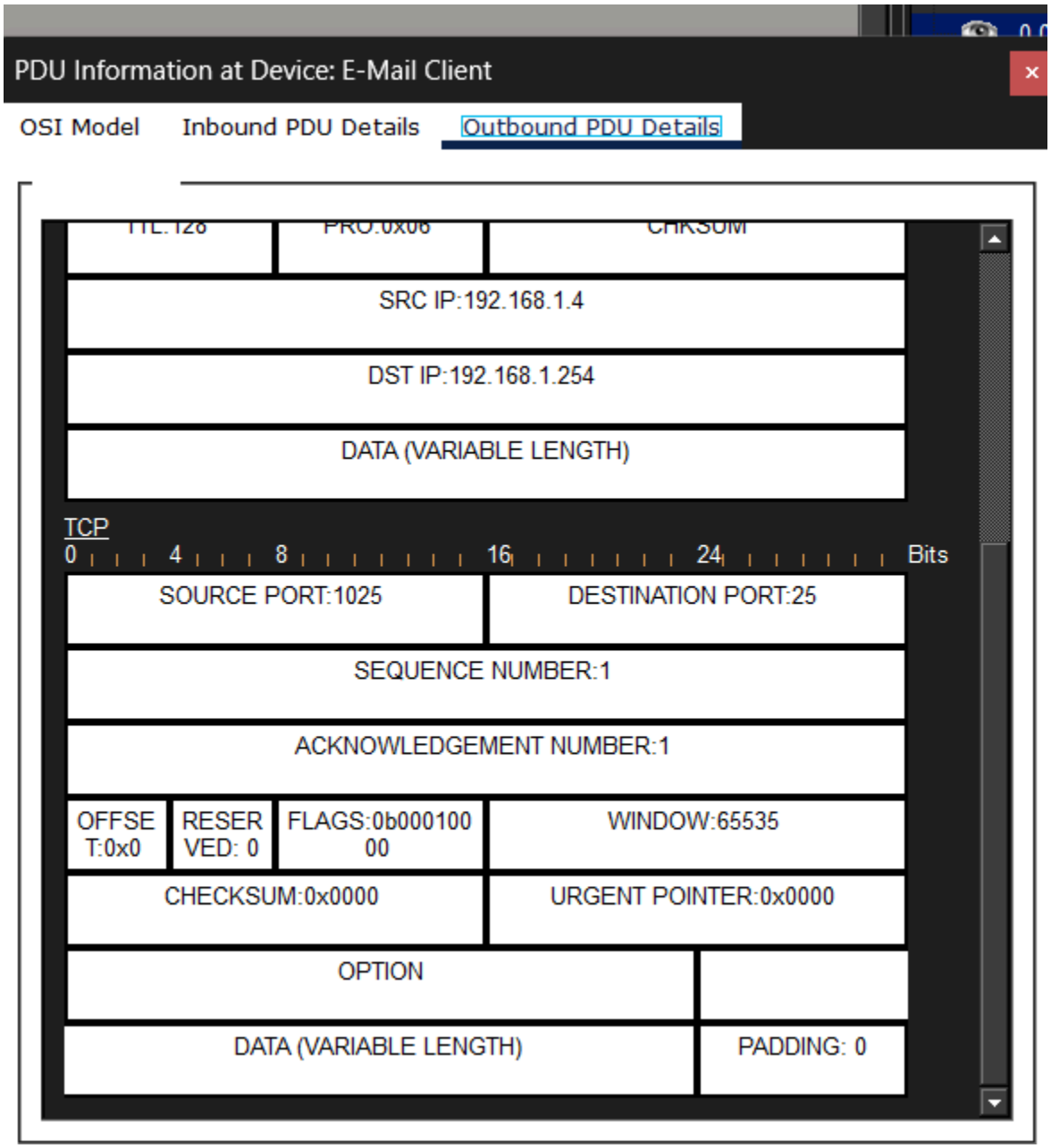
f.



How are the port and sequence numbers different than before?

- เกิดการสลับตำแหน่งโดย Source Port กลายเป็น 25 และ Destination Port กลายเป็น 1026
- ACK NUM ขยับเป็น 1 เพื่อตอบรับซองแรก และค่า Flags เป็น 0x12 (SYN + ACK)

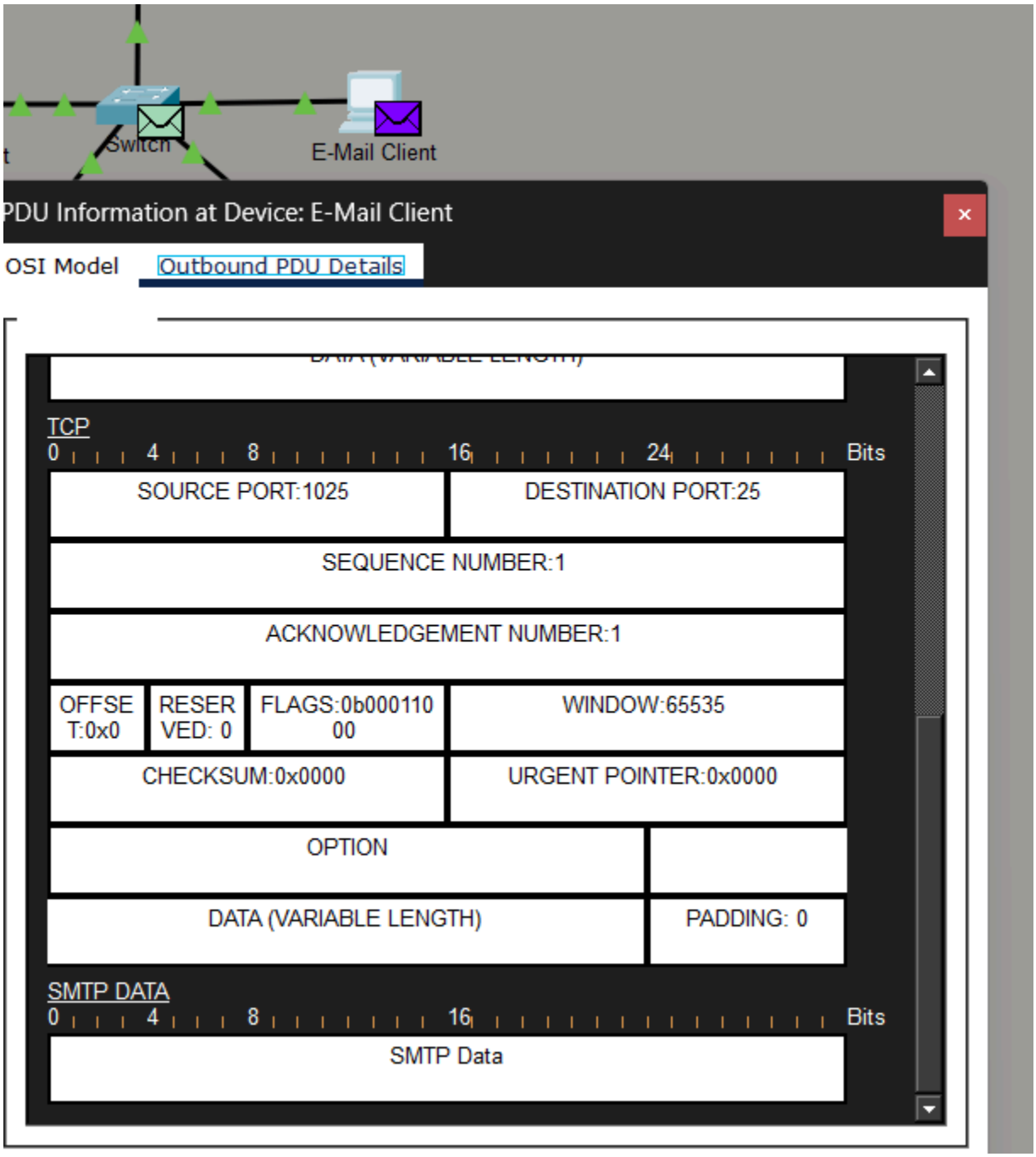
h.



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

- port and source port are the same as the first picture ,but ack and seq number are both 1 which are not the same as previous two

i.



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

- Ports: หมายเลขพอร์ตยังคงเป็น 1025 และ 25 เหมือนเดิม
- Numbers: ค่า SEQ NUM และ ACK NUM จะขยับเป็น 1 ทั้งคู่ ต่อเนื่องมาจากขั้นตอนการในข้อ h ก่อนหน้า

Associated Protocols:

- TCP Port 25: คือโปรโตคอล SMTP ใช้ส่งเมล
- TCP Port 110: คือโปรโตคอล POP3 ใช้รับเมล