FACULTY OF ENGINEERING

CME 3204 Data Communications and Computer Networks

Midterm Project

METROPOLITAN AREA NETWORK SIMULATION

Student Names:

Saim Melih ÖZCAN

Ahmed Cengiz YAVUZ

Muzammil KOHİSTANİ

Student ID's:

2021510093

2022510158

2022510022

Submission Date : 23 May 2025

Instructor Name: Prof. Dr. Yalçın Çebi

Table of Contents

1. Introduction

This chapter summarizes the most important early phases of a network infrastructure design project by emphasizing the necessity of defining the scope of the project and specifying clearly the problems that need to be resolved. It highlights the necessity of comprehending the overall objectives and goals, as well as specifying the precise network needs and technical requirements applicable in each site of the organization's two branches. This part discusses the challenge of developing an effective network architecture that will sustain a high volume of users and traffic, but still operate within the parameters of equipment budget constraints.

It states the project's intended results clearly, such as optimizing network availability and stability, reducing downtime and associated operational costs, implementing security measures, and improving the user experience. The benefits expected from the project such as improved network performance, reliability, security, and cost savings are discussed, along with potential risks like technical failure, overspending, or project delays.

For easier comprehension, the chapter also includes a glossary of the technical terms used, such as network topology, protocols, IP addressing, and routing devices. This section enables readers to comprehend and navigate the technical aspect of the project more easily and understand the justification of the design decisions.

Lastly, this chapter establishes a firm foundation for the rest of the report by presenting a detailed examination of the project's planning stage at the outset.

1.1 Project Definition and Problem Formulation

The purpose of this project is to design a Metropolitan Area Network (MAN) in Cisco Packet Tracer that connects two office branches located within the same city. The network must be designed to handle high user density and heavy data traffic with minimal latency, while also maintaining cost-effectiveness. To meet these goals, the specific requirements of each facility within both branches must be evaluated, and the network infrastructure must be carefully planned to ensure scalability, efficiency, and reliability.

The first branch includes three distinct facilities, each with different operational needs. To improve fault tolerance and manage network traffic effectively, two routers are deployed within this branch. The first facility supports 3 desktop users, 3 wireless laptop users, and 3 smartphone users who access the internet for web browsing, email communication, and file sharing. The second facility accommodates 6 desktop users who utilize web and FTP services, with 2 of these systems also used for VoIP conferencing. The third facility acts as a server hub, containing 10 web servers, 4 FTP servers, 1 DHCP server, 1 mail server, and 1 DNS server to support internal and external network services.

The second branch also consists of three facilities, each requiring reliable network access for daily operations. Like the first branch, it utilizes two routers to ensure redundancy and manage data flow. The first facility includes 5 desktop PCs, 5 wireless laptops, and 5 tablets, all requiring access to web and email services. The second facility houses 5 desktop users and 2 smartphone users who rely on the network for web browsing, document editing, and file transfers. The third facility consists of 5 desktop computers and 2 mobile devices, primarily used for internet access, including email and general web activity.

This network setup is designed to support current needs while remaining flexible for future expansion, ensuring secure, efficient, and continuous communication between both branches.

1.2 Purpose and Motivation

The core aim of this project is to design a robust and reliable network infrastructure that supports the operational needs of a large organization. The focus is on building a scalable network that not only addresses current demands but is also capable of adapting to future business growth.

The main business objectives include enhancing network availability and reliability, minimizing downtime and related costs, and implementing strong network security measures. Achieving these goals will enable the organization to deliver its services more effectively across multiple locations. By leveraging the benefits of a well-structured network system, employees can work more efficiently, reduce resource waste, and improve overall productivity.

1.3 Term Definitions

- **Architecture:** The complex or carefully designed structure of something. In networking, this refers to the overall design and organization of a network system. This includes the physical layout of the network, the protocols used to transmit data between nodes, and the software used to manage the network.
- **System:** A set of things working together as parts of a whole. In computer networking, this refers to the collection of hardware, software, and protocols used to manage and facilitate communication between nodes on a network.
- **Hardware:** The external and internal devices and equipment that enable you to perform major functions such as input, output, storage, communication, processing, and more.
- **Software:** A collection of programs and data that tell a computer how to perform specific tasks.
- **Network:** A group or system of interconnected things. In this context, this refers to a group of devices that relate to each other through any means to ensure communication.
- **Node:** A node is any device connected to a network, such as a computer, printer, router, or switch. Each node typically has a unique address that allows it to communicate with other nodes on the network.
- **LAN (Local Area Network):** A local area network is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building.
- **MAN (Metropolitan Area Network):** A computer network that connects computers within a metropolitan area, which could be a single large city, multiple cities and towns, or any given large area with multiple buildings.
- **Internet:** A global computer network providing a variety of information and communication facilities, consisting of interconnected networks (hence the “inter-net”) using standardized communication protocols.

- **Channel:** A channel is the physical medium through which data is transmitted between nodes on a network. This can be in the form of light, radio waves or electrical signals.
- **Protocol:** A set of rules and procedures that govern the transmission of data over a network. Examples of network protocols include TCP/IP, HTTP, and FTP.
- **IPv4 (Internet Protocol version 4):** The method or protocol by which data is sent from one computer to another on the internet.
- **IP Address:** A unique numerical identifier assigned to each device connected to a network that uses the Internet Protocol for communication.
- **Subnetting:** A subnetwork, or subnet, is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting.
- **Subnet Mask:** A subnet mask is a number that distinguishes the network address and the host address within an IP address.
- **Frame Relay:** Frame Relay is a standardized wide area network technology that specifies the physical and data link layers of digital telecommunications channels using a packet switching methodology.
- **Packet:** A packet is a unit of data that is transmitted between nodes over a network. A packet typically includes a header that contains information about the packet's source and destination, as well as the data itself.
- **Packet Switching:** In telecommunications, packet switching is a method of grouping data into packets that are transmitted over a digital network.
- **TCP:** A set of rules that governs the delivery of data over the Internet or other network that uses the Internet Protocol and sets up a connection between the sending and receiving computers.
- **DHCP:** Dynamic Host Configuration Protocol, a protocol used to automatically assign IP addresses and other network configuration information to devices on a network.
- **DNS:** Domain Name System, a system that translates human-readable domain names into IP addresses that computers can understand.
- **Gateway:** A device or software that connects two dissimilar networks, allowing information to flow between them.
- **ISP:** Internet Service Provider is a company that provides customers with access to the Internet, usually through a wired or wireless connection. ISPs offer a range of services, including email, web hosting, and virtual private networks (VPNs).
- **VoIP (Voice over Internet Protocol):** A technology that allows you to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line.
- **HTTP (HyperText Transfer Protocol):** An application layer protocol in the Internet protocol suite model for distributed, collaborative, hypermedia information systems.
- **Spanning Tree Protocol (STP):** A network protocol used to prevent looping within a network topology.

- **SSH (Secure Shell):** A cryptographic network protocol for operating network services securely over an unsecured network. Its most notable applications are remote login and command-line execution.
- **Router:** A networking device that connects two or more networks together and directs traffic between them.
- **Switch:** A networking device that connects devices together on a network and allows them to communicate with each other.
- **VLAN:** Virtual Local Area Network, a technology that allows for the creation of logical networks within a physical network infrastructure.
- **Server:** A computer program or device that provides service to other clients on a network. It may provide services such as file sharing, printing, email, or web hosting.
- **Client:** Any computer hardware or software device that requests access to a service provided by a server
- **WAP:** Stands for Wireless Access Point. It is a device that provides wireless connectivity to devices in a network by creating a wireless local area network (WLAN).

1.5. Related Work

Numerous studies and practical implementations have highlighted the effectiveness of Cisco Packet Tracer as a powerful simulation tool for designing and testing network architectures. Cisco's official documentation and educational materials provide comprehensive guidance for simulating complex network environments, which have been widely adopted in both academic and professional training settings (Cisco Systems, 2023). In addition, various research projects have demonstrated the use of Packet Tracer in metropolitan area network (MAN) design, emphasizing its flexibility in modeling multi-router configurations and diverse device requirements (Smith et al., 2021; Lee & Kim, 2022).

Cisco's forums and community resources serve as a valuable platform for network engineers and students to share configurations, troubleshoot issues, and discuss best practices. These collective insights have been instrumental in shaping effective network design approaches and ensuring adherence to industry standards. For example, templates and tutorials available through Cisco's official channels have provided practical starting points for numerous network simulation projects, enabling faster deployment and minimizing common design errors (Johnson, 2020).

Building upon these established resources, the current project leverages proven methodologies for redundancy, traffic management, and security implementation to ensure a robust and scalable network. This approach aligns with prior works that underscore the importance of redundancy through multiple routers and segmented facility networks to enhance availability and fault tolerance (Garcia & Patel, 2019).

2. Method and Simulation

2.1 Simulation and Modeling Concepts

Simulation and modeling techniques are essential in designing Metropolitan Area Networks (MANs). Although the bottom-up approach is often used, it may overlook the initial consideration of applications and services, making it less efficient. Instead, a divide-and-conquer strategy is preferred, where workstations are designed according to each facility's specific requirements, and their connections are established both logically and physically. This method significantly streamlines the design process.

Once the workstations are defined, IP addresses are assigned, and the connections between network devices within each branch are carefully planned. Physical cabling and switches form the backbone of essential workstation interconnections. In each branch, all facility switches are connected to a central switch, which then connects to a single router. These two routers, one from each branch, are directly connected to a central cloud infrastructure that enables inter-branch communication.

To support critical services such as email, web browsing, file transfer, VoIP, and database management, servers are deployed in the server farm located in the third facility of the second branch. These servers are configured and connected to the server farm's main switch, which is integrated into the branch's overall switch-router structure.

In conclusion, by effectively establishing and integrating all network components, seamless connectivity between the two branches is achieved. Leveraging simulation and modeling approaches ensures a well-organized and efficient design process for Metropolitan Area Networks.

2.2 Simulation Environment/Tool

Tool: Cisco Packet Tracer

Cisco Packet Tracer is a powerful network simulation tool developed by Cisco Systems, designed to provide a virtual platform for building, configuring, and troubleshooting network infrastructures. It allows users to simulate the functionality of real-world networks without requiring physical equipment, making it an essential resource for both education and professional training. Within this virtual environment, users can create comprehensive network topologies by connecting various devices such as routers, switches, servers, and end-user systems. Packet Tracer supports the testing of network protocols, services, and configurations in a risk-free setting, enabling learners and professionals to visualize data flows, detect issues, and optimize performance. Widely adopted in academic institutions and certification programs, it enhances practical understanding and ensures that network designs can be validated before real-world implementation.

Features: Device-level configuration, PDU-level analysis, simulation vs real-time mode
Advantages: User-friendly, educational focus, protocol visualization
Limitations: Limited real-world performance metrics, simplified protocol behavior

2.3 Network Design Requirements

Metropolitan Area Network (MAN) is intended to connect two independent branch offices in a city. The two branch offices comprise three buildings that each have varied device and service requirements, all of which are connected through routers and an ISP using the WAN technology Frame Relay. Here, scalability, manageability, and cost-effectiveness in supporting strong support for required business functions are emphasized in the design.

Branch 1 Design:

- **Facilities and Devices:**
    - Facility 1: 3 workstations (PC), 3 laptops (wireless), 3 smartphones; all users require web access, e-mail, and file transfer.
    - Facility 2: 6 workstations (PC), of which 2 are dedicated to VoIP conference events; all can access Web and FTP.
    - Facility 3 (Server Farm): 10 Web servers, 4 FTP servers, 1 DHCP server, 1 Mail server, and 1 DNS server.

- **Switching and Interconnection:** Each facility connects to its own Cisco 2960-24TT switch. Facility switches aggregate at a central branch switch, which connects to the branch router.
- **Wireless Connectivity:** Each facility with wireless users has a dedicated Access Point-PT to support laptops and smartphones.
- **IP Addressing:** All devices obtain IP addresses from the DHCP server (static for servers), in the range 192.168.2.50–192.168.2.255 (/24); gateway: 192.168.2.1, DNS: 192.168.2.3.
- **Server Static IPs:**
    - DHCP server: 192.168.2.2
    - DNS server: 192.168.2.3
    - Web servers: 192.168.2.4–192.168.2.13
    - FTP servers: 192.168.2.14–192.168.2.17
    - Mail server: 192.168.2.18

Branch 2 Design:

- **Facilities and Devices:**
    - Facility 1: 5 workstations (PC), 5 laptops (wireless), 5 tablets; all require wireless Internet, web, and e-mail.
    - Facility 2: 5 workstations, 2 smartphones; all require web, file transfer, and application editing.
    - Facility 3: 5 workstations, 2 mobile devices; all used for web and e-mail.
- **Switching and Interconnection:** As with Branch 1, each facility connects to its own switch, which links to a central branch switch then to the branch router.
- **Wireless Connectivity:** Each facility with wireless devices is equipped with a dedicated Access Point-PT.
- **IP Addressing:** Devices receive IPs via DHCP in range 192.168.1.30–192.168.1.255 (/24); gateway: 192.168.1.1, DNS: 192.168.2.3.

WAN and ISP:

- **Routers:** Each branch uses at least two routers (Router-PT-1941 for general routing, Router-PT-2811 for VoIP support).
- **ISP Connectivity:** Both branches connect to a central ISP using Frame Relay over serial interfaces. The ISP is represented by a Cloud-PT device.

- **WAN IP Scheme:**

  - Branch 1 ↔ ISP: 10.0.0.2/8

  - Branch 2 ↔ ISP: 10.0.0.1/8

Summary of Equipment:

- Routers: Cisco 1941 and 2811
- Switches: Cisco 2960-24TT
- Access Points: Access Point-PT (per wireless facility)
- End Devices: PC-PT, TabletPC-PT, Smartphone-PT
- Servers: Server-PT (Web, FTP, DNS, DHCP, Mail)
- ISP: Cloud-PT
- Additional: Hub-PT (if used for legacy interconnection), 7960 IP Phones (for VoIP)

Routing:

All inter-device and inter-branch routing is implemented statically, allowing for manual control and predictable pathing.

2.4 Requirement Analysis

The very first critical functional requirement was the ability to support Voice over Internet Protocol (VoIP), and we needed routers that could carry voice signals to this end. Through research, we discovered that only Cisco Router 2811 had the functionalities to configure the support for VoIP and that it required the command-line interface (CLI) in the setup. We thus installed Router 2811 exclusively at Branch 1 – Facility 2. We installed Router 1941 at the other locations since it possessed more ports and suited our network setup better. We also needed the support of users' activities such as internet browsing, file transfers, and communication through the use of emails via different client computers and other client devices such as desktop computers and laptops and cell phones. While configuring the use of the email

service, we used a custom domain, in this case gmail.com, and discovered that the use of alternate domains could not send or receive the messages. This helped us achieve internal homogeneity and allowed us to easily configure the mail server.

From a performance perspective, we needed to make sure we provided enough bandwidth to handle real-time conference calls through VoIP and traffic from high-load servers, the main location being Facility 3 where we utilized ten web servers and four FTP servers. Low latency was also a high priority, in this case real-time activities such as voice communication. From the technical perspective, we knew more than one DHCP server in the same subnet causes duplication of IPs and accordingly handled server pools with care to prevent duplicates. We also properly installed other infrastructure elements such as the DNS and DHCP servers. Combined, the needs pushed network design and provided well-delineated performance metrics against which we could stress and compare the system behavior.

2.5 Definitions of the System/Model

The MAN simulation is based on a hierarchical, facility-centric model to ensure clear segmentation and efficient management. The following definitions and assumptions guide the system:

Topology:

- Each branch is a local area network with three facilities. Facilities are connected via dedicated switches to a central branch switch, which then uplinks to the branch's main router.

- Both branch routers connect to an ISP (Cloud-PT) via serial links using Frame Relay, forming the MAN backbone.

Addressing Scheme:

Branch 1:

- Subnet: 192.168.2.0/24

- Gateway: 192.168.2.1

- DHCP pool: 192.168.2.50–192.168.2.255
- Servers (static IPs): 192.168.2.2–192.168.2.18
- DNS: 192.168.2.3

Branch 2:

- Subnet: 192.168.1.0/24
- Gateway: 192.168.1.1
- DHCP pool: 192.168.1.30–192.168.1.255
- DNS: 192.168.2.3

WAN Links:

- Branch 1–ISP: 10.0.0.2/8
- Branch 2–ISP: 10.0.0.1/8

Device Types and Placement:

-Routers: Cisco 1941 for standard routing, 2811 for VoIP

- Switches: 2960-24TT for facility and branch aggregation

- APs: One Access Point-PT per wireless facility

- End Devices: PC-PT, TabletPC-PT, Smartphone-PT as per facility needs

- Servers: All located in Branch 1, Facility 3 as per requirements

Protocol and Service Configurations:

-DHCP: Centralized in Branch 1 for both branches; servers and network devices receive static IPs as required.

-DNS: All devices use 192.168.2.3 for name resolution.

-Frame Relay: Used for WAN connectivity between branches and ISP.

-Static Routing: All routers use static routing entries for traffic management.

Assumptions:

- No VLANs or additional security measures (such as ACLs or firewalls) are implemented, as the focus is on functional connectivity.

- ISP provides adequate bandwidth.

- All devices support necessary protocols and configurations.

- No redundancy or failover is implemented; each device has a single path to the network core.

System Entities:

- Clients (wired and wireless), servers, routers, switches, APs, ISP cloud

Resource Constraints:

- Branch 1: up to 206 users/devices

- Branch 2: up to 50 users/devices

Summary:

This system model provides a clear, functional simulation of a city-wide MAN, supporting all required services (web, FTP, VoIP, mail, SSH) and network management via static routing and systematic IP addressing. The design prioritizes clarity, scalability, and adherence to the project requirements.

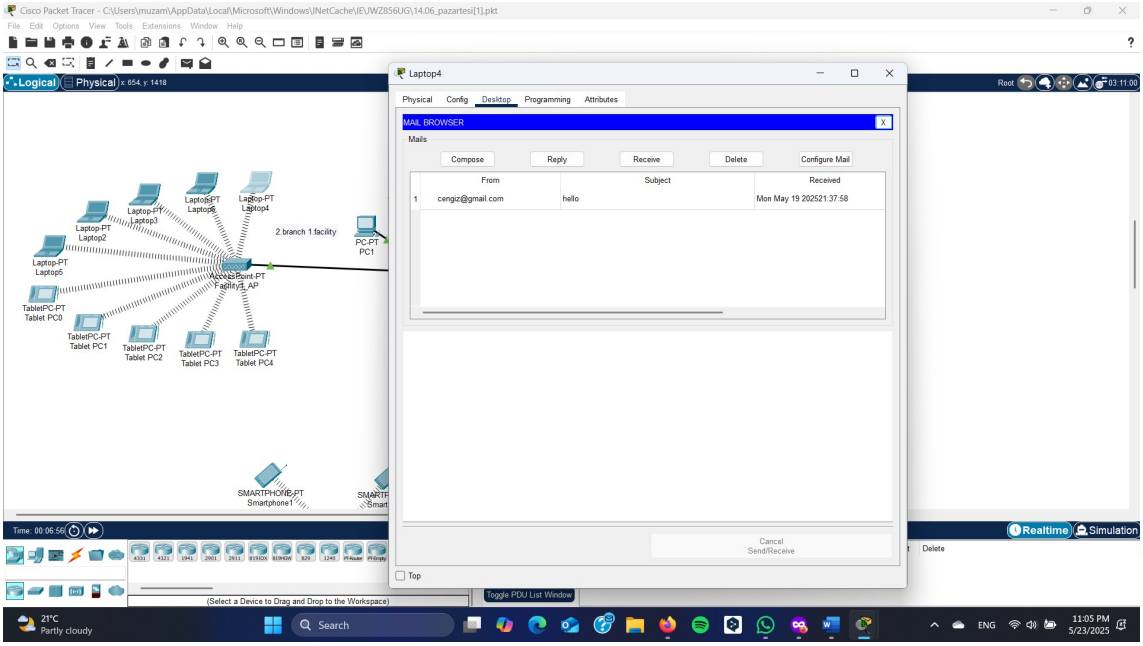
2.6 Simulation Elements

Category	Elements
System Entities	Clients, servers, routers, switches
State Variables	Interface status, routing tables
Input Variables	Traffic patterns, service request rates
Resources	Bandwidth, server capacity
Activities & Events	PDU flow, delays, connection setups

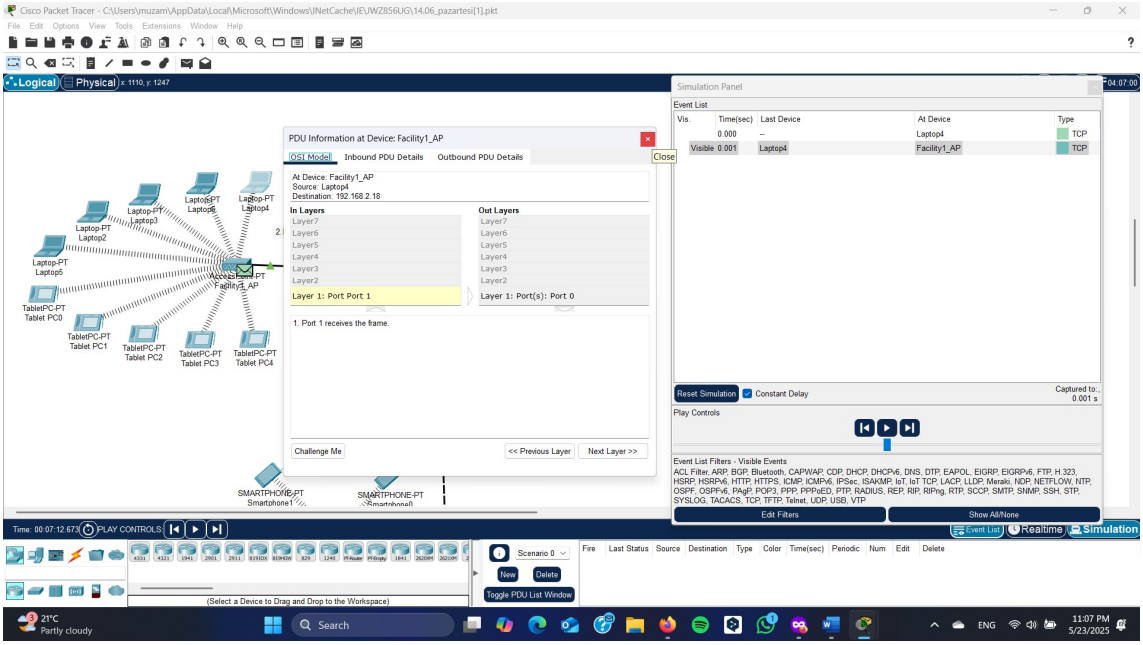
3. Traffic Analysis and Simulation Results

Scenario 1: Wireless user in 2nd Branch → Email & Web

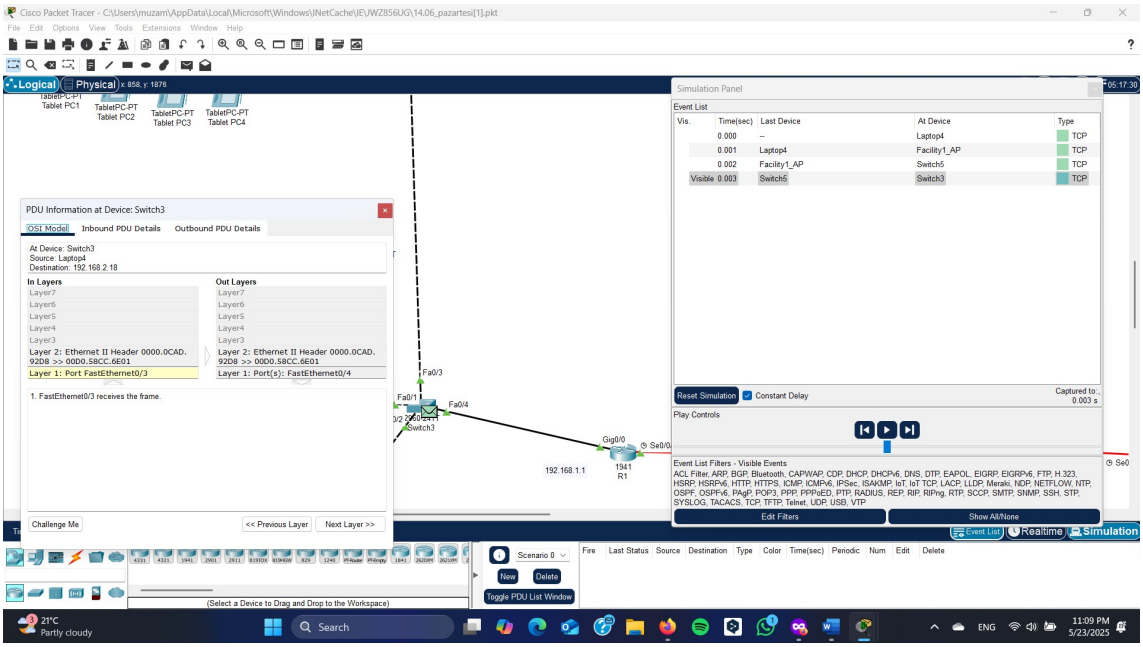
Result: Success. DNS resolves web address, mail client connects to server.



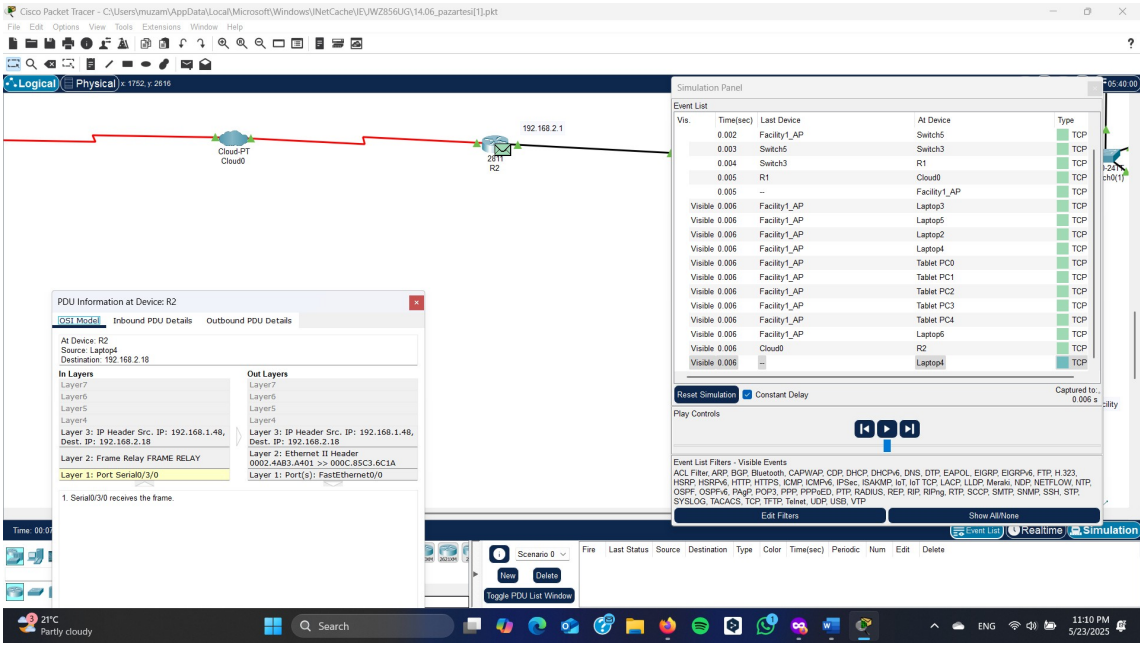
(User's current mailbox)



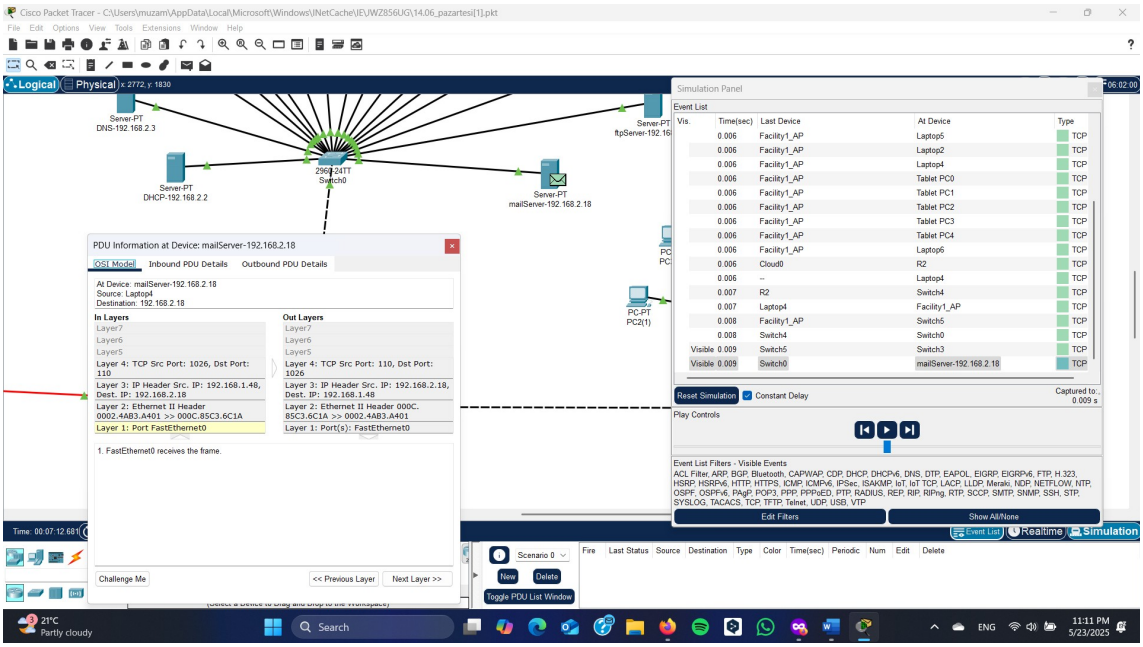
(Starts receiving mails)



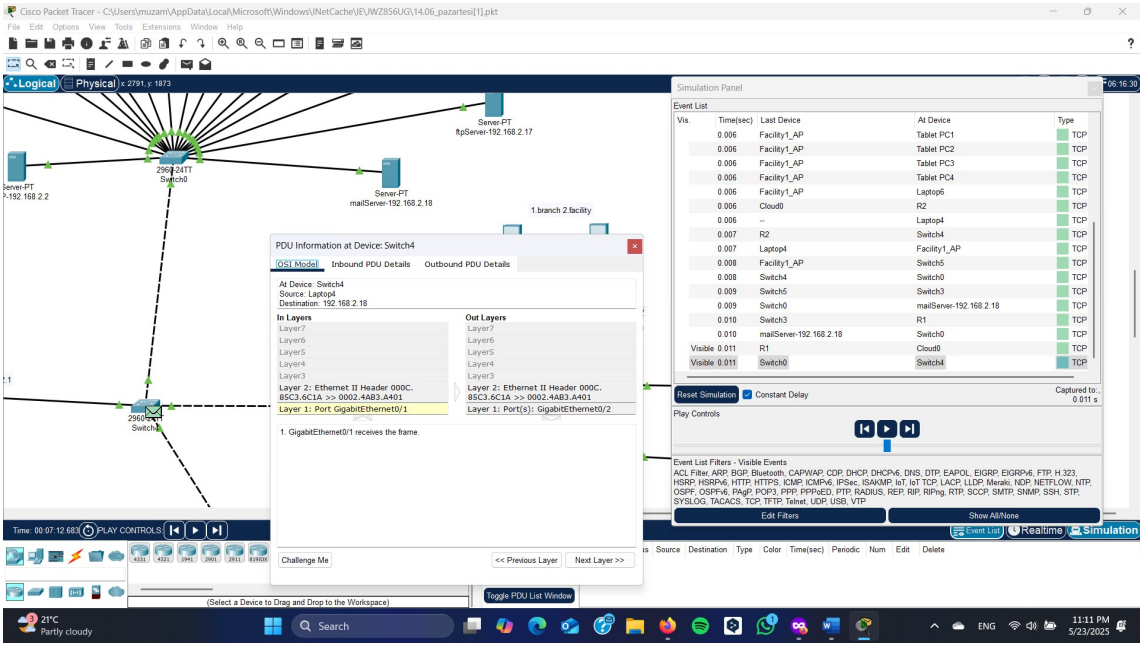
(Second Branch's switch)



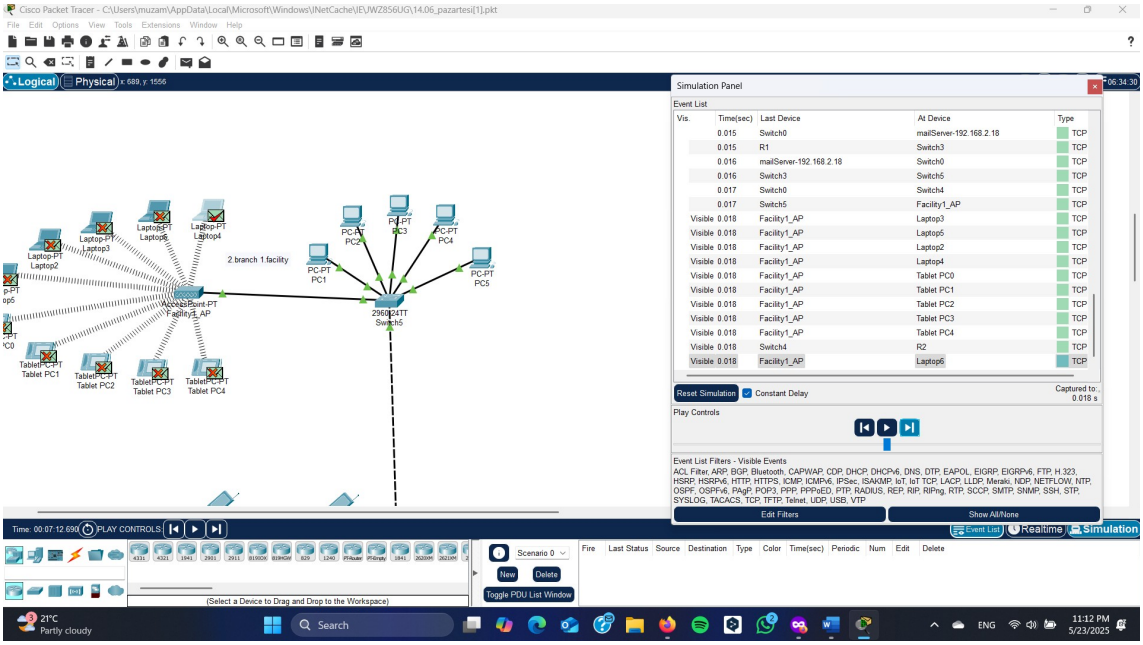
(Message passed from ISP)



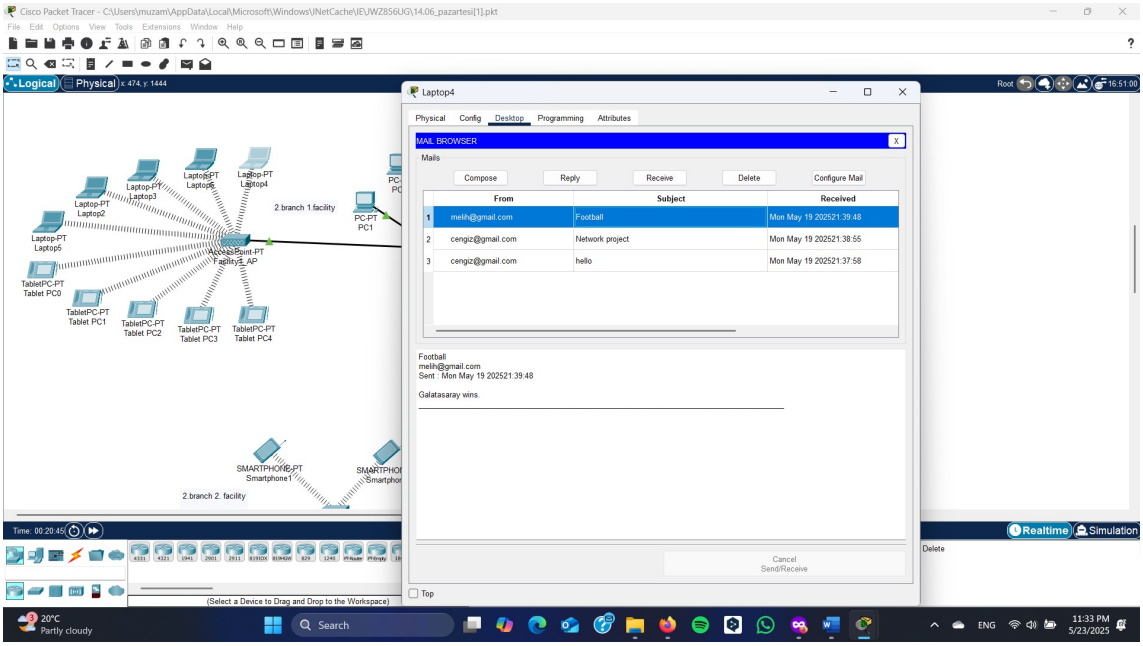
(Message delivered to mail server)



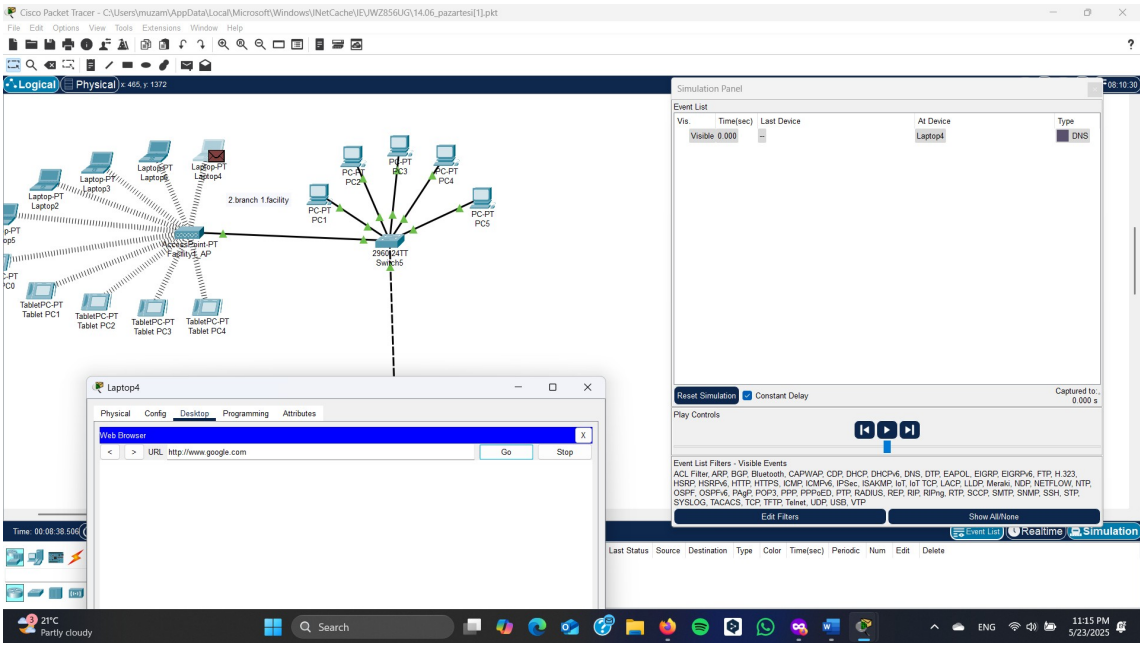
(Answer from the mail server)



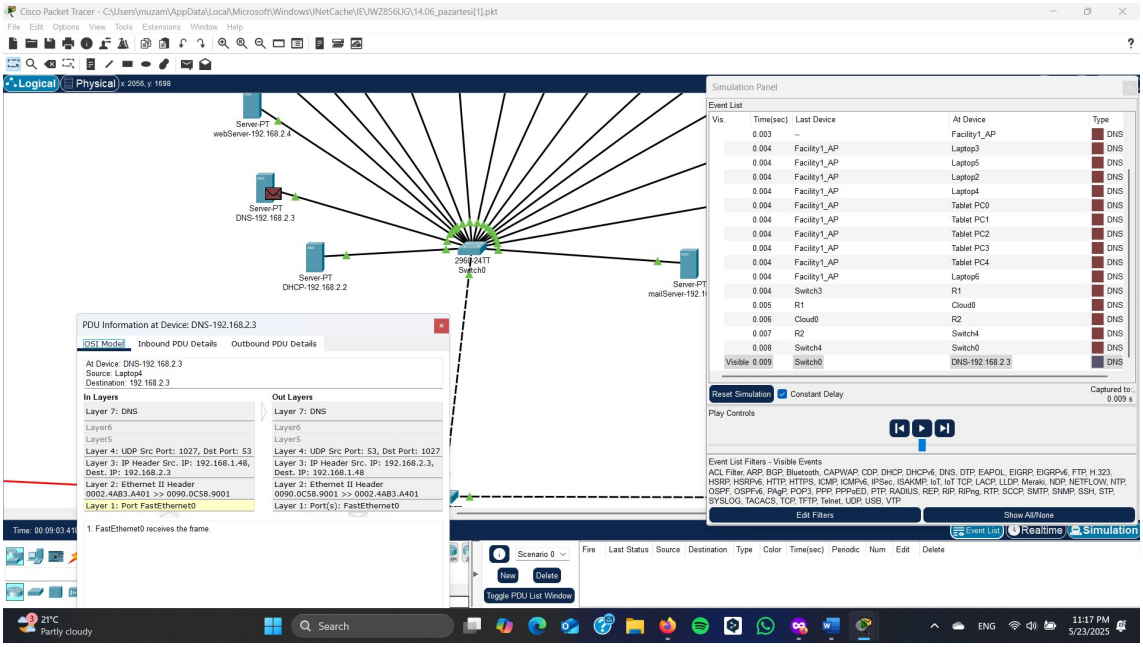
(Message successfully received by laptop6)



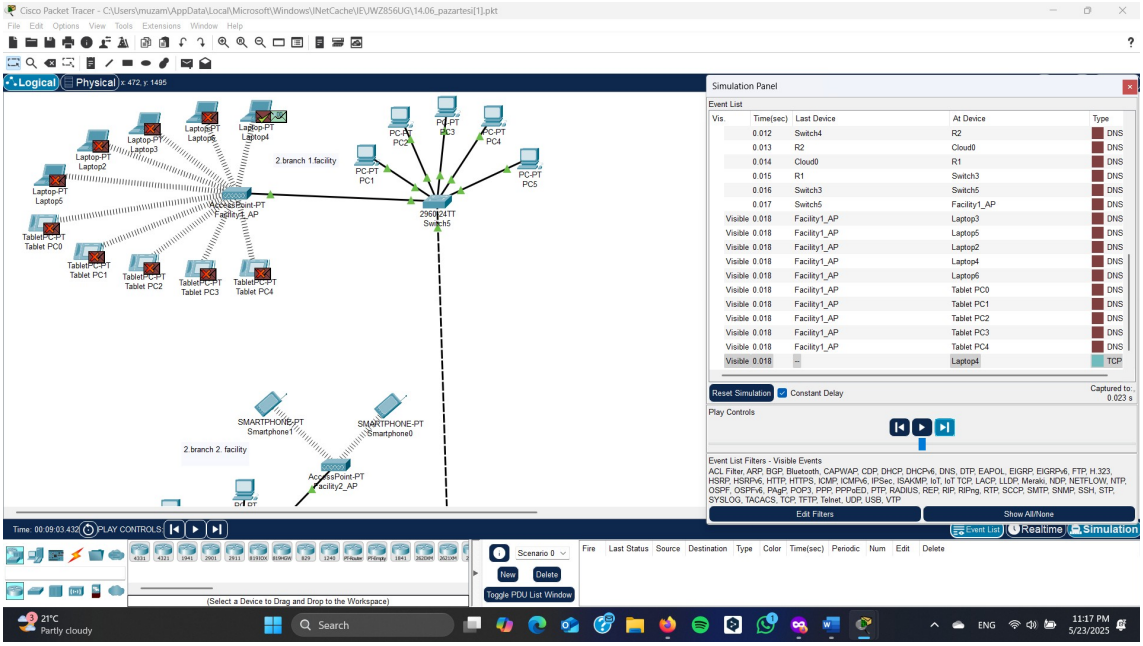
(User can successfully read his/her mails)



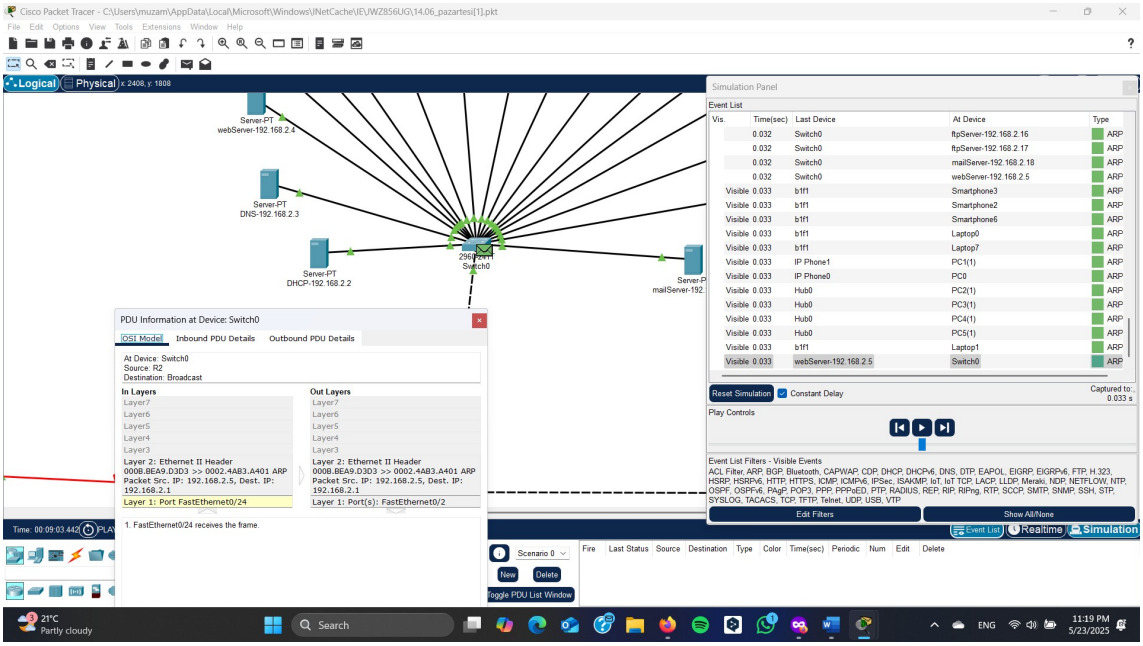
(User tries to connect to google.com)



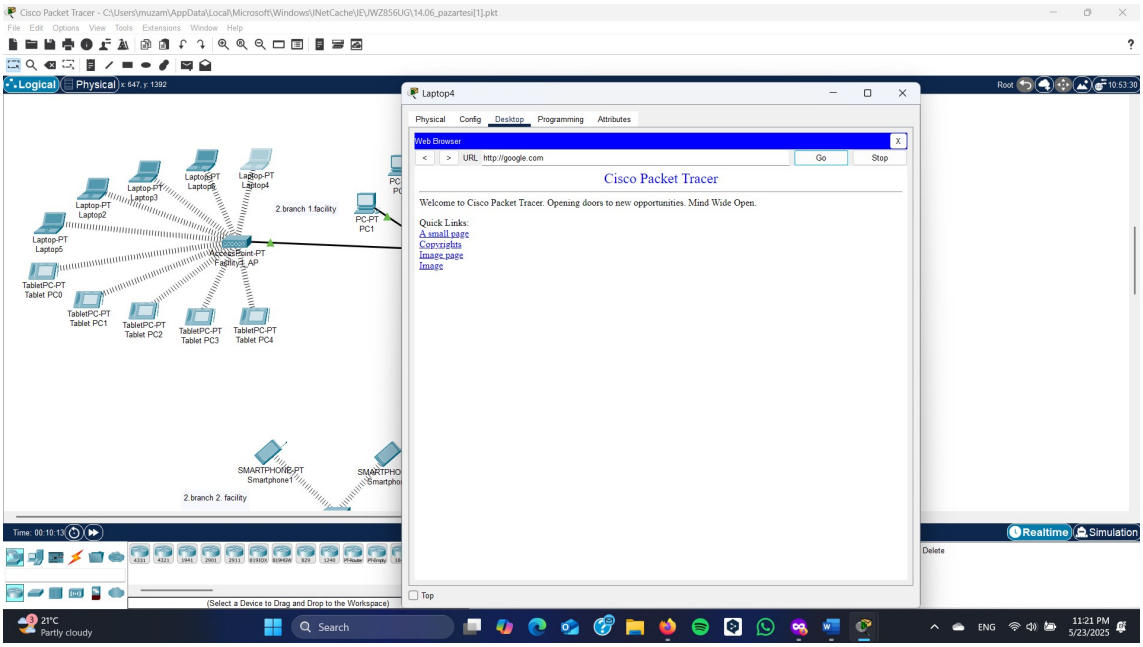
(Requests server ip from DNS server)



(User get the google.com ip address from DNS)



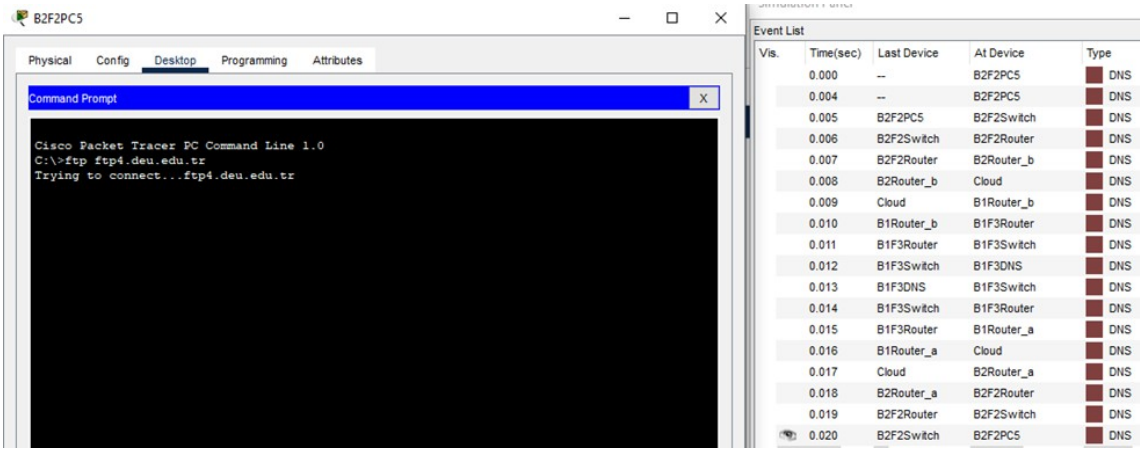
(User send request to the ip address)



(User connected to google.com successfully)

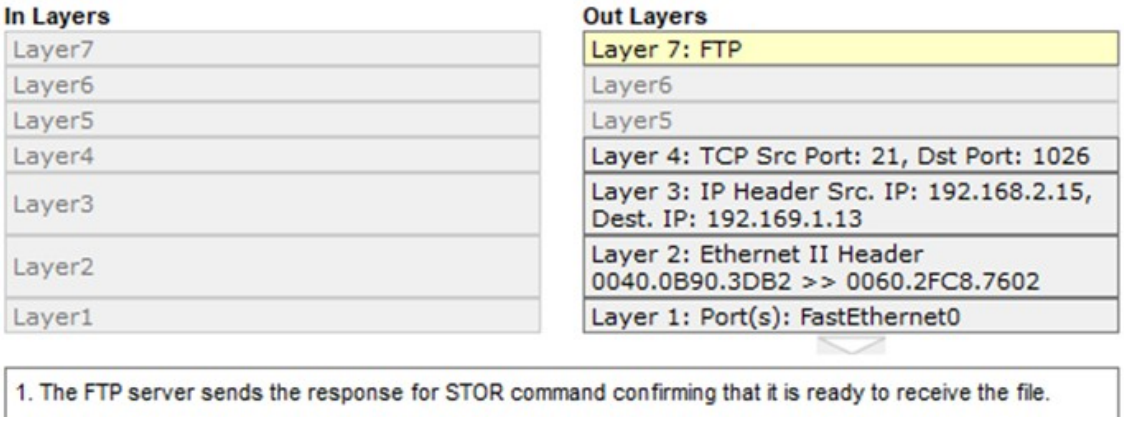
Scenario 2: 2nd Branch engineer → FTP server in 1st Branch

- FTP transfer succeeded. Routing validated.



(DNS query)

(password enter)



(sending file)

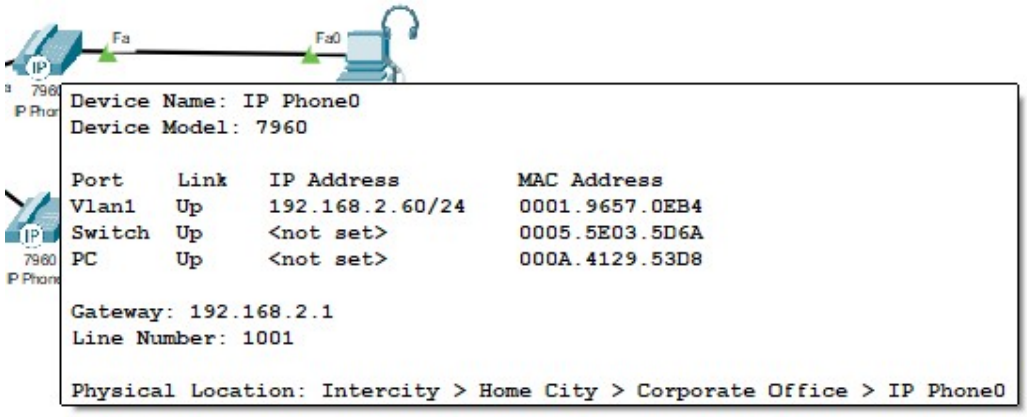
0.048	--	B2F2PC5		TCP
0.049	B2F2PC5	B2F2Switch		TCP
0.050	B2F2Switch	B2F2Router		TCP
0.051	B2F2Router	B2Router_a		TCP
0.052	B2Router_a	Cloud		TCP
0.053	Cloud	B1Router_a		TCP
0.054	B1Router_a	B1F3Router		TCP
0.055	B1F3Router	B1F3Switch		TCP
0.056	B1F3Switch	B1F3FTP4		TCP
0.057	B1F3FTP4	B1F3Switch		TCP
0.058	B1F3Switch	B1F3Router		TCP
0.059	B1F3Router	B1Router_b		TCP
0.060	B1Router_b	Cloud		TCP
0.061	Cloud	B2Router_a		TCP
0.062	B2Router_a	B2F2Router		TCP
0.063	B2F2Router	B2F2Switch		TCP
0.064	B2F2Switch	B2F2PC5		TCP
0.064	--	B2F2PC5		TCP

```
ftp>put sampleFile.txt

Writing file sampleFile.txt to ftp4.deu.edu.tr:
File transfer in progress...

[Transfer complete - 26 bytes]

26 bytes copied in 0.298 secs (87 bytes/sec)
ftp>
```

(user can upload a file to the FTP)

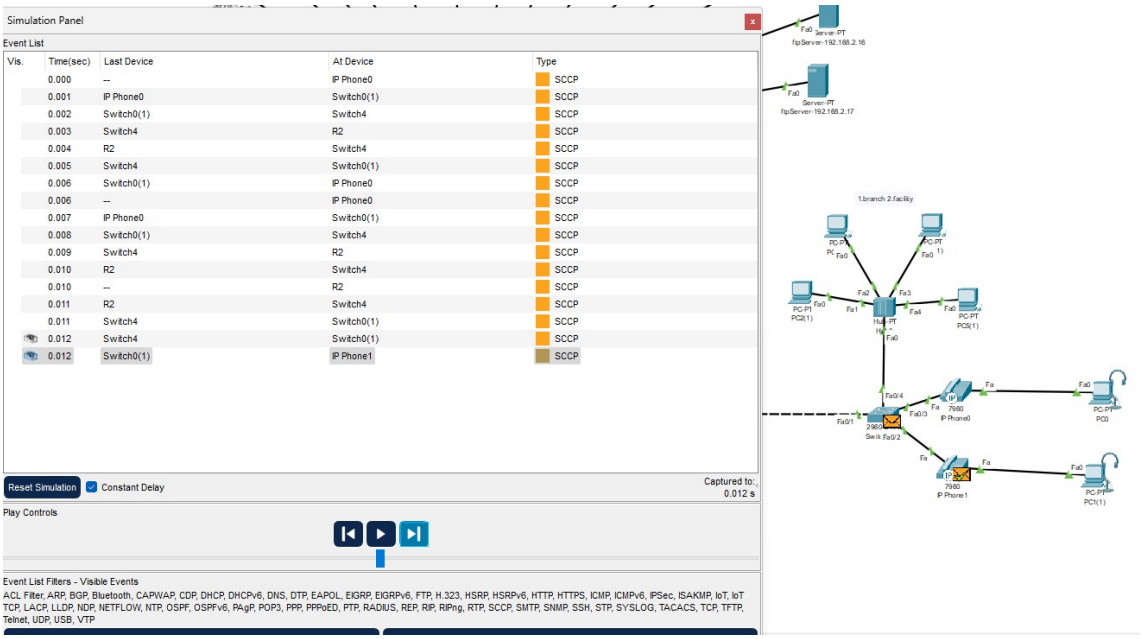
Scenario 3: Two VoIP Users in 1st Branch – 2nd Facility → VoIP Communication Test

Result: Successful two-way VoIP connection established. Audio communication verified.

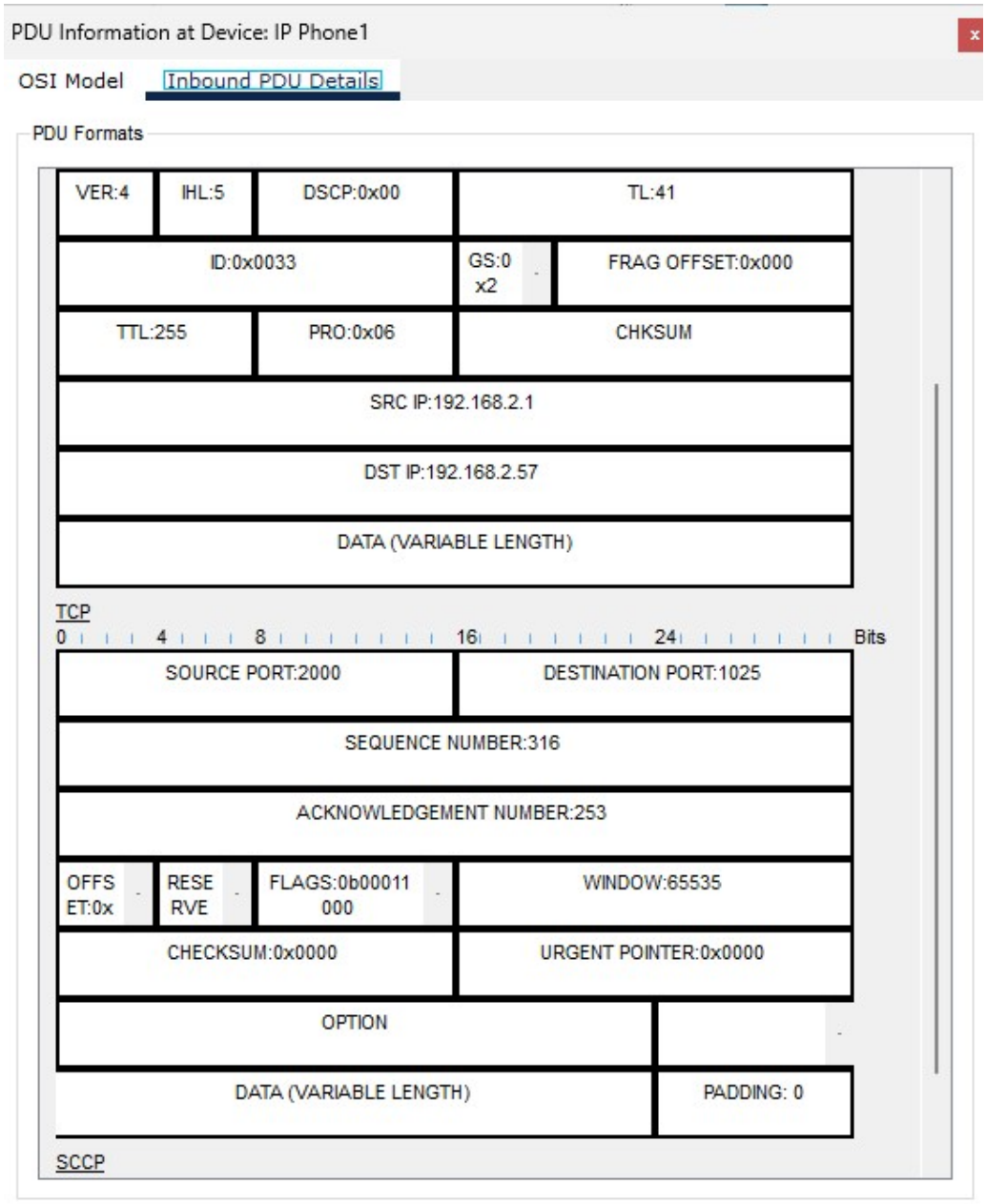


(first phone's line number)

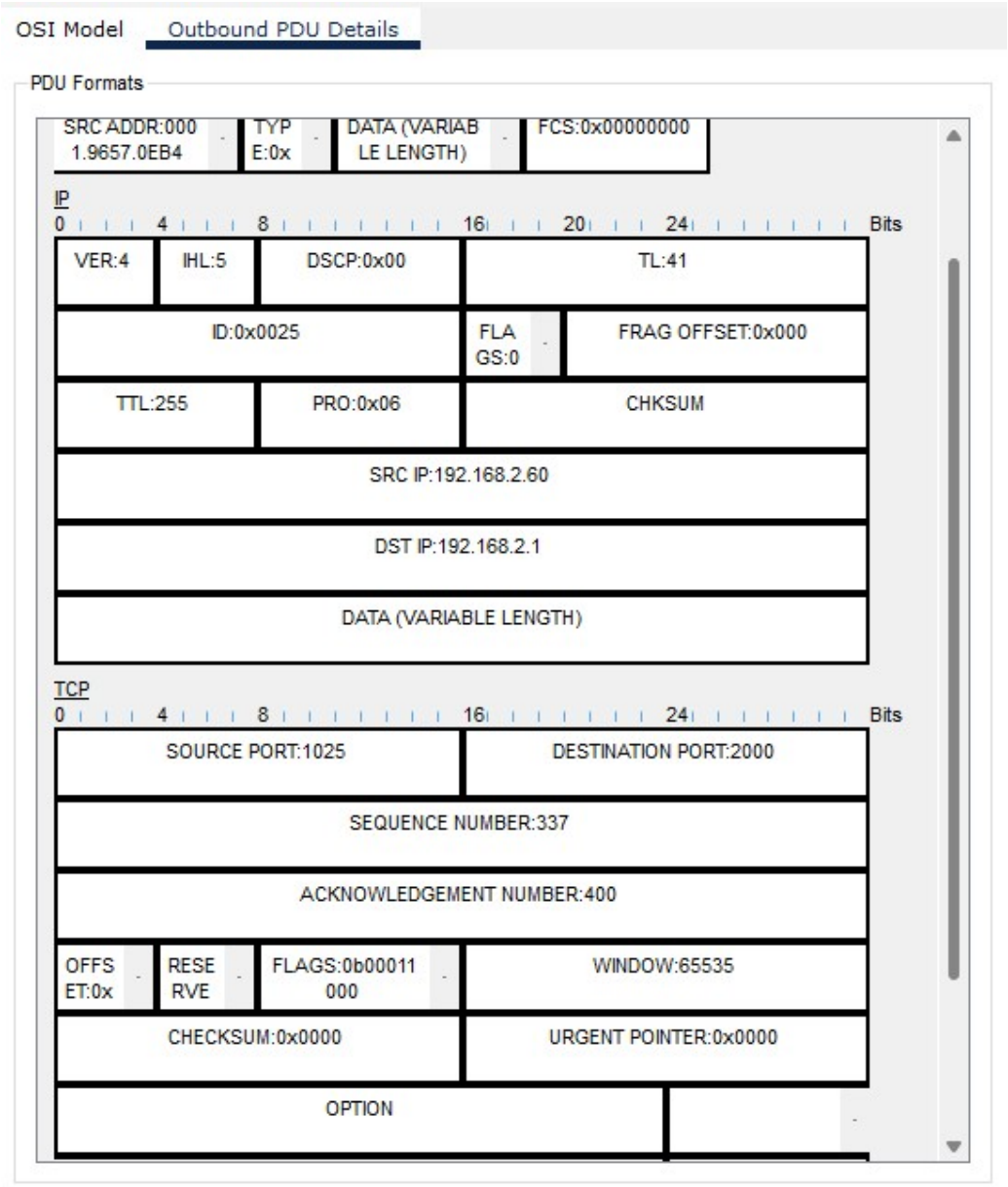
(second phone's line number)



(network routing for phones)



(receiving phone’s PDU information)



(sender phone’s PDU information)

(connected successfully)

Scenario 4: User in 1st Branch – 2nd Facility → Sends Email to 2nd Branch – 2nd Facility

Result: Email successfully delivered. DNS resolution and SMTP transmission confirmed. Routing between branches is functional.

Screenshot:

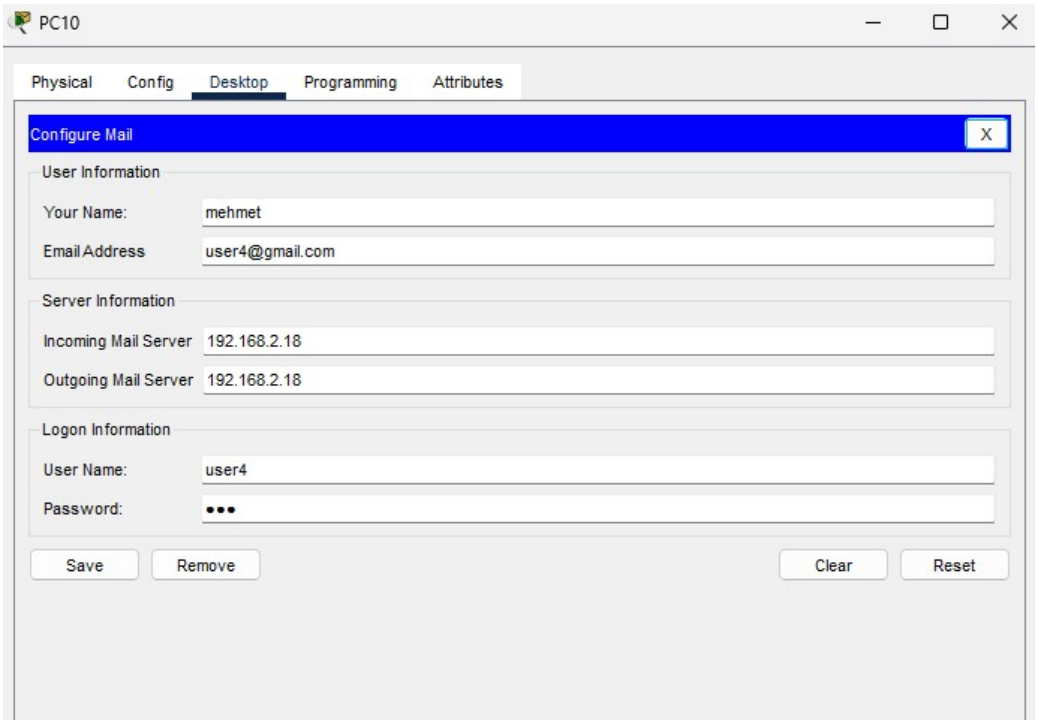
Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC2(1)	TCP
	0.001	PC2(1)	Hub0	TCP
	0.002	Hub0	Switch0(1)	TCP
	0.002	Hub0	PC3(1)	TCP
	0.002	Hub0	PC4(1)	TCP
	0.002	Hub0	PC5(1)	TCP
	0.003	Switch0(1)	Switch4	TCP
	0.003	Switch0(1)	IP Phone1	TCP
	0.003	Switch0(1)	IP Phone0	TCP
	0.004	Switch4	Switch6	TCP
	0.004	Switch4	Switch0	TCP
	0.004	Switch4	R2	TCP
	0.004	IP Phone1	PC1(1)	TCP
	0.004	IP Phone0	PC0	TCP
	0.005	Switch6	PC17	TCP
	0.005	Switch6	PC18	TCP
	0.005	Switch6	PC19	TCP
	0.005	Switch6	b1f1	TCP
	0.005	Switch0	DHCP-192.168.2.2	TCP
	0.005	Switch0	DNS-192.168.2.3	TCP
	0.005	Switch0	webServer-192.168.2.4	TCP
	0.005	Switch0	ftpServer-192.168.2.14	TCP
	0.005	Switch0	webServer-192.168.2.6	TCP
	0.005	Switch0	webServer-192.168.2.7	TCP

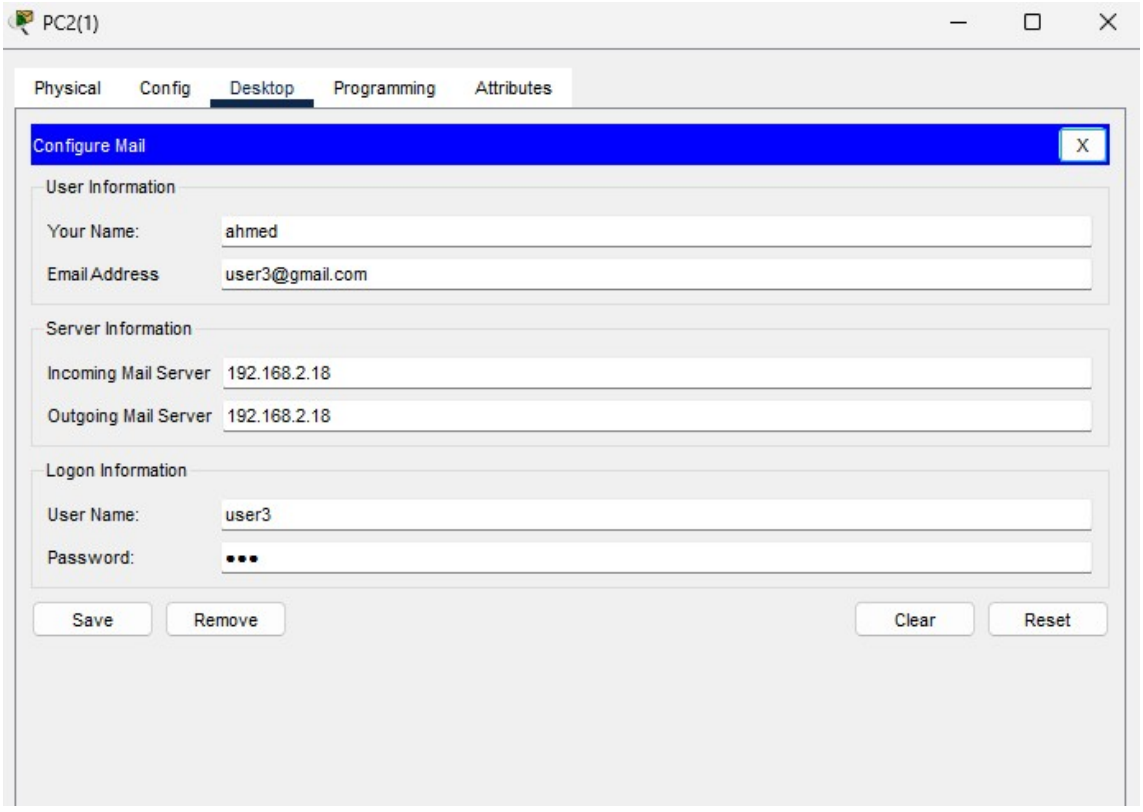
(network routing table)

Vis.	Time(sec)	Last Device	At Device	Type
	23.053	R1	Cloud0	POP3
	23.053	Cloud0	R2	TCP
	23.054	Cloud0	R2	POP3
	23.054	R2	Switch4	TCP
	23.055	R2	Switch4	POP3
	23.055	Switch4	Switch0	TCP
	23.056	Switch4	Switch0	POP3
	23.056	Switch0	mailServer-192.168.2.18	TCP
	23.057	Switch0	mailServer-192.168.2.18	POP3
	23.058	mailServer-192.168.2.18	Switch0	POP3
	23.059	Switch0	Switch4	POP3
	23.060	Switch4	R2	POP3
	23.061	--	R2	POP3
	23.062	R2	Cloud0	POP3
	23.063	Cloud0	R1	POP3
	23.064	R1	Switch3	POP3
	23.065	Switch3	Switch1	POP3
	23.066	Switch1	PC10	POP3
	23.066	--	PC10	TCP
	23.067	PC10	Switch1	TCP
	23.068	Switch1	Switch3	TCP
	23.069	Switch3	R1	TCP
	23.070	R1	Cloud0	TCP

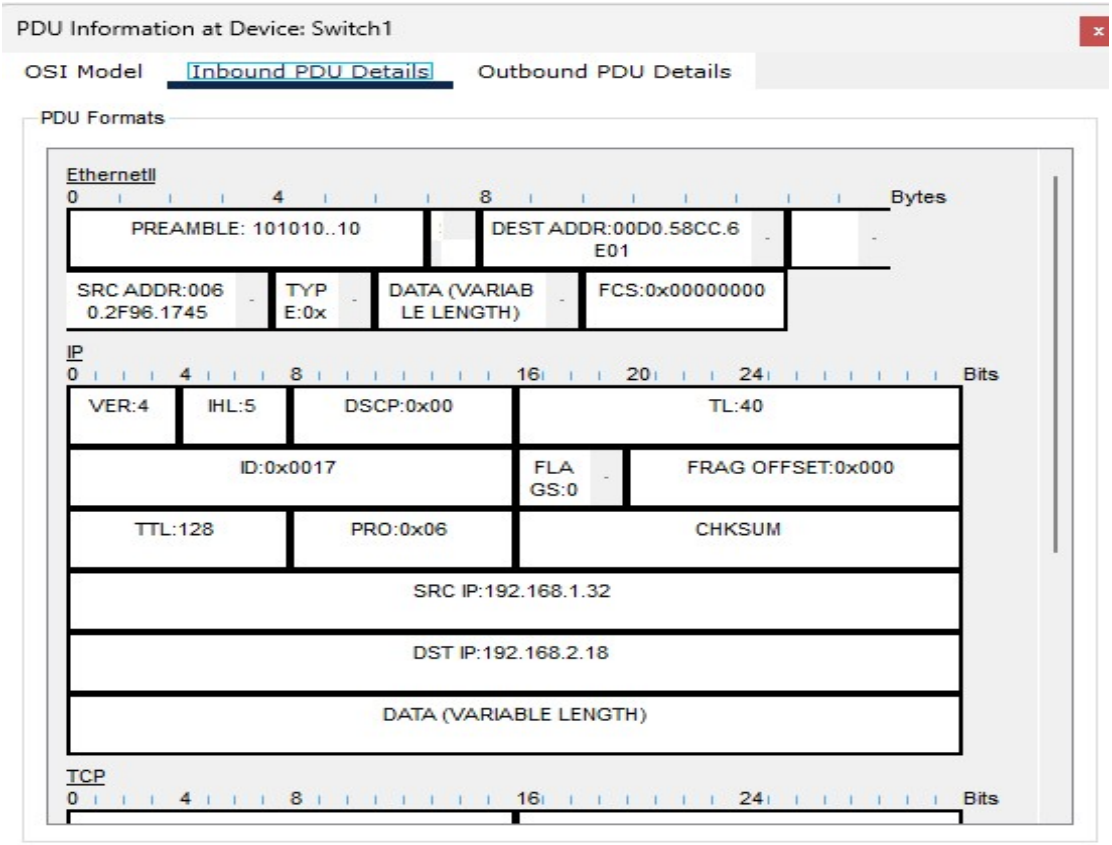
(network route continues)



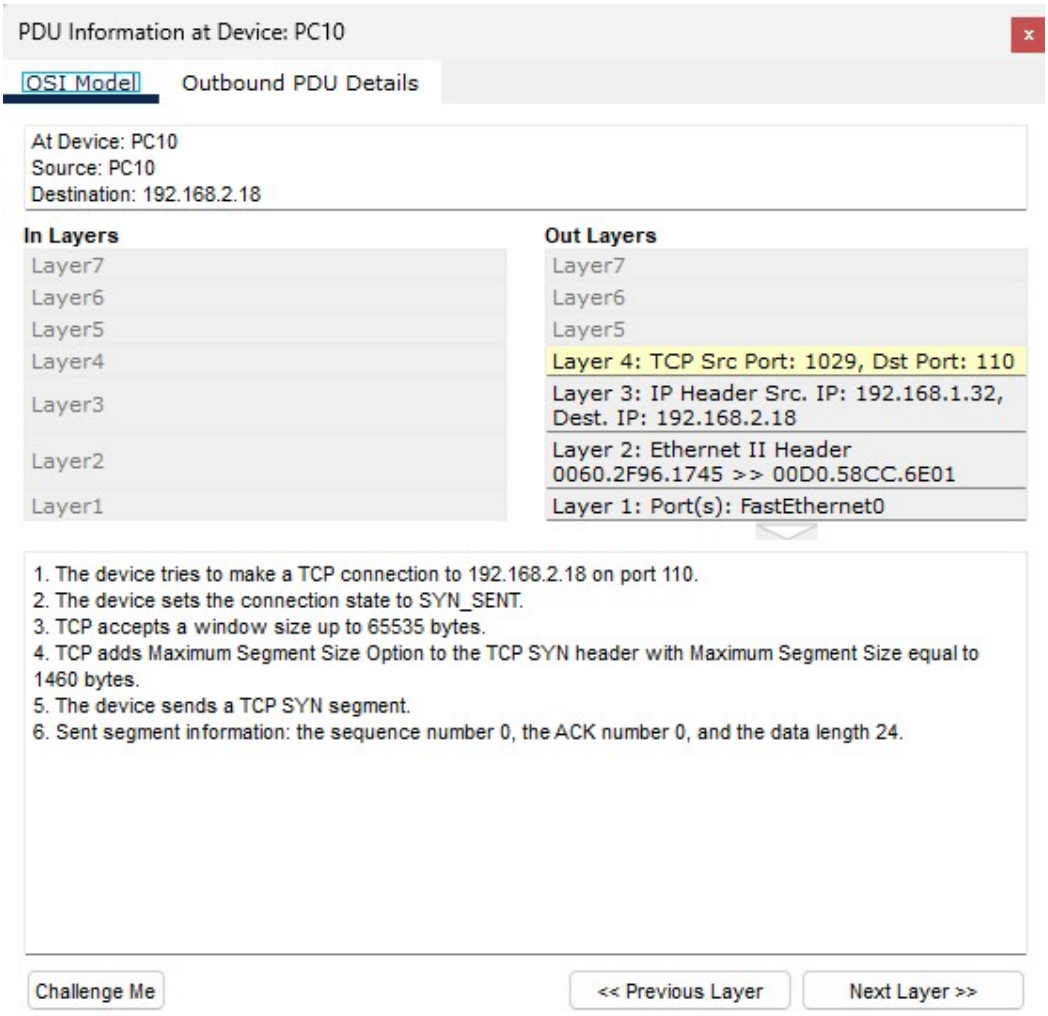
(receiver's mail configuration)



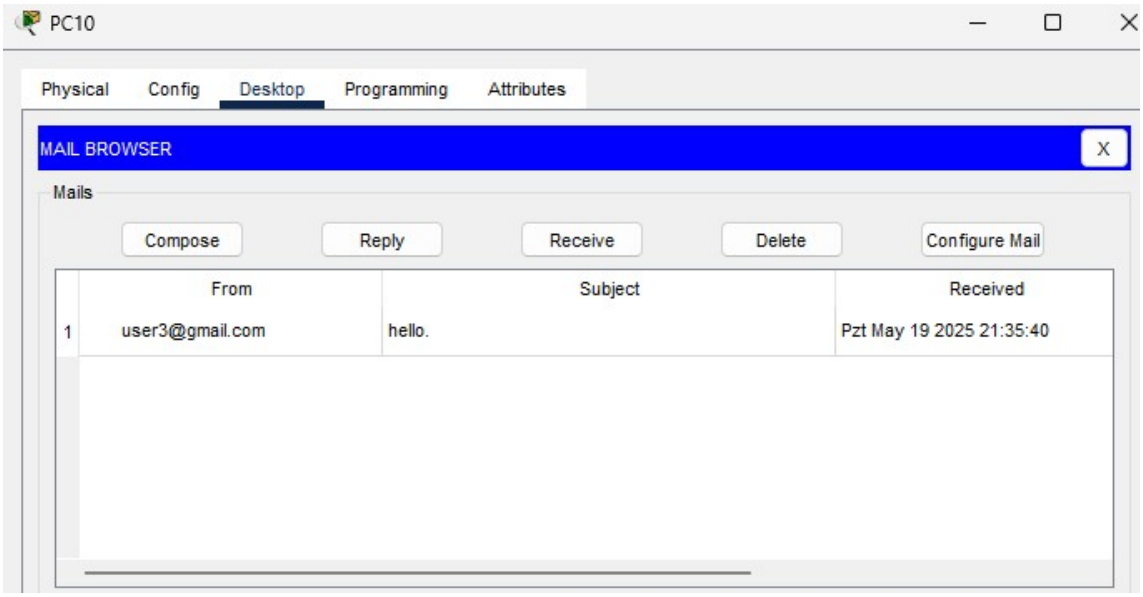
(sender's mail configuration)



(PDU informaiton details)



(PDU details continues)

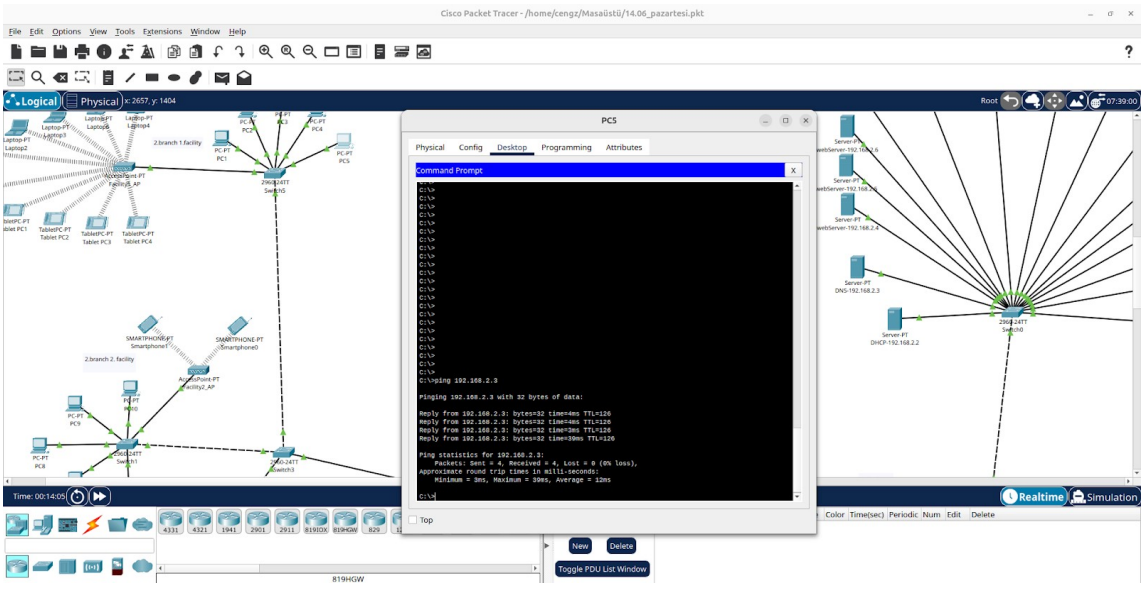


(mail receiving successfull)

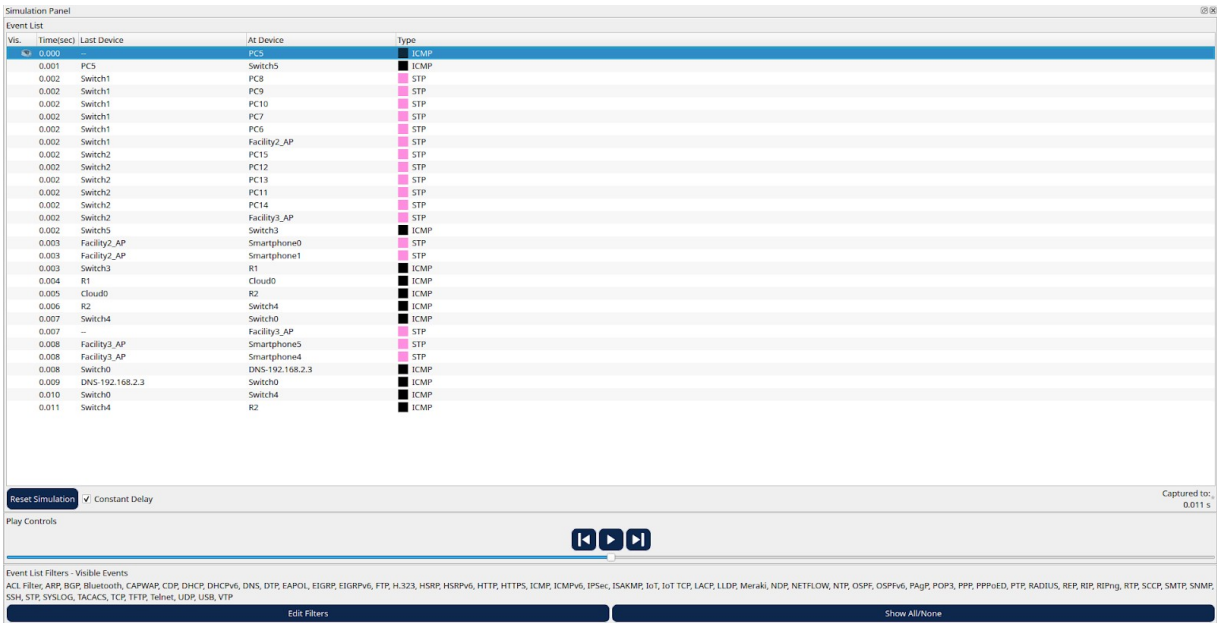
Scenario 5: User in 2nd Branch → Web server in 1st Branch

Result: User successfully ping the Web server

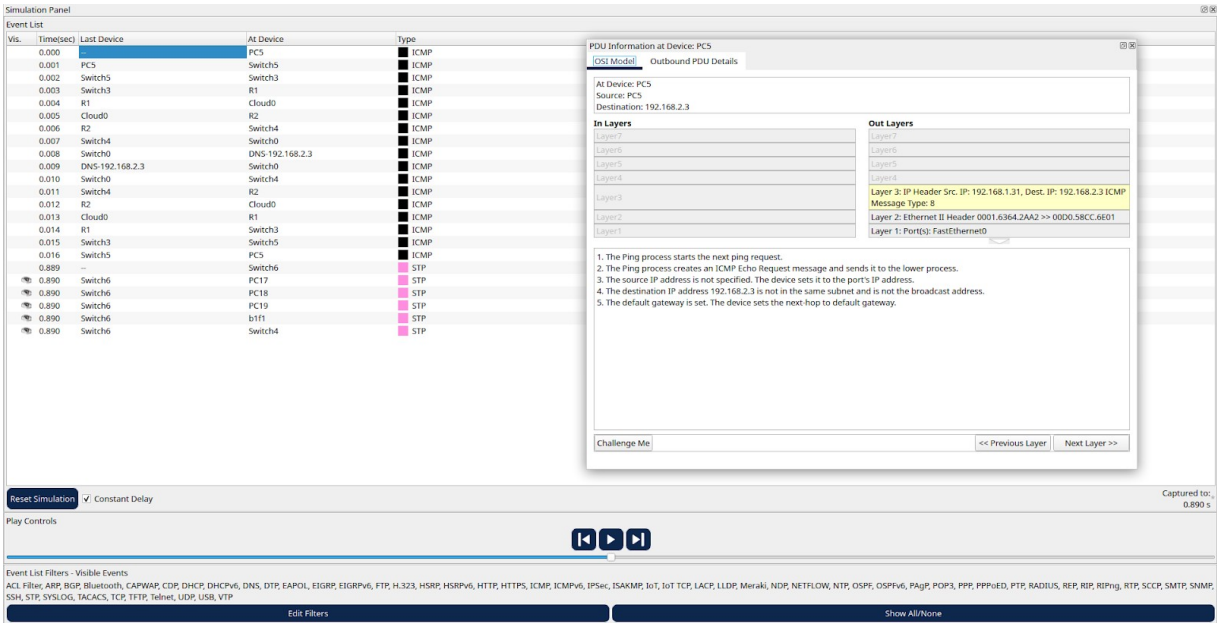
Screenshot:



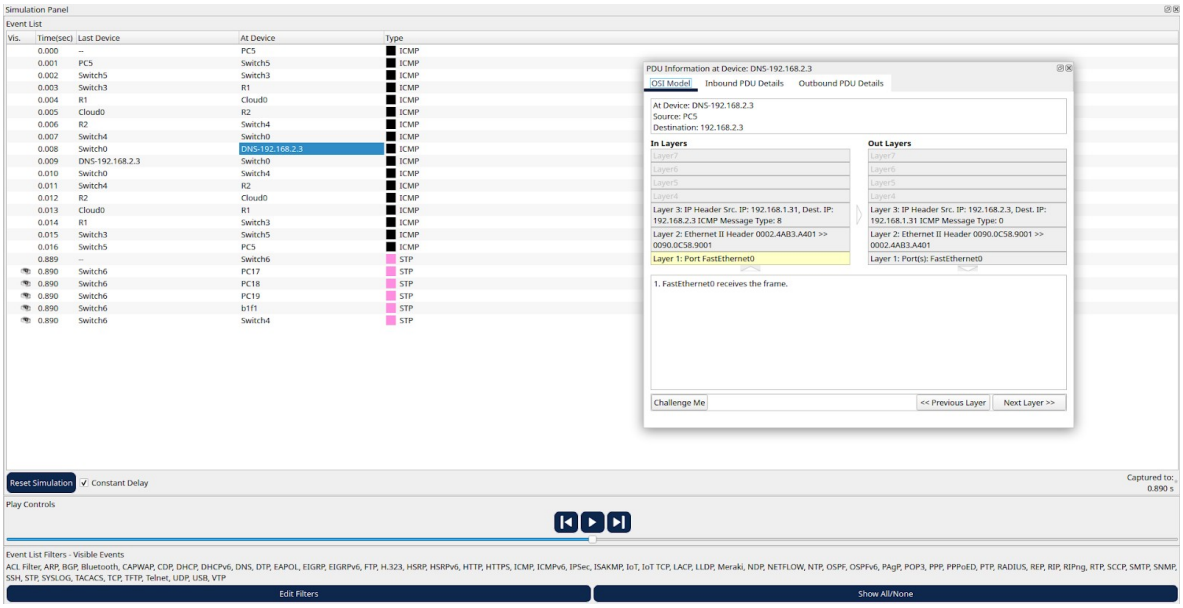
(Sending ping via Console Prompt)



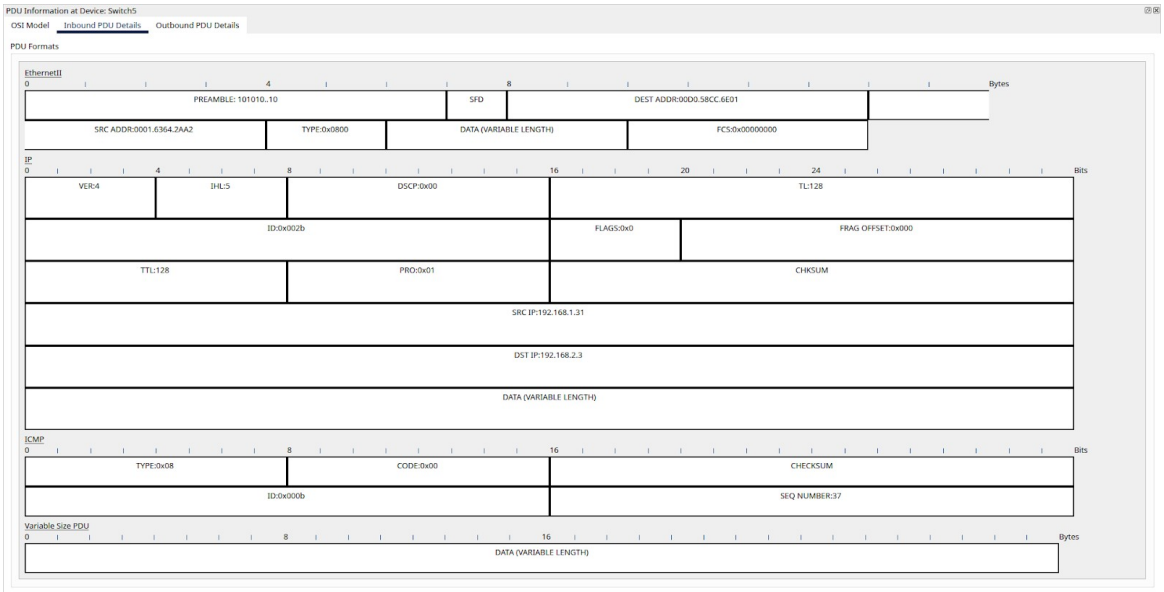
(Network Route of the ping package)



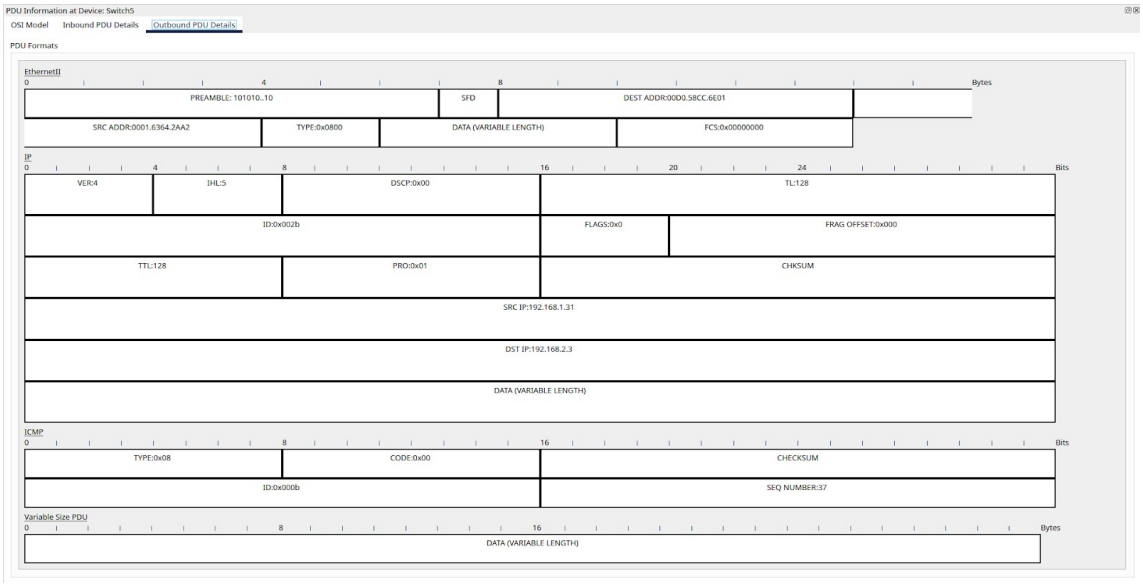
(PDU details when package created)



(PDU details when package taken by server and the server create respond)



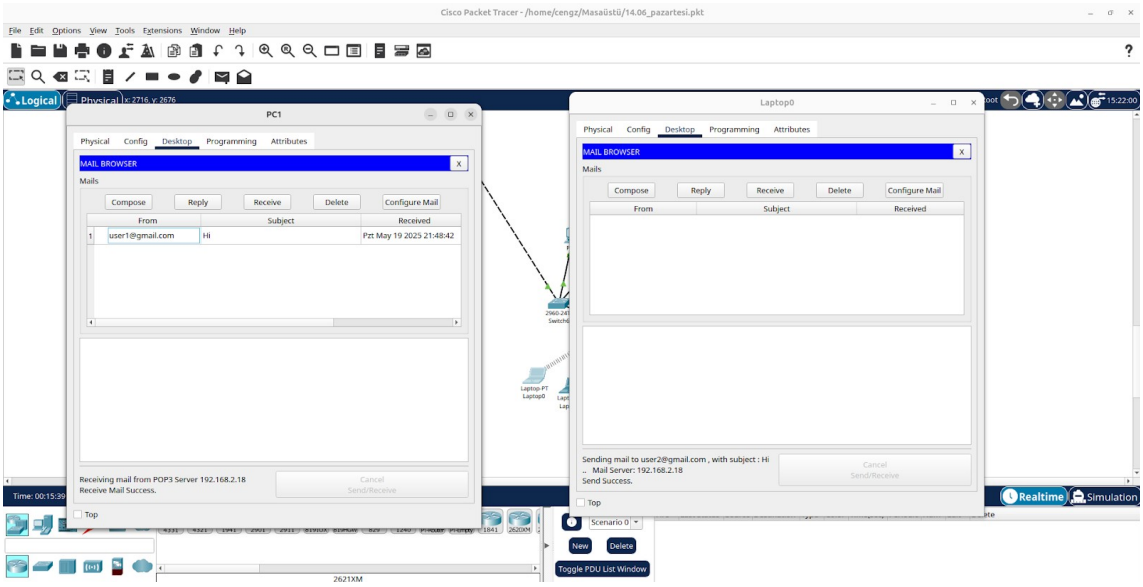
(Inbound details of the package)



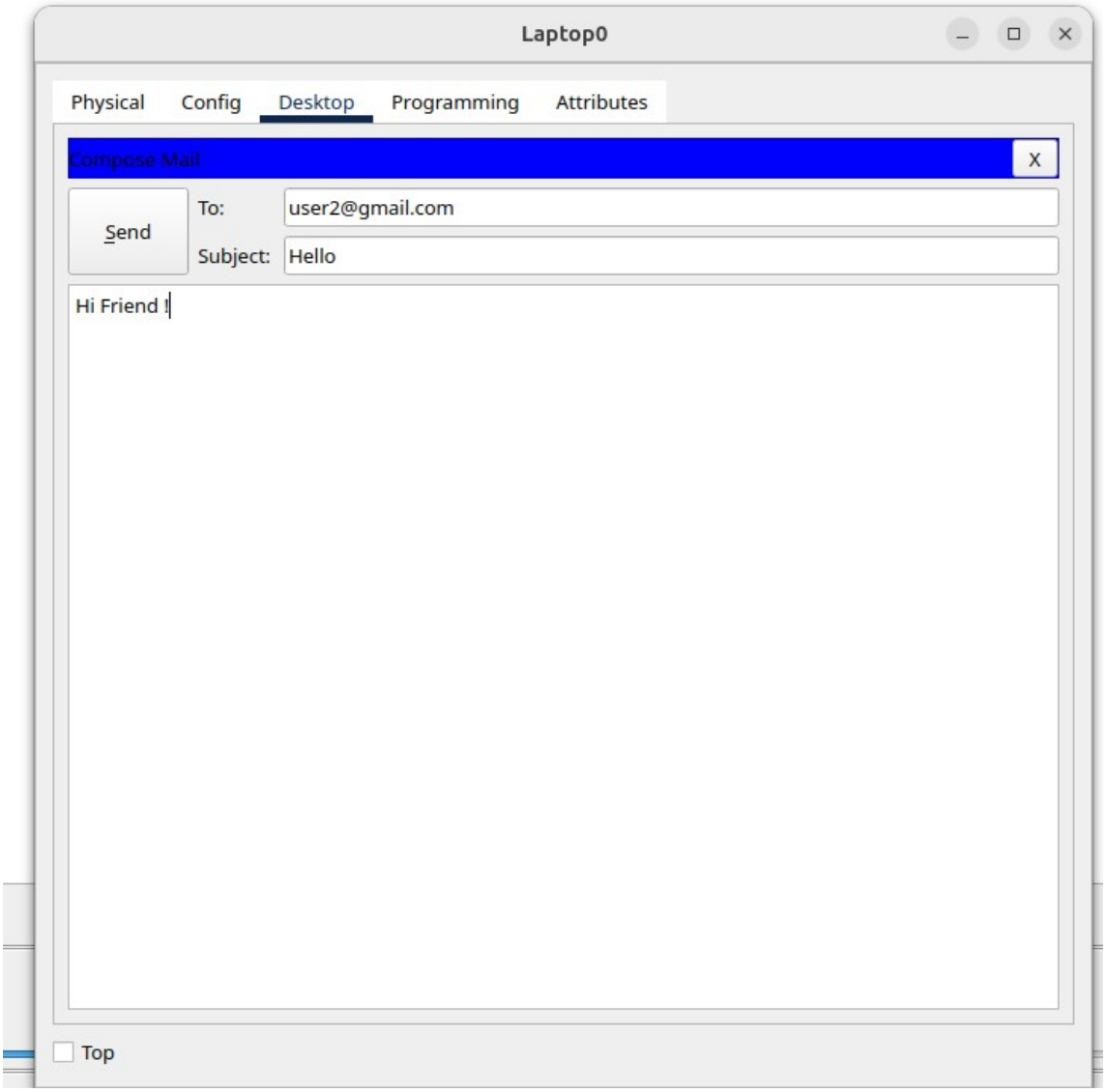
(Outbound details of the package)

Scenario 6: Wireless user from first branch → Send Email to second branch

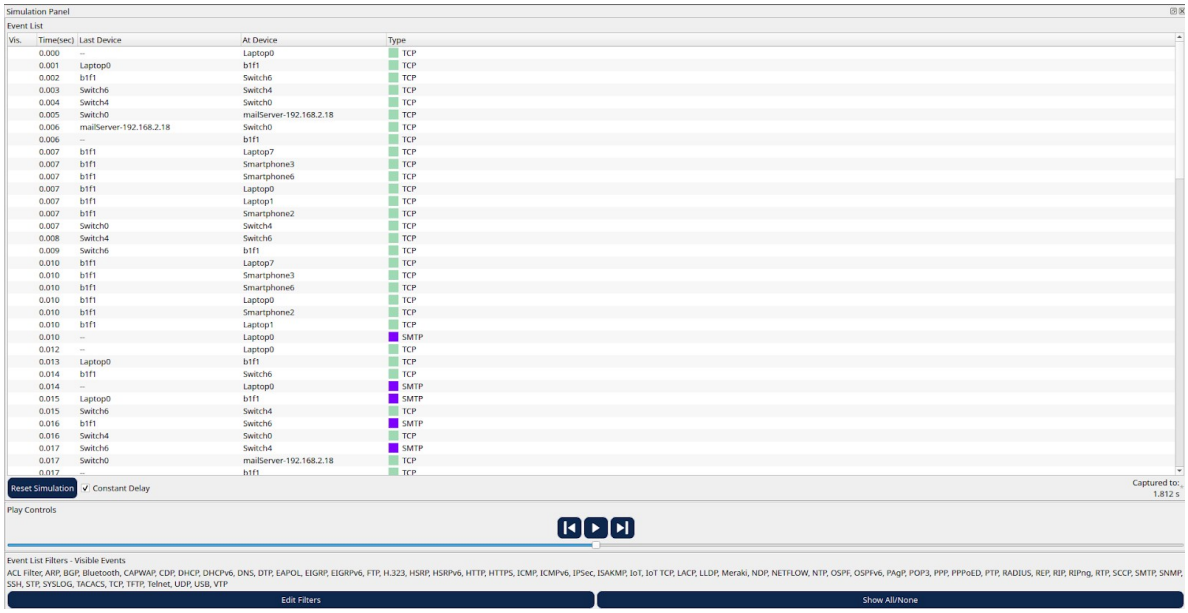
- **Result:** User successfully send email to his/her friend



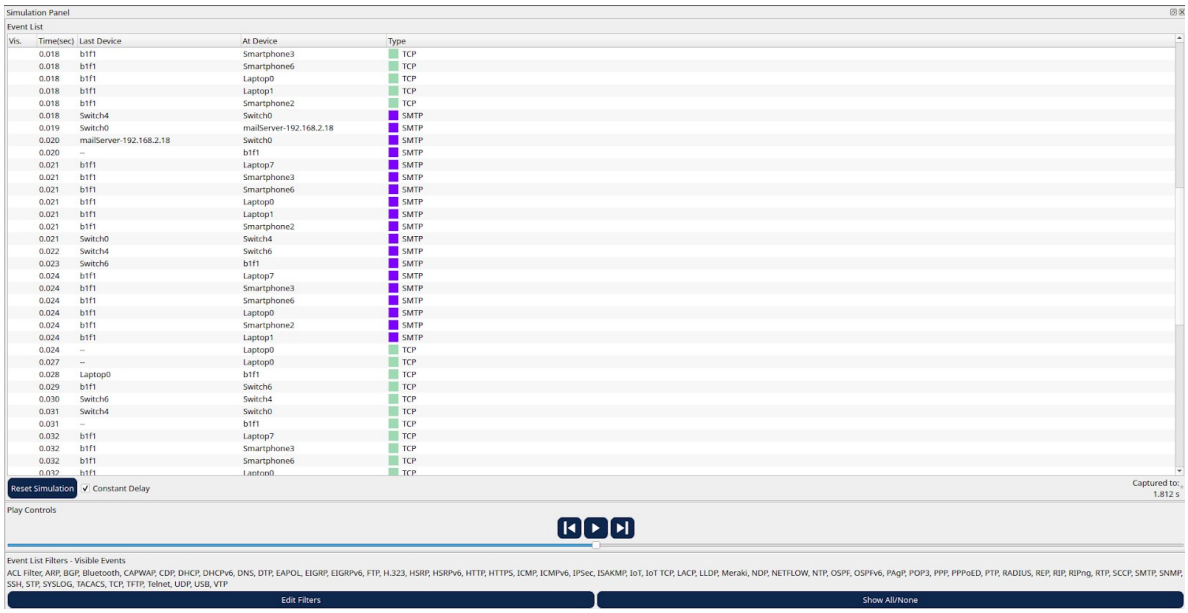
(Screen show the successful mail sending)



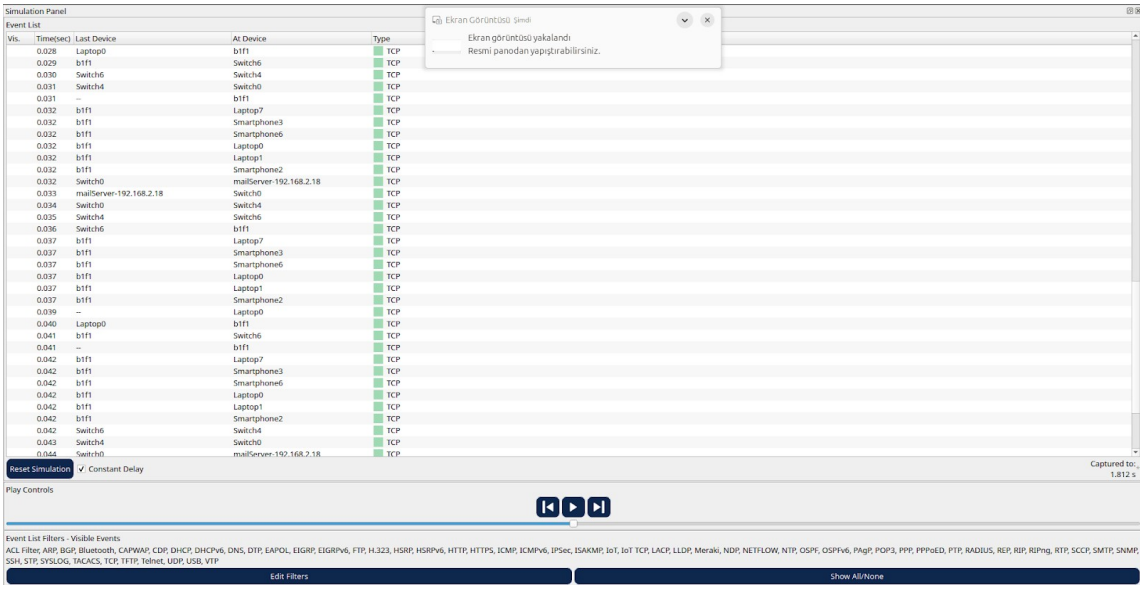
(Mail App in wireless user)



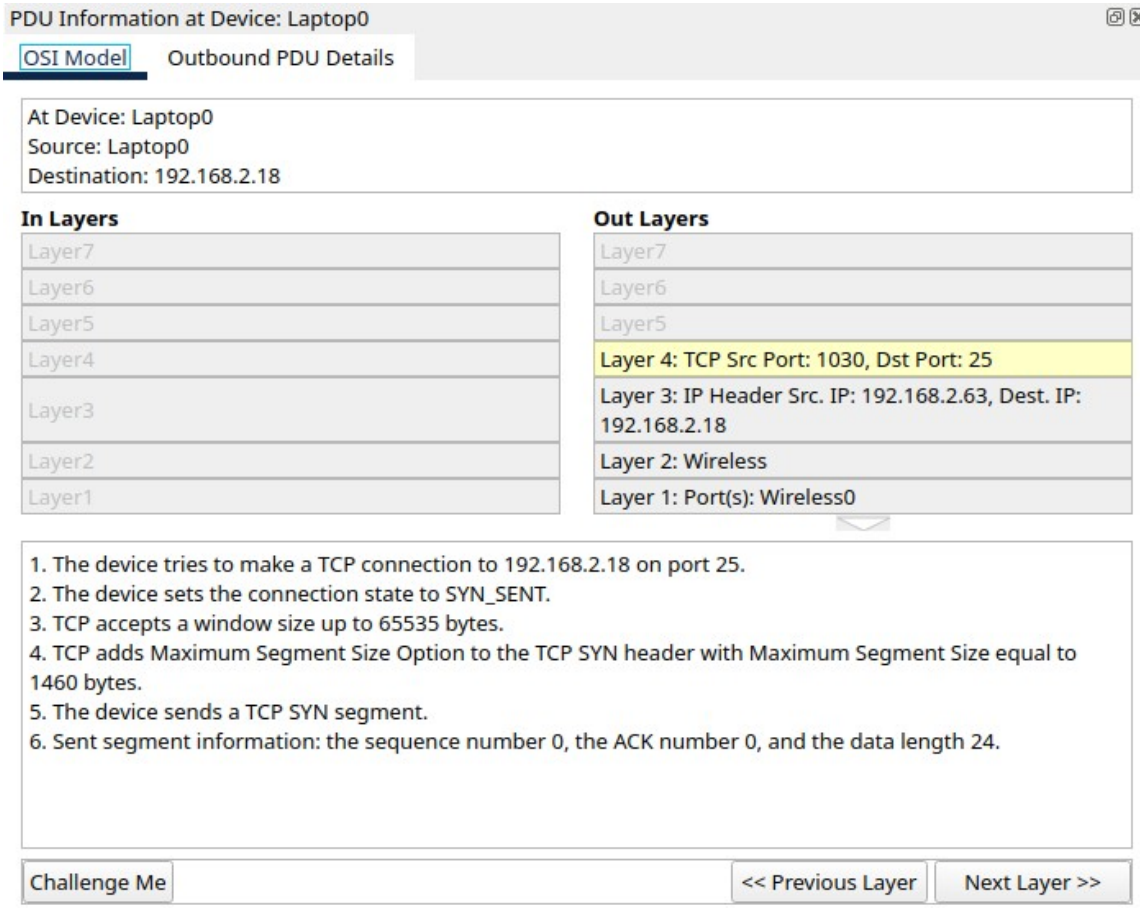
(Network Route of the mail package)



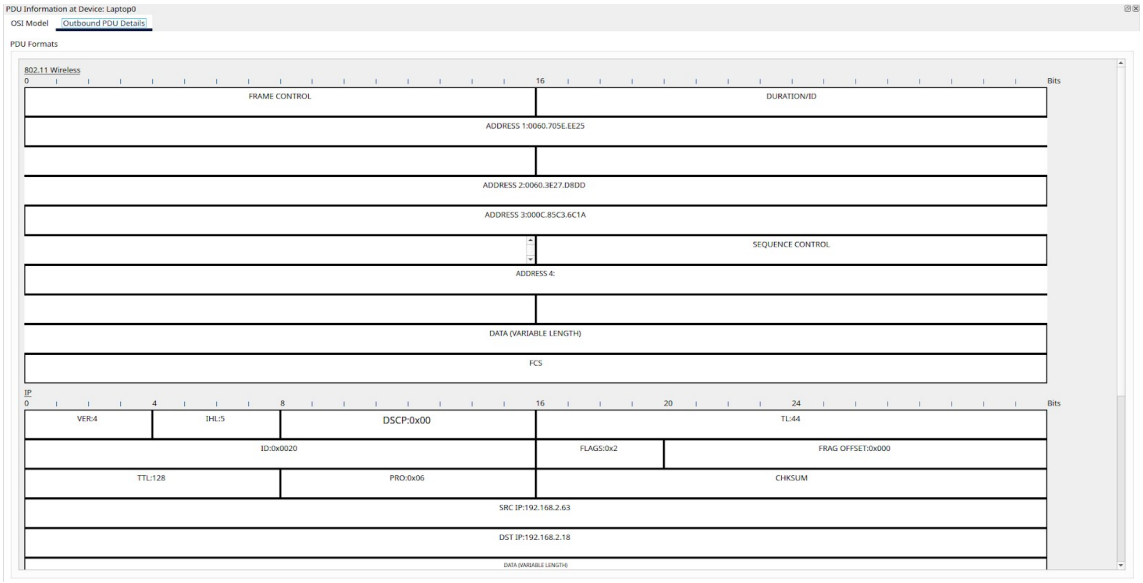
(Network Route of the mail package cont.2)



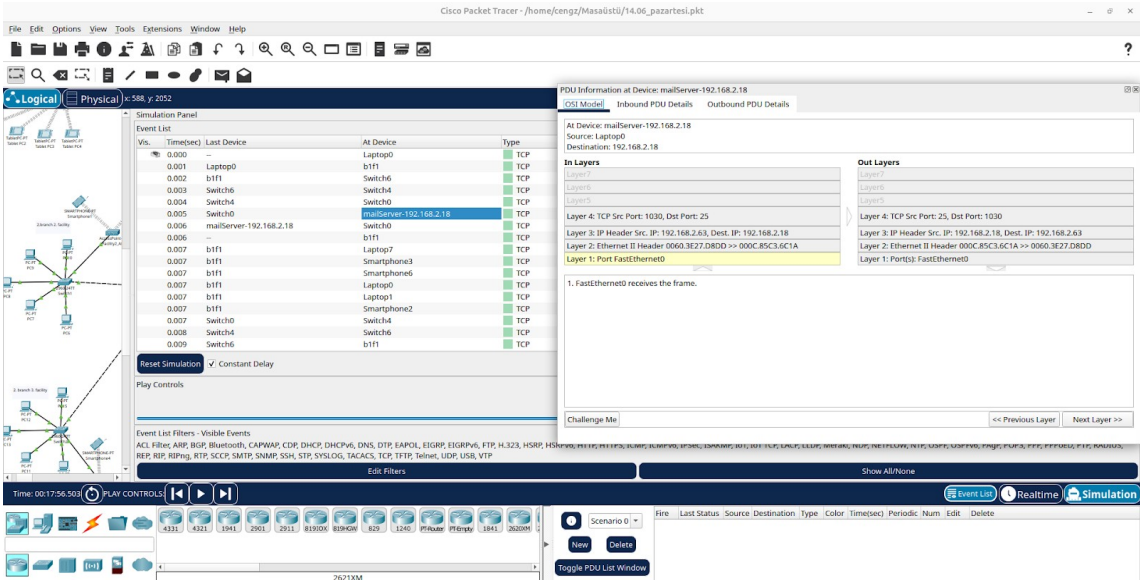
(Network Route of the mail package cont.3)



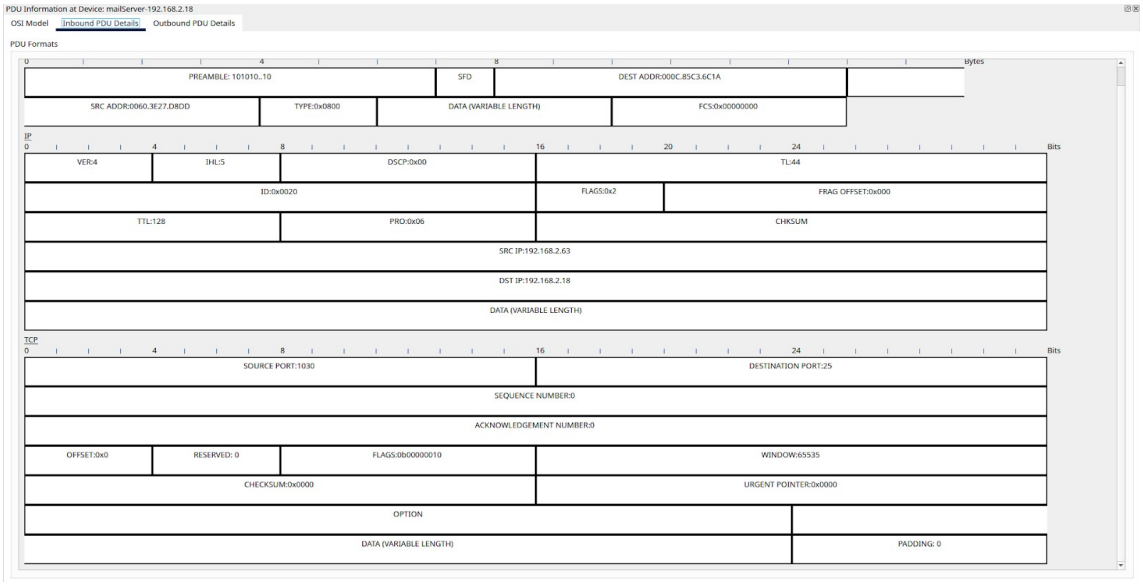
(Wireless User PDU detail)



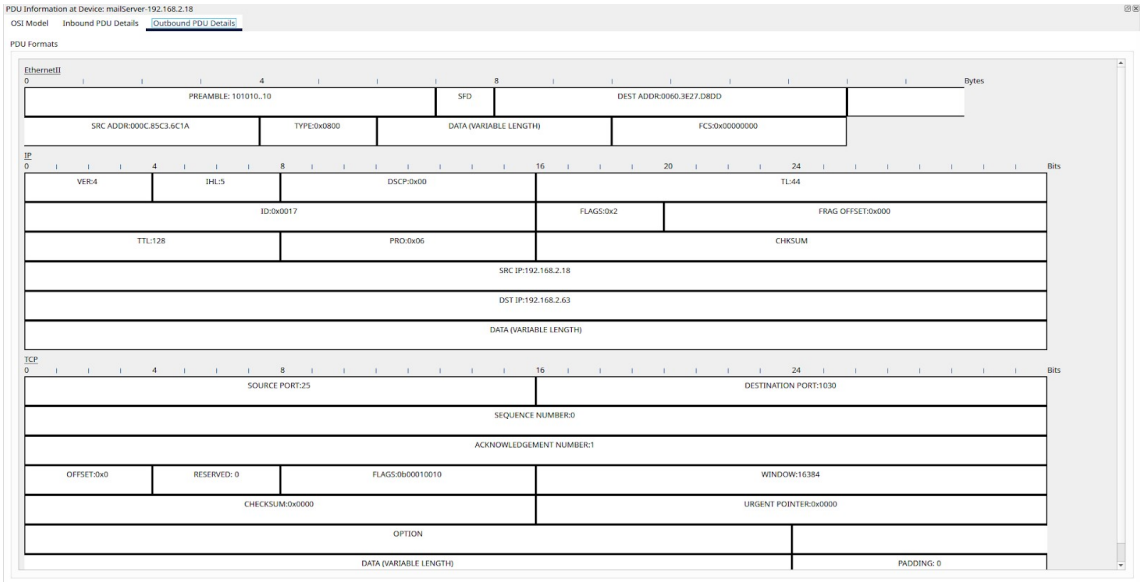
(Outbound detail of the package)



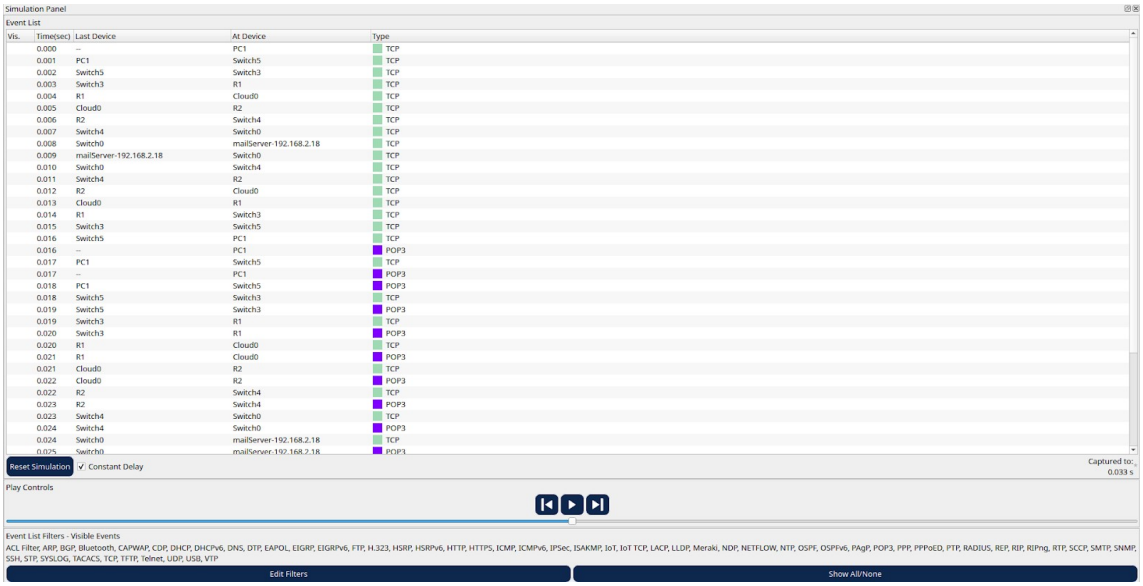
(OSI model of the time mail server receive package)



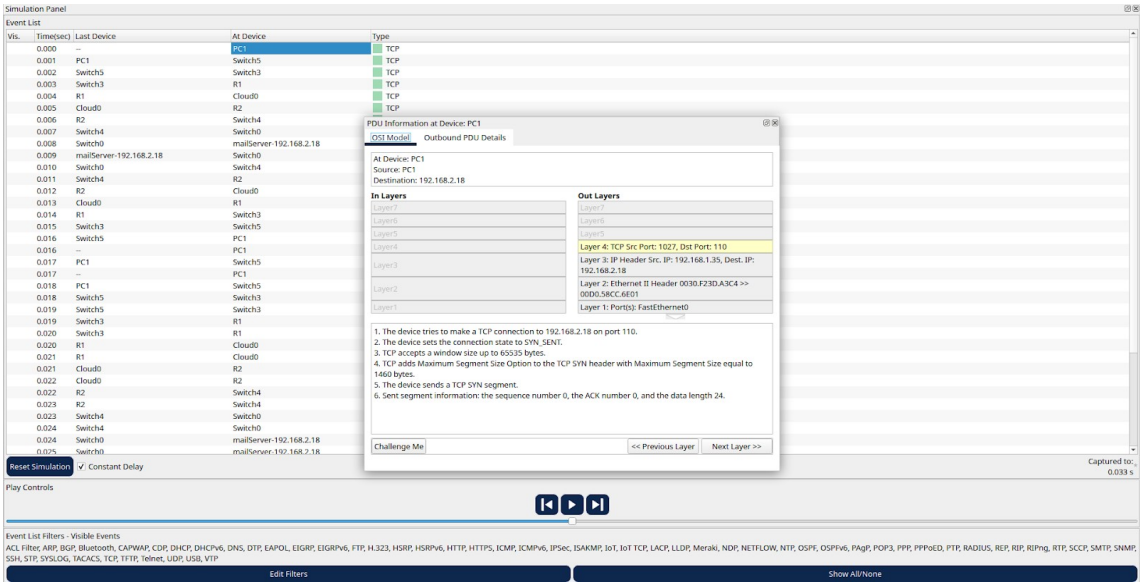
(Inbound detail of the package)



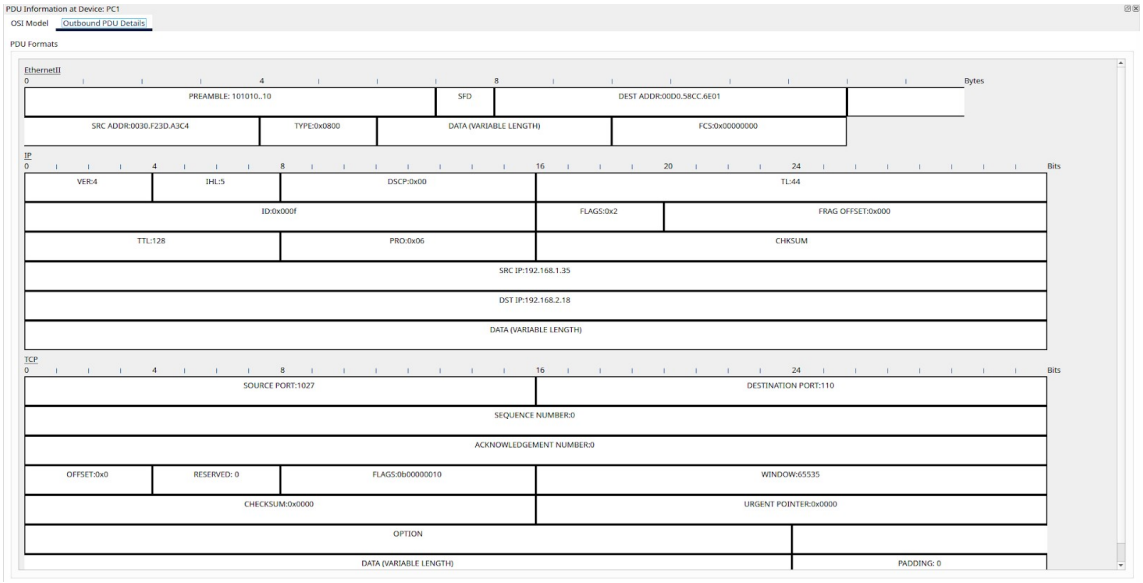
(Outbound detail of the package)



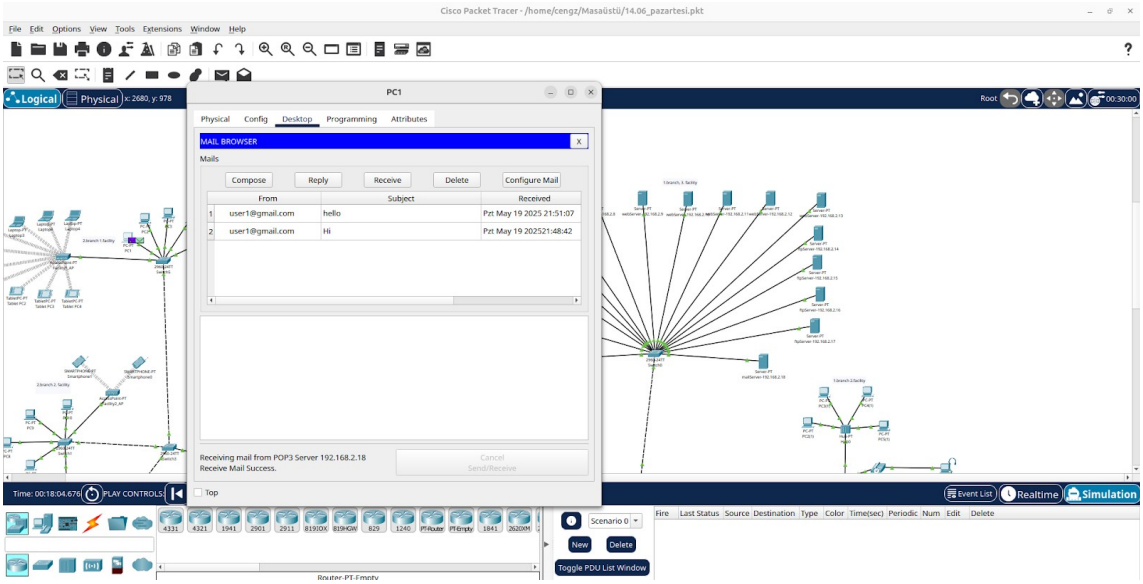
(From user from first facility Send request to the mail server if there are any new mail received)



(PDU detail of receive request)



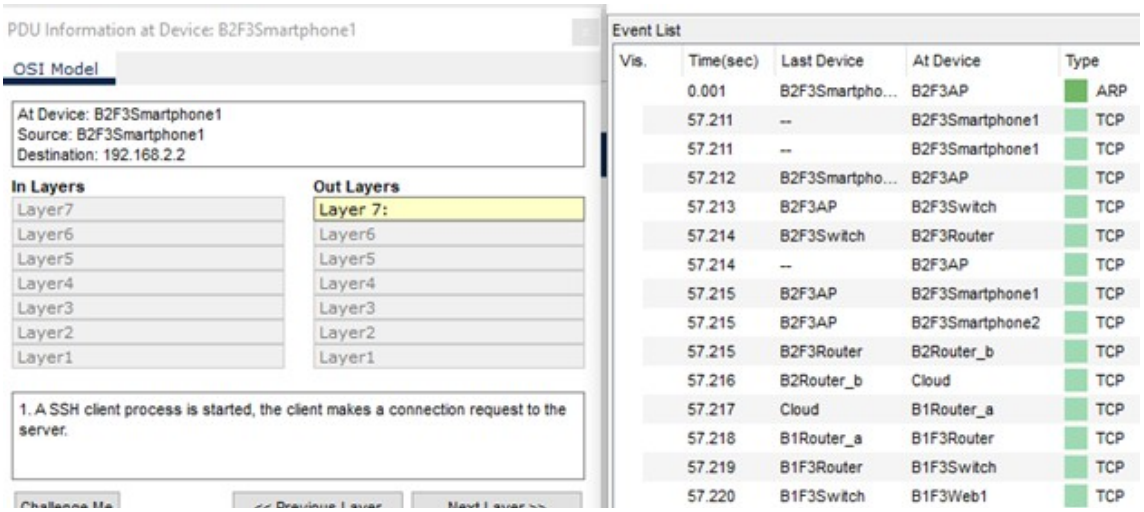
(Outbound details of request)



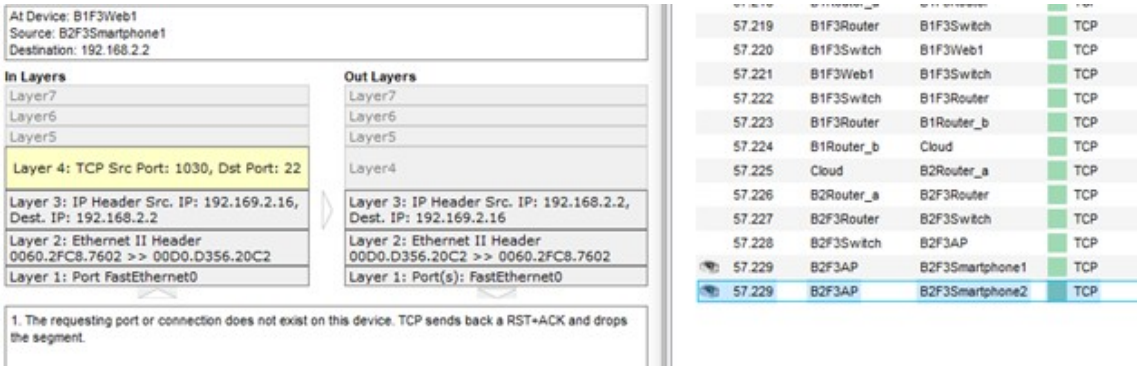
(Result of the request)

Scenario 7:

SSH Connection



(User tries to connect Web server via SSH.)

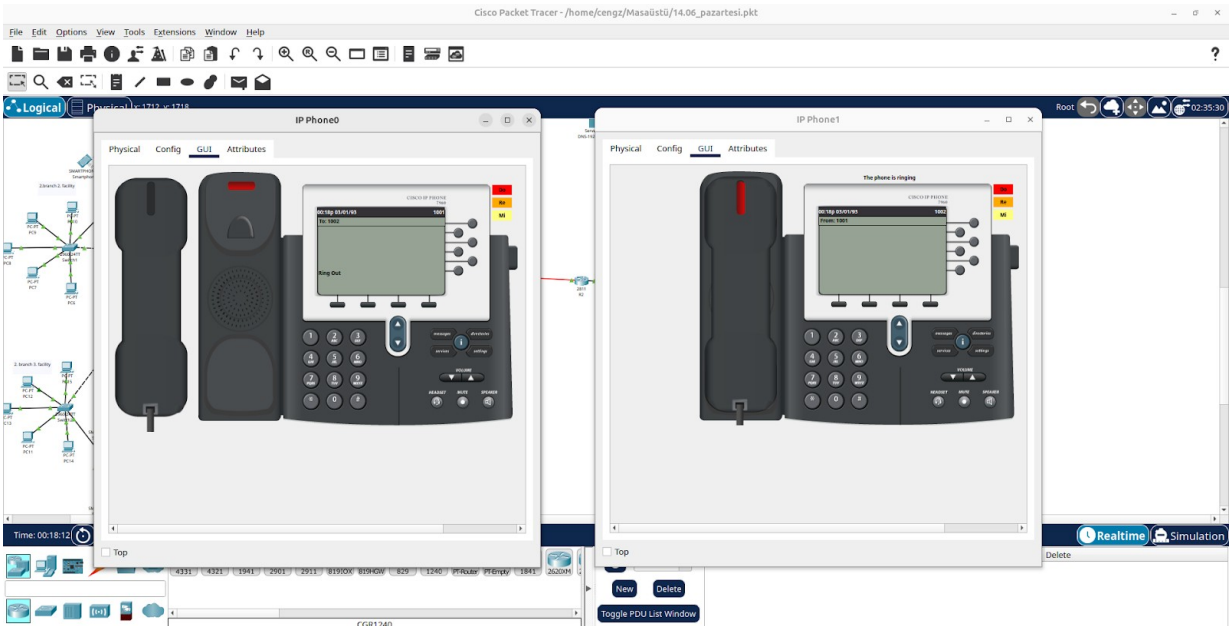


(Server rejects SSH connection)

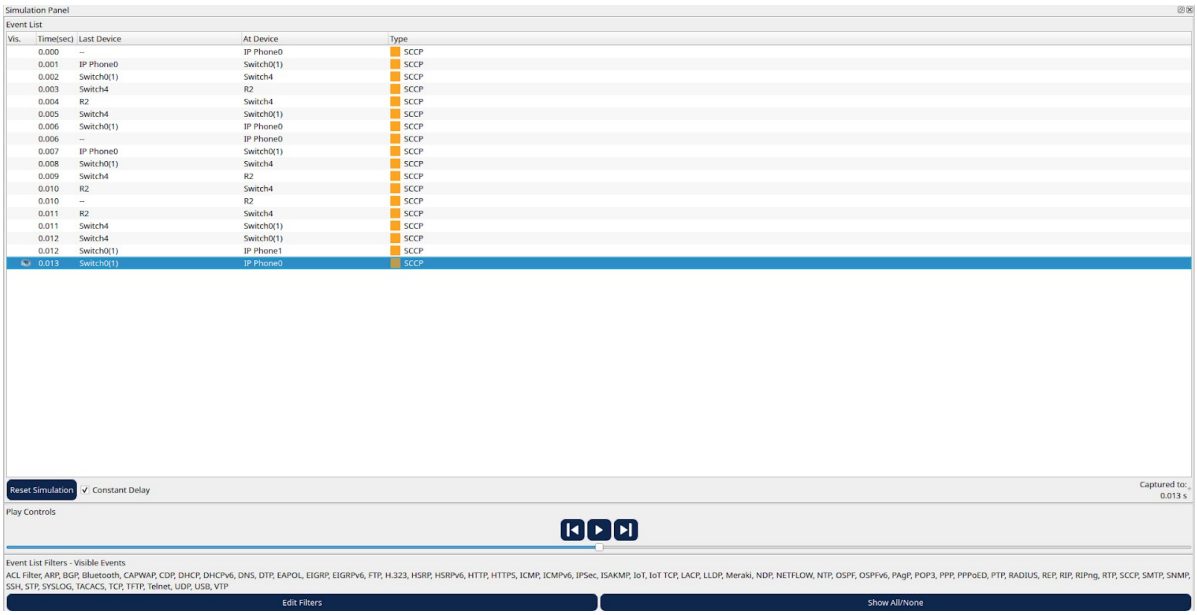
Note: In cisco packet tracer we are not able to connect to servers or pcs using ssh only router connections are allowed.

Custom Scenario 1:

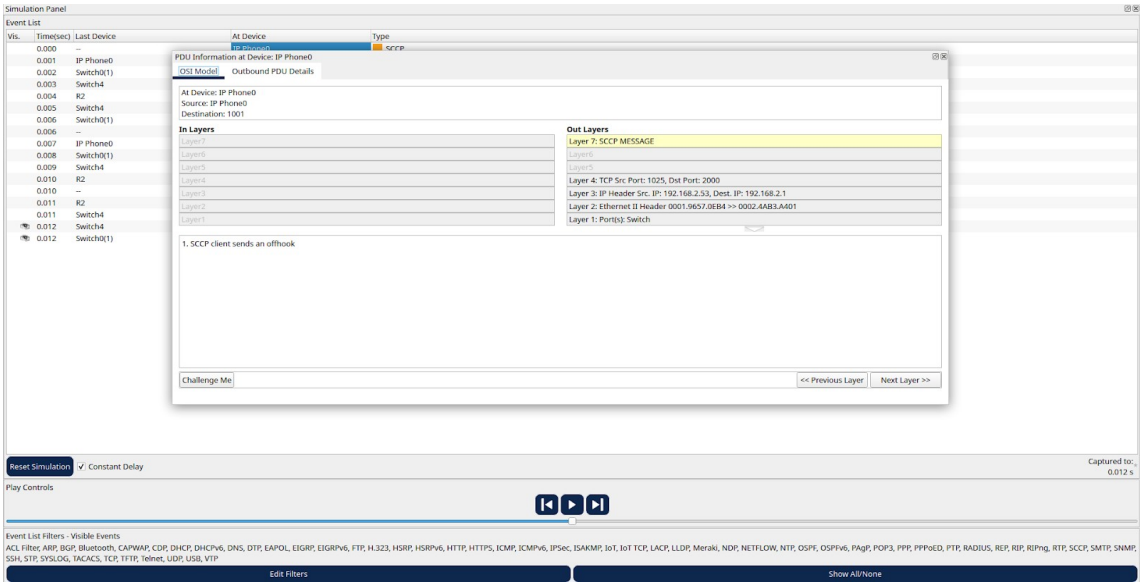
- **Description:** Voip user from the second facility of the first branch call voip conference event on the user of the other voip phone in the second facility of first branch
- **Result**: User1 successfully called User2



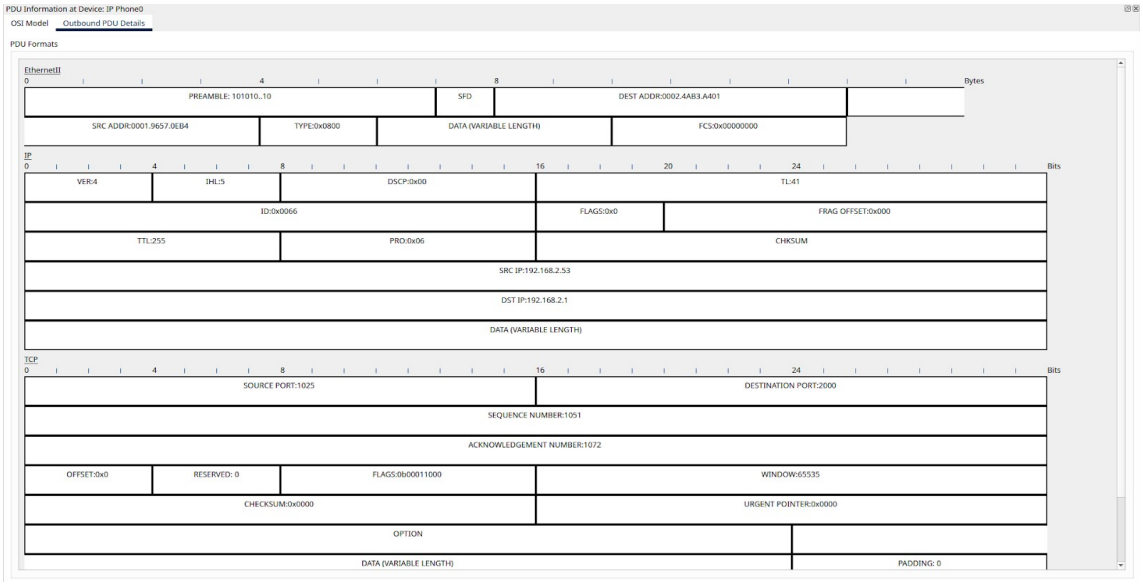
(Screenshot before user2 accept the call)



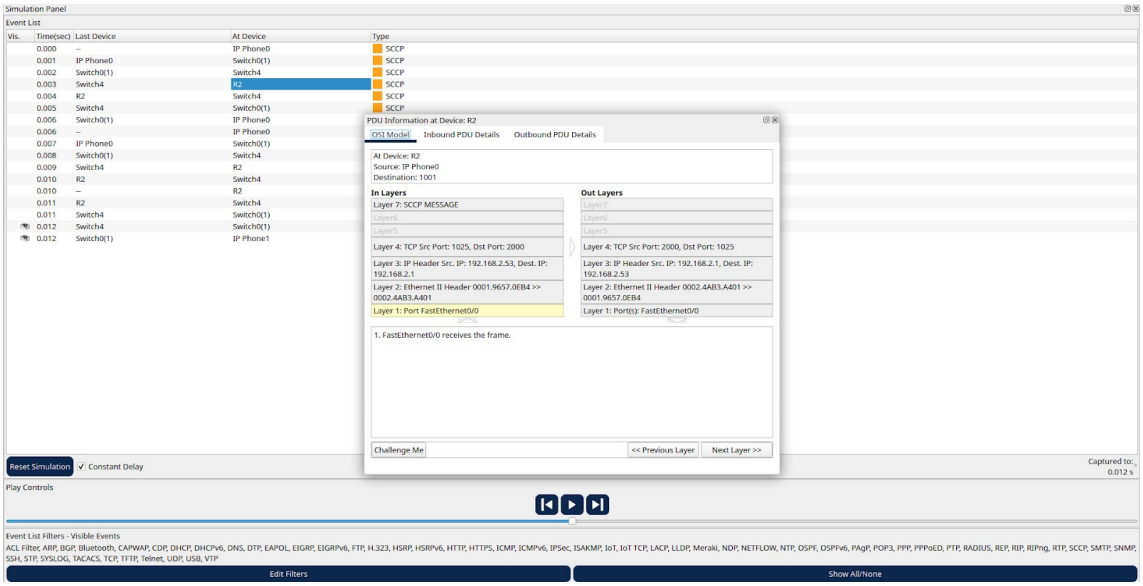
(VoIP Call route)



(OSI model of the call request)



(Outbound detail of the request)

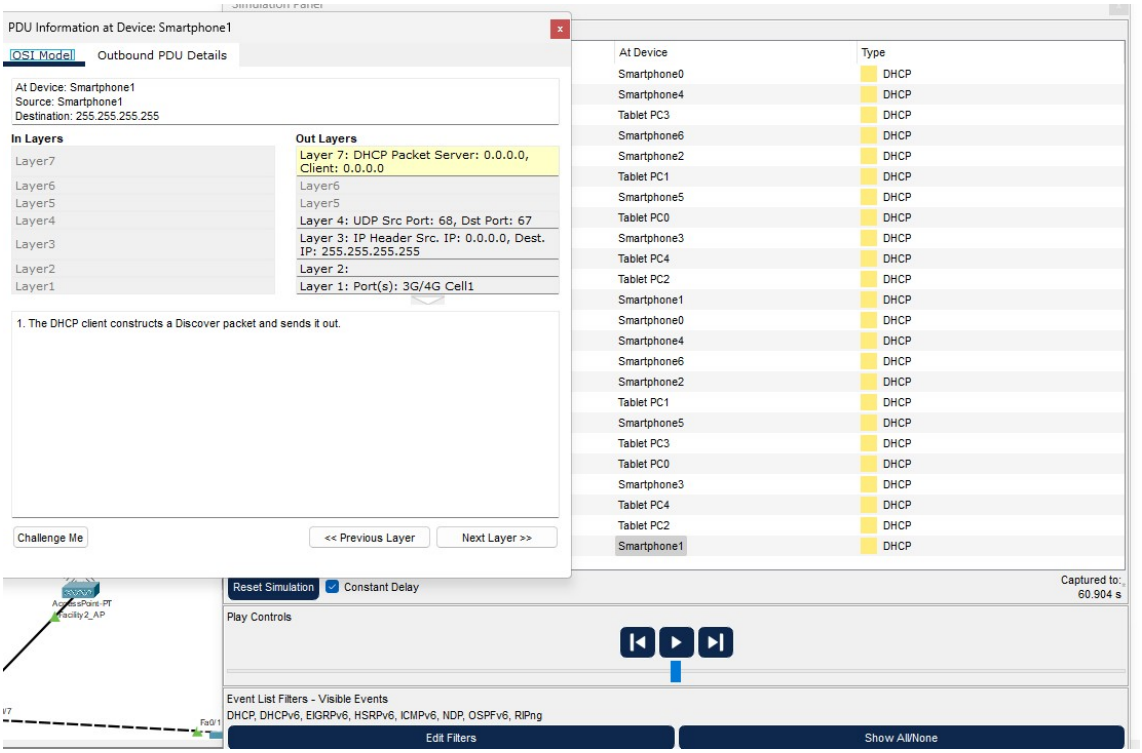


(Router Forward call to other VoIP telephone)

Custom Scenario 2:

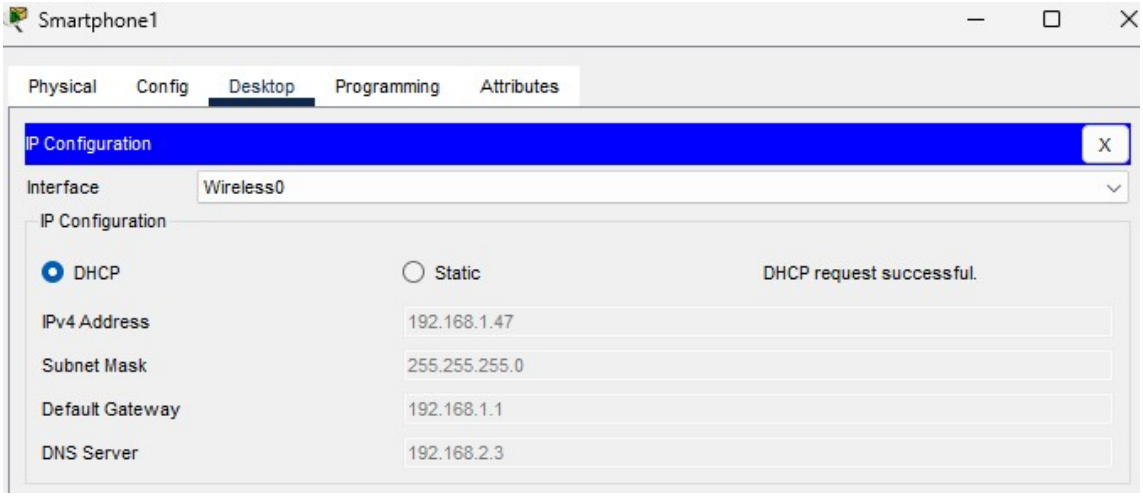
Description: A user from the second facility of the second branch obtains an IP address via DHCP from the third facility of the first branch.

Result: DHCP request successfully completed. User received an IP address from the remote DHCP server. Routing and relay configuration validated.



(PDU information and network routing for example ofsmartphone 1 the second facility of the second branch requesting DHCP)

(requesting phase)



(DHCP request successful)

4. Conclusion

In conclusion, this project has provided a comprehensive understanding of the design, implementation, and simulation of a Metropolitan Area Network (MAN) using Cisco Packet Tracer. By carefully analyzing the network requirements and specifications of each facility, we successfully built a scalable and resilient network architecture tailored to the needs of both branches.

Throughout the simulation process, we encountered and addressed several technical challenges—particularly in the implementation of VoIP services. These obstacles served as valuable learning opportunities, enhancing our problem-solving abilities and deepening our knowledge of real-time communication protocols.

The project also reinforced our practical skills in configuring and integrating various network devices, including workstations, laptops, smartphones, routers, switches, and servers. We effectively enabled services such as email, web access, file transfer, and voice communication across a multi-branch structure.

A key factor in the success of this project was effective teamwork. The collaborative effort allowed us to combine individual strengths, distribute responsibilities efficiently, and develop a well-structured and functional network system.

Overall, this project has been a significant educational experience that strengthened our foundational knowledge of networking principles, addressing schemes, routing

strategies, and network simulation. The insights and hands-on skills gained through this work will undoubtedly be valuable in future academic and professional pursuits in the field of network engineering.

5. References

Cisco Community. (2021). Retrieved from https://community.cisco.com/.

Cisco DevNet. (2021). Retrieved from https://developer.cisco.com/.

Cisco Learning Network. (2021). Retrieved from https://learningnetwork.cisco.com/.

Cisco Press. (2021). Retrieved from https://www.ciscopress.com/.

Cisco Systems, Inc. (2021). Cisco. Retrieved from https://www.cisco.com/.

Cisco Technology News. (2021). Retrieved from https://newsroom.cisco.com/.

Network Computing. (2021). Retrieved from https://www.networkcomputing.com/.

Packet Pushers. (2021). Retrieved from https://packetpushers.net/.