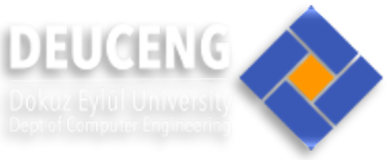
DOKUZ EYLUL UNIVERSITY

ENGINEERING FACULTY

DEPARTMENT OF COMPUTER ENGINEERING



METROPOLITAN AREA NETWORK SIMULATION PROJECT

By:

2022510013 – Yasamin Valishariatpanahi
2022510046 – Sara Mahyanbakhshayesh

Spring 2025
Izmir

TABLE OF CONTENTS

TABLE OF FIGURES *2*

CHAPTER ONE INTRODUCTION *5*

1.1 Project Definition and Problem Formulation **5**

1.2 Purpose and Motivation of the Project **5**

1.3 Term Definitions **6**

1.4 Related Work **7**

CHAPTER TWO METHOD AND SIMULATION *7*

2.1. Simulation and Modeling Concepts **7**

2.2. Simulation Environment/Tool **8**

2.3. Network Design Requirements **9**

2.4. Requirement Analysis **10**

2.5. Definitions of the System/Model **10**

2.6. Simulation Elements **21**

CHAPTER THREE TRAFFIC ANALYSIS AND SIMULATION RESULTS *29*

Scenario 1: Email Communication and Web Access **29**

Scenario 2: FTP File Transfer Between Branch Facilities **40**

Scenario 3: Internal VoIP Communication Within a Facility **46**

Scenario 4: Email Access Denied Between Facilities Due to Permission Restrictions **53**

Scenario 5: Inter-Branch Ping Test from Client to Web Server **55**

Scenario 6: Cross-Branch Email Communication Between Laptop Users **60**

Scenario 7: Remote Web Server Access via SSH from a Smartphone **65**

Additional Scenario 8: A Tablet User Receives and Replies to a Message **73**

Additional Scenario 9: A VoIP User Calls an Unidentified Number **82**

CHAPTER FOUR PROBLEMS ENCOUNTERED *87*

CHAPTER FIVE CONCLUSION *88*

CHAPTER SIX REFERENCES *89*

TABLE OF FIGURES

Figure 1: General Design of the System 10
Figure 2: Branch 1 - Facility 1 11
Figure 3: Branch 1 - Facility 2 11
Figure 4: Branch 1 - Facility 3 12
Figure 5: Branch 2 - Facility 1 13
Figure 6: Branch 2 - Facility 2 13
Figure 7: Branch 2 - Facility 3 14
Figure 8: Physical Design of the System - Home City 14
Figure 9: Physical Design of the System - Branches inside Home City 15
Figure 10: Physical Design of the System - Corporate Office (ISP) 15
Figure 11: Physical Design of the System - Corporate Office (ISP) - Wiring Closet 16
Figure 12: Physical Design of the System - Branch 1 16
Figure 13: Physical Design of the System - Branch 1 – Router - Wiring Closet 17
Figure 14: Physical Design of the System - Branch 1 - Facility 1 - Wiring Closet 17
Figure 15: Physical Design of the System - Branch 1 - Facility 2 - Wiring Closet 18
Figure 16: Physical Design of the System - Branch 1 - Facility 3 - Wiring Closet 18
Figure 17: Physical Design of the System - Branch 2 – Router - Wiring Closet 19
Figure 18: Physical Design of the System - Branch 2 - Facility 1 - Wiring Closet 19
Figure 19: Physical Design of the System - Branch 2 - Facility 2 - Wiring Closet 20
Figure 20: Physical Design of the System - Branch 2 - Facility 3 - Wiring Closet 20
Figure 21: DHCP Server – Config 21
Figure 22: DHCP Server - Services 21
Figure 23: DNS Server - Config 22
Figure 24: DNS Server - Services 22
Figure 25: FTP1 Server – Config 23
Figure 26: FTP1 Server - Services 23
Figure 27: FTP2 Server – Config 24
Figure 28: FTP2 Server - Services 24
Figure 29: FTP3 Server – Config 25
Figure 30: FTP3 Server - Services 25
Figure 31: FTP4 Server – Config 26
Figure 32: FTP4 Server - Services 26
Figure 33: Mail Server - Config 27
Figure 34: Mail Server – Services 27
Figure 35: E-Mail Configuration Example for PC1-F1B1 28
Figure 36: Web Server 1 (Google.com) – Config 28
Figure 37: Composing an email from Smartphone1-F1B1 to Laptop1-F1B2 30
Figure 38: Receive an email in Branch 2 31
Figure 39: Simulation Panel 32

Figure 40: PDU Information at Device - Laptop1-F1B2 – OSI Model....33
Figure 41: PDU Information at Device - Laptop1-F1B2 – Inbound PDU details....34
Figure 42: Browsing Web....36
Figure 43: Simulation Panel....37
Figure 44: PDU Information at Device - Laptop1-F1B2 – OSI Model....38
Figure 45: PDU Information at Device - Laptop1-F1B2 – Inbound PDU details....39
Figure 46: Code Example....41
Figure 47: Command Prompt - PC1-F2B2....42
Figure 48: Simulation Panel....43
Figure 49: PDU Information at Device - FTP1 – OSI Model....44
Figure 50: PDU Information at Device - FTP1 – Inbound PDU details....45
Figure 51: VoIP Devices Call - F2B1....47
Figure 52: Simulation Panel....48
Figure 53: PDU Information at Device – VoIP1-F2B1 – OSI Model....49
Figure 54: PDU Information at Device - VoIP1-F2B2 – Inbound PDU details....50
Figure 55: PDU Information at Device – VoIP2-F2B1 – OSI Model....51
Figure 56: PDU Information at Device - VoIP2-F2B2 – Inbound PDU details....52
Figure 57: PC2-F2B1 Sending an Email to Smartphone1-F2B2....54
Figure 58: Smartphone1-F2B2 Failed to Receive....54
Figure 59: Command Prompt - TabletPC2-F1B2....56
Figure 60: Simulation Panel....57
Figure 61: PDU Information at Device – TabletPC2-F1B2 – OSI Model....58
Figure 62: PDU Information at Device - TabletPC2-F1B2 – Inbound PDU details....59
Figure 63: Sending an Email from Laptop1-F1B1 to Laptop1-F1B2 (Success)....61
Figure 64: Simulation Panel....62
Figure 65: PDU Information at Device – Laptop1-F1B1 – OSI Model....63
Figure 66: PDU Information at Device - Laptop1-F1B1 – Inbound PDU details....64
Figure 67: Telnet/SSH Client....66
Figure 68: SSH Client ping result....67
Figure 69: Simulation Panel....68
Figure 70: PDU Information at Device – R1-F3B1 – OSI Model (In Layer)....69
Figure 71: PDU Information at Device - R1-F3B1 – Inbound PDU details (In Layer)....70
Figure 72: PDU Information at Device – R1-F3B1 – OSI Model (Out Layer)....71
Figure 73: PDU Information at Device - R1-F3B1 – Inbound PDU details (Out Layer)....72
Figure 74: Received Email (Success)....74
Figure 75: Reply to the Email (Success)....75
Figure 76: Simulation Panel (Receive)....76
Figure 77: PDU Information at Device - TabeletPC5-F1B2 – OSI Model (Receive)....77
Figure 78: PDU Information at Device - TabletPC5-F1B2 – Inbound PDU details (Receive)....78
Figure 79: Simulation Panel (Reply)....79
Figure 80: PDU Information at Device - TabeletPC5-F1B2 – OSI Model (Reply)....80
Figure 81: PDU Information at Device - TabletPC5-F1B2 – Inbound PDU details (Reply)....81
Figure 82: Calling 5522 which is undefined result in Unknown Number....83
Figure 83: Simulation Panel....84
Figure 84:PDU Information at Device – VoIP1-F2B1 – OSI Model....85

Figure 85: PDU Information at Device - VoIP1-F2B2 – Inbound PDU details 86

CHAPTER ONE
INTRODUCTION

1.1 Project Definition and Problem Formulation

A **Metropolitan Area Network (MAN)** is a large-scale computer network that spans a city or metropolitan region, interconnecting multiple local area networks (LANs) or campus networks. MANs provide high-speed connectivity, enabling communication between businesses, government organizations, and institutions. They are typically implemented using fiber-optic cables, leased lines, or wireless communication technologies.

In this project, we aim to design and simulate a **Metropolitan Area Network (MAN)** that connects two distinct branch offices within a city via an **Internet Service Provider (ISP)** using **Cisco Packet Tracer**. Each branch office consists of multiple facilities, each with unique networking requirements such as internet access, email communication, file sharing, VoIP communication, and web hosting. The network must be designed to support seamless data transmission, efficient routing, and optimal resource utilization.

The project involves:

- Designing a **topology** that includes routers, switches, wireless access points, and end devices.
- Implementing a **structured IP addressing scheme** using IPv4/IPv6.
- Configuring networking services such as **DNS, DHCP, FTP, HTTP, SMTP, and VoIP**.
- Simulating and testing various network scenarios, including file transfers, web browsing, and voice communication.
- Analyzing network traffic, performance, and potential bottlenecks.

This project will provides a comprehensive insight into **network design principles**, **traffic engineering**, **security considerations**, and **performance optimization** in a real-world networking scenario.

1.2 Purpose and Motivation of the Project

The main objective of this project is to create a **scalable, cost-effective, and efficient network architecture** that meets the growing demands of businesses and organizations. The motivations behind this project include:

- **Practical Understanding of MAN Design**: Learning how to interconnect multiple facilities through routers and an ISP.

- **Simulation-Based Learning**: Gaining hands-on experience using **Cisco Packet Tracer** for designing, configuring, and testing networks.
- **Network Performance Optimization**: Understanding best practices for achieving minimal latency, high reliability, and efficient bandwidth utilization.
- **Security and Reliability Considerations**: Implementing **firewalls, encryption protocols, and access control** to protect sensitive data and ensure secure communication.
- **Future Scalability**: Designing the network to support future expansion without requiring a complete overhaul.

By undertaking this project, students will enhance their **problem-solving abilities**, **network troubleshooting skills**, and **technical knowledge** in designing enterprise-level networks.

1.3 Term Definitions

To fully understand the project, it is essential to define key networking terms:

- **Network**: A system of interconnected devices that communicate using wired or wireless connections.
- **Wireless**: A communication method that transmits data without physical cables, typically using radio waves.
- **Nodes**: Devices such as computers, routers, and switches connected to a network.
- **Ethernet**: A wired networking standard used for local area networks (LANs) to enable communication between devices.
- **Frame**: A unit of data transmitted over a network at the **Data Link Layer** of the OSI model.
- **Access Point (AP)**: A device that provides wireless connectivity to a wired network.
- **Switch**: A networking device that connects multiple devices within a LAN and forwards data based on MAC addresses.
- **Router**: A device that connects multiple networks and directs data packets between them.
- **Packet**: A small unit of data transmitted over a network that contains source and destination information.
- **Network Architecture**: The overall structure of a network, including its topology, components, and protocols.
- **Protocol**: A set of rules that govern data communication between devices.
- **IP Address**: A unique identifier assigned to a device on a network, either **IPv4 (e.g., 192.168.1.1)** or **IPv6 (e.g., 2001:db8::ff00:42:8329)**.
- **TCP (Transmission Control Protocol)**: A reliable communication protocol that ensures ordered data delivery.
- **Channel**: A communication pathway that carries data between devices.
- **Workstation**: A powerful computing device used for business or technical applications.
- **Server**: A computer that provides services such as web hosting, file storage, and email handling.

- **DNS (Domain Name System)**: A system that translates domain names (e.g., www.google.com) into IP addresses.
- **FTP (File Transfer Protocol)**: A protocol used to transfer files between a client and a server.
- **HTTP (Hypertext Transfer Protocol)**: A protocol used for web browsing and retrieving web pages.
- **POP (Post Office Protocol)**: A protocol used for retrieving emails from a mail server.
- **SMTP (Simple Mail Transfer Protocol)**: A protocol used to send emails.
- **VoIP (Voice over Internet Protocol)**: A technology that enables voice communication over the internet.
- **Domain**: A human-readable address (e.g., example.com) used to access websites.
- **ISP (Internet Service Provider)**: A company that provides internet access to users and businesses.
- **SSH (Secure Shell)**: A protocol used for secure remote access to network devices.

1.4 Related Work

The design and implementation of **Metropolitan Area Networks** have been widely explored in academia and industry. Several studies focus on **network performance, security, and scalability**. Key research contributions include:

- **Maria, A. (1997)**: "Introduction to modeling and simulation" – Discusses fundamental concepts of network modeling and simulation.
- **Issariyakul & Hossain (2009)**: "Simulation of Computer Networks" – Provides insights into network simulation methodologies.
- **IEEE and ACM research papers**: Discuss topics such as **traffic engineering, IP subnetting, and network security**.
- **Enterprise Network Design Case Studies**: Provide real-world implementations of large-scale networks for organizations and businesses.

By analyzing existing works, this project aligns with **industry best practices** and contributes to the field of network engineering. It integrates theoretical knowledge with **practical implementation**, ensuring a comprehensive learning experience.

CHAPTER TWO
METHOD AND SIMULATION

2.1. Simulation and Modeling Concepts

Simulation and modeling are fundamental components of any network design, as they provide insight into how a network will behave under different conditions. The simulation process began by identifying the different components of the network, including routers, switches, end devices, and the various connections between them. These components were then

modeled using Cisco Packet Tracer, a powerful tool that allows for visualizing network topologies and testing configurations in real-time. This initial modeling helped us anticipate potential issues and ensure that the design would be robust enough to handle the demands of both branch offices.

The iterative design process was key to refining the network architecture. By starting with small, basic units such as individual workstations and wireless devices, we were able to build up the design incrementally, adding complexity as we went along. This method ensured that any issues could be identified and resolved at each stage of the process, rather than waiting until the entire network was built. This allowed us to focus on optimizing individual components before scaling them up to larger, more complex systems. Moreover, the bottom-up approach helped us speed up the process of getting the network up and running, which was essential for meeting the project's timeline.

Another critical aspect of network modeling was understanding the flow of network traffic. Traffic patterns can vary widely depending on the number of users, the types of devices in use, and the kind of services required. The network traffic characterization process helped us analyze the type of data that would be transmitted across the network, whether it was voice, video, email, or large file transfers. By simulating these traffic patterns, we were able to test how well the network would perform under different loads, ensuring that there were no bottlenecks and that the network could handle peak usage without degradation in performance.

The simulation also provided insights into the behavior of protocols used in the network, such as DHCP, DNS, and FTP. These protocols play a critical role in ensuring that devices can find each other on the network and access the necessary services. Testing these protocols in the simulated environment allowed us to identify any misconfigurations or potential issues before the network was actually deployed. This step was essential in ensuring that the network would be both functional and reliable, providing a seamless user experience for those relying on it for communication and data transfer.

2.2. Simulation Environment/Tool

The network design requirements were developed after careful analysis of the needs of each branch and its respective facilities. The goal was to create a network that could support multiple users and devices, ensuring that everyone would have reliable access to network resources. A key requirement was scalability. As both branches were part of a Metropolitan Area Network (MAN), the design had to accommodate future growth, such as additional workstations, laptops, or servers. The network had to be adaptable, with the ability to add new devices or expand capacity without significant disruptions.

Another important design consideration was redundancy. In the event of a failure, the network needed to ensure that users could still access critical services. This was achieved by using at least two routers per branch and multiple links between facilities. If one router or connection failed, the network could route traffic through another path, ensuring high availability. This redundancy was especially important for the services hosted on the server

farm in the third facility of the first branch, as these servers supported critical functions like Web hosting, FTP, and email services.

The design also had to prioritize security and data integrity. Sensitive data, such as emails or FTP file transfers, had to be protected from unauthorized access. We implemented various security measures, including firewalls, encryption, and VPNs (Virtual Private Networks), to ensure secure communication between branches and remote users. In addition, the network had to be configured in such a way that data would be transmitted efficiently, without unnecessary delays or bottlenecks. This required traffic shaping and quality of service (QoS) mechanisms to prioritize important traffic, such as VoIP calls or video conferences.

Lastly, the network design had to balance performance and cost. While it was important to use high-quality hardware and software to ensure reliable service, the design also needed to stay within budget constraints. This meant selecting devices that offered the best performance-to-cost ratio while still meeting the network's requirements. For instance, we chose Cisco routers and switches, which are known for their reliability and performance, but we ensured that the selected models would provide the necessary features without exceeding the budget.

2.3. Network Design Requirements

The network design requirements were developed after careful analysis of the needs of each branch and its respective facilities. The goal was to create a network that could support multiple users and devices, ensuring that everyone would have reliable access to network resources. A key requirement was scalability. As both branches were part of a Metropolitan Area Network (MAN), the design had to accommodate future growth, such as additional workstations, laptops, or servers. The network had to be adaptable, with the ability to add new devices or expand capacity without significant disruptions.

Another important design consideration was redundancy. In the event of a failure, the network needed to ensure that users could still access critical services. This was achieved by using at least two routers per branch and multiple links between facilities. If one router or connection failed, the network could route traffic through another path, ensuring high availability. This redundancy was especially important for the services hosted on the server farm in the third facility of the first branch, as these servers supported critical functions like Web hosting, FTP, and email services.

The design also had to prioritize security and data integrity. Sensitive data, such as emails or FTP file transfers, had to be protected from unauthorized access. We implemented various security measures, including firewalls, encryption, and VPNs (Virtual Private Networks), to ensure secure communication between branches and remote users. In addition, the network had to be configured in such a way that data would be transmitted efficiently, without unnecessary delays or bottlenecks. This required traffic shaping and quality of service (QoS) mechanisms to prioritize important traffic, such as VoIP calls or video conferences.

Lastly, the network design had to balance performance and cost. While it was important to use high-quality hardware and software to ensure reliable service, the design also needed to stay within budget constraints. This meant selecting devices that offered the best performance-to-cost ratio while still meeting the network's requirements. For instance, we chose Cisco routers and switches, which are known for their reliability and performance, but we ensured that the selected models would provide the necessary features without exceeding the budget.

2.4. Requirement Analysis

The requirement analysis phase was critical to ensuring that we understood the specific needs of each facility before proceeding with the design. We began by analyzing the types of devices that would be used in each facility, such as workstations, smartphones, and wireless devices, and determining the services that each device would require. This included Web access, FTP transfers, email communication, and VoIP support. By understanding the specific needs of each facility, we could plan how the network would be structured, how IP addresses would be assigned, and which devices would need to be connected to the network at any given time.

The analysis also extended to the traffic patterns of the network. We needed to understand how data would flow between devices, particularly in the context of scenarios such as VoIP calls or large file transfers over FTP. For example, workstations in the first facility of the first branch needed to have reliable VoIP support for conference calls, while the server farm in the third facility required a high level of availability and performance for services like web hosting and FTP. This analysis helped guide the decision-making process when it came to selecting appropriate network hardware (e.g., routers, switches, wireless access points) and configuring service protocols such as DHCP and DNS.

2.5. Definitions of the System/Model

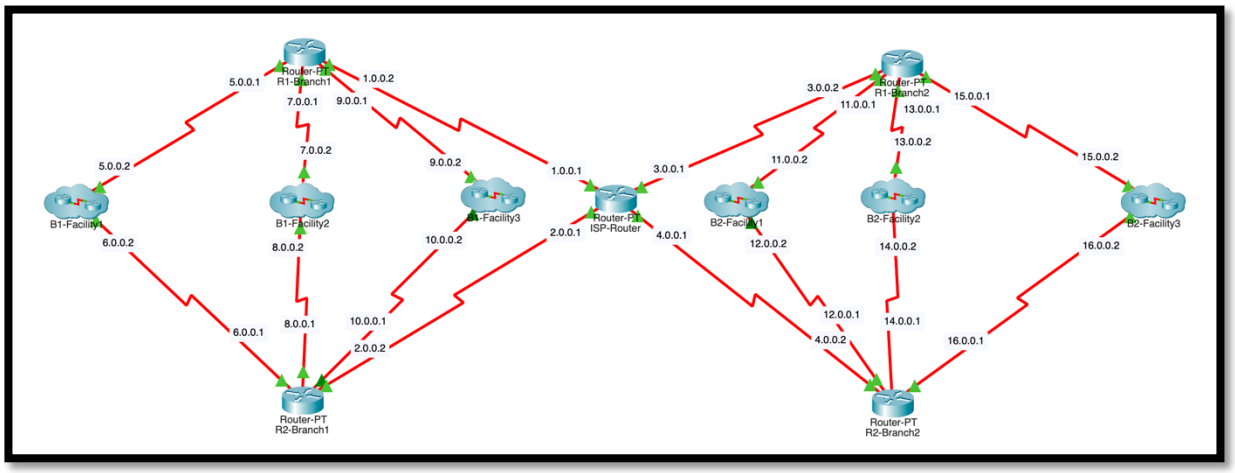


Figure 1: General Design of the System

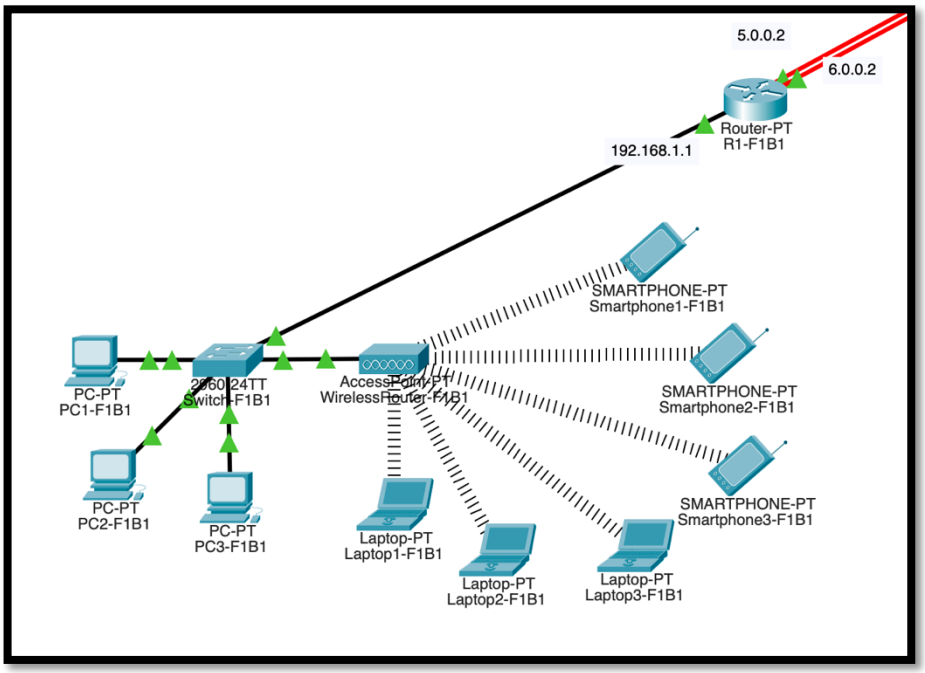


Figure 2: Branch 1 - Facility 1

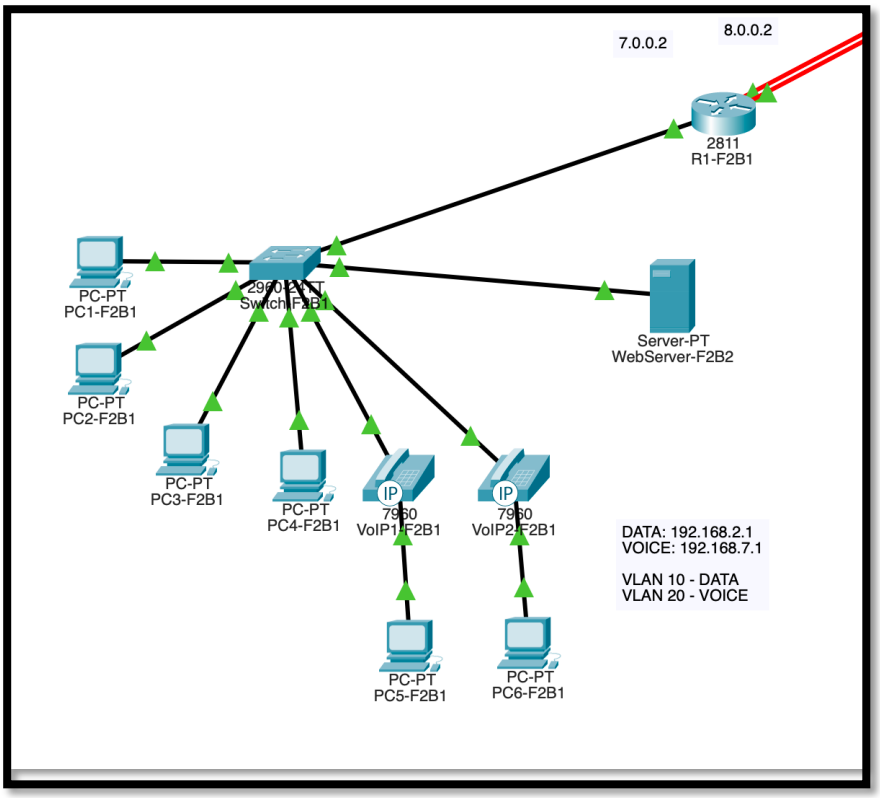


Figure 3: Branch 1 - Facility 2

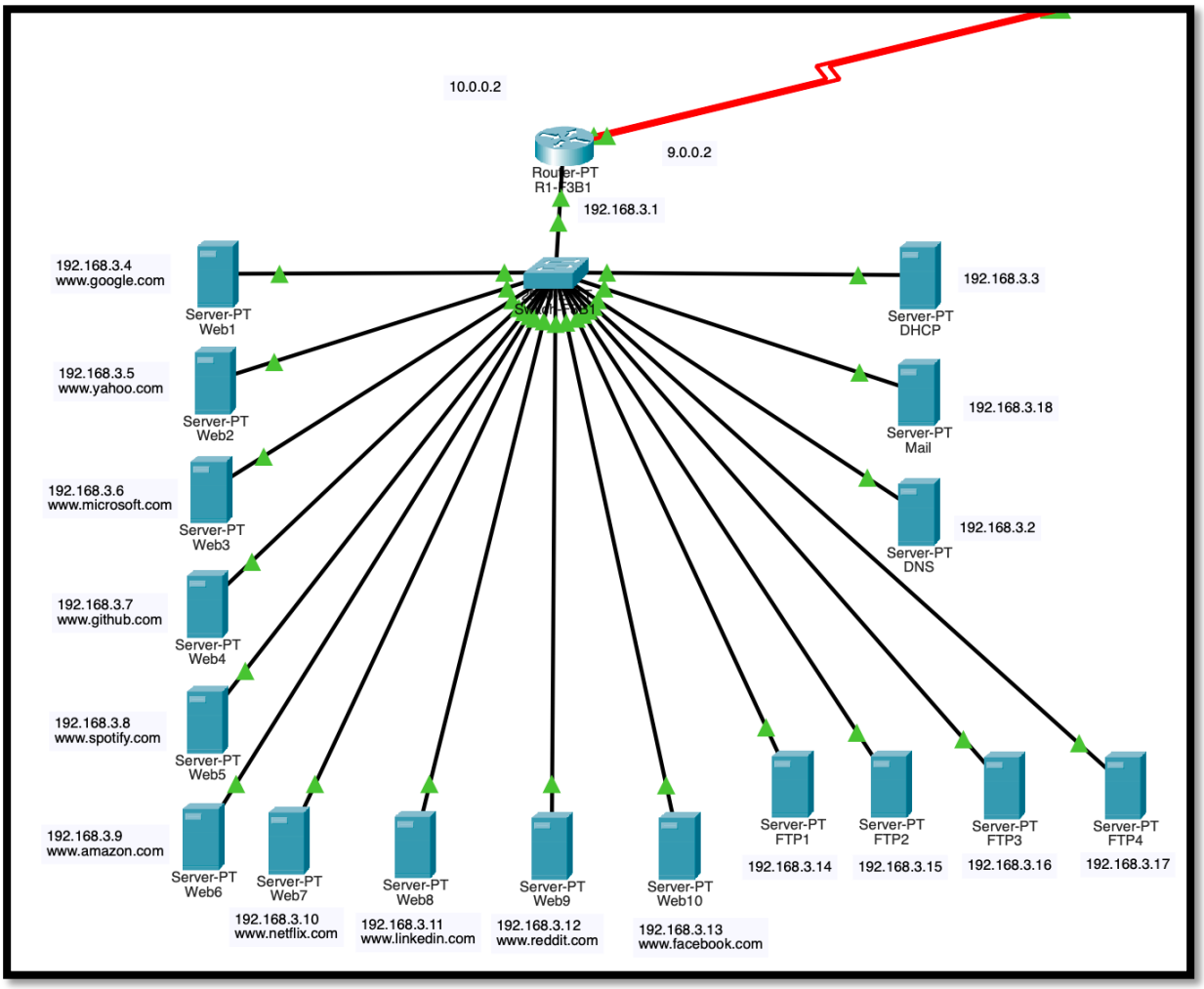


Figure 4: Branch 1 - Facility 3

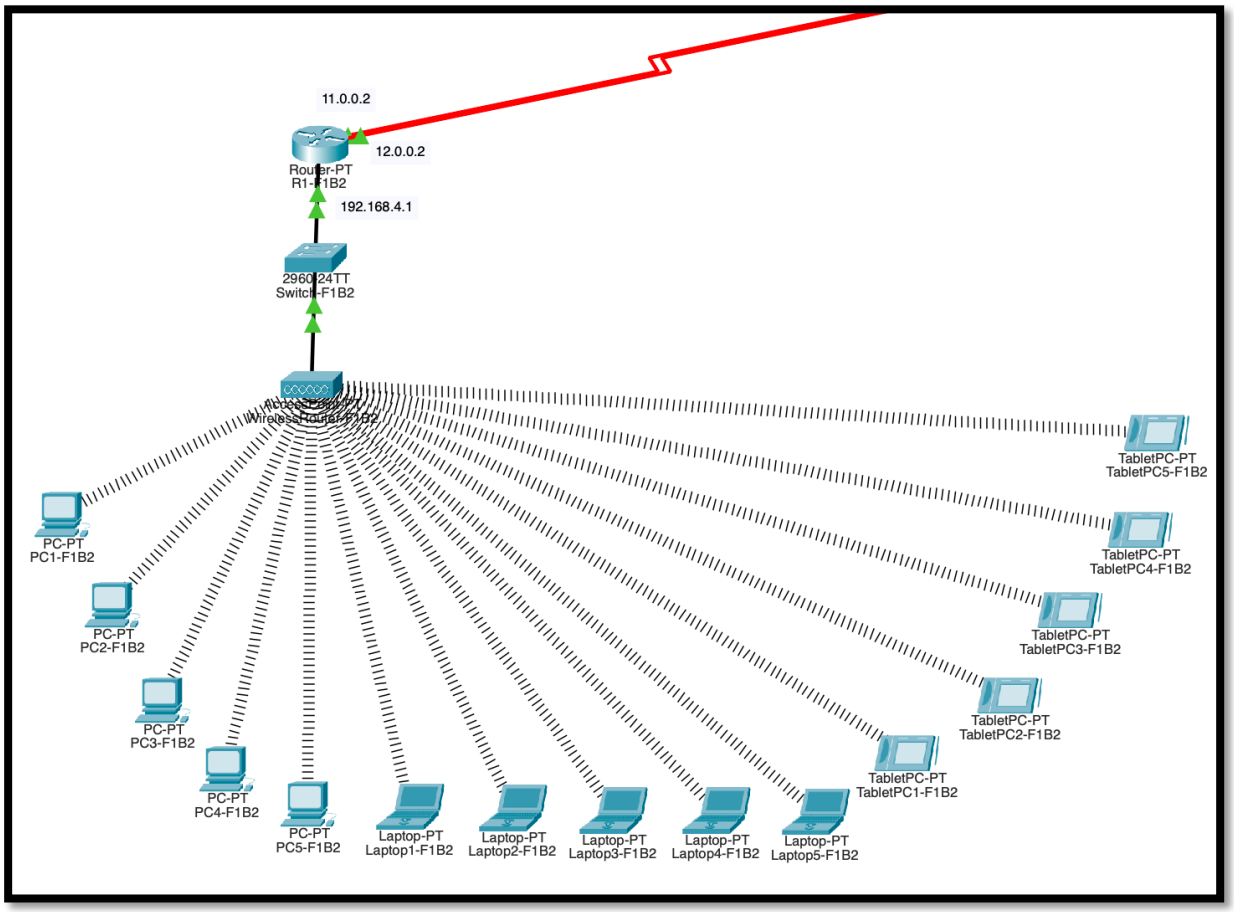


Figure 5: Branch 2 - Facility 1

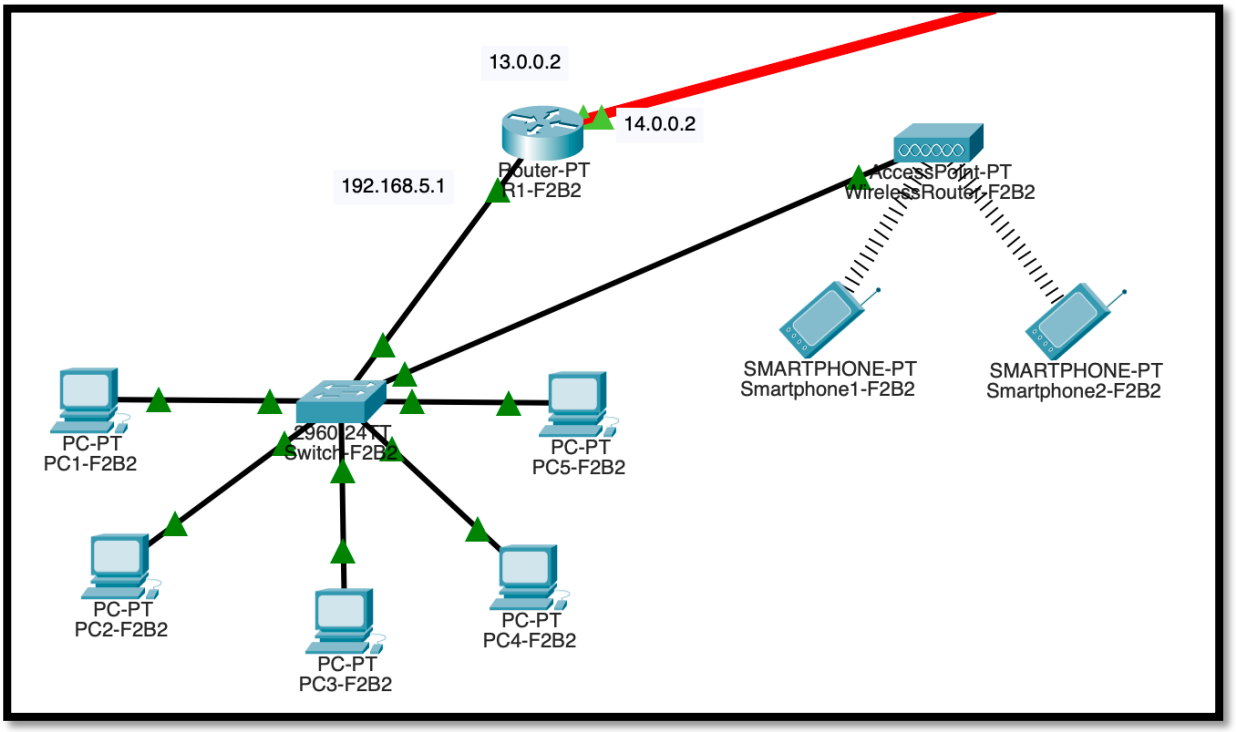


Figure 6: Branch 2 - Facility 2

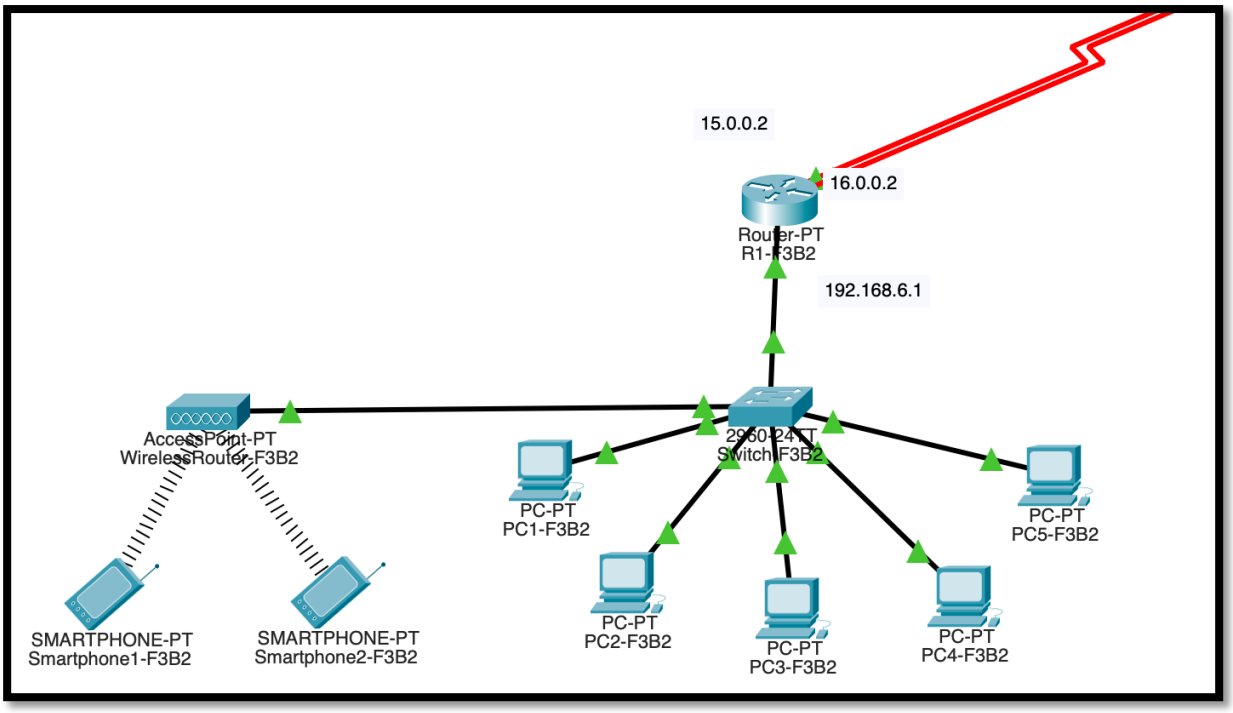


Figure 7: Branch 2 - Facility 3

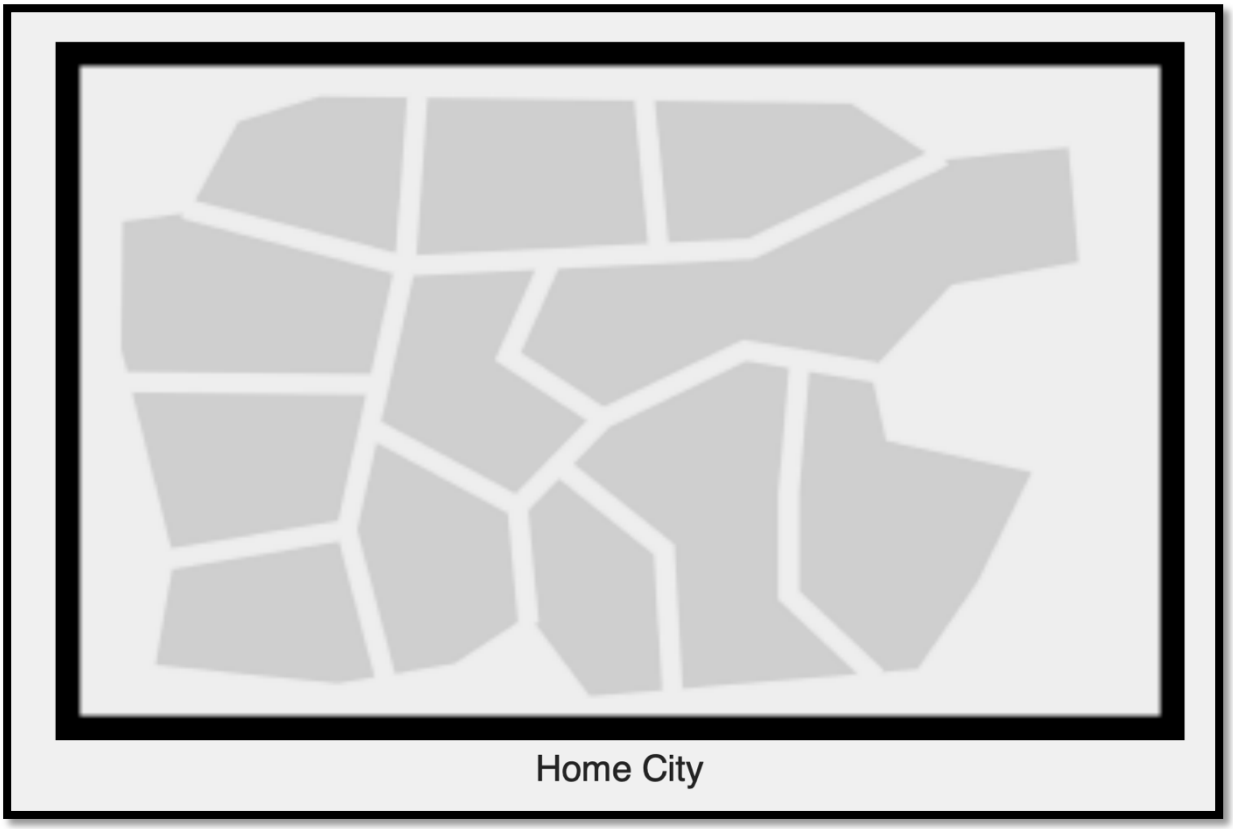


Figure 8: Physical Design of the System - Home City

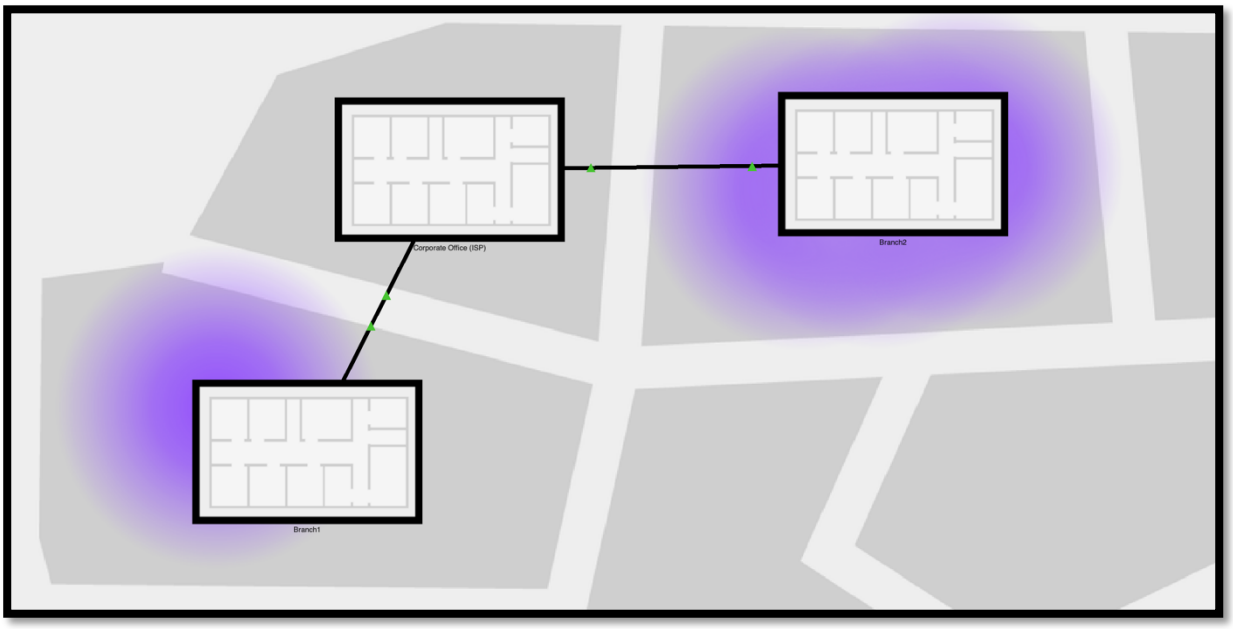


Figure 9: Physical Design of the System - Branches inside Home City

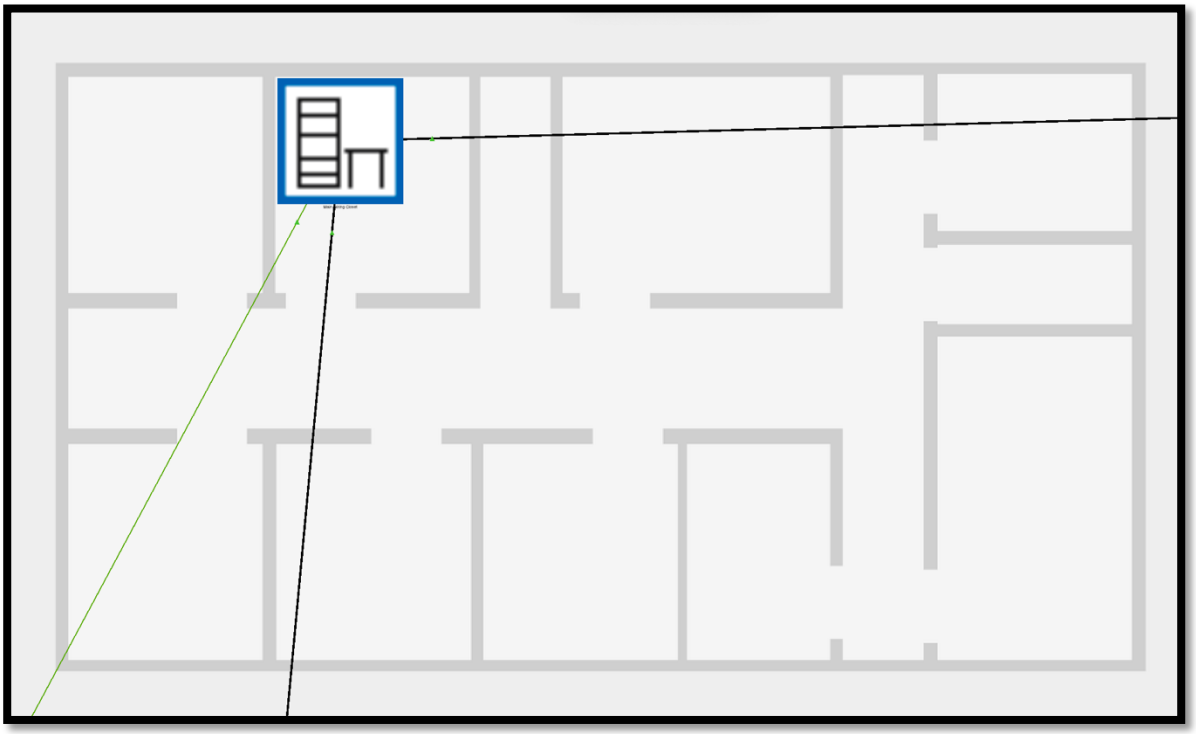


Figure 10: Physical Design of the System - Corporate Office (ISP)

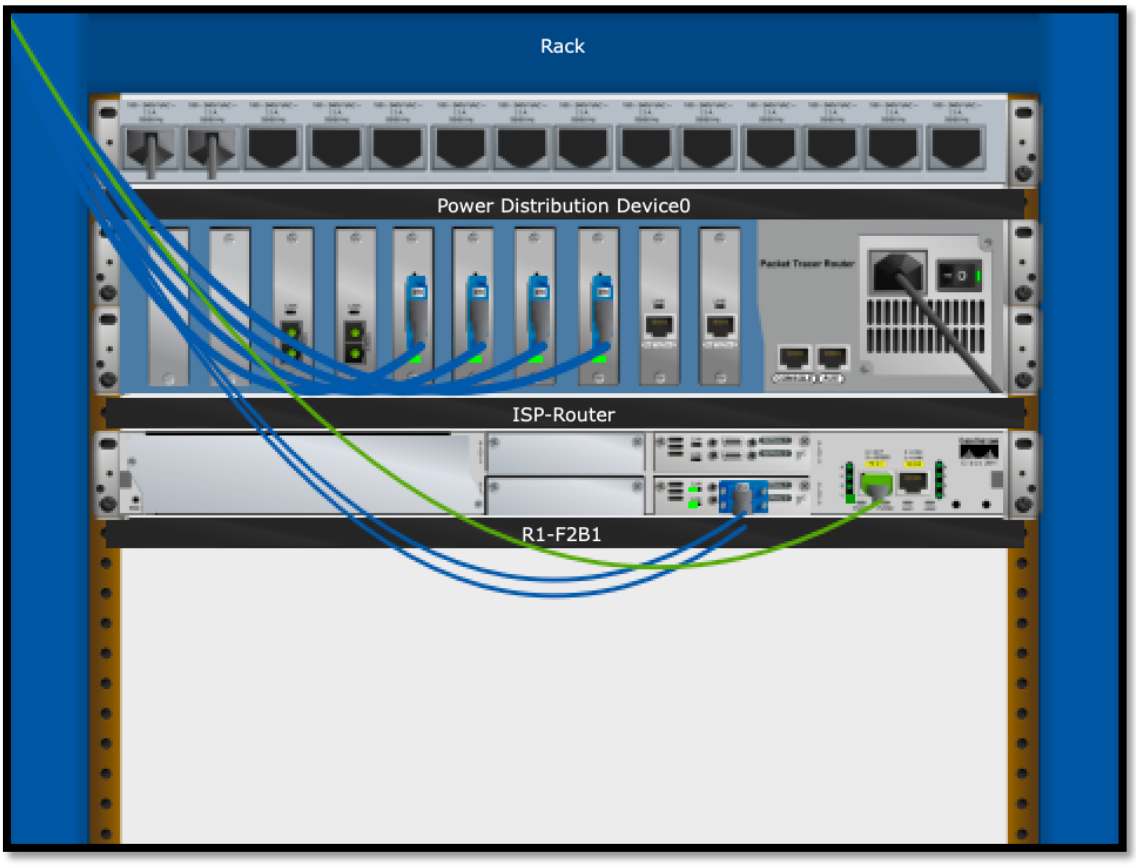


Figure 11: Physical Design of the System - Corporate Office (ISP) - Wiring Closet

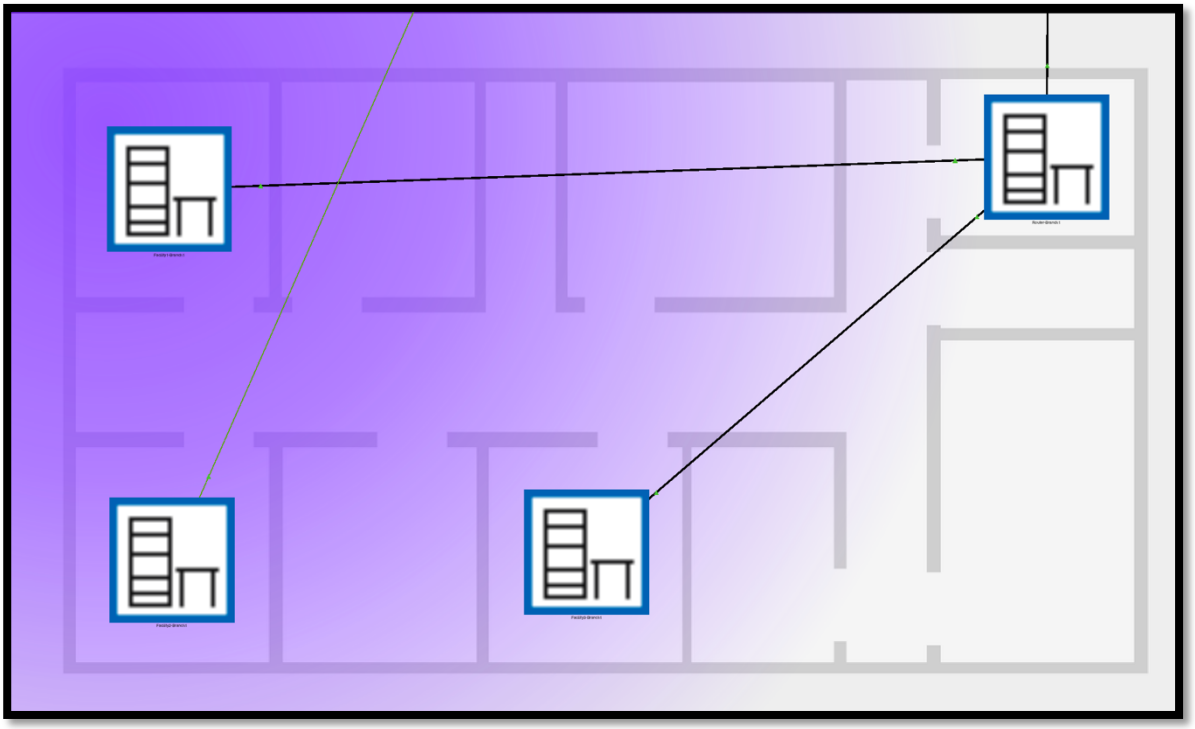


Figure 12: Physical Design of the System - Branch 1

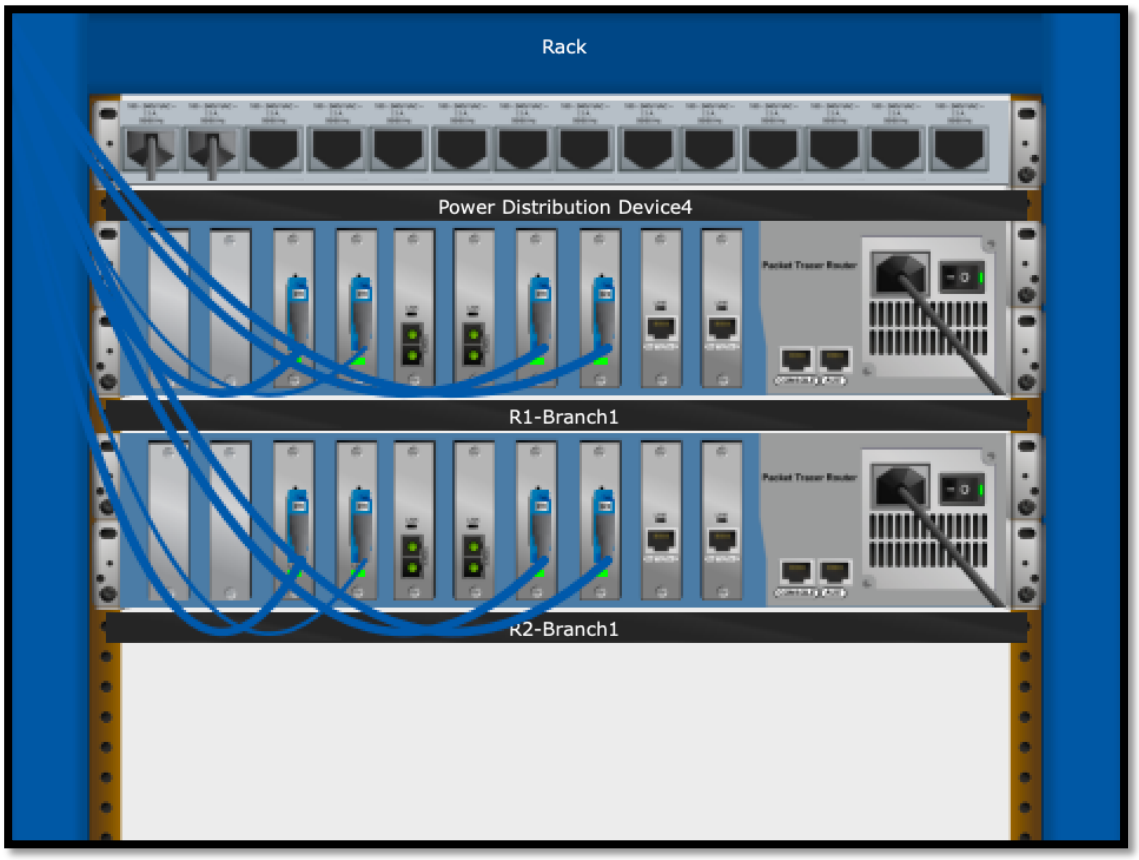


Figure 13: Physical Design of the System - Branch 1 – Router - Wiring Closet

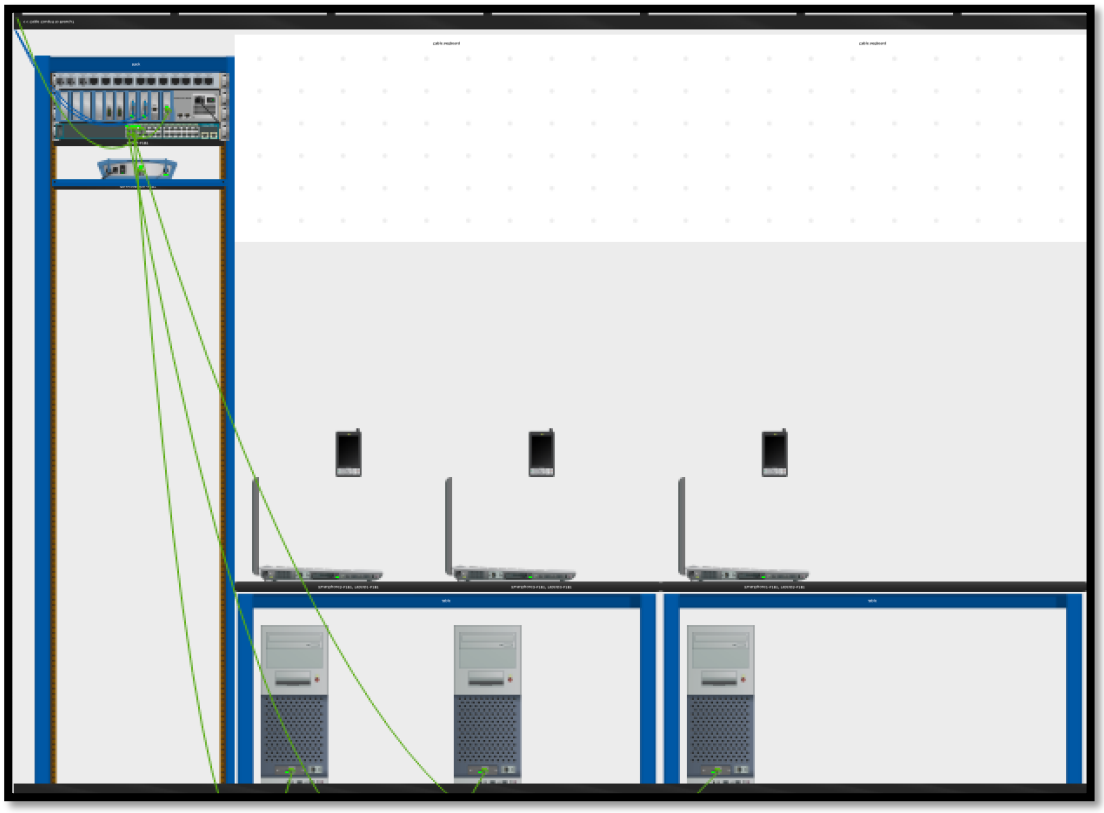


Figure 14: Physical Design of the System - Branch 1 - Facility 1 - Wiring Closet

Figure 15: Physical Design of the System - Branch 1 - Facility 2 - Wiring Closet

Figure 16: Physical Design of the System - Branch 1 - Facility 3 - Wiring Closet

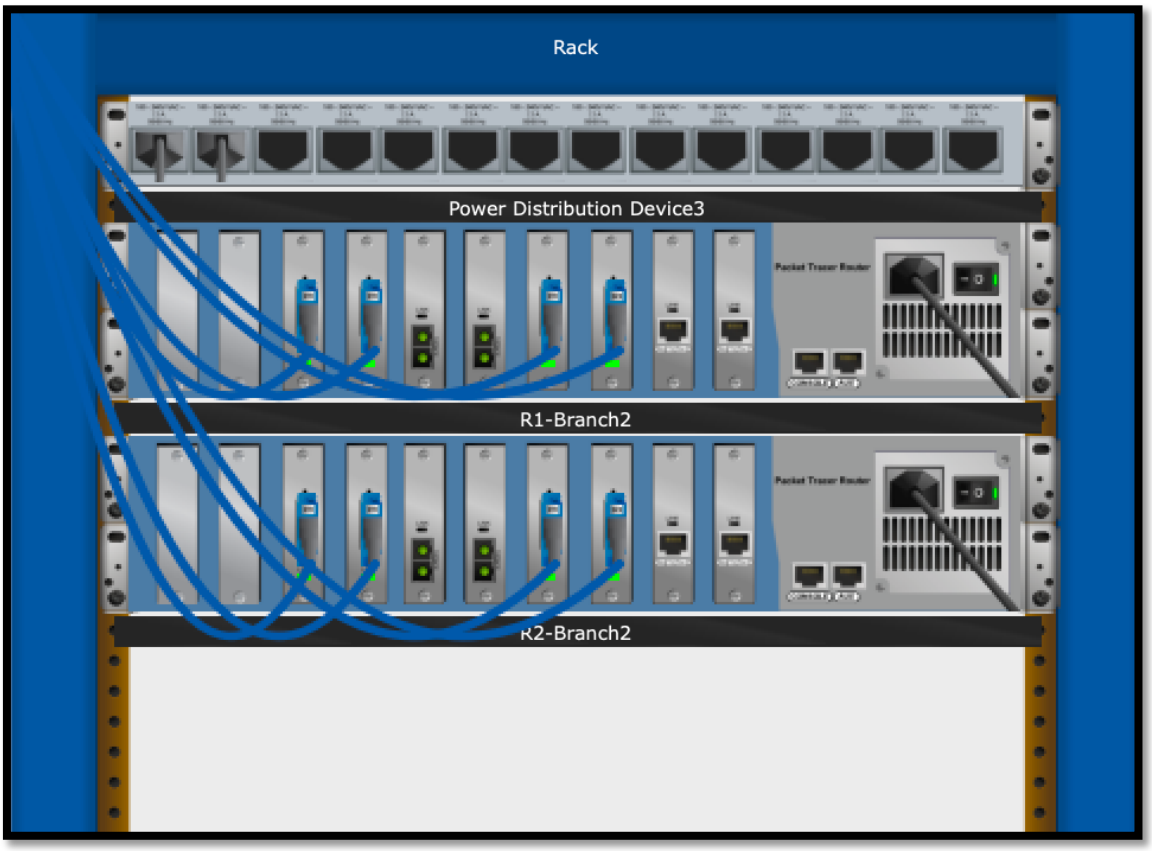


Figure 17: Physical Design of the System - Branch 2 – Router - Wiring Closet

Figure 18: Physical Design of the System - Branch 2 - Facility 1 - Wiring Closet

Figure 19: Physical Design of the System - Branch 2 - Facility 2 - Wiring Closet

Figure 20: Physical Design of the System - Branch 2 - Facility 3 - Wiring Closet

2.6. Simulation Elements

System entities:

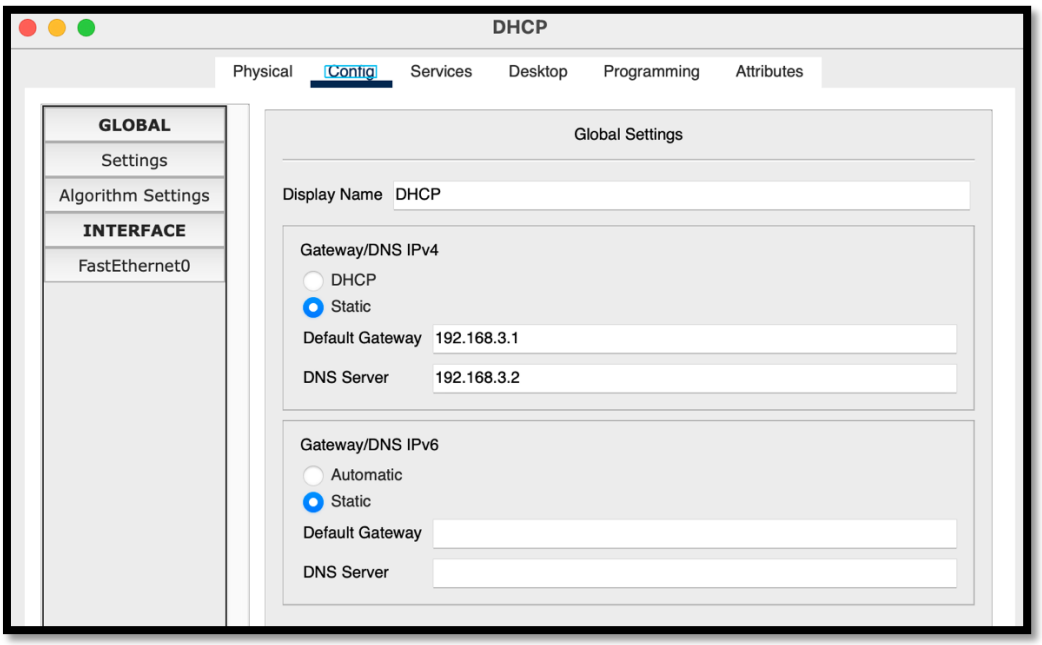


Figure 21: DHCP Server – Config

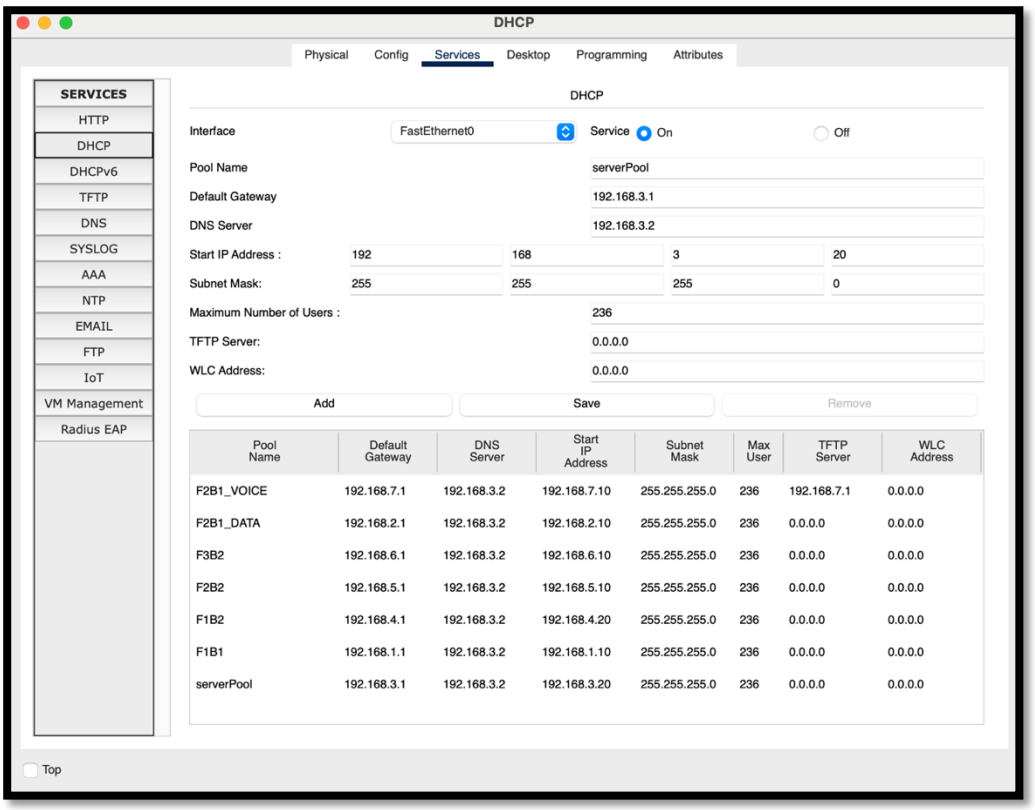


Figure 22: DHCP Server - Services

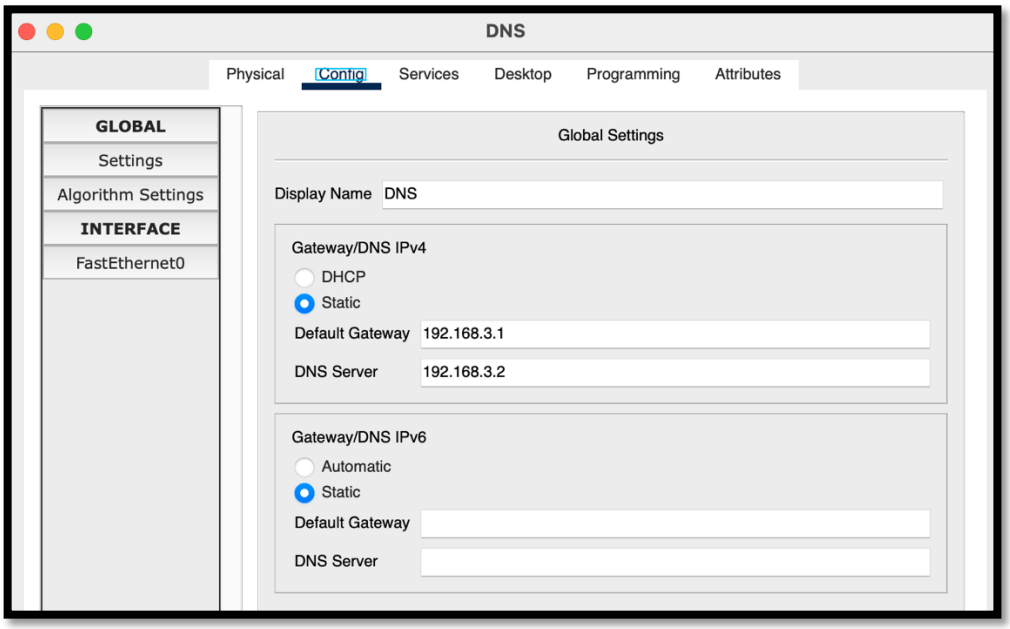


Figure 23: DNS Server - Config

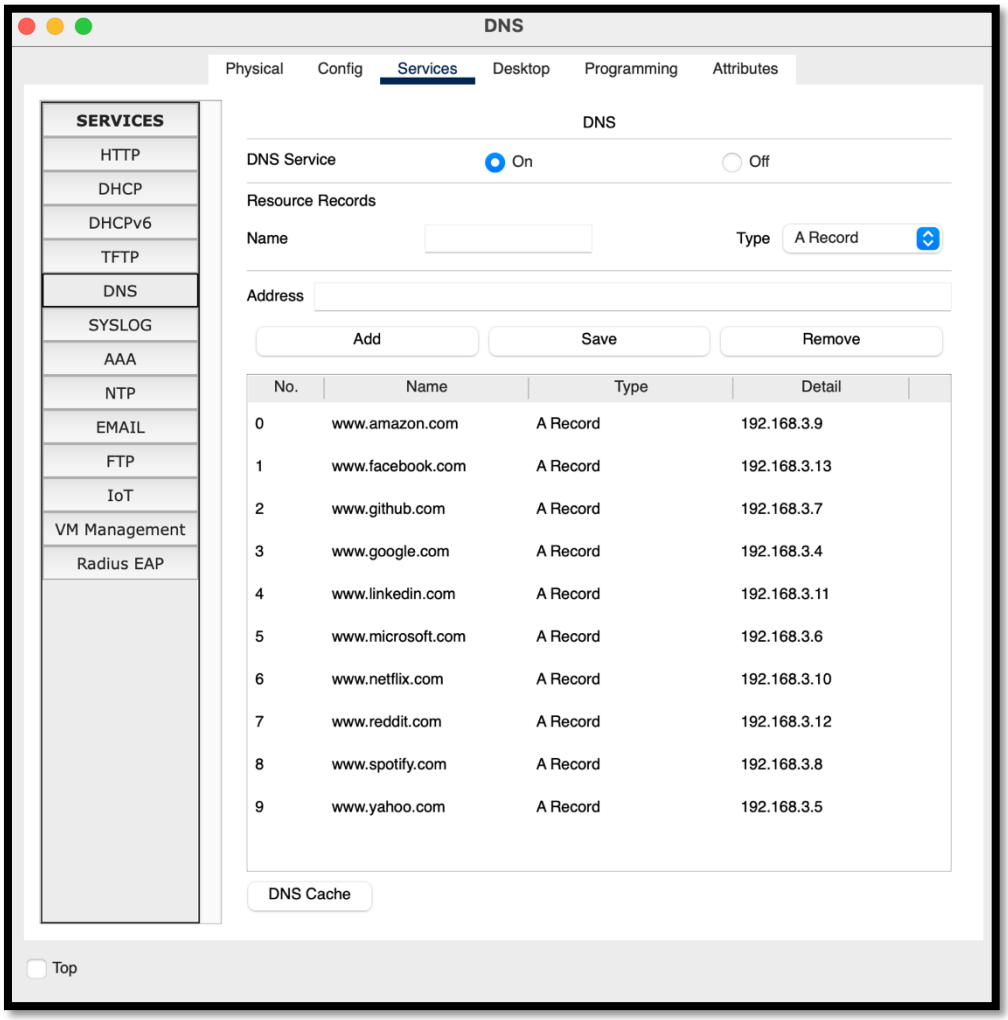


Figure 24: DNS Server - Services

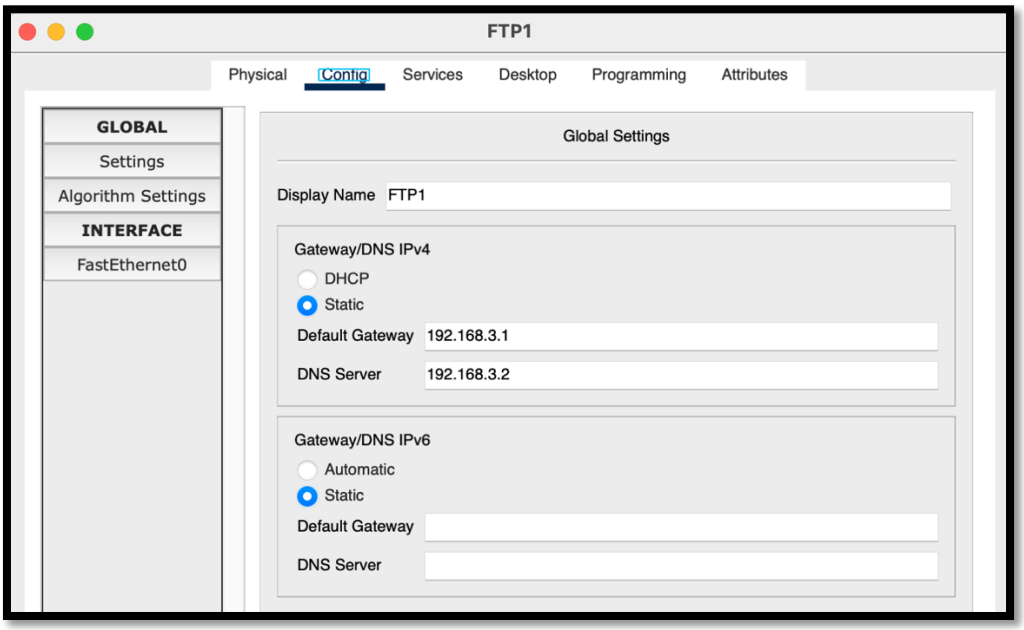


Figure 25: FTP1 Server – Config

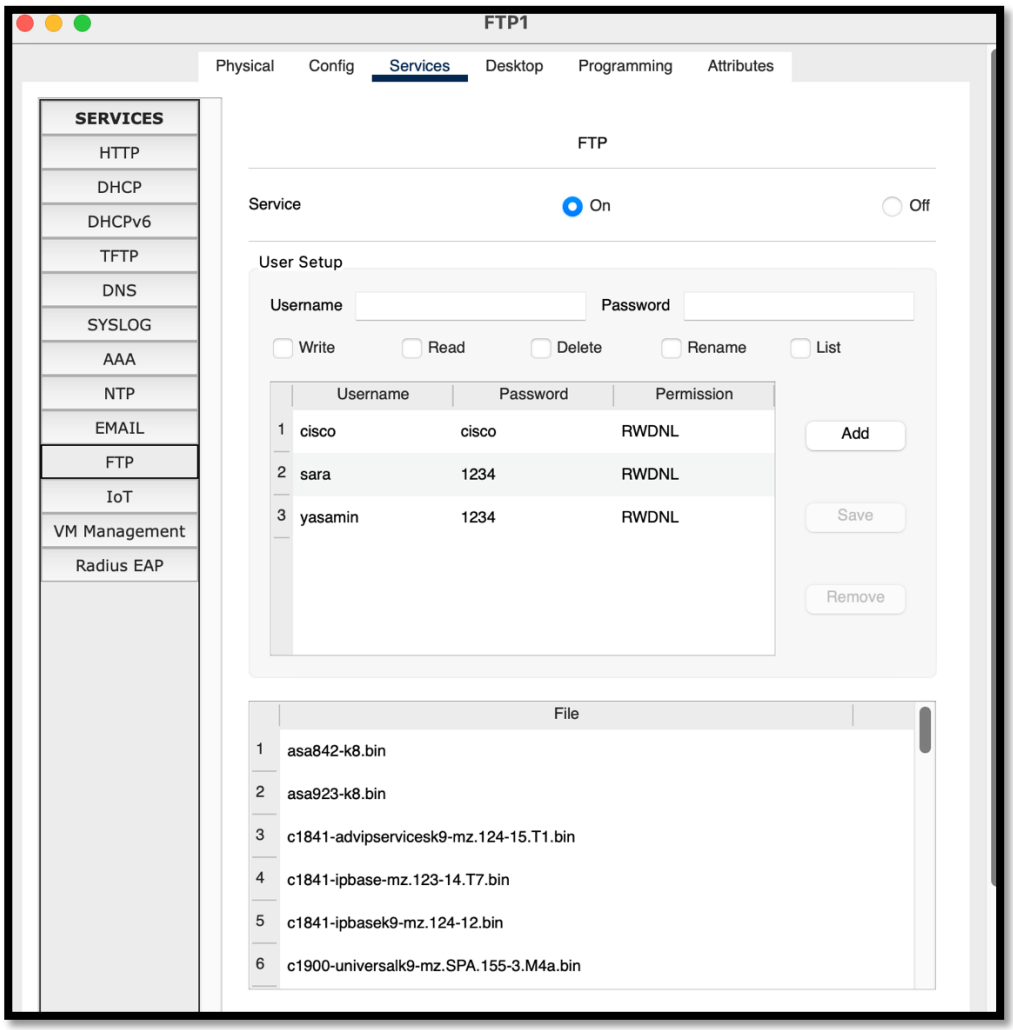


Figure 26: FTP1 Server - Services

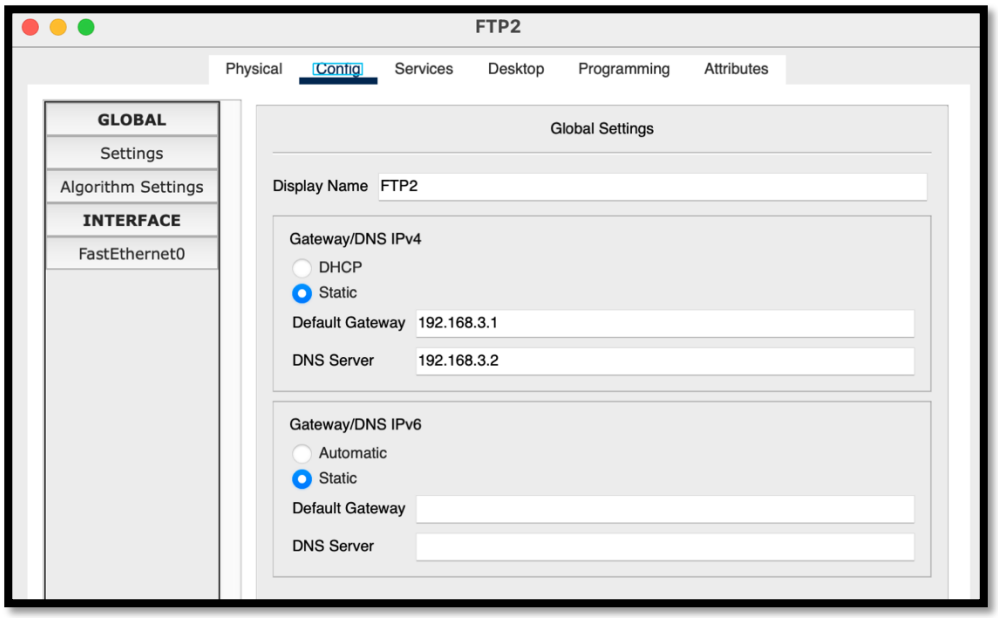


Figure 27: FTP2 Server – Config

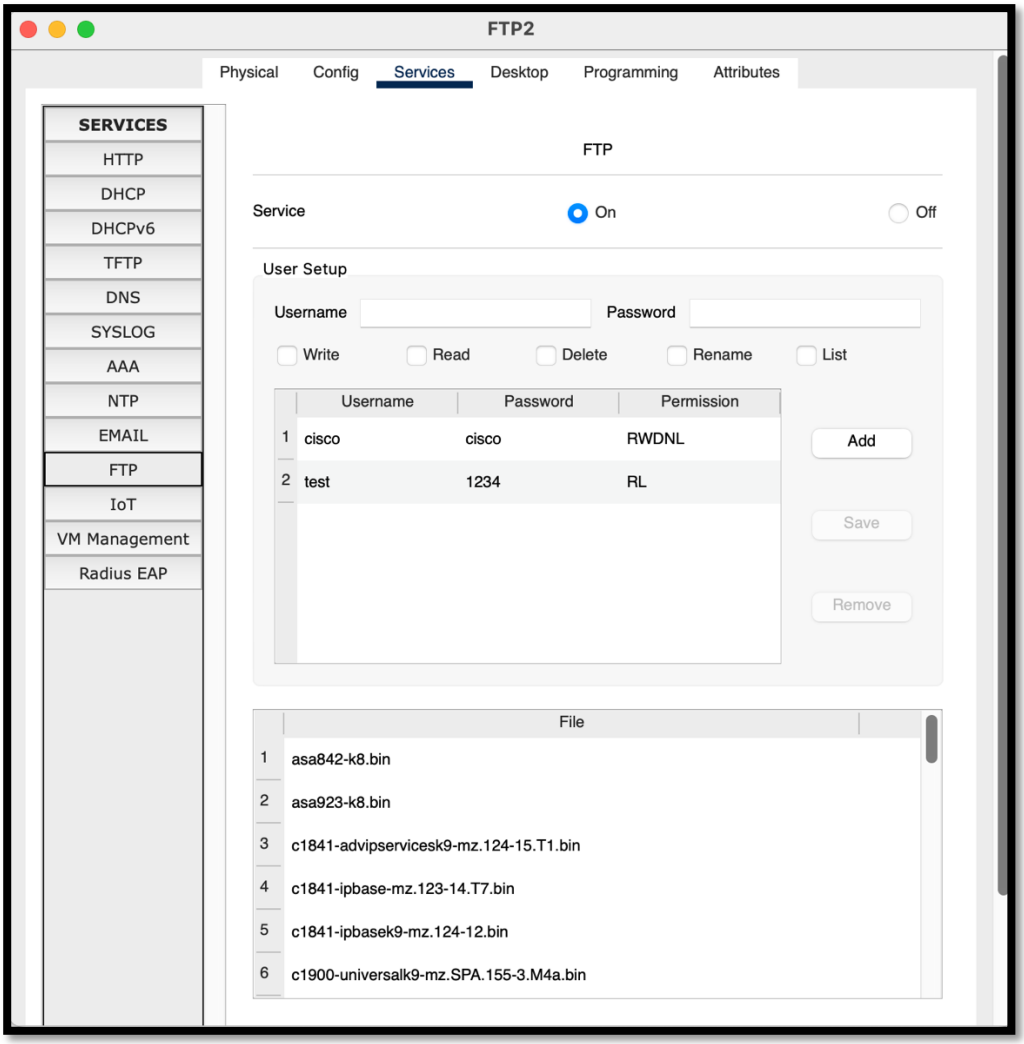


Figure 28: FTP2 Server - Services

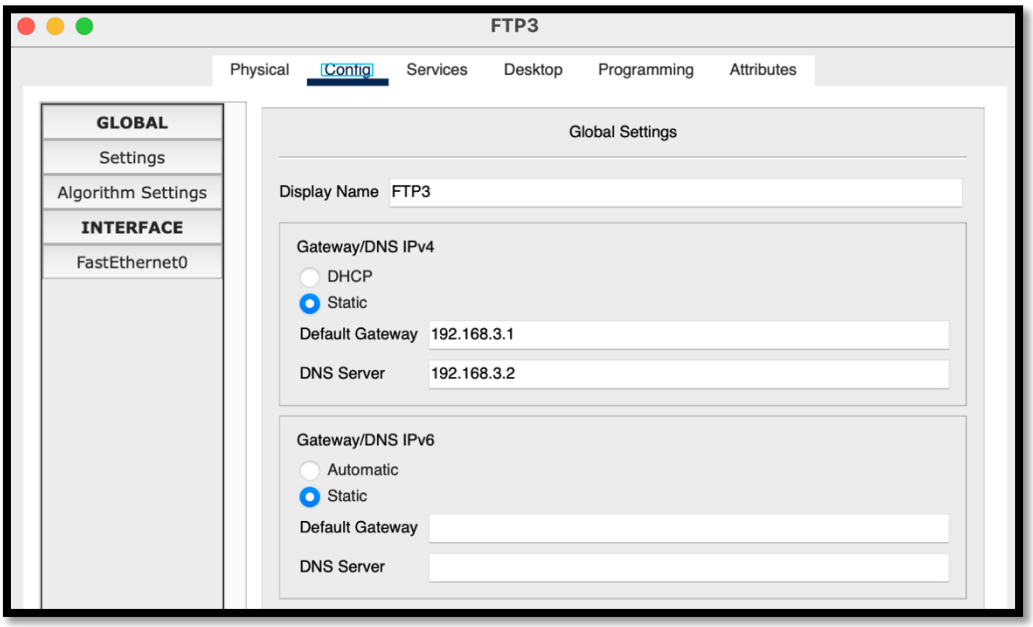


Figure 29: FTP3 Server – Config

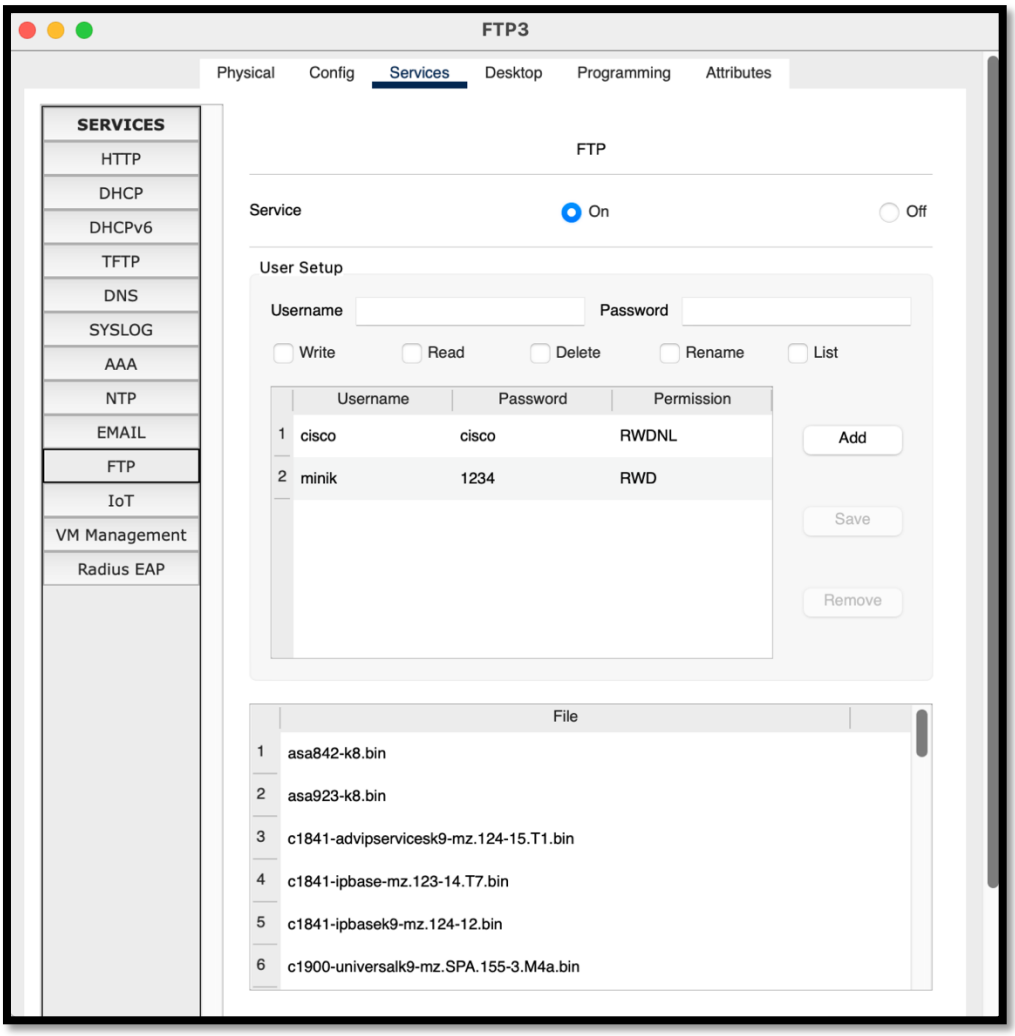


Figure 30: FTP3 Server - Services

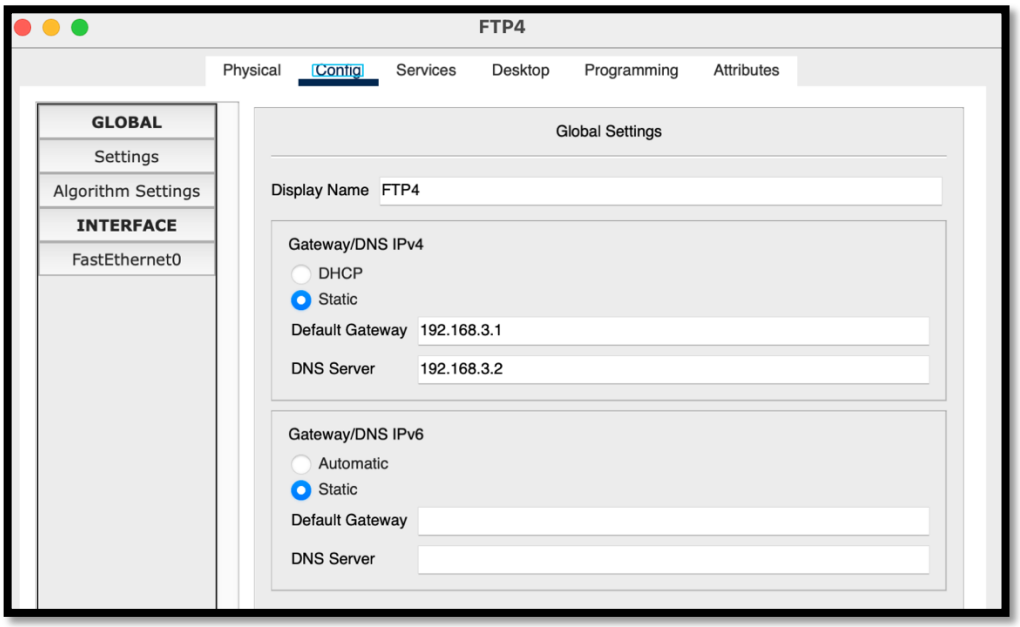


Figure 31: FTP4 Server – Config

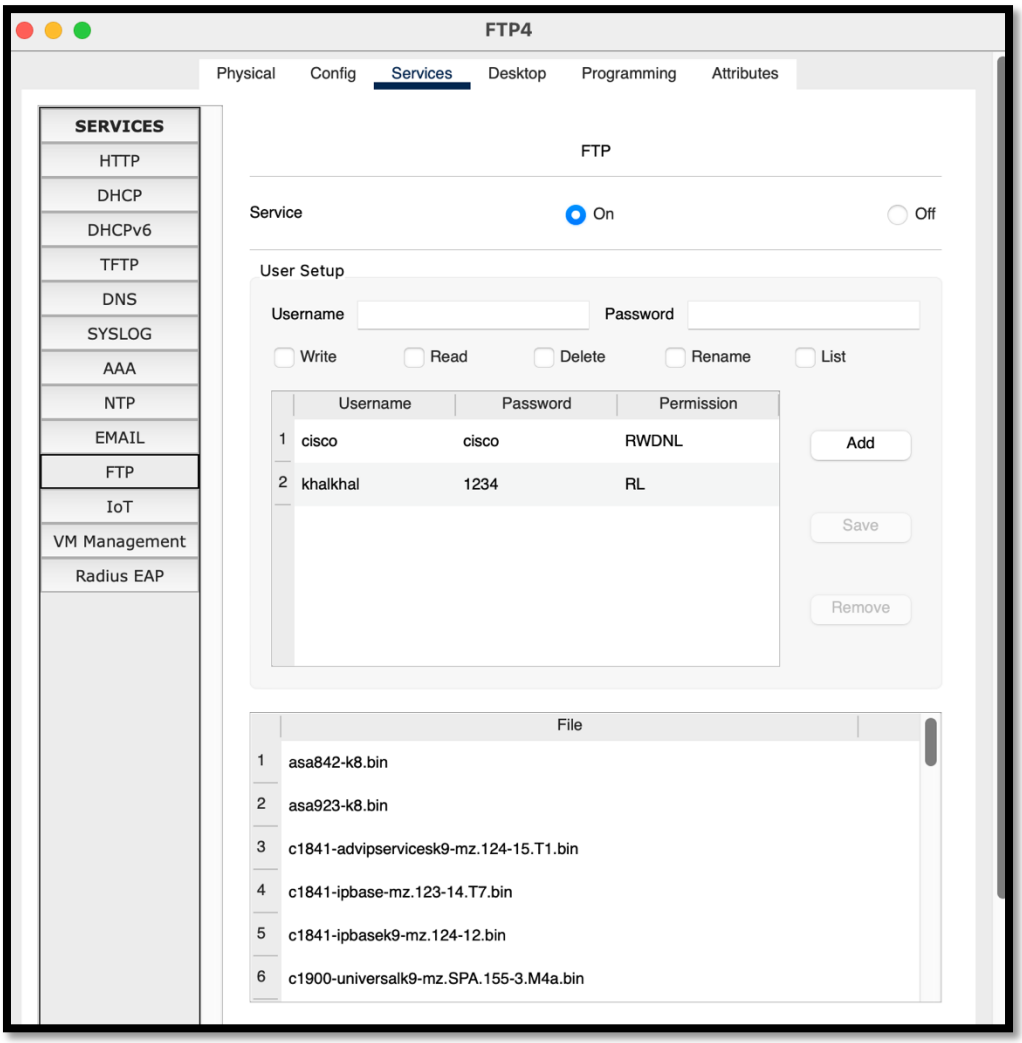


Figure 32: FTP4 Server - Services

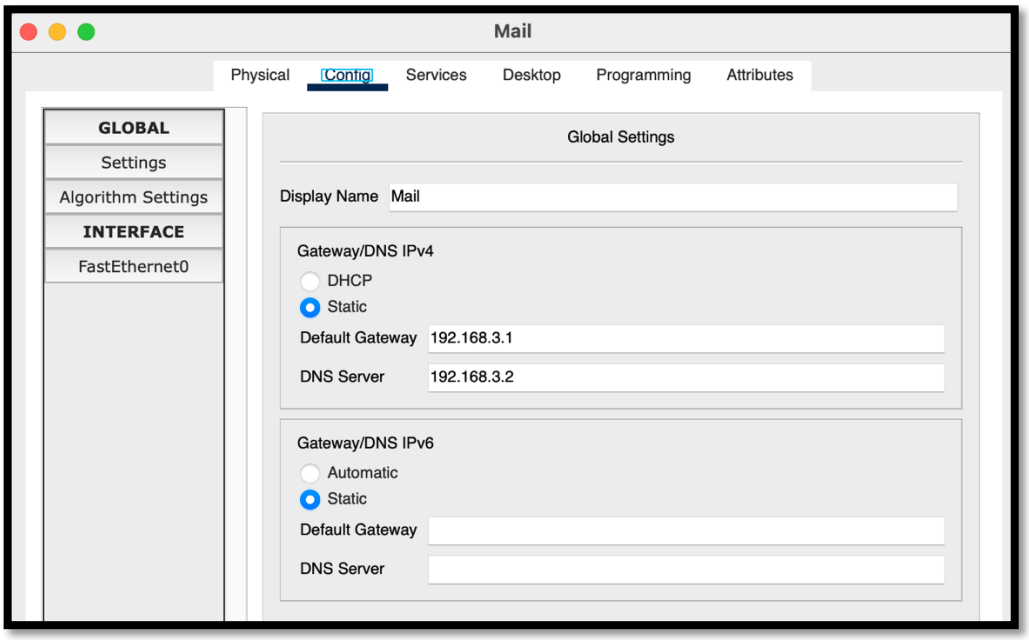


Figure 33: Mail Server - Config

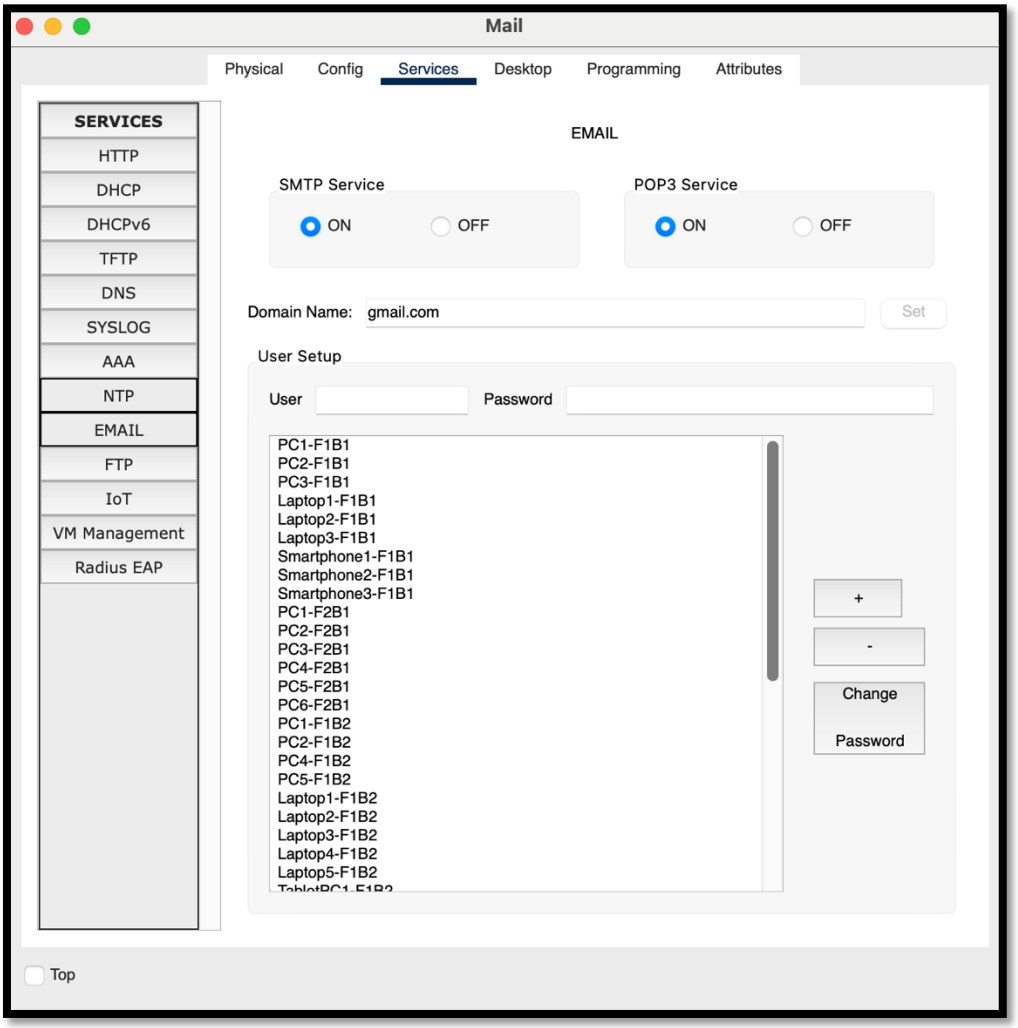


Figure 34: Mail Server – Services

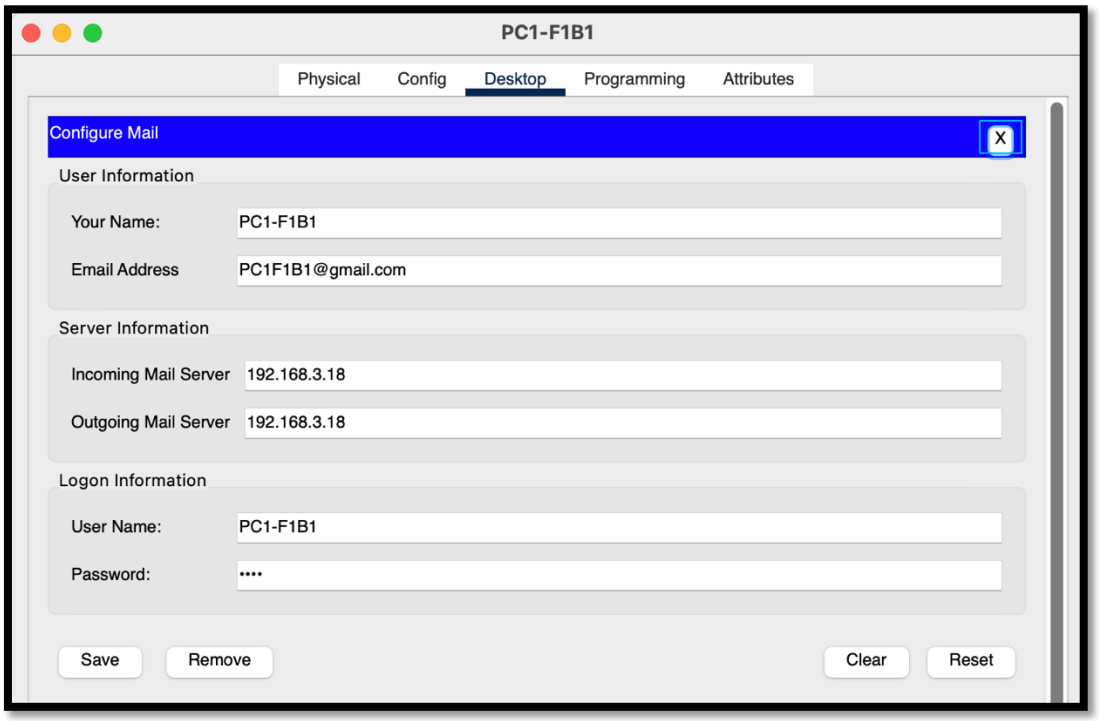


Figure 35: E-Mail Configuration Example for PC1-F1B1

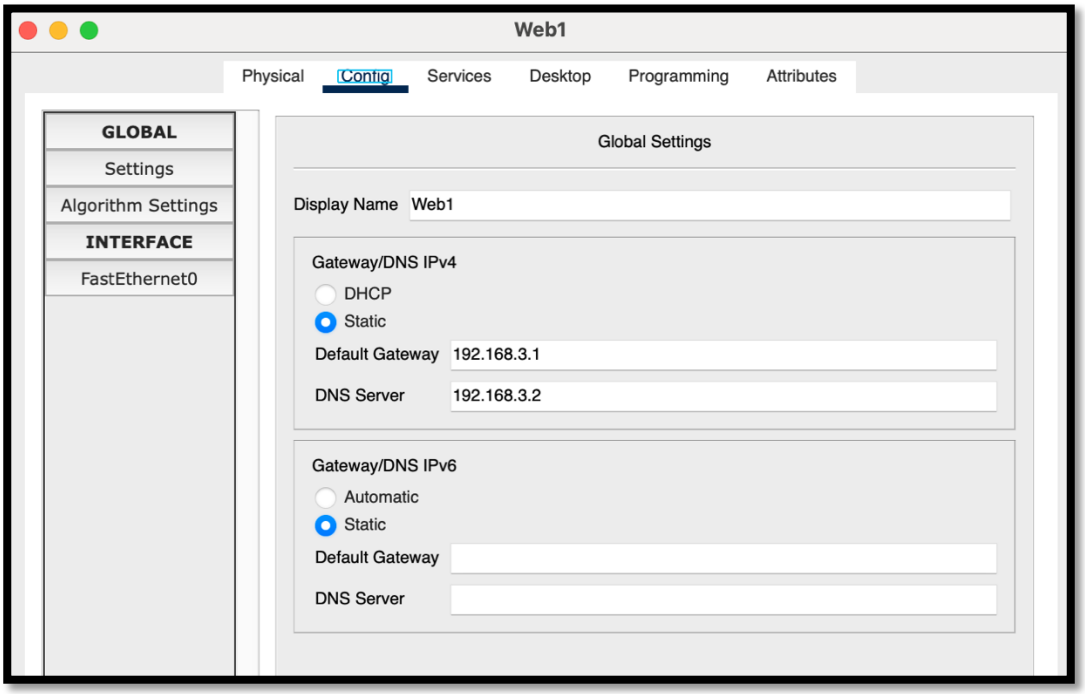


Figure 36: Web Server 1 (Google.com) – Config

In this Network exits 10 Web Server which all of them have the same config as Web Server 1, but they have different unique IPs.

CHAPTER THREE
TRAFFIC ANALYSIS AND SIMULATION RESULTS

Scenario 1: Email Communication and Web Access

A wireless user from first facility of second branch wants to read emails and browse Web.

A **wireless user from Facility 1 of Branch 2** wants to read emails and browse the Web. In this scenario, **Smartphone1-F1B1** composes and sends an email to **Laptop1-F1B2** using the centralized mail server. Later, **Laptop1-F1B2** accesses the network to retrieve and read the received email. Below is a detailed explanation of the **Email Process**:

📩 **Email Sending and Receiving Process**

📤 **Sending Email (Smartphone1-F1B1 → Mail Server):**

1. **DHCP Configuration:** Smartphone1-F1B1 connects to the wireless network and requests an IP address from the DHCP server. The server responds with an IP address, along with the default gateway and DNS server details.
2. **Mail Server Address Resolution (DNS):** The smartphone queries the DNS server to resolve the domain name of the mail server (e.g., mail.company.net; which in this example @google.com has been used.) to its IP address.
3. **Access Control (ACL):** Routers or switches apply Access Control Lists to verify whether Smartphone1-F1B1 is permitted to access the mail server. If allowed, the traffic is forwarded.
4. **TCP Session Initialization:** A TCP connection is established between the smartphone and the mail server using SMTP. TCP ensures reliable delivery of the outgoing message.
5. **Email Submission:** The smartphone submits the email to the mail server, which queues and stores the message in the inbox of the intended recipient — Laptop1-F1B2's account.
6. **Data Flow Through Network:**
    - The email originates from the smartphone and is passed through the **Facility 1 switch** and **Access Point (AP-PT)**.
    - It reaches the **local router**, then the **Branch 2 router**, followed by the **ISP router** (if external).
    - Finally, it reaches the **server farm router** and the **mail server** via the **server farm switch**.

Receiving Email (Laptop1-F1B2 → Mail Server):

1. **DHCP Initialization:** Laptop1-F1B2 connects to its local wireless network and receives an IP configuration from the DHCP server, enabling it to access network services.
2. **DNS Query:** Similar to the sending process, the laptop performs a DNS lookup to get the mail server's IP address.
3. **ACL Check:** ACLs on network devices ensure that the laptop is authorized to access the mail server for incoming email retrieval.
4. **TCP Connection Establishment:** The laptop initiates a secure TCP connection with the mail server to retrieve new messages.
5. **Fetching Email Content:** The mail server verifies the user credentials, checks the inbox, and sends the received email (originally sent from Smartphone1-F1B1) to the laptop's email client.
6. **Network Traversal:** The connection follows a similar path in reverse:
   from **Laptop1-F1B2 → Facility 2 switch and AP → local router → Branch 2 router → ISP → server farm router → mail server**.

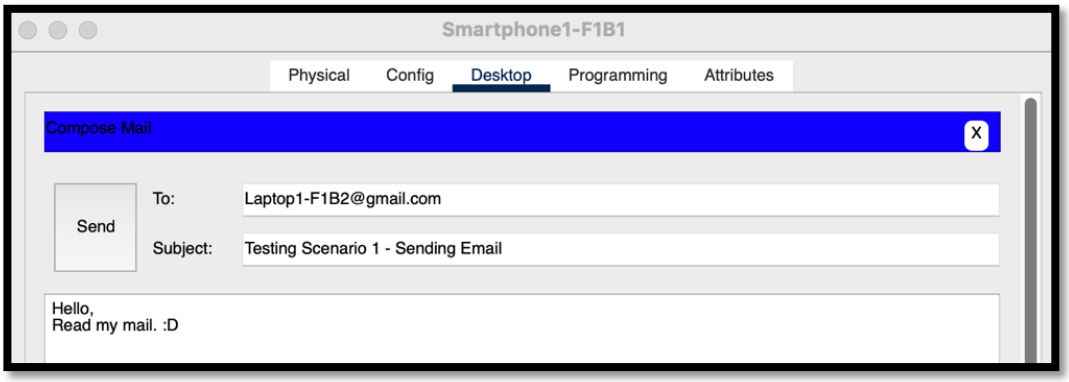


Figure 37: Composing an email from Smartphone1-F1B1 to Laptop1-F1B2

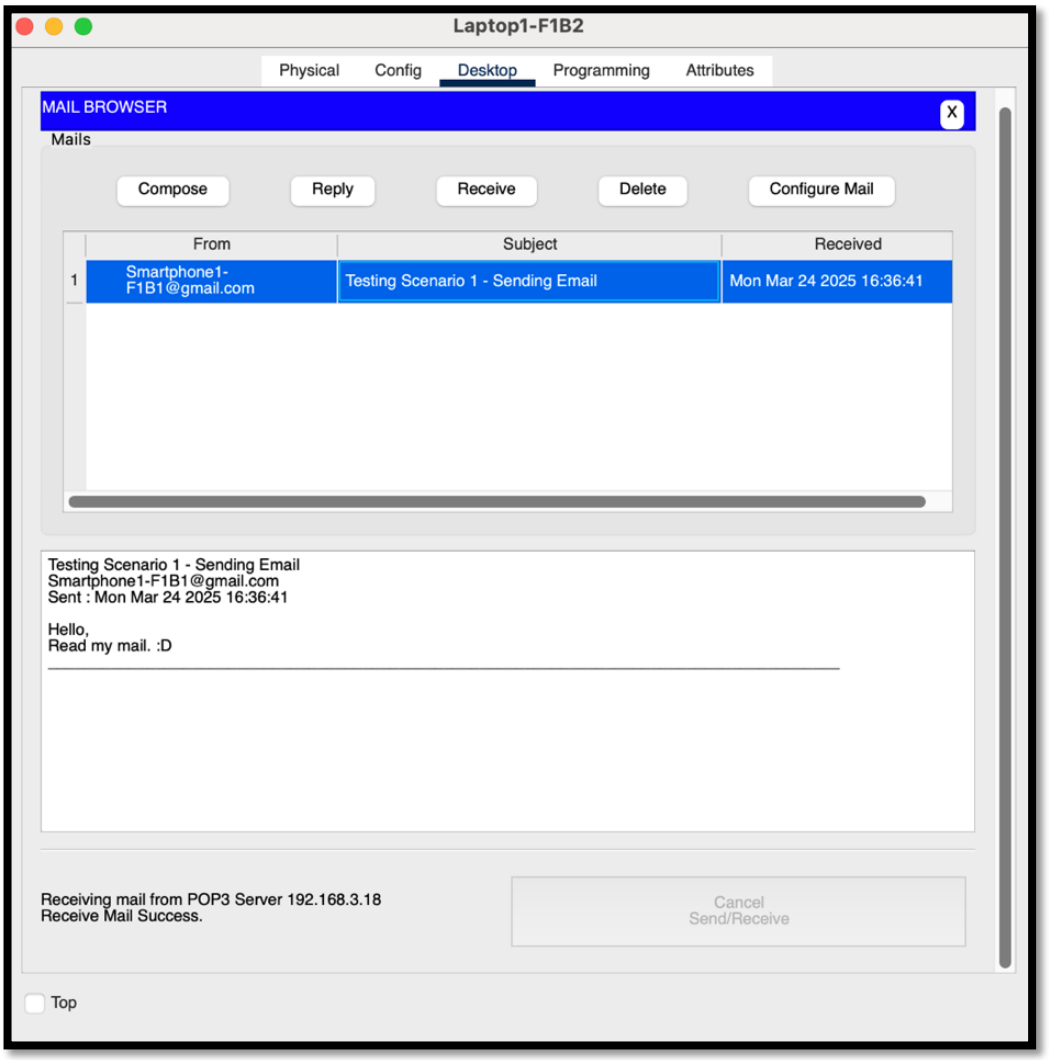


Figure 38: Receive an email in Branch 2

Figure 38 shows the received email that has been send from branch 1 to the branch 2.

The following is the Result of the Simulation of sending/receiving Email process:

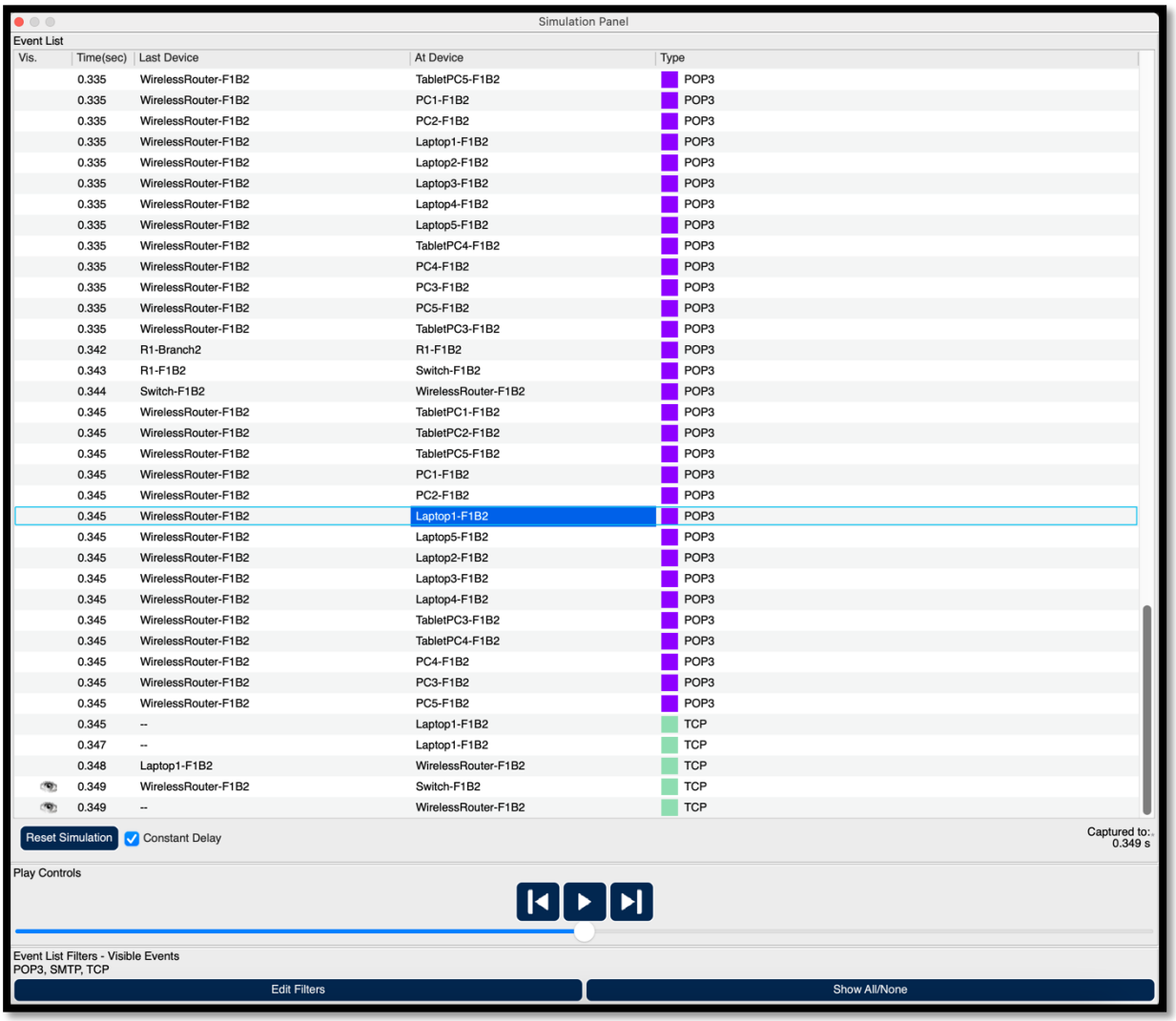


Figure 39: Simulation Panel

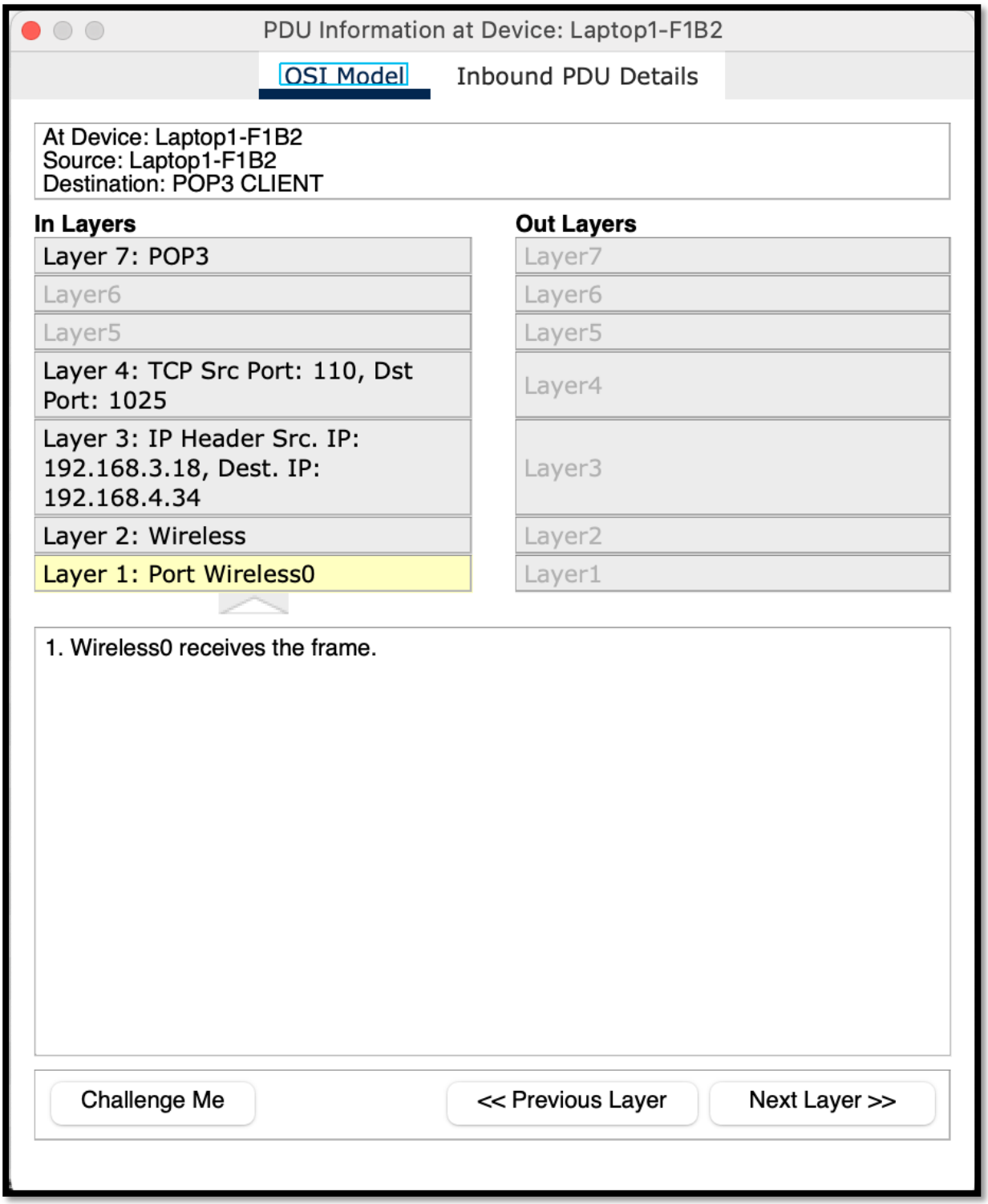


Figure 40: PDU Information at Device - Laptop1-F1B2 – OSI Model

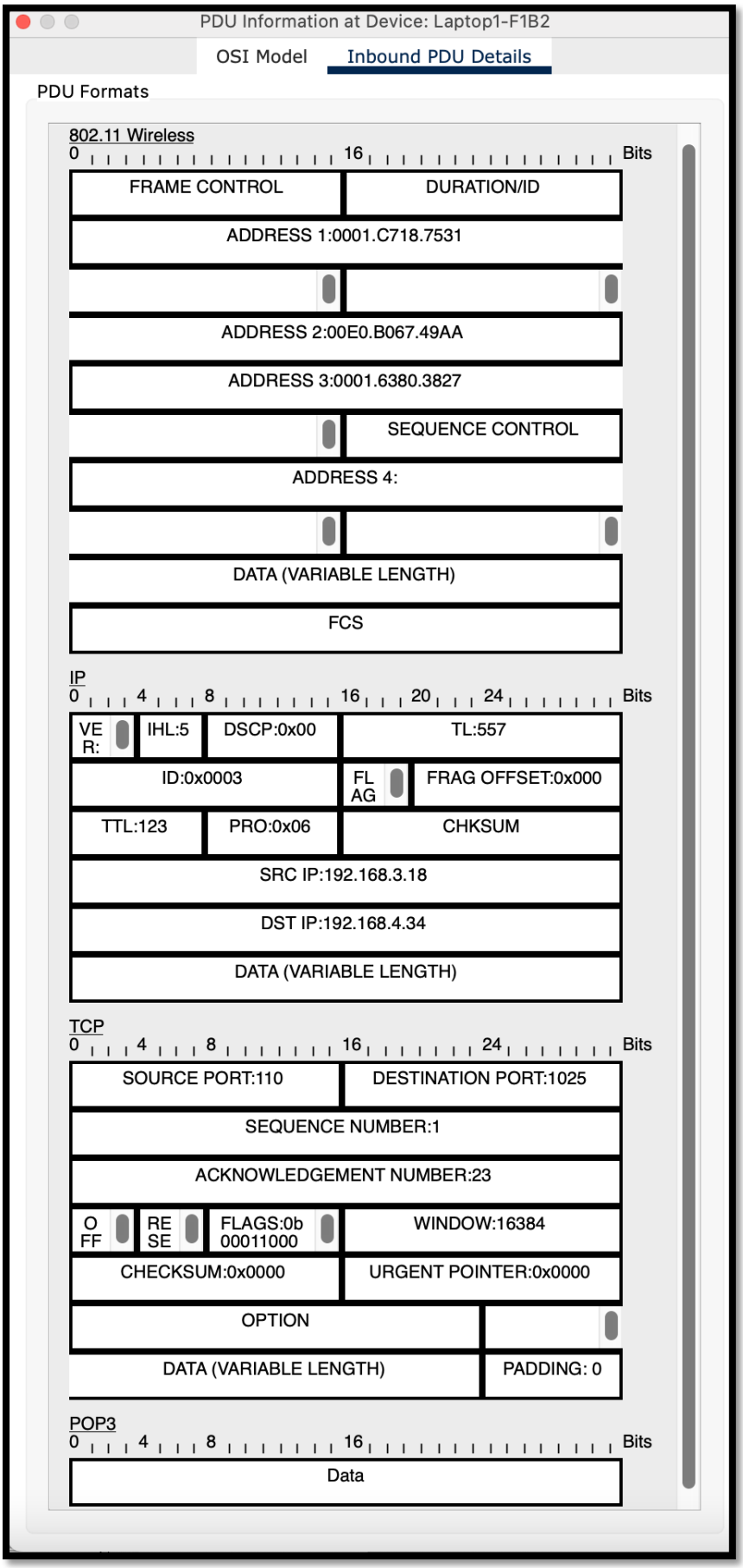


Figure 41: PDU Information at Device - Laptop1-F1B2 – Inbound PDU details

🌐 Web Browsing Process – Scenario 1 (Wireless User: Facility 1, Branch 2)

After sending and receiving emails, the user from **Laptop1-F1B1** now wants to browse websites using their mobile browser. The steps below explain how the web browsing request is processed through the network:

1. **DHCP Configuration:**
   When Laptop1-F1B1 connects to the wireless access point, it requests an IP address and network settings. The DHCP server assigns the IP address, subnet mask, default gateway, and DNS server, allowing the device to access internal and external network resources.

2. **Domain Name Resolution (DNS Lookup):**
   The user enters a website address (e.g., www.google.com) in the browser. To locate the server, the laptop sends a DNS query to resolve the domain name into an IP address. The DNS server (assigned via DHCP) responds with the destination web server's IP.

3. **Access Control Enforcement (ACL):**
   Before outbound traffic leaves the local network, routers or firewalls apply Access Control Lists. These ACLs check whether Laptop1-F1B1 is authorized to access websites on the internet. If permitted, the connection request is allowed to continue.

4. **TCP Connection and Secure Session Establishment:**
   The Laptop initiates a TCP handshake with the web server using port 80 (HTTP) or port 443 (HTTPS). In most cases, HTTPS is used, and a TLS handshake is performed to establish a secure, encrypted session between the client and server.

5. **Web Request and Response:**
   Once the connection is established, the browser sends an HTTP request to fetch the desired webpage. The web server processes the request and sends back the webpage's content — including HTML, CSS, images, scripts, and other assets — for the browser to render.

6. **Network Path Traversal:**
   - The request flows from **Laptop1-F1B1** through the **Facility 1 switch**.
   - It passes the **Access Point (AP-PT)** and reaches the **local router**.
   - From there, the data is forwarded to the **Branch 2 router**, then to the **ISP router**.
   - The ISP routes the packets over the internet to the **destination web server**.
   - The web server's response follows the reverse path back to the laptop.

7. **Page Rendering:**
   The browser on Laptop1-F1B1 processes the server's response and displays the website to the user. As the user navigates the site, additional requests are made and follow the same path.

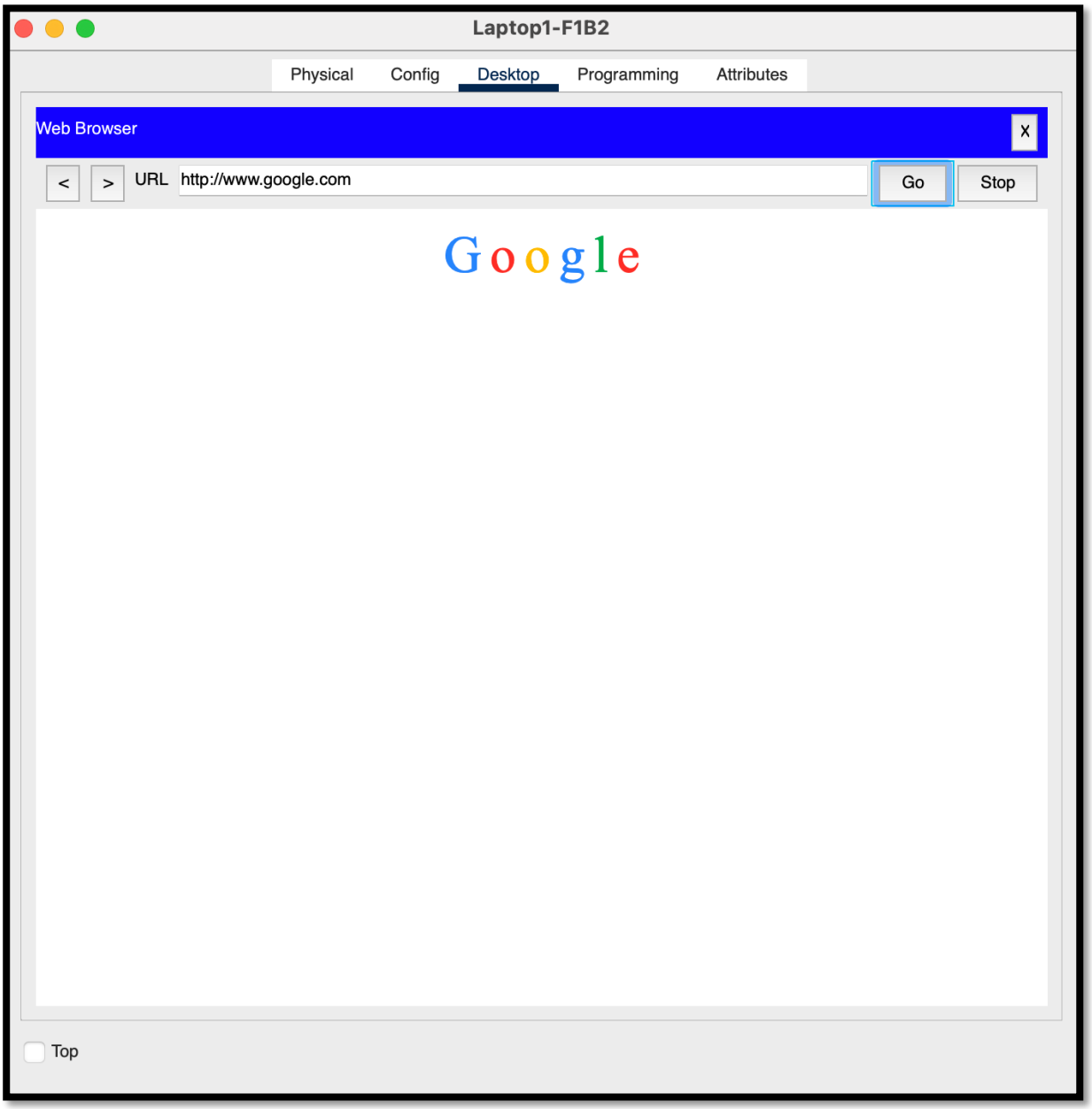


Figure 42: Browsing Web

The following is the Result of the Realtime and Simulation of Web Browsing process:

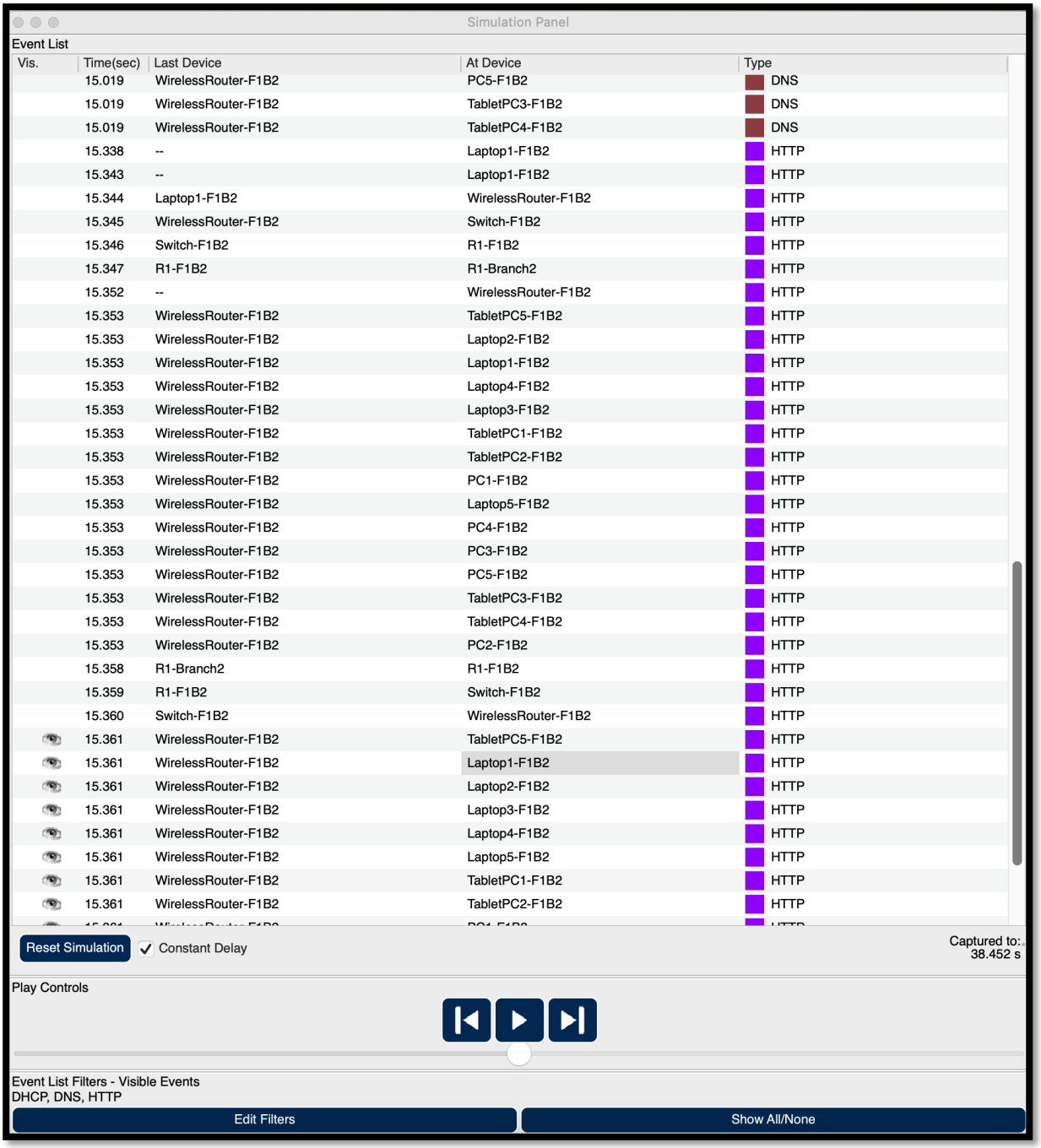


Figure 43: Simulation Panel

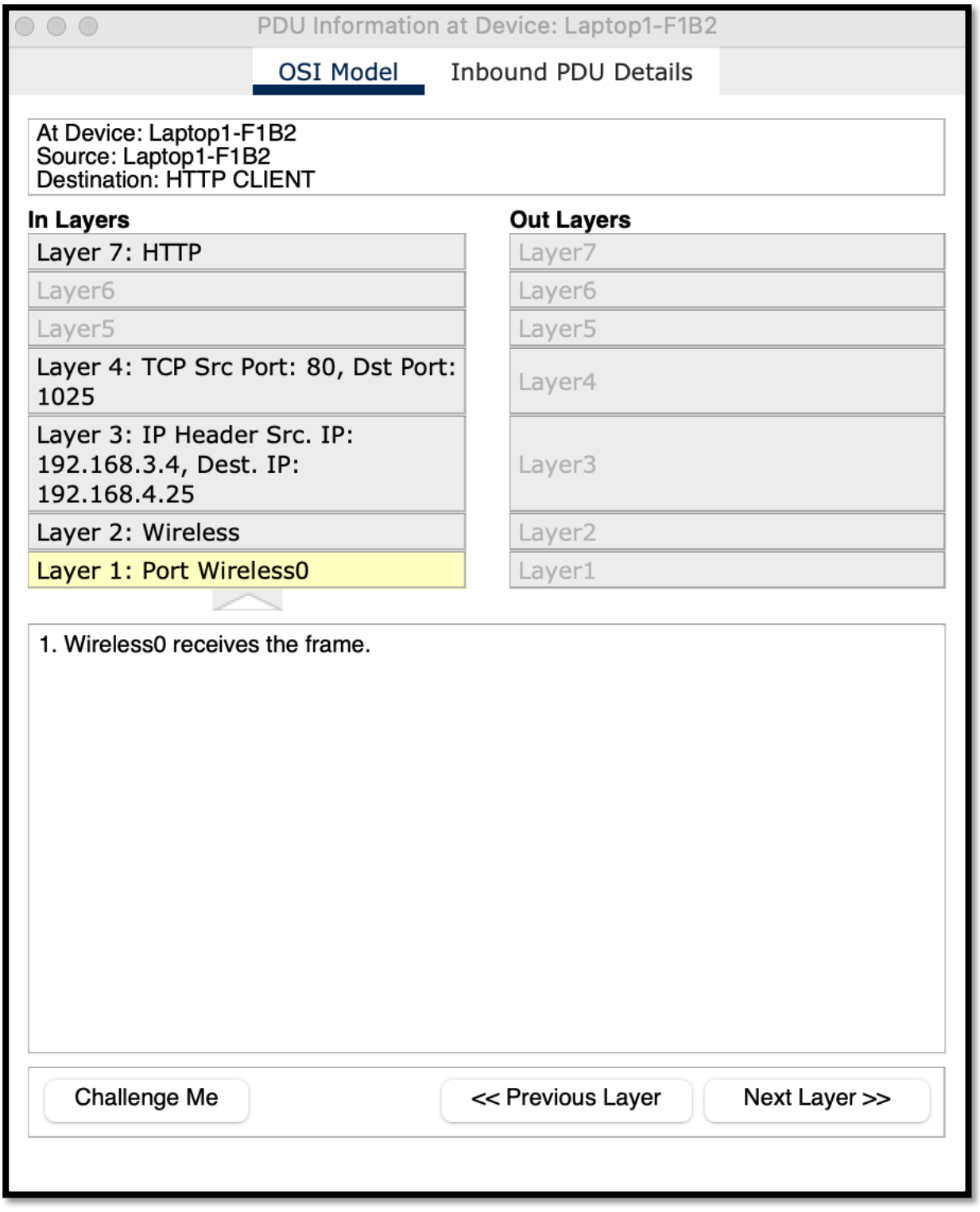


Figure 44: PDU Information at Device - Laptop1-F1B2 – OSI Model

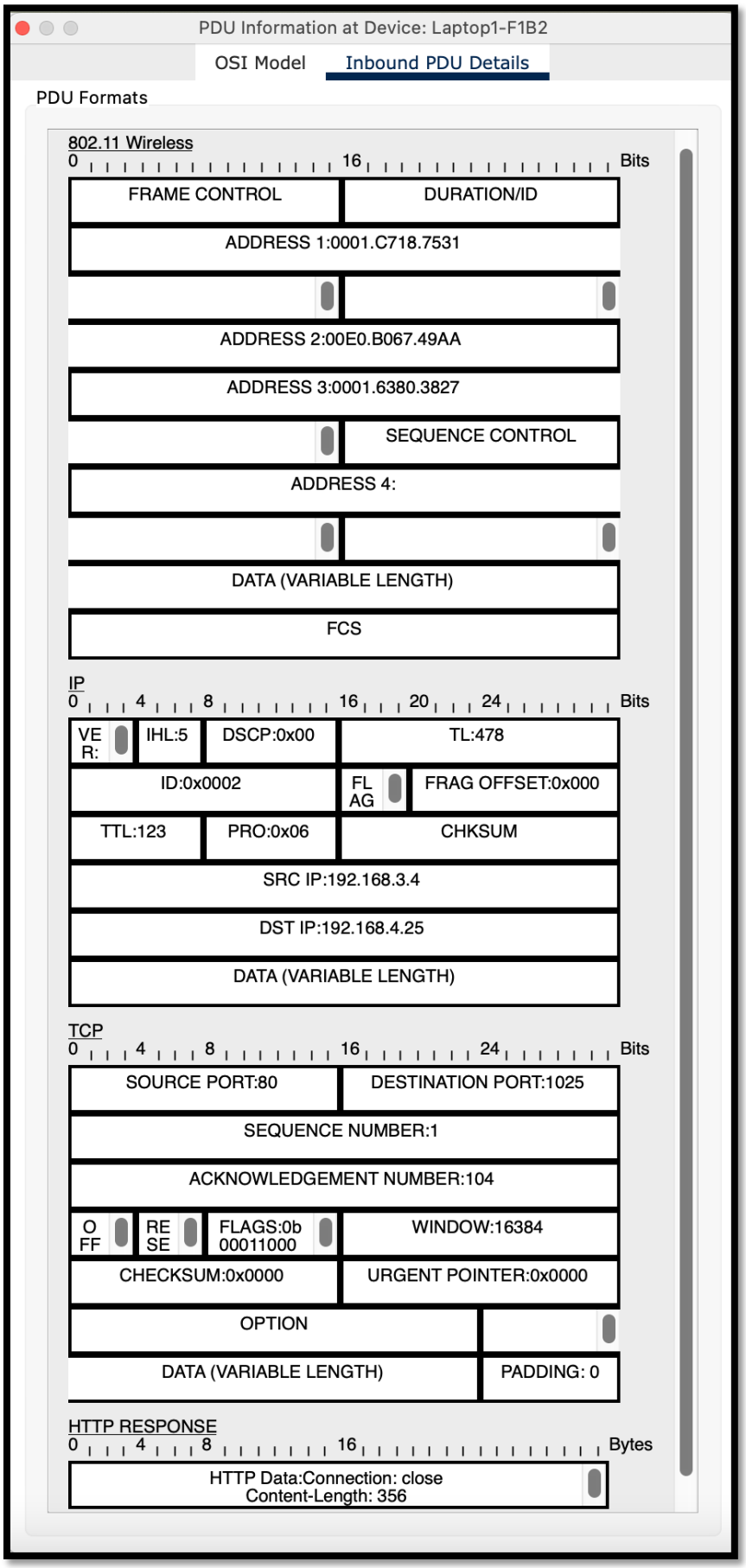


Figure 45: PDU Information at Device - Laptop1-F1B2 – Inbound PDU details

Scenario 2: FTP File Transfer Between Branch Facilities

A computer engineer from the second facility of the second branch developed a web application and wants to send his/her code files to an FTP server in the third facility of the first branch.

A **computer engineer working on PC1-F2B2** (Second Facility, Branch 2) has developed a web application and intends to **transfer code files to an FTP server (FTP1) located in the Third Facility of Branch 1**. Below is a step-by-step description of the **File Transfer Process**:

📁 **File Transfer Process (PC1-F2B2 → FTP1)**

🖥️ **1. Establishing Network Connectivity:**

- When PC1-F2B2 boots up and joins the local wired network, it automatically sends a DHCP request.
- The **DHCP server** responds by assigning an IP address along with the subnet mask, gateway, and DNS configuration, enabling the PC to access internal and external network resources.

🔐 **2. FTP Server Authentication:**

- The engineer launches an FTP client (or uses a terminal) and initiates a connection to the FTP server's domain or IP.
- To gain access, valid **login credentials** are required. These credentials are verified by the FTP1 server before the file transfer can proceed.

📡 **3. Routing and Network Path Determination:**

- The internal routing protocol, such as **RIP (Routing Information Protocol)**, calculates the most efficient path for data packets from Branch 2 to Branch 1.
- Packets are forwarded through the **local facility switch**, then pass through the **Branch 2 router**.
- From there, they traverse the **inter-branch link**, reaching the **Branch 1 core router**, and finally arrive at the **local router and switch of Facility 3**, where the FTP server is hosted.

🔒 **4. Security and Traffic Control:**

- Before traffic is allowed between facilities, **Access Control Lists (ACLs)** on intermediary routers and firewalls examine the source, destination, and service port (commonly port 21 for FTP or port 22 for SFTP).
- If **SFTP (Secure FTP)** is used instead of plain FTP, encryption protocols like SSH are employed to protect the data during transit.

🔁 **5. Data Transmission:**

- After authentication and access are verified, the engineer begins uploading code files.
- The FTP client divides large files into packets and sends them sequentially over a **reliable TCP connection**, ensuring complete and ordered delivery.

🔄 6. Final Delivery and Storage:

- Packets arrive at **FTP1** via the **Facility 3 switch**, and the FTP server reassembles them into the original files.
- The server stores the files in the designated user directory or shared project space, making them available for deployment, backup, or team collaboration.

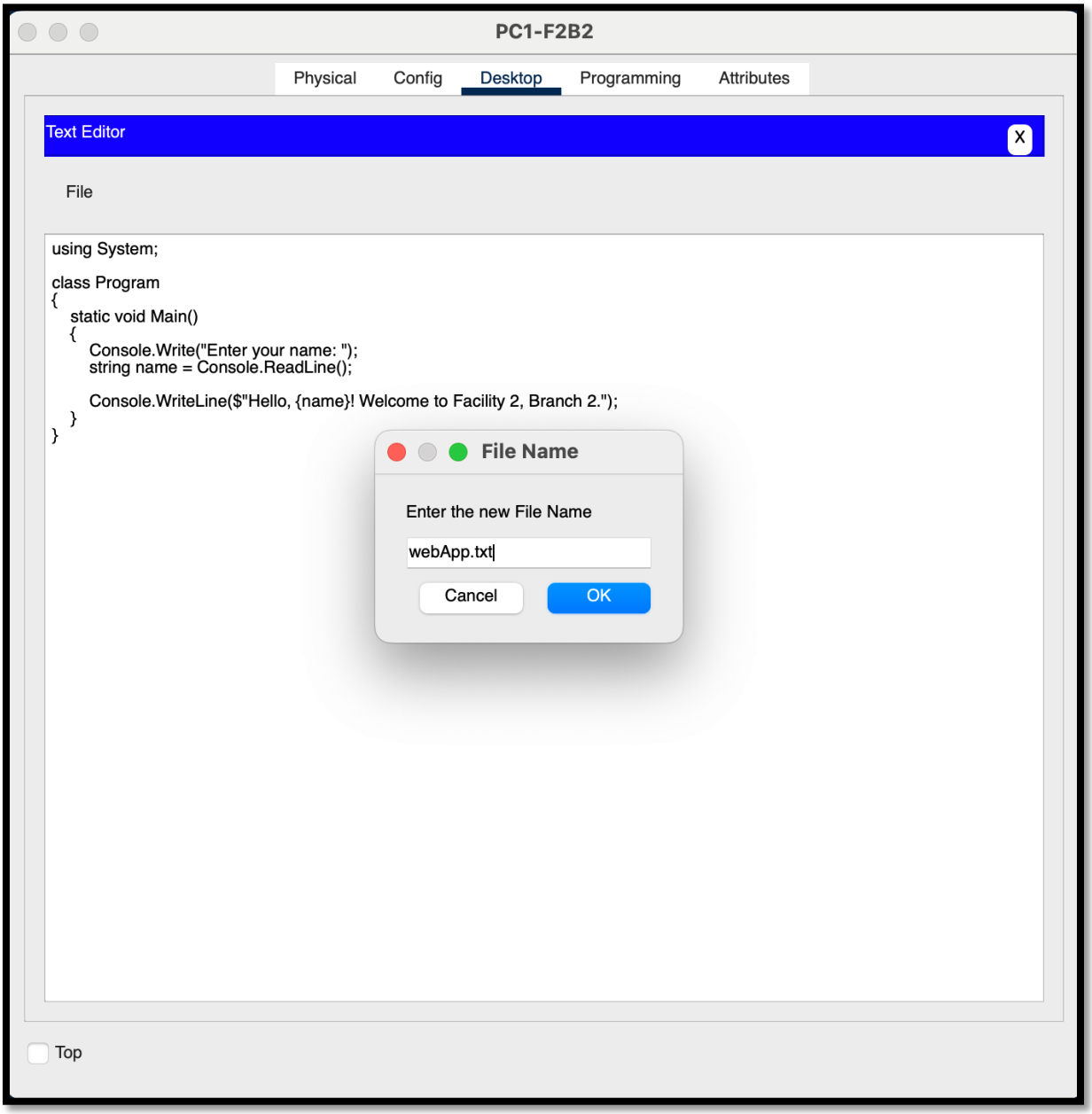


Figure 46: Code Example

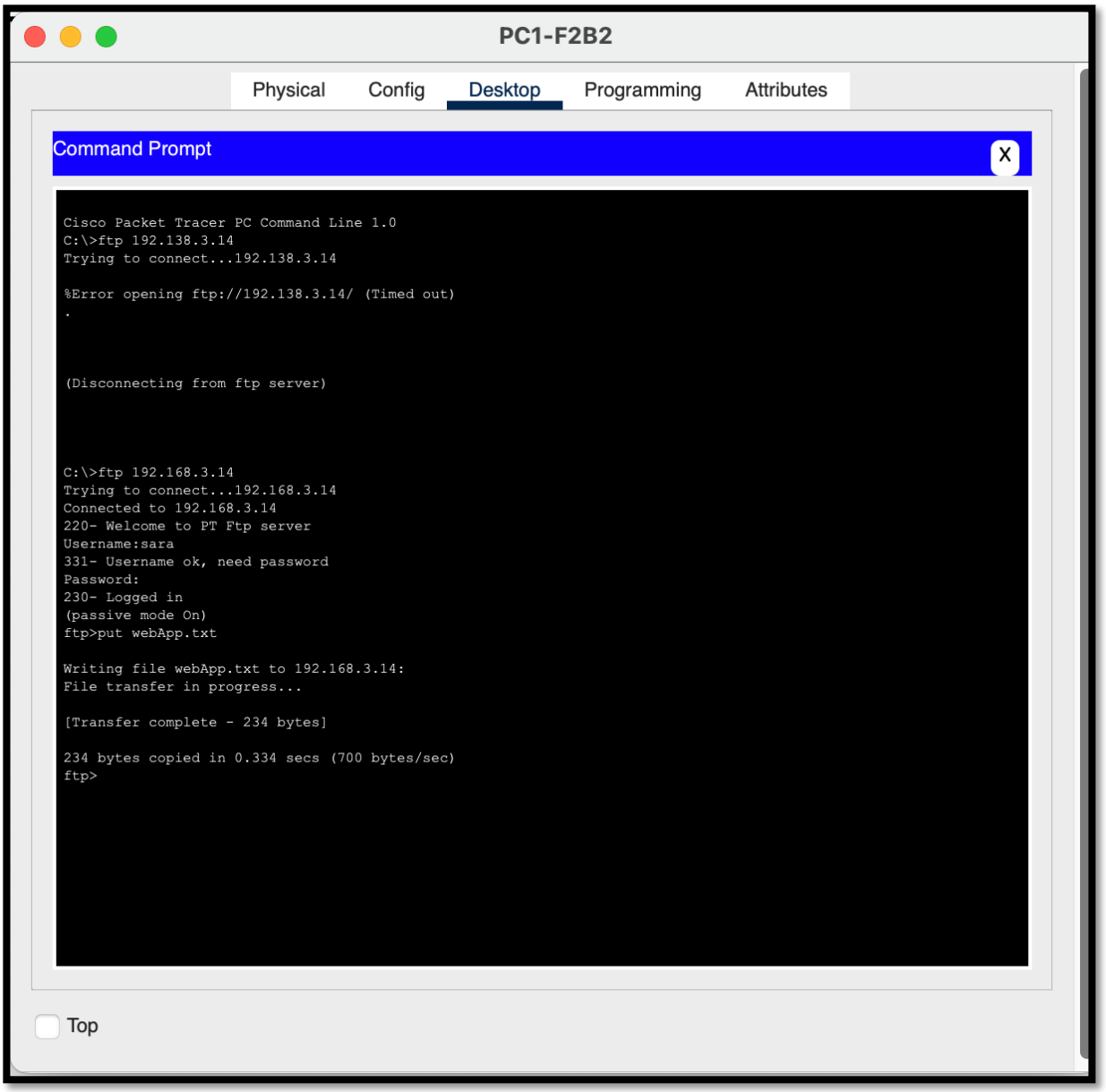


Figure 47: Command Prompt - PC1-F2B2

The following is the Result of the Simulation of sending file through FTP server:

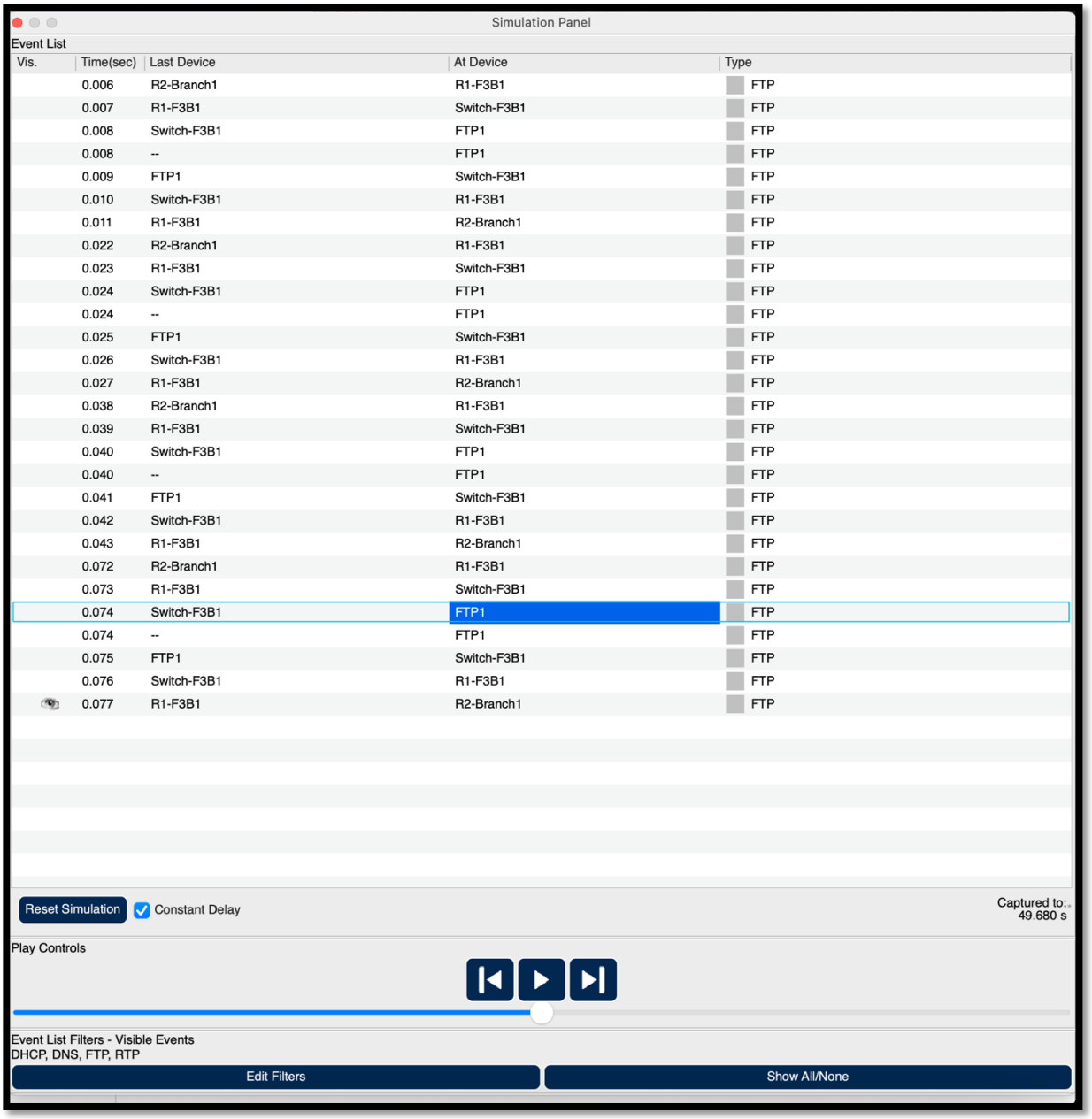


Figure 48: Simulation Panel

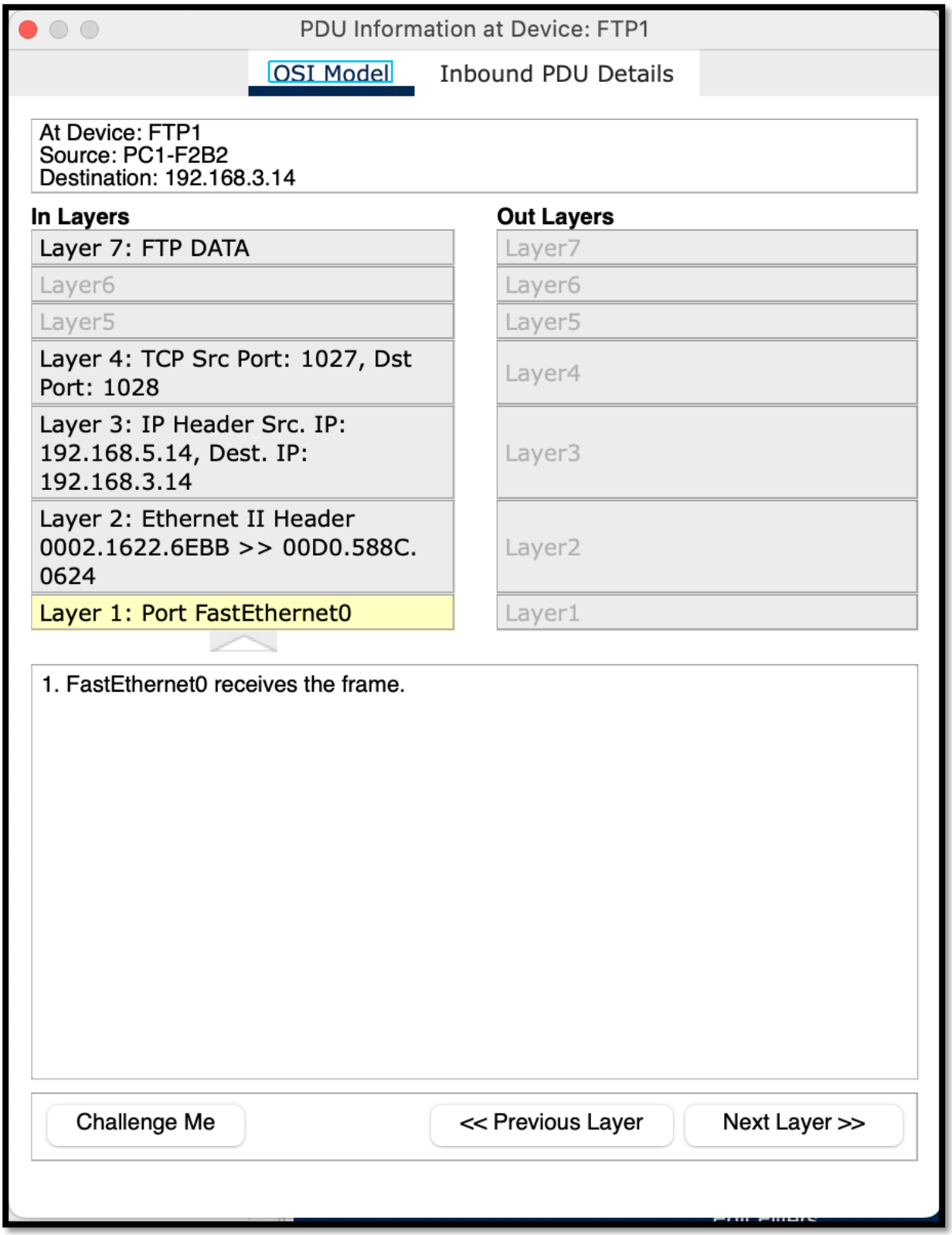


Figure 49: PDU Information at Device - FTP1 – OSI Model

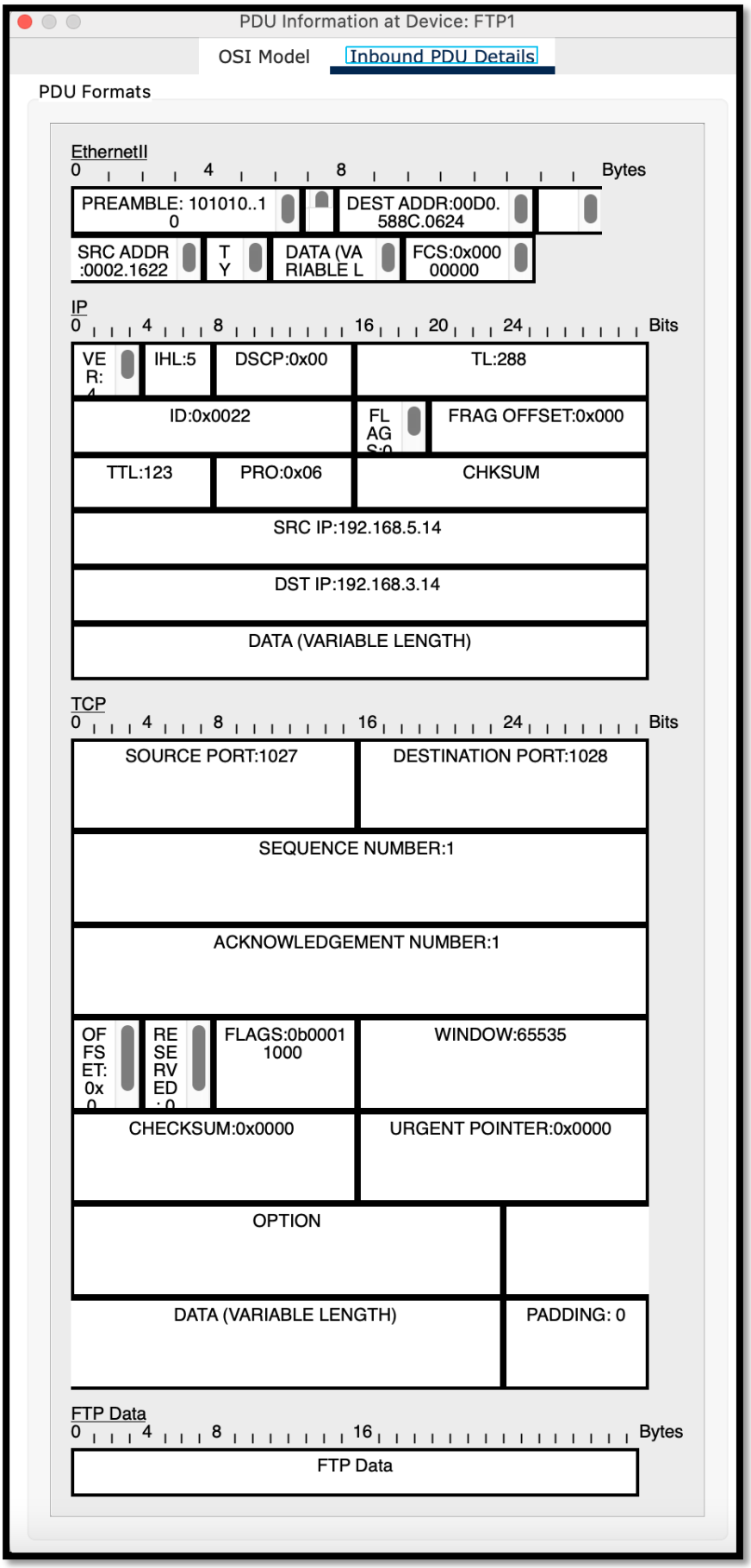


Figure 50: PDU Information at Device - FTP1 – Inbound PDU details

Scenario 3: Internal VoIP Communication Within a Facility

Two users from the second facility of the first branch want to talk via VoIP.

In this scenario, two employees in the **second facility of Branch 1** — using **VoIP1-F2B1** and **VoIP2-F2B1** — intend to communicate using **Voice over IP (VoIP)** technology. Both devices are located within the same local facility and rely on internal network infrastructure to establish a real-time audio conversation.

☎️ VoIP Communication Process (VoIP1-F2B1 ↔ VoIP2-F2B1)

1. IP Assignment via DHCP:

As the VoIP phones power up and connect to the internal network, each device sends a DHCP discovery request. The **local DHCP server** assigns IP addresses, subnet mask, gateway, and DNS settings, enabling network-level communication.

2. Network QoS Configuration:

To guarantee smooth voice transmission, **Quality of Service (QoS)** policies are enforced. VoIP traffic is tagged (typically using DSCP markings) and given priority over less time-sensitive data like email or web browsing to prevent latency, jitter, or packet loss.

3. VoIP Device Setup:

Each user configures their VoIP phone or soft client with login credentials and SIP settings. These credentials are verified by the system, allowing the phones to interact with the internal VoIP services.

4. SIP Registration with Internal Server:

The devices then register with the **internal SIP server**, which acts as the signaling entity. It maintains a mapping of each user's SIP address and IP, enabling it to locate and connect endpoints during call setup.

5. Call Setup and Establishment:

When one user initiates a call, the request is sent to the SIP server, which negotiates session parameters and signals the second phone. Once accepted, the SIP server facilitates the connection, after which the **RTP (Real-Time Protocol)** stream is established **directly between the two VoIP phones**, enabling peer-to-peer voice transmission.

6. Secure Voice Transmission:

To protect the conversation from eavesdropping or tampering, **Secure RTP (SRTP)** is used. This ensures that voice packets are encrypted and authenticated before being sent over the network.

7. Monitoring and Performance Management:

Throughout the session, **network monitoring tools** check the quality of the VoIP traffic, keeping track of latency, jitter, and packet delivery. Any anomalies are flagged for troubleshooting to maintain consistent call quality.

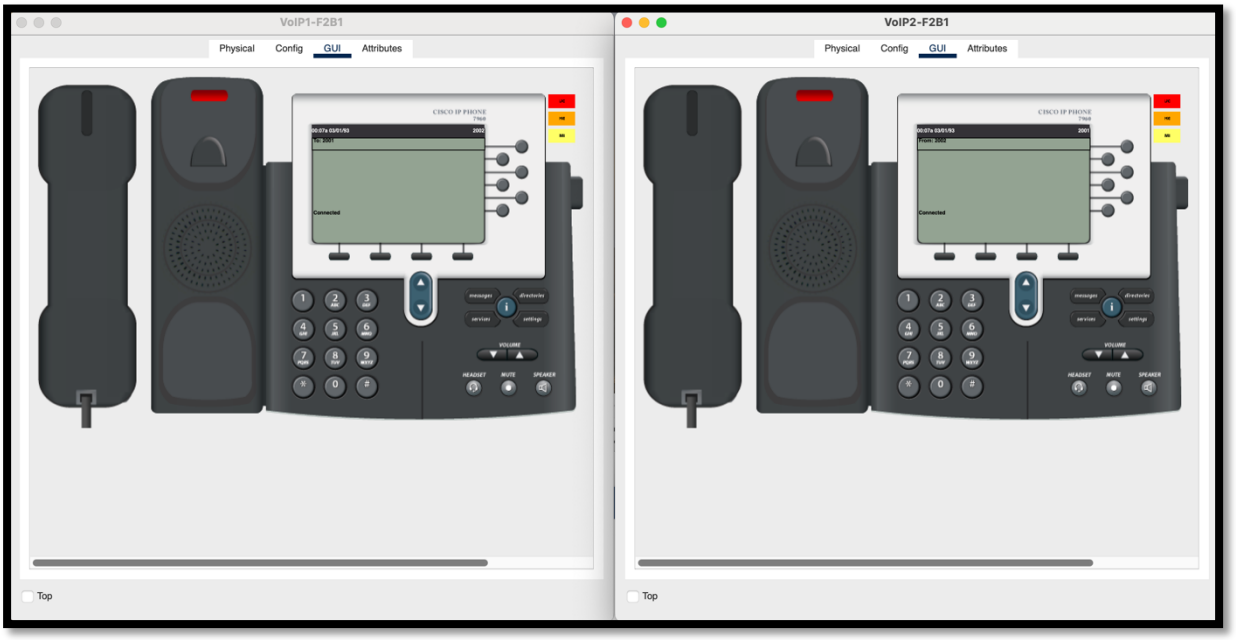


Figure 51: VoIP Devices Call - F2B1

The following is the Result of the Simulation of VoIP Communication:

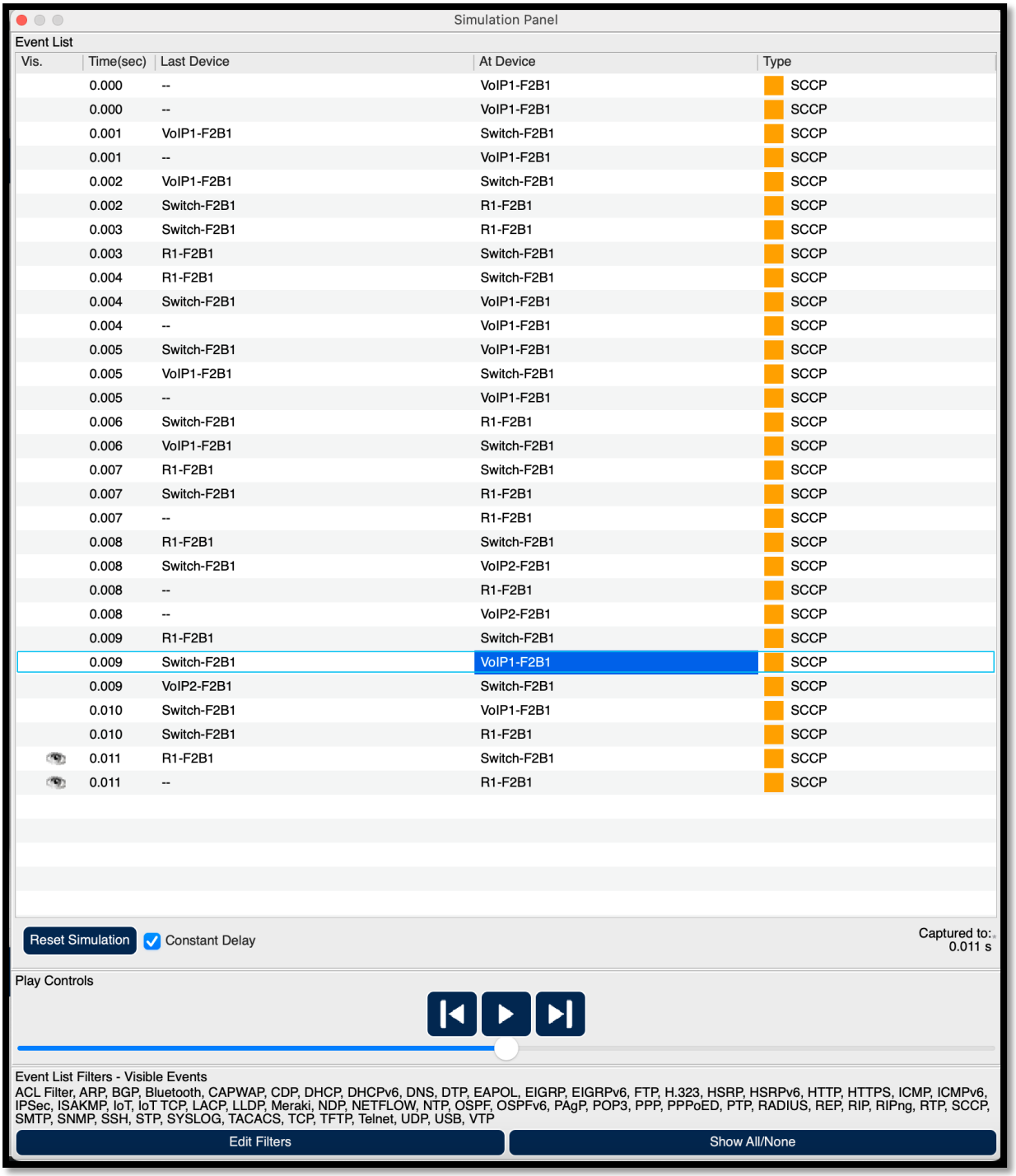


Figure 52: Simulation Panel

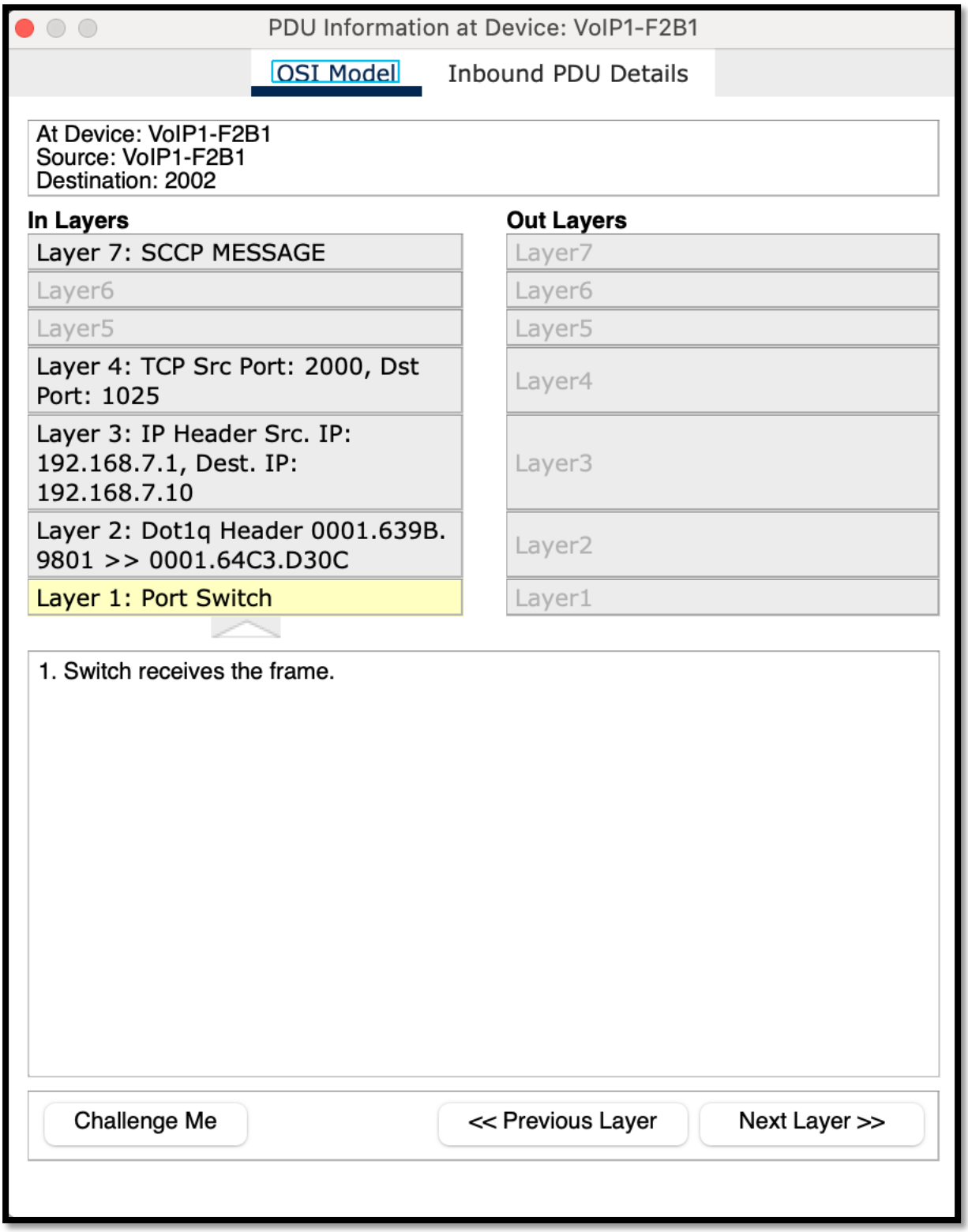


Figure 53: PDU Information at Device – VoIP1-F2B1 – OSI Model

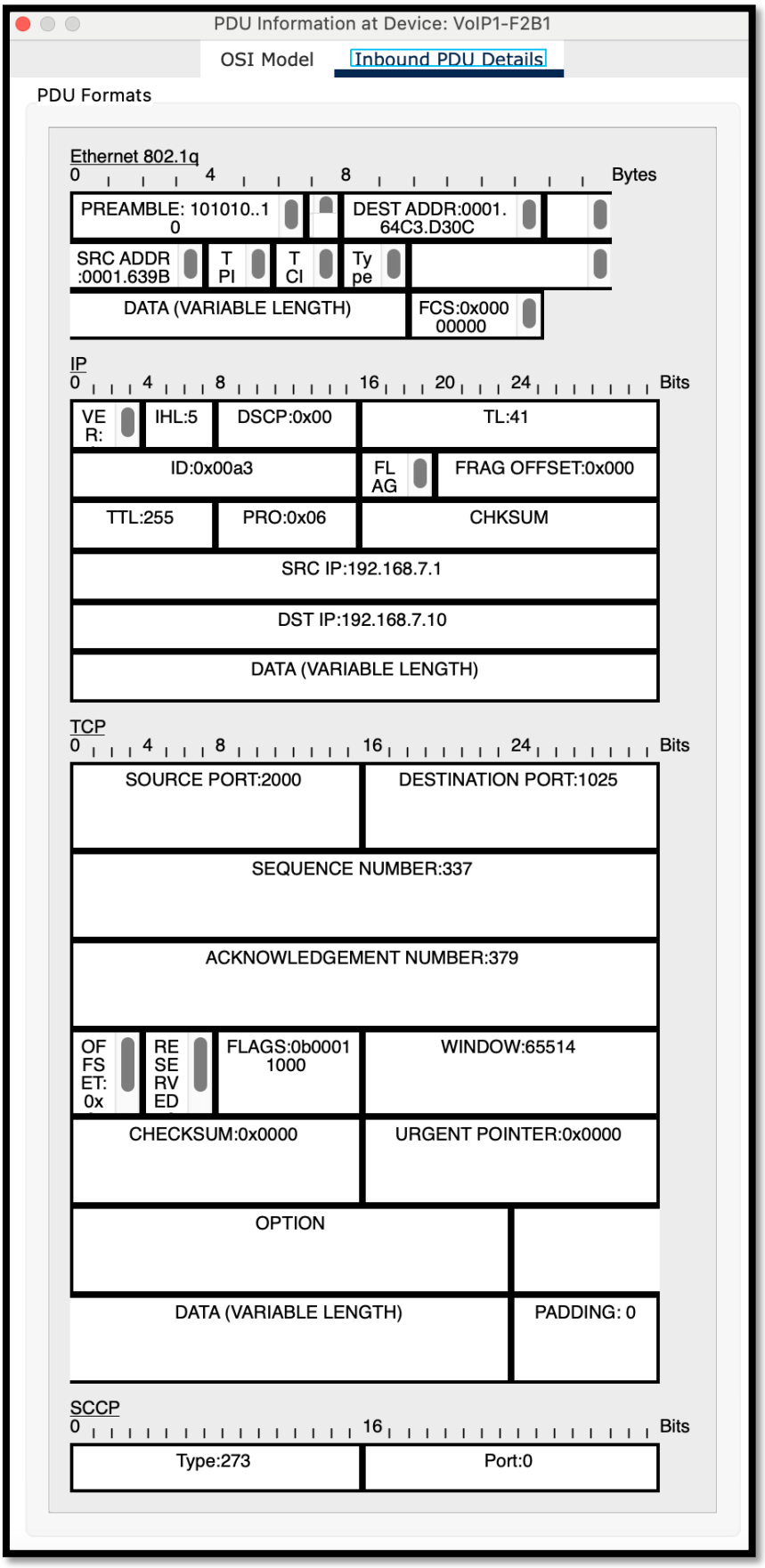


Figure 54: PDU Information at Device - VoIP1-F2B2 – Inbound PDU details

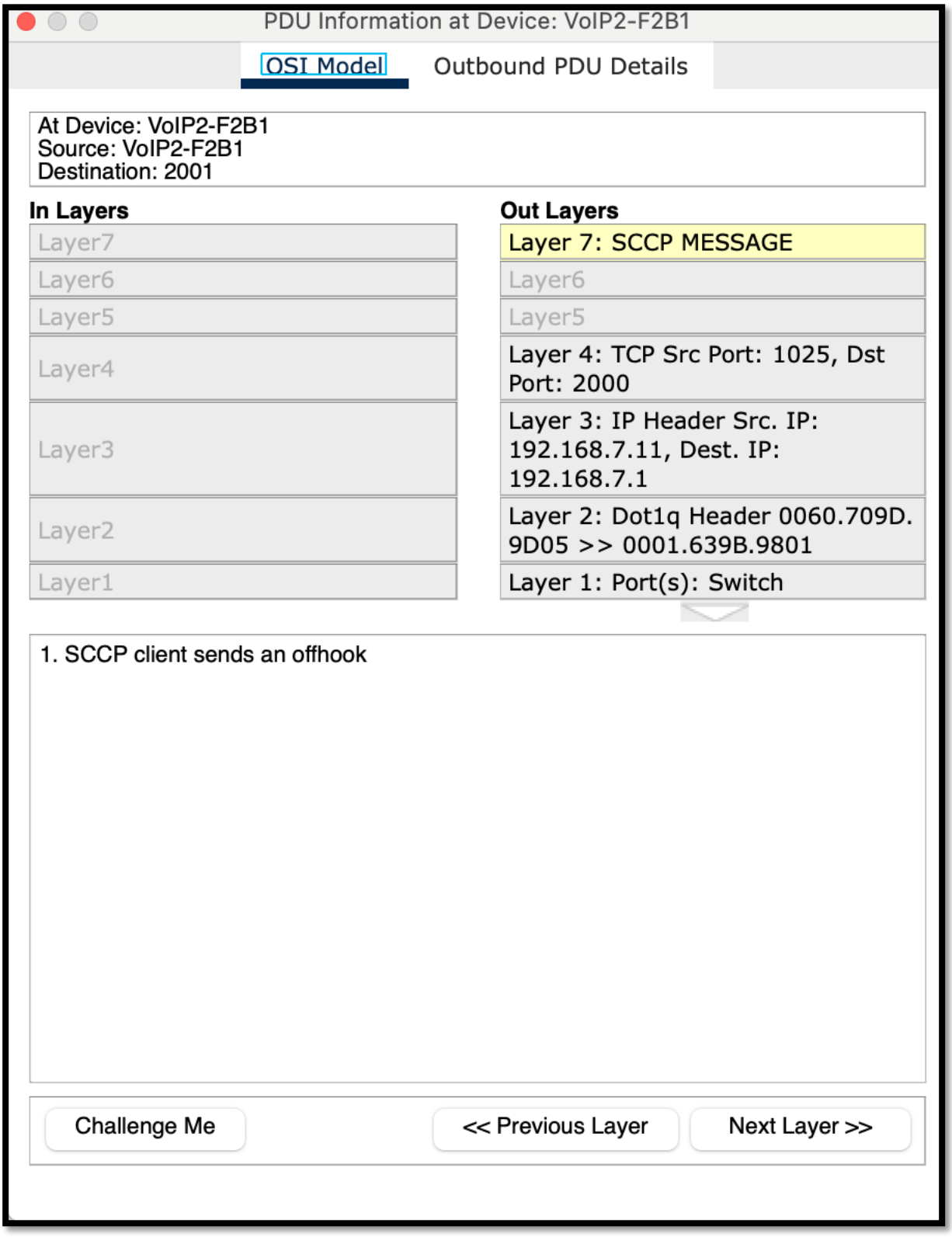


Figure 55: PDU Information at Device – VoIP2-F2B1 – OSI Model

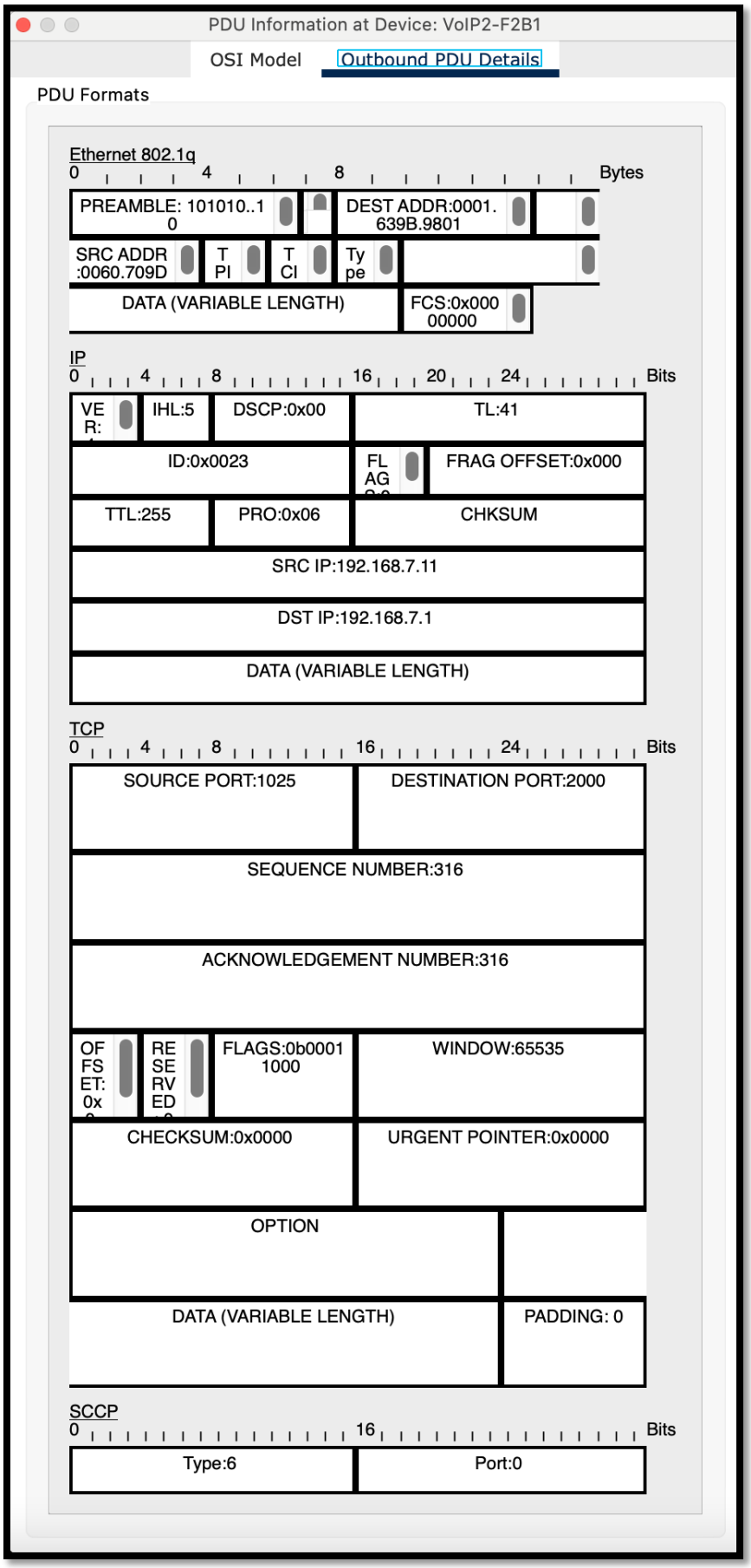


Figure 56: PDU Information at Device - VoIP2-F2B2 – Inbound PDU details

Scenario 4: Email Access Denied Between Facilities Due to Permission Restrictions

A user in the second facility of the first branch wants to send an email message to his friend in the second facility of the second branch.

In this scenario, a user located in the **second facility of Branch 1** — using **PC2-F2B1** — attempts to send an email message to a colleague using **Smartphone1-F2B2** in the **second facility of Branch 2**. However, the message delivery fails due to restricted access permissions on both ends of the network.

Email Communication Failure (PC2-F2B1 → Smartphone1-F2B2)

1. Network Initialization:

As with other users, **PC2-F2B1** and **Smartphone1-F2B2** obtain their network configurations (IP address, gateway, DNS, etc.) through **DHCP**. Both devices are properly connected to their local networks and can reach other permitted services.

2. Email Composition and Send Attempt:

The user on **PC2-F2B1** composes an email and attempts to send it using an email client configured to communicate with the internal mail server via **SMTP (Simple Mail Transfer Protocol)**.

3. SMTP Authentication Failure:

When the email client attempts to authenticate with the **mail server**, the login attempt fails. This occurs because the mail server's **Access Control List (ACL)** or user database does not include credentials for devices in either **F2B1** or **F2B2**. As a result:

- **Authentication is rejected**, and the email cannot be transmitted.
- The server does not permit communication from unauthorized users or devices to maintain system security and prevent misuse.

4. No Delivery to Smartphone1-F2B2:

Since **Smartphone1-F2B2** also lacks access permissions to the email system, it cannot retrieve or even detect incoming messages addressed to it. The device is effectively isolated from the mail server's services.

5. Security Enforcement via ACLs:

Network-level **ACLs and mail server policies** are in place to **prevent unauthorized email access**. These security measures are intended to limit communication to approved users, reducing the risk of spam, phishing, or internal misuse.

6. Outcome:

The attempted email communication fails silently or returns an error to the sender indicating that authentication was unsuccessful. **No email is delivered**, and both users are unable to communicate via email until proper access rights are granted by network administrators.

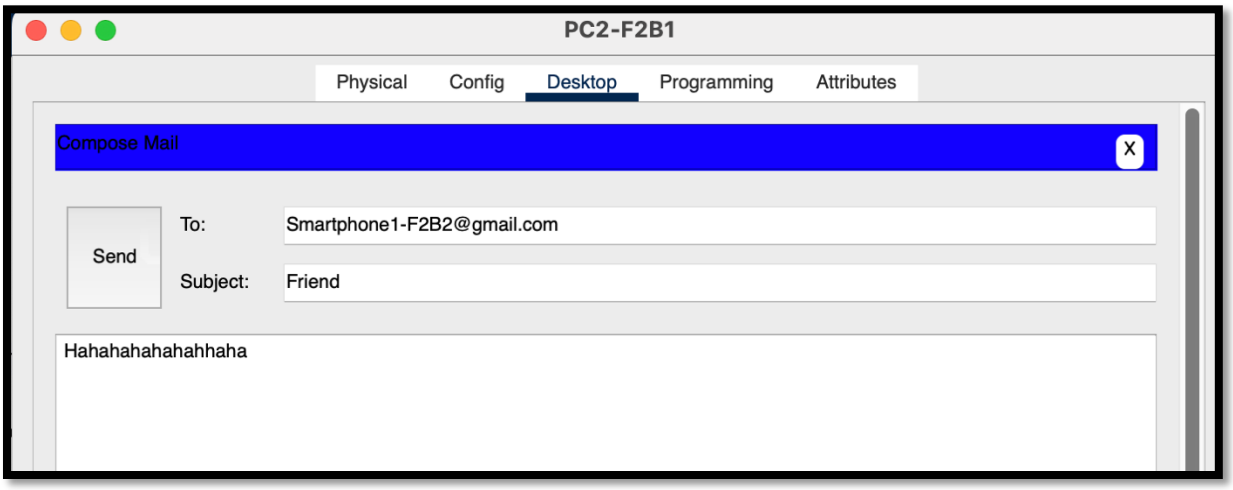


Figure 57: PC2-F2B1 Sending an Email to Smartphone1-F2B2

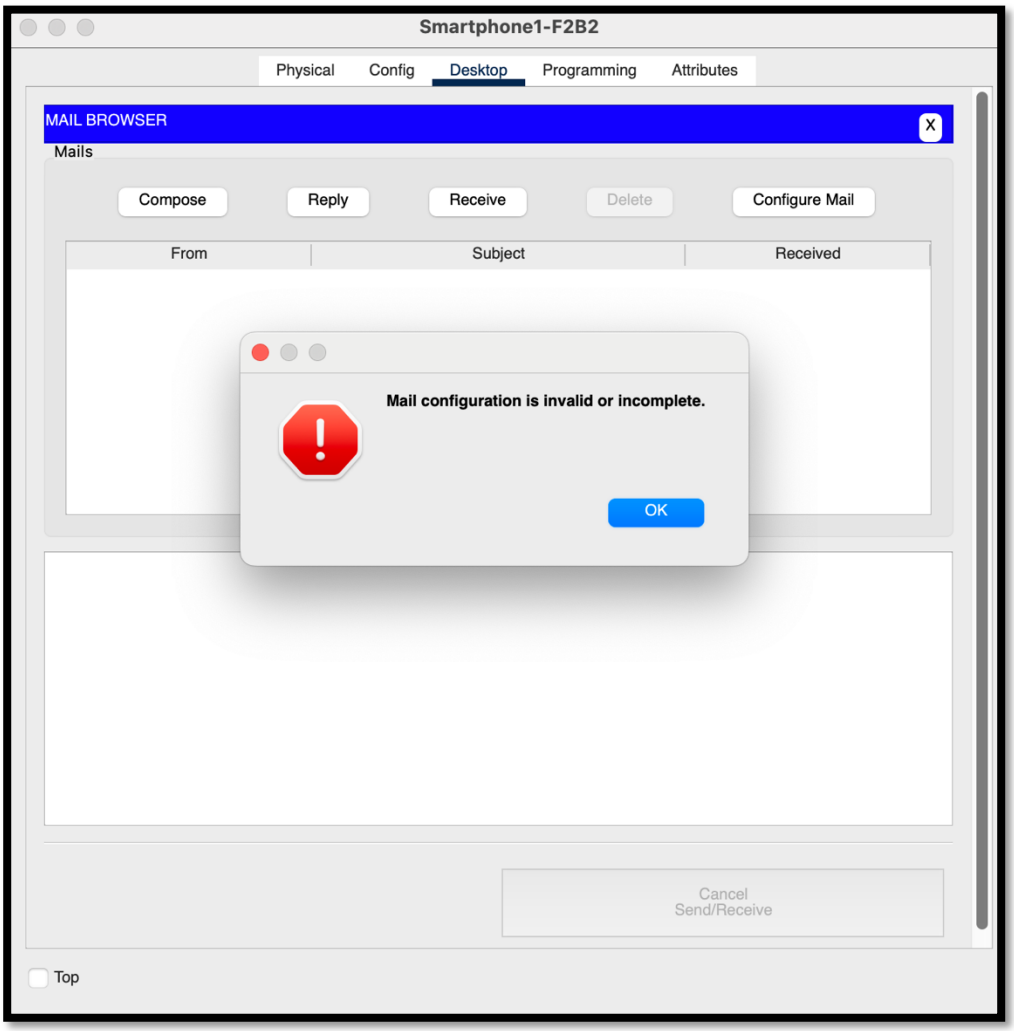


Figure 58: Smartphone1-F2B2 Failed to Receive

Scenario 5: Inter-Branch Ping Test from Client to Web Server

A user from the first facility of the second branch pings the Web server of the second facility of the first branch.

In this scenario, a user located in the **first facility of Branch 2**, using **TabletPC2-F1B2**, wants to verify the reachability of a **Web Server located in the second facility of Branch 1** — specifically, **WebServer-F2B1**. To do so, the user initiates a **ping command** to test connectivity and measure basic network performance across branch locations.

📶 **Ping Process (TabletPC2-F1B2 → WebServer-F2B1)**

1. IP Address Assignment and Network Readiness:

Before the connectivity test begins, **TabletPC1-F1B2** obtains an IP address through **DHCP**, receiving essential network settings such as the default gateway and DNS server information. Similarly, **WebServer-F2B1** must already be configured with a valid static IP or DHCP-assigned address to ensure it can respond to network requests.

2. Initiating the Ping Command:

The user executes a **ping** command from the device's terminal or command prompt, targeting the IP address of **WebServer-F2B1**. This command triggers the transmission of **ICMP Echo Request** packets toward the destination server.

3. Inter-Branch Packet Routing:

The ICMP packets follow the network path outlined below:

- First, the packets pass through the **local switch** and **router** in **Facility 1 of Branch 2**.
- From there, they are forwarded to the **Branch 2 main router**, which handles routing toward the **Branch 1 network**.
- The packets traverse the **inter-branch connection**, eventually entering the **main router of Branch 1**.
- Finally, they are routed through the **Branch 1 Facility 2 router and switch**, reaching the **WebServer-F2B1**.

4. ICMP Echo Reply from the Web Server:

Once **WebServer-F2B1** receives the Echo Request, it generates an **ICMP Echo Reply** and sends it back toward the original sender — TabletPC1-F1B2 — provided no firewall or ACL blocks the ICMP traffic.

5. Return Path of the Reply Packets:

The Echo Reply packets retrace the original route in reverse — traveling from Branch 1's second facility back through routers, across the inter-branch link, and ultimately arriving at **TabletPC1-F1B2** in Branch 2's first facility.

6. Result Interpretation on the User's Device:

The ping results are displayed on **TabletPC2-F1B2**, showing metrics such as:

- **Round-trip time (RTT)** for each packet.

- **Packet loss**, if any.
- An overall summary indicating whether the **WebServer-F2B1 is reachable** and the general responsiveness of the inter-branch network.

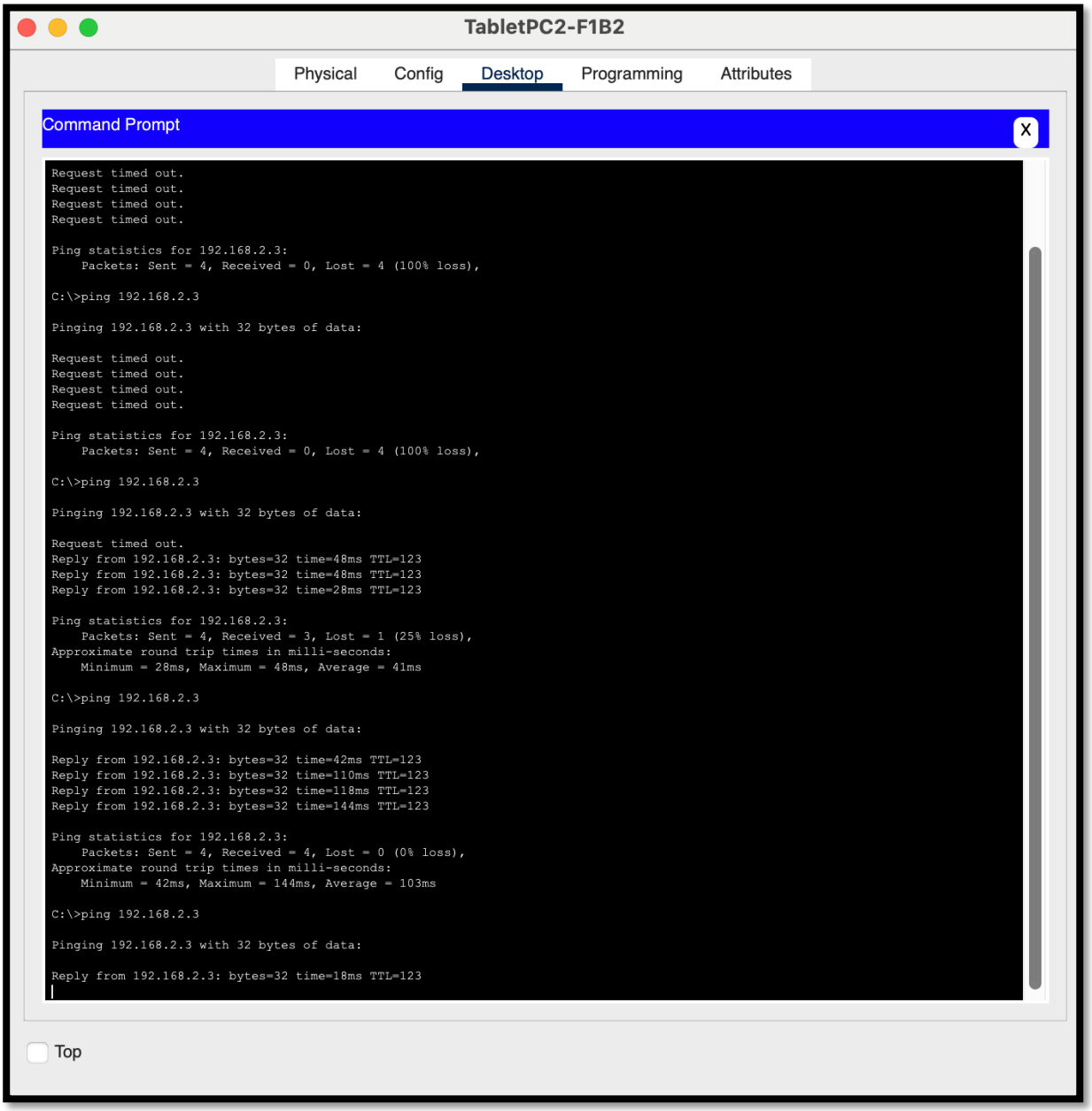


Figure 59: Command Prompt - TabletPC2-F1B2

The following is the Result of the Simulation of Pining to the Web Server:

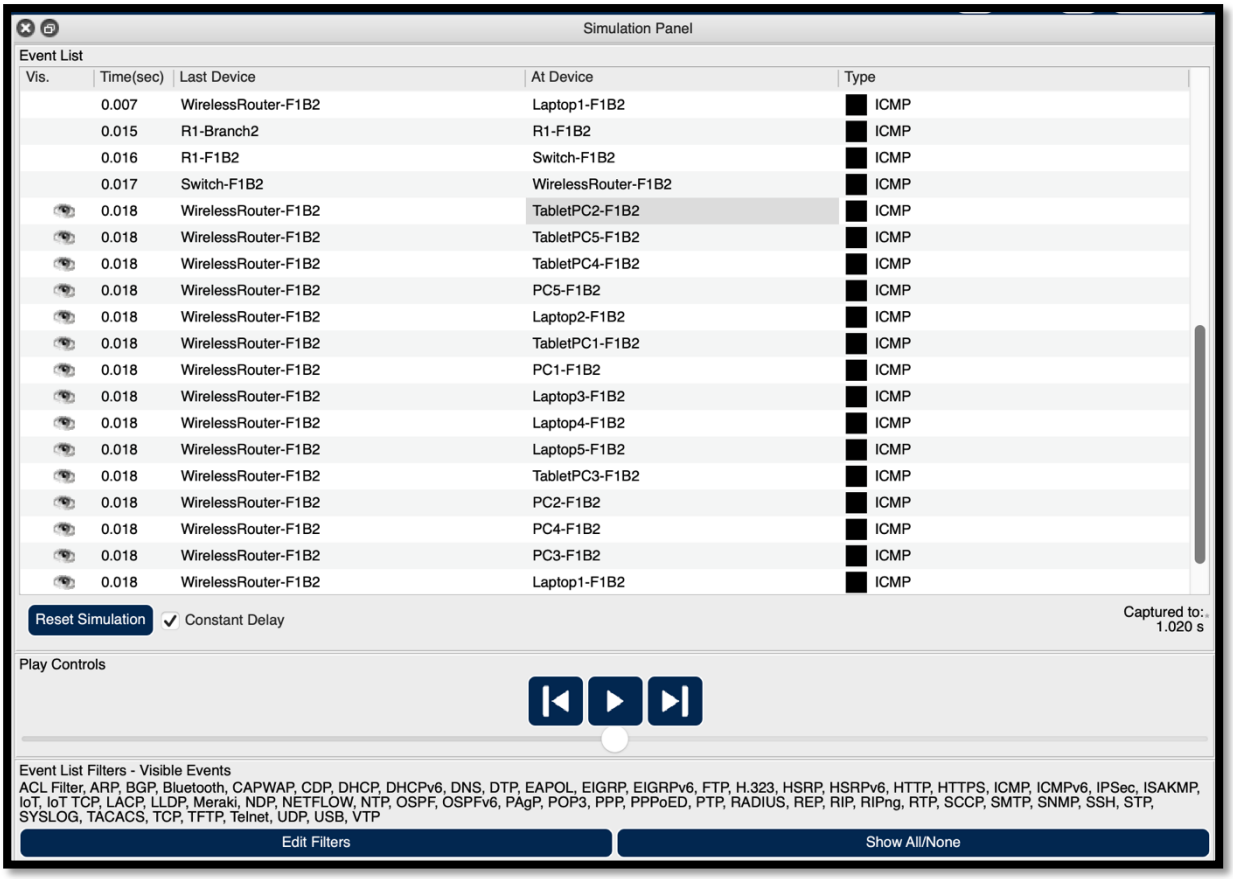


Figure 60: Simulation Panel

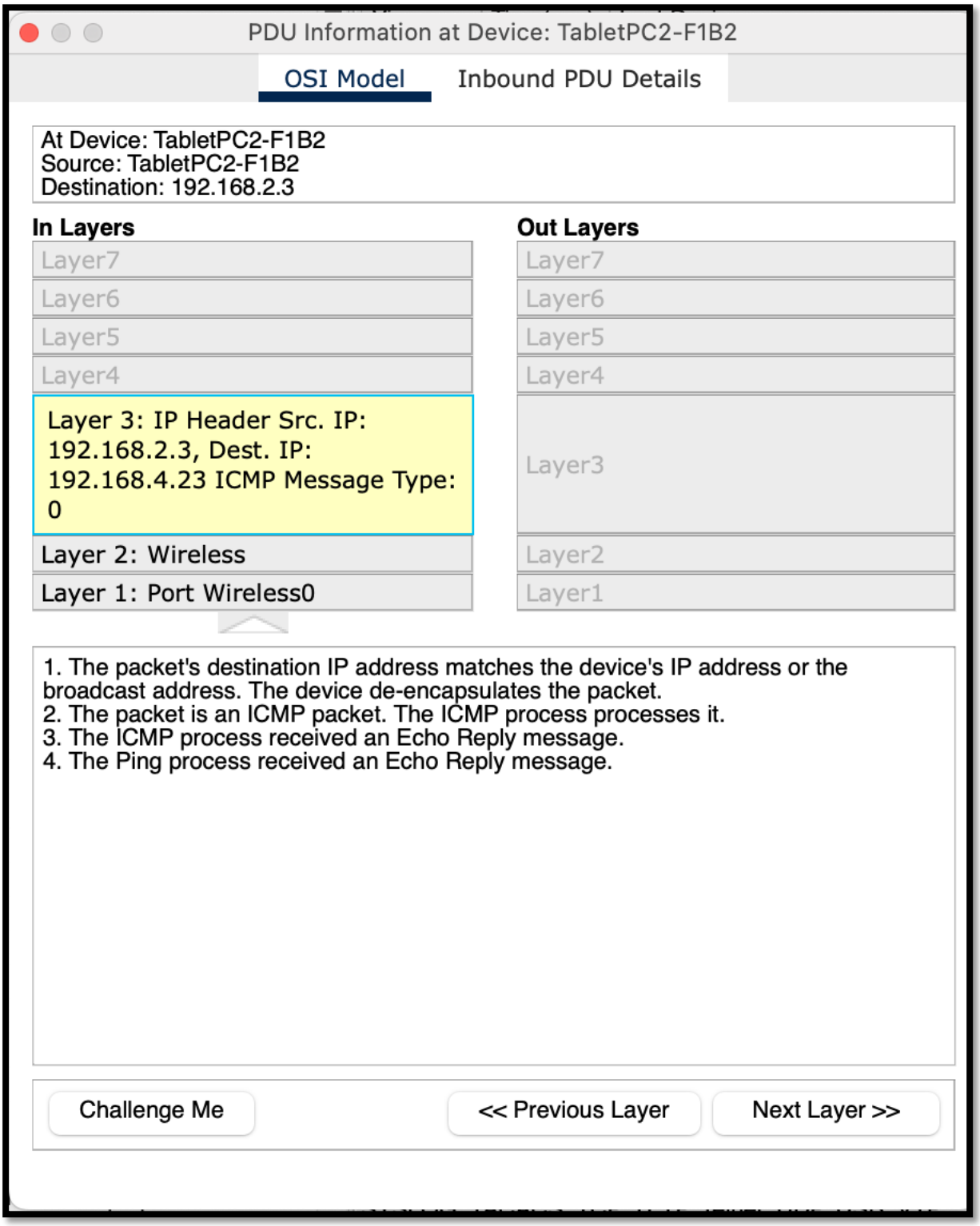


Figure 61: PDU Information at Device – TabletPC2-F1B2 – OSI Model

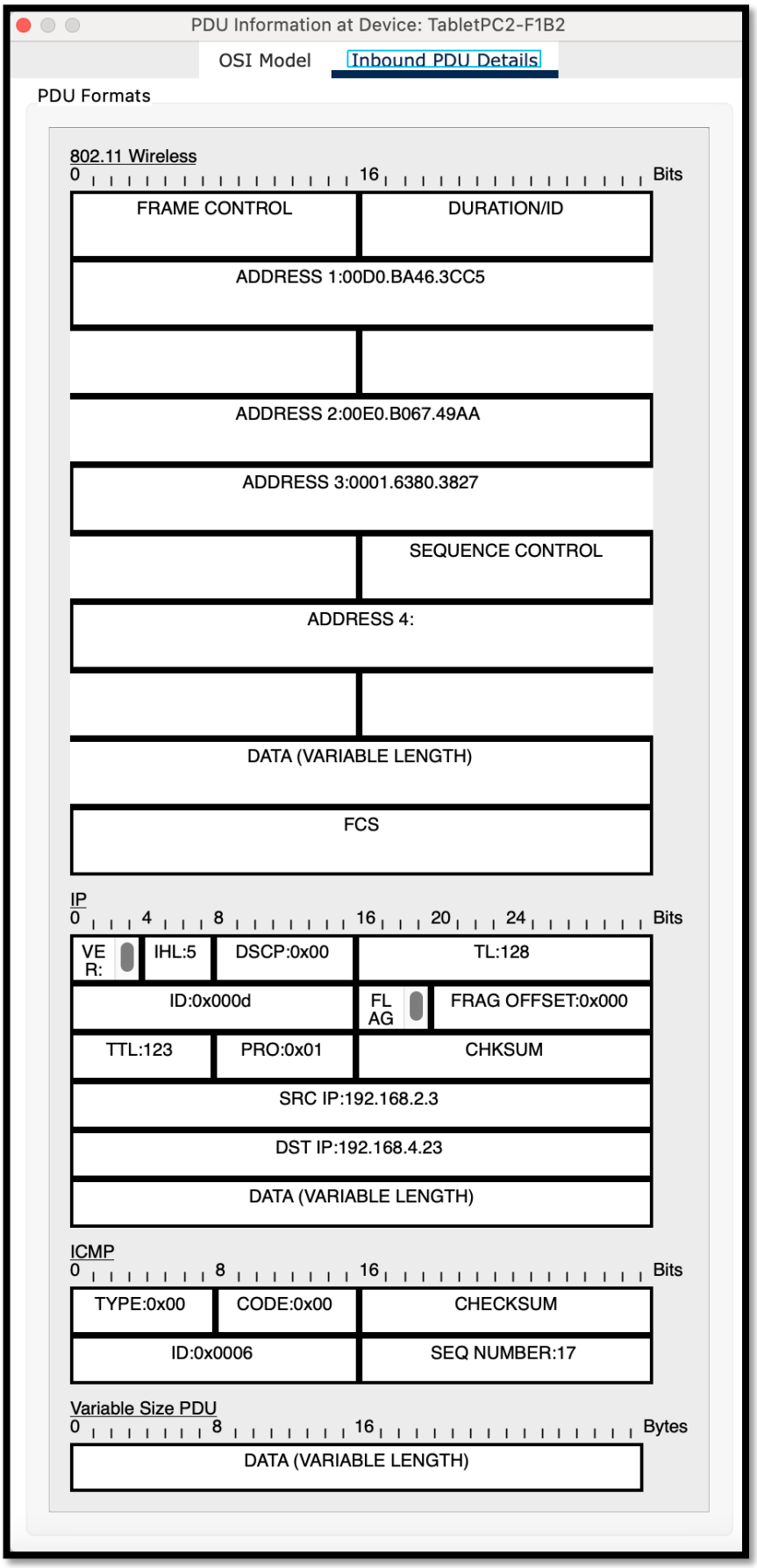


Figure 62: PDU Information at Device - TabletPC2-F1B2 – Inbound PDU details

Scenario 6: Cross-Branch Email Communication Between Laptop Users

A laptop user from the first branch office's first facility wants to send an e-mail to her friend in the first facility of the second branch office.

In this scenario, a user in the **first facility of Branch 1**, using **Laptop1-F1B1**, wants to send an email to a friend located in the **first facility of Branch 2**, using **Laptop1-F1B2**. Both users have the necessary permissions to access the internal mail system, enabling successful email communication.

📤 **Email Sending Process (Laptop1-F1B1 → Laptop1-F1B2)**

1. Network Initialization via DHCP:

Laptop1-F1B1 connects to the network and acquires its IP address, subnet mask, gateway, and DNS information through the **DHCP server** operating within the local facility network. This enables the laptop to access internal and external network services.

2. Email Client Configuration:

The user configures their email client with the appropriate settings:

- **SMTP server address and port** for sending emails.
- **IMAP or POP3 server** for incoming mail.
- Authentication credentials (username and password) provided by the organization's email system.

3. Composing the Email:

With the client ready, the user drafts the message and enters the email address of the intended recipient — **Laptop1-F1B2** — ensuring the message is properly formatted and ready for dispatch.

4. Sending the Email via SMTP:

Upon clicking "Send," the email client communicates with the **outgoing mail server** using **SMTP (Simple Mail Transfer Protocol)**. The email is securely transmitted to the server, where it is queued for delivery.

5. Inter-Branch Email Routing:

The **mail server** looks up the recipient's domain using **DNS resolution** and identifies the correct destination server for **Laptop1-F1B2**. The email is then routed across the internal network:

- It travels through **Branch 1's router**, passes through the **inter-branch connection**, and is delivered to **Branch 2's mail server**, where it is associated with the recipient's mailbox.

6. Recipient Mailbox and Notification:

The message is stored in **Laptop1-F1B2's inbox** on the mail server. When the recipient opens their email client or refreshes their inbox, the client connects to the mail server using **IMAP or POP3**, retrieves the new message, and displays it to the user.

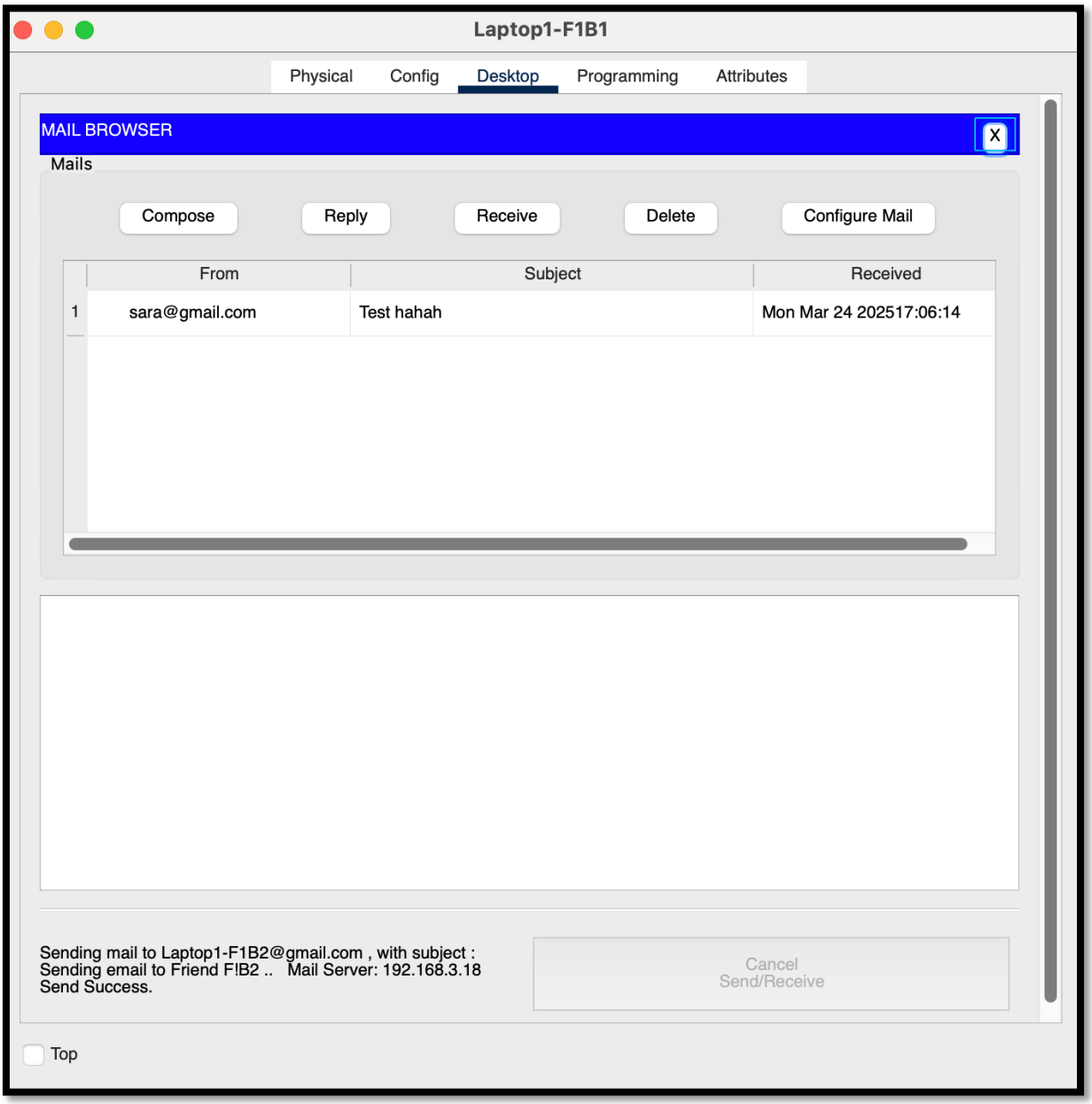


Figure 63: Sending an Email from Laptop1-F1B1 to Laptop1-F1B2 (Success)

The following is the Result of the Simulation of Email Communication between Laptop Users:

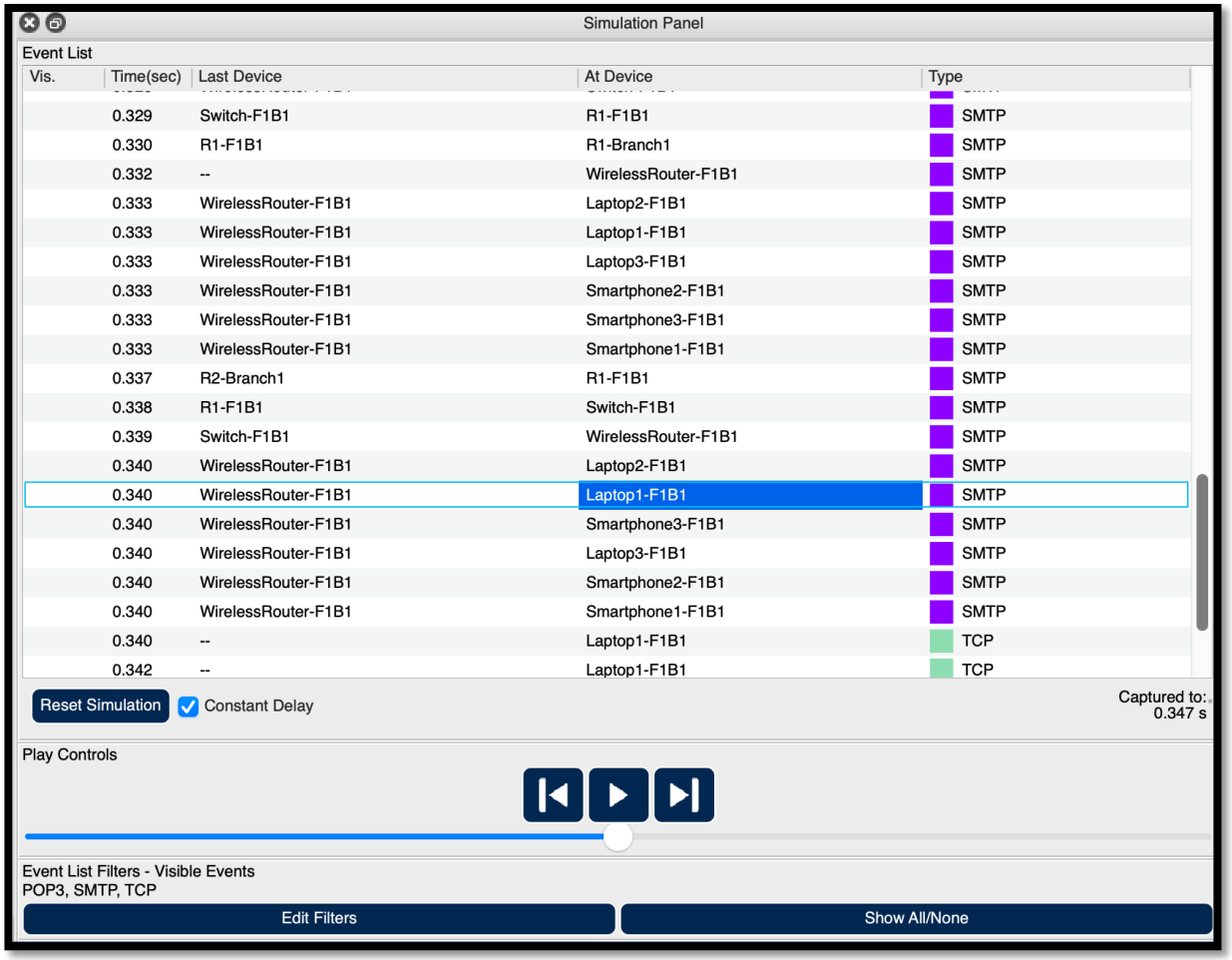


Figure 64: Simulation Panel

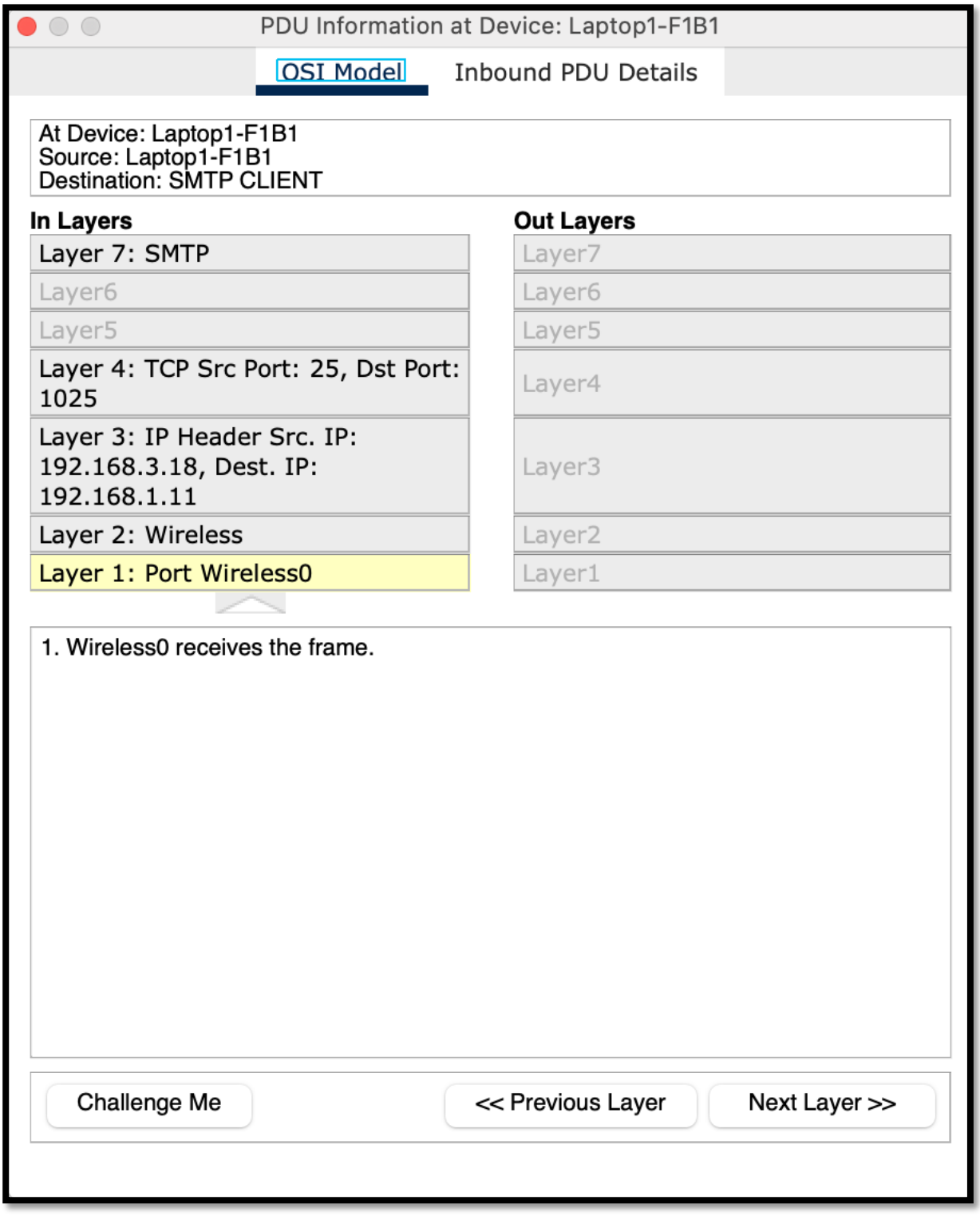


Figure 65: PDU Information at Device – Laptop1-F1B1 – OSI Model

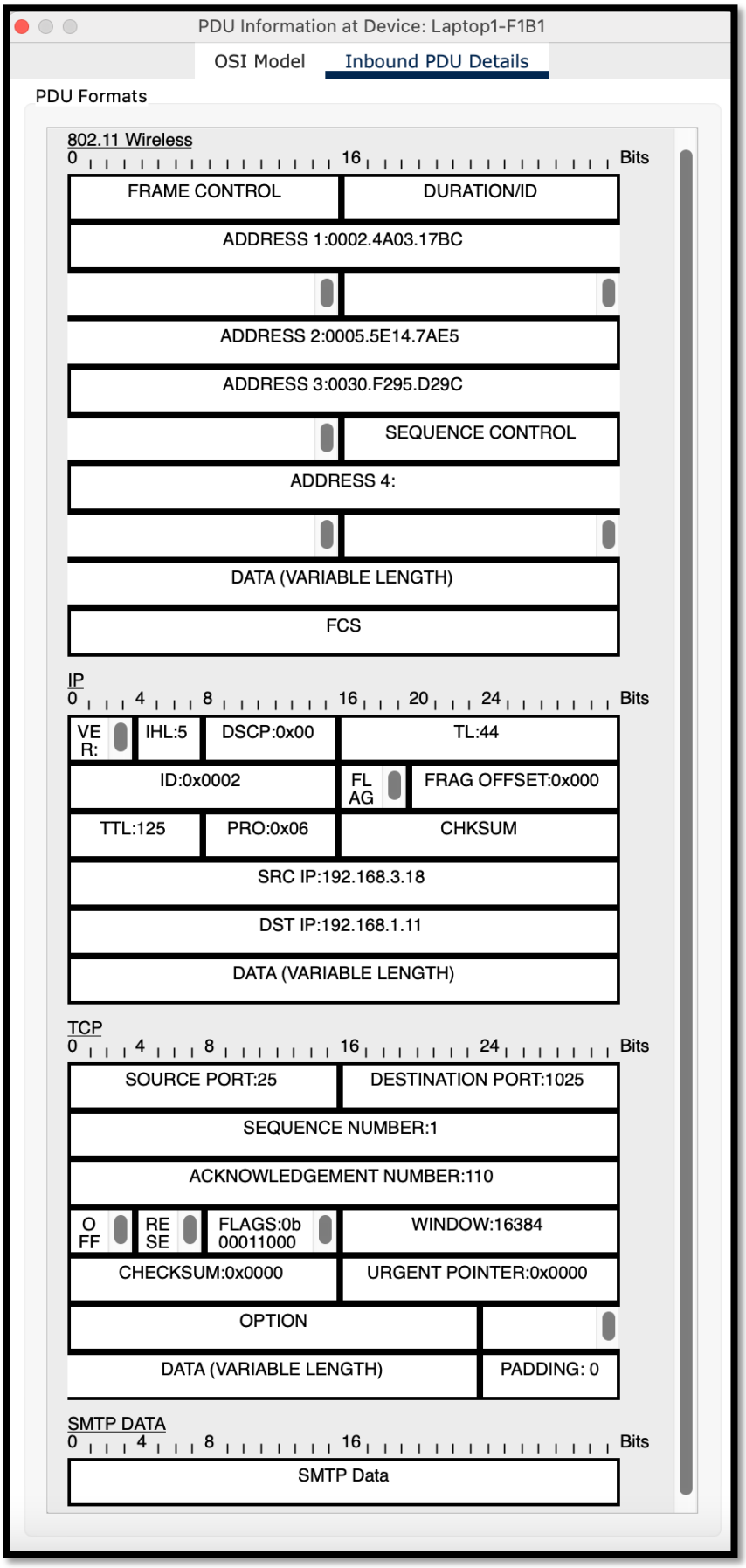


Figure 66: PDU Information at Device - Laptop1-F1B1 – Inbound PDU details

Scenario 7: Remote Web Server Access via SSH from a Smartphone

A smartphone user from the third facility of the second branch office wants to use SSH to connect to a Web server in the third facility of the first branch office.

In this scenario, a user located in the **third facility of Branch 2**, using **Smartphone1-F3B2**, needs to remotely access a **web server (Web6 – 192.168.3.9, www.amazon.com)** hosted in the **third facility of Branch 1**. This is achieved through a secure SSH (Secure Shell) session, allowing the user to perform administrative tasks from a mobile device across branches.

🔐 **SSH Connection Process (Smartphone1-F3B2 → Web6 in F3B1)**

1. Wireless Network Connection and IP Assignment:

The smartphone connects to the facility's **Wi-Fi network** and automatically receives an **IP address via DHCP**, along with a default gateway and DNS settings. This step ensures the device is network-ready to initiate a remote session.

2. SSH Client Configuration:

The user launches an **SSH client app** on their smartphone. The app is configured with:

- The **target IP address** of the web server (192.168.3.9).
- The necessary **login credentials** (either a username/password pair or SSH private key).
- Port **22**, used by default for SSH connections.

3. Inter-Branch Routing of SSH Traffic:

Once the connection is initiated:

- Packets leave **Smartphone1-F3B2**, passing through the **local access point**, **switch**, and **router** in Facility 3 of Branch 2.
- The packets are then routed through the **main Branch 2 router**, crossing the **inter-branch link** toward **Branch 1**.
- Within Branch 1, packets are forwarded to the **third facility's router**, which delivers them to the destination **web server**.

4. SSH Session Establishment:

Upon receiving the request:

- The **SSH daemon (sshd)** on Web6 initiates a **secure handshake**, negotiating encryption keys for the session.
- The user is then **prompted for authentication**. A successful login grants access to the web server's terminal over a secure channel.

5. Access Control and Network Security:

To ensure a secure session:

- **ACLs and firewall rules** must permit SSH traffic between the two facilities.

- Only authorized users should be allowed to access the server through **SSH-2 protocol**, which provides enhanced encryption and integrity.
- **Security monitoring systems** track the session to detect unauthorized access or abnormal behavior.

6. Verification and Administrative Access:

Once connected:

- The user gains **command-line access** to Web6 and can perform administrative tasks remotely.
- Network administrators are encouraged to **log and monitor SSH activity** for compliance and security assurance.

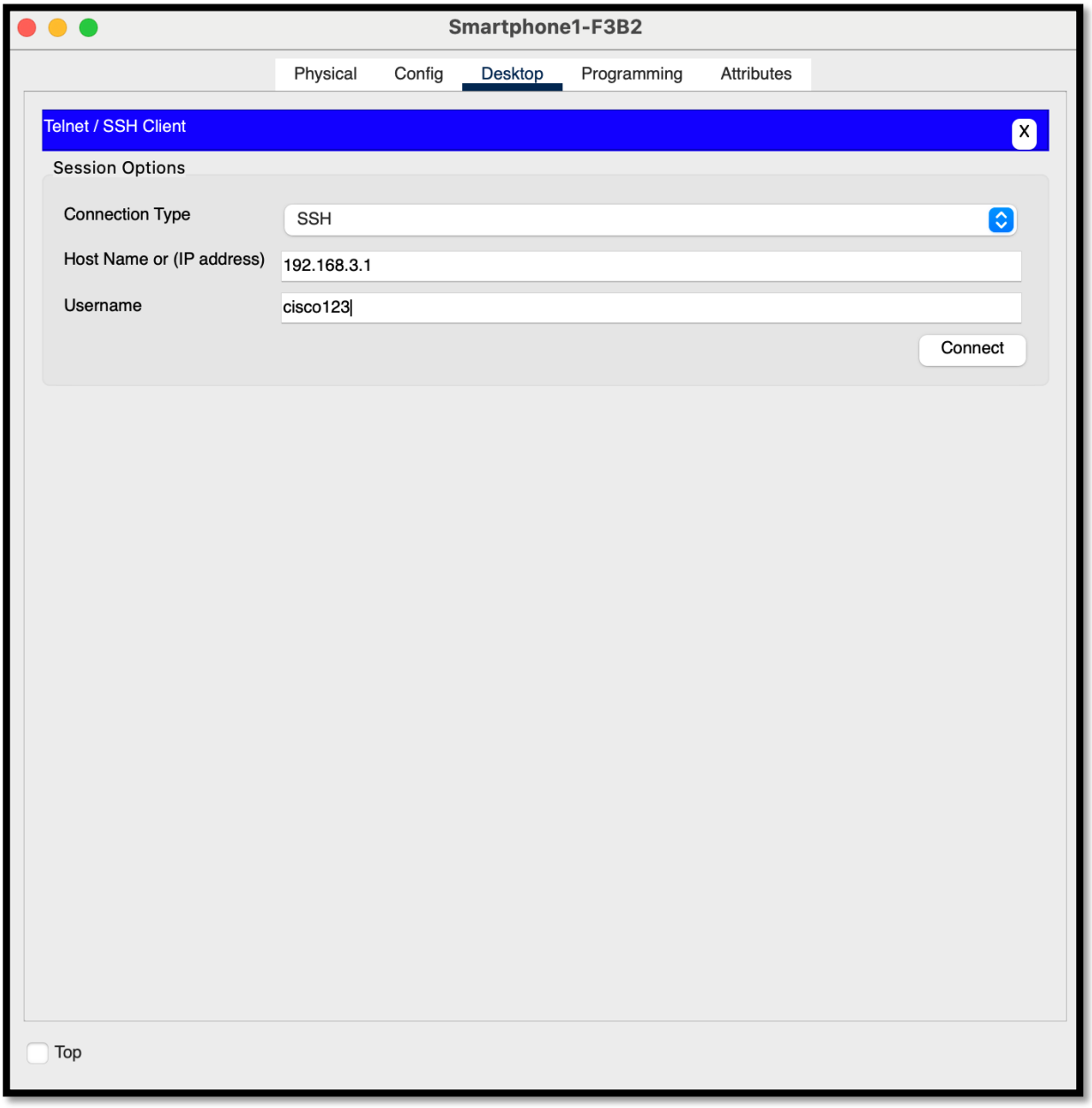


Figure 67: Telnet/SSH Client

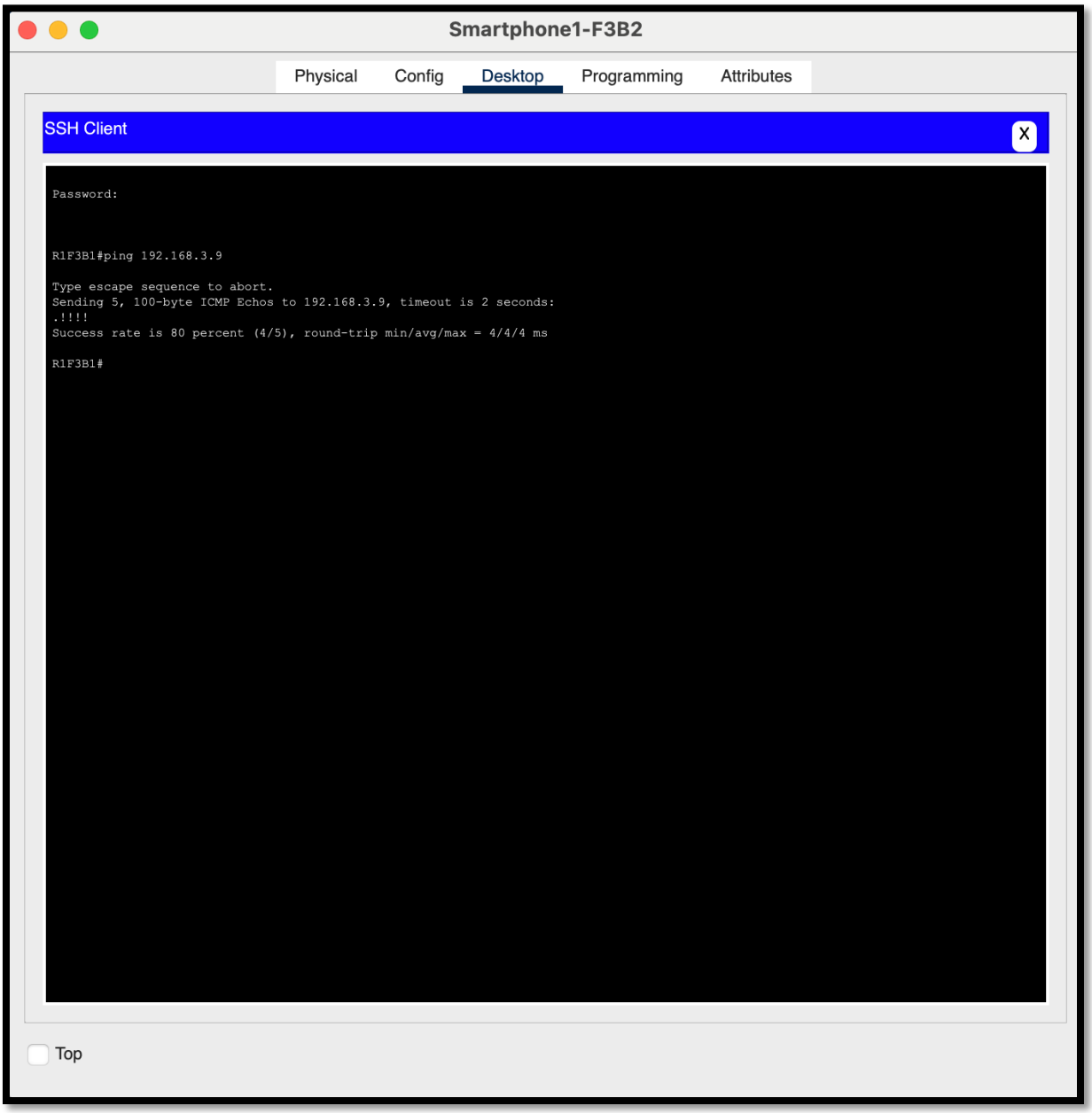


Figure 68: SSH Client ping result

The following is the Result of the Simulation of Remote Web Server Access via SSH:

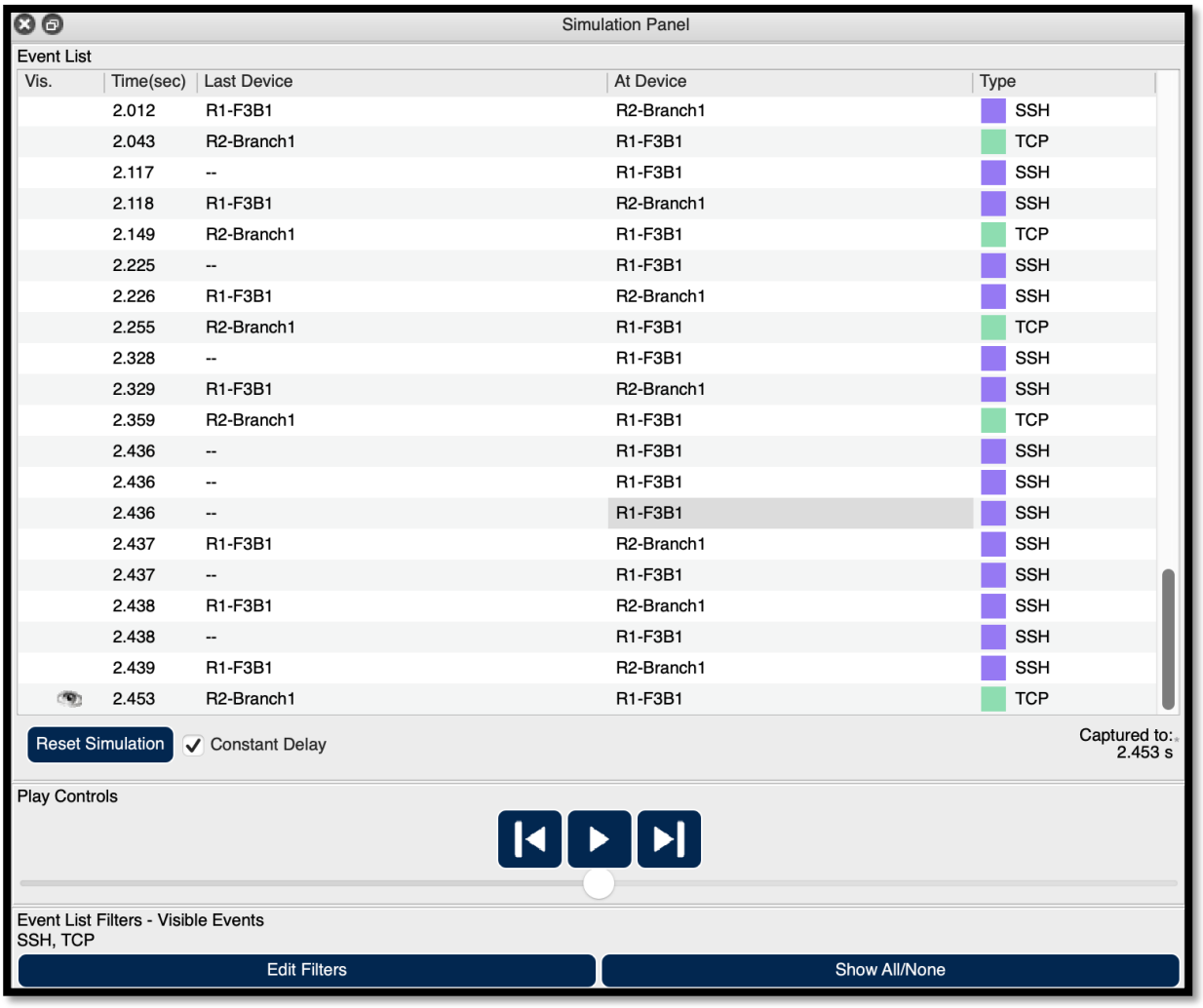


Figure 69: Simulation Panel

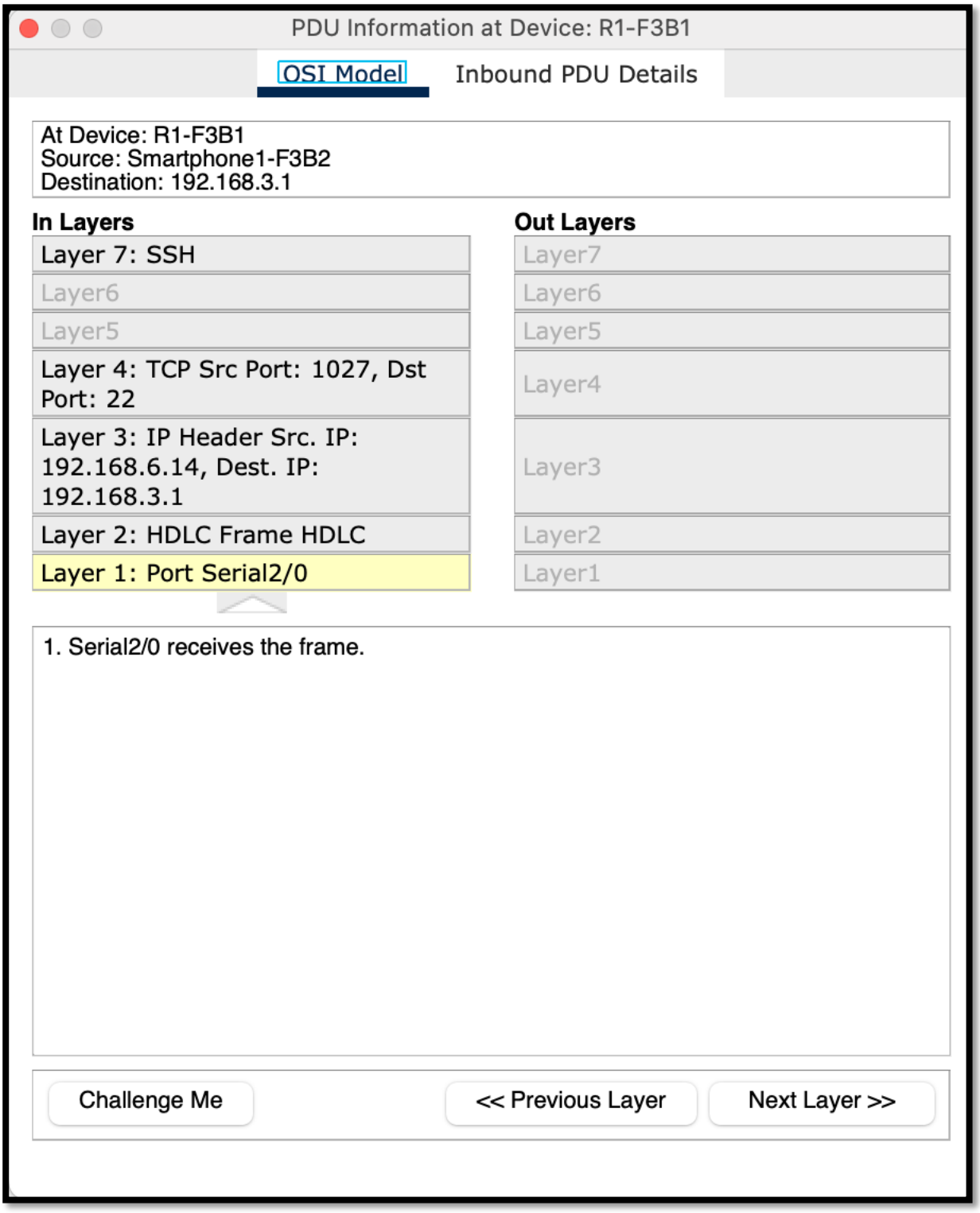


Figure 70: PDU Information at Device – R1-F3B1 – OSI Model (In Layer)

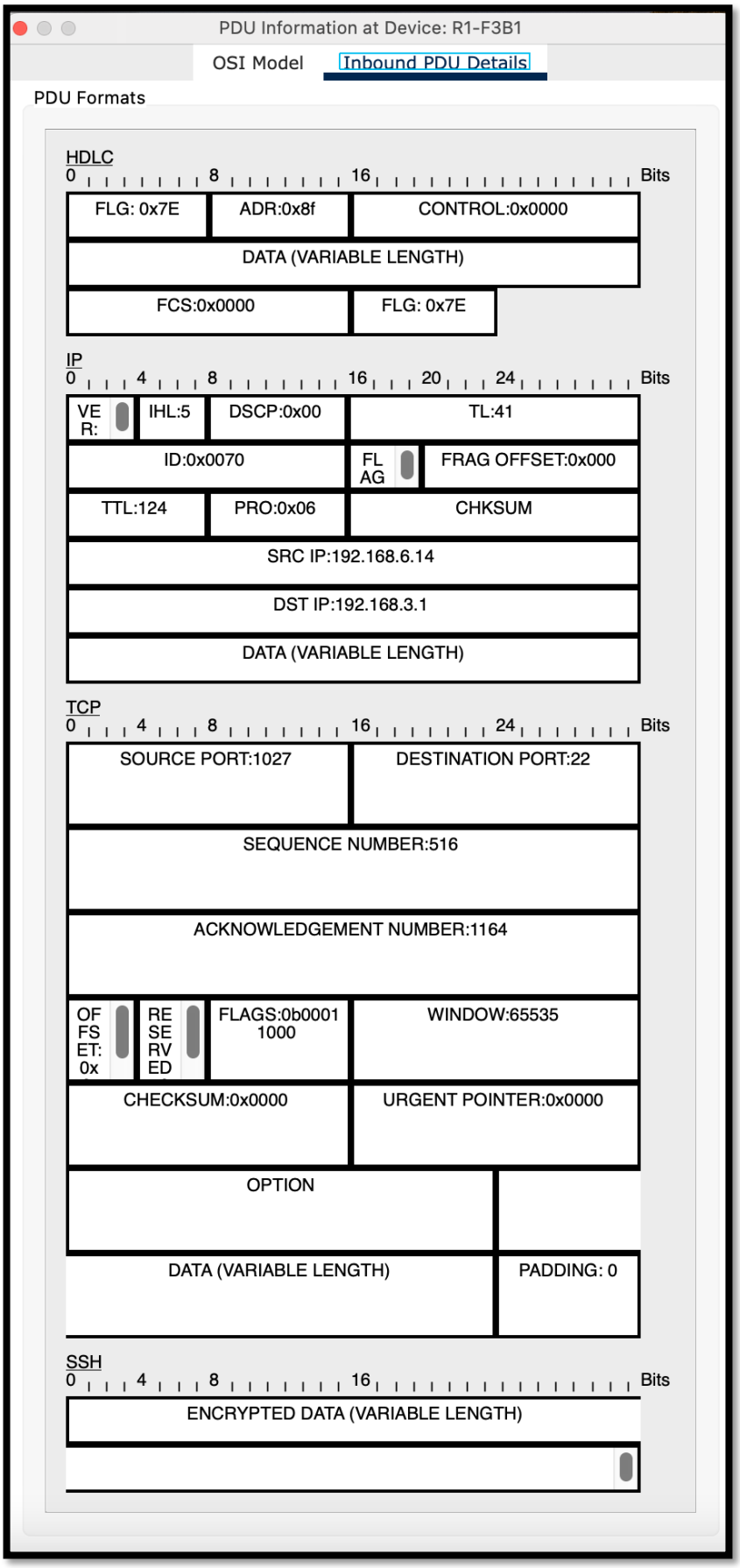


Figure 71: PDU Information at Device - R1-F3B1 – Inbound PDU details (In Layer)

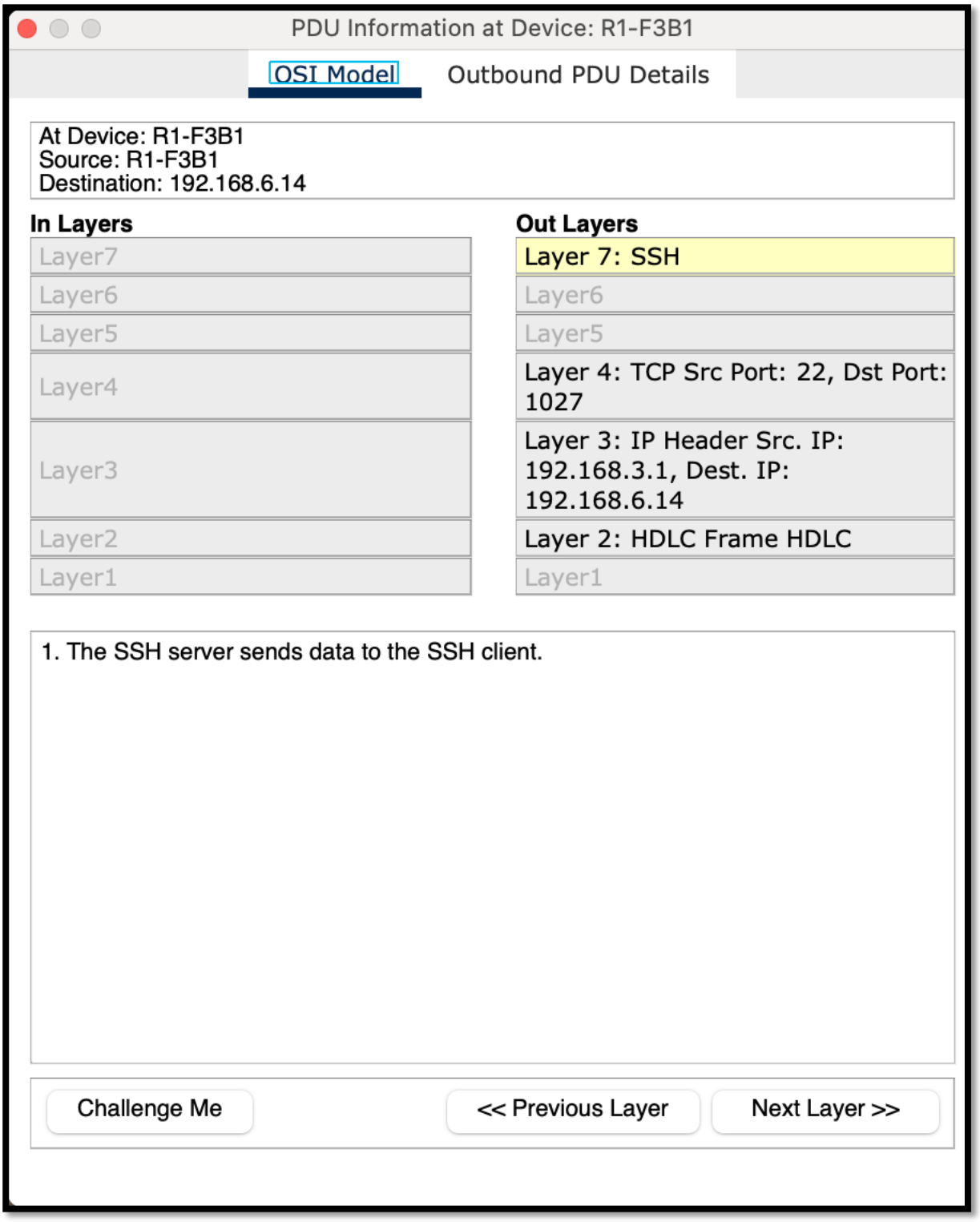


Figure 72: PDU Information at Device – R1-F3B1 – OSI Model (Out Layer)

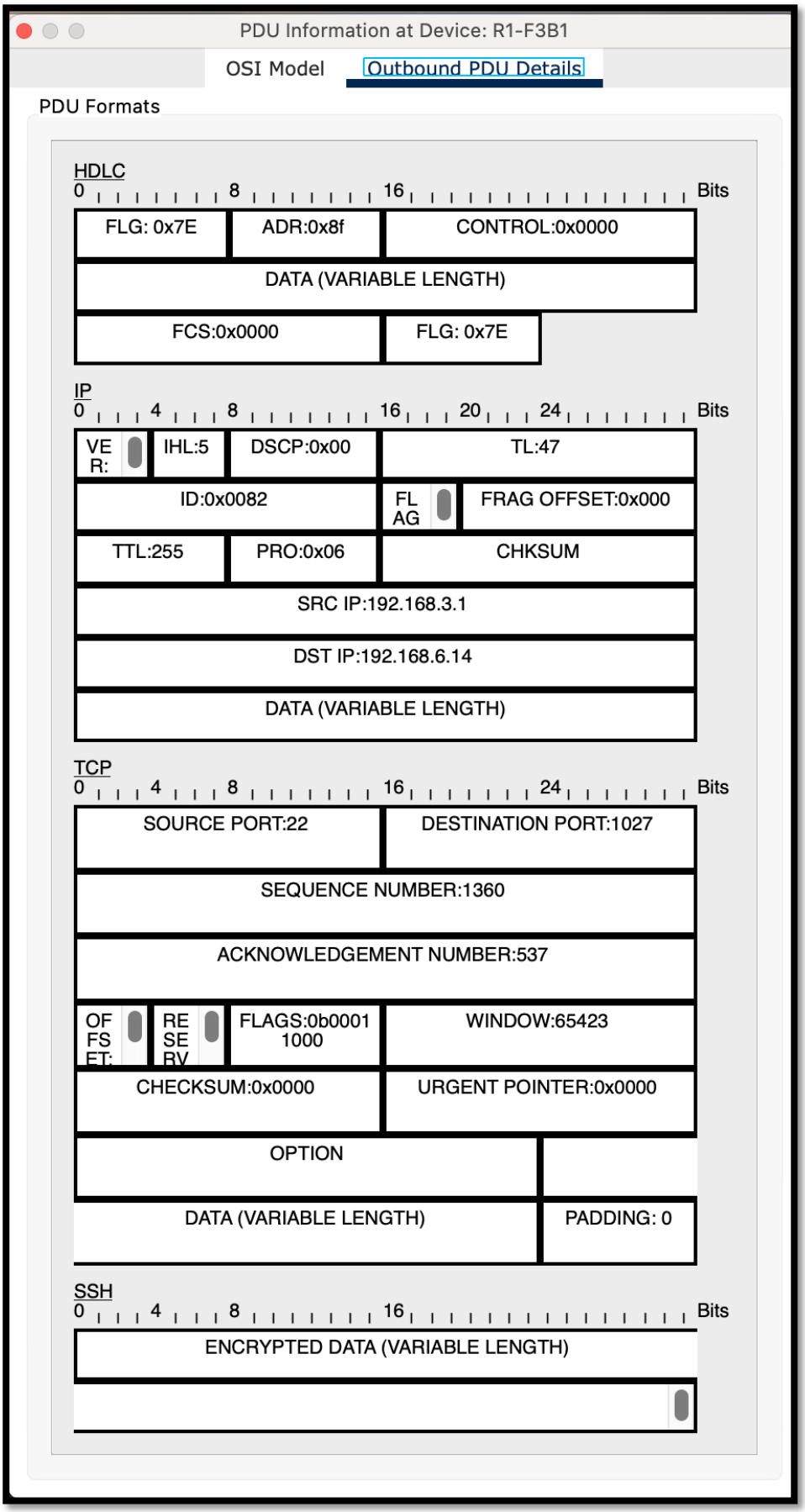


Figure 73: PDU Information at Device - R1-F3B1 – Inbound PDU details (Out Layer)

Additional Scenario 8: A Tablet User Receives and Replies to a Message

A tablet User from the first facility of the second branch wants to receive and reply to a message.

In this scenario, a user located in the **first facility of Branch 2**, using **TabletPC5-F1B2**, intends to **receive a message** (e.g., an email or instant message) and then **send a reply** to the sender. This process relies on proper network access, message server permissions, and routing through the appropriate communication protocols.

💬 **Message Reception and Reply Process (TabletPC5-F1B2)**

1. Network Initialization and IP Assignment:

TabletPC5-F1B2 connects to the wireless network of Facility 1 and receives an **IP address, default gateway, and DNS settings** from the local **DHCP server**, enabling access to internal and external services.

2. Client Application Setup:

The user utilizes a **messaging or email application** that has been previously configured with valid credentials. This client will use protocols such as:

- **IMAP or POP3** to receive messages (for email)
- **SMTP** to send responses (for email)
- Or a **real-time messaging protocol** if using a chat platform

3. Receiving the Message:

The client checks for new messages from the **server**:

- A **DNS query** may be issued to resolve the domain name of the message server to an IP address.
- Once resolved, the client **connects to the message server** (e.g., a mail server) and authenticates.
- If the tablet has access permissions, the server responds by **delivering the new message** to the tablet.

4. Access Control Check:

Before retrieving the message, **Access Control Lists (ACLs)** and **firewall rules** ensure that TabletPC5-F1B2 is permitted to communicate with the mail or messaging server.

- If permissions are granted, the communication proceeds.
- If access is denied, the message retrieval fails, and the user is notified.

5. Message Viewing and Response:

Upon receiving the message:

- The user opens it on the tablet.
- They type a reply and send it back using the configured client application.

6. Message Delivery (Reply):

- The client uses **SMTP or another sending protocol** to forward the reply message to the server.
- The server then handles **routing the message** to the recipient, using DNS if necessary to locate the correct destination server.

7. Network Flow:

Both incoming and outgoing packets:

- Travel through the **access point**, **local switch**, and **router** at Facility 1 of Branch 2.
- May pass through **inter-branch or internet routing**, depending on the recipient's location.
- Are securely delivered using encrypted connections if supported (e.g., SSL/TLS for email).

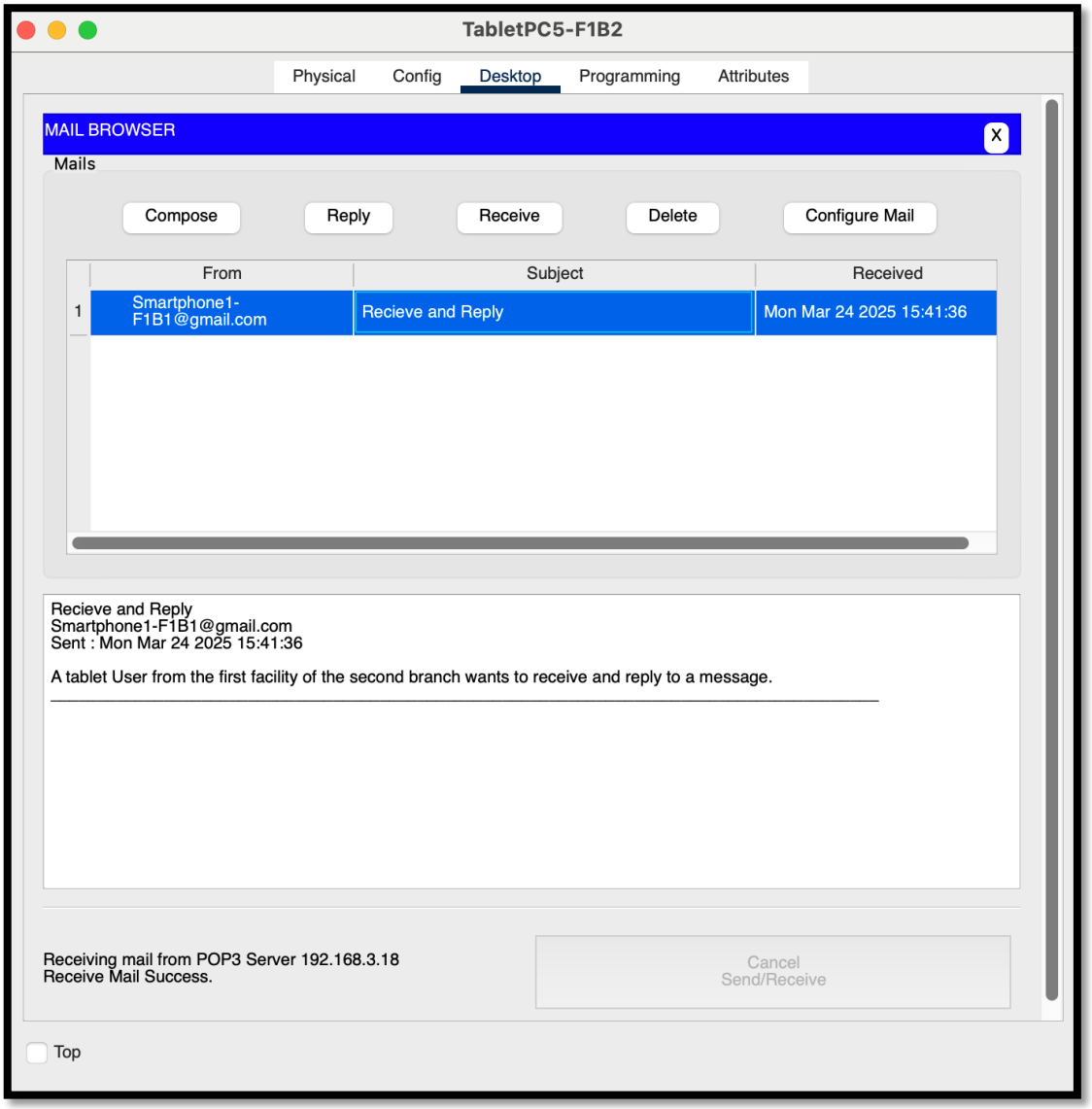


Figure 74: Received Email (Success)

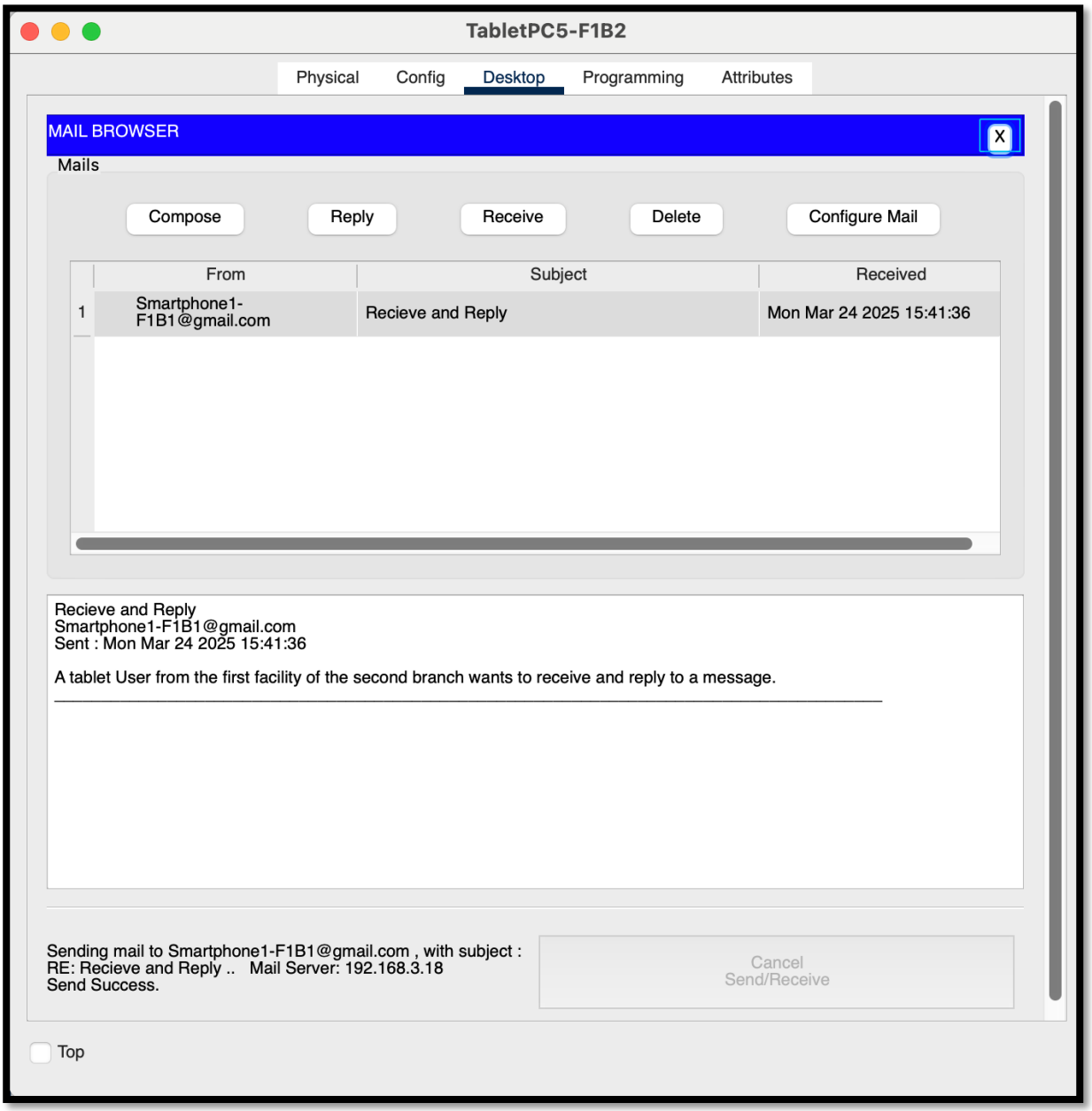


Figure 75: Reply to the Email (Success)

The following is the Result of the Simulation of Receive and Reply a Message:

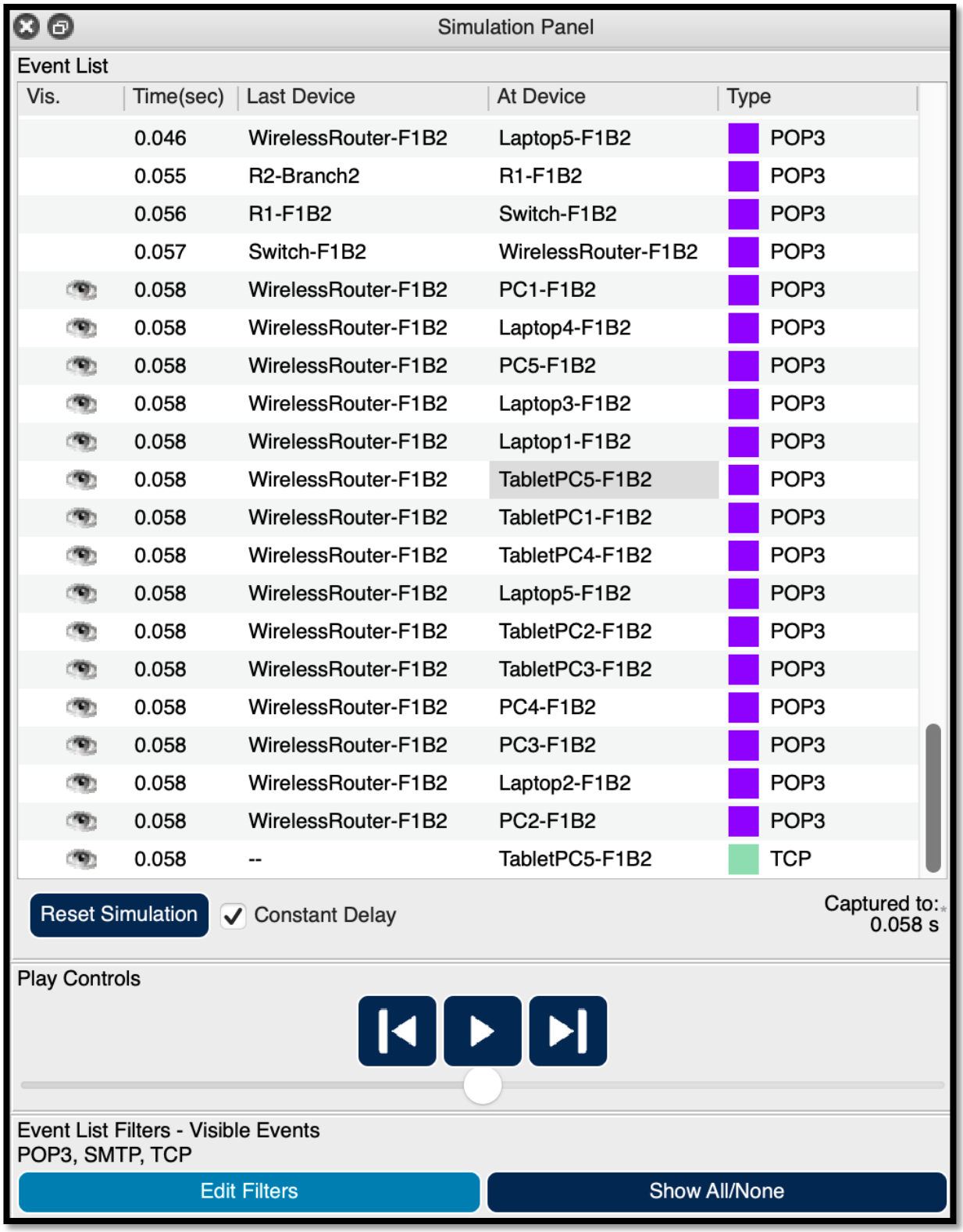


Figure 76: Simulation Panel (Receive)

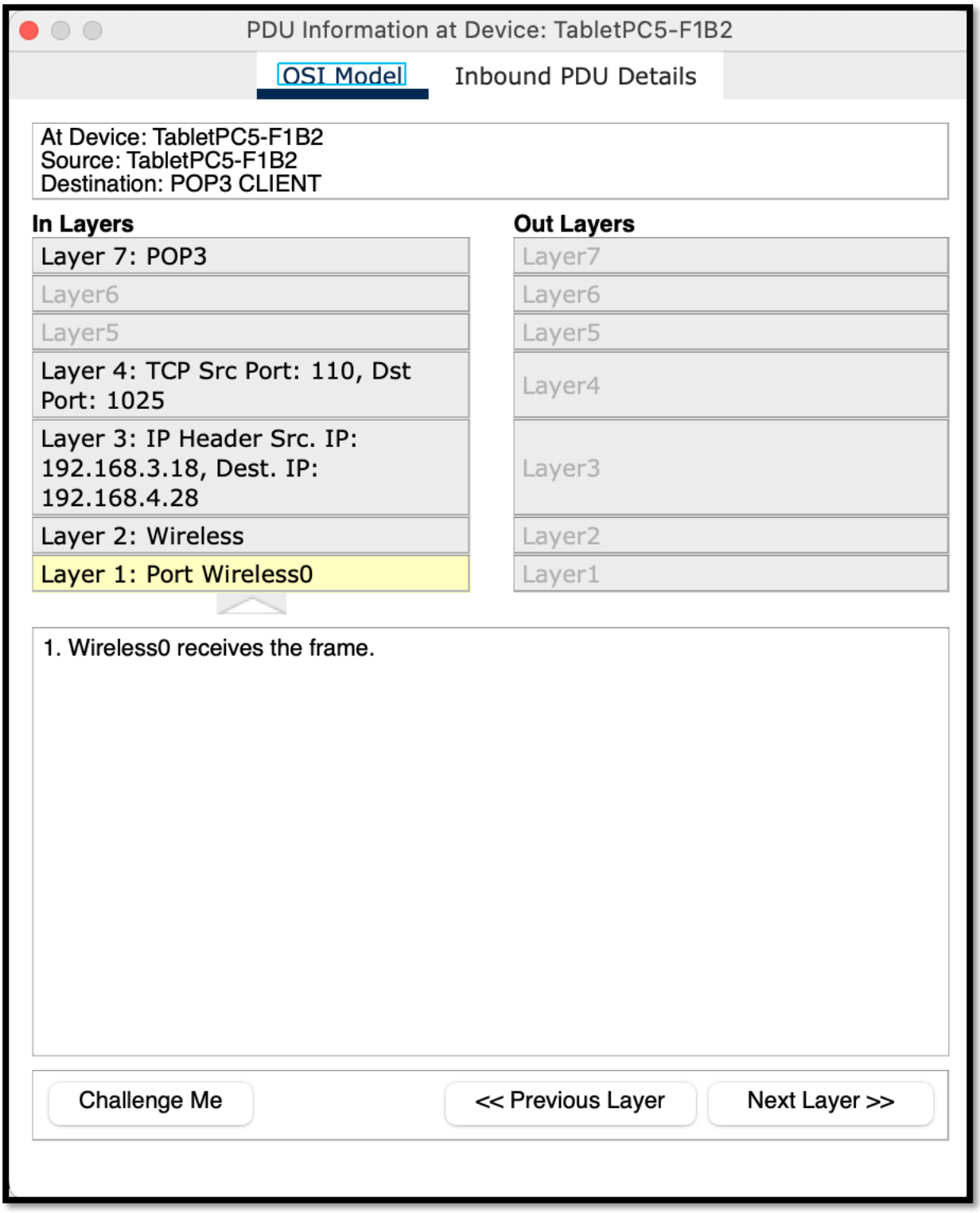


Figure 77: PDU Information at Device - TabeletPC5-F1B2 – OSI Model (Receive)

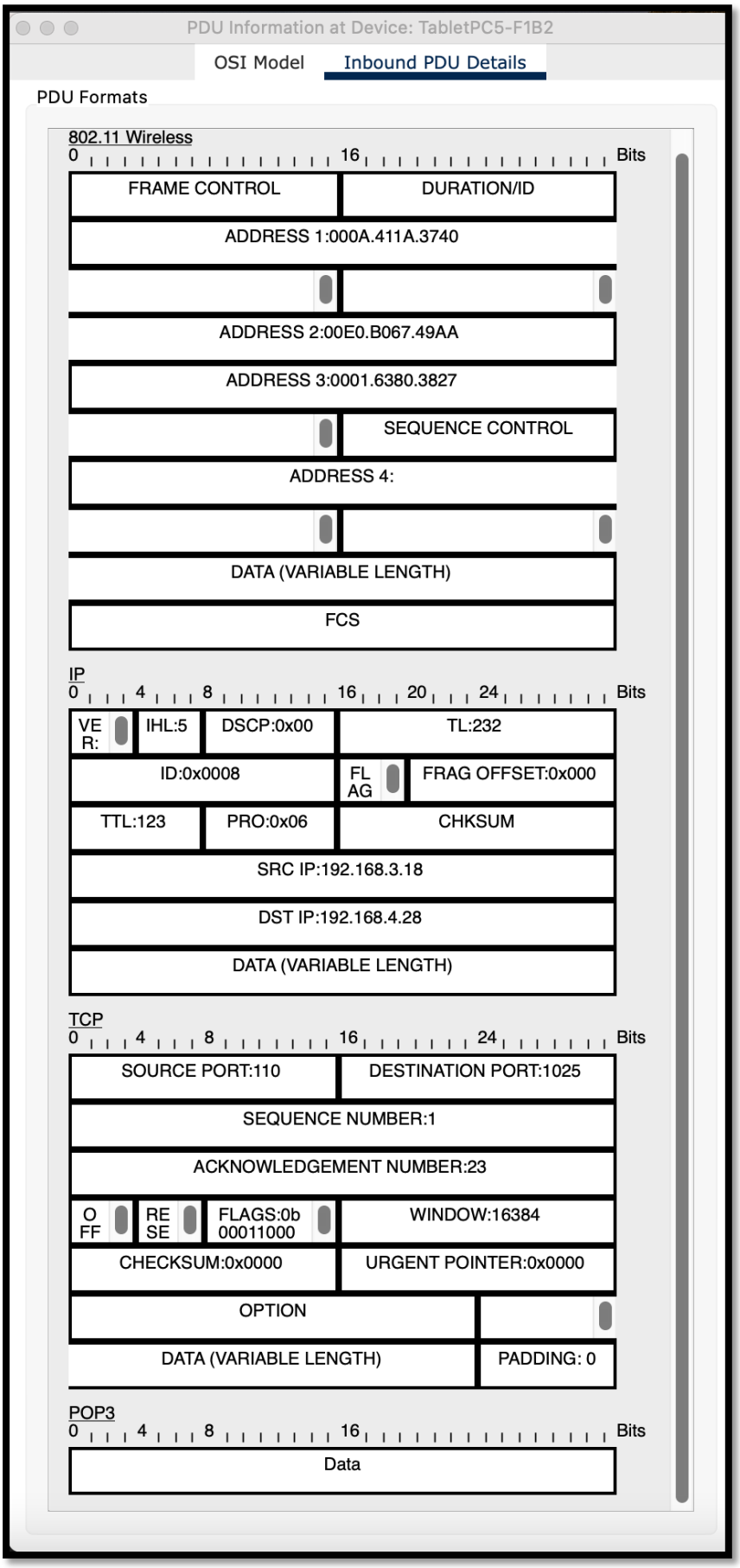


Figure 78: PDU Information at Device - TabletPC5-F1B2 – Inbound PDU details (Receive)

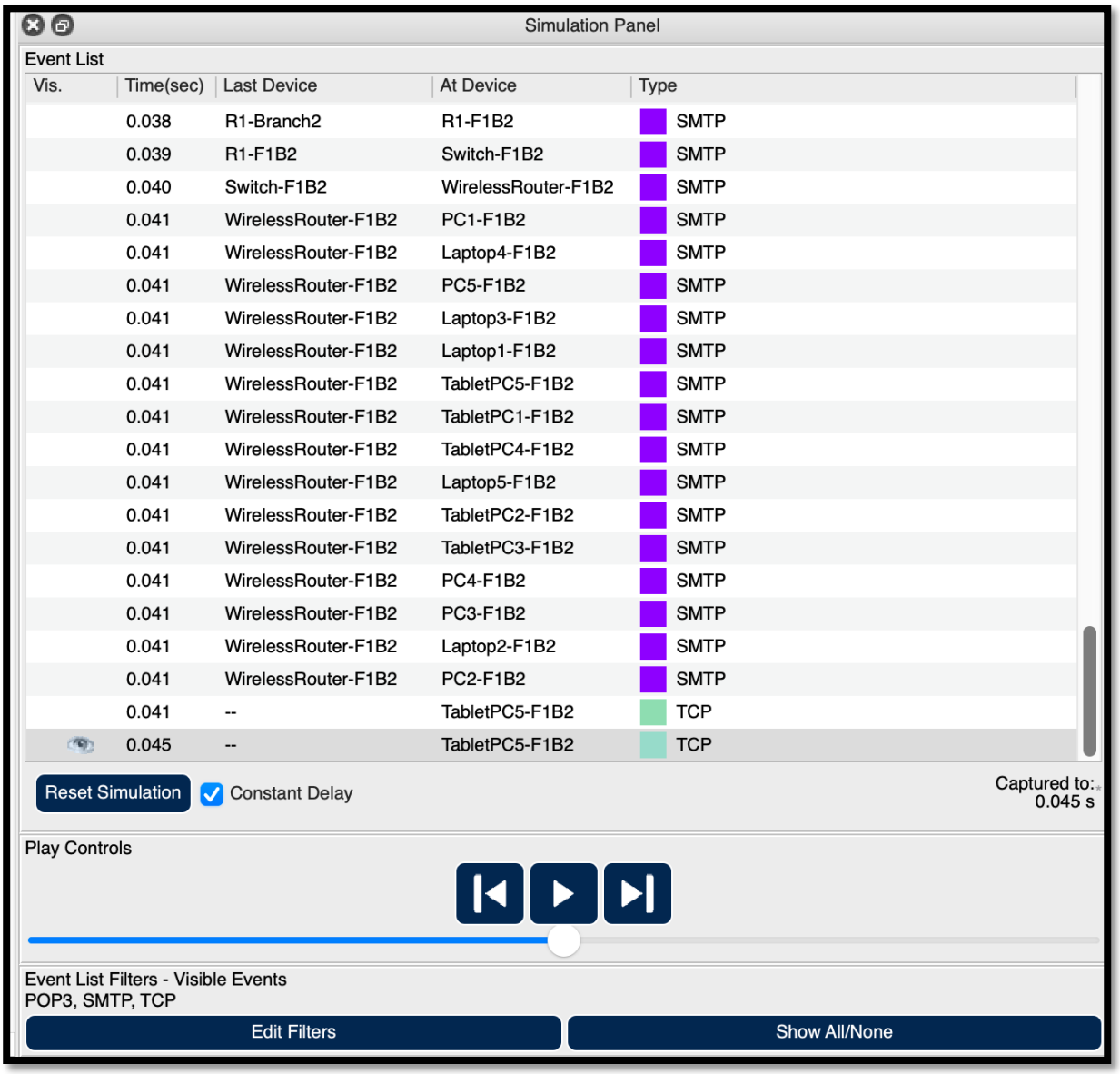


Figure 79: Simulation Panel (Reply)

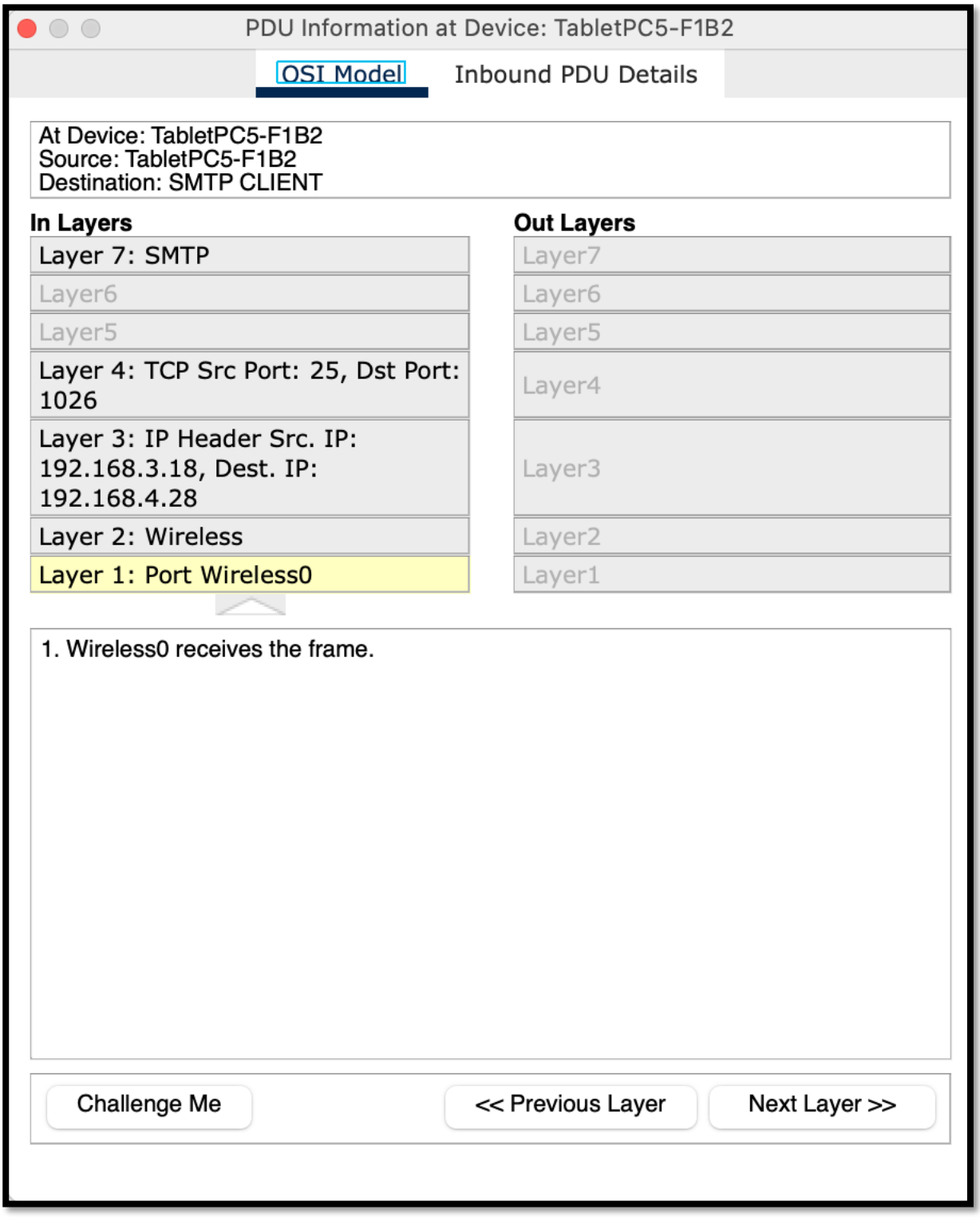


Figure 80: PDU Information at Device - TabeletPC5-F1B2 – OSI Model (Reply)

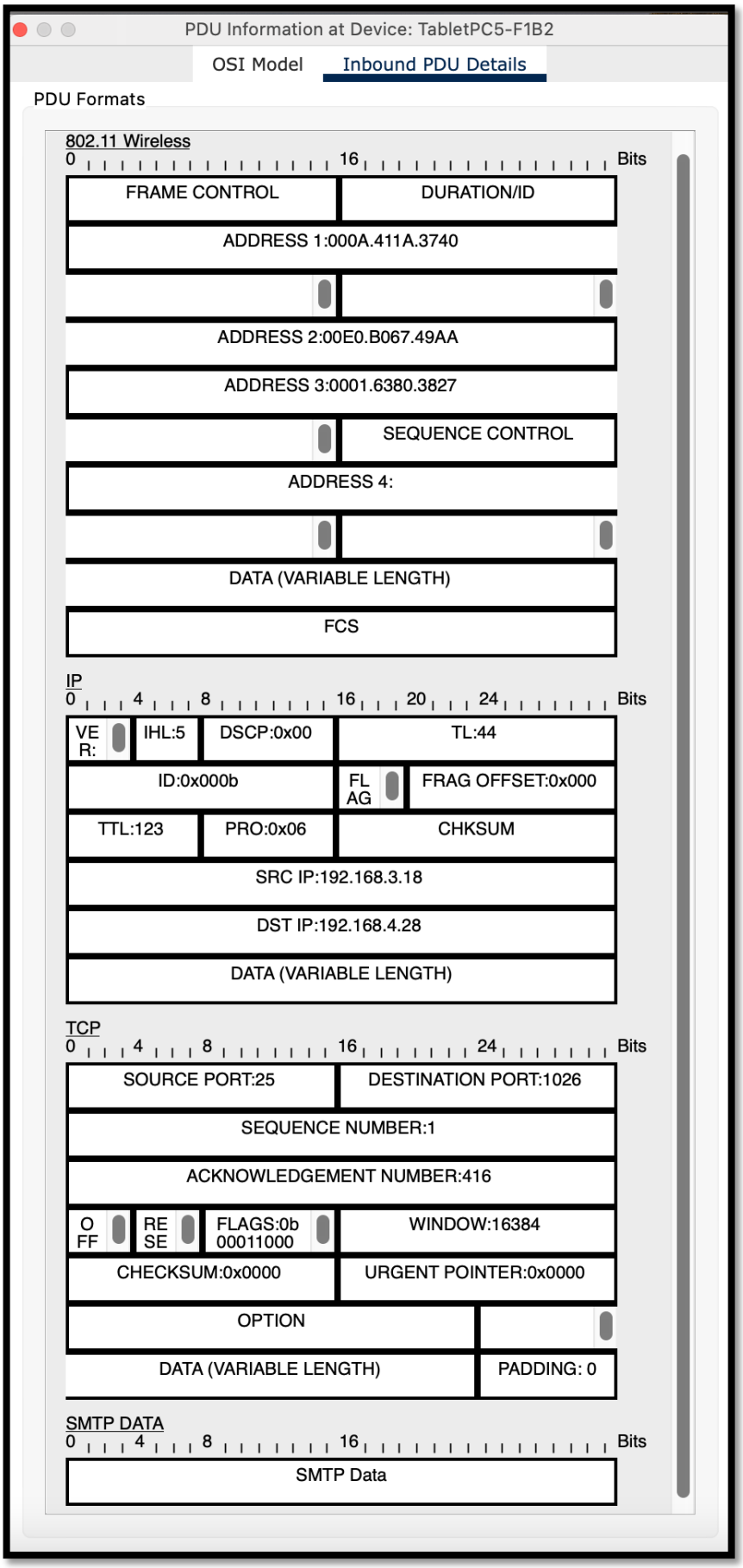


Figure 81: PDU Information at Device - TabletPC5-F1B2 – Inbound PDU details (Reply)

Additional Scenario 9: A VoIP User Calls an Unidentified Number

User from the first branch of the second facility call an unidentified number.

In this scenario, a user in the **second facility of the first branch** uses **VoIP1-F2B1** to initiate a voice call to an **unidentified or external number** that is not registered within the internal VoIP system. This action demonstrates how VoIP traffic is processed when the destination is not part of the local communication infrastructure.

📞 **Outbound VoIP Call Process to an Unidentified Number**

1. IP Address Configuration:

VoIP1-F2B1 connects to the local network and obtains its IP address, subnet mask, gateway, and DNS settings from the **DHCP server**, allowing it to participate in network communications.

2. VoIP Device Registration:

The VoIP device registers with the internal **SIP (Session Initiation Protocol) server**, which handles call control and routing for voice communications.

3. Call Initiation:

The user dials an **unidentified or external number** using the VoIP phone interface. Since the number is not recognized within the internal SIP directory:

- The SIP server attempts to route the call externally if such routing is configured.
- If **external call routing (like PSTN gateway or VoIP trunk)** is not available, the call will fail.

4. Routing and ACL Evaluation:

The SIP server or network infrastructure checks **Access Control Lists (ACLs)** and **call policies**:

- If the user lacks permission to make external calls, the request is blocked.
- If the policy permits outbound calls, the SIP server forwards the request to an **external VoIP gateway** or **Internet Telephony Service Provider (ITSP)**.

5. Gateway Handling (If Allowed):

If external VoIP routing is supported:

- The SIP server or PBX system forwards the call to a **VoIP-to-PSTN gateway**, which translates the VoIP call into a format suitable for public phone networks.
- The call proceeds to the external number via the internet or PSTN.

6. Call Rejection or Failure (If Blocked):

If no external call routing is configured, or if the ACLs deny access:

- The call fails with a **"number unreachable"** or **"call rejected"** message.
- The user may hear an error tone or a system-generated voice message indicating that the number could not be reached.

7. Logging and Monitoring:

All call attempts (successful or failed) are **logged by the SIP server** or call manager. Administrators can review these logs for:

- **Security auditing**
- **Policy enforcement**
- **Troubleshooting unauthorized call attempts**

Figure 82: Calling 5522 which is undefined result in Unknown Number

The following is the Result of the Simulation of VoIP calling an Undefined Number:

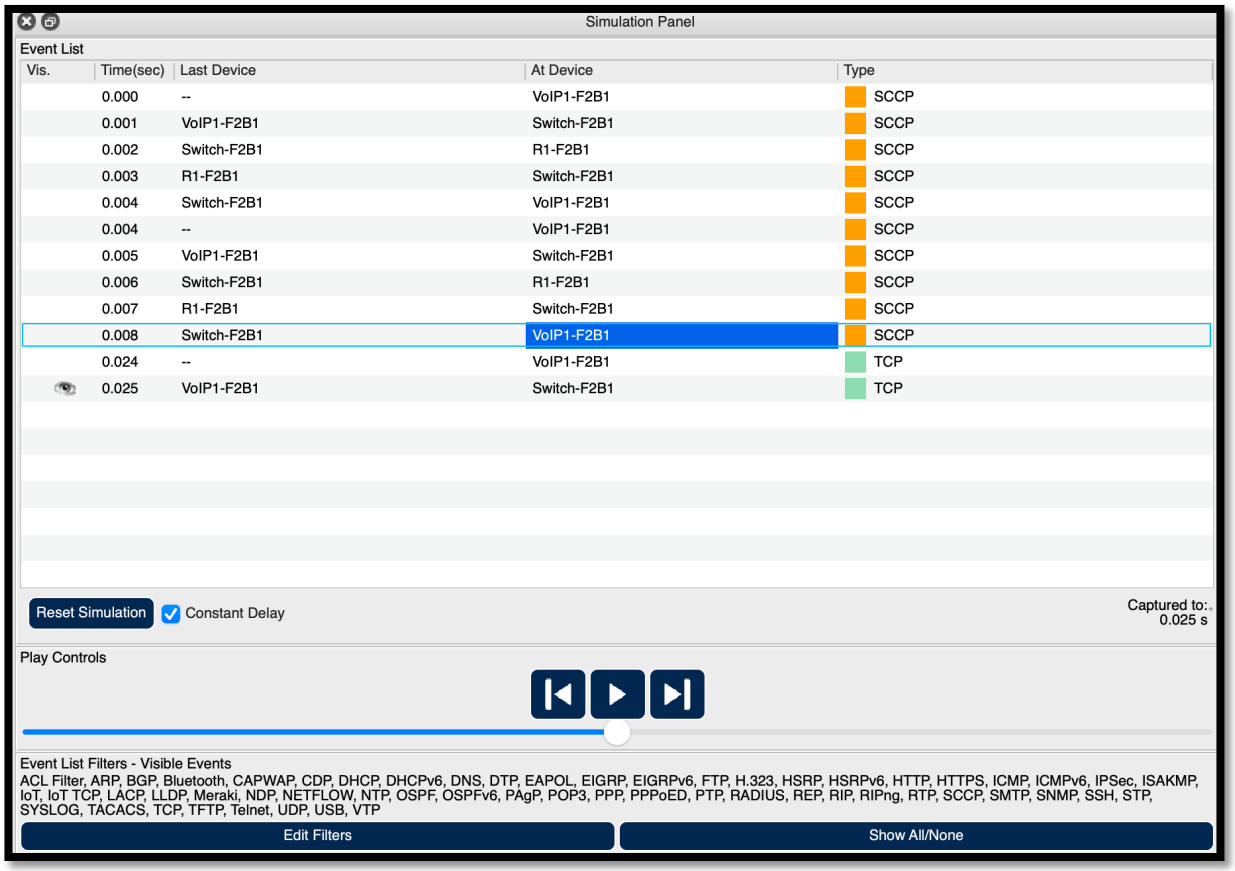


Figure 83: Simulation Panel

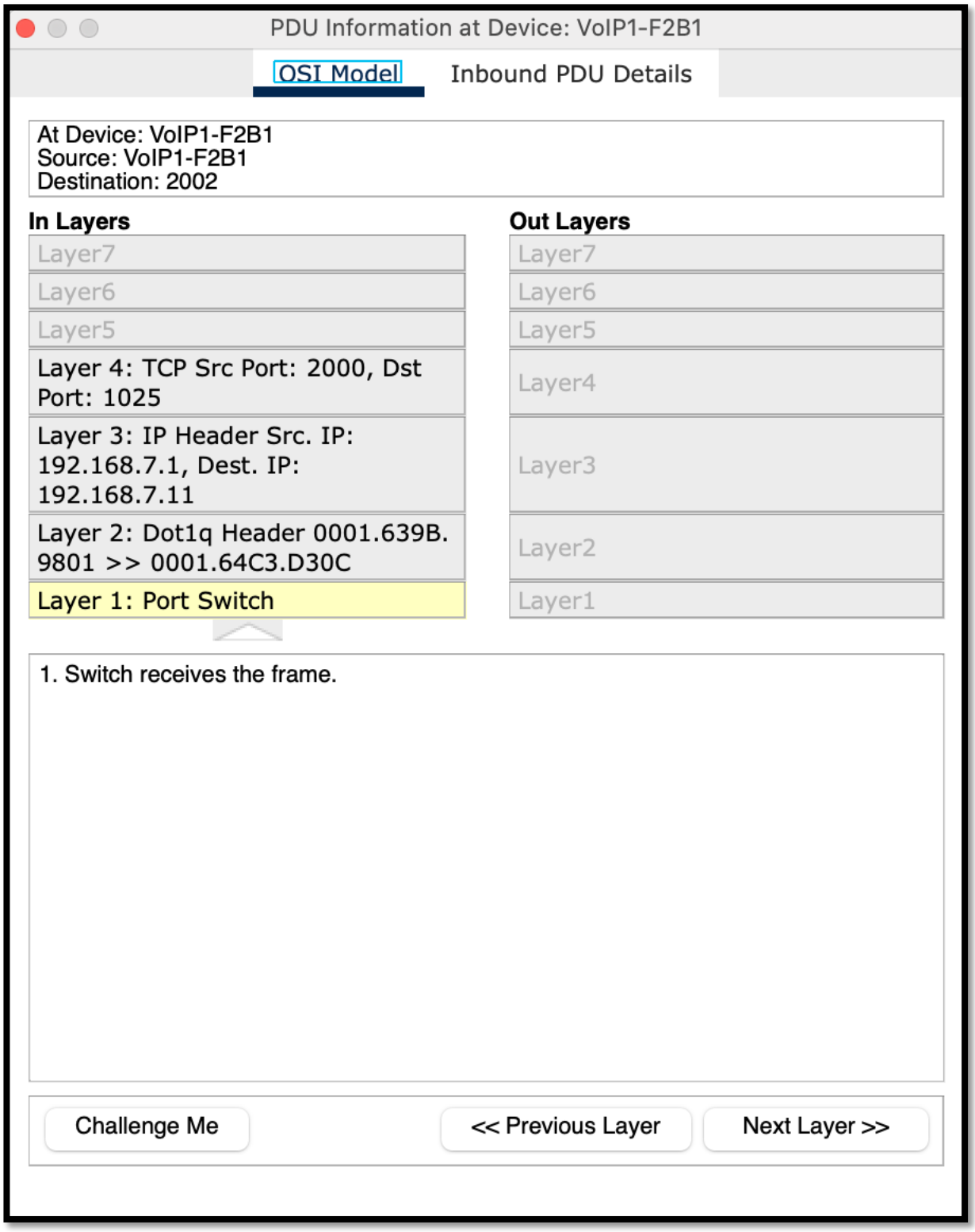


Figure 84:PDU Information at Device – VoIP1-F2B1 – OSI Model

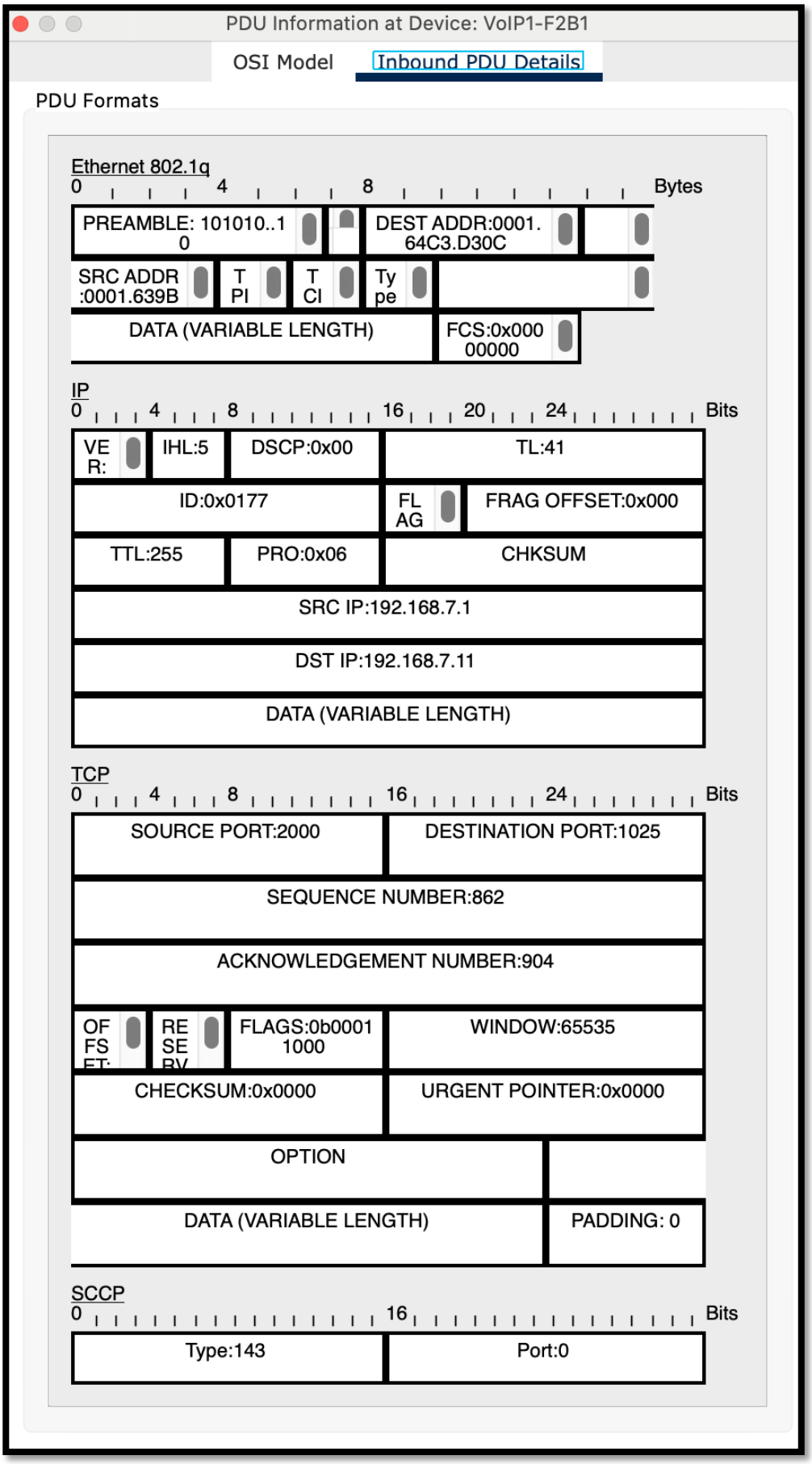


Figure 85: PDU Information at Device - VoIP1-F2B2 – Inbound PDU details

CHAPTER FOUR
PROBLEMS ENCOUNTERED

Throughout the course of the project, several challenges were encountered that required careful attention and troubleshooting. One of the primary issues involved network connectivity and device communication within the simulation. Initially, there were difficulties in establishing stable connections between different network devices, particularly between routers and switches. This required adjusting the configuration settings multiple times to ensure proper routing protocols and IP addressing were correctly set. These issues were primarily related to misconfigurations of the router interfaces and the failure to set up appropriate static routes, which led to communication breakdowns across the network.

Another challenge faced was the limited capabilities of Cisco Packet Tracer in simulating more complex network scenarios. While the tool is quite effective for learning fundamental concepts, certain advanced features required for real-world network configurations were not fully supported. This included limitations in configuring certain routing protocols and the inability to simulate more sophisticated security measures. These constraints forced us to think creatively and adapt to the software's capabilities, ensuring that we could still implement the required network functionalities within the bounds of the tool's features.

Finally, there were issues with simulating network traffic accurately, particularly during the simulation of real-time data transmission between different branches. Some of the traffic behaviors, such as delays and packet loss, were difficult to replicate with high fidelity. Although Simulation Mode helped in visualizing network traffic, it was challenging to mimic real-world latency and performance issues accurately. Despite these limitations, the team was able to adjust the network design and simulation parameters to achieve a functional and educational representation of the Metropolitan Area Network (MAN).

CHAPTER FIVE
CONCLUSION

In the Metropolitan Area Network Simulation project, we designed a network that connected two branches, each containing three distinct facilities, to support various functions such as user communication, file transfers, and web browsing. To ensure the network operated smoothly, it was essential to select and configure the right hardware—routers, switches, servers, and wireless devices—that would facilitate reliable connectivity. The successful implementation of the project was the result of continuous learning, thorough research, step-by-step accuracy checks, and strong collaboration among the group members. Each member actively participated in configuring devices and troubleshooting issues, allowing the team to complete the project through consistent effort and clear communication. The group carefully tested the network scenarios and verified that the chosen topology and architecture met the required features and functionality. Opting for a Metropolitan Area Network (MAN) instead of a Wide Area Network (WAN) gave us better control over security and speed, enabling efficient and secure communication within and between facilities. As a result, users across all facilities could successfully carry out their specific tasks, share servers between branches, and communicate regardless of whether they were in the same building or at a remote location. Through this long-term project, the team gained hands-on experience in network design, configuration, protocol implementation, and simulation using Cisco Packet Tracer. It also taught us valuable lessons in teamwork, task distribution, and the importance of synchronized efforts in achieving a complex technical goal.

CHAPTER SIX
REFERENCES

[1] Maria, A. (1997). *Introduction to modeling and simulation*. In *Proceedings of the 29th conference on Winter simulation*(pp. 7-13).

[2] Issariyakul, T., & Hossain, E. (2009). *Introduction to network simulation with NS2*. Springer Science & Business Media.

[3] Tanenbaum, A. S., & Wetherall, D. (2020). *Computer Networks* (6th ed.). Pearson.

[4] Stallings, W. (2017). *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud*. Pearson.

[5] Cisco Networking Academy. (2021). *CCNA Routing and Switching: Introduction to Networks*. Cisco Press.

[6] Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach* (8th ed.). Pearson.

[7] IEEE and ACM conference papers on MAN design, traffic engineering, and security in large-scale networks.

[8] RFC 791 – *Internet Protocol (IP)*, Internet Engineering Task Force (IETF).

[9] RFC 793 – *Transmission Control Protocol (TCP)*, Internet Engineering Task Force (IETF).

[10] RFC 2460 – *Internet Protocol Version 6 (IPv6) Specification*, Internet Engineering Task Force (IETF).

[11] RFC 1035 – *Domain Names - Implementation and Specification* (DNS), Internet Engineering Task Force (IETF).

[12] Computer Networking. (2019). How to configure an FTP server in Packet Tracer. https://computernetworking747640215.wordpress.com/2019/11/22/how-to-configure-an-ftp-server-in-packet-tracer/

[13] W7Cloud. Configuration of SSH on Cisco Switch in Packet Tracer. https://w7cloud.com/configuration-of-ssh-on-cisco-switch/

[14] YouTube. (2020). Web Traffic Simulation using Cisco Packet Tracer. https://www.youtube.com/watch?v=FF52mhKjmz0

[15] YouTube. (2020). Email Server Configuration in Cisco Packet Tracer | Cisco Packet Tracer Email Server | Mail Server. https://www.youtube.com/watch?v=otAZaqjjwl0

[16] YouTube. (2020). DNS, SMTP, FTP, and WEB Server configuration in Packet Tracer. https://www.youtube.com/watch?v=zad_sqJvtDQ

[17] Sharan IT Computer Blog. (2015). DHCP FAILED APIPA IS USED. https://sharanitcomputer.blogspot.com/2015/12/dhcp-failed-apipa-is-used.html

[18] IBM. The Fundamentals of Networking – IBM Cloud Learn Hub. https://www.ibm.com/think/topics/networking

[19] Computer Networking. (2018). Wireless Router configuration in Cisco Packet Tracer. https://computernetworking747640215.wordpress.com/2018/06/22/wireless-router-configuration-in-cisco-packet-tracer/