DOKUZ EYLÜL UNIVERSITY
FACULTY OF ENGINEERING
DEPARTMENT OF COMPUTER ENGINEERING

CME 3204
Data Communications and Computer Networks

METROPOLITAN AREA NETWORK SIMULATION PROJECT

by
2020510030 - Berkay Dinç
2020510034 - Yusuf Gassaloğlu
2020510066 - Güney Söğüt

CHAPTER 1

1. Introduction

This section summarizes the fundamental ideas of the metropolitan area network (MAN) project and includes background data, the problem domain, key concepts, the importance of the project, and the crucial role that Cisco Packet Tracer plays in our processes.

The main goal of our project is to improve and optimize the infrastructure of a metropolitan area network (MAN), taking into account issues like scalability limitations, security vulnerabilities, network congestion, and management difficulties. The fundamental framework of our MAN investigation is composed of key terms and concepts like routers, switches, subnets, VLANs (Virtual Local Area Networks), IP addressing, and security protocols.

This project is driven by the necessity to optimize and update MAN infrastructures in order to address changing security threats and technical demands. Through strengthening security protocols, optimizing network performance, and increasing administrative effectiveness, we strengthen the robust and resilient communication infrastructure that is necessary for both company productivity and society connectivity.

Metropolitan area networks (MANs) are essential networks that connect local and wide area networks and serve medium-sized geographic areas like cities and college campuses. Comprehending the development, features, and importance of MANs offers a framework for our project's goals and results.

As a result, Cisco Packet Tracer becomes our main tool for simulation and design. It allows us to mimic network behaviors, model intricate network topologies, and test suggested fixes in a virtual setting. It is a priceless tool for our network design and deployment projects because of its user-friendly interface and extensive feature set.

1.1. Project Definition and Problem Formulation

1.1.1 Definition of the Problem

A company needs a dependable and effective network connection for its two branch offices, which are situated in the same city. To support a range of user activities, these branches must seamlessly share resources and communicate with one another. To meet these needs, a design for a Metropolitan Area Network (MAN) will be created, and a simulation will be conducted.

1.1.2 Project Formulation

Using Cisco Packet Tracer software, this project attempts to create, simulate, and analyze a MAN. Two geographically separated branch offices will be connected by the MAN, allowing users to access common resources and carry out necessary duties. Our specifics tasks are as follows:

Network Design:

- There will be consideration of various connection technologies between the Internet Service Provider (ISP) and the MAN.
- Plans will be made for the network architecture of every branch office, which consists of three different locations with different server and user requirements.
- It will be decided which network hardware—routers, switches, etc.—and how to configure it—IP addressing, routing protocols, etc.

User Activity Simulation

- User activities will be defined for each facility, taking into account workstations, wireless users, tablets, smartphones, and servers.
- Web browsing, email, file transfers (FTP), VoIP calls, remote access (SSH), and ping queries should all be included in this list of activities.
- We will create comprehensive scenarios that show communication between various branches and services for a minimum of seven user activities.
  There will be two more user-defined tasks that highlight particular network features.

Network Simulation and Analysis

- User activities will be defined for each facility, taking into account workstations, wireless users, tablets, smartphones, and servers.
- Web browsing, email, file transfers (FTP), VoIP calls, remote access (SSH), and ping queries should all be included in this list of activities.
- We will create comprehensive scenarios that show communication between various branches and services for a minimum of seven user activities.
- There will be two more user-defined tasks that highlight particular network features.

Success Criteria

- A well-thought-out, thoroughly documented MAN architecture that satisfies the requirements.
- A working simulation of Cisco Packet Tracer that faithfully captures the architecture of the network.
- A complete report that discusses the project in detail, evaluates the simulation results, and shows that the author has a solid grasp of network concepts.
  Originality and inventiveness in the user activity situations and design.

Following the project's successful conclusion, we will have the following deliverables.

A plan for design

- A thorough map, resembling a high-level network diagram, that describes the physical layout of the network, including the kind and location of devices (switches and routers) in each branch and their connections to the internet and other networks.

- Configuration parameters include how each device will be "programmed" to communicate with one another and effectively route data.

A simulation for our design

- A virtual representation of the intended network created with Cisco Packet Tracer.
- With the help of this model, we will have a way to mimic common user actions (such as emailing or holding video conferences) and observe how the network responds.
- Before constructing the actual network, our team might have a possibility to find possible bottlenecks or design flaws by examining the simulation findings.

1.2. The purpose and motivation of the project

The Metropolitan Area Network (MAN) Simulation Project is our secret weapon when it comes to solving the challenging task of establishing office networks. You know how sometimes we take classes and learn all these theories, but we never really know how they work in practice? This effort, however, rewrites that story. Using Cisco Packet Tracer to create and optimize office network configurations is the key to success.

Consider this: rather than only reading about network design, we are able to build networks from the ground up that are specifically suited to the requirements of actual office spaces. That's significant given the importance dependable and efficient networks are to the seamless operation of businesses.

Additionally, this endeavor is a career goldmine. It's more important to acquire real abilities that we can showcase to potential employers than it is to just receive a grade. They want proof that we are capable of establishing networks in office settings right away, and this project provides just that.

Completing this assignment is necessary for professional and scholarly growth. It closes the knowledge gap between theory and practice by giving students practical experience and skills that they can use right away in the industry. We highlight the project's relevance and potential influence on educating students for careers in network engineering, system administration, and related sectors by framing it as an improved solution to the current issue of developing office topologies.

The main benefits of the project include:

- Tailored solutions: We gain experience in designing office network topologies that are specifically optimized for the unique requirements and constraints of office environments.

- Practical skills development: Through hands-on simulation, we acquire proficiency in using network simulation tools and implementing real-world network configurations.

- Business relevance: The project addresses a pressing need for skilled professionals capable of designing and managing office networks effectively, enhancing the employability of graduates.

- Innovation and efficiency: By leveraging simulation tools, we can explore and test different network designs and configurations, leading to more innovative and efficient solutions for office topologies.

1.3. Term Definitions

1.3.1 Router

Definition: A network device that forwards data packets between computer networks. Routers operate at the network layer of the OSI model and use routing tables to determine the best path for forwarding packets. They can connect different network segments and facilitate communication between devices on separate networks.

1.3.2 Switch

Definition: A network device that connects multiple devices within a local area network (LAN) and forwards data packets between them. Switches operate at the data link layer of the OSI model and use MAC addresses to determine the destination of incoming packets. They provide efficient and secure communication within LANs by creating dedicated connections between devices.

1.3.3 Server

Definition: A computer or software application that provides services or resources to other computers, known as clients, within a network. Servers can fulfill various roles, such as hosting websites, storing files, managing user authentication, and running applications accessible to network users.

1.3.4 FTP Server (File Transfer Protocol Server)

Definition: A type of server that enables the transfer of files between computers over a network using the File Transfer Protocol (FTP). FTP servers allow users to upload, download, and manage files stored on the server, making them accessible to authorized users or clients.

1.3.5 NTP Server (Network Time Protocol Server)

Definition: A server that synchronizes the time of computers and other devices within a network. NTP servers maintain accurate time by receiving time signals from reliable sources, such as atomic clocks or other NTP servers, and distributing them to network clients. Synchronized time is essential for coordinating activities, logging events, and ensuring consistency in distributed systems.

1.3.6 Mail Server

Definition: A server that handles the sending, receiving, and storage of email messages within a network. Mail servers use protocols such as SMTP (Simple Mail Transfer Protocol)

for sending emails and POP3 (Post Office Protocol) or IMAP (Internet Message Access Protocol) for retrieving emails from mailboxes.

1.3.7 Ethernet

Definition: A widely used networking technology that defines the physical and data link layers of the OSI model for wired LANs. Ethernet networks use coaxial cables, twisted pair cables, or fiber-optic cables to transmit data between devices. Ethernet employs CSMA/CD (Carrier Sense Multiple Access with Collision Detection) for managing access to the network medium and ensuring reliable communication.

1.3.8 DNS (Domain Name System)

Definition: A hierarchical naming system that translates domain names, such as www.example.com, into IP addresses, such as 192.0.2.1, enabling computers to locate and communicate with each other on the Internet or private networks. DNS servers maintain databases of domain name records and provide name resolution services to network clients.

1.3.9 IP (Internet Protocol)

Definition: A network protocol that defines the rules for addressing and routing packets of data across networks. IP operates at the network layer of the OSI model and assigns unique IP addresses to devices connected to a network, facilitating communication between them. IPv4 and IPv6 are the two main versions of the Internet Protocol.

1.3.10 DHCP (Dynamic Host Configuration Protocol)

Definition: A network protocol that automatically assigns IP addresses and other network configuration parameters to devices within a network. DHCP servers dynamically allocate IP addresses from a pool of available addresses and provide additional configuration information, such as subnet masks, default gateways, and DNS server addresses, to DHCP clients.

1.3.11 TCP (Transmission Control Protocol)

Definition: A reliable, connection-oriented transport protocol that provides error checking, flow control, and congestion avoidance mechanisms for transmitting data between devices on a network. TCP operates at the transport layer of the OSI model and ensures that data packets are delivered accurately and in the correct order, making it suitable for applications requiring guaranteed delivery, such as web browsing, email, and file transfer.

1.3.12 VoIP Phones (Voice over Internet Protocol Phones)

Definition: Telephones or communication devices that use VoIP technology to transmit voice calls over IP networks, such as the Internet or corporate LANs. VoIP phones convert analog voice signals into digital data packets for transmission over IP networks, enabling cost-effective and feature-rich voice communication services.

1.3.13 SSH (Secure Shell)

Definition: A cryptographic network protocol that provides secure, encrypted communication and remote access to devices over unsecured networks. SSH allows users to securely log in to remote servers or devices, execute commands, transfer files, and tunnel other network services, protecting sensitive data from eavesdropping and tampering.

1.3.14 Node

Definition: A device or connection point within a network that can send, receive, or process data. Nodes can include computers, servers, routers, switches, printers, or any other networked device.

1.3.15 Packet

Definition: A unit of data transmitted over a network. A packet typically consists of a header, payload, and trailer. The header contains control information, such as source and destination addresses, while the payload carries the actual data being transmitted.

1.3.16 Channel

Definition: A communication pathway or medium through which data is transmitted between nodes in a network. Channels can be physical, such as copper wires, fiber-optic cables, or wireless radio frequencies, or logical, such as virtual connections established over a shared network infrastructure.

1.3.17 Protocol

Definition: A set of rules, conventions, or standards governing the format, timing, sequencing, and error handling of communication between nodes in a network. Protocols define how data is transmitted, received, and processed, ensuring compatibility and interoperability among networked devices.

1.3.18 System

Definition: A collection of interconnected components or elements that work together to perform a specific function or task. In the context of the MAN Simulation Project, a system may refer to the network infrastructure, including hardware devices, software applications, and communication protocols, configured to simulate a metropolitan area network.

1.3.19 Architecture

Definition: The overall structure, design, and organization of a system or network. Network architecture defines the arrangement of nodes, channels, protocols, and other elements within a network, as well as the interactions and relationships between them. It encompasses both the physical layout of hardware components and the logical framework of software protocols and services.

1.3.20 Topology

Definition: The physical or logical layout of interconnected devices and communication links in a network. Network topology defines how nodes are arranged and how data is transmitted between them. In the context of the project, students design and implement various network topologies suitable for office environments.

1.3.21 Configuration

Definition: The process of setting up and adjusting the parameters of network devices and services to meet specific requirements. Configuration involves tasks such as assigning IP addresses, configuring routing protocols, and establishing security policies within the simulated network environment.

1.4. Related Work

Several initiatives have investigated the design and simulation of metropolitan area networks (MANs) to maximize network performance and resource allocation among geographically dispersed locations. Here, we talk about two pertinent projects that are somewhat similar to ours:

- Zafer Yalçın et al. **Metropolitan Area Network Simulation for University Campuses** [1] builds and simulates a MAN between two university campuses using Cisco Packet Tracer. With a particular focus on supporting online learning resources and video conferencing applications, this project aims to give faculty, staff, and students dependable network access. It uses Packet Tracer for simulation, just like our project, and takes care of the needs of the user for email, file transfers, and web browsing. To serve a wider range of business-critical applications, our project builds on this by adding features like Voice over IP (VoIP) calls and remote access.

- Doğukan Berk Özer et al. use Cisco Packet Tracer to model and simulate a Metropolitan Area Network (MAN) connecting two university campuses in **Metropolitan Area Network on Cisco Packet Tracer** [2]. The project highlights the significance of network security and integrates firewalls as a means of safeguarding against possible hazards.

These related projects demonstrate the usefulness of Cisco Packet Tracer for network simulation and offer insightful information about MAN design principles. By adding more user functionalities and emphasizing network performance optimization for business communication within a Metropolitan Area Network, our project expands on these foundations.

CHAPTER 2

2. Method and Simulation

Our abstract dives deeply into the intricate considerations of modeling and simulating a metropolitan area network (MAN) infrastructure, focusing on routing, switch technologies, VoIP (Voice over Internet Protocol), and RIP (Routing Information Protocol) as fundamental components. The objectives of this methodology are to improve performance, strengthen security, increase scalability, guarantee dependability, and simplify management in the MAN environment.

Increasing scalability is accomplished by utilizing dynamic routing and VLAN (Virtual Local Area Network) technology. By enabling logical network segmentation, VLANs enhance traffic isolation, resource allocation, and network efficiency. In order to support smooth network expansion and rising demand without sacrificing performance, dynamic routing technologies dynamically modify routing tables in response to changes in network topology.

We came across limitations that affected our design choices as we went through the modeling and simulation phases. Our decision to select reasonably priced hardware and software solutions that still fulfill performance standards was influenced by budgetary restrictions. Effective equipment deployment and cable management techniques were required due to physical space constraints. Respect for privacy laws, industry standards, and data protection legislation was required due to regulatory compliance concerns. Planning for IP addresses, bandwidth management, and resource distribution have to be done optimally due to resource availability limits. Requirements for compatibility ensured that VoIP systems, switch technologies, routing protocols, and network services could all function seamlessly together.

In order to build a MAN infrastructure that is both high-performance and resilient enough to support VoIP communications, while also guaranteeing scalability, security, reliability, and effective management practices that are specifically designed to meet the changing needs of contemporary digital connectivity, our modeling approach carefully considered these requirements and constraints.

2.1. Simulation and Modeling Concepts

Advantages of Simulation and Modeling Compared to Real Implementations:

2.1.1 Benefits of Modeling and Simulation over Real Implementations:

- ***Cost-Effectiveness:*** By enabling testing and experimenting of many scenarios without the need for physical hardware, modeling and simulation lower the expenses related to development and testing in real-world settings.

- ***Risk Reduction:*** By identifying possible problems, bottlenecks, or vulnerabilities in a system before it is actually implemented, simulation helps to reduce the risks and uncertainties that come with introducing new procedures or technology.

- ***Flexibility and Scalability:*** Simulation environments offer flexibility for experimentation and optimization since they are easily scalable, replicable, and adaptable to different scenarios, setups, and needs.

- ***Time Efficiency:*** Rapid prototyping, iteration, and controlled evaluation of alternative solutions are made possible by modeling and simulation, which speeds up the project's design, development, and testing phases.

2.1.2 Challenges of Modeling and Simulation:

- ***Model Accuracy:*** It can be difficult to create accurate models that faithfully capture the dynamism and complexity of real systems. The model's assumptions, simplifications, or uncertainties could cause differences between the simulated and real behaviors.

- ***Validation and Verification:*** Strict validation and verification procedures are needed to ensure that the model faithfully replicates real-world occurrences and behaviors, which is necessary to ensure the validity and dependability of simulation results.

- ***Resource Restrictions:*** The size, accuracy, and complexity of simulations may be restricted by computing resources, such as memory, processing power, or storage.

- ***Interpretation and Generalization:*** Domain expertise, critical analysis, and careful examination of contextual elements and assumptions may be necessary when interpreting simulation output and turning discoveries into practical insights or decisions.

2.2. Cisco Packet Tracer

2.2.1 Architecture and Modeling Concepts:

Cisco Packet Tracer employs a client-server architecture. The client side consists of a graphical user interface (GUI) where users design network topologies and configure devices.

The server side runs the simulation engine, which executes user-defined configurations and models network behavior based on predefined protocols and algorithms.

2.2.3 Modeling Approach:

Packet Tracer adopts a discrete-event simulation approach to model the behavior of computer networks. It simulates the transmission of data packets between network devices based on predefined configurations and network protocols, such as routing, switching, and addressing.

2.2.4 Capabilities:

- Supports simulation of various network devices, including routers, switches, PCs, servers, and VoIP phones.
- Provides a comprehensive set of network protocols, services, and features for configuring and testing network environments.
- Includes simulation modes for real-time, simulation, and hybrid (real-time and simulation) operation.

2.2.5 Limitations:

- May lack some advanced networking features and protocols found in production environments.
- Resource constraints may limit scalability and performance for large-scale or complex network simulations.
- Limited support for integration with external systems or third-party software tools.

2.2.6 Programming or Running a Simulation:

The GUI interface of Cisco Packet Tracer is its main operating mechanism, enabling users to interactively simulate network behavior, configure devices, and create network topologies. Users can connect devices with cables, drag and drop network components onto a virtual workspace, and use the integrated setup dialogs to customize the parameters of each device.

2.2.7 Modules, Libraries, Components:

Packet Tracer includes a library of network devices, interfaces, protocols, and simulation scenarios that users can utilize to design and simulate various network topologies and configurations. Some key components include:

- ***Routers:*** Represented by various Cisco router models, supporting routing protocols like OSPF and EIGRP.
- ***Switches:*** Represented by Cisco Catalyst switches, supporting VLANs, spanning tree protocol (STP), and port security features.
- ***PCs and Servers:*** Simulated host devices running operating systems like Windows and Linux, capable of running applications and services.
- ***VoIP Phones:*** Simulated IP phones for testing voice-over-IP (VoIP) communication.

- ***Simulation Modes:*** Real-time mode for live interaction, simulation mode for offline testing, and hybrid mode for a combination of real-time and simulated operation.

2.2.8 Disadvantages:

- Limited scalability and support for complex enterprise network configurations.
- May lack some advanced networking features and protocols found in production environments.
- Not suitable for large-scale or performance-intensive simulations due to resource constraints.

2.2.8 Advantages:

- User-friendly interface suitable for beginners and educational purposes.
- Comprehensive set of network devices, protocols, and features for simulating real-world network scenarios.
- Interactive simulations that allow users to visualize and understand network behaviors.

2.3. Network Design Requirements

2.3.1 Design Overview:

We chose a tree topology in our network design since it is scalable and allows for effective branch and facility connections. Robust voice communication capabilities are ensured by the strategic deployment of Cisco 2811 routers for VoIP configuration and inter-facility routing. Network performance and security are maximized by the strategic placement of managed switches for traffic control and local network segmentation. In order to offer extensive coverage for wireless communication, wireless access points (APs) are established. TCP/IP is used for general communication on our network, along with DHCP for automated IP assignment, SMTP/POP3/IMAP for email services, HTTP/HTTPS for web access, FTP for file transfers, and VoIP protocols for smooth voice connections. In order to facilitate IP management, data interchange, and communication throughout the network, we have also included dedicated mail servers, FTP servers, and a DHCP server. In order to provide a stable and secure network environment, firewall rules, VLAN segmentation, access control lists, and centralized network management tools are used to strengthen network security.

2.3.2 Design Components:

2.3.2.1 First Branch:

- **First Facility:**

  Users: 3 Workstation (PC) users, 3 Wireless (laptop) users, 3 Smartphone users

Capabilities: Browsing the web, sending emails, transferring files

- **Second Facility:**
  Users: 6 Workstation users
  Capabilities: Web browsing, FTP usage, VoIP conference support for 2 workstations
- **Third Facility (Server Farm):**
  10 Web Servers
  4 FTP Servers
  1 DHCP Server
  1 Mail Server
  1 Domain Name Server (DNS)

2.3.2.2 Second Branch:

- **First Facility:**
  Users: 5 Workstation users, 5 Wireless users, 5 Tablet users
  Capabilities: Wireless internet access, web browsing, email usage
- **Second Facility:**
  Users: 5 Workstation users, 2 Smartphone users
  Capabilities: Web browsing, application editing, file transfer
- **Third Facility:**
  Users: 5 Workstation users, 2 Mobile device users
  Capabilities: Web browsing, email communication

2.4. Requirement Analysis

In-depth consideration of the functional needs, performance requirements, and limitations is given to the design and simulation of a Metropolitan Area Network (MAN) that links two geographically separated branch offices in a metropolis.

2.4.1 Functional Requirements

Infrastructure Requirements

- **Routers**: Provide redundancy by installing at least two routers in each branch office. In the event that a single router experiences issues, this guarantees continuous network operation. Effective traffic routing to the internet and branch-to-branch communication should be made possible by router settings.

- **ISP Connection:** Create a dependable and secure link between the Internet Service Provider and the Man. Depending on your budget and bandwidth needs, take into consideration a variety of solutions such as fiber optic cables, broadband internet connections, or specialized leased lines.

Branch Infrastructure

Three separate locations with different user needs and functionalities will make up each branch office network.

First Branch - First Facility

- **Users**: Three workstations (PCs), three laptop wireless users, and three smartphone users are present in Facility 1.All of the users in this facility have the ability to browse the web, send emails and transfer files by using their devices.
- **Activities**: Email correspondence, file transfers, and web browsing (think about installing network printers for this facility's wireless and mobile customers).
- **Devices**: For wired communication, each workstation needs to have a network interface card (NIC). It is important to put wireless access points strategically across the building to guarantee that laptops and cellphones have enough Wi-Fi coverage.

First Branch - Second Facility

- **Users**: Six PC workstations.
- **Activities**: Internet browsing and file transfers (FTP).
- **Requirement**: Two Workstations for Conference Call VoIP Systems Depending on the solution selected, these workstations may need additional hardware or software for VoIP capabilities.

First Branch - Third Facility

- **Users**: A server farm of 10 Web servers, 4 FTP servers, 1 DHCP server, 1 mail server, and 1 domain name server (DNS) is present in the third facility.

Second Branch - First Facility

- **Users**: Five workstations, five laptops using wireless technology, and five tablet users
- **Activities**: Email communication and web browsing (using wireless to access the Internet)
- **Devices**: To ensure smooth Wi-Fi connectivity for laptops and tablets, outfit workstations with network interface cards (NICs) and locate wireless access points in strategic locations, much like Facility 1 in the first branch. Use network security protocols such as WPA2 encryption while using wireless networks.

Second Branch - Second Facility

- **Users**: Two smartphones and five workstations
- **Activities**: Web browsing, editing software, and file transfer devices are among the activities. The right software for editing apps should be installed on workstations.

Second Branch - Third Facility

- **Users:** Two mobile devices and five workstations
- **Activities**: Email correspondence and web browsing
- **Devices**: It could be necessary to configure mobile devices further in order to access the business email server.

Services

- **Internet access**: To provide a seamless user experience, prioritize email and web browsing traffic.

- **Email Communication**: Plan the network to effectively manage email traffic, both from within and outside the company.
- **File Transfer (FTP)**: Depending on the security needs for file sharing within the network, select either FTP or SFTP as the secure file transfer protocol.
- **VoIP Conference Calls**: Give the two workstations set aside for VoIP conference calls priority when allocating bandwidth. Examine VoIP software and hardware options based on your budget and the technology you've selected.

2.4.2 Non-functional Requirements

Performance

- **User Capacity**: 50 concurrent users total across both branches should be supported by the network design. This covers those who use smartphones, wireless devices, and desktops. When calculating the necessary network bandwidth, take future growth and peak demand periods into account.
- **Bandwidth**: Enough bandwidth to ensure that even during periods of high usage, performance remains acceptable.
- **Latency**: Reduce network latency to guarantee responsive email correspondence, conference calls via VoIP, and online surfing (where applicable).
- **Scalability**: A modular network architecture that is easily expandable to handle future increases in the number of users and network traffic by adding more network devices and bandwidth.

2.5. Definitions of the System/Model

2.5.1 Used Network Topologies

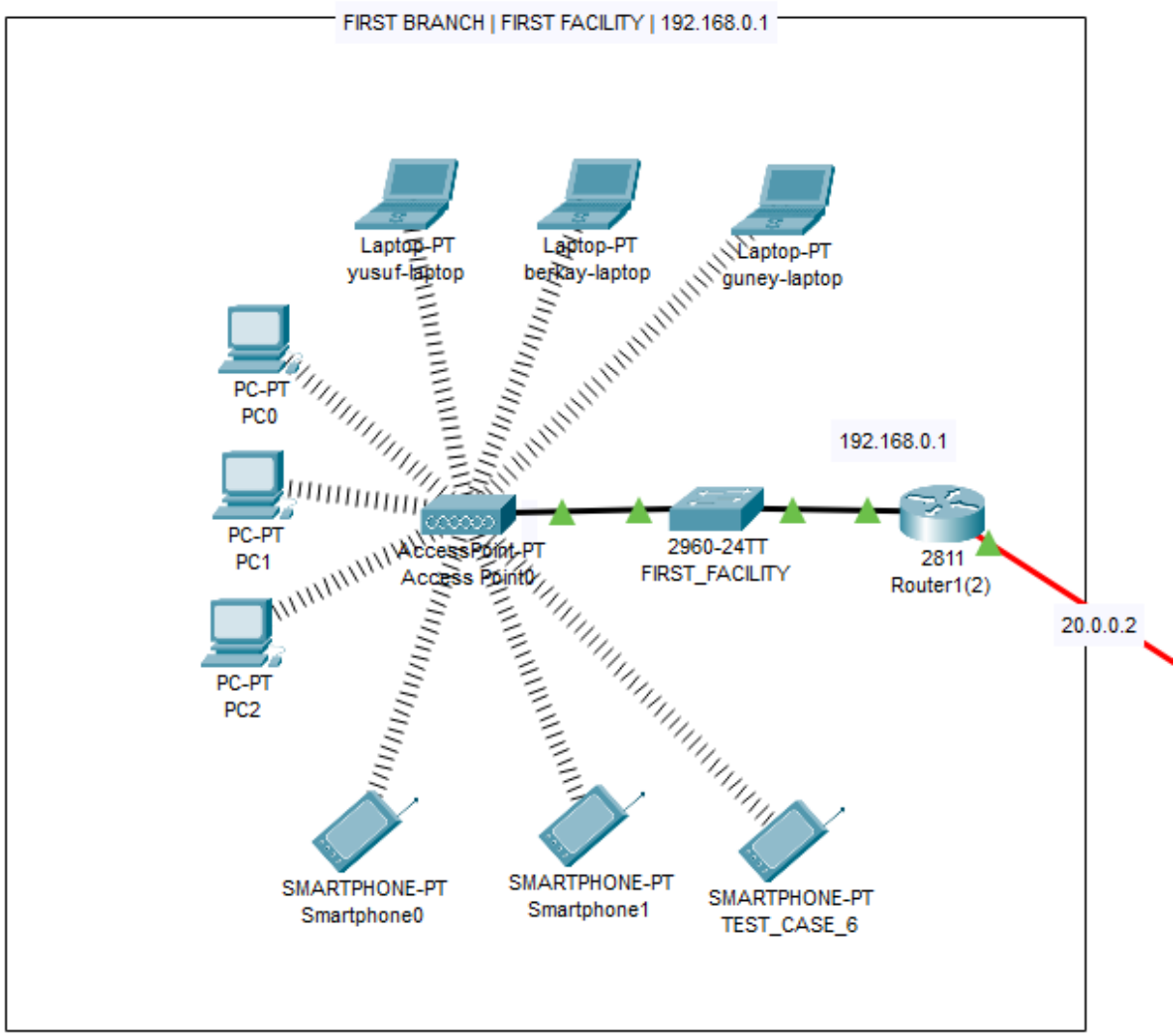

Figure 2.5.1: Star topology (1.1. office)

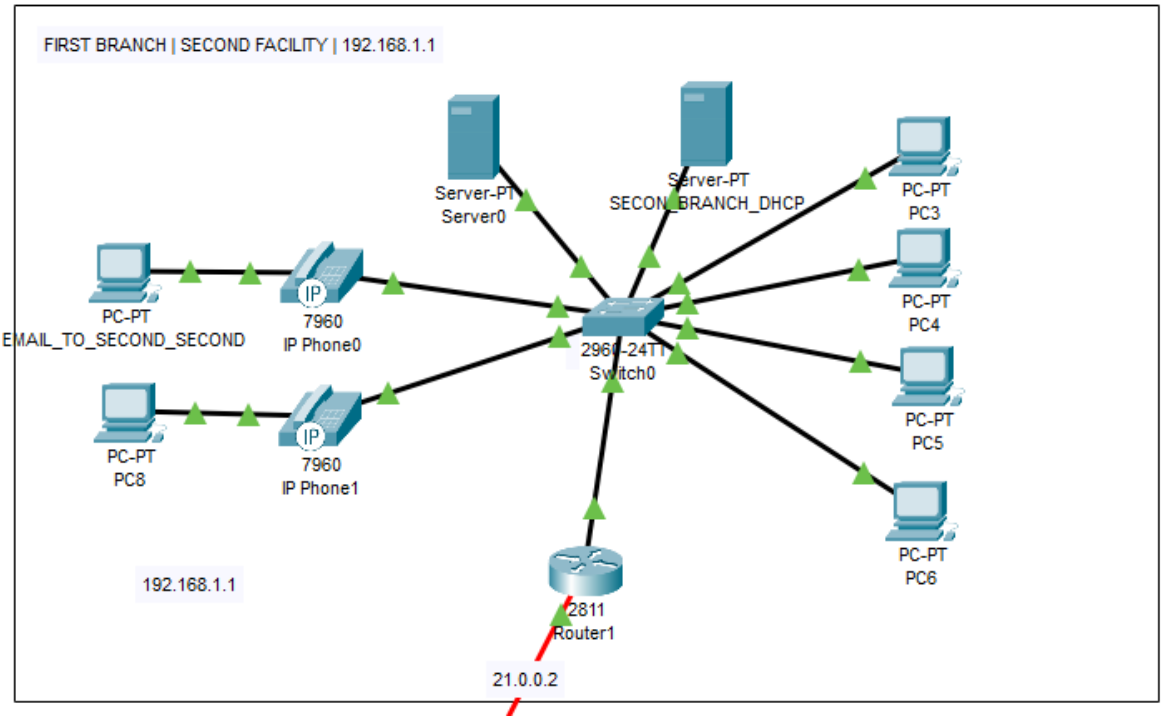

Figure 2.5.2: Star topology (1.2. office)

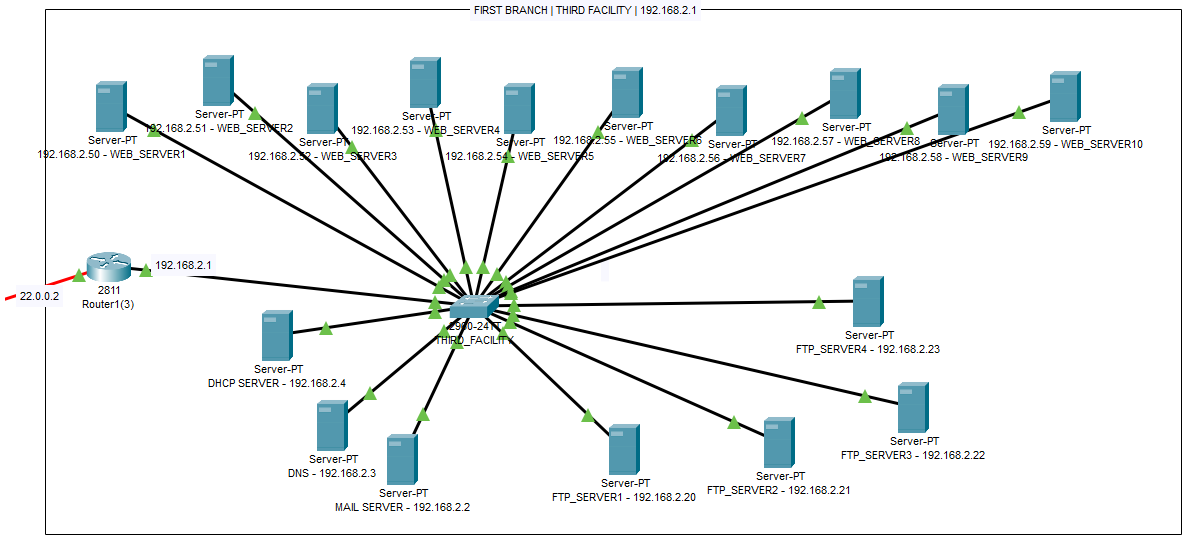

Figure 2.5.3: Star topology (1.3. office)

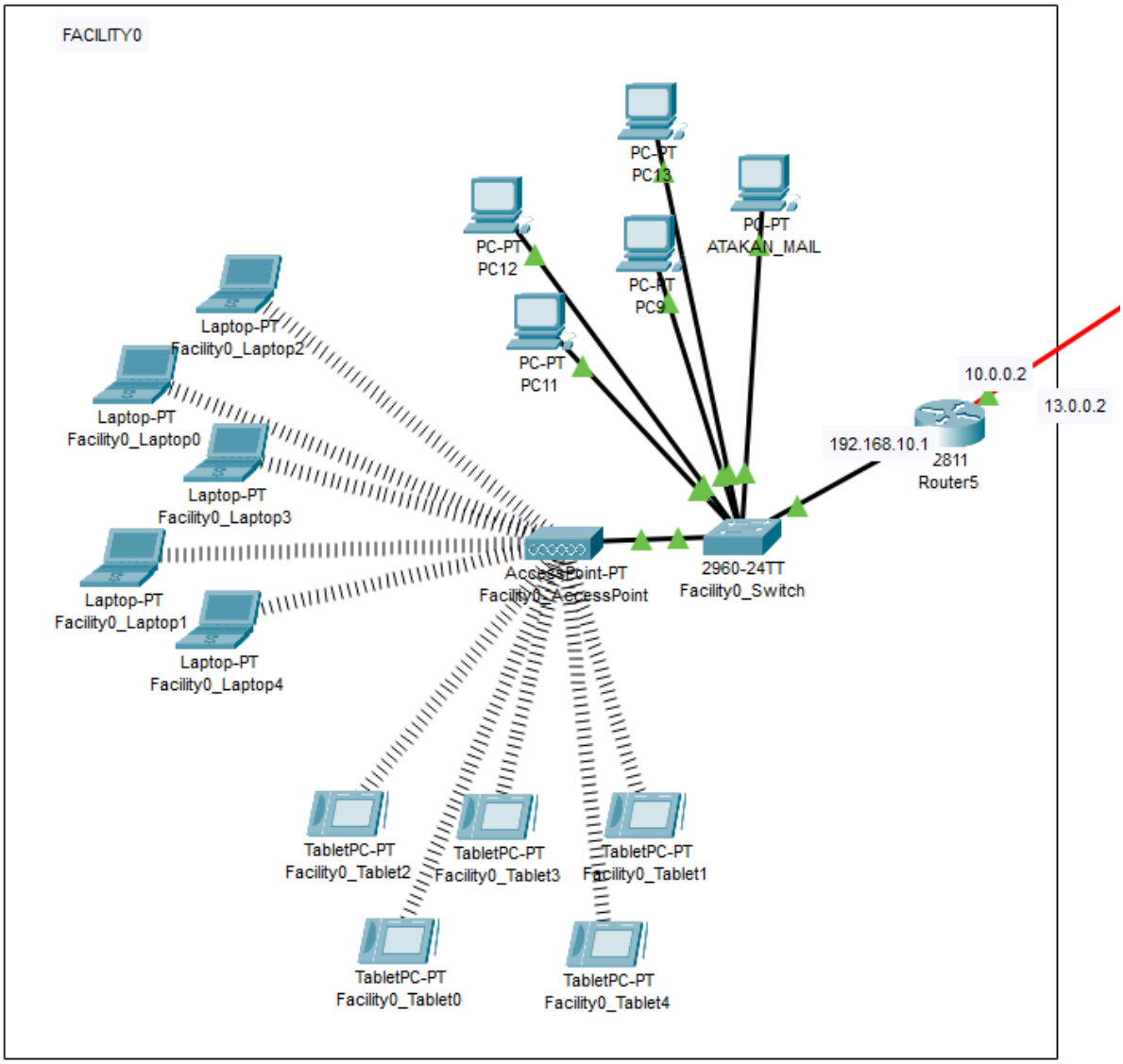

Figure 2.5.4: Hybrid topology (bus topologie + star topologie | 2.1. office)

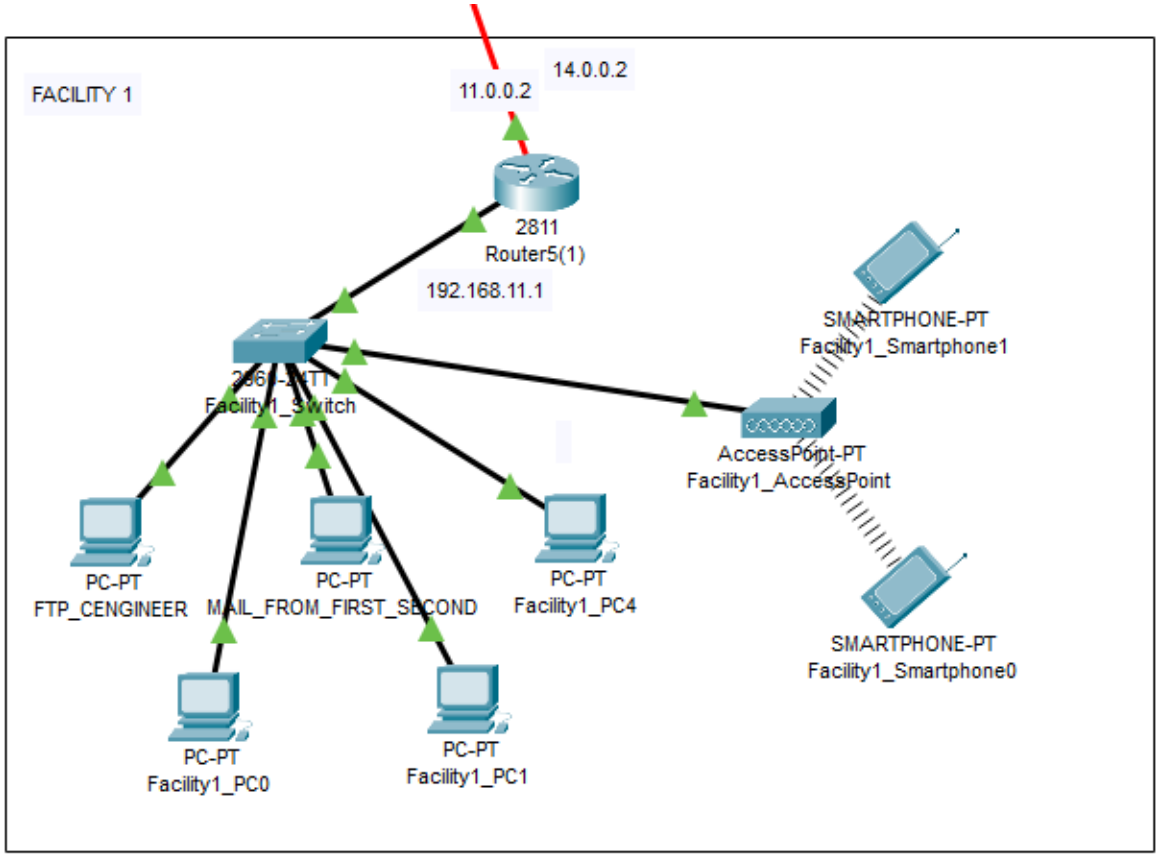

Figure 2.5.5: Hybrid topology (bus topologie + star topologie | 2.2. office)

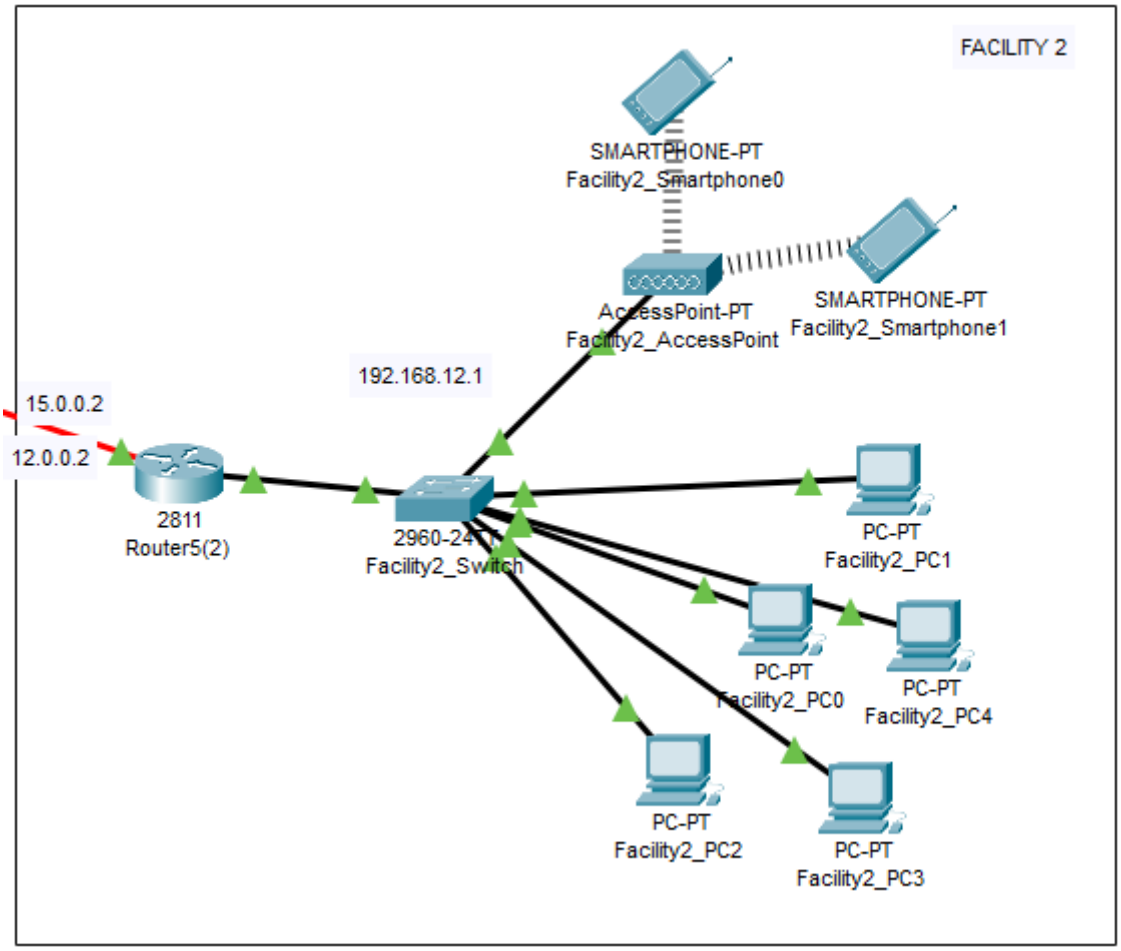

Figure 2.5.6: Hybrid topology (bus topology + star topologie | 2.3. office)

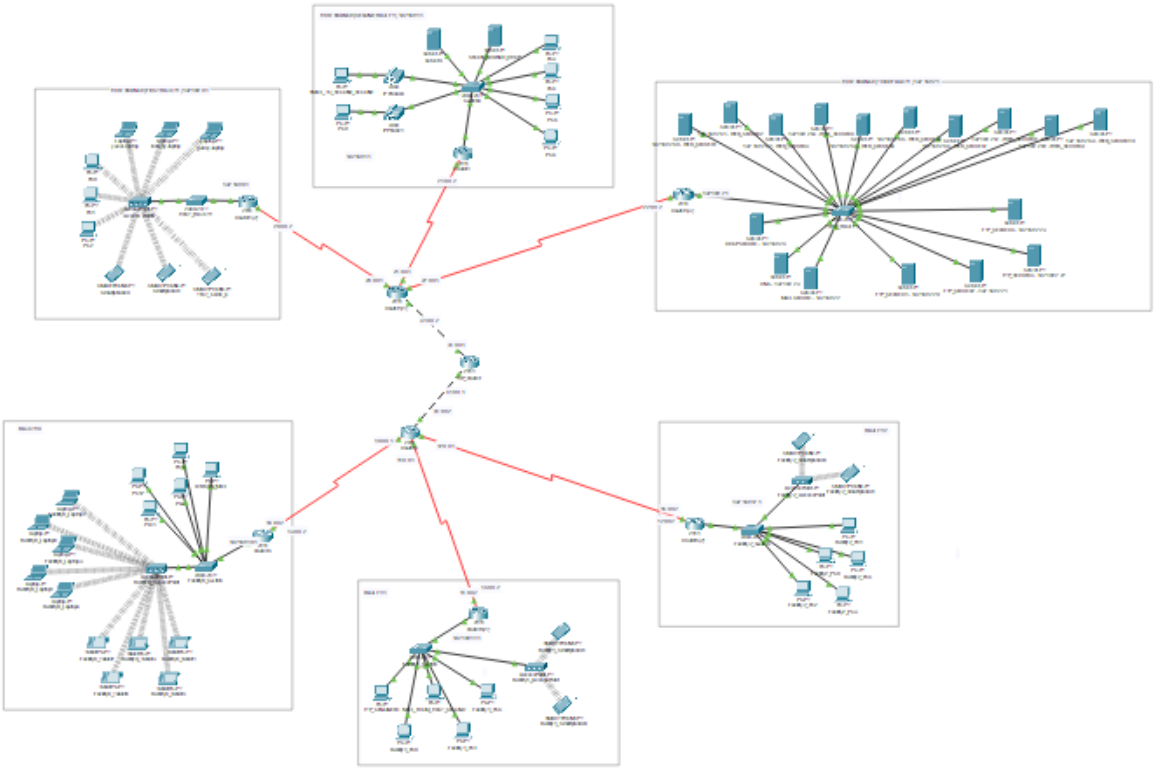

Figure 2.5.7: Tree topology (Used Model)

2.5.1 Alternative Network Model

In the alternative models, each branch connects to two routers for redundancy. Traffic control could not be achieved in this model. For this reason, this model did not work properly. This model needs some further development.

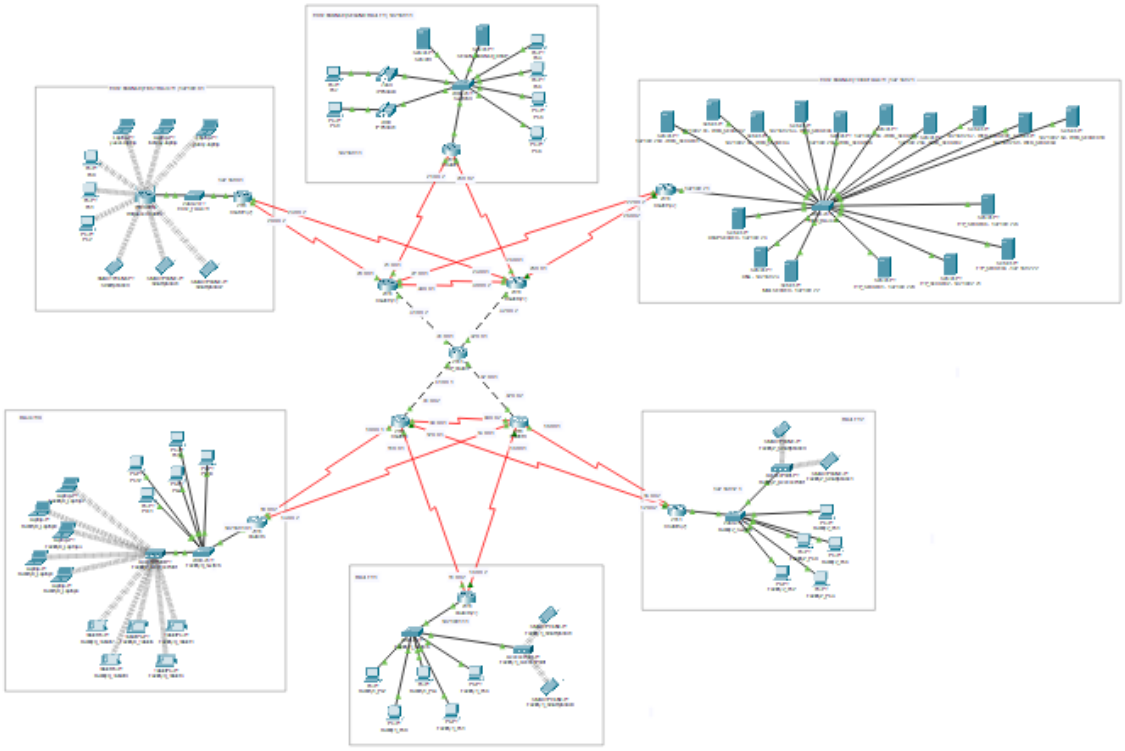

Figure 2.5.8: Alternative Model

2.6. Simulation Elements

Figure 2.6.1: Laptop Physical Configuration Sample

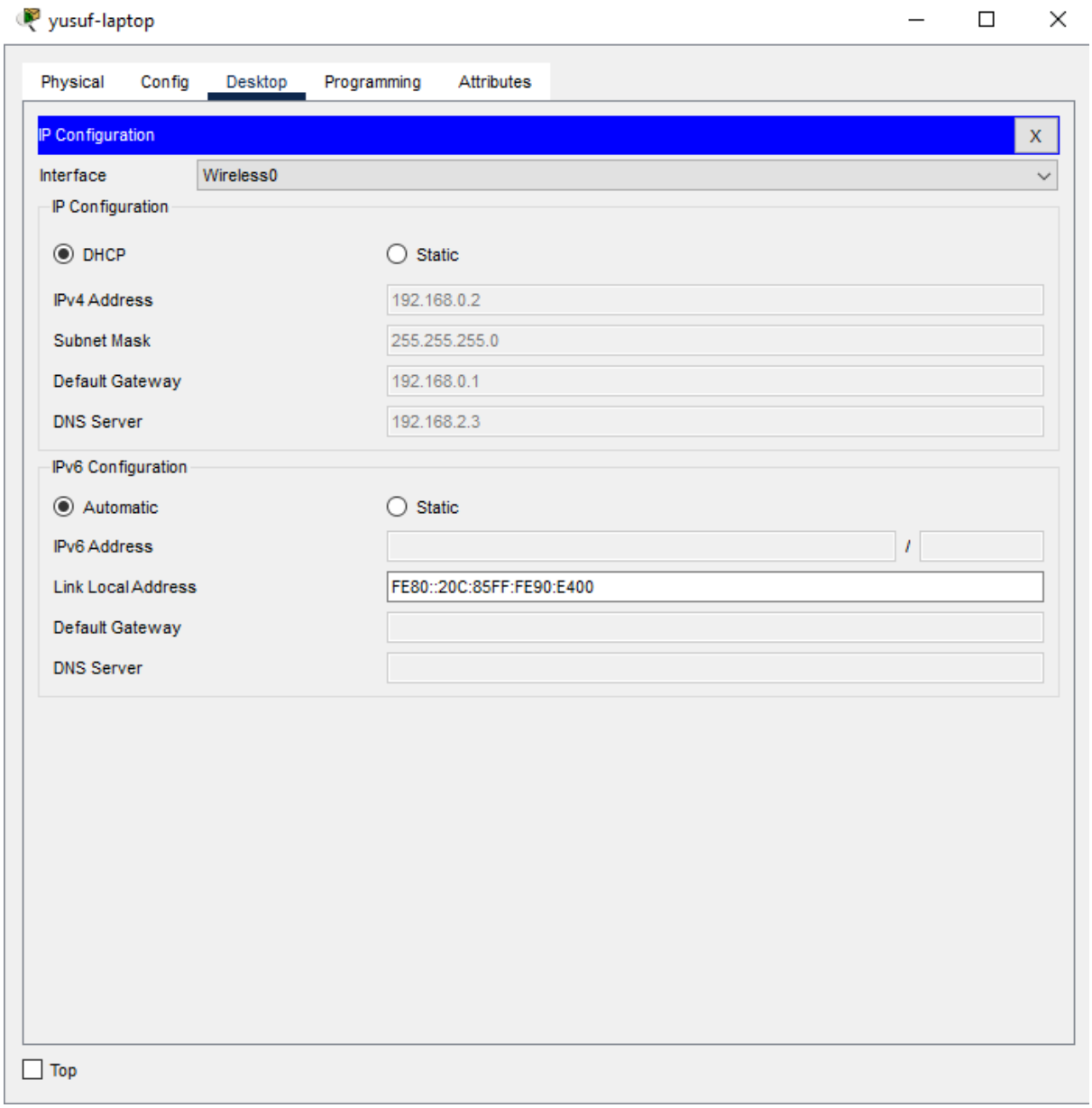

Figure 2.6.2: Laptop IP Configuration Sample

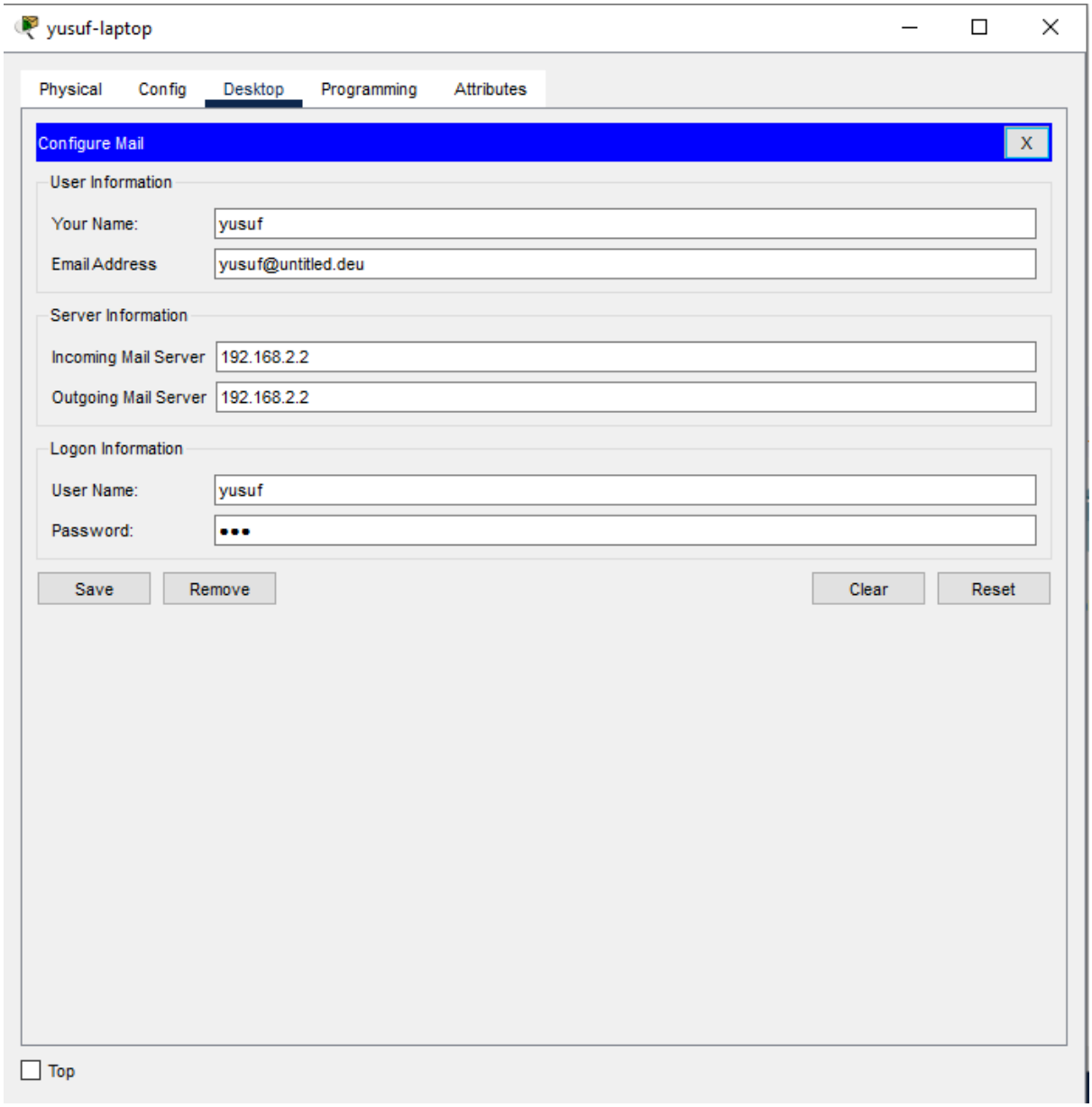

Figure 2.6.3: Mail Configuration Sample

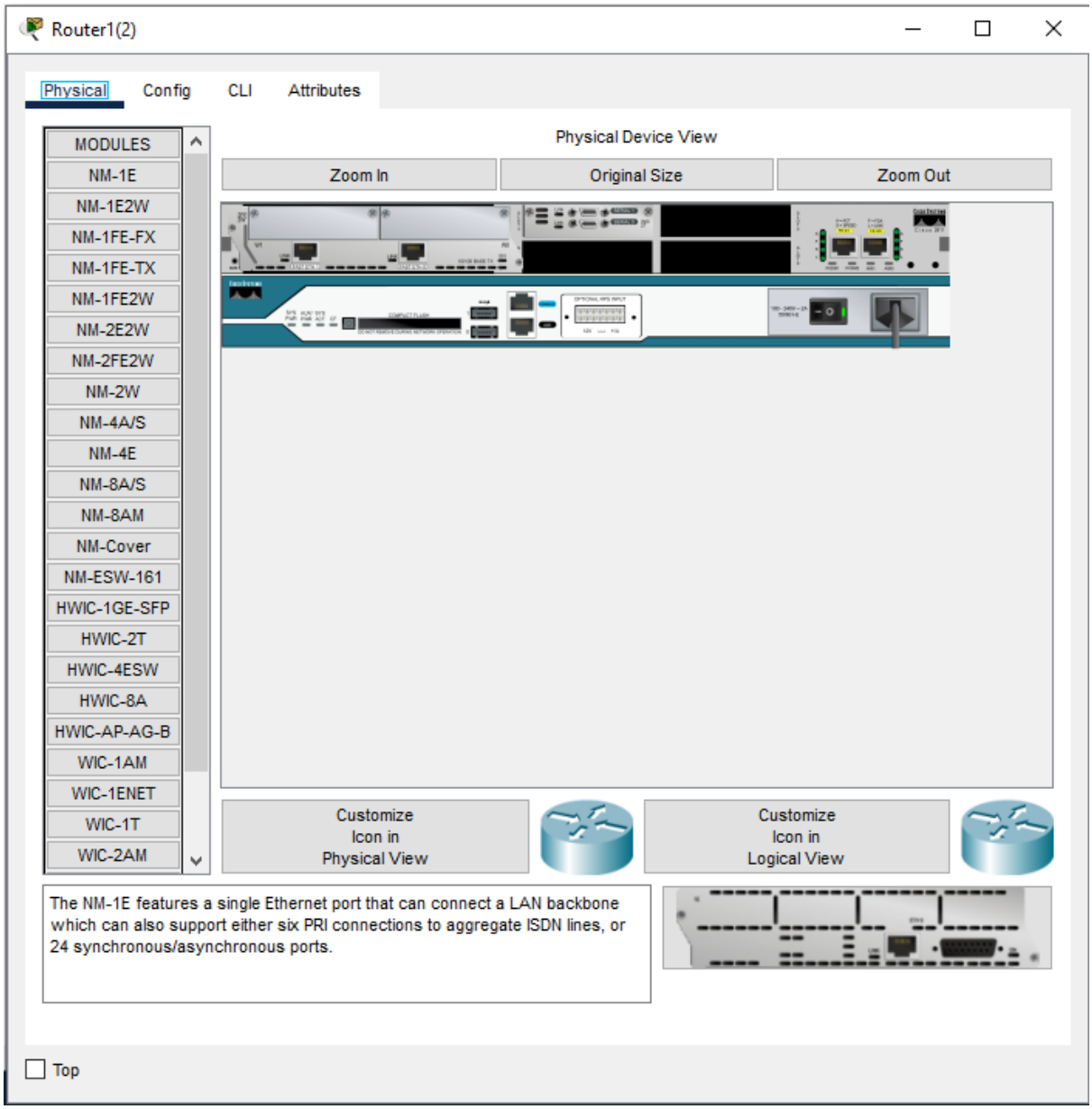

Figure 2.6.4: Router Physical Configuration Sample

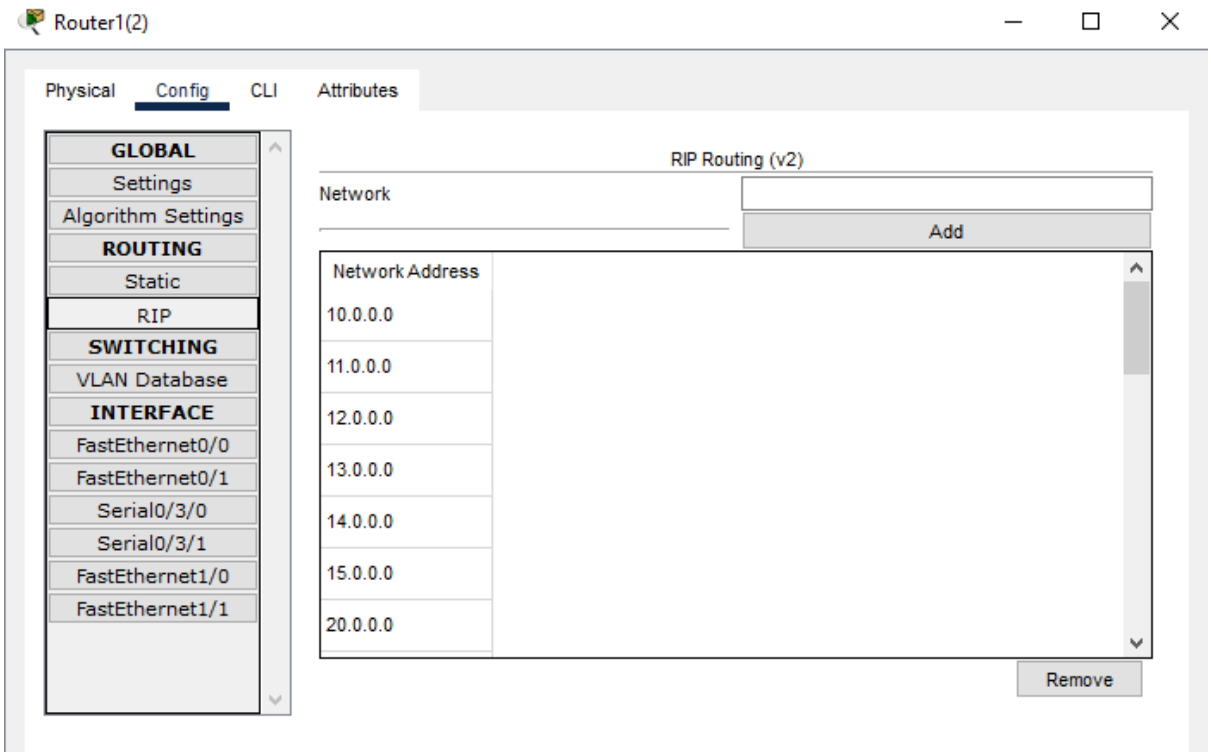

Figure 2.6.5: Router RIP Configuration Sample

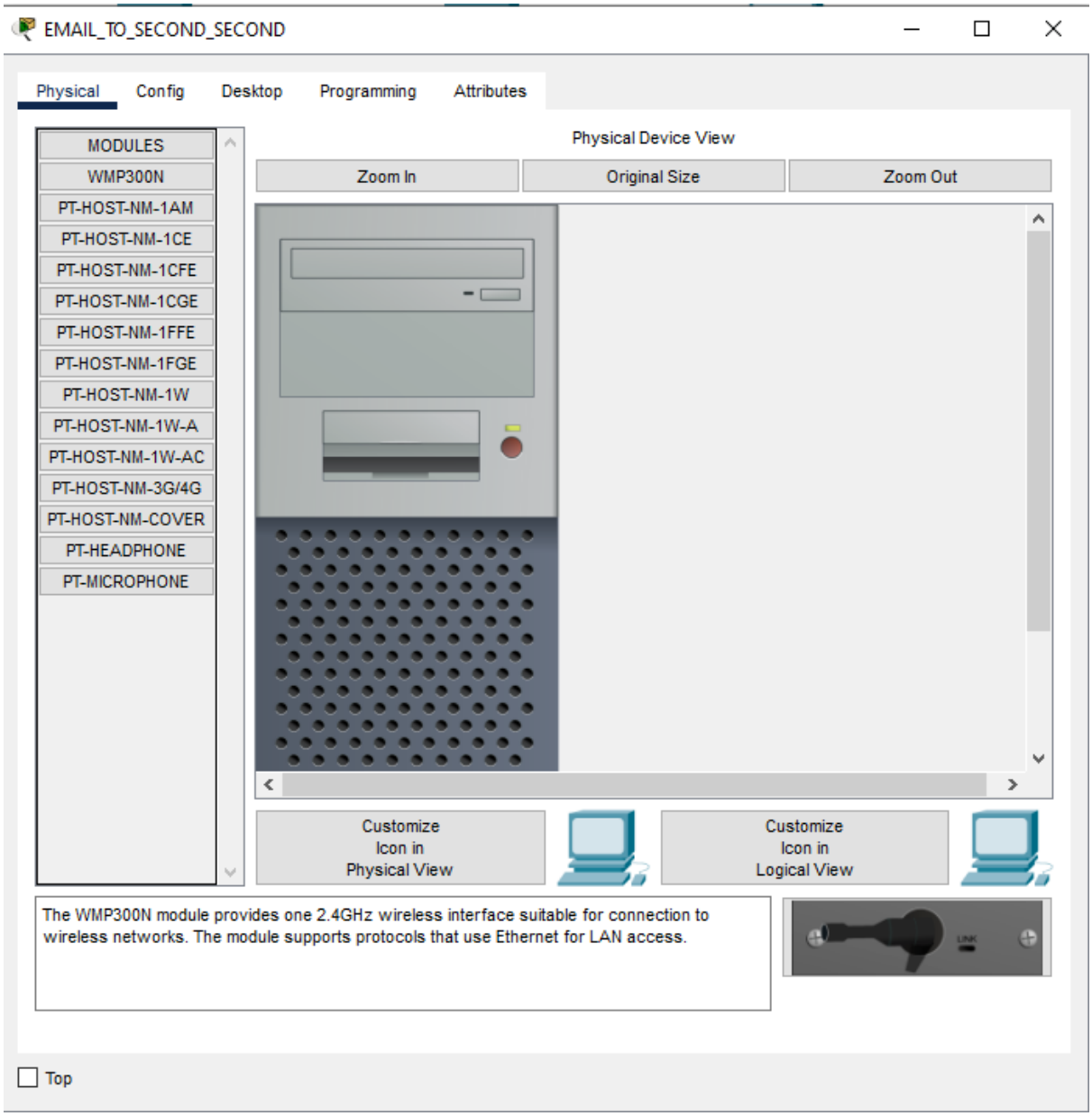

Figure 2.6.6: PC Physical Configuration Sample

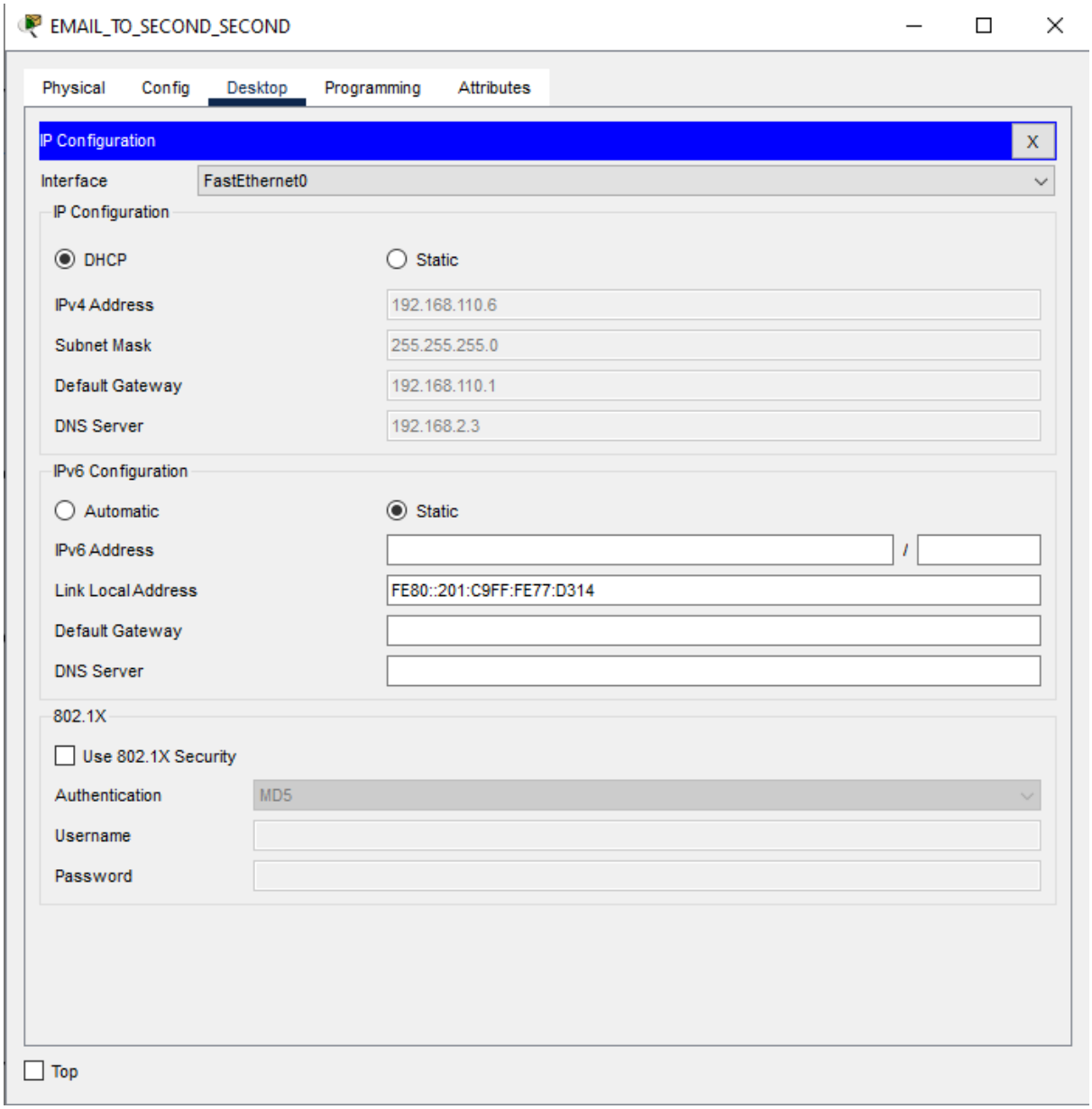

Figure 2.6.7: PC with IP Phone IP Configuration Sample

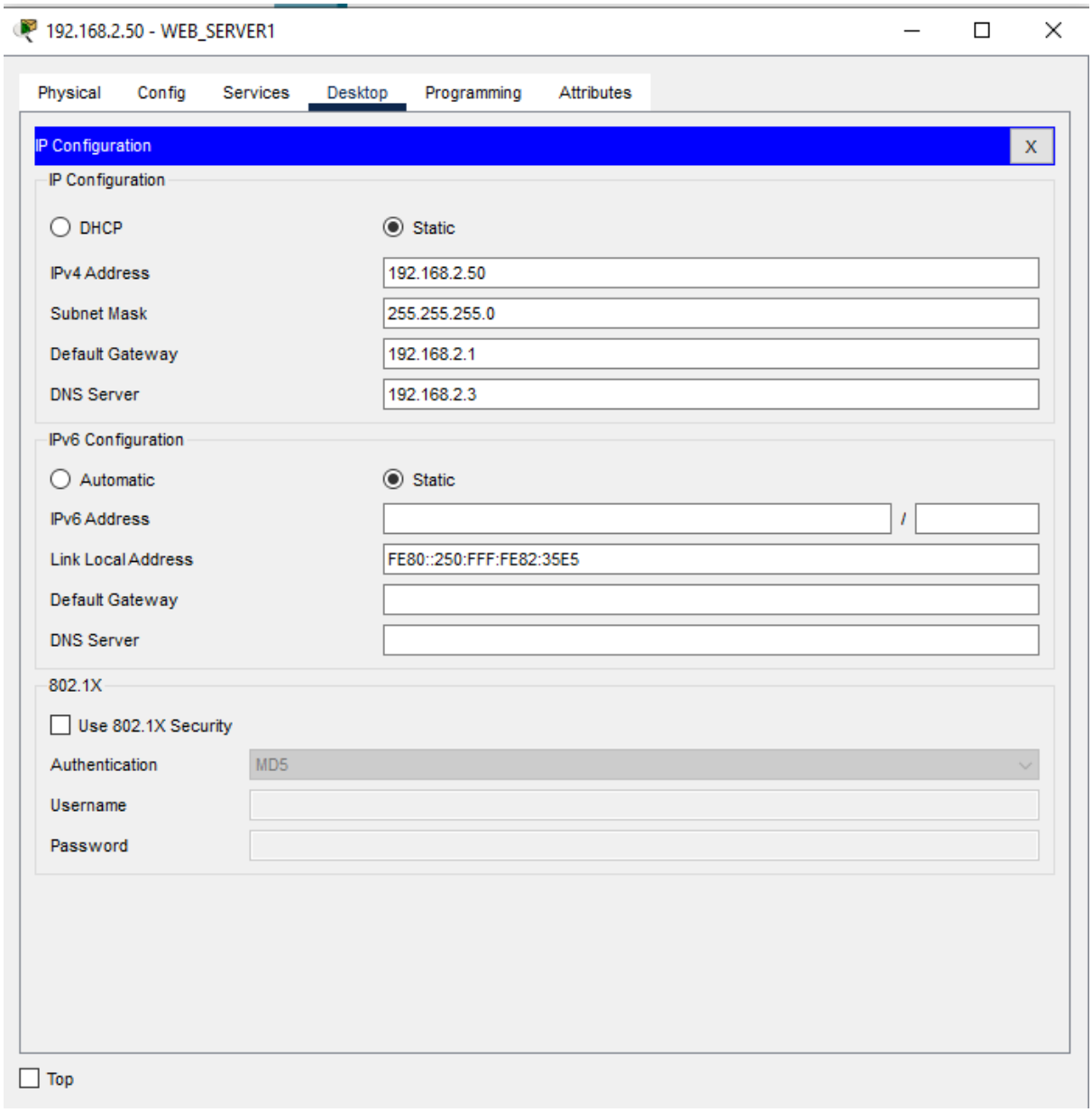

Figure 2.6.8: Web Server IP Configuration Sample

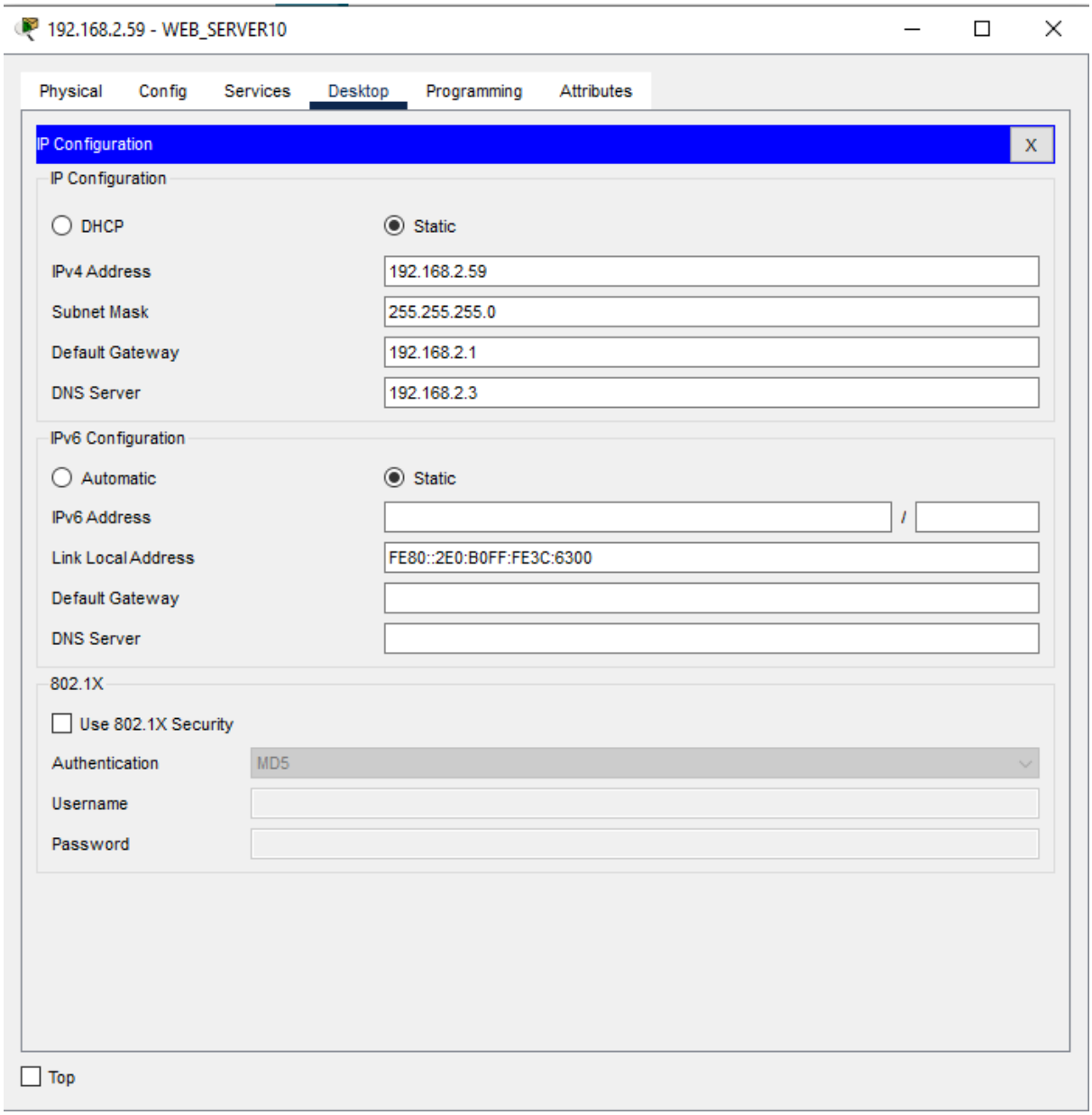

Figure 2.6.9: Web Server IP Configuration Sample

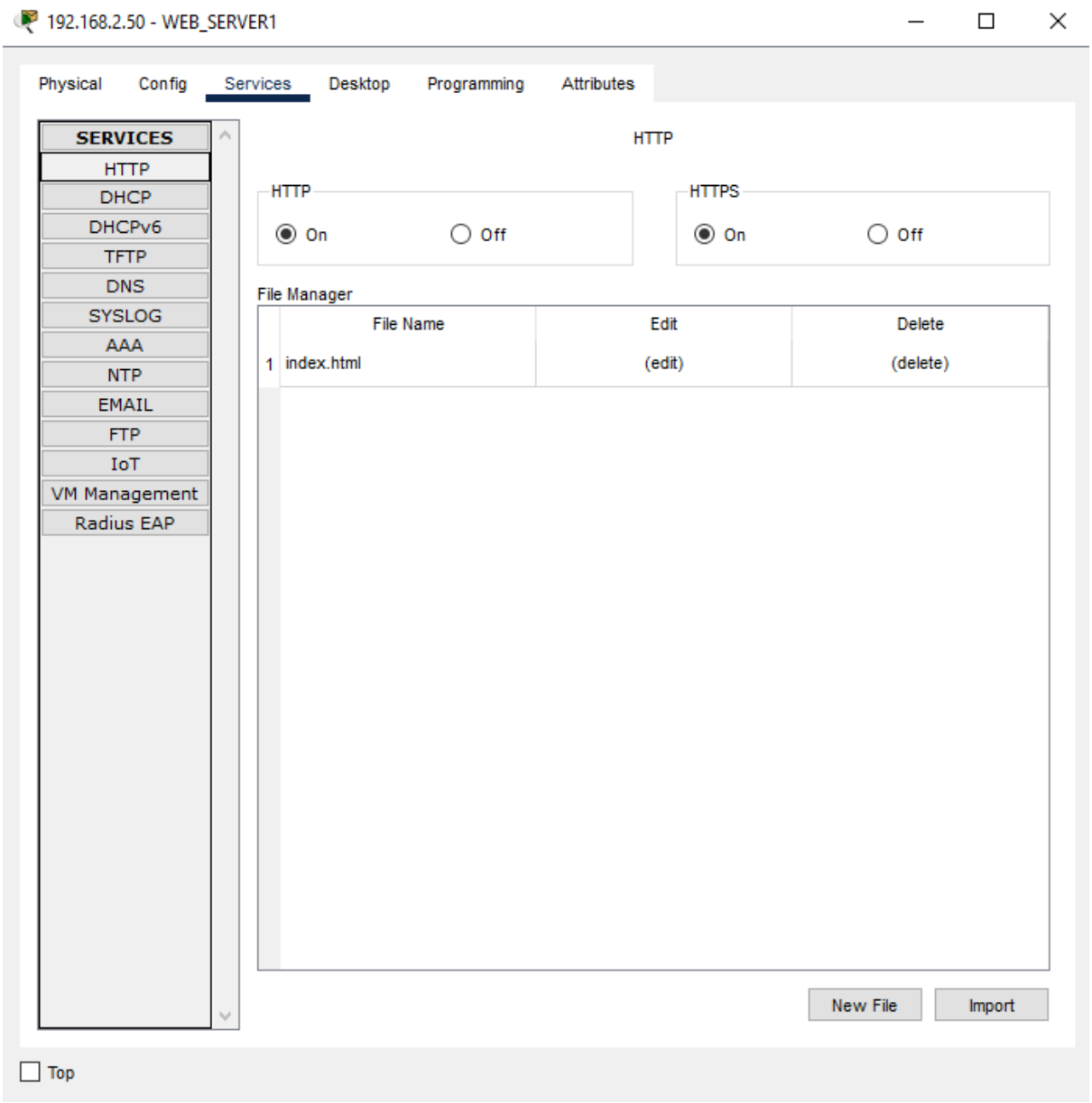

Figure 2.6.10: Web Server HTTP Service Configuration Sample

Figure 2.6.11: Web Site Sample

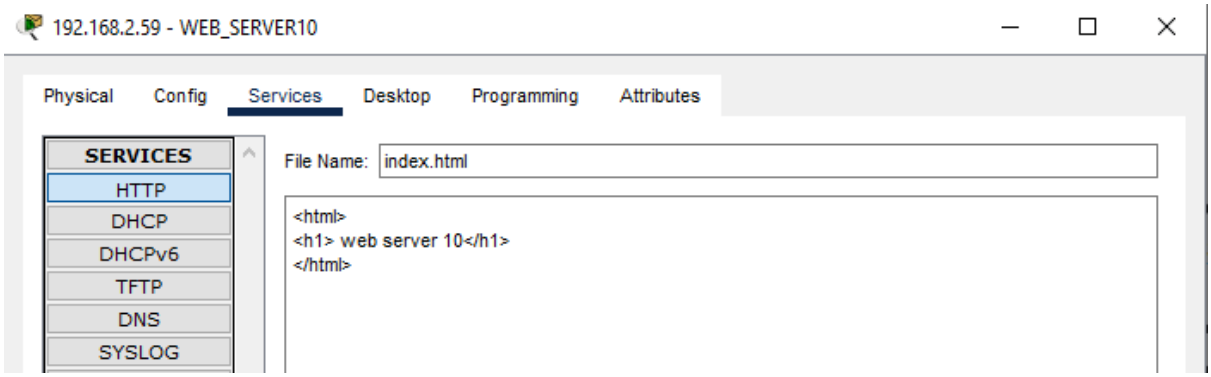

Figure 2.6.12: Web Site Sample

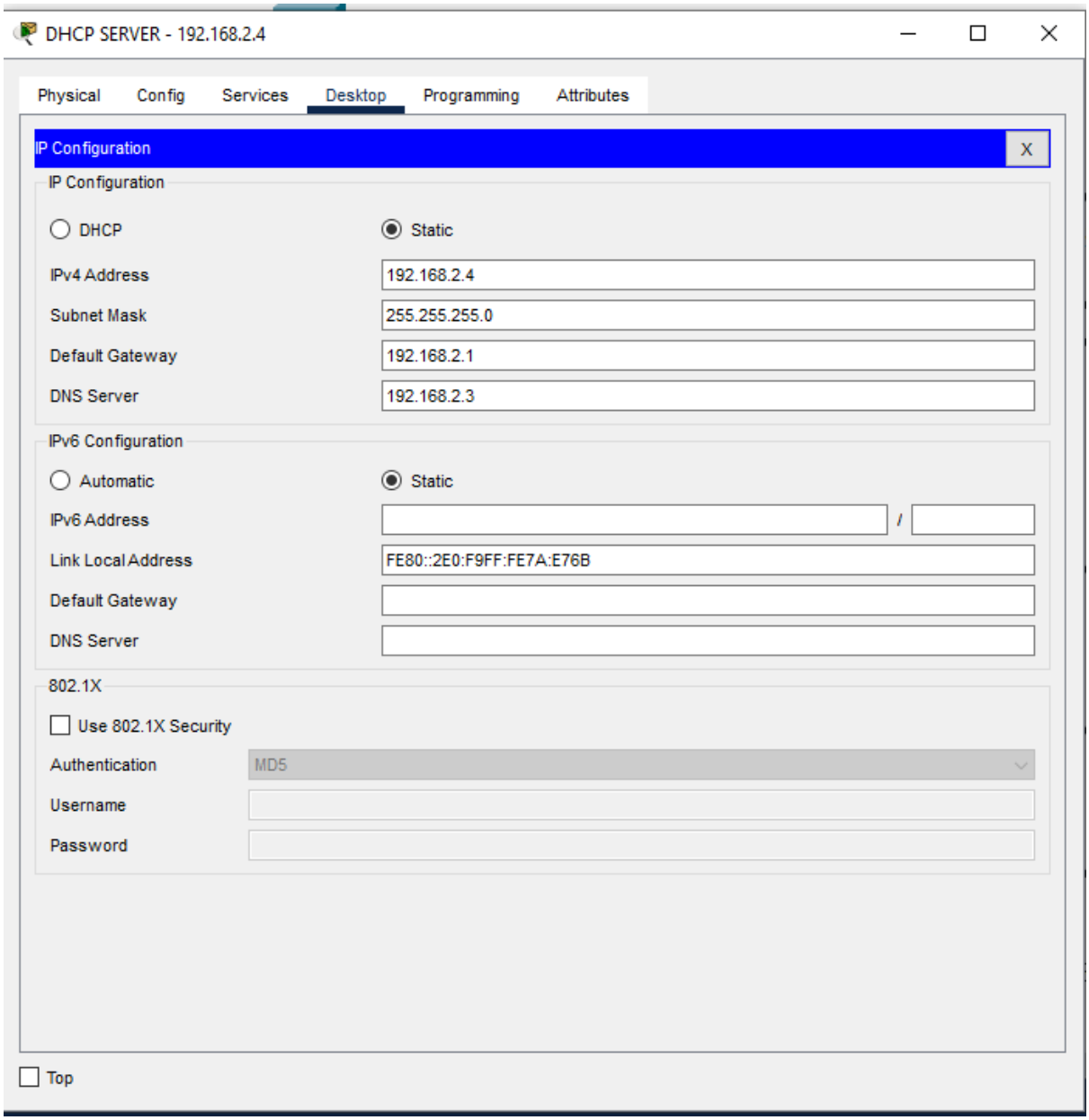

Figure 2.6.13: DHCP Server IP Configuration Sample

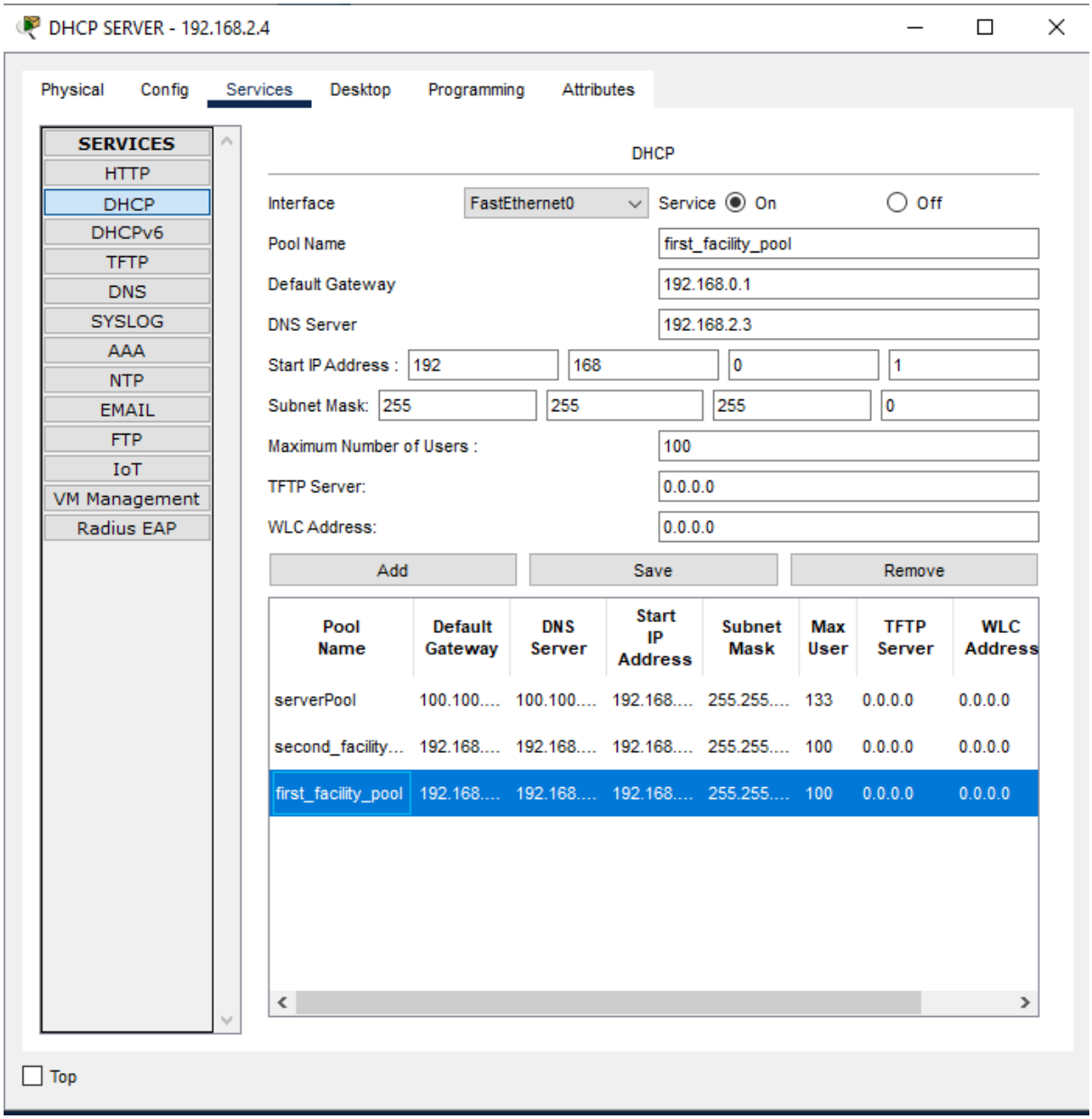

Figure 2.6.14: DHCP Server DHCP Service Pool Configurations

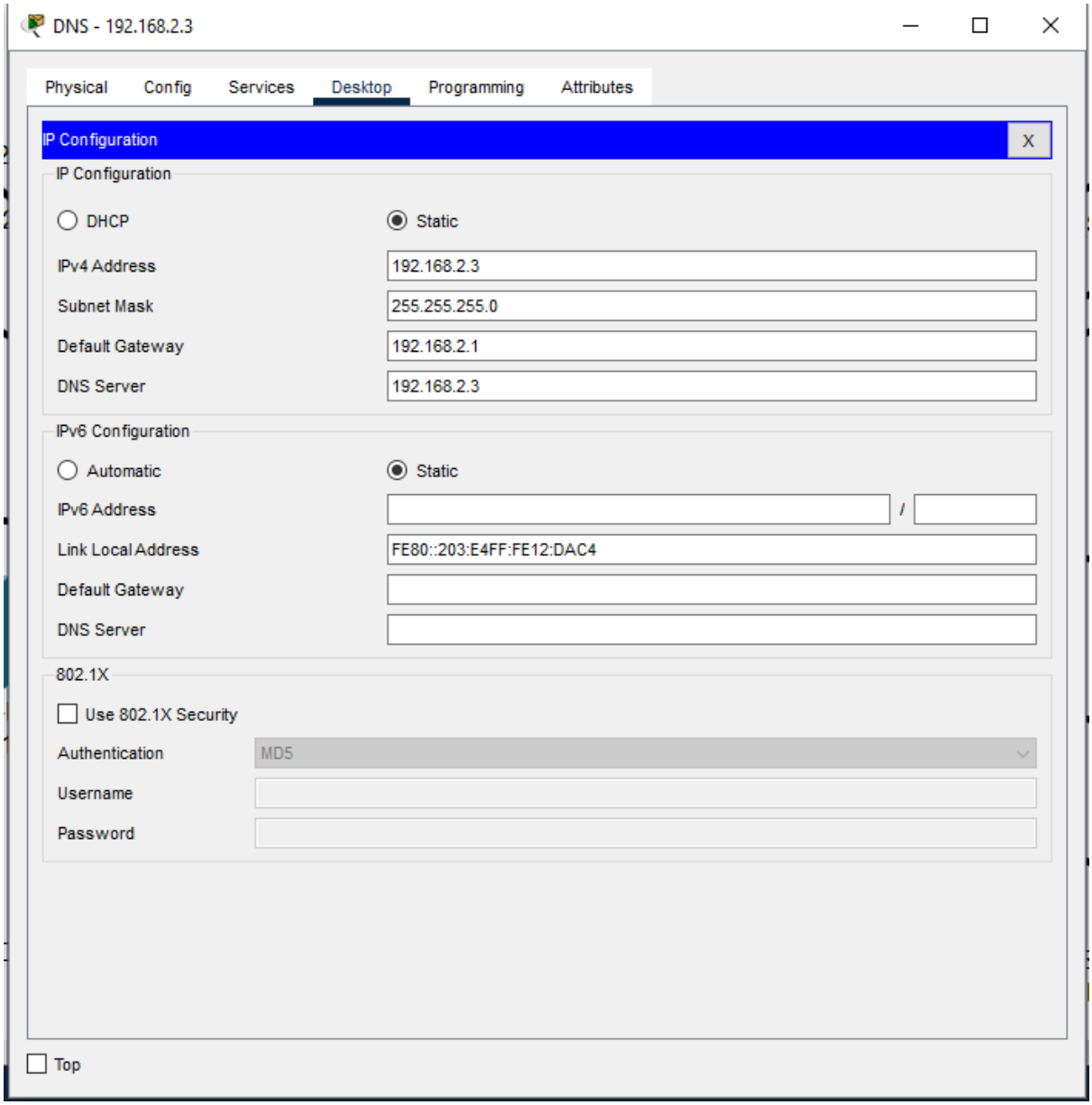

Figure 2.6.15: DNS Server IP Configuration

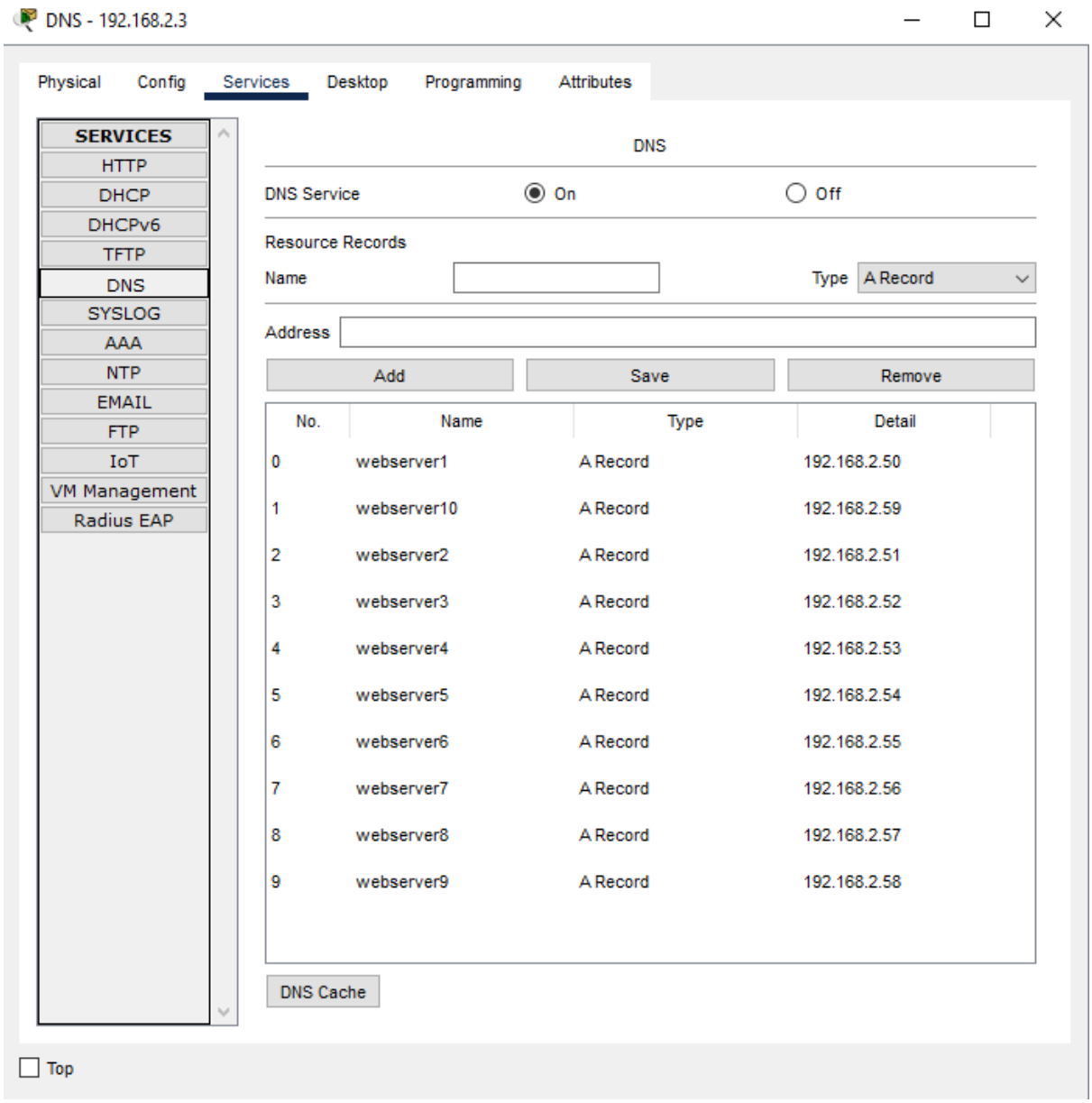

Figure 2.6.16: DNS Server DNS Service Configuration

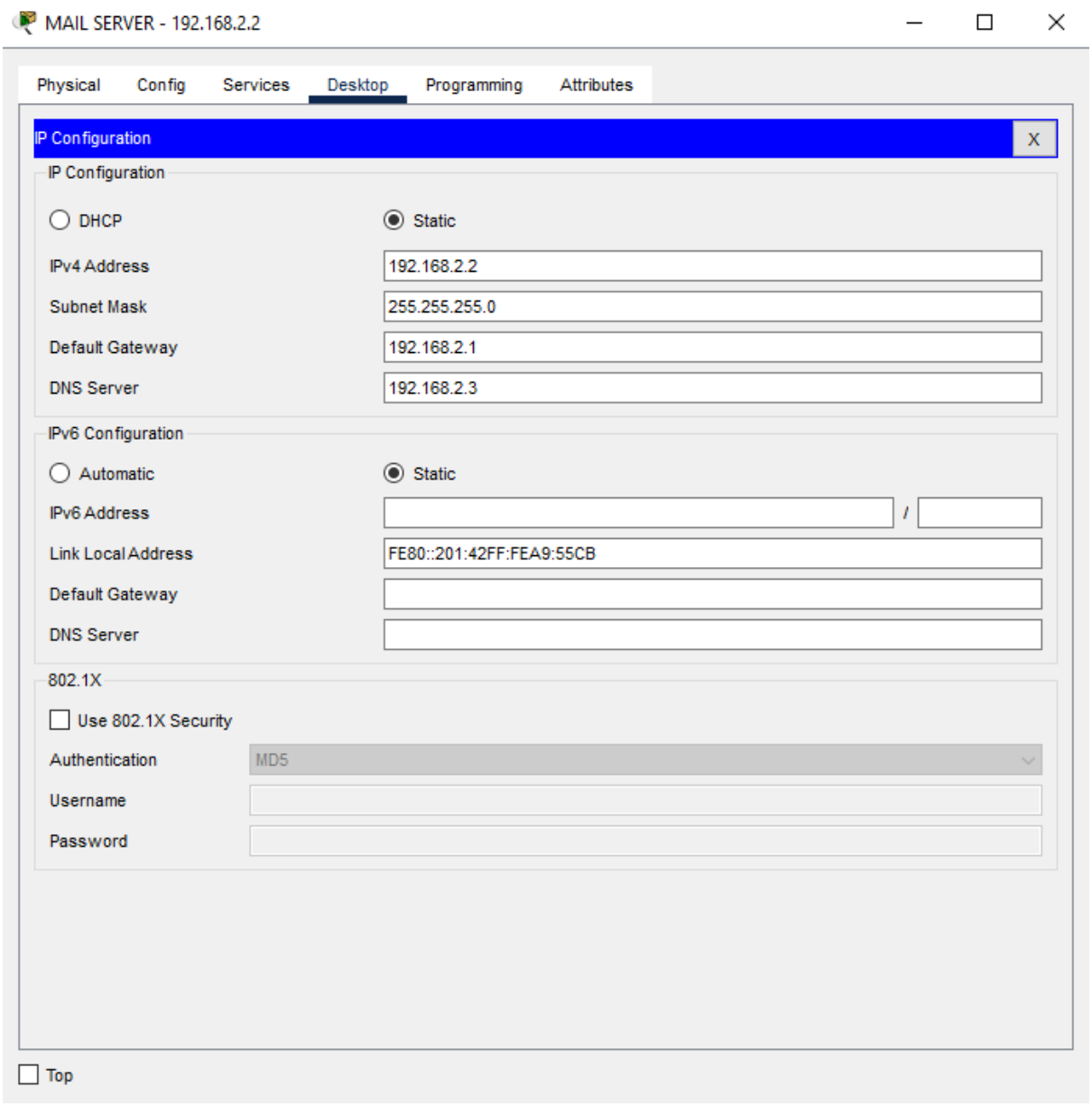

Figure 2.6.17: Mail Server Mail Service Configuration

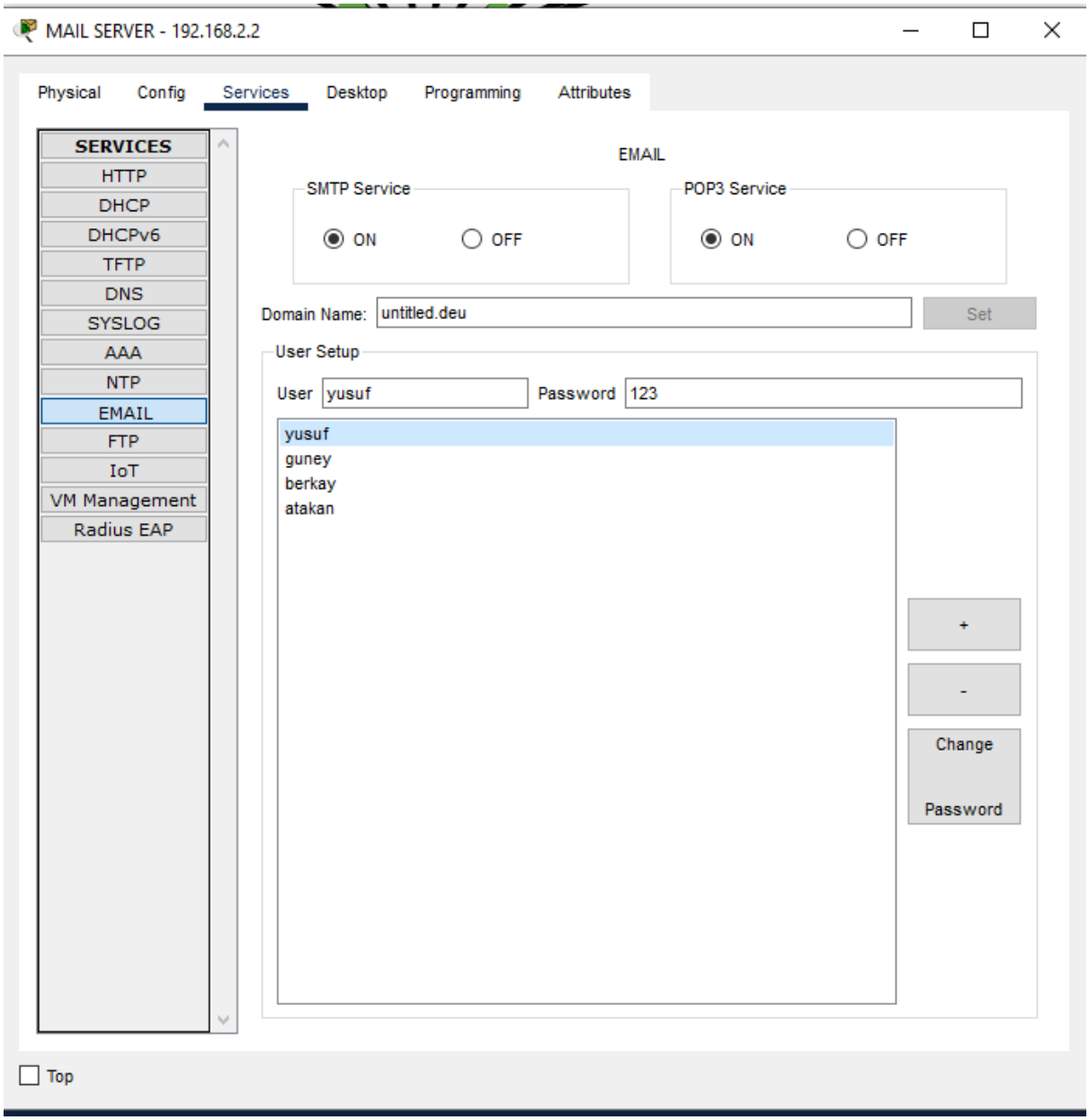

Figure 2.6.18: Mail Server Configuration

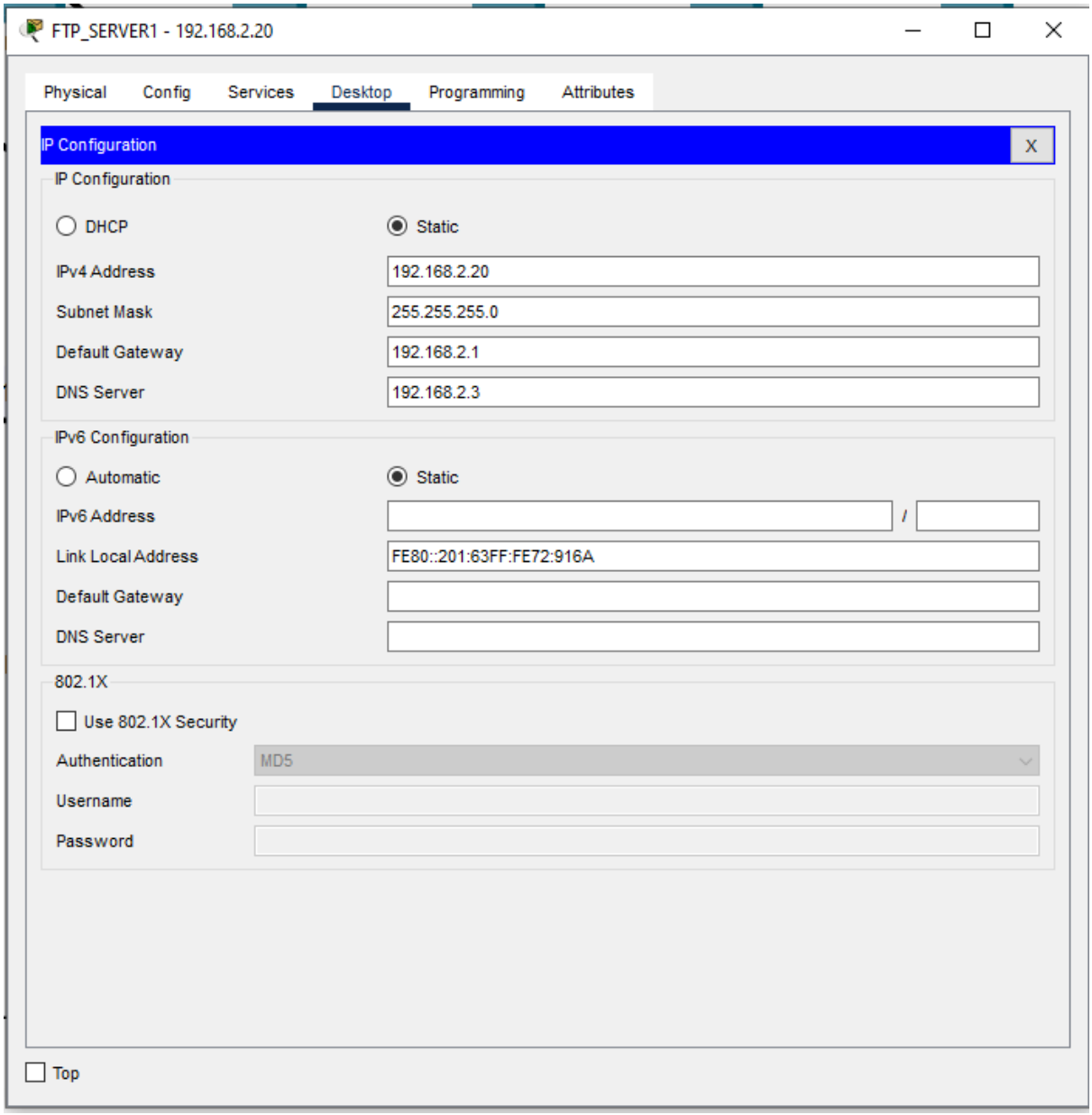

Figure 2.6.19: FTP Server IP Configuration

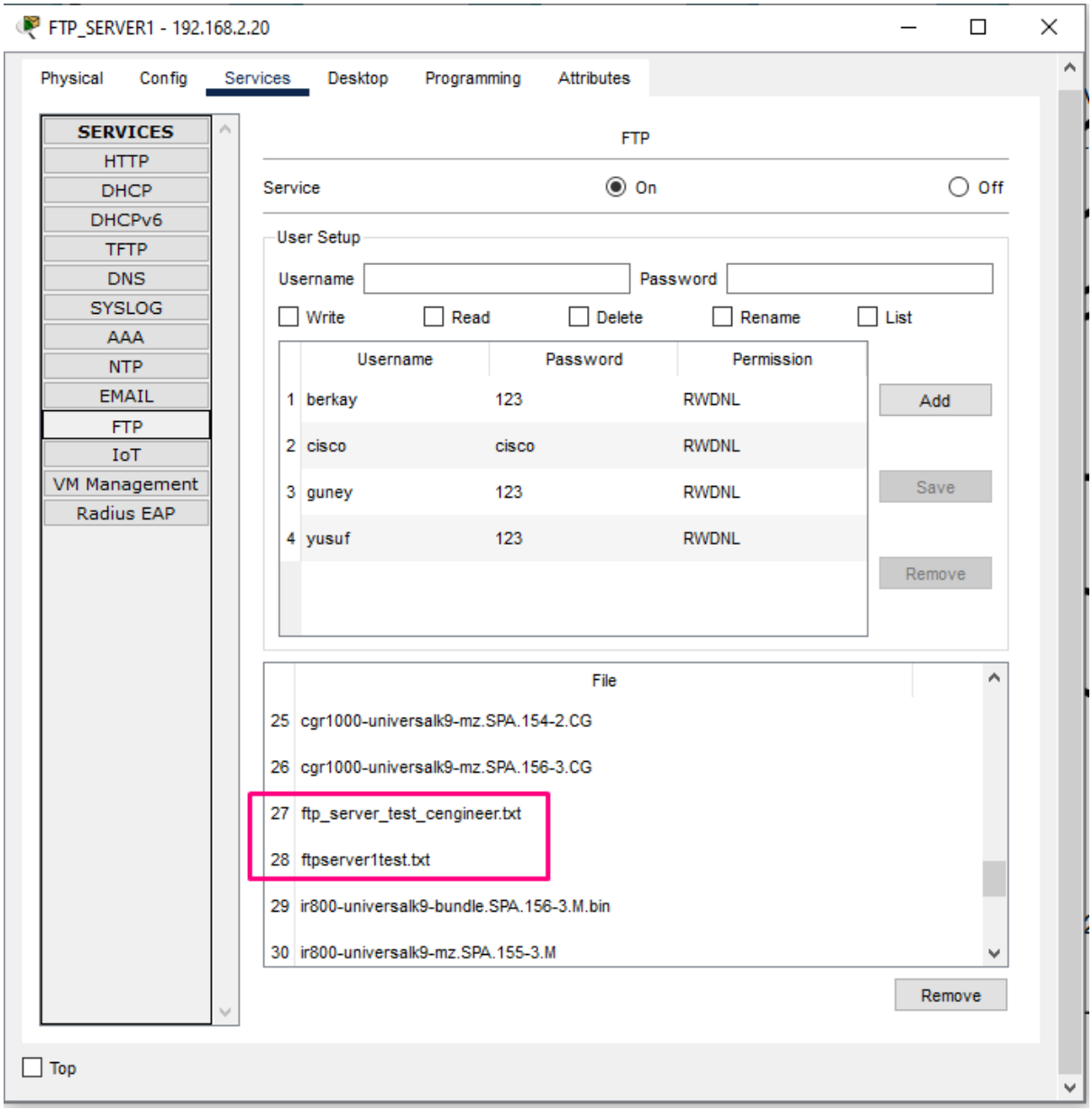

Figure 2.6.20: FTP Server FTP Service Users and Files Sample

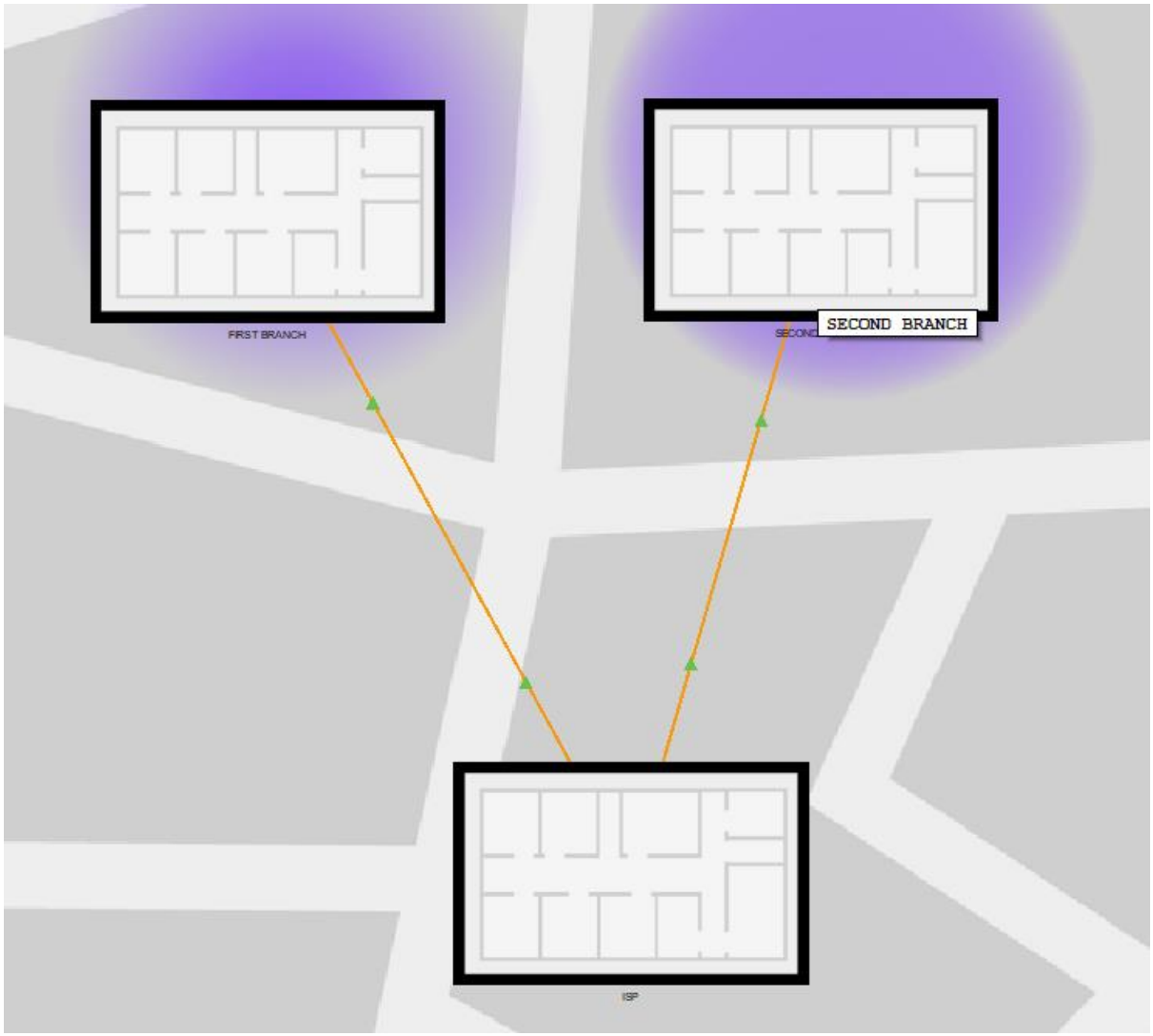

Figure 2.6.21: MAN Physical View

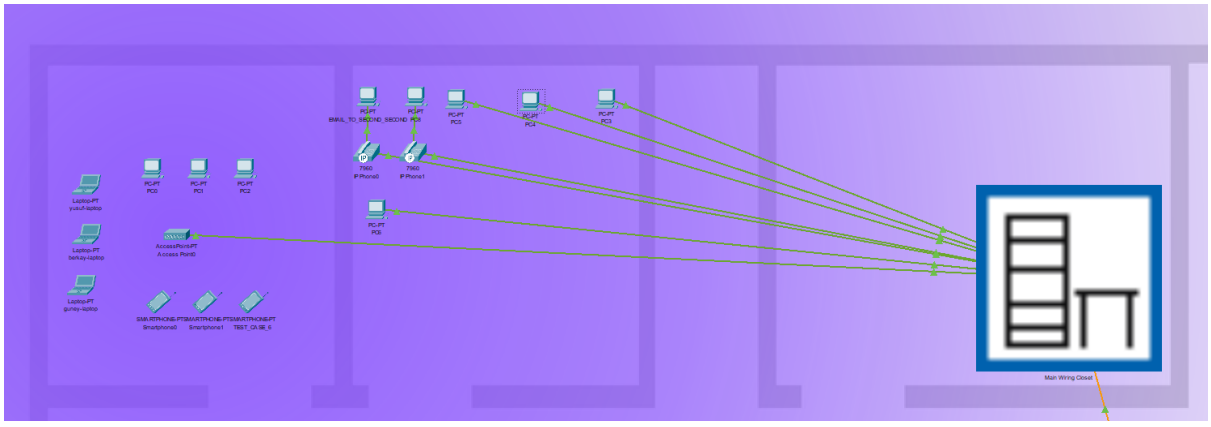

Figure 2.6.22: First Branch Physical View

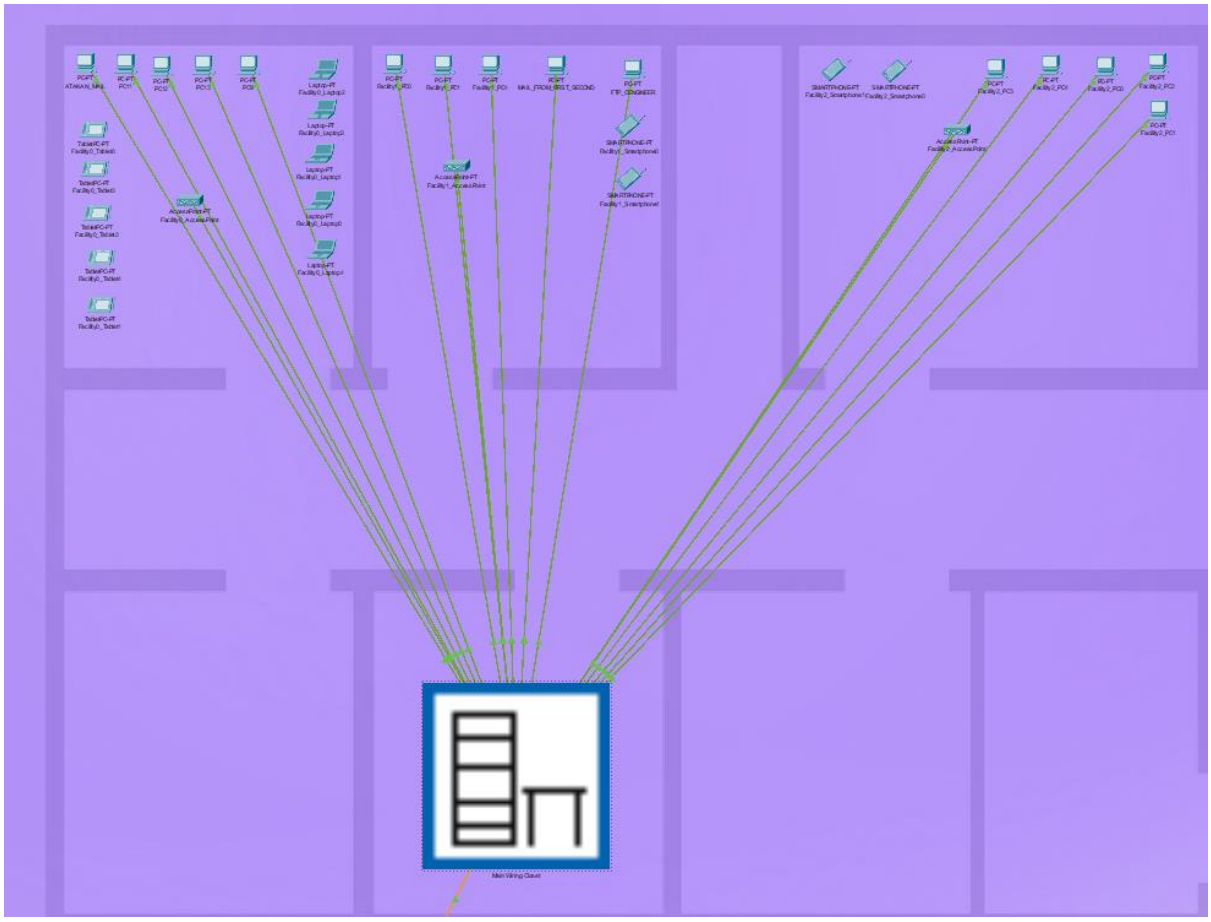

Figure 2.6.23: Second Branch Physical View

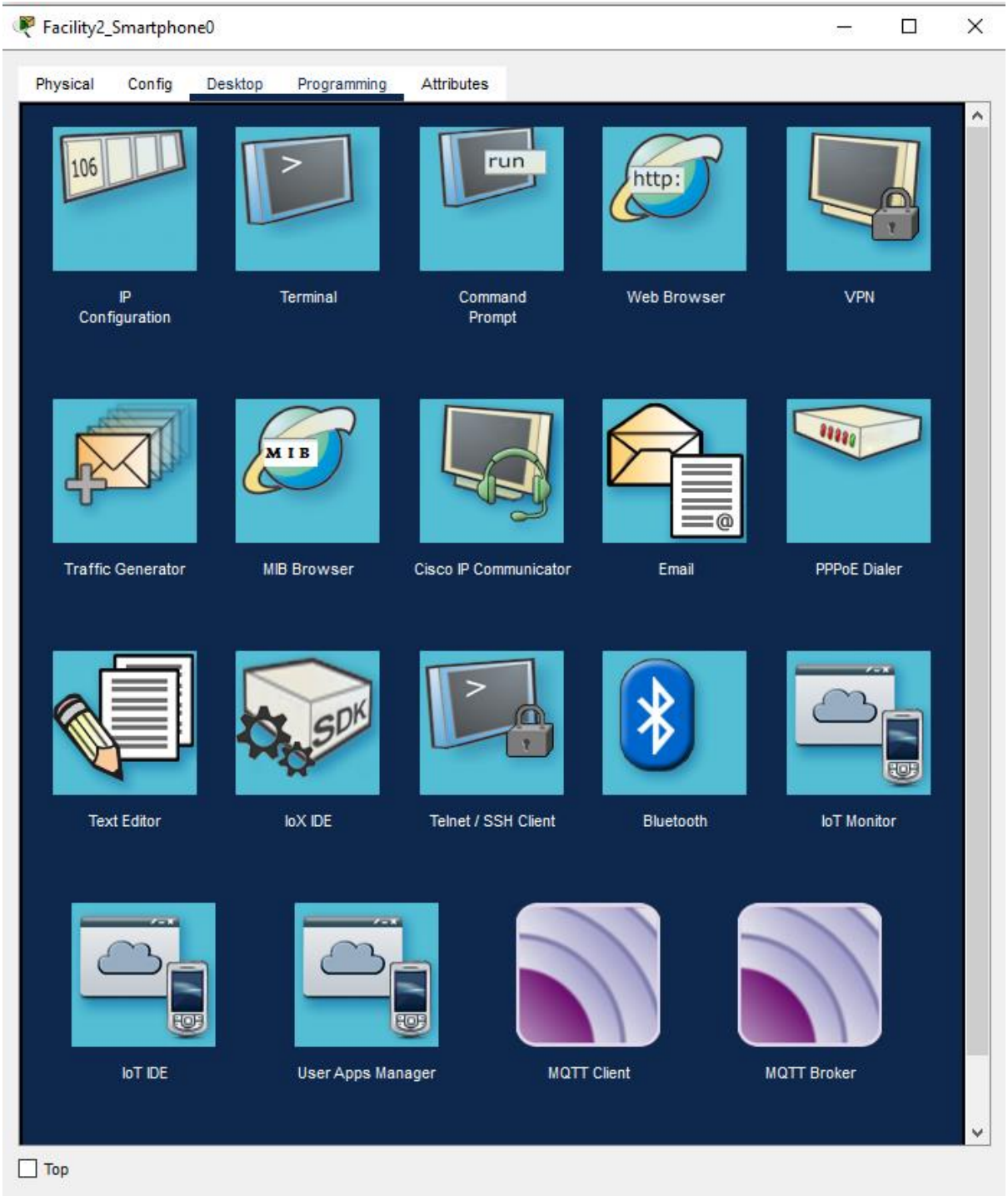

Figure 2.6.24: Editing and updating applications

2.7 Network Model Diagrams

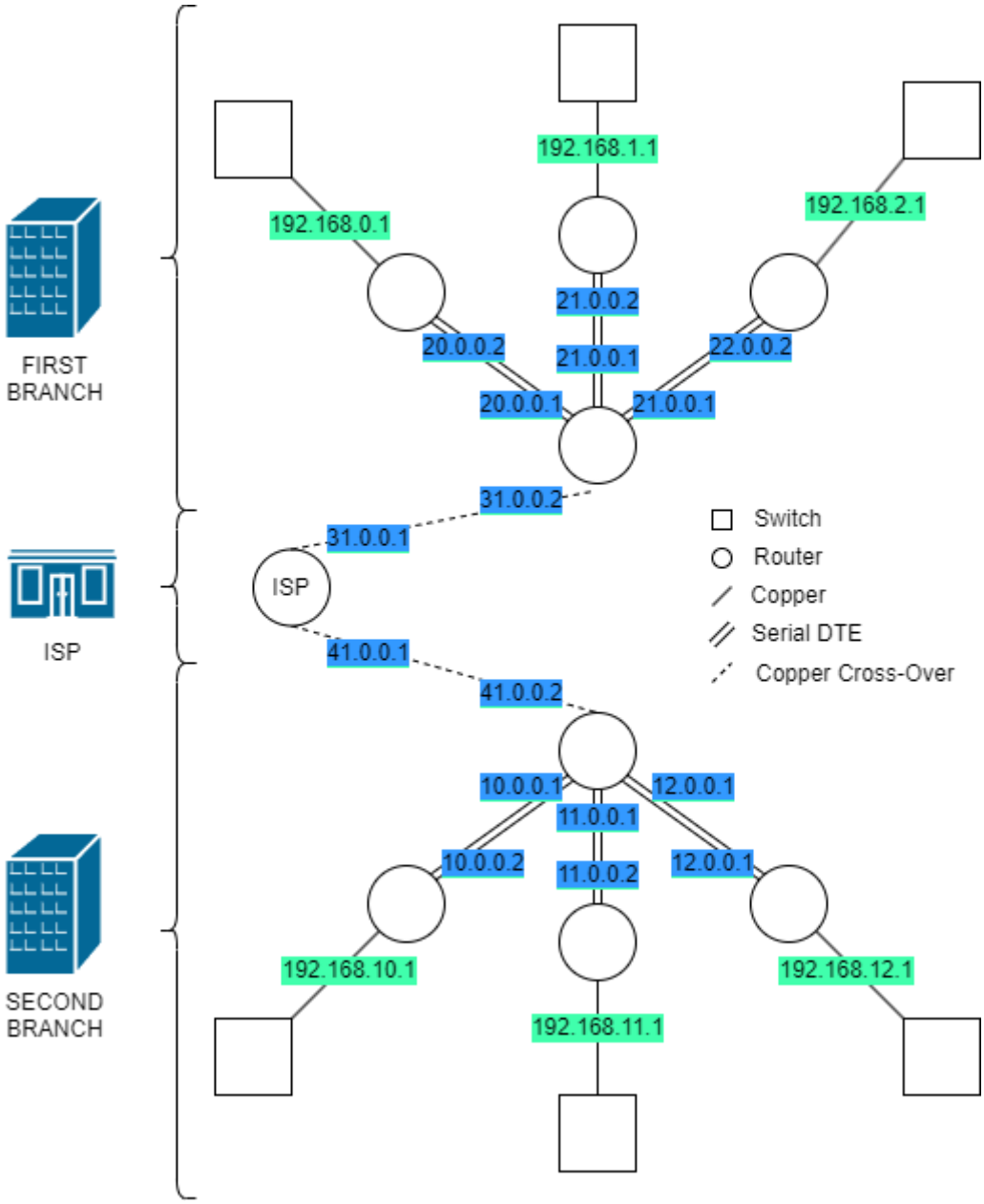

Figure 2.7.1: MAN Model Diagram

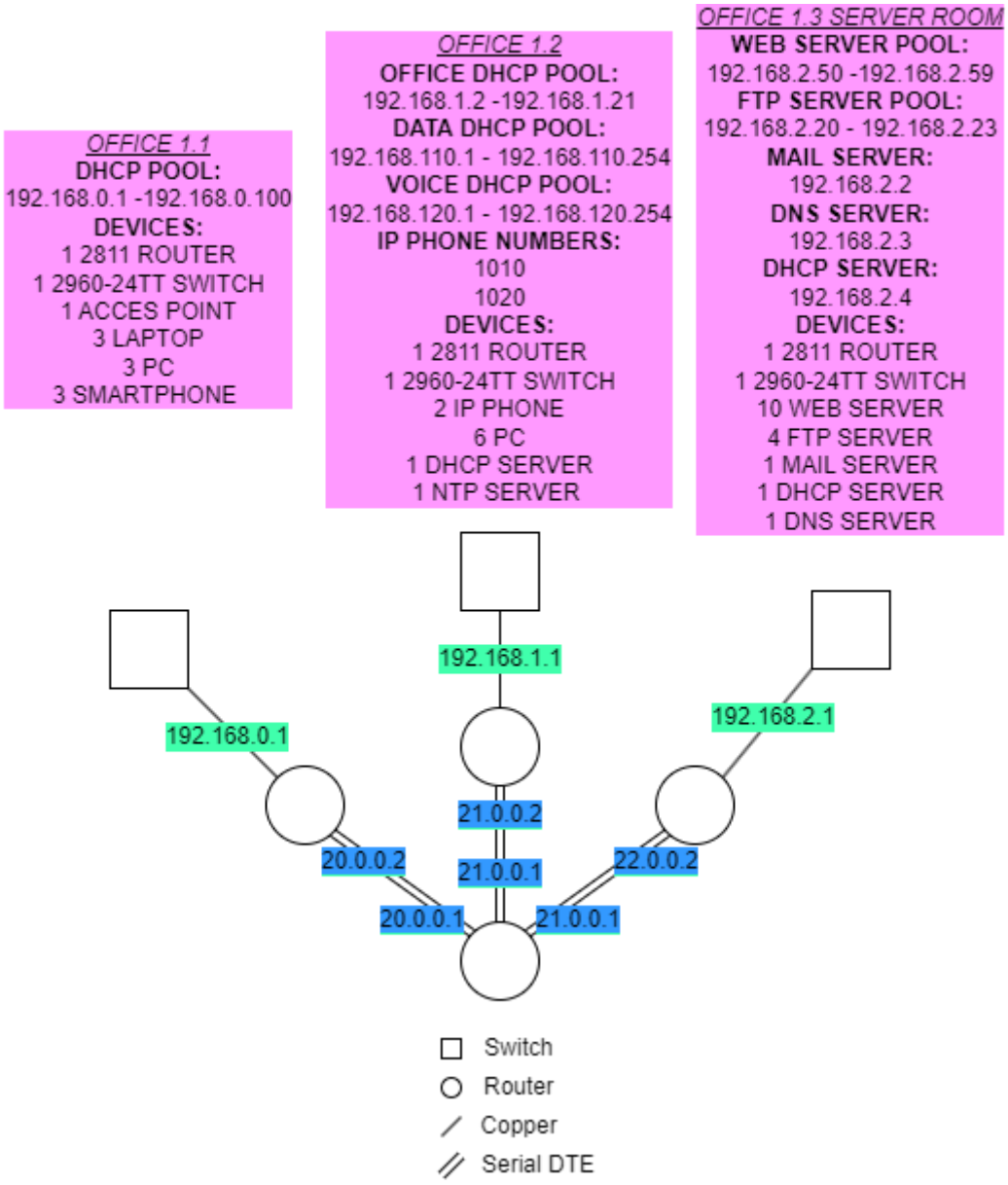

Figure 2.7.2: First Branch Diagram

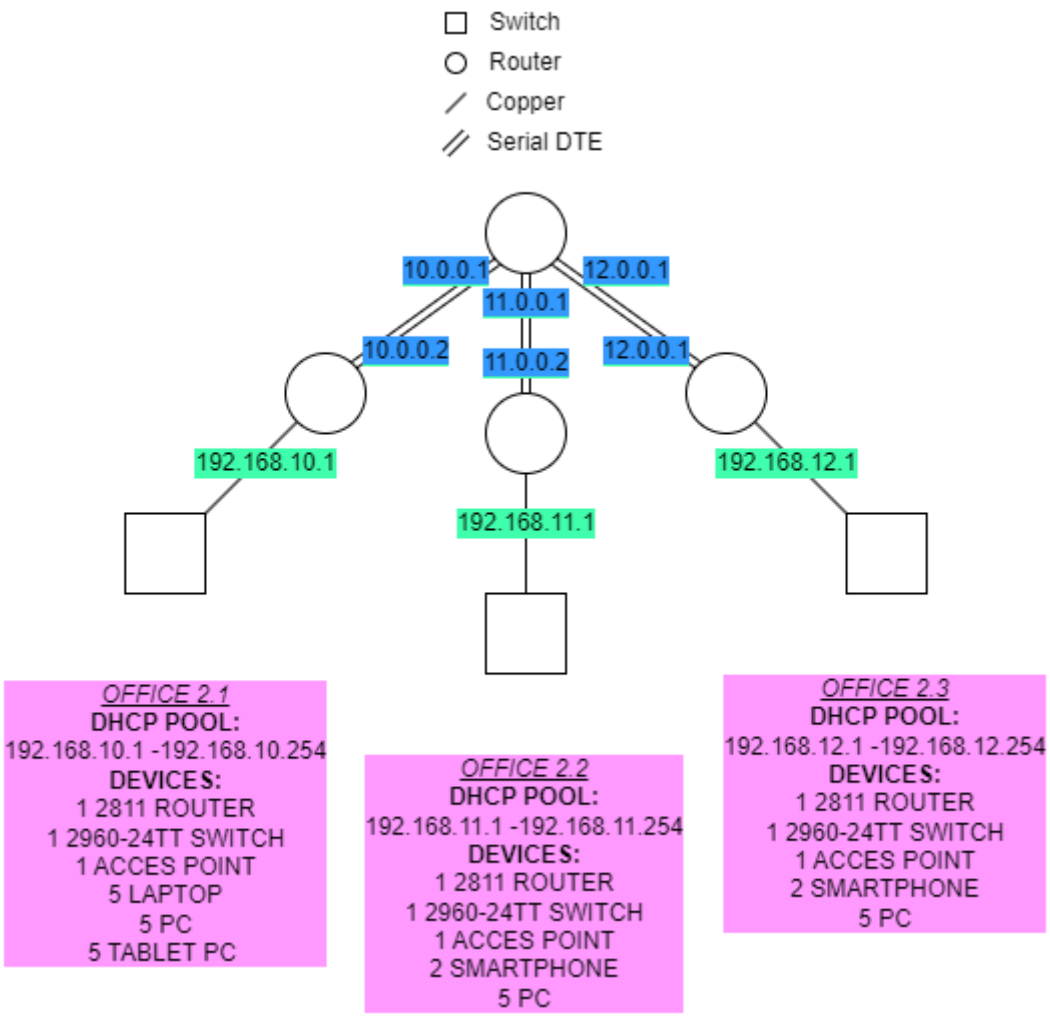

Figure 2.7.3: Second Branch Diagram

CHAPTER 3

3. Traffic Analysis and Simulation Results

3.1 Simulation Scenarios

3.1.1. Reading emails and Browsing the web

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

Reading emails - Network Functionality

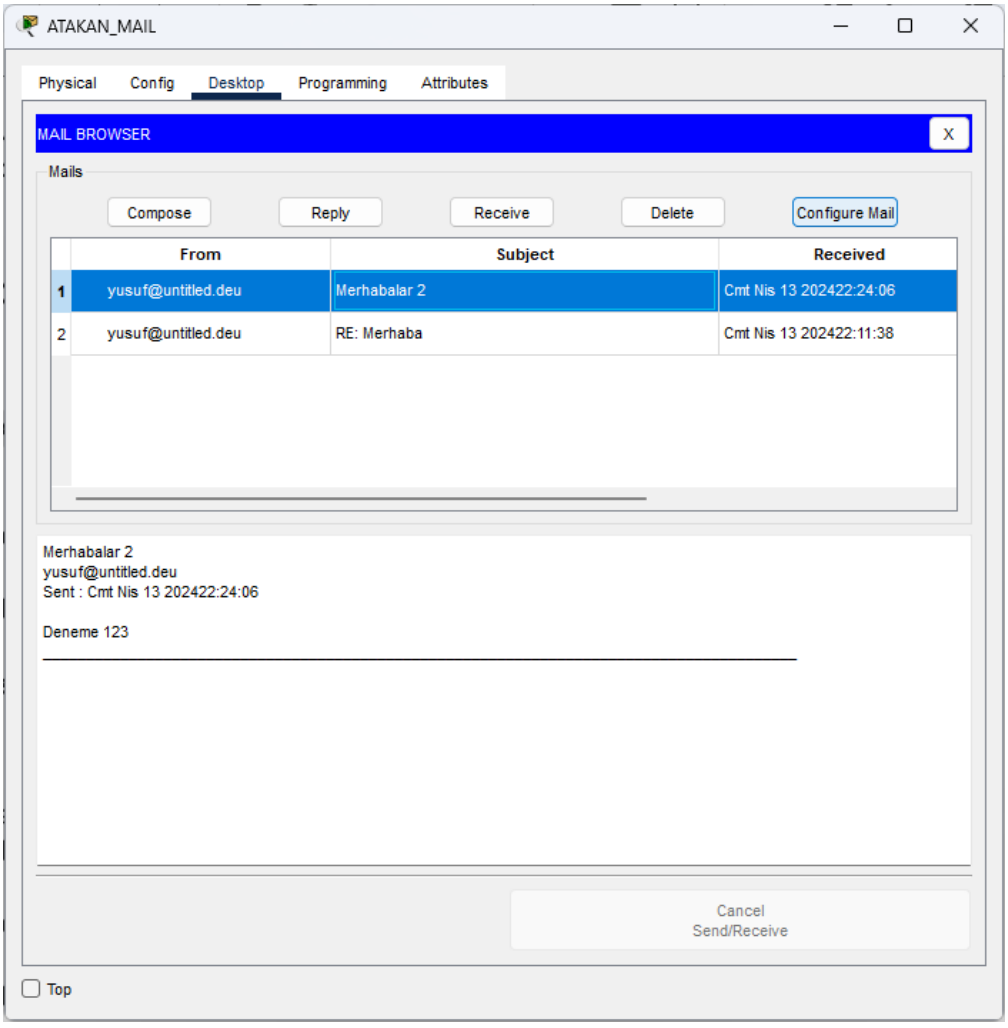

Figure 3.1.1: Email functionality

Reading emails - Protocol Data Units Content

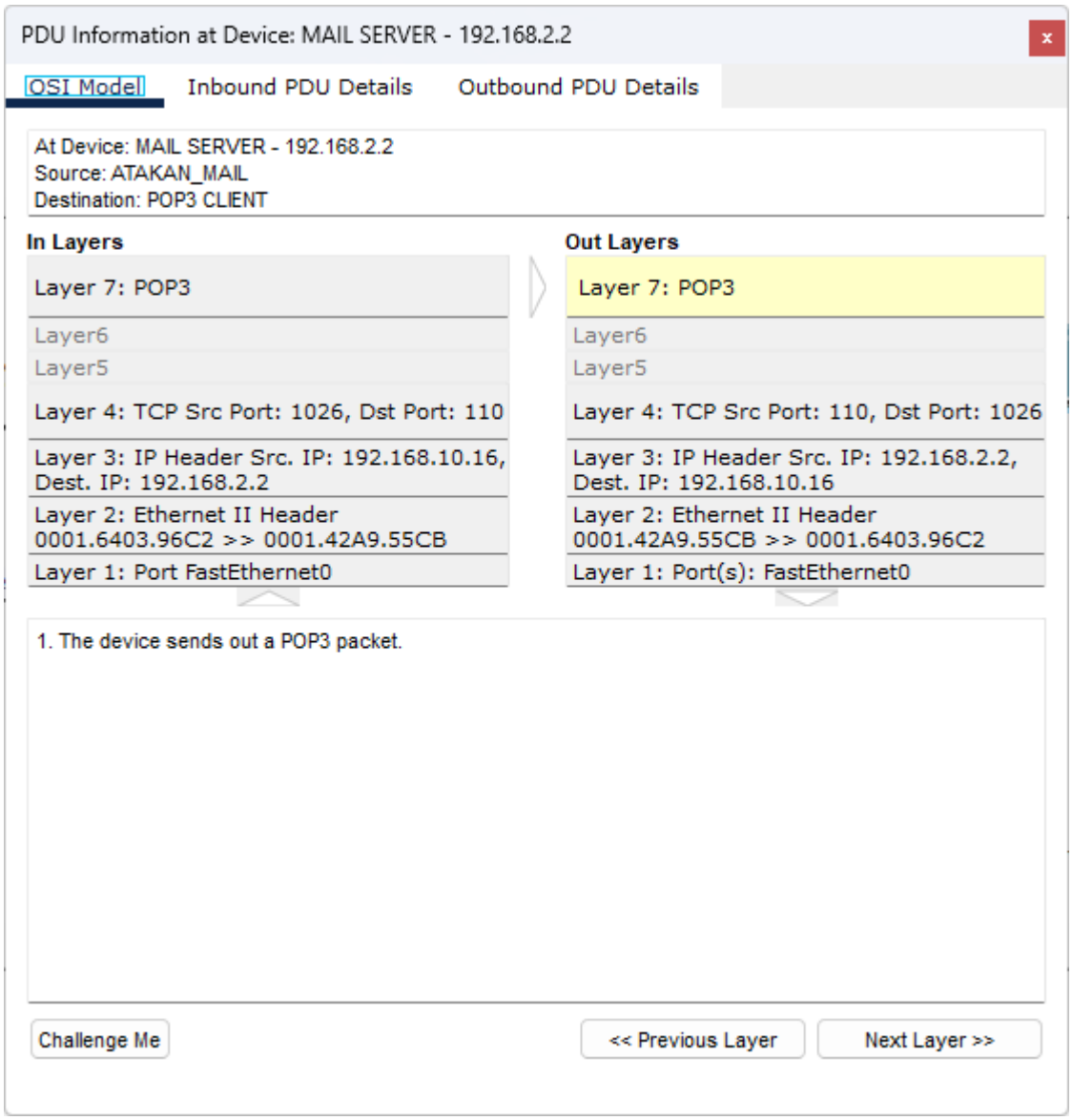

Figure 3.1.2: The outgoing PDU view

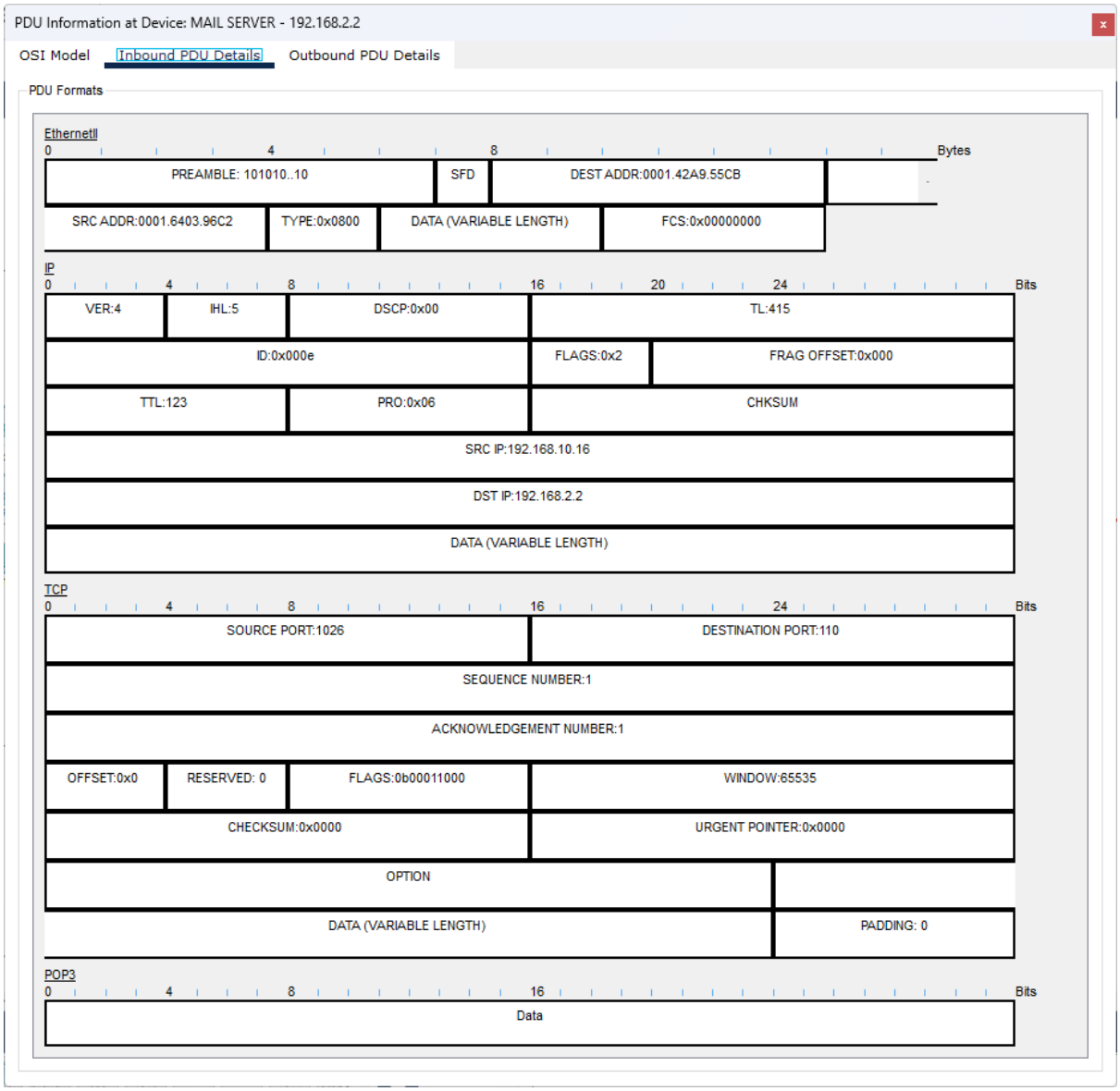

Figure 3.1.3: The outgoing PDU content

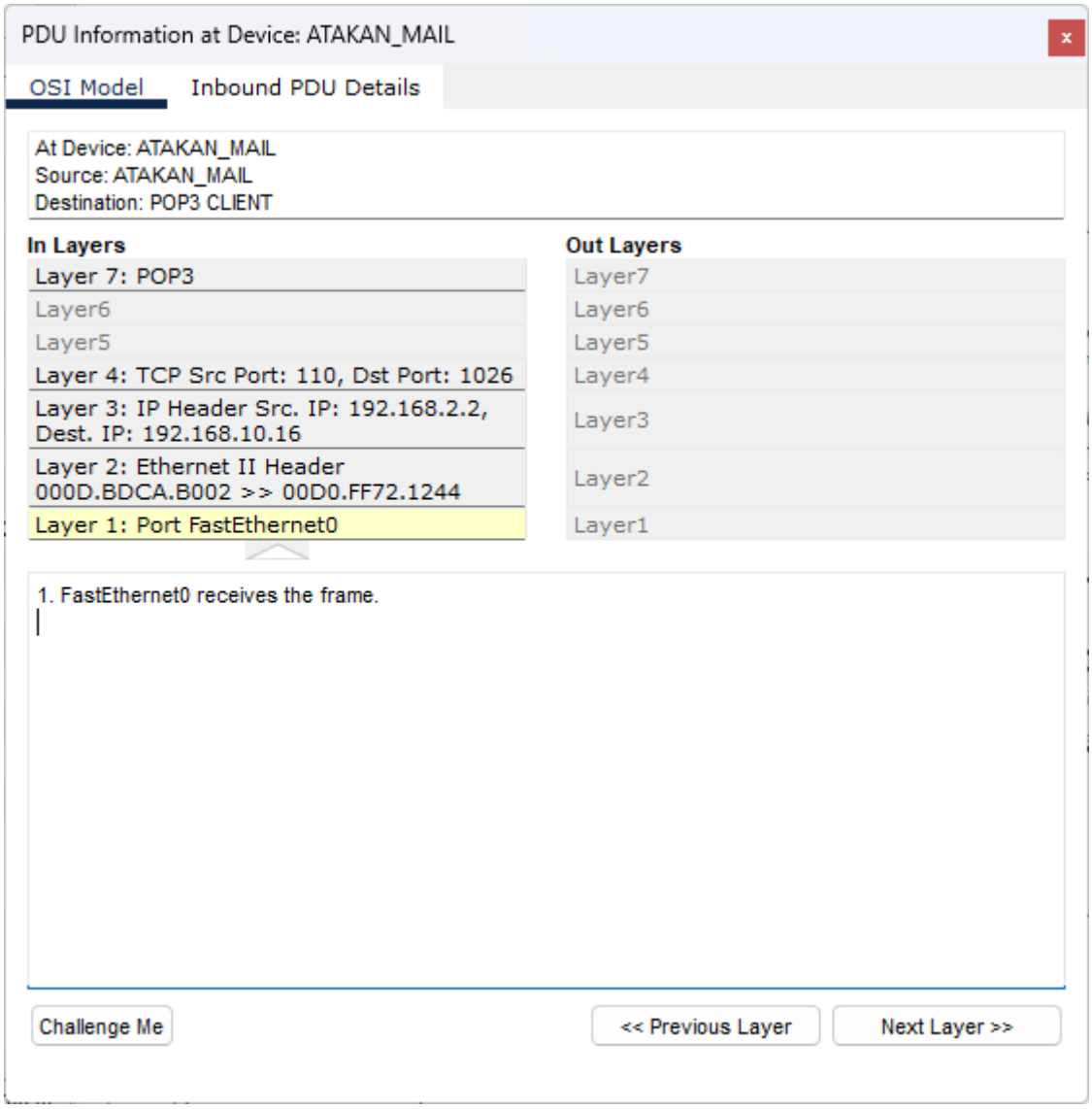

Figure 3.1.4: The incoming PDU overview

Figure 3.1.3: The incoming PDU overview

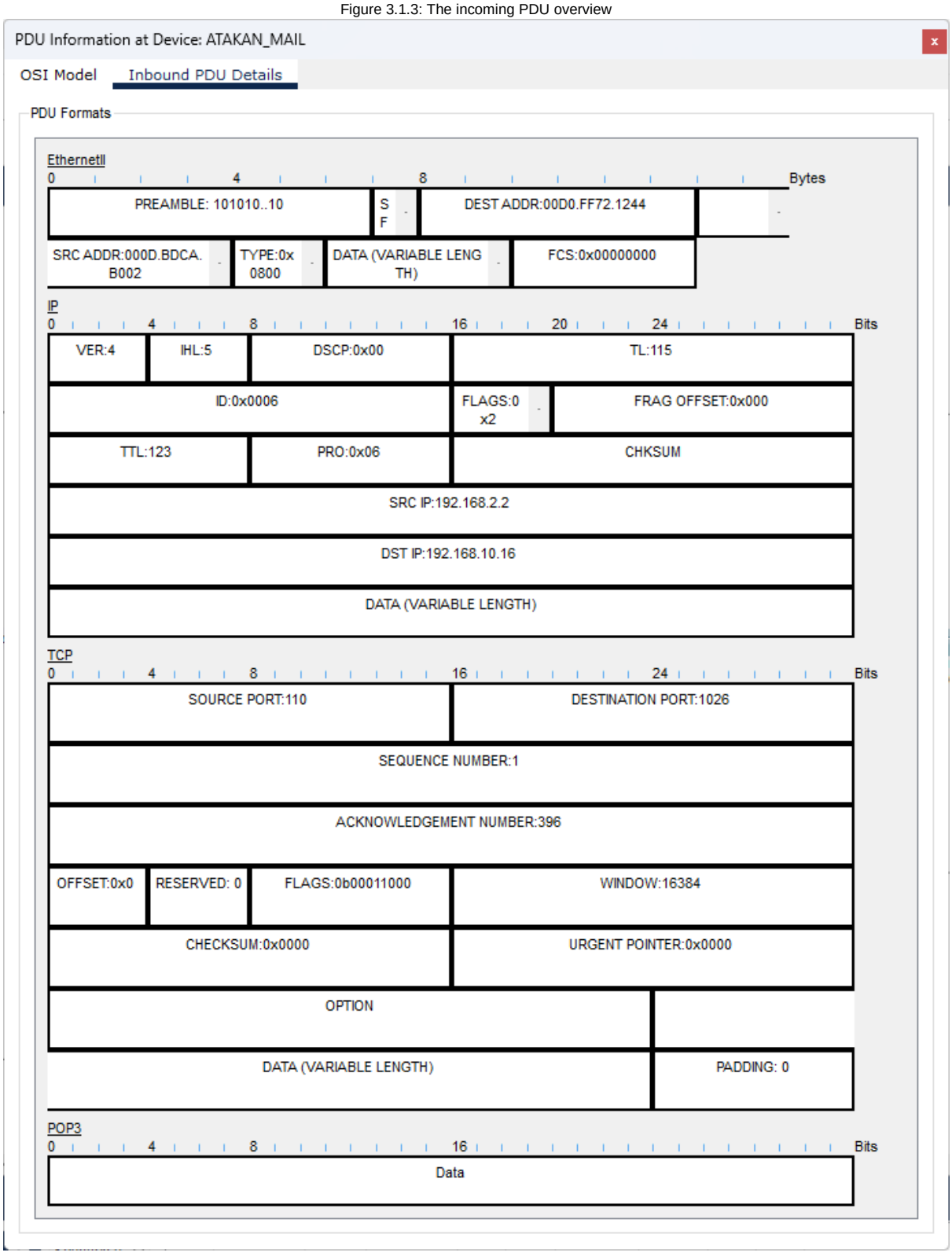

Figure 3.1.5: The incoming PDU content

Reading emails - Relevant Events List

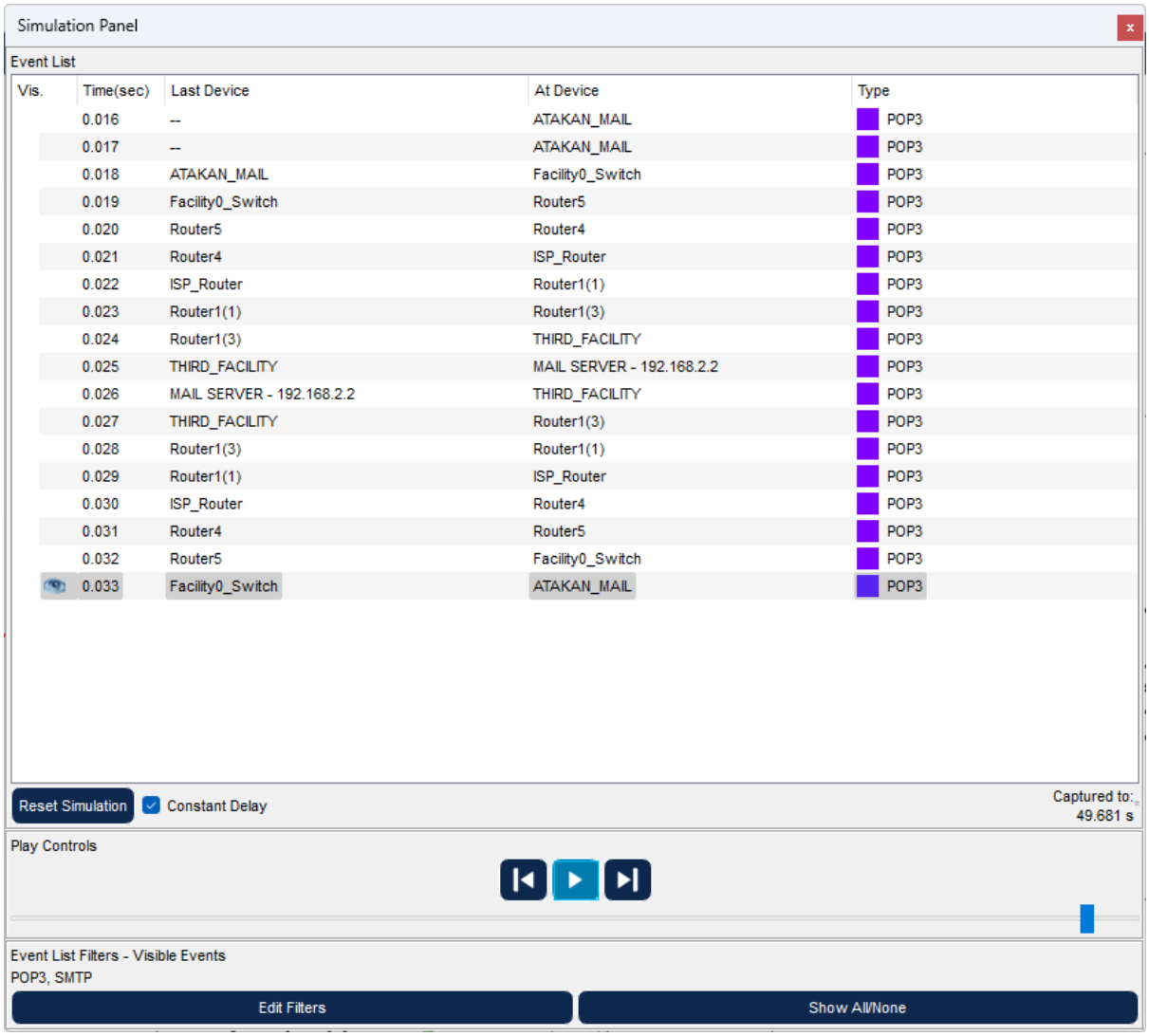

Figure 3.1.6: The relevant event list of received emails

Browsing the web - Network Functionality

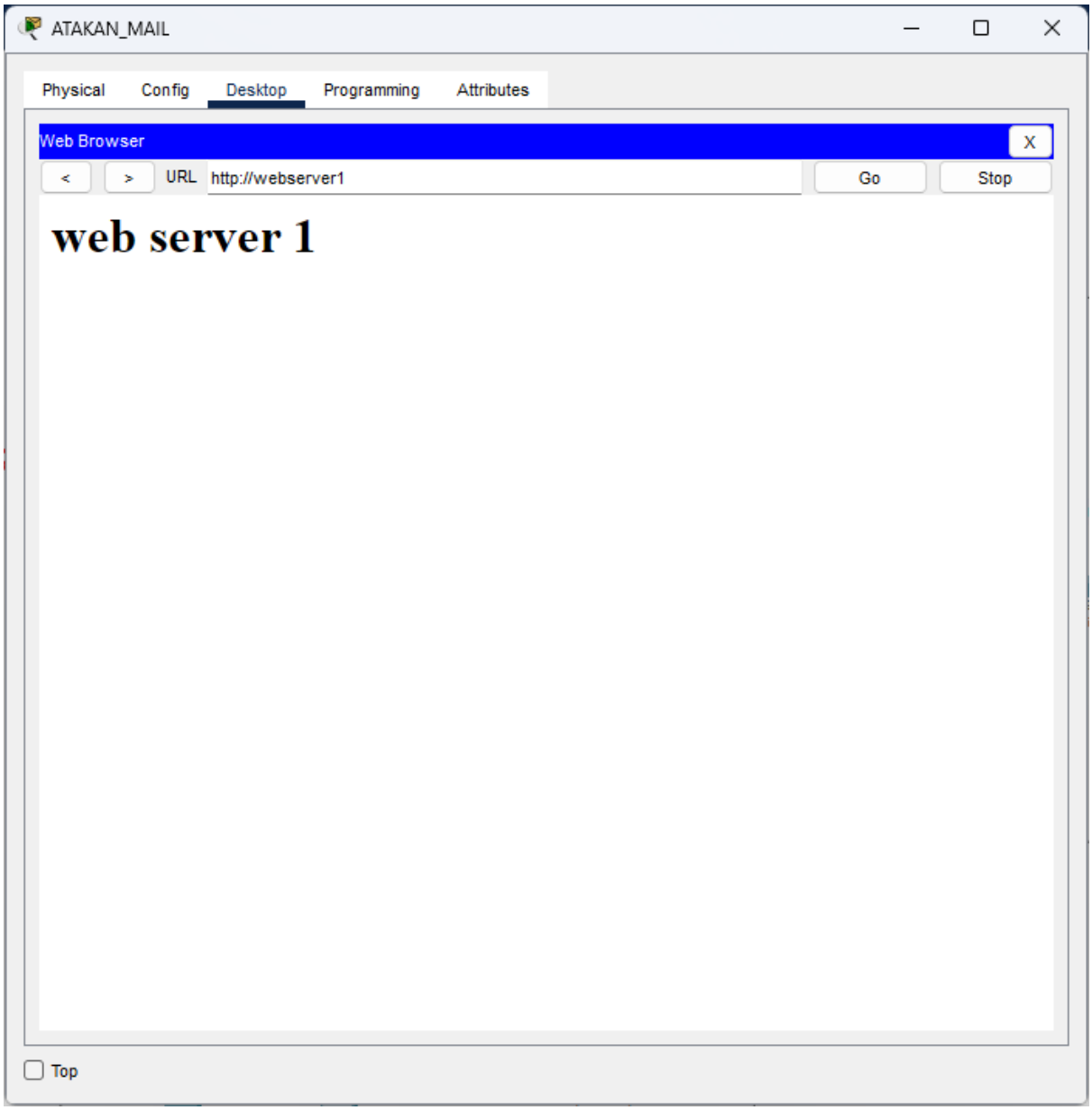

Figure 3.1.7: Network functionality of browsing the web

Browsing the web- Protocol Data Units Content

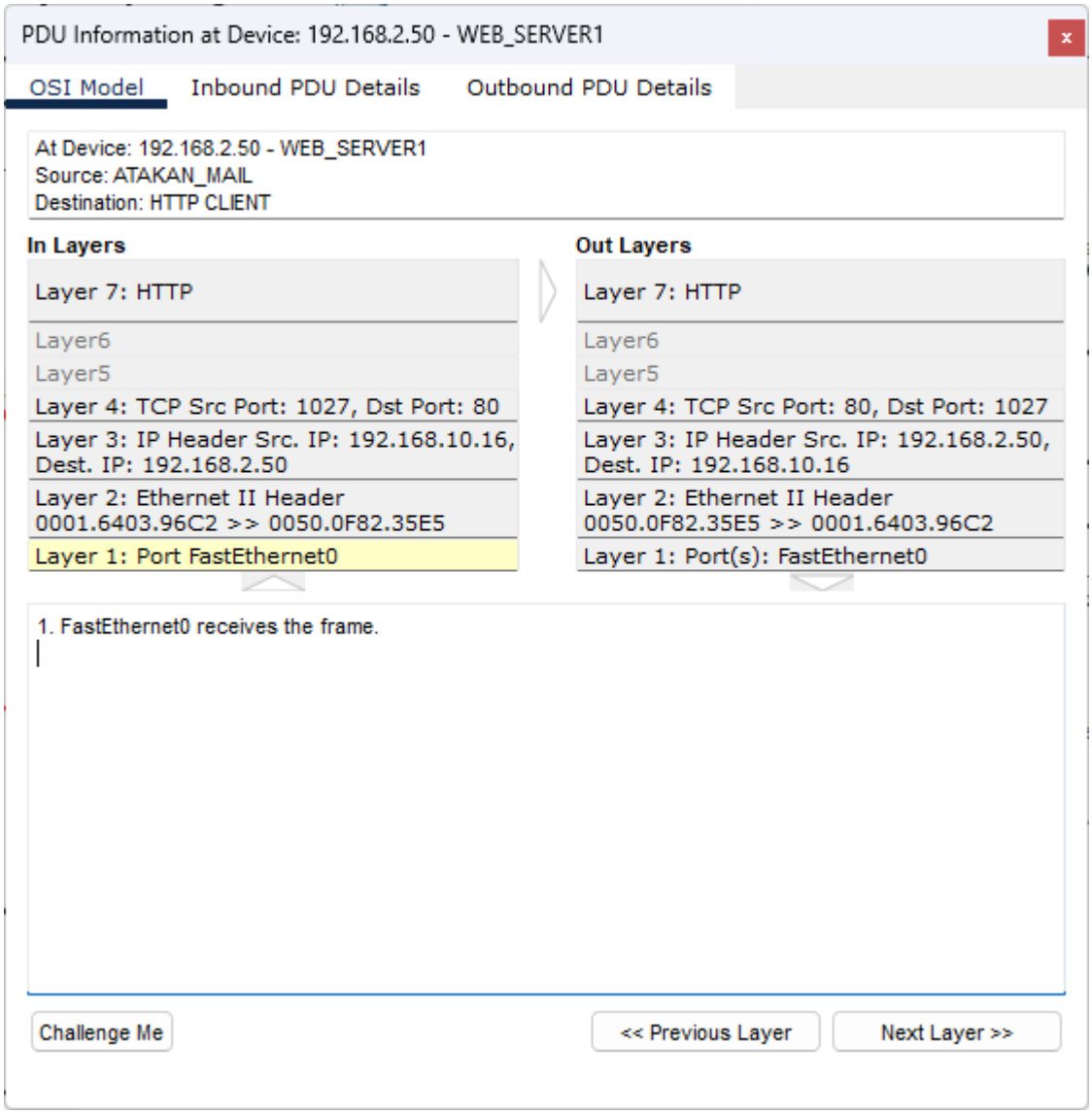

Figure 3.1.8: The outgoing PDU content

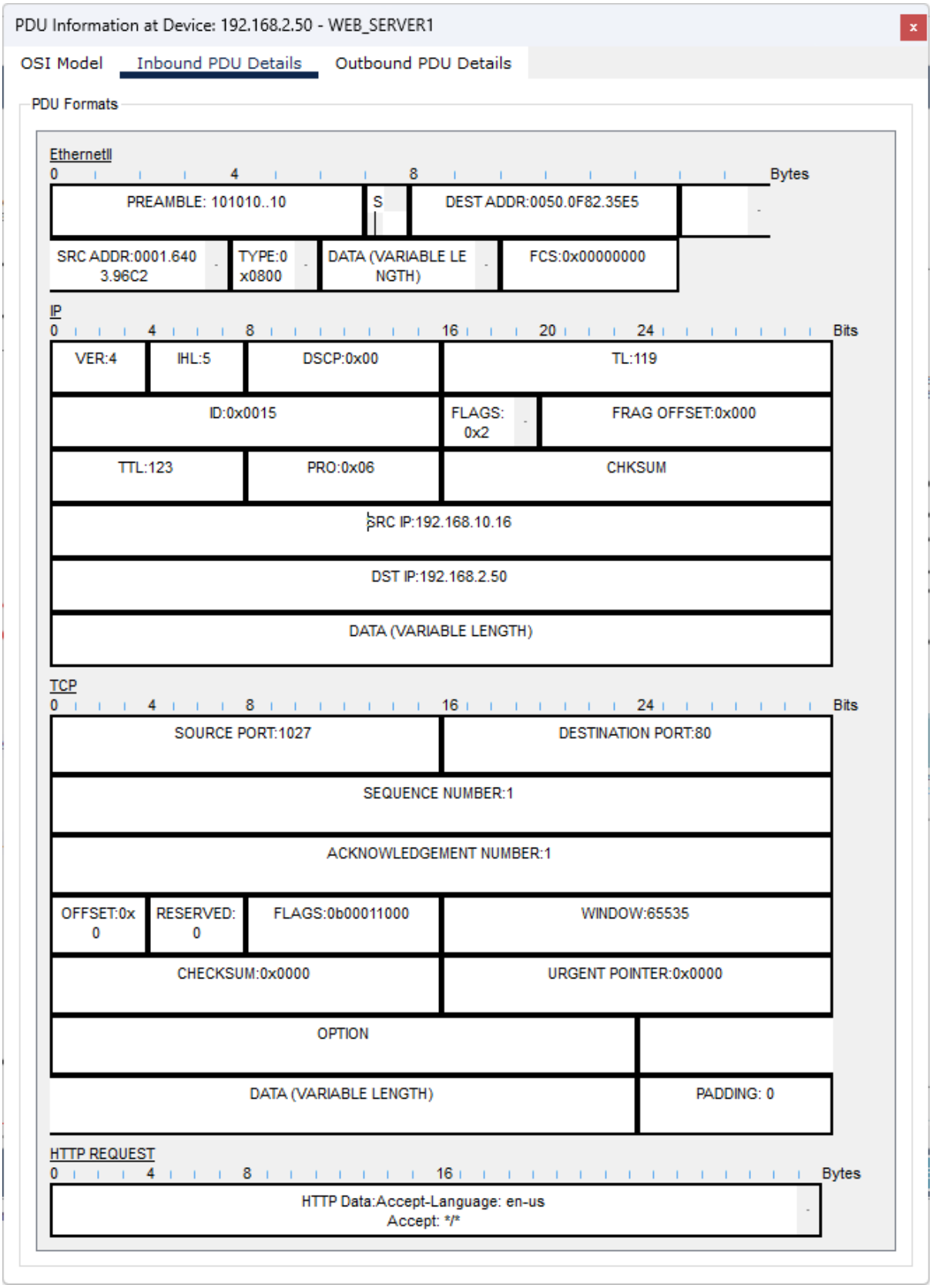

Figure 3.1.9: The outgoing PDU content

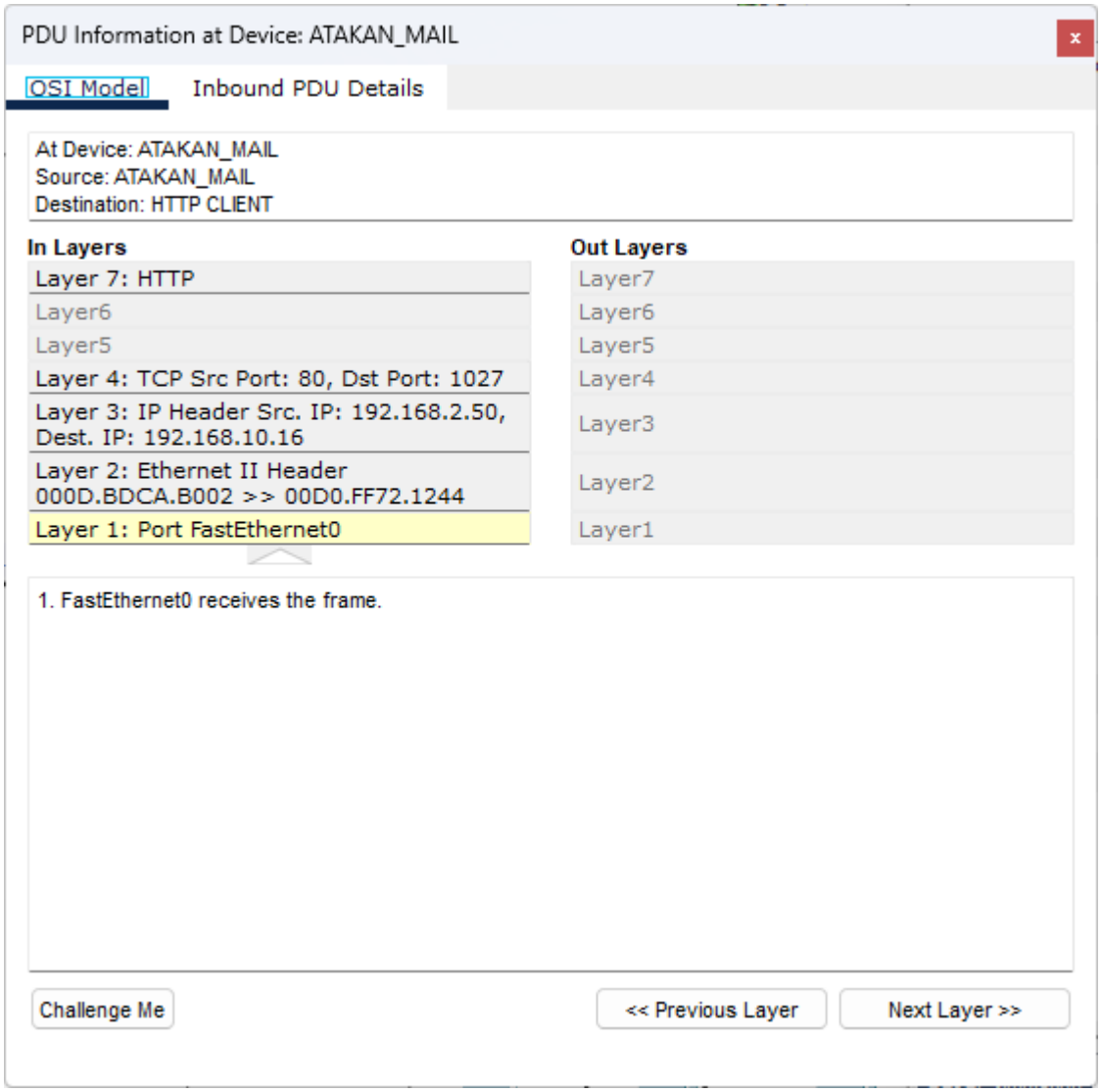

Figure 3.1.10: The incoming PDU overview

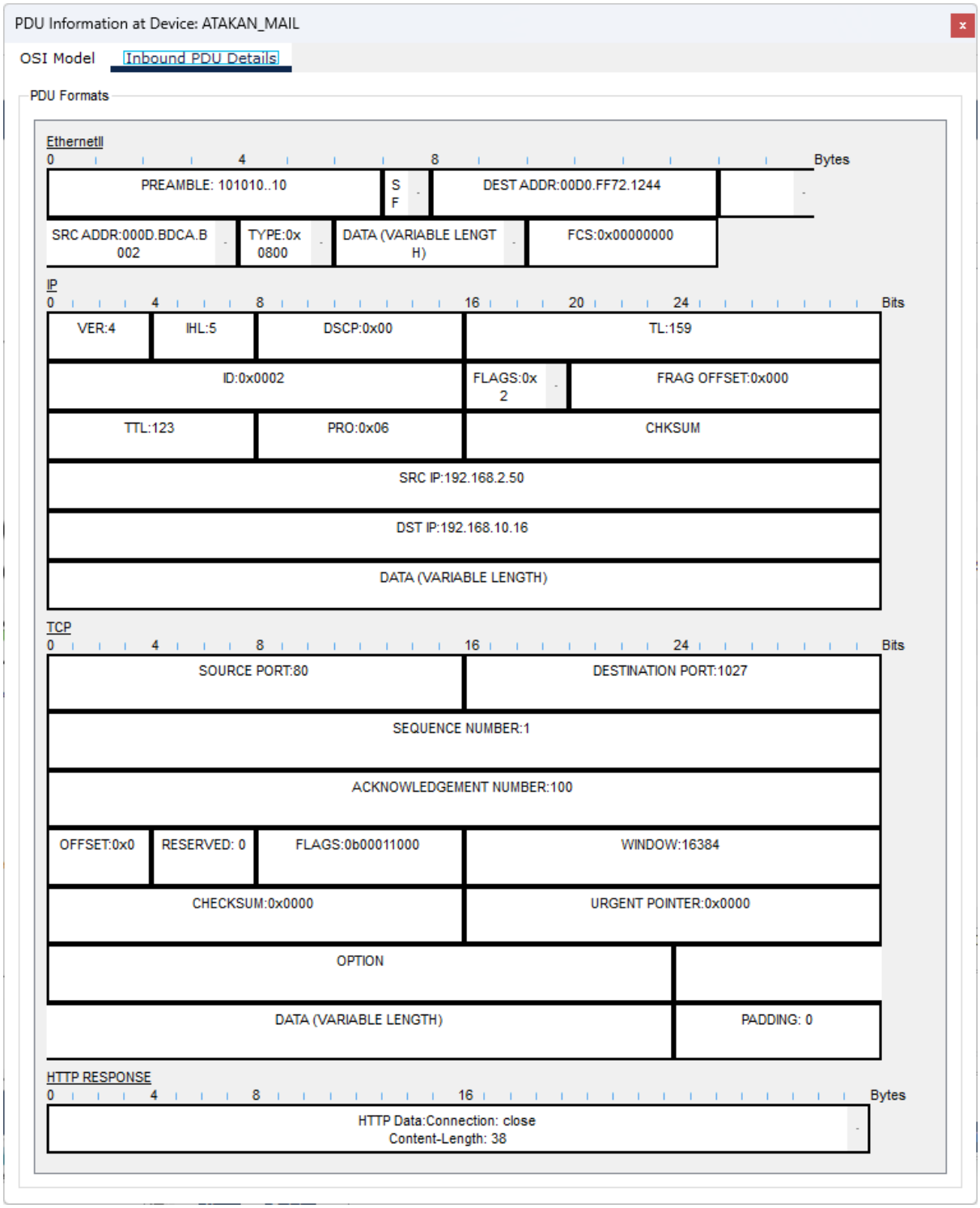

Figure 3.1.11: The incoming PDU content

Browsing the web - Relevant Events List

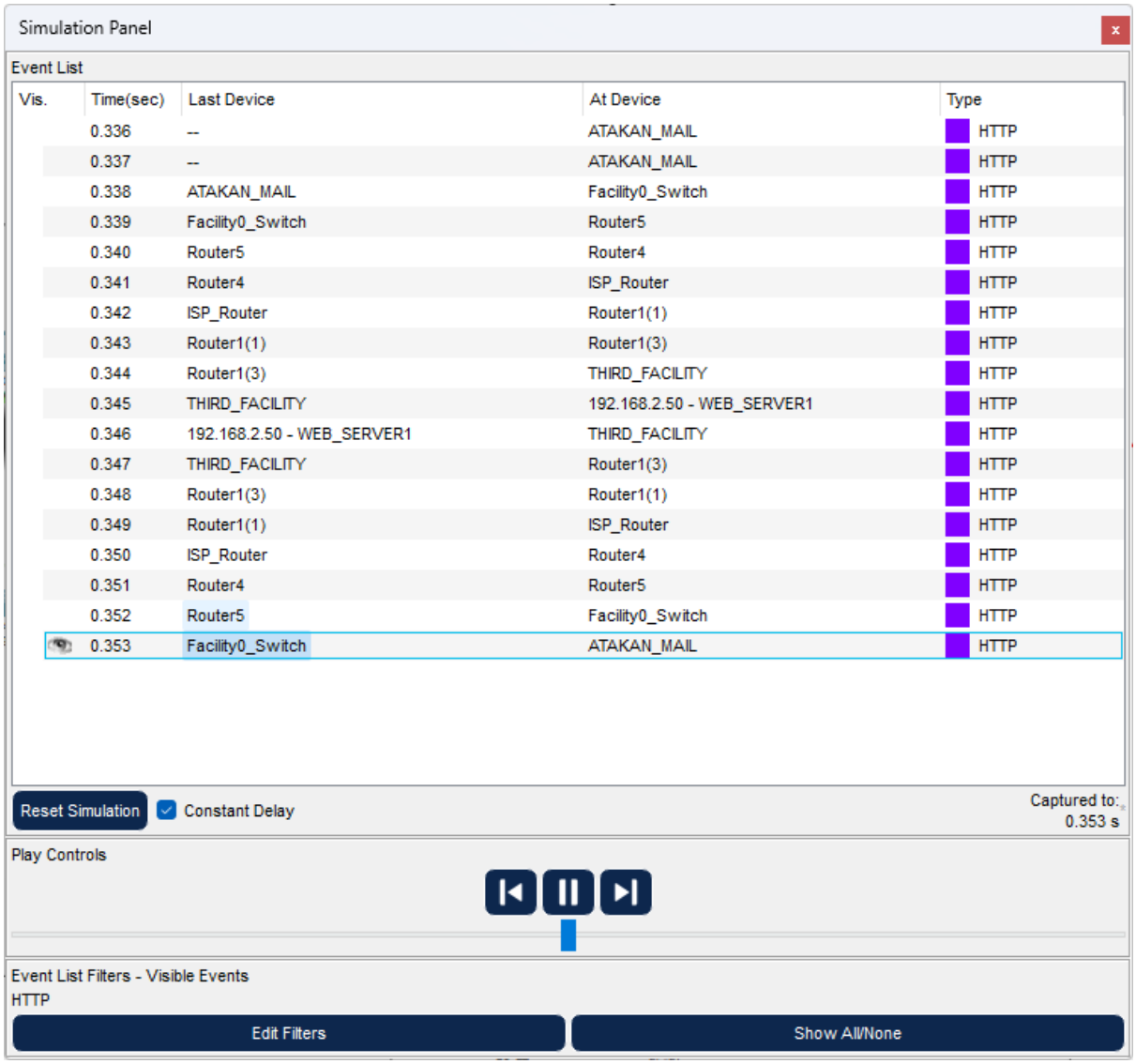

Figure 3.1.12: The relevant event list of browsing the web

3.1.2. Sending code files over FTP

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

Network Functionality

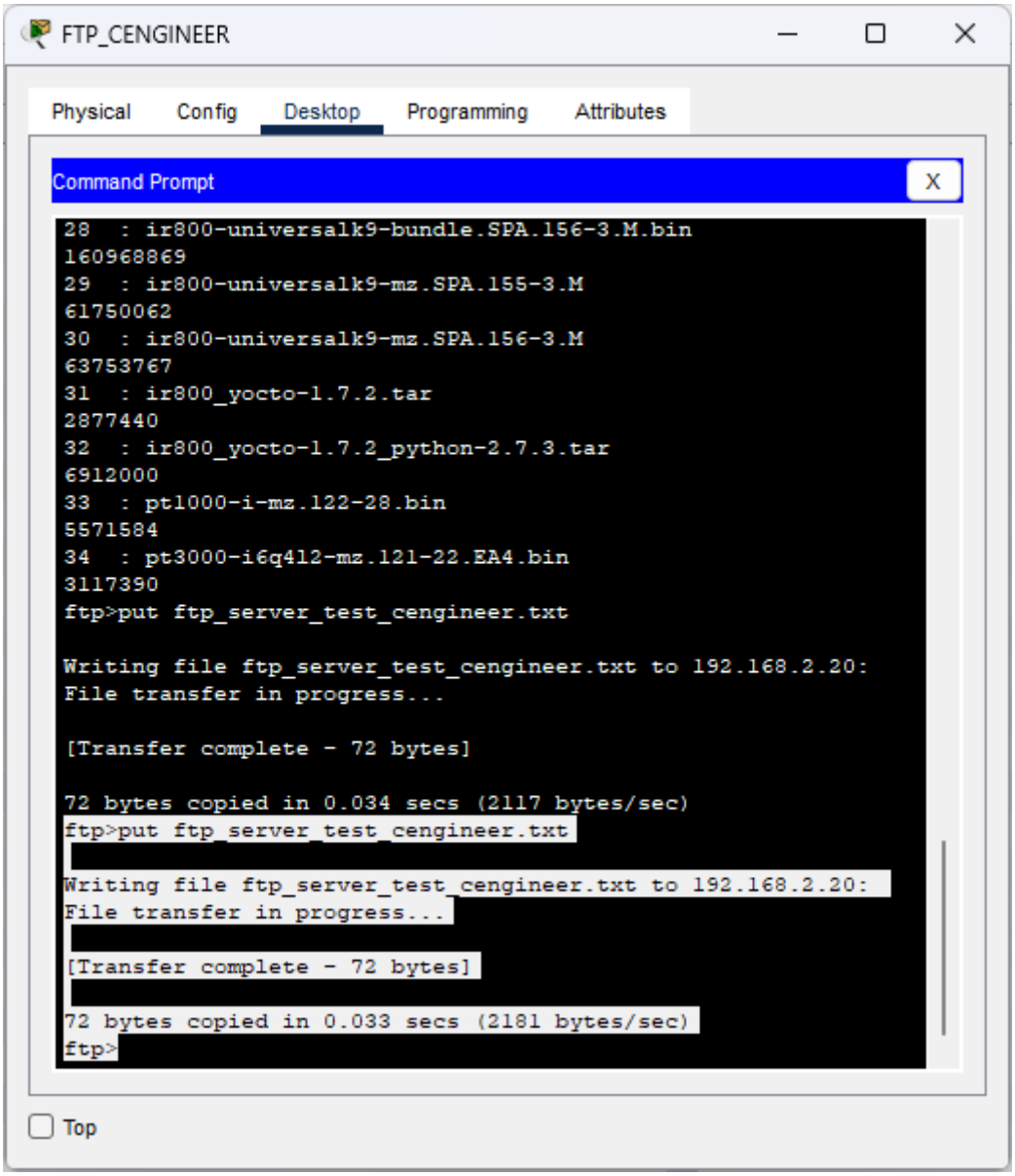

Figure 3.2.1: FTP network functionality

Protocol Data Units Content

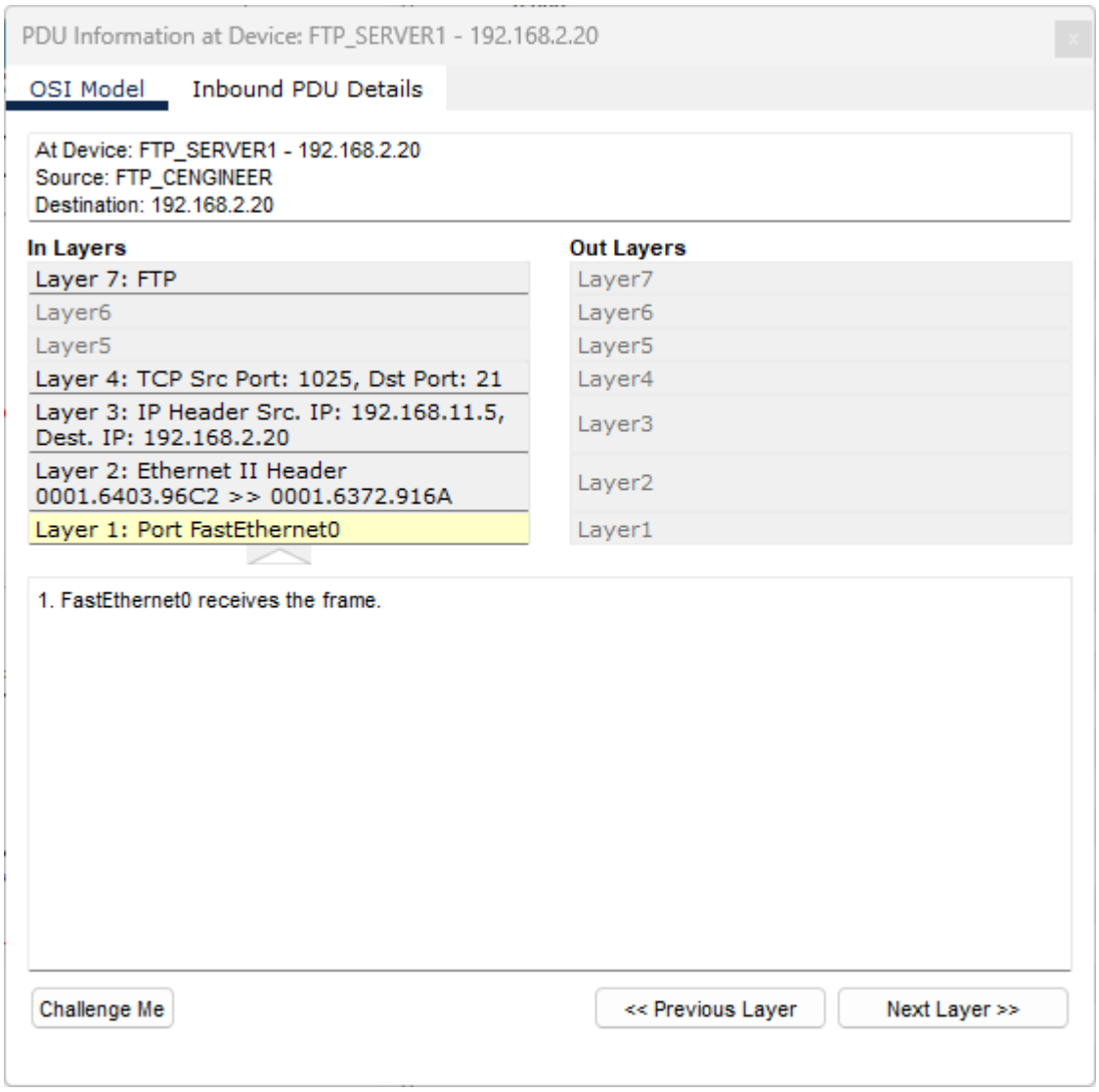

Figure 3.2.2: PDU overview of FTP functionality

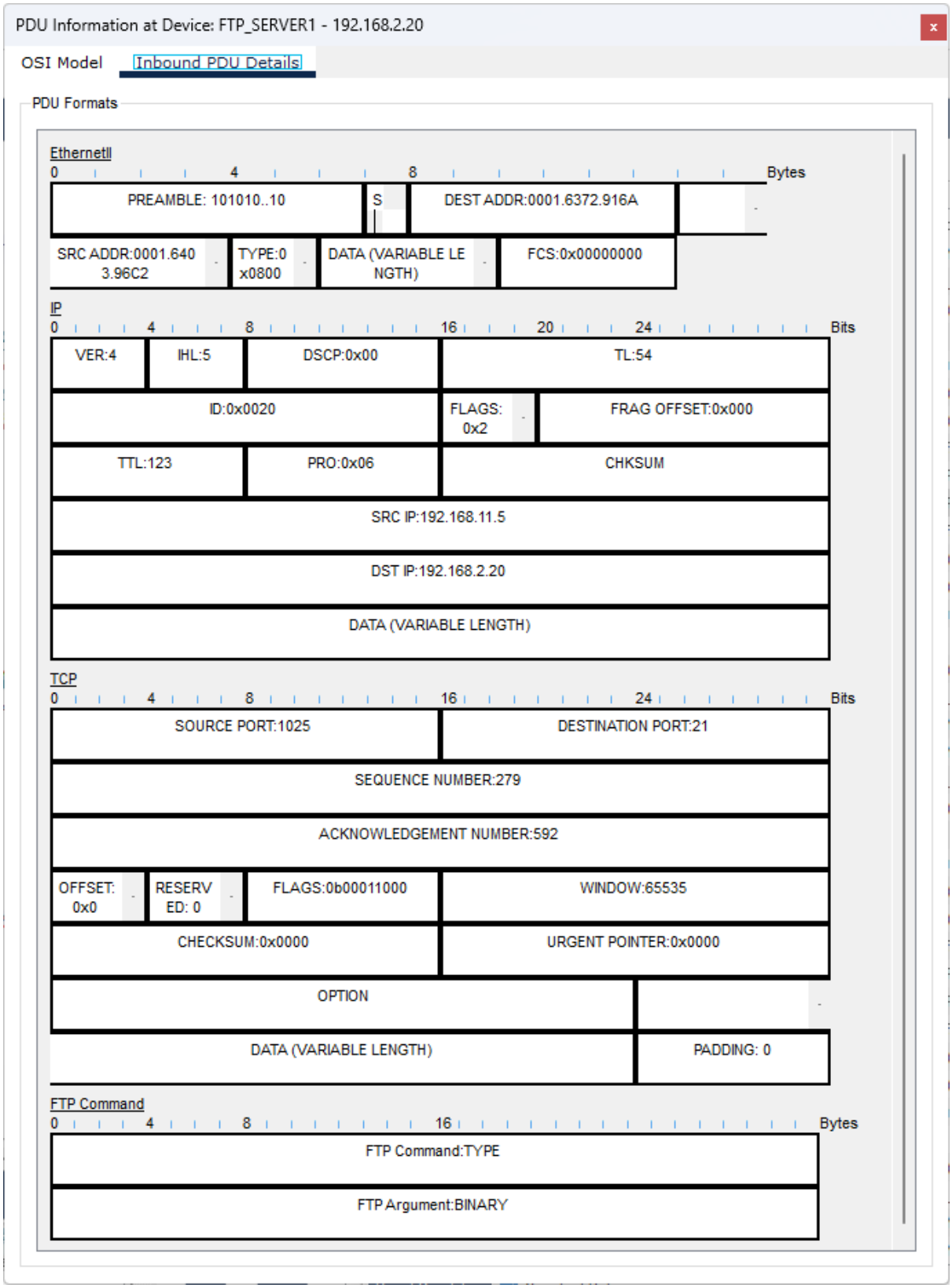

Figure 3.2.3: The actual PDU content of FTP

Relevant Events List

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	FTP_CENGINEER	FTP
	0.001	FTP_CENGINEER	Facility1_Switch	FTP
	0.002	Facility1_Switch	Router5(1)	FTP
	0.003	Router5(1)	Router4	FTP
	0.004	Router4	ISP_Router	FTP
	0.005	ISP_Router	Router1(1)	FTP
	0.006	Router1(1)	Router1(3)	FTP
	0.007	Router1(3)	THIRD_FACILITY	FTP
	0.008	THIRD_FACILITY	FTP_SERVER1 - 192.168.2.20	FTP
	0.008	--	FTP_SERVER1 - 192.168.2.20	FTP
	0.009	FTP_SERVER1 - 192.168.2.20	THIRD_FACILITY	FTP
	0.010	THIRD_FACILITY	Router1(3)	FTP
	0.011	Router1(3)	Router1(1)	FTP
	0.012	Router1(1)	ISP_Router	FTP
	0.013	ISP_Router	Router4	FTP
	0.014	Router4	Router5(1)	FTP
	0.015	Router5(1)	Facility1_Switch	FTP
	0.016	Facility1_Switch	FTP_CENGINEER	FTP
	0.016	--	FTP_CENGINEER	FTP
	0.017	FTP_CENGINEER	Facility1_Switch	FTP
	0.018	Facility1_Switch	Router5(1)	FTP
	0.019	Router5(1)	Router4	FTP
	0.020	Router4	ISP_Router	FTP
	0.021	ISP_Router	Router1(1)	FTP
	0.022	Router1(1)	Router1(3)	FTP
	0.023	Router1(3)	THIRD_FACILITY	FTP
	0.024	THIRD_FACILITY	FTP_SERVER1 - 192.168.2.20	FTP
	0.024	--	FTP_SERVER1 - 192.168.2.20	FTP
	0.025	FTP_SERVER1 - 192.168.2.20	THIRD_FACILITY	FTP
	0.026	THIRD_FACILITY	Router1(3)	FTP
	0.027	Router1(3)	Router1(1)	FTP
	0.028	Router1(1)	ISP_Router	FTP
	0.029	ISP_Router	Router4	FTP
	0.030	Router4	Router5(1)	FTP
	0.031	Router5(1)	Facility1_Switch	FTP
	0.032	Facility1_Switch	FTP_CENGINEER	FTP
	0.032	--	FTP_CENGINEER	FTP

Reset Simulation | Constant Delay | Captured to: 49.869 s

Play Controls

Event List Filters - Visible Events

FTP

Edit Filters | Show All/None

Figure 3.2.4: The first part of the relevant FTP event list

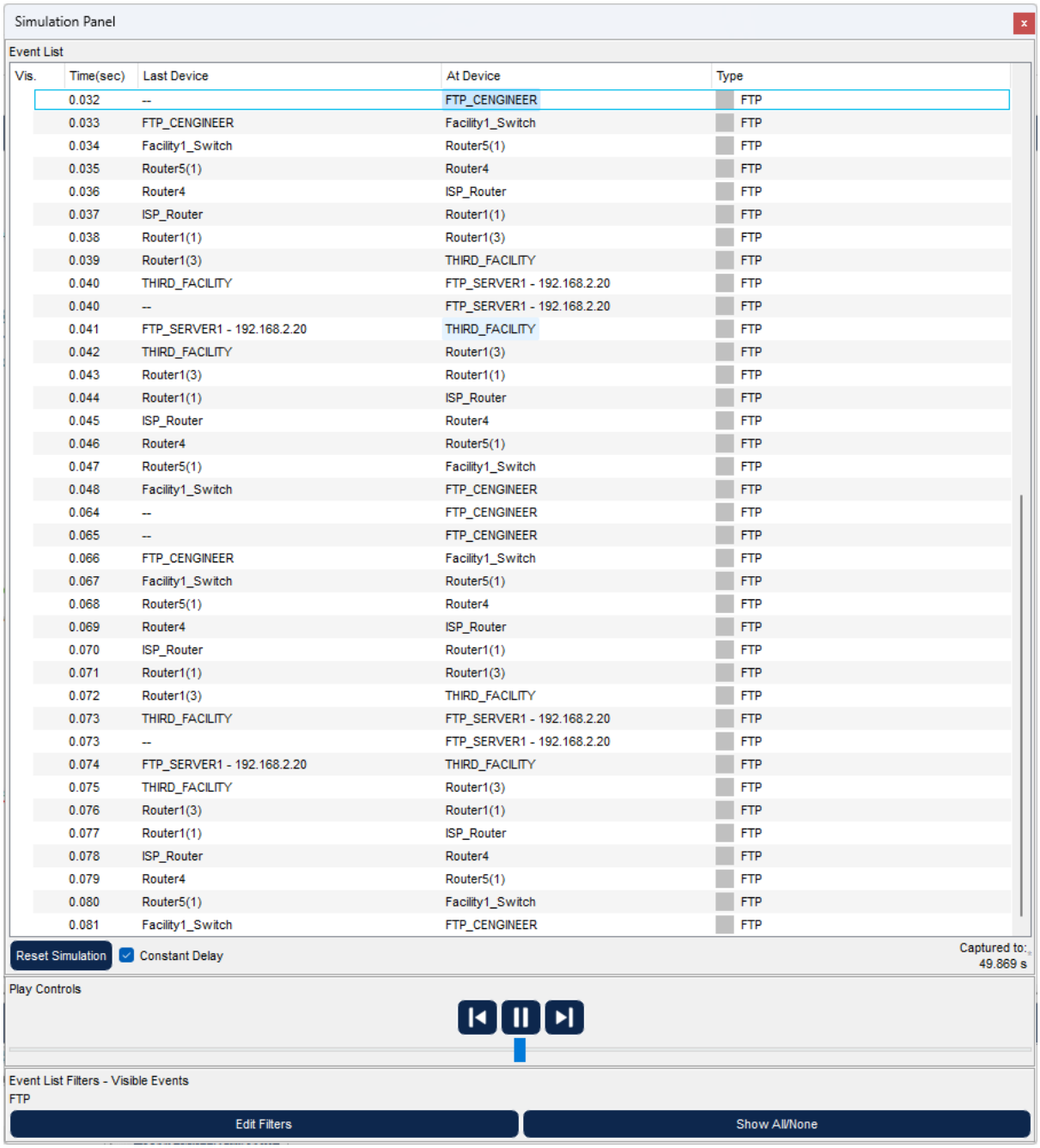

Figure 3.2.4: The second part of the relevant FTP event list

3.1.3. Talking via VoIP

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

Network Functionality

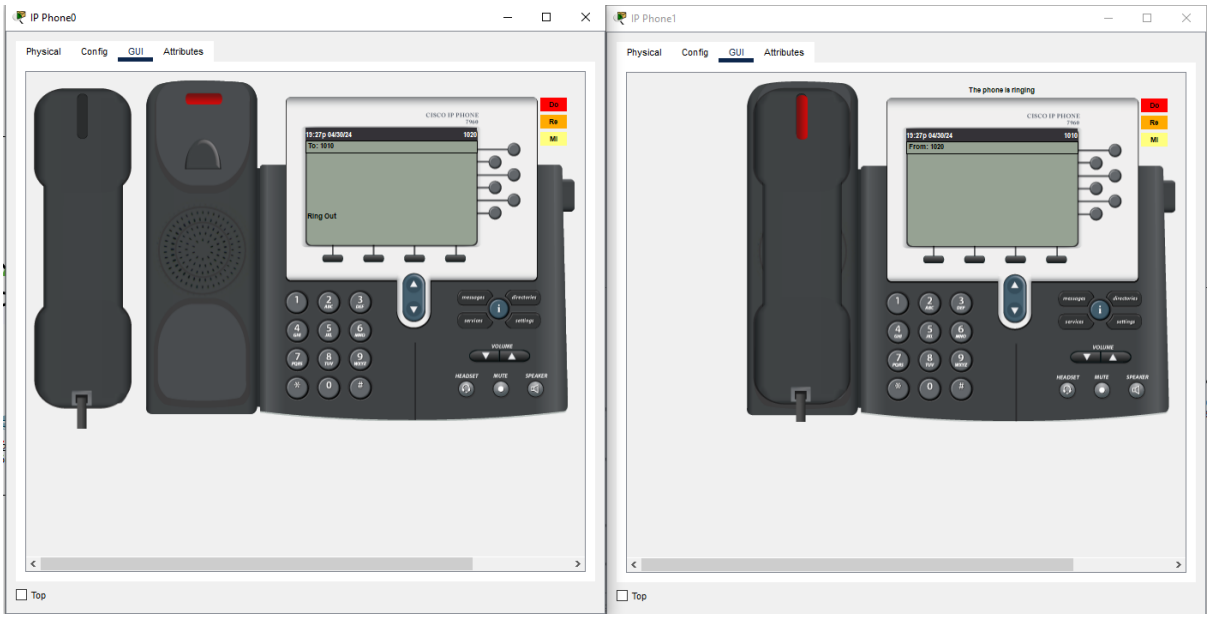

Figure 3.3.1: Calling another IP phone

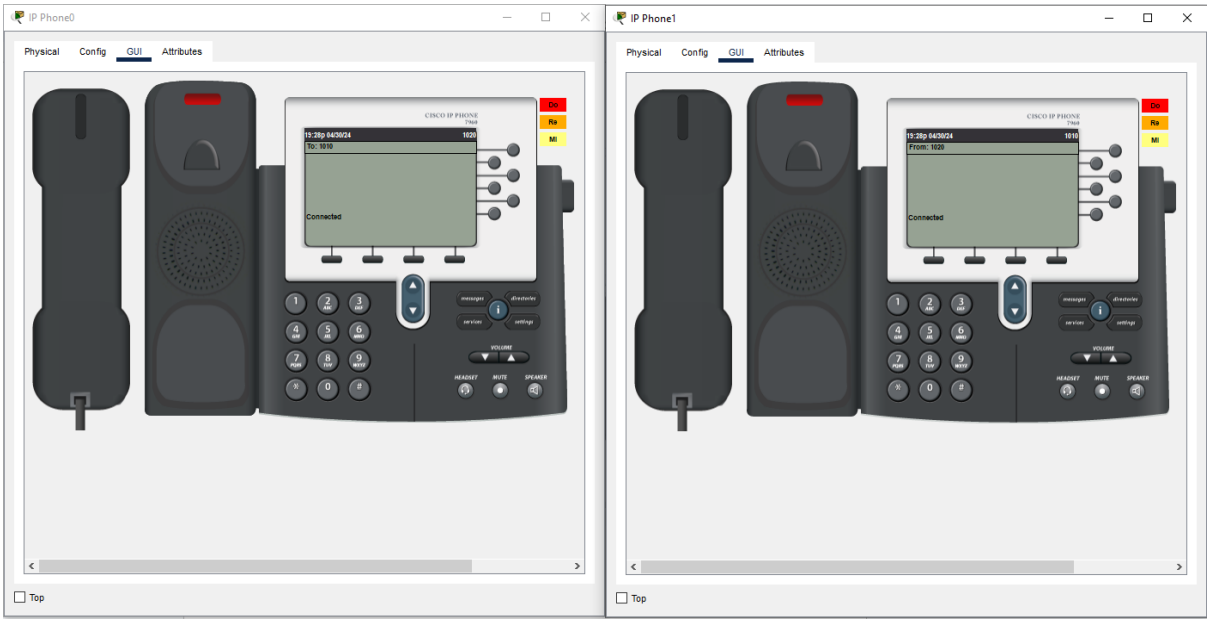

Figure 3.3.2: Connected IP phones

Protocol Data Units Content

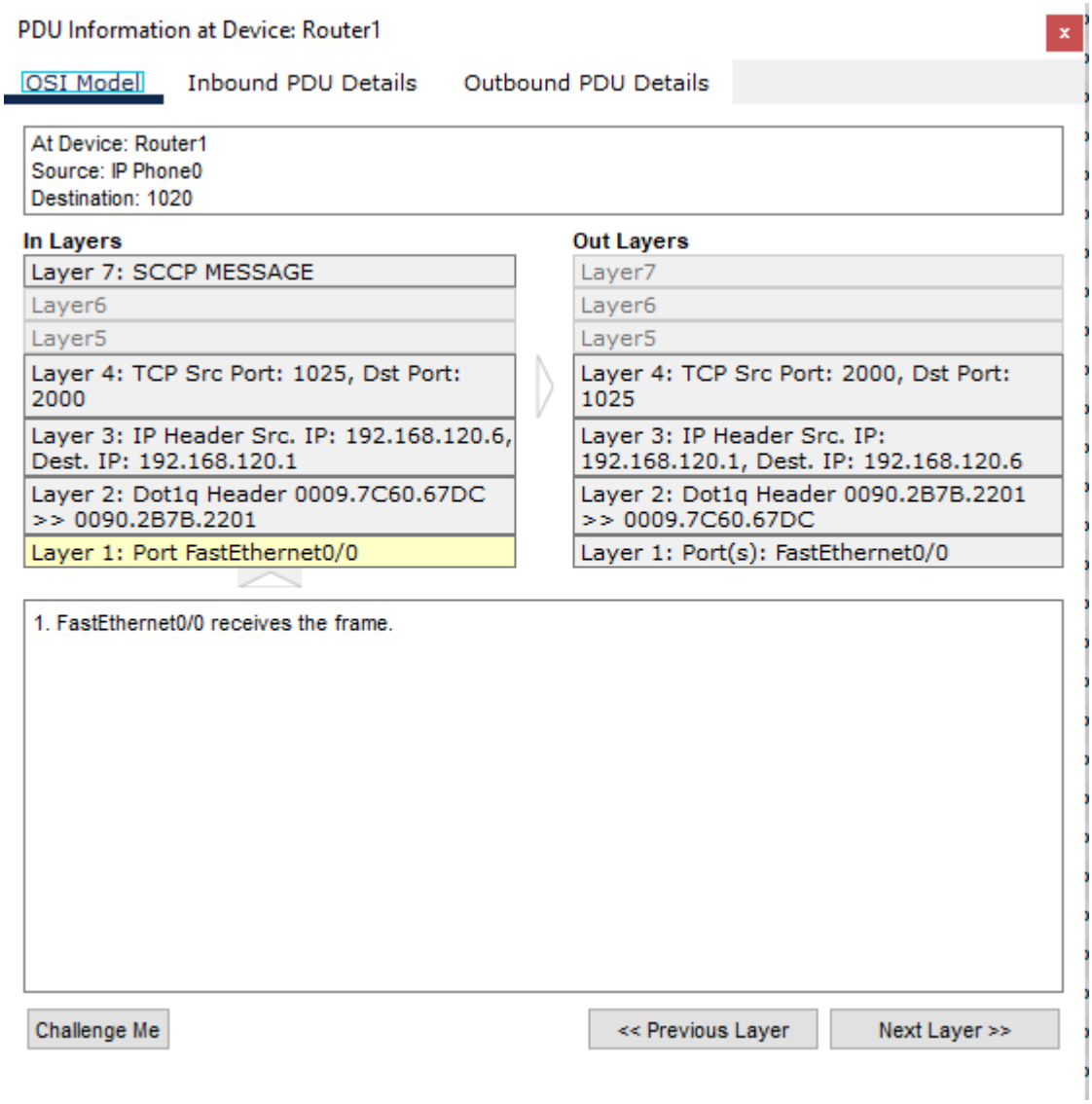

Figure 3.3.3: OSI Model

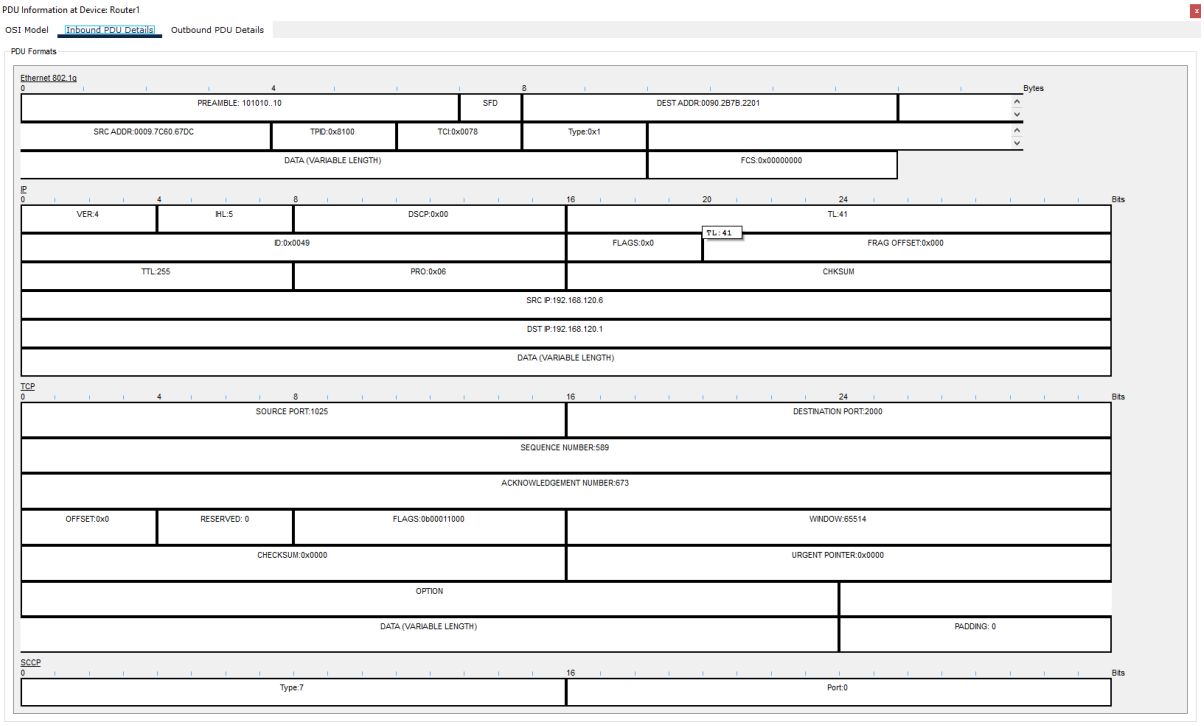

Figure 3.3.4: PDU Details

Relevant Events List

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	IP Phone0	SCCP
	0.001	IP Phone0	Switch0	SCCP
	0.002	Switch0	Router1	SCCP
	0.003	Router1	Switch0	SCCP
	0.004	Switch0	IP Phone0	SCCP
	0.004	--	IP Phone0	SCCP
	0.005	IP Phone0	Switch0	SCCP
	0.006	Switch0	Router1	SCCP
	0.007	Router1	Switch0	SCCP
	0.007	--	Router1	SCCP
	0.008	Router1	Switch0	SCCP
	0.008	Switch0	IP Phone1	SCCP
	0.008	--	IP Phone1	SCCP
	0.009	Switch0	IP Phone0	SCCP
	0.009	IP Phone1	Switch0	SCCP
	0.010	Switch0	Router1	SCCP
	0.011	Router1	Switch0	SCCP
	0.011	--	Router1	SCCP
	0.012	Router1	Switch0	SCCP
	0.012	Switch0	IP Phone0	SCCP
	0.013	Switch0	IP Phone1	SCCP
	0.013	IP Phone0	Switch0	SCCP
	0.013	--	IP Phone1	SCCP
	0.013	--	IP Phone0	SCCP
	0.014	IP Phone1	Switch0	SCCP
	0.014	Switch0	Router1	SCCP
	0.014	IP Phone0	Switch0	SCCP
	0.014	--	IP Phone1	SCCP
	0.015	IP Phone1	Switch0	SCCP
	0.015	Switch0	Router1	SCCP
	0.015	Router1	Switch0	SCCP
	0.015	--	Switch0	SCCP
	0.016	Switch0	Router1	SCCP
	0.016	Router1	Switch0	SCCP
	0.016	Switch0	IP Phone1	SCCP
	0.016	--	Switch0	SCCP
	0.017	Switch0	Router1	SCCP
	0.017	Router1	Switch0	SCCP
	0.017	Switch0	IP Phone0	SCCP
	0.017	--	Router1	SCCP

Figure 3.3.5: Connected IP phones event list

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.008	Router1	Switch0	SCCP
	0.008	Switch0	IP Phone1	SCCP
	0.008	--	IP Phone1	SCCP
	0.009	Switch0	IP Phone0	SCCP
	0.009	IP Phone1	Switch0	SCCP
	0.010	Switch0	Router1	SCCP
	0.011	Router1	Switch0	SCCP
	0.011	--	Router1	SCCP
	0.012	Router1	Switch0	SCCP
	0.012	Switch0	IP Phone0	SCCP
	0.013	Switch0	IP Phone1	SCCP
	0.013	IP Phone0	Switch0	SCCP
	0.013	--	IP Phone1	SCCP
	0.013	--	IP Phone0	SCCP
	0.014	IP Phone1	Switch0	SCCP
	0.014	Switch0	Router1	SCCP
	0.014	IP Phone0	Switch0	SCCP
	0.014	--	IP Phone1	SCCP
	0.015	IP Phone1	Switch0	SCCP
	0.015	Switch0	Router1	SCCP
	0.015	Router1	Switch0	SCCP
	0.015	--	Switch0	SCCP
	0.016	Switch0	Router1	SCCP
	0.016	Router1	Switch0	SCCP
	0.016	Switch0	IP Phone1	SCCP
	0.016	--	Switch0	SCCP
	0.017	Switch0	Router1	SCCP
	0.017	Router1	Switch0	SCCP
	0.017	Switch0	IP Phone0	SCCP
	0.017	--	Router1	SCCP
	0.018	Router1	Switch0	SCCP
	0.018	Switch0	IP Phone1	SCCP
	0.018	--	Router1	SCCP
	0.019	Router1	Switch0	SCCP
	0.019	Switch0	IP Phone0	SCCP
	0.019	--	Router1	SCCP
	0.020	Router1	Switch0	SCCP
	0.020	Switch0	IP Phone0	SCCP
	0.021	Switch0	IP Phone1	SCCP

Figure 3.3.6: Connected IP phones event list

3.1.4. Sending emails to another branch

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

Network Functionality

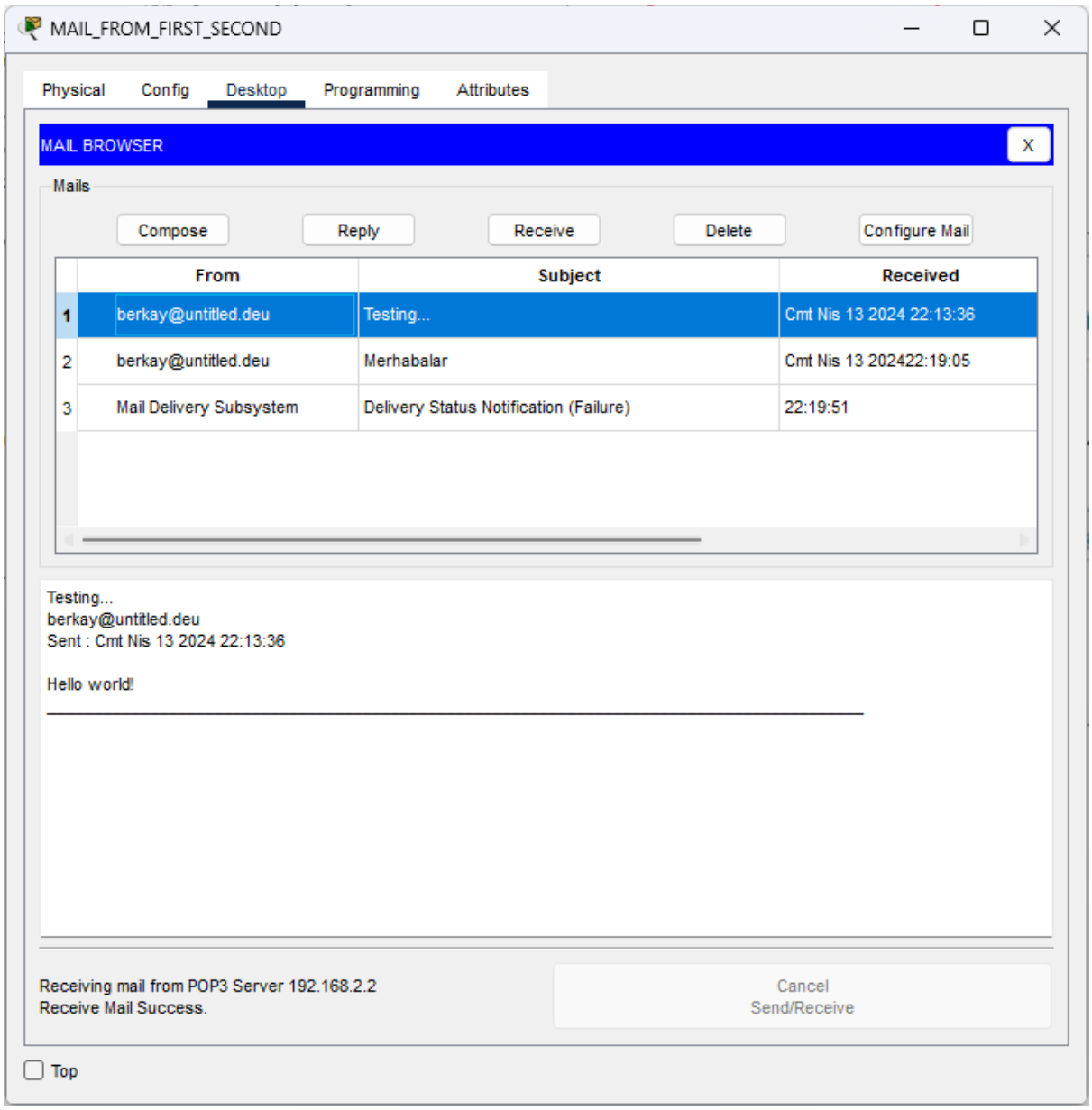

Figure 3.4.1: The received email from the second facility of the first branch

Protocol Data Units Content

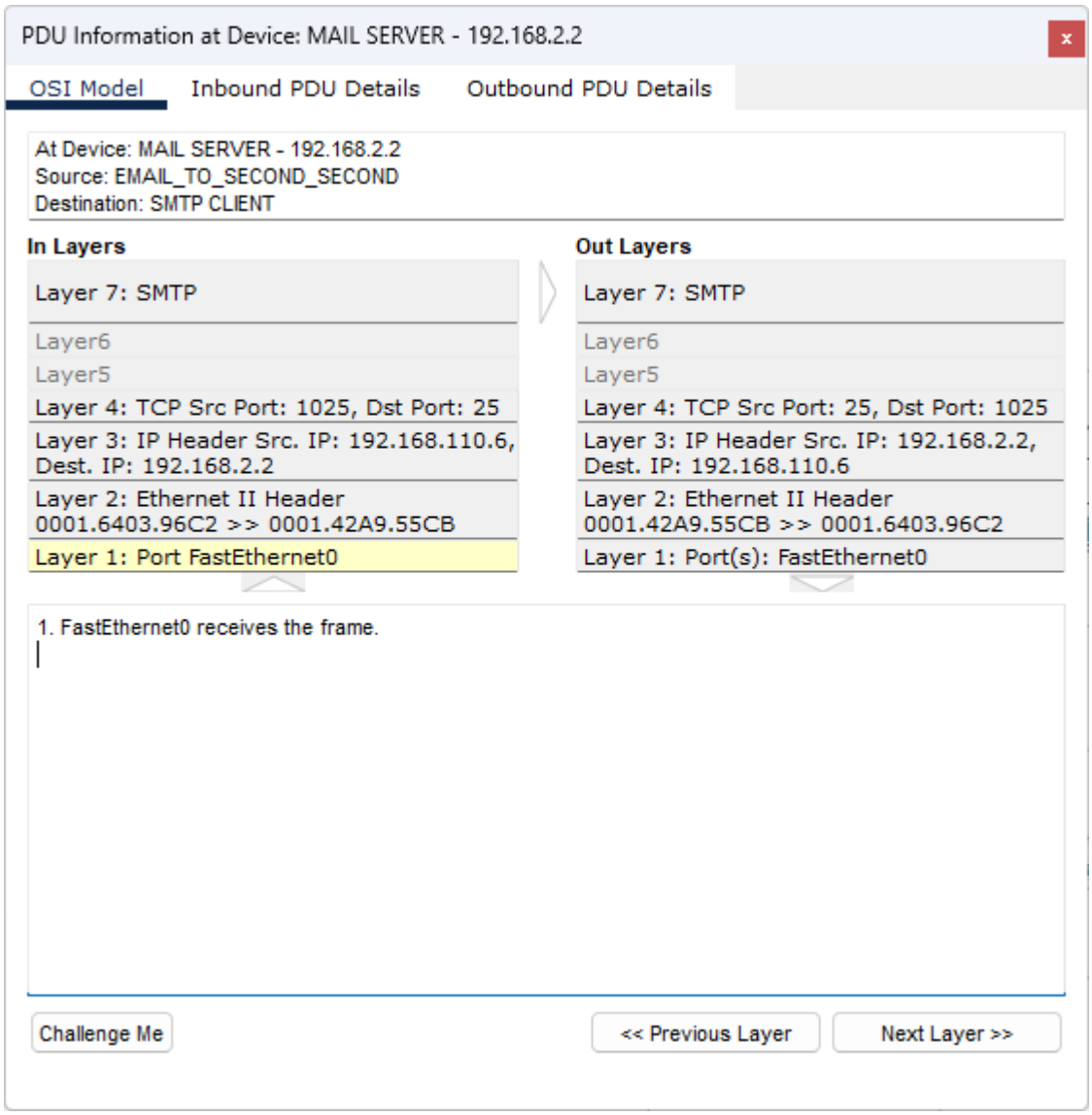

Figure 3.4.2: The PDU overview of the outgoing packet

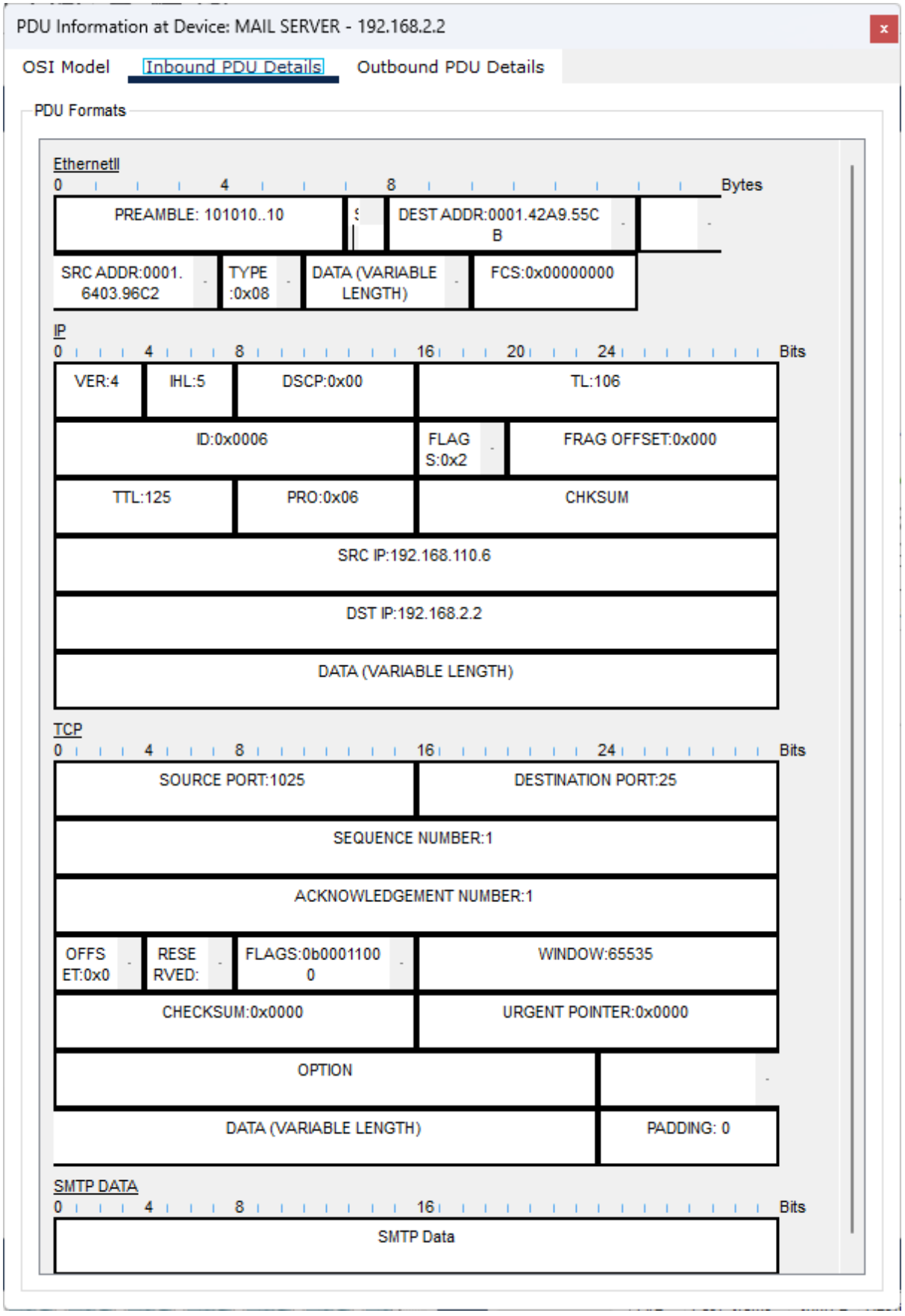

Figure 3.4.3: The PDU content of the outgoing packet

Relevant Events List

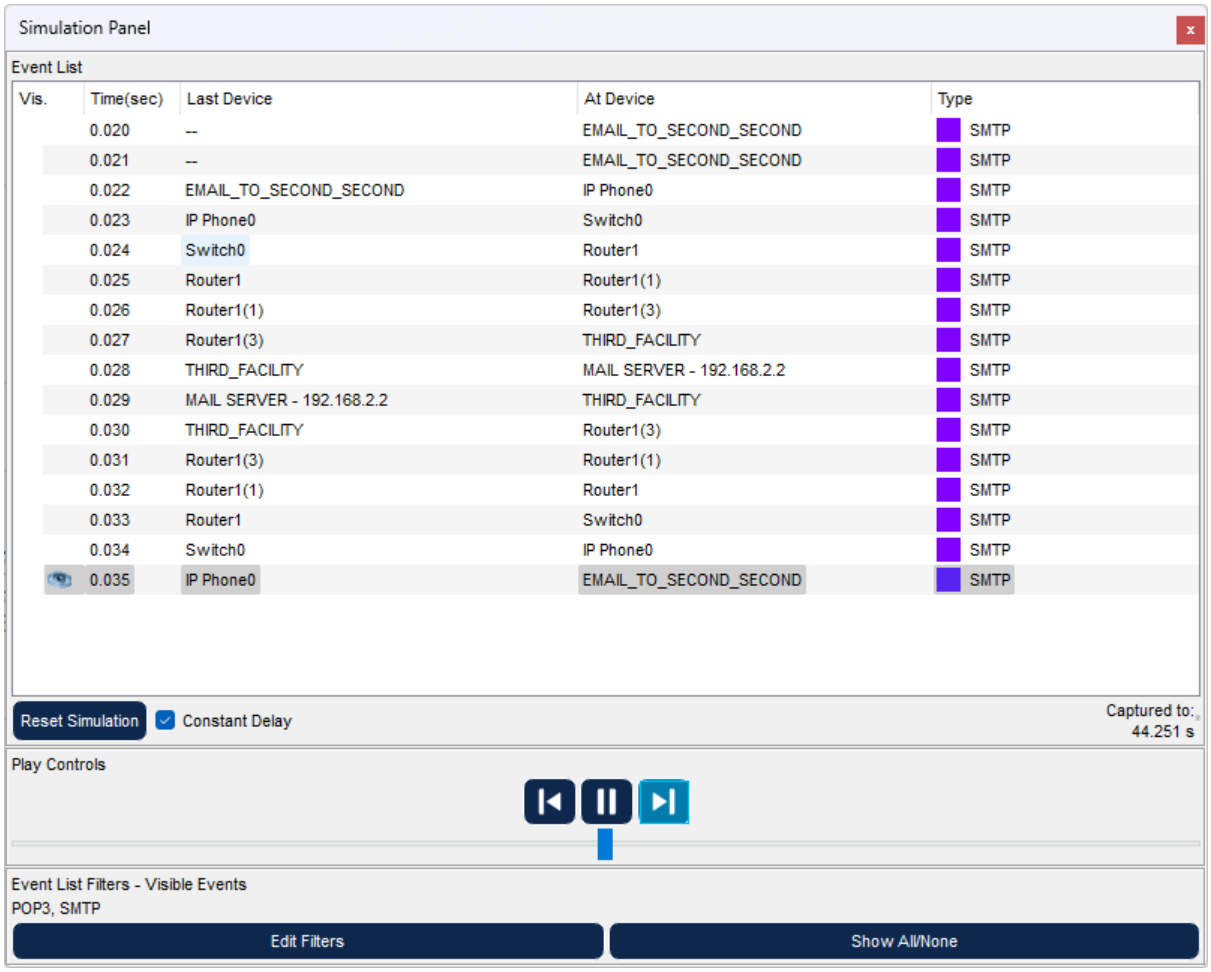

Figure 3.4.4: The relevant PDU content of sending email

3.1.5. Pinging the web server of the other branch

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

Network Functionality

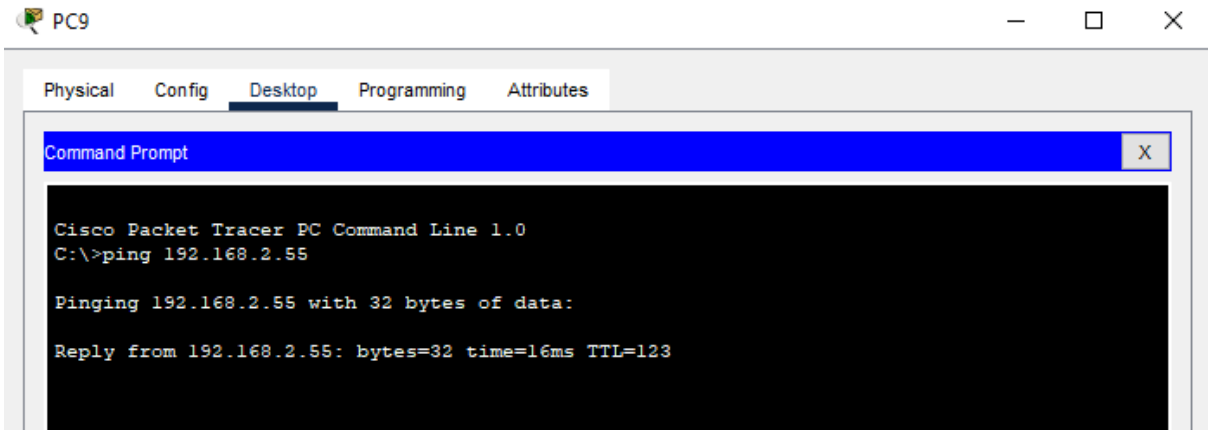

Figure 3.5.1: Pinging web server from cmd prompt

Protocol Data Units Content

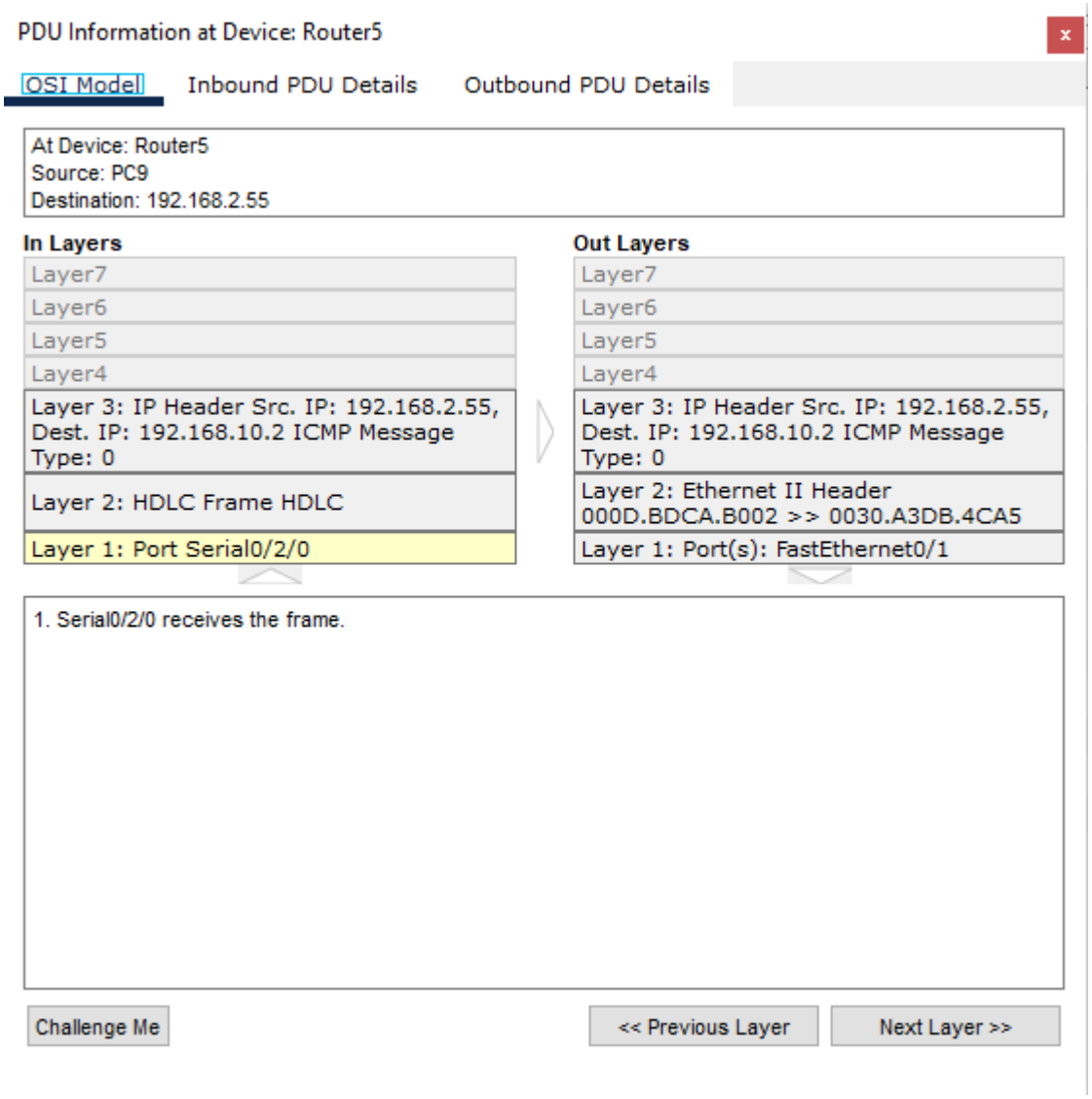

Figure 3.5.2: OSI Model

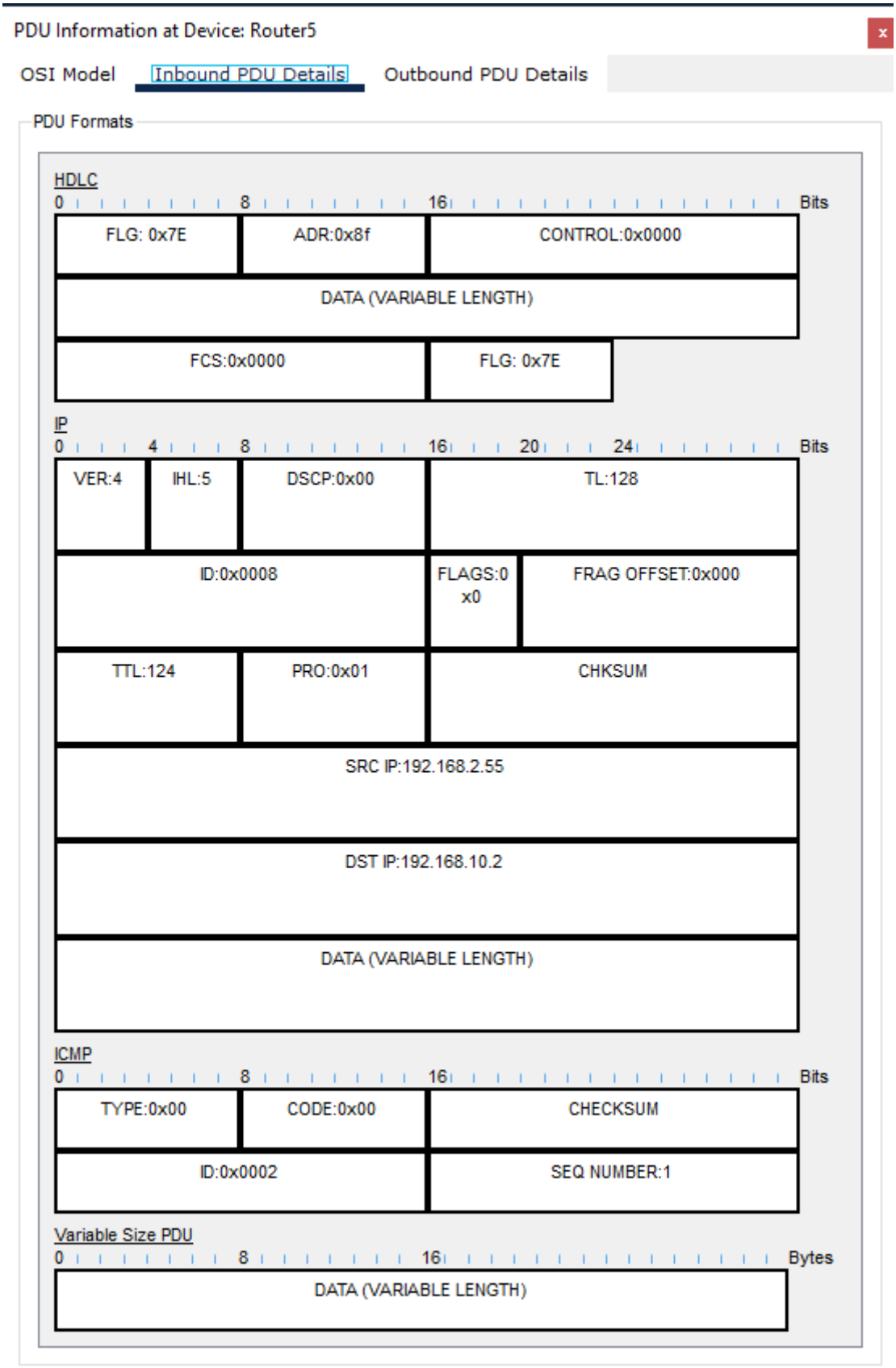

Figure 3.5.3: Inbound PDU model

Relevant Events List

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC9	ICMP
	0.001	PC9	Facility0_Switch	ICMP
	0.002	Facility0_Switch	Router5	ICMP
	0.003	Router5	Router4	ICMP
	0.004	Router4	ISP_Router	ICMP
	0.005	ISP_Router	Router1(1)	ICMP
	0.006	Router1(1)	Router1(3)	ICMP
	0.007	Router1(3)	THIRD_FACILITY	ICMP
	0.008	THIRD_FACILITY	192.168.2.55 - WEB_SERVER6	ICMP
	0.009	192.168.2.55 - WEB_SERVER6	THIRD_FACILITY	ICMP
	0.010	THIRD_FACILITY	Router1(3)	ICMP
	0.011	Router1(3)	Router1(1)	ICMP
	0.012	Router1(1)	ISP_Router	ICMP
	0.013	ISP_Router	Router4	ICMP
	0.014	Router4	Router5	ICMP
	0.015	Router5	Facility0_Switch	ICMP
	0.016	Facility0_Switch	PC9	ICMP
	1.019	--	PC9	ICMP

Figure 3.5.4: Event List

3.1.6. Sending emails to another branch on a laptop

A laptop user from first facility of first branch office wants to send email to her friend in the first facility of the second branch office.

Network Functionality

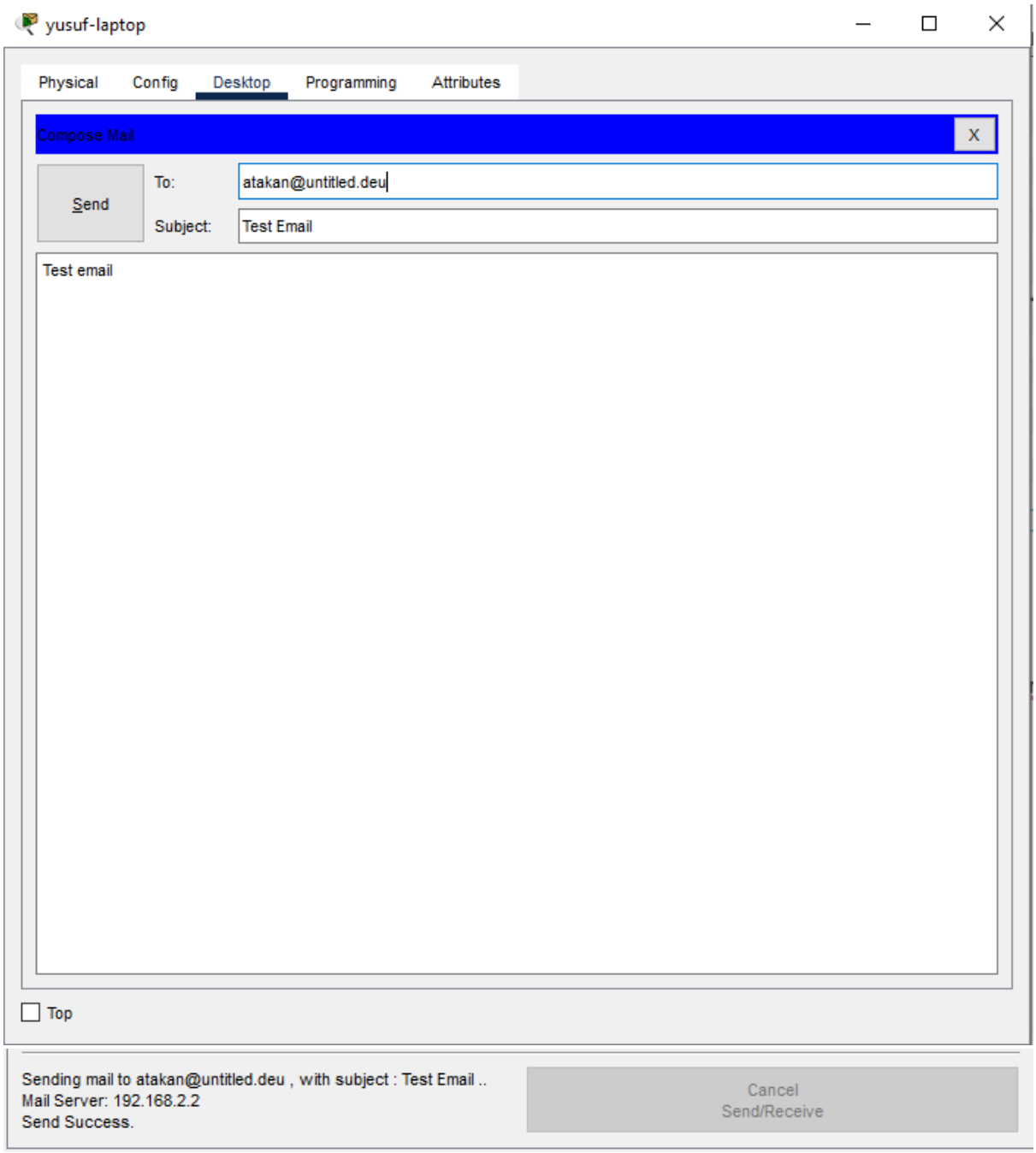

Figure 3.6.1: Sending Email

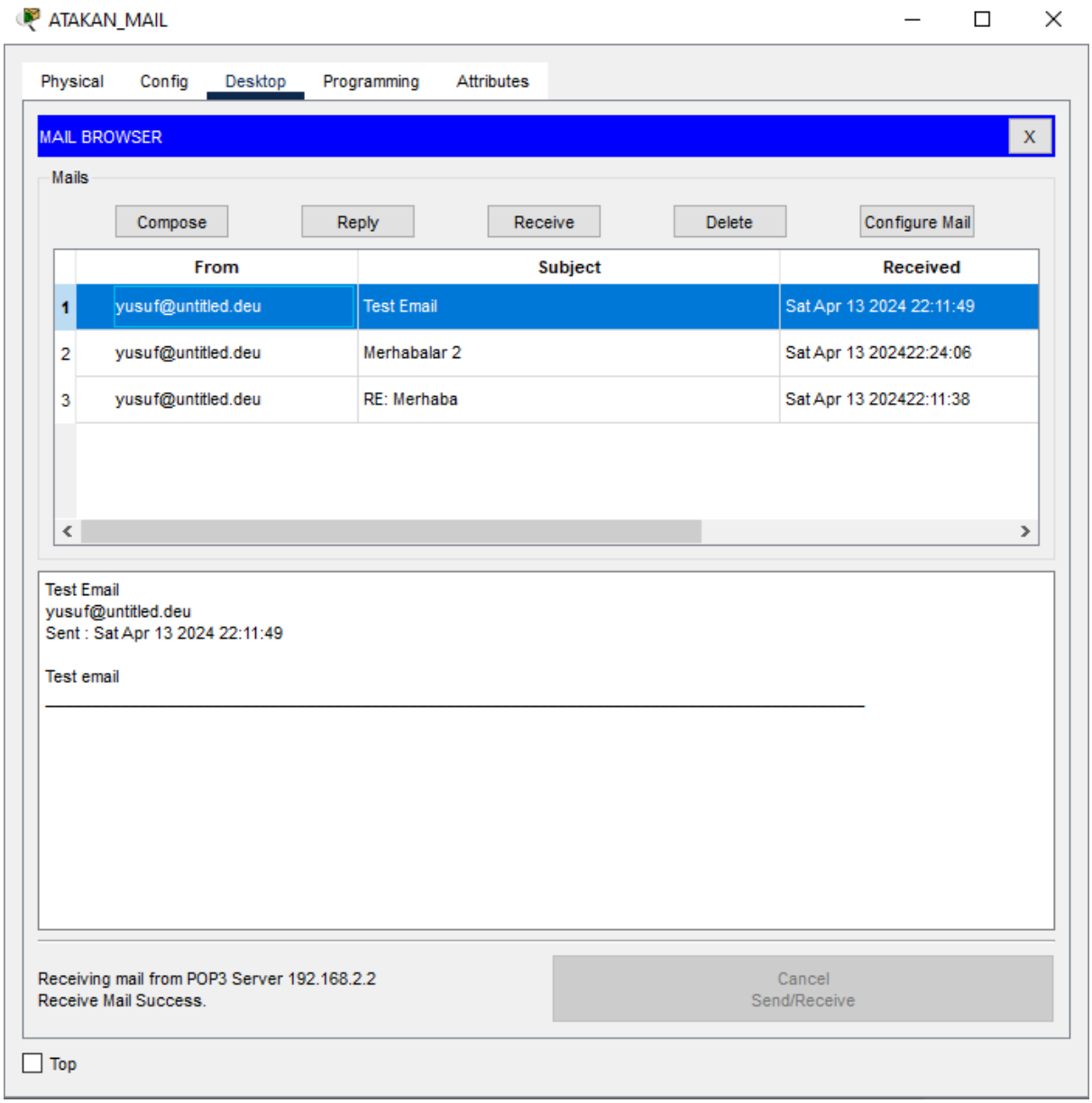

Figure 3.6.2: Receiving mail

Protocol Data Units Content

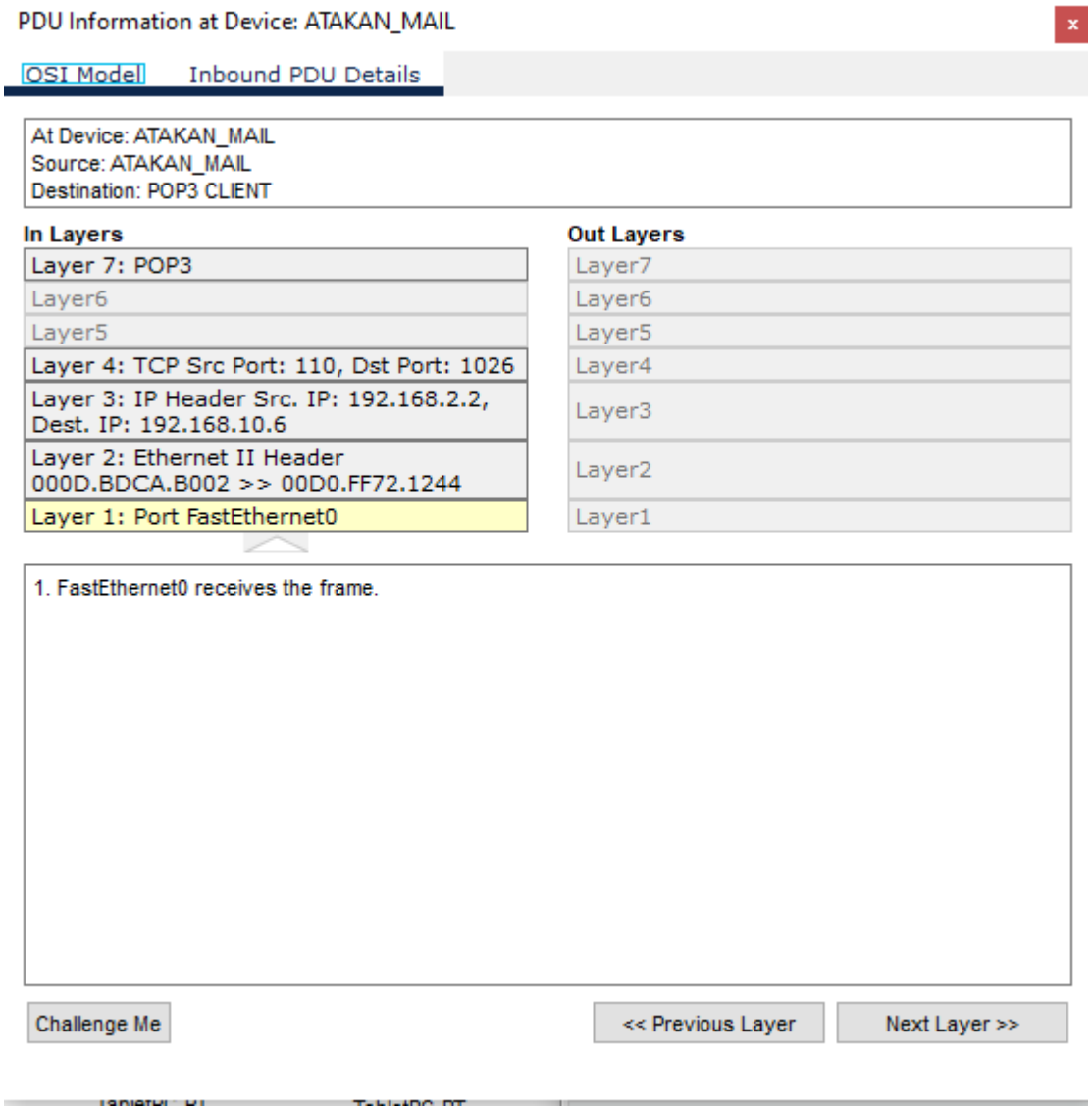

Figure 3.6.3: OSI Model

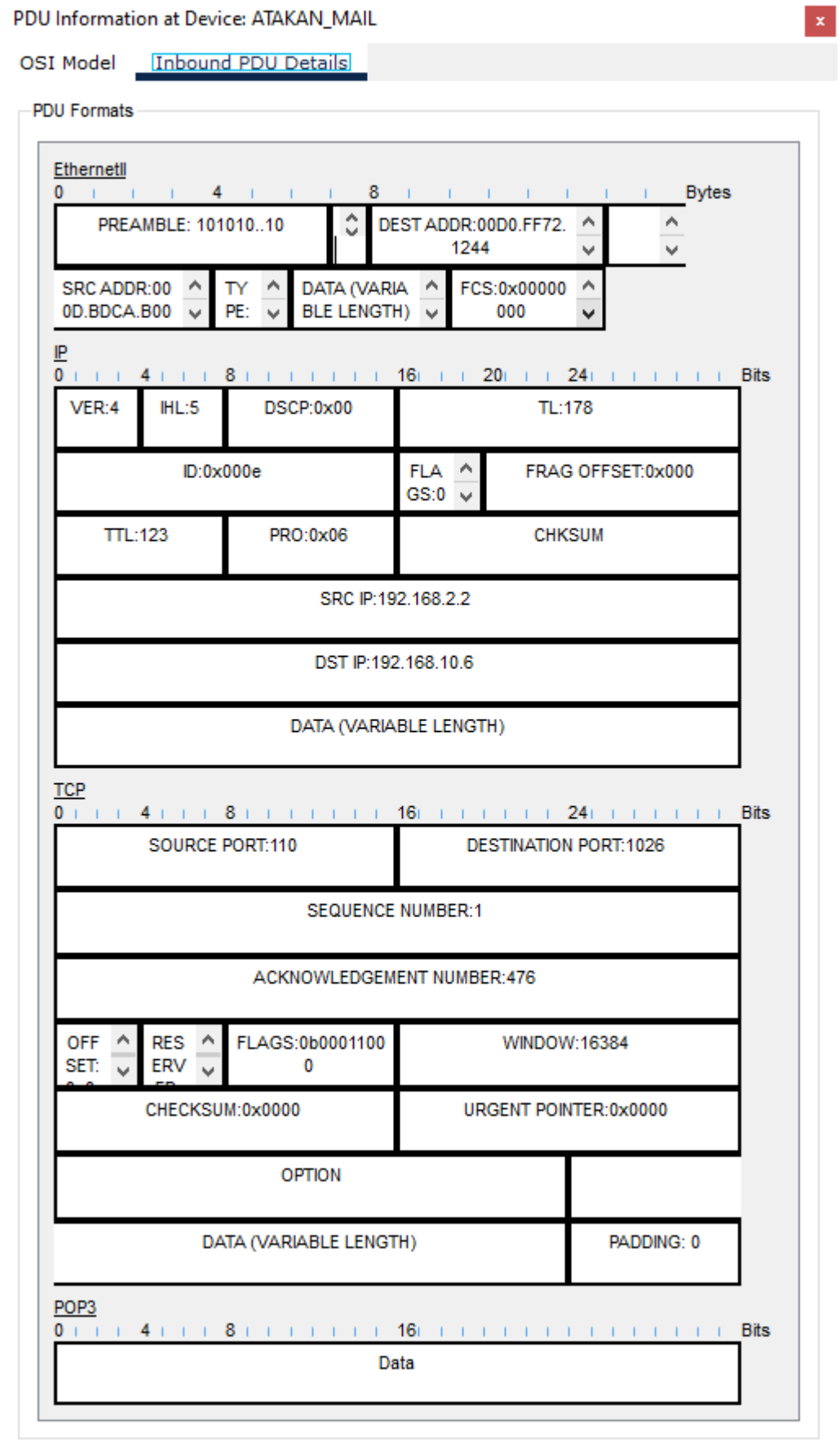

Figure 3.6.4: PDU Details

Relevant Events List

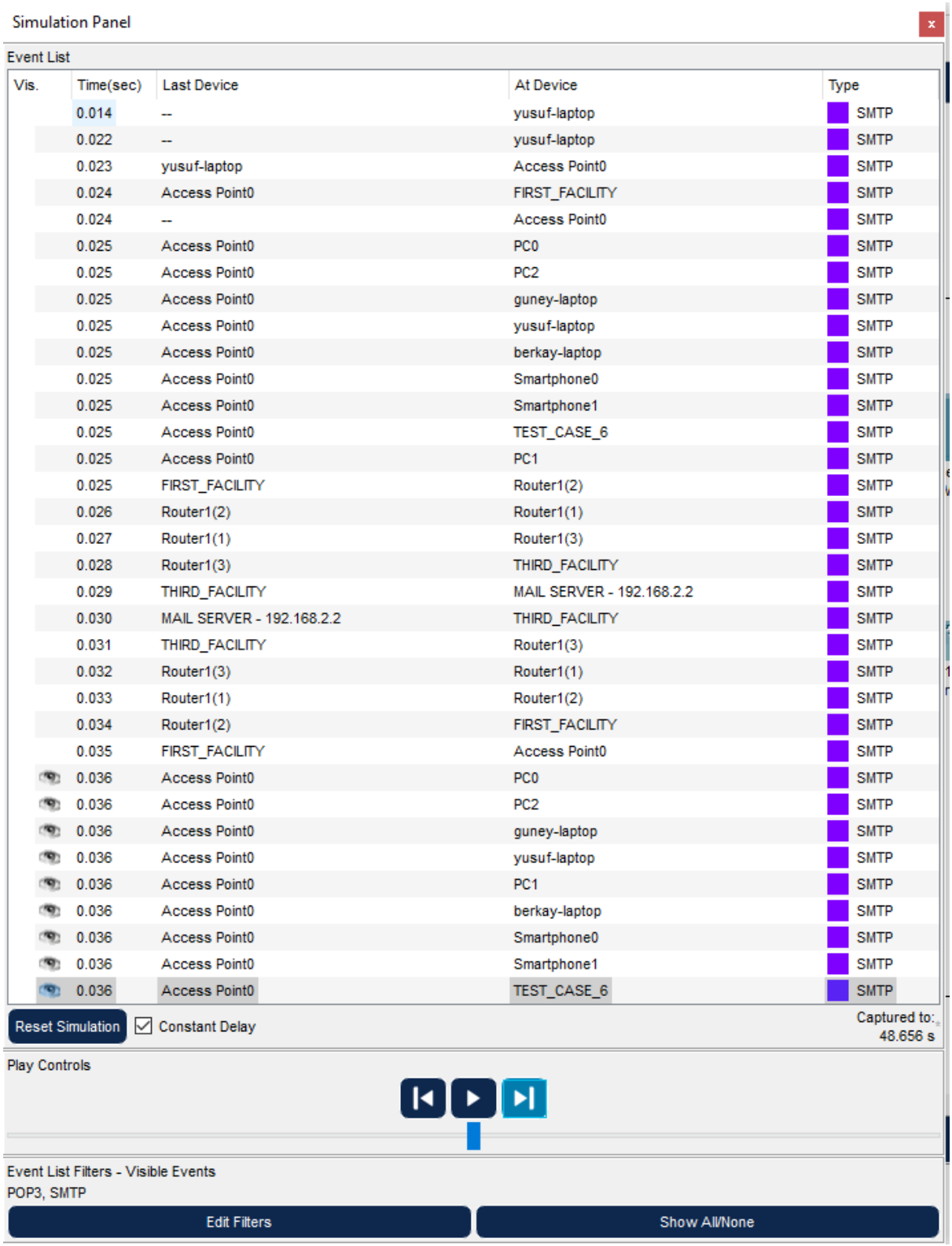

Figure 3.6.1: Sending Email Event List

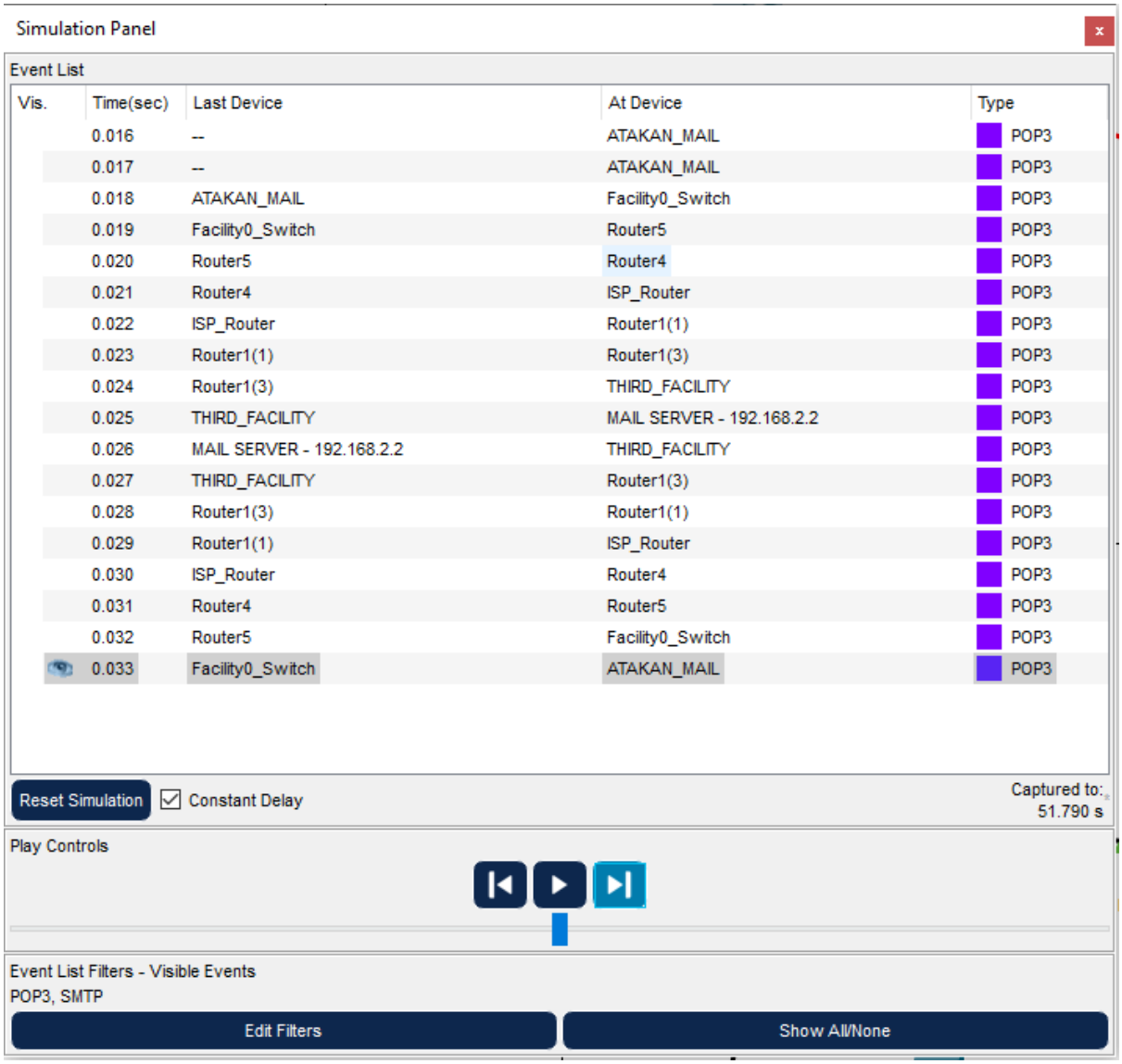

Figure 3.6.2: Sending Email Event List

3.1.7. Web server connection via SSH

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

Network Functionality

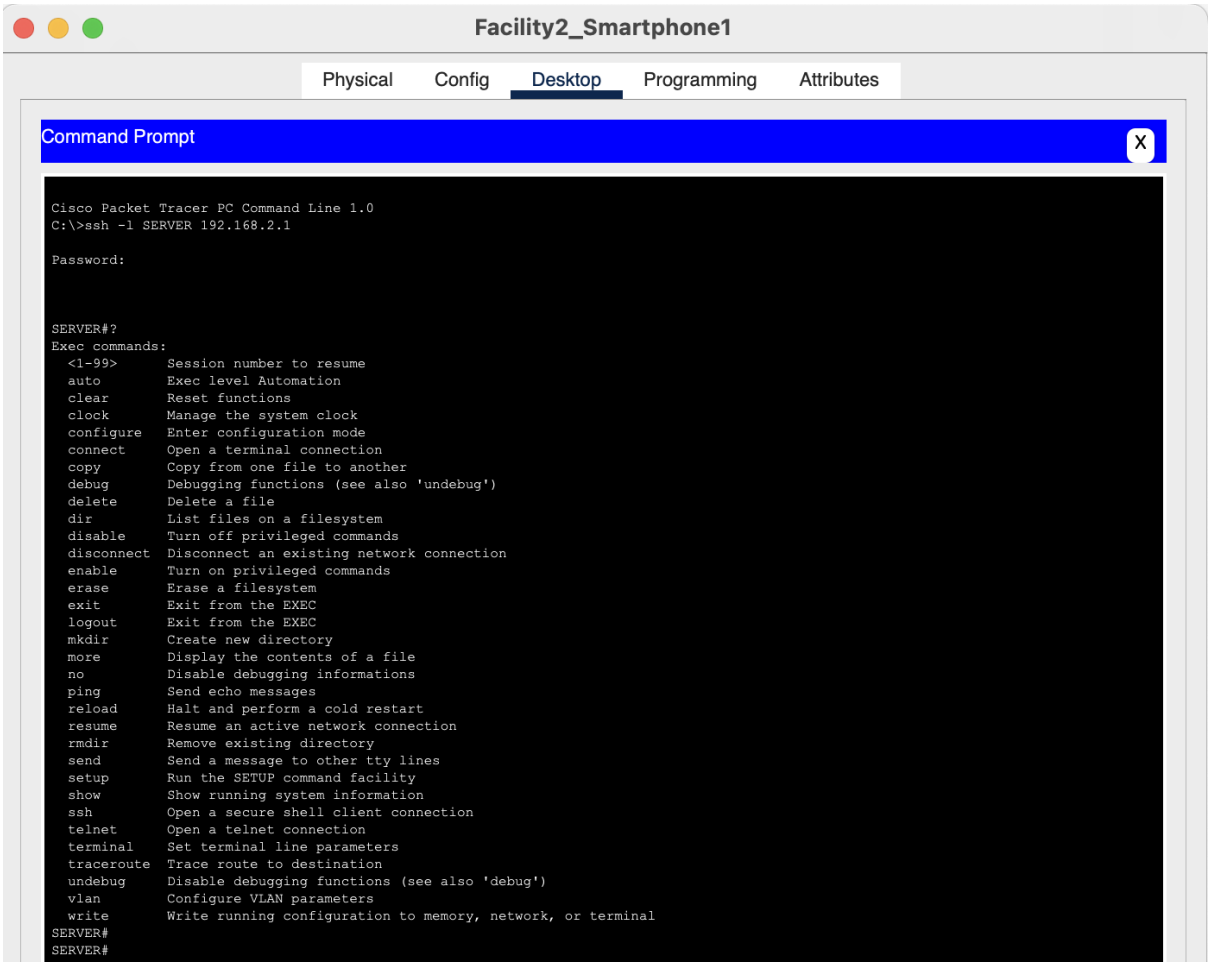

Figure 3.7.1: The network functionality of “ssh”

Protocol Data Units Content

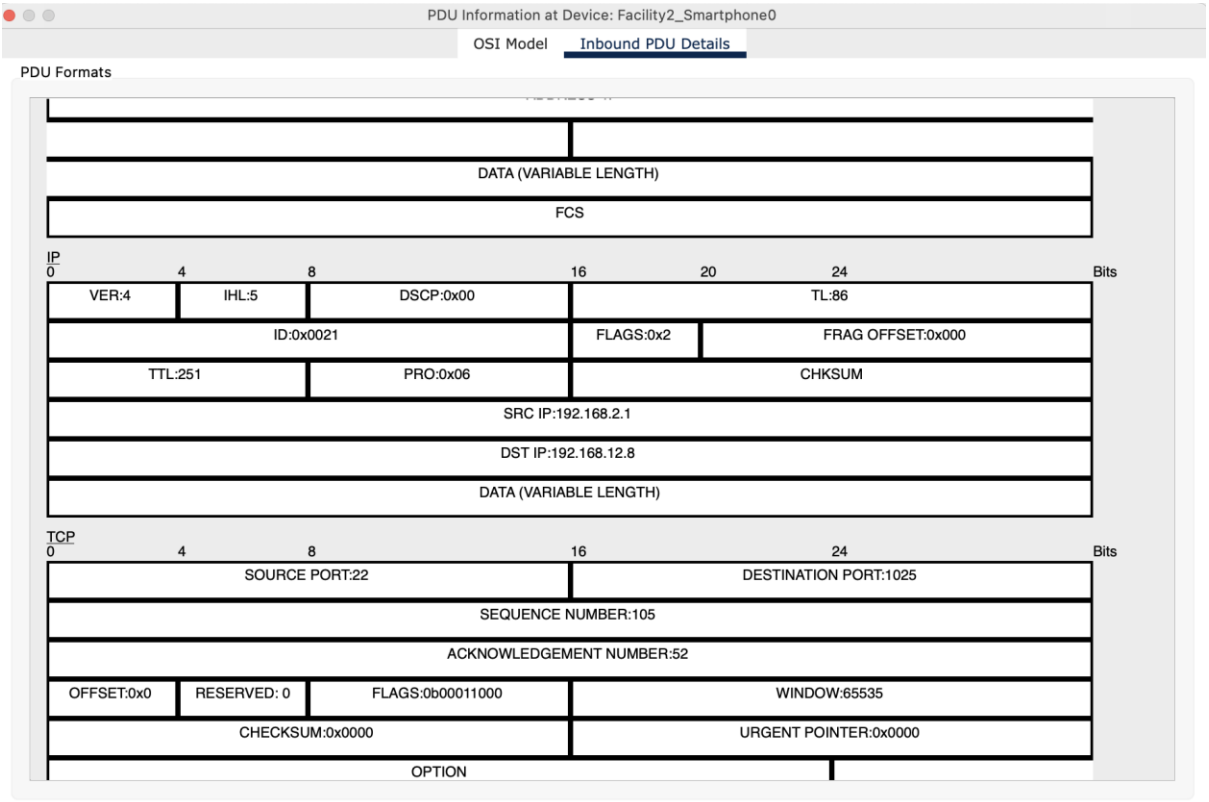

Figure 3.7.2: The received PDU content after SSH connection

Relevant Events List

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.026	--	Router1(3)	SSH
	0.027	Router1(3)	Router1(1)	SSH
	0.028	Router1(1)	ISP_Router	SSH
	0.029	ISP_Router	Router4	SSH
	0.030	Router4	Router5(2)	SSH
	0.031	Router5(2)	Facility2_Switch	SSH
	0.032	Facility2_Switch	Facility2_AccessPoint	SSH
	0.033	Facility2_AccessPoint	Facility2_Smartphone1	SSH
	0.033	--	Facility2_Smartphone1	SSH
	0.033	Facility2_AccessPoint	Facility2_Smartphone0	SSH
	0.033	--	Facility2_Smartphone1	SSH
	0.035	--	Facility2_Smartphone1	SSH
	0.036	Facility2_Smartphone1	Facility2_AccessPoint	SSH
	0.037	Facility2_AccessPoint	Facility2_Switch	SSH
	0.038	Facility2_Switch	Router5(2)	SSH
	0.039	Router5(2)	Router4	SSH
	0.040	Router4	ISP_Router	SSH
	0.041	ISP_Router	Router1(1)	SSH
	0.041	--	Facility2_AccessPoint	SSH
	0.042	Facility2_AccessPoint	Facility2_Smartphone0	SSH
	0.042	Facility2_AccessPoint	Facility2_Smartphone1	SSH
	0.042	Router1(1)	Router1(3)	SSH
	0.093	--	Facility2_Smartphone1	SSH
	0.097	--	Facility2_Smartphone1	SSH
	0.098	Facility2_Smartphone1	Facility2_AccessPoint	SSH
	0.099	Facility2_AccessPoint	Facility2_Switch	SSH
	0.100	Facility2_Switch	Router5(2)	SSH
	0.100	--	Facility2_AccessPoint	SSH
	0.101	Facility2_AccessPoint	Facility2_Smartphone0	SSH
	0.101	Facility2_AccessPoint	Facility2_Smartphone1	SSH
	0.101	Router5(2)	Router4	SSH
	0.102	Router4	ISP_Router	SSH
	0.103	ISP_Router	Router1(1)	SSH
	0.104	Router1(1)	Router1(3)	SSH
	0.104	--	Router1(3)	SSH
	0.104	--	Router1(3)	SSH
	0.105	Router1(3)	Router1(1)	SSH
	0.105	--	Router1(3)	SSH
	0.106	--	Router1(3)	SSH

Reset Simulation | Constant Delay | Captured to: 46.097 s

Figure 3.7.3: Event list view during the ssh connection

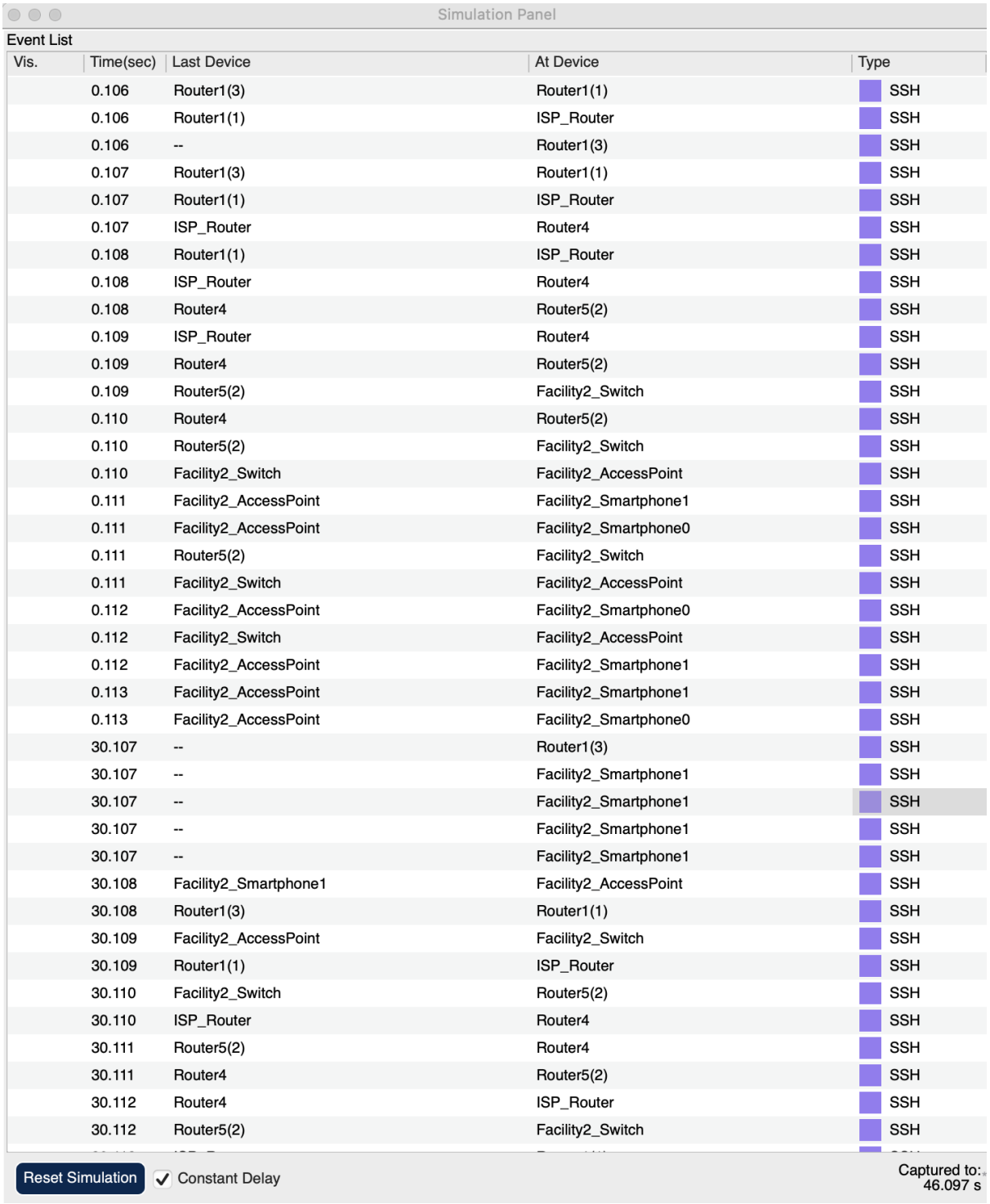

Figure 3.7.4: Event list view during the ssh connection

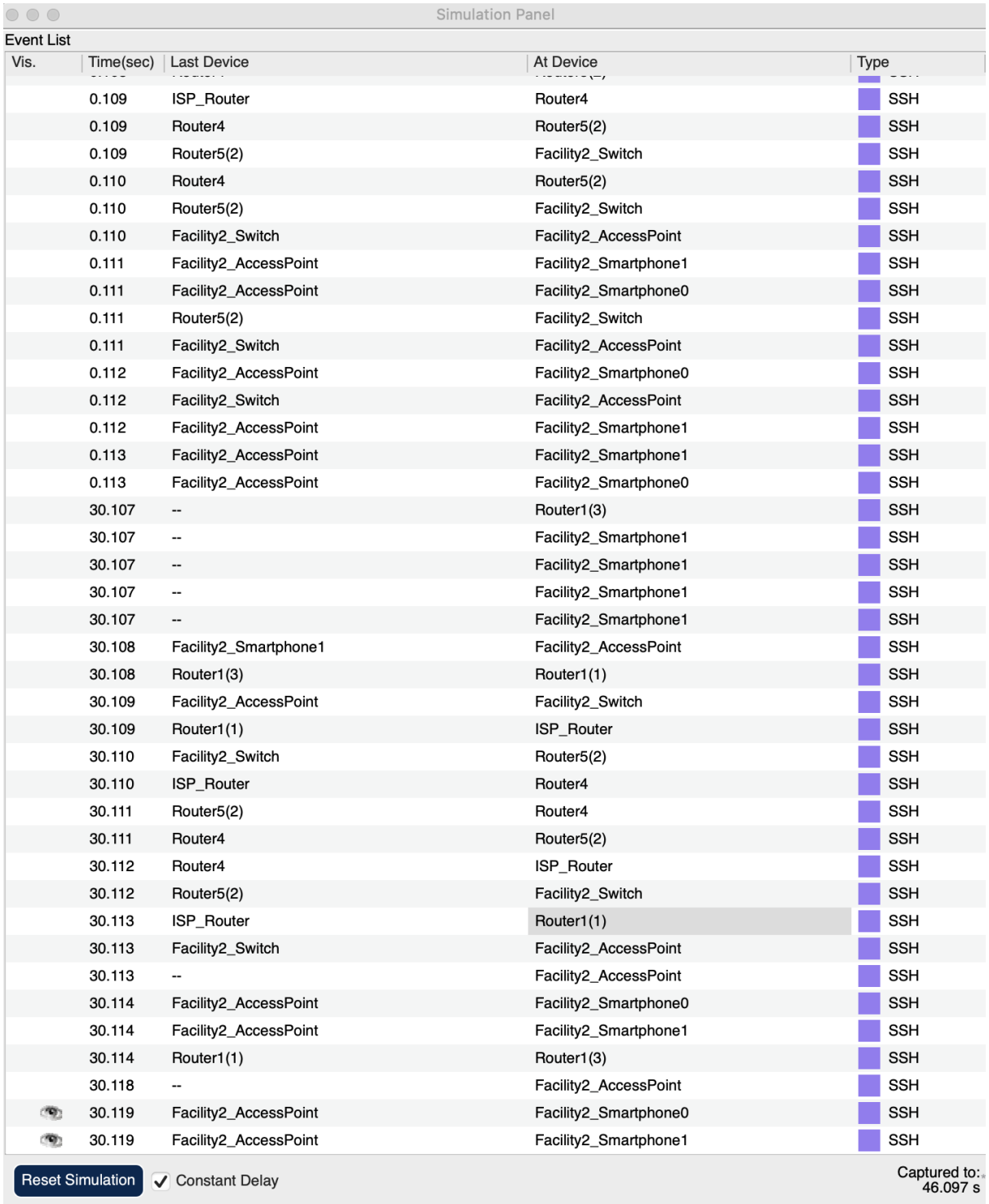

Figure 3.7.5: Event list view during the ssh connection

3.1.8 EXTRA: DNS Resolution

A user from the third facility of the second branch wants to resolve the address of “webserver1” domain.

Network Functionality

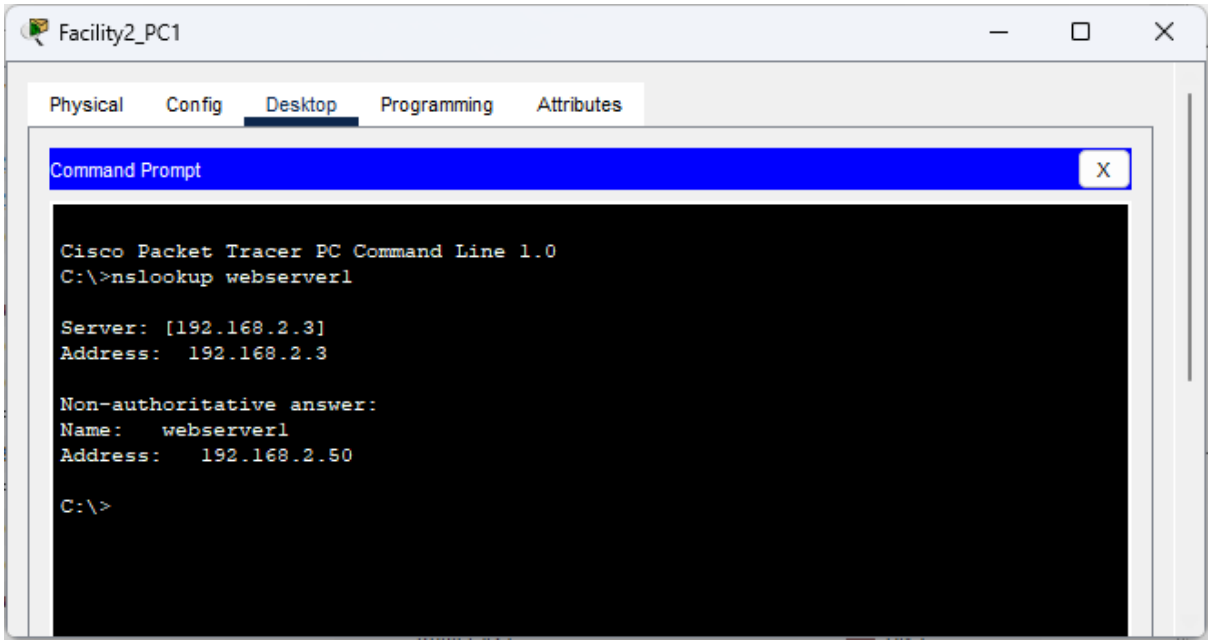

Figure 3.8.1: The network functionality of “nslookup”

Protocol Data Units Content

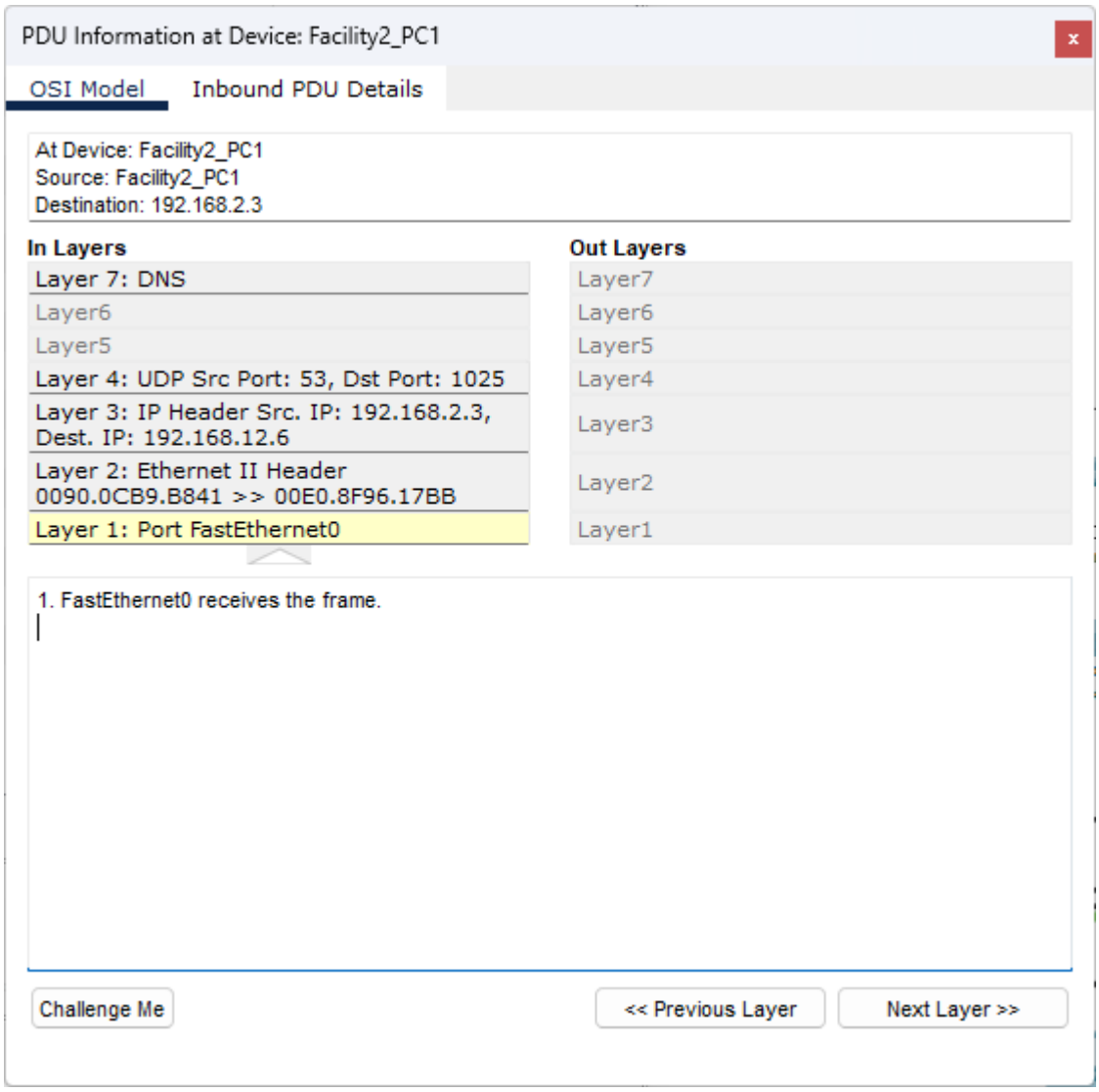

Figure 3.8.2: The overview of PDUs of the DNS lookup

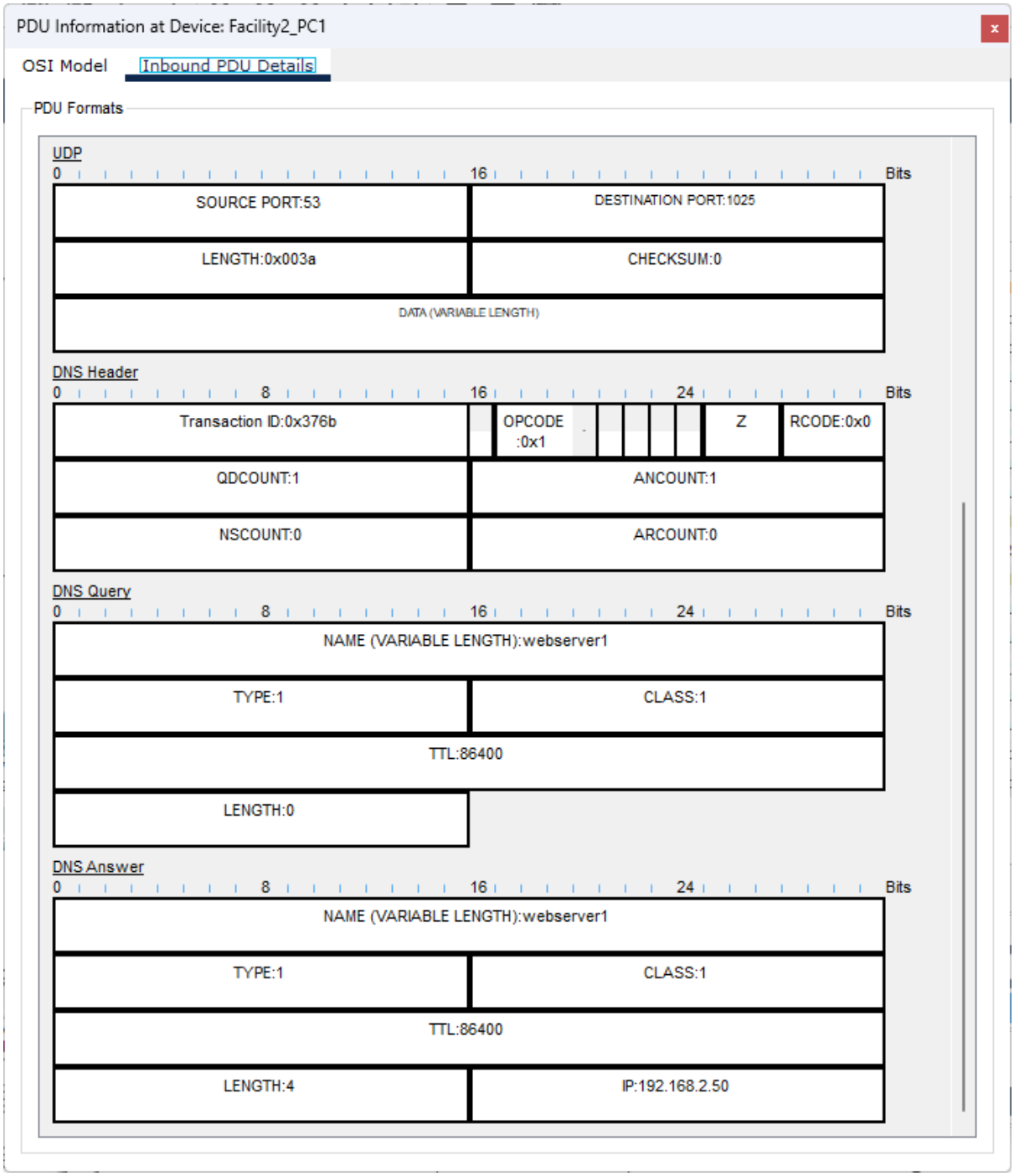

Figure 3.8.3: The received PDU content of the DNS lookup

Relevant Events List

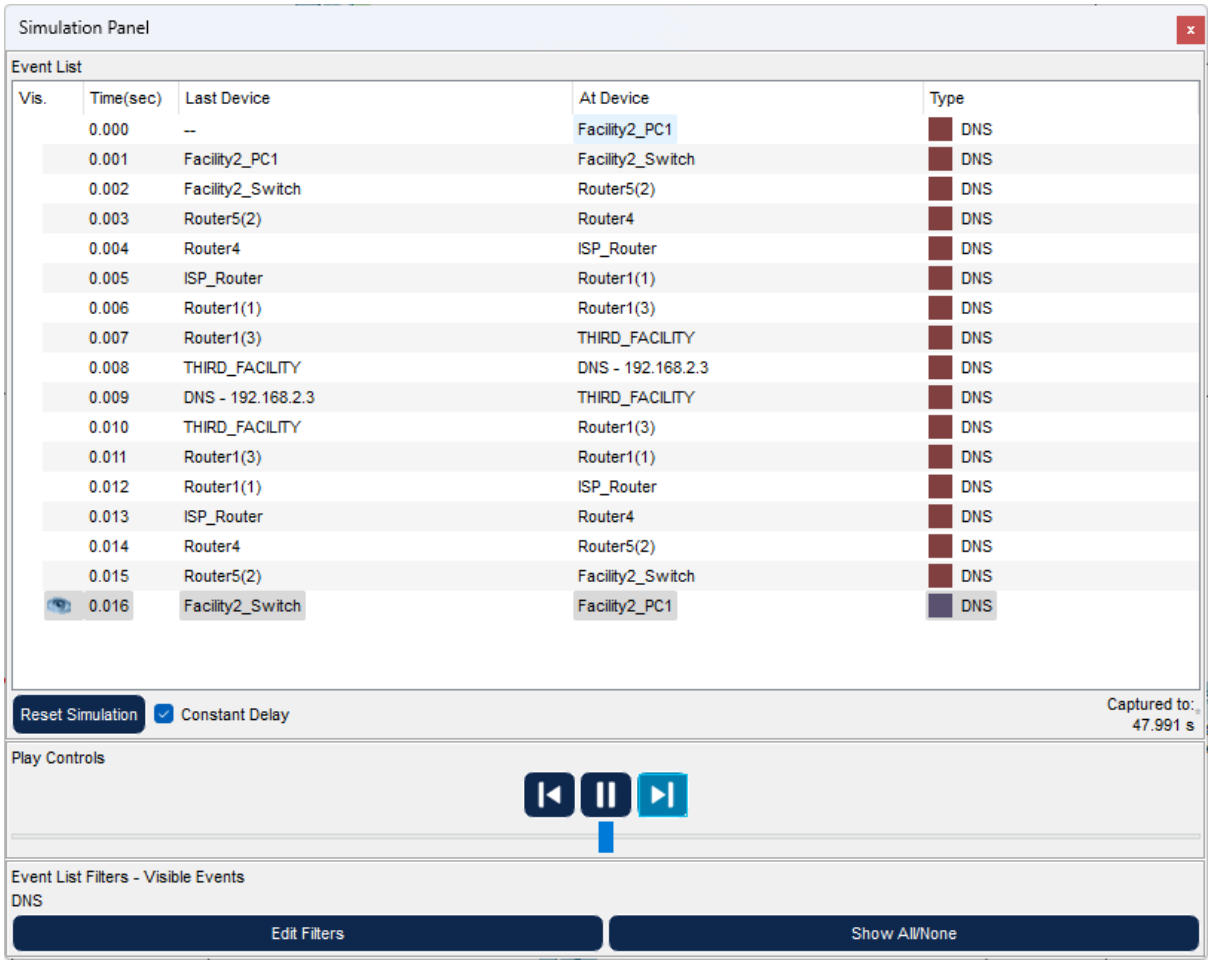

Figure 3.8.4: Receiving email event list

3.1.9 EXTRA: Tracing route to a web server

A user from the second facility of the second branch wants to trace the route from themself to a web server in the third facility of the first branch.

Network Functionality

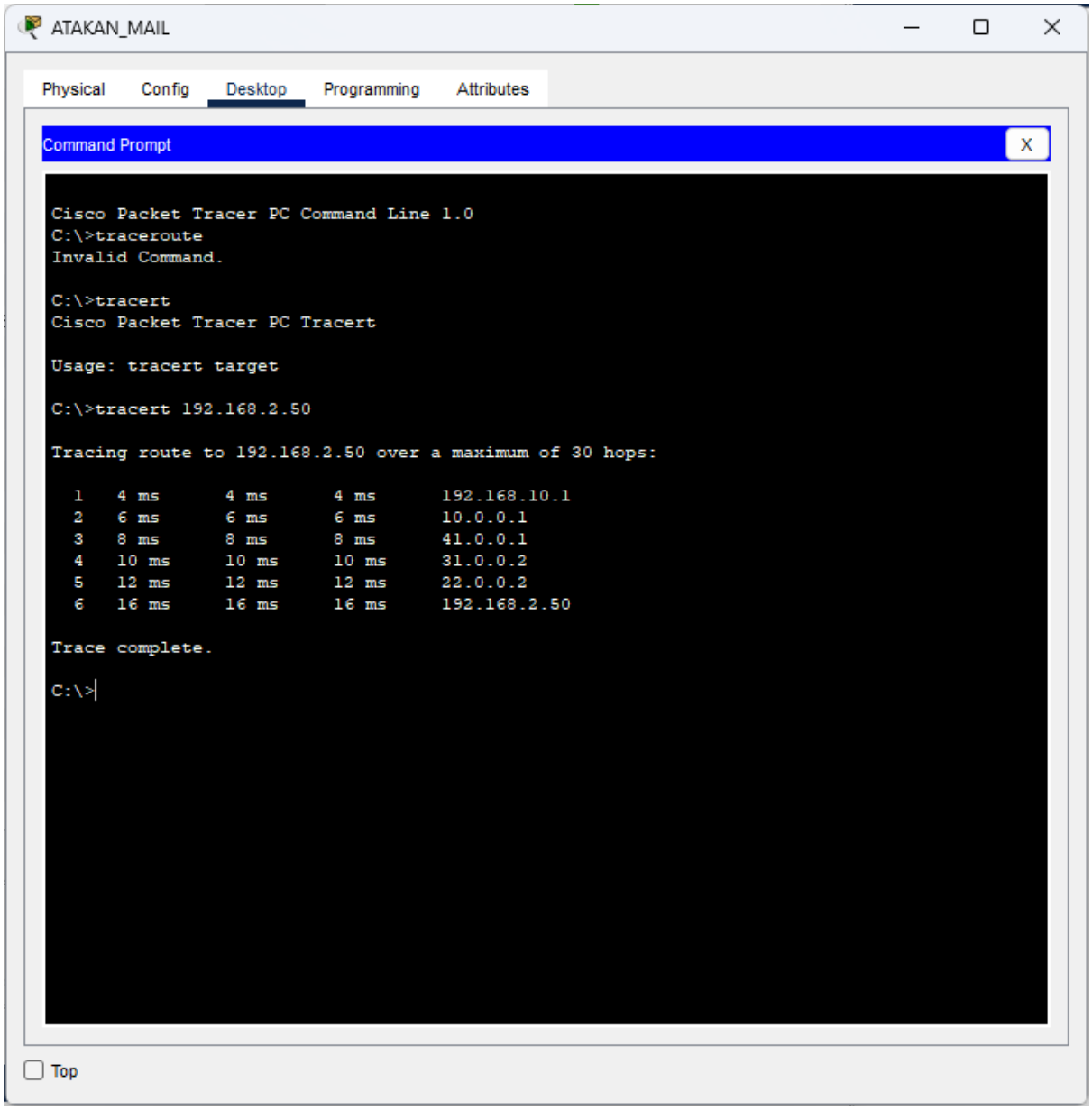

Figure 3.9.1: The network functionality of “tracert”

Protocol Data Units Content

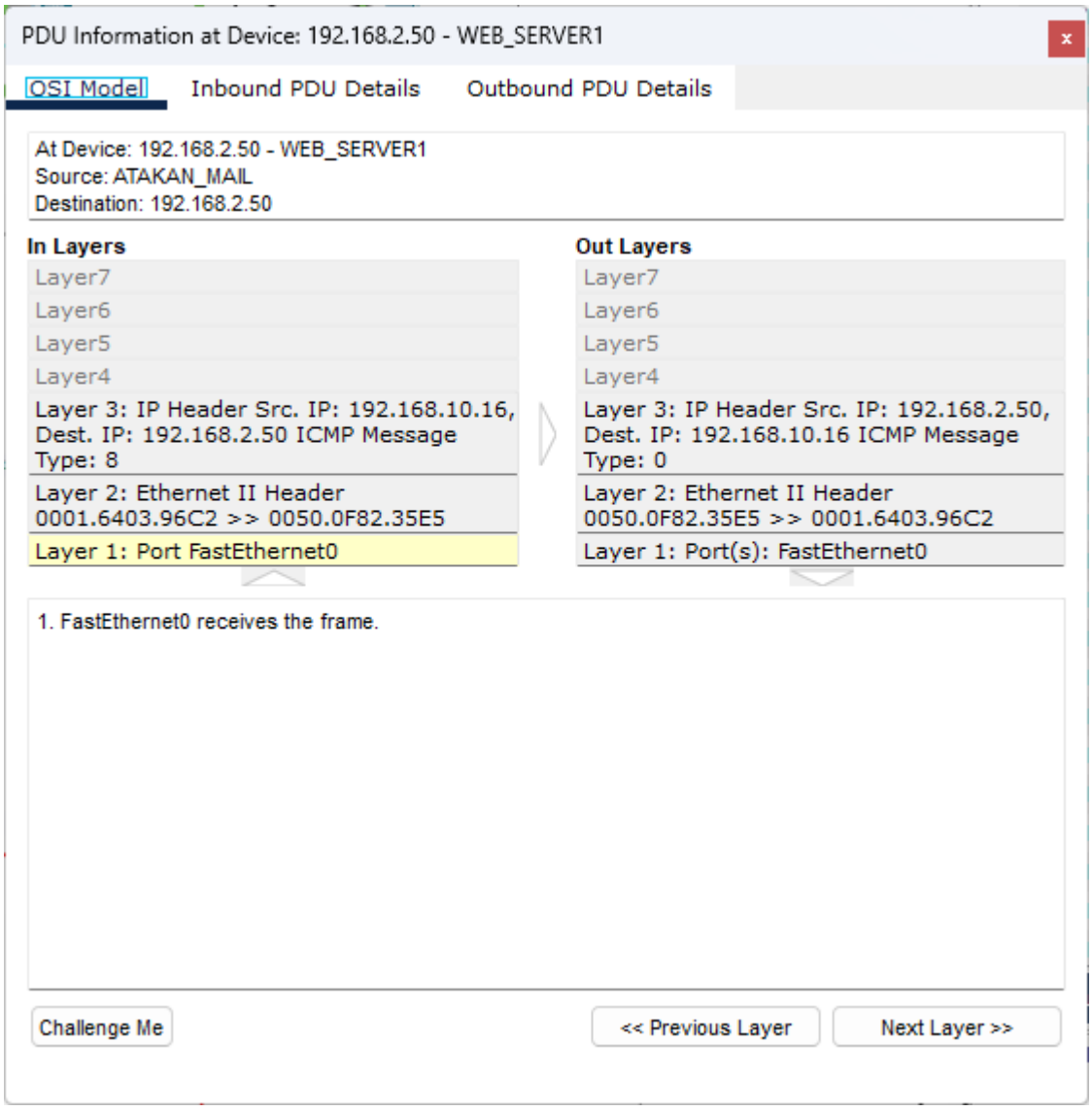

Figure 3.9.2: The PDU overview of “tracert”

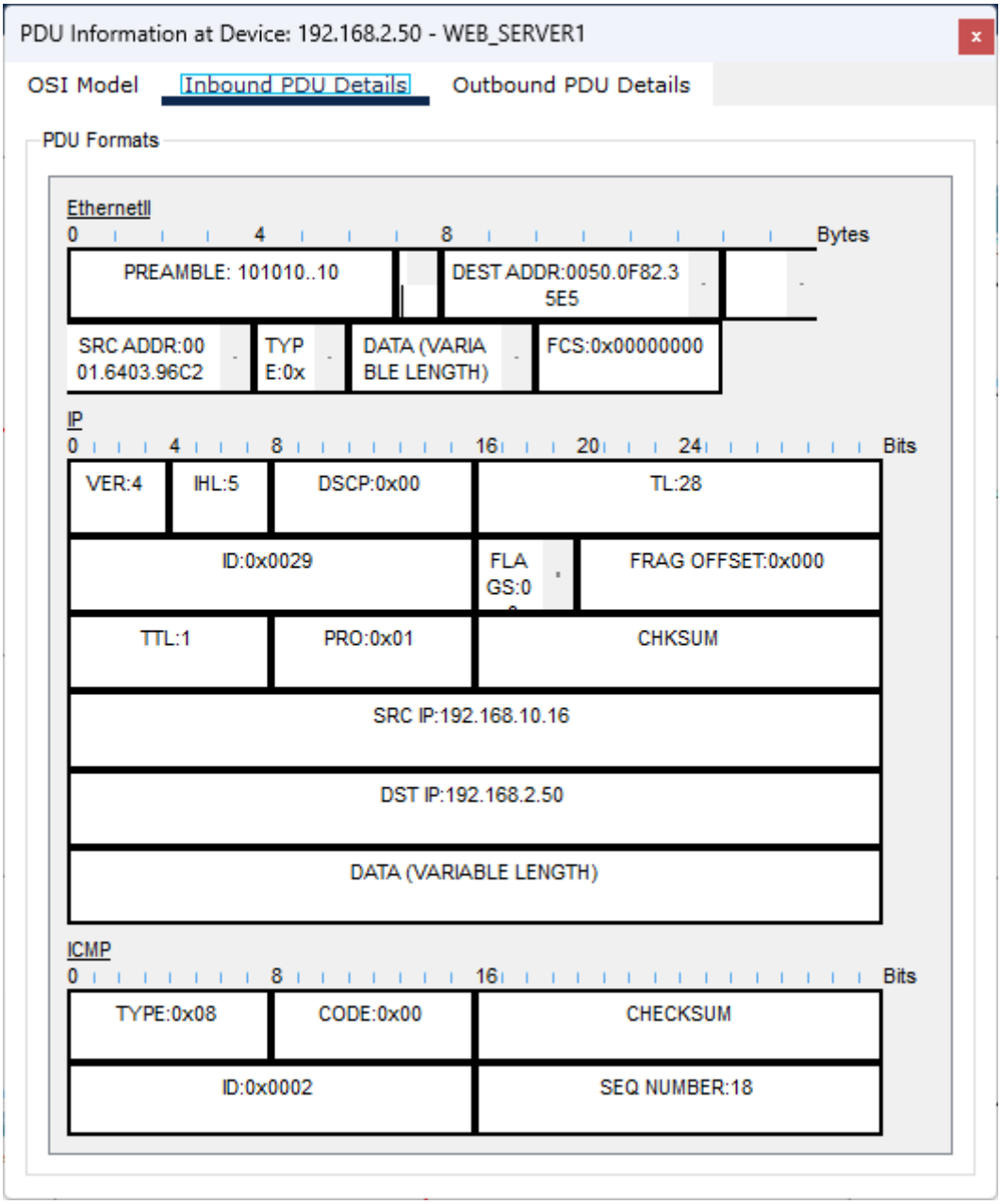

Figure 3.9.3: The actual content of PDUs

Relevant Events List

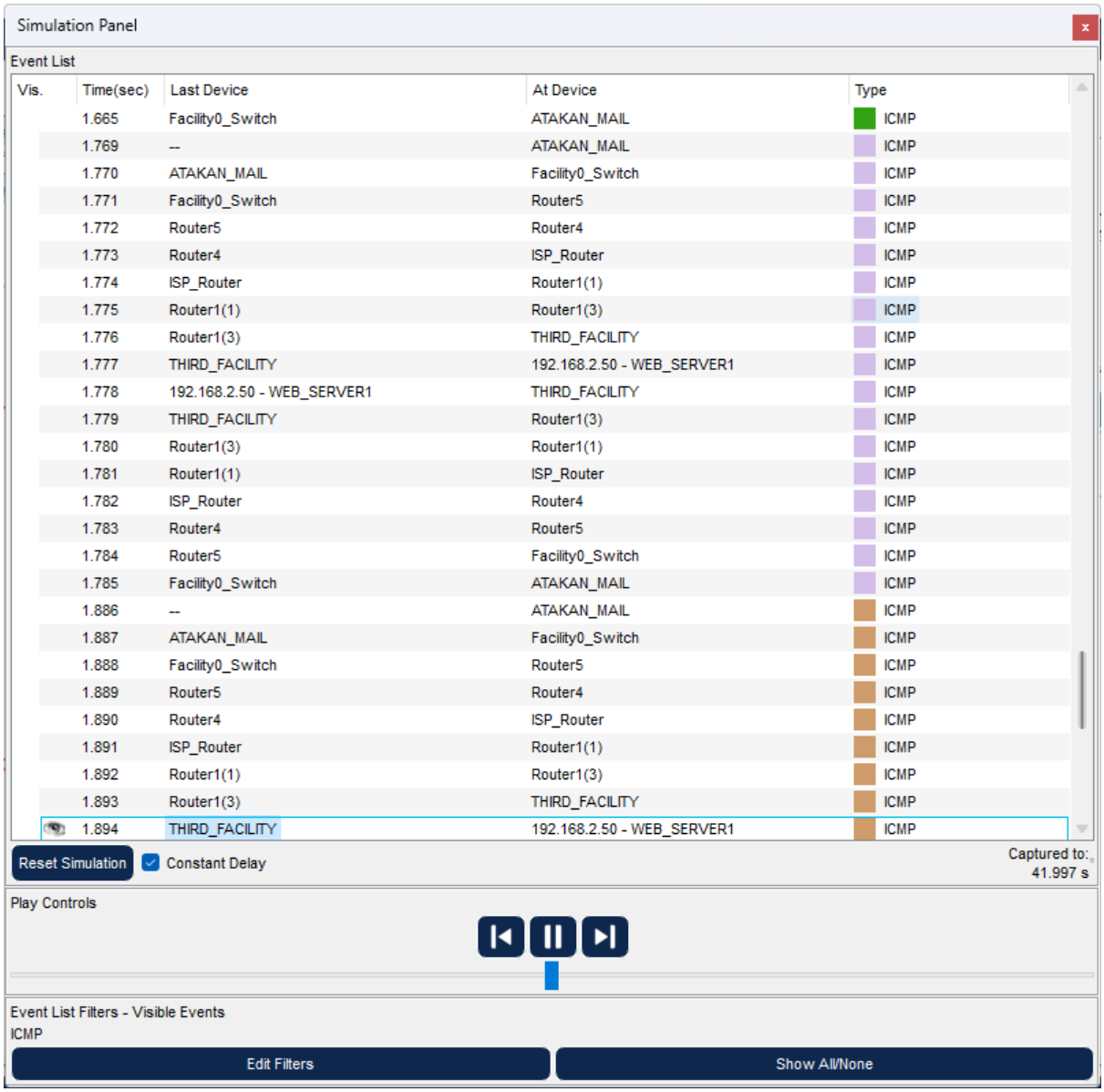

Figure 3.9.4: The relevant event list of the route (the full content is omitted since it has a lot of entries, only the final route is included)

CHAPTER 4

4. Conclusion

We have successfully created and studied a plan for linking two branch offices within a city as part of our Metropolitan Area Network (MAN) simulation project. We will provide a summary of our accomplishments and bright prospects for the future.

4.1 Achievements

We looked at ISP connection choices and built a strong network architecture with routers. The user demands of each branch office network were carefully considered during construction, allowing for file transfers, web browsing, email, and even VoIP conversations for authorized users. Secure email communication, secure file transfer protocols, and dependable internet access with priority were listed as essential network services By considering scalability during design, the network can adjust to potential increases in traffic and user numbers.

4.2 Future Work

Creating a more detailed network simulation can help test the design's performance under different loads. Network protection can be improved through the use of security measures like firewalls, network segmentation, and user authentication protocols. Proactive troubleshooting and real-time monitoring are made possible by network management system design. Investigating the integration of cloud services may offer more flexibility and lessen the strain on servers.

The company's network will benefit from this project as a launchpad for building a strong and interconnected future. A high-performing and secure network that meets communication and collaboration needs for years to come is ensured by the knowledge acquired and the blueprint created, which serve as a basis for additional research and improvement.

5. Useful Resources

1 - WLAN Configuration - Wireless Access Points Configuration Using Cisco Packet Tracer
(https://www.youtube.com/watch?v=llHpl5Fg9kQ)

2- How to configure DHCP for different subnet in Cisco Router | Packet Tracer
(https://www.youtube.com/watch?v=55WCk5ncd4k)

3- How to setup a basic Voice Over IP network in Packet Tracer
(https://www.youtube.com/watch?v=6EjqgURNfLM)

4- Configuring DHCP using Cisco iOS - DHCP Server & DHCP Helper
(https://www.youtube.com/watch?v=GCaR8e-16bs)

5- Packet Tracer Simulation Tips
(https://www.youtube.com/watch?v=E2Epcje2fpU)

6. References

[1] Yalçın, Pul, & Öztürk. (2021, June 11). *Metropolitan Area Network Simulation for University Campuses*. GitHub. Retrieved May 2, 2024, from https://github.com/zaferyalcin/Metropolitan-Area-Network-Simulation

[2] Özer, Şimşek, & Balaban. (2020, April 8). *METROPOLITAN AREA NETWORK on CISCO PACKET TRACER*. GitHub. Retrieved May 2, 2024, from https://github.com/dogukanberkozer/Metropolitan_Area_Network_Simulation