CME3204

Data Communications and Network Design

Term Project Assignment

MAN Simulation

A report by

2019510015 Hatice Şule Alaoğlu

2019510095 Serra Ceylin Öznalbant

2019510051 Emrecan Karaçayır

Outline

[1 Introduction 1](#_Toc134769033)

[1.1 Project Definition and Problem Formulation 1](#_Toc134769034)

[1.2 The purpose and motivation of the project 2](#_Toc134769035)

[1.3 Term Definitions 2](#_Toc134769036)

[1.4 Related Work 3](#_Toc134769037)

[2 Method and Simulation 4](#_Toc134769038)

[2.1 Simulation and Modeling Concepts 4](#_Toc134769039)

[2.2 Simulation Environment/Tool 4](#_Toc134769040)

[2.3 Network Design Requirements 5](#_Toc134769041)

[2.3.1 Network Devices and Components 6](#_Toc134769042)

[2.3.2 Network Cost Analysis 7](#_Toc134769043)

[2.3.3 Network Architecture 7](#_Toc134769044)

[2.3.4 Protocols Used in Network 14](#_Toc134769045)

[2.4 Requirement Analysis 15](#_Toc134769046)

[2.4.1 Web Browsing 15](#_Toc134769047)

[2.4.2 Email Service 18](#_Toc134769048)

[2.4.3 FTP Service 20](#_Toc134769049)

[2.4.4 VoIP Service 22](#_Toc134769050)

[2.4.5 DHCP Service 24](#_Toc134769051)

[2.4.6 DNS Service 26](#_Toc134769052)

[2.5 Definitions of the System/Model 28](#_Toc134769053)

[2.5.1 The Network Topology 28](#_Toc134769054)

[2.5.2 IP Addressing Schema 30](#_Toc134769055)

[2.5.3 Routing 34](#_Toc134769056)

[3 Traffic Analysis and Simulation Results 36](#_Toc134769057)

[3.1 Scenarios 36](#_Toc134769058)

[3.1.1 Scenario 1 36](#_Toc134769059)

[3.1.2 Scenario 2 47](#_Toc134769060)

[3.1.3 Scenario 3 53](#_Toc134769061)

[3.1.4 Scenario 4 58](#_Toc134769062)

[3.1.5 Scenario 5 65](#_Toc134769063)

[3.1.6 Scenario 6 69](#_Toc134769064)

[3.1.7 Scenario 7 73](#_Toc134769065)

[3.1.8 Scenario 9 76](#_Toc134769066)

[3.1.9 Scenario 9 78](#_Toc134769067)

[3.2 Configurations 81](#_Toc134769068)

[4 Conclusion 89](#_Toc134769069)

[5 References 90](#_Toc134769070)

# Introduction

The focus of this chapter is on the project definition and problem formulation of a network infrastructure design project. A clear understanding of the goals and objectives of the project, as well as the network requirements and specifications for each facility in the two branches of the organization, can be expected. The challenges involved in designing an efficient network architecture that supports maximum users and traffic load while keeping the cost of hardware equipment in mind are outlined.

The purpose and motivation of the project are also explained, including improving network availability and reliability, reducing network downtime and associated costs, enhancing network security, and optimizing the overall user experience. The benefits of implementing this project, such as better network performance, increased security and reliability, improved user experience, and reduced network downtime and related expenses, are highlighted. Potential risks, such as unexpected technical glitches, budget overruns, and project delays, are also identified.

A list of term definitions that will be useful in understanding the technical terminology used in the project is included. These definitions cover topics such as network architecture, protocols, IP addresses, routers, and more. By providing a clear understanding of the technical terms and concepts used in the project, the progress of the project can be better followed, and the network design decisions that are made can be understood.

Overall, this chapter provides a comprehensive introduction to the network infrastructure design project and sets the stage for the rest of the document.

## Project Definition and Problem Formulation

The goal of our project is to create a network that connects two branches of an office in a city using Cisco Packet Tracer software. Our aim is to ensure that the network architecture supports maximum users and traffic load with minimum delay, all while keeping the cost of hardware equipment in mind.

To accomplish this, we must carefully analyze the network requirements and specifications of each facility in the two branches. For example, the first branch office has three distinct facilities, each with different requirements. The first facility has 10 workstation users, 3 wireless users, and 3 smartphone users who need internet access to browse the web, send e-mails, and transfer files using their devices. The second facility has 5 workstation users who use web and FTP, with 3 of these workstations used for VoIP conference events. The third facility has a server farm with 5 web servers, 2 FTP servers, 1 DHCP server, 1 mail server, and 1 domain name server (DNS).

Similarly, the second branch has three distinct facilities with different requirements. The first facility has 10 workstation users, 5 wireless users, and 10 tablet users who require wireless internet access to browse the web and use e-mail applications. The second facility has 10 workstation users and 5 smartphone users who need internet access to browse the web, edit applications, and transfer files. The third facility has 10 workstations and 5 mobile devices that need internet access to browse the web, send and receive e-mails.

In summary, we must carefully consider the network needs of each facility in the two branches to design an efficient network architecture. We will ensure that the topology supports the necessary requirements while balancing the cost of hardware equipment and system requirements.

## The purpose and motivation of the project

Like we explained before the key concept of this project is to establish a strong and resilient network infrastructure for the facilities of a large organization. The objective is to enhance the productivity and efficiency of the organization by ensuring that its network infrastructure can meet both current and future business requirements.

The project's primary business goals are to improve network availability and reliability, reduce network downtime and associated costs, enhance network security, and optimize the overall user experience. By meeting these objectives, the organization can gain a competitive edge, increase customer satisfaction, and ultimately boost revenue growth.

Implementing this project has numerous benefits, including better network performance, increased security and reliability, improved user experience, and reduced network downtime and related expenses. Nevertheless, there are also potential risks such as unexpected technical glitches, budget overruns, and project delays. To mitigate these risks, the project team will meticulously plan and execute each project phase, relying on industry best practices for network design and implementation.

## Term Definitions

* **Architecture:** In networking, architecture refers to the overall design and organization of a network. This includes the physical layout of the network, the protocols used to transmit data between nodes, and the software used to manage the network. A well-designed network architecture should be reliable, scalable, and secure.
* **Channel:** A channel is the physical medium through which data is transmitted between nodes on a network. Channels can take many forms, including wired (e.g. Ethernet cables) and wireless (e.g. Wi-Fi or cellular).
* **CUCM:** Cisco Unified Communications Manager is a software-based call-processing system designed to manage voice, video, and messaging communications. It provides a scalable, highly available, and secure platform for managing various communication devices and applications.
* **DHCP:** Dynamic Host Configuration Protocol, a protocol used to automatically assign IP addresses and other network configuration information to devices on a network.
* **DNS:** Domain Name System, a system that translates human-readable domain names into IP addresses that computers can understand.
* **Gateway:** A device or software that connects two dissimilar networks, allowing information to flow between them. Protocol: A set of rules and procedures that govern the transmission of data over a network. Examples of network protocols include TCP/IP, HTTP, and FTP.
* **IP Address:** Internet Protocol Address, a unique numerical identifier assigned to each device connected to a network that uses the Internet Protocol for communication.
* **ISP:** Internet Service Provider is a company that provides customers with access to the Internet, usually through a wired or wireless connection. ISPs offer a range of services, including email, web hosting, and virtual private networks (VPNs).
* **ITN:** Inner Transit Networks that are used to connect different facilities within the same branch of the company.
* **Network:** A group of interconnected devices, such as computers, printers, servers, and other equipment, that can communicate with each other and share resources.
* **Node:** A node is any device connected to a network, such as a computer, printer, router, or switch. Each node typically has a unique address that allows it to communicate with other nodes on the network.
* **OSPF:** Open Shortest Path First is a routing protocol used for Internet Protocol (IP) networks that determines the shortest path for data to travel from one node to another.
* **OTN:** Outer Transit Networks used to connect different branches of the company to each other.
* **Packet:** A packet is a unit of data that is transmitted between nodes over a network. A packet typically includes a header that contains information about the packet's source and destination, as well as the data itself.
* **Protocol:** A set of rules and procedures that govern the transmission of data over a network. Examples of network protocols include TCP/IP, HTTP, and FTP.
* **Router:** A networking device that connects two or more networks together and directs traffic between them.
* **Server:** A computer program or device that provides functionality to other devices, such as clients, on a network. It may provide services such as file sharing, printing, email, or web hosting.
* **Switch:** A networking device that connects devices together on a network and allows them to communicate with each other.
* **System:** In the context of networking, a system refers to the collection of hardware, software, and protocols used to manage and facilitate communication between nodes on a network. Examples of networking systems include LANs (Local Area Networks), WANs (Wide Area Networks), and the internet.
* **VLAN:** Virtual Local Area Network, a technology that allows for the creation of logical networks within a physical network infrastructure.
* **WAP:** Stands for Wireless Access Point. It is a device that provides wireless connectivity to devices in a network by creating a wireless local area network (WLAN).

## Related Work

In our team's experience, we found that the Cisco forums and example templates were incredibly helpful resources when working with Cisco Packet Tracer software. The forums provided a platform for us to ask questions and receive answers from experienced users, which helped us overcome obstacles we encountered during our projects. Additionally, the example templates and tutorials provided by Cisco gave us a starting point to build upon and helped us understand how to use the software more effectively.

Overall, we found that leveraging these resources helped us work more efficiently and effectively with the Cisco Packet Tracer software.

# Method and Simulation

In this chapter, we will be discussing the network topology, IP addressing schema, and routing protocols that we have implemented in our network. Firstly, we will describe the physical layout of our network and the devices used in its construction. Next, we will discuss the IP addressing scheme that we have designed, including the different subnets used to segment our network. We will also explain the reasons behind our choice of IP addressing scheme and how it satisfies our network requirements.

Following this, we will delve into the routing protocols used in our network. We will explain the differences between the routing protocols and justify our choice of protocol. We will also describe the configuration of the routing protocol on each device in our network and explain the routing decisions made by our routers.

Overall, this chapter will provide a comprehensive overview of the network topology, IP addressing schema, and routing protocols implemented in our network. By the end of this chapter, readers should have a clear understanding of the design choices made in our network and how they contribute to the functionality of our network.

## Simulation and Modeling Concepts

In networking, simulation and modeling are important techniques that can be used to test and analyze the behavior of network designs before they are implemented in a real-world setting. One type of simulation that is particularly relevant to networking is discrete-event simulation, which models the behavior of a system as a sequence of events that occur at specific points in time.

In the context of our network design project, we are using a tool called Cisco Packet Tracer, which is a software application that allows us to simulate and model our network design. By creating a virtual environment that mimics the behavior of a real network, we can test the performance of our design and analyze its behavior under different conditions and scenarios.

The benefits of using simulation and modeling in networking include cost-effectiveness, flexibility, and the ability to test and analyze designs in a controlled environment. Simulation and modeling allow us to test a wide range of scenarios and configurations that would be difficult or impossible to replicate in a real-world setting, without incurring the costs associated with physical hardware and infrastructure.

However, there are also limitations to the accuracy of simulation and modeling, particularly in accounting for unexpected events and environmental factors that may not be captured in the simulation. In addition, the behavior of the simulated network may not always match that of a real-world network, which can make it difficult to predict how a design will perform in practice.

Despite these challenges, simulation and modeling remain powerful tools for network design and optimization, as they allow us to identify potential issues and optimize designs before deploying them in a real-world setting. By carefully considering the benefits and limitations of simulation and modeling, we can develop more effective and efficient network designs that meet the needs of our users and stakeholders.

## Simulation Environment/Tool

The simulation tool we have chosen for our project is Cisco Packet Tracer. This tool uses a graphical user interface to allow users to simulate network designs and test their functionality. It models network devices such as routers, switches, and servers, as well as communication protocols and traffic patterns.

One advantage of using Cisco Packet Tracer is that it is easy to use and has a user-friendly interface. Additionally, it allows for cost-effective testing and analysis of network designs, as it is not necessary to have physical hardware to test the system. However, there are also limitations to using simulation tools such as Cisco Packet Tracer. One limitation is that the simulation may not accurately capture all aspects of the real-world environment, including unexpected events and environmental factors. Another limitation is that the performance of the simulated network may not be a perfect reflection of the actual network.

The modeling approach used in Cisco Packet Tracer is based on discrete-event simulation. This means that the simulation is based on discrete events, such as the arrival of packets, and the simulation proceeds in a series of steps, with each step representing a fixed unit of time.

In terms of capabilities and limitations, Cisco Packet Tracer has a wide range of features and supports a variety of protocols and technologies. However, it may not support all of the advanced features of some networking devices.

To program or run the simulation in Cisco Packet Tracer, users can use a drag-and-drop interface to add and configure network devices and protocols. Additionally, the tool provides a scripting interface for more advanced users.

The modules, libraries, and components used in Cisco Packet Tracer include a variety of network devices and protocols, as well as a range of simulation settings and parameters. Some of the key components include routers, switches, wireless access points, and firewalls, as well as protocols such as TCP/IP, ICMP, and DHCP.

## Network Design Requirements

Like explained in the first chapter, our network design must be secure, fast and easily scalable. It should become larger and larger without getting impossible to maintain. We have carefully designed every aspect of this network considering these main ideologies.

* **Security:**
  + **Secure from the outer world:** Our network is a private network by its design. We use private cable lines that are connecting our main offices (branches) thus no shared information with the outside world in our backbone. These cable lines are private leased lines that we rented to us by the local ISP. Our network is connected to the rest of the Internet by external cable lines that are not part of our backbone network. To us, these separations are essential making the network safe. We control our network.
  + **Secure inside:** All of our services and applications like Wi-Fi, FTP, SSH and EMAIL are protected with required security measures, passwords etc.
  + **Secure outside:** Even though we are not used NATs in this design, in future implementations we have left extra measures to be explored like Firewalls and invisibility in the Internet. Also, because in our private network we never used a public IP address, direct reaching of our devices is impossible from outside, private IP addresses protects us from the rest of the Internet.
* **Maintainability:** All of our efforts went to making the network easy to understand thus easy to maintain. With any problem arise in the future, our schemas and specifications will be more than enough to identify and resolve the issue. Because we used industries best practices, the solutions to the problems are usually easier to solve in a more meaningful manner.
* **Size:** The current size of our MAN is relatively small but that doesn’t mean that it will stay that small. With the further details on every aspect of this network about how we tried to address expansion of the network, there will be no concerns left in this section.
* **Performance:** In our design we aimed to service 1Gbps or 1000Mbps in our private network. All of our network devices are capable serving aimed speeds. But for our end-devices, we limited their speeds to 100Mbps each, using the Fast-Ethernet instead of Gigabit-Ethernet. The main reasons behind our decision are the stability and the cost. In our stress tests we found that copper cables are not very well suited to serve these kinds of speeds. Our ITN’s and inner facility networks use copper cables but our OTN’s use fiber optic cables. We chose fiber optics for OTN’s because of the distances can go up to kilometers in a MAN thus we had to go for the: better option for network reliability. Also, in our working environment (Cisco Packet Tracer) we couldn’t use some of the devices because some of them lack much needed modules and expansions we desired to use.

Our network architecture is carefully thought to be easily customizable and can be resilient to circumstances that would arrive in future. In the current form we propose one router (gateway) by each facility and one border router by each branch then those facility routers together with the branch router creates our branch ITNs (Inner Transit Network). Branches are connected with their border routers.

In the future, the design might use different number of gateways by facility or different number of border gateways and maybe there will be a backbone outside of facilities to be the central focus of the network. But the main point is, our design allows for radical changes. We also implemented some of the latest technologies and best practices. Some of them are:

* **OSPF:** A dynamic routing protocol that we will discuss more in the routing section.
* **WPA2-PSK (AES):** We have used the current standard to protect our network from outsiders. WPA2-PSK (AES) is a security protocol used to encrypt wireless network connections. It stands for Wi-Fi Protected Access 2 with Pre-Shared Key and Advanced Encryption Standard.
* **HTTPS:** We didn’t limit current configuration to use HTTPS for the testing purposes but after the completion of the testing process, we will allow only Secure HTTP connections.
* **SSH over TELNET:** In our simulation environment Packet Tracer we are allowed to connect devices that are only network equipment. So, we didn’t had chance to test SSH or TELNET connection to host devices. With our best efforts trying to integrate SSH was limited to routers. With that in mind, we used SSH over TELNET for its security reasons nevertheless.

### Network Devices and Components

* 45 Workstations (PC-PT)
* 13 Smartphones (SMARTPHONE-PT)
* 12 Servers (Server-PT)
* 10 Tablets (TabletPC-PT)
* 10 Routers (9 Cisco 2911, 1 Cisco 2811 -purposed as CUCM-)
* 8 Laptops (Laptop-PT)
* 7 Switches (Cisco 2960-24TT)
* 3 IP Phones (Cisco 7960)
* 2 DSL Modems (DSL-Modem-PT)
* 1 Cloud (Cloud-PT)

### Network Cost Analysis

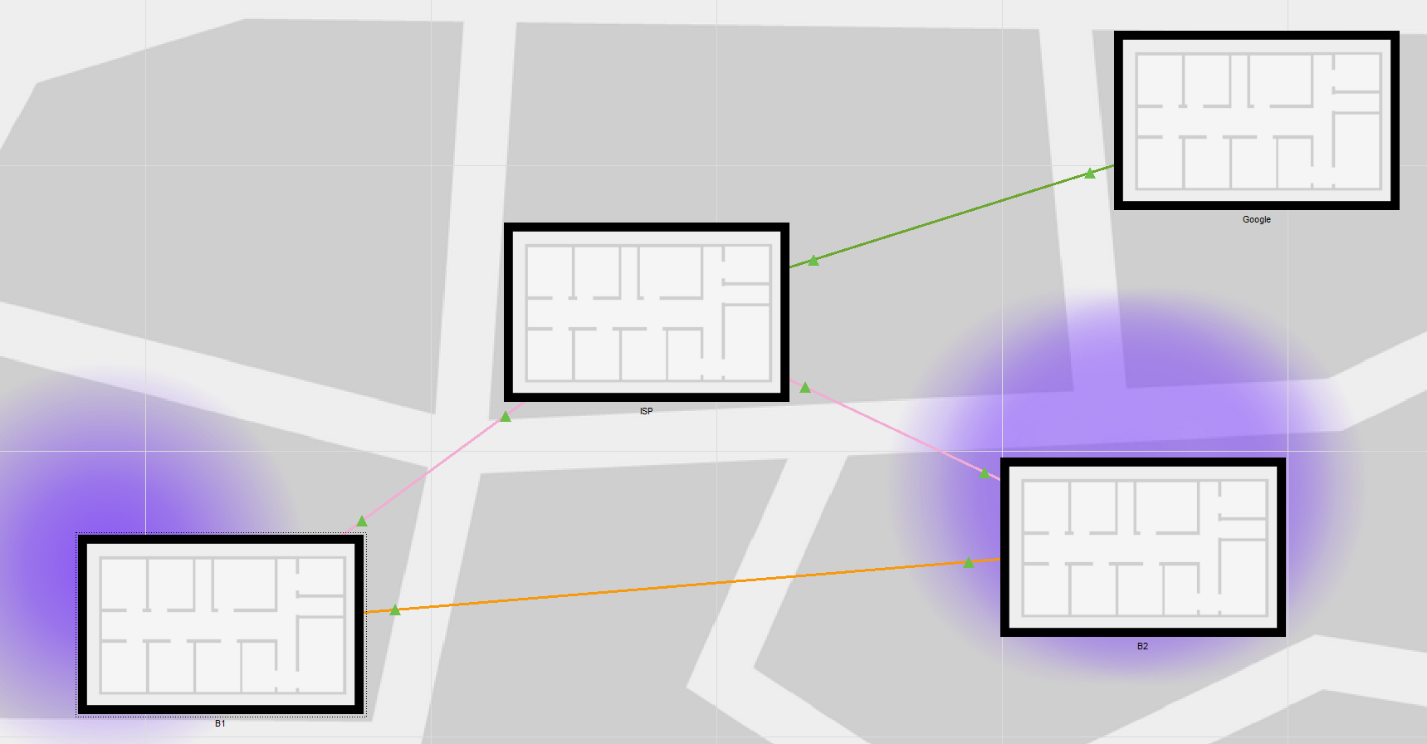
* **Workstation (45):** Dell Precision 3260 Compact – ($1,240.00 each) $55,800.00
* **Smartphone (13):** Google Pixel 6a – ($449.00 each) $5,837.00
* **Server (10):** HPE ProLiant G10 2U – ($2,785.00 each) $27,850.00
* **Tablet (10):** Apple iPad 9th Gen – ($305.00 each) $3,050.00
* **Router (10):** Cisco 2911 – ($3,550.00 each) $35,500.00
* **Laptop (8):** Dell Precision 7560 Workstation – ($1,355.00 each) $10,840.00
* **Switch (7):** Cisco WS-C2960-24TT-L – ($1,525.00 each) $10,625.00
* **IP Phone (3):** Cisco 7960 – ($55.00 each) $165.00
* **DSL Modem (2):** Motorola NVG510 – ($120.00 each) $240.00
* **Fiber Optic Cabling:** FiberShack SC/APC – ($2 per meter) $600.00
* **Copper Cabling:** Jadaol CAT7 – ($1 per meter) $600.00
* **ISP Leased Line:** Vodafone 1Gbps managed – (Monthly $1,125.00) $40,500.00
* **Network Design:** Consultancy and design fee $10,875.00
* **Labor:** Building the network $3,800.00
* **Total (with end-devices): $206,282.00**
* **Total (without end-devices): $130,755.00**

Prices and the total cost are estimate values and can be changed during the process. Product prices are MSRP and bulk purchase prices can be lower. Each device/component carefully selected to represent our logical design.

### Network Architecture

We designed the network in Cisco Packet Tracer. Software does a great job at presenting the architecture and giving a good sense of what to expect in real world representation.

We start by the general overview of the network. In the next figure overview of the network’s physical design will be shown.

Figure 1.1: Overview of the network’s physical design

In the figure 1.1 a portion of the city can be seen. This city is where our network resides. You can see in the bottom left corner our B1 office. That office is connected to B2 office with the orange fiber optic cable. Between our two offices, you can see the factionary ISP building. ISP provides Internet connections with DSL to both of our offices through their phone line. Also in the top right corner, you can see another factionary building which is Google’s building. Google’s building is used to represent the Internet. With extra fiber lines we can connect other offices later in the future. This was the high-level overview of our physical design. In the next figure we will see the inside of the office B1.

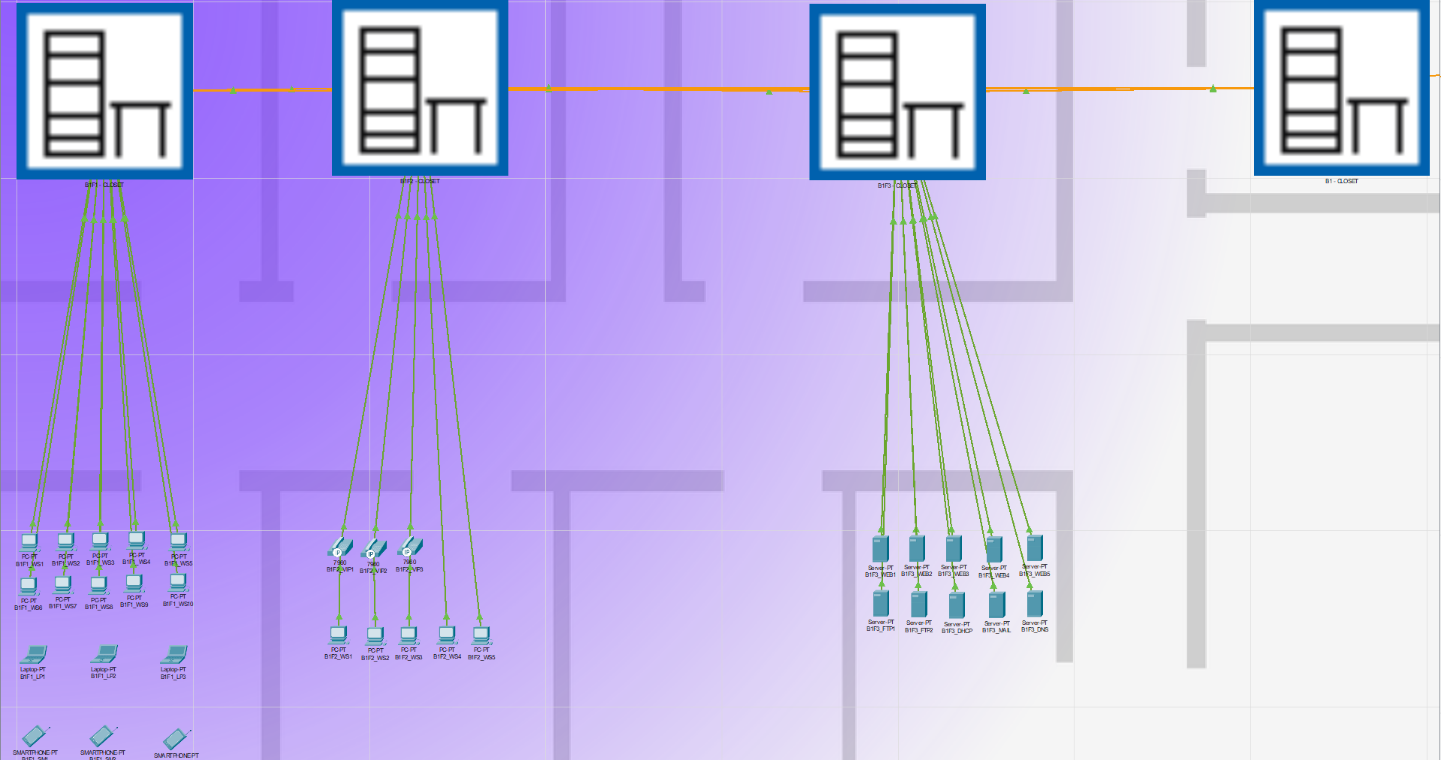


Figure 1.2: Overview of the branch B1’s network’s physical design

Office B1 is fictionally divided into three facilities. Each facility has network closets. Orange line between them is the fiber optic cable. They are connected to each other and also connected to B1 main closet. Inside B1 main closet, there is a Modem which is B1’s gate to the Internet. There is also the main gateway (router) for this branch. Then another fiber optic cable also originates from there to ISP’s infrastructure.

Actually, this physical design is not very accurate for our special purposes for this network. Facilities should have their own buildings and branches should be campuses of offices.

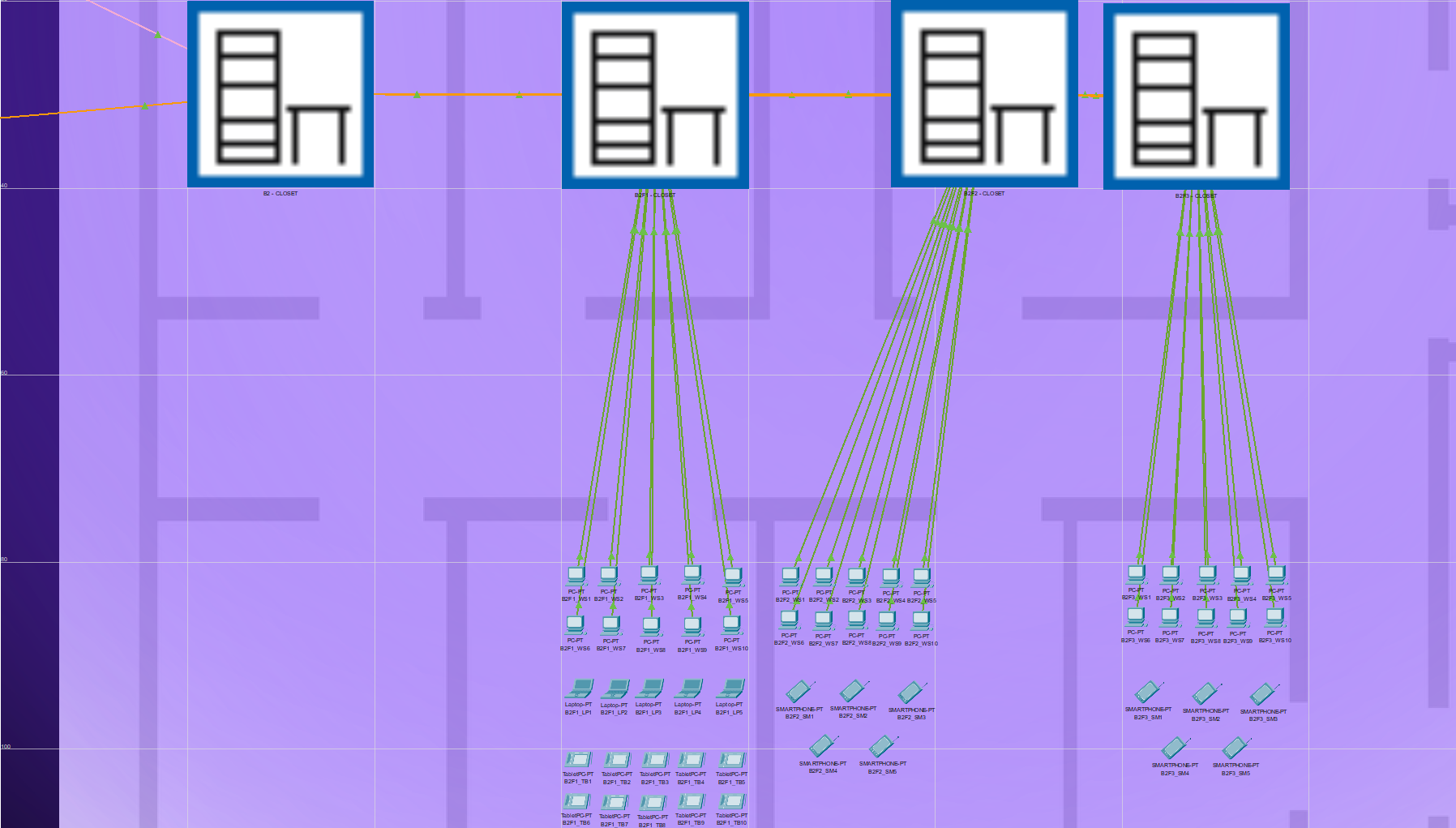


Figure 1.3: Overview of the branch B2’s network’s physical design

After our physical examination of the network, it is time to look at the logical architecture and the innerworkings of the design. In the next figure there will be an overview of the whole logical design of the network.

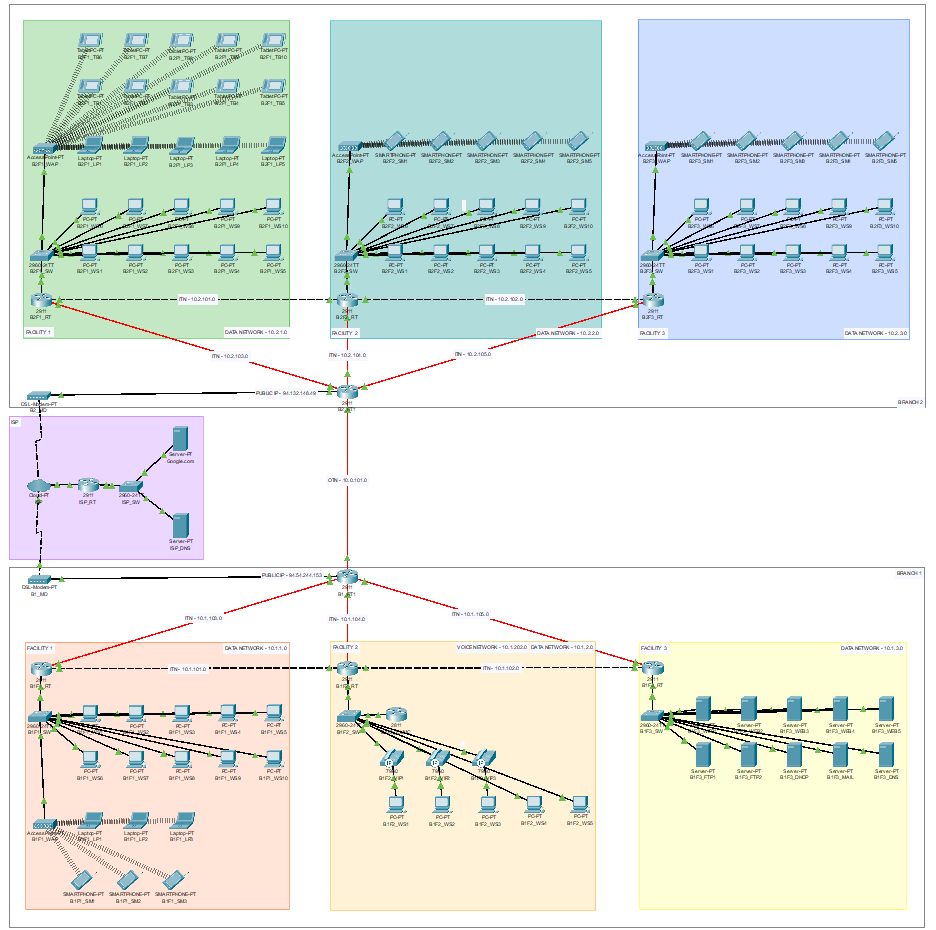


Figure 2.1: Overview of the network’s logical design

In the figure 2.1 logical overview of the network can be seen. Inside the boxes with the black outlines, branches can be seen. Red, orange and yellow boxes represent facilities in the B1 branch. Green, mint and blue boxes represent facilities in the B2 branch. The purple box represents ISP and the Internet. In the next figure we will discuss the first branch.

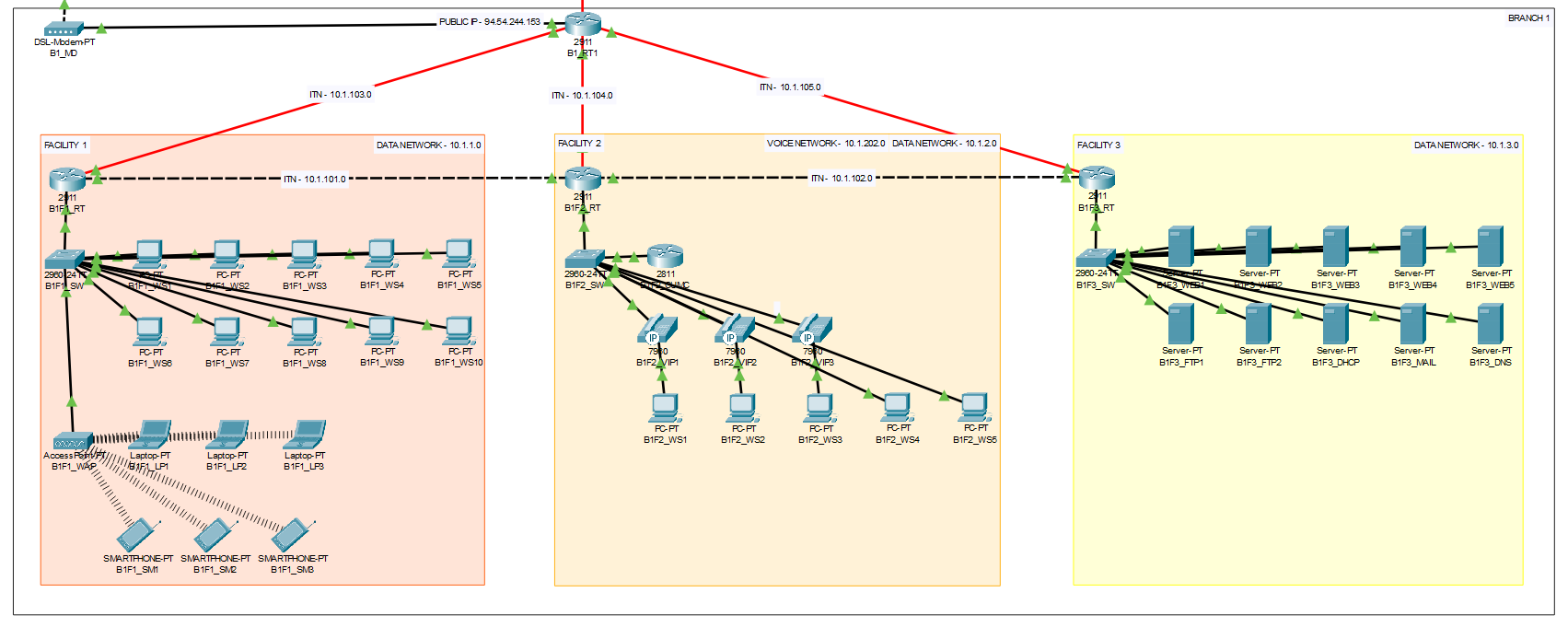


Figure 2.2: Overview of the branch B1’s network’s logical design

In the figure 2.2, we can see the exact wiring and components of the branch B1. In the top left corner, a DSL model can be seen. This modem is used to access the Internet. The modem assigns a public IP address to B1 border router. We assigned one border router in this design but it can be increased on demand. B1\_RT is the border router referred is the router that allows us to connect to other branches and the Internet.

Facility 1 houses 10 workstations (WS), 3 laptops (LP) and 3 smartphones (SM). While workstations connect to the network by the switch (SW), laptops and smartphones are connected by Wi-Fi. The wireless connection is provided by the wireless access point (WAP). The switch is connected to the Facility main router (RT).

Facility 2 houses 5 workstations (WS) and 3 IP phones (VIP). Communications are handled by the CUCM router. We used VLANs to achieve the separation of voice and data networks. We achieved this by the VLAN configuration in the switch then further configured facility main router to route between voice and data VLANs. First IP phone given by number 1201 second one 1202 and third one 1203.

Facility 3 houses 5 servers that serve different purposes. First 5 servers are used as web servers. 6 and 7 used for FTP. Also, we have DHCP, MAIL and DNS servers.

Our DNS server translates domains that it has A records for. And also, if the requested domain is not known, it forwards unknown domains to the ISP’s DNS server.

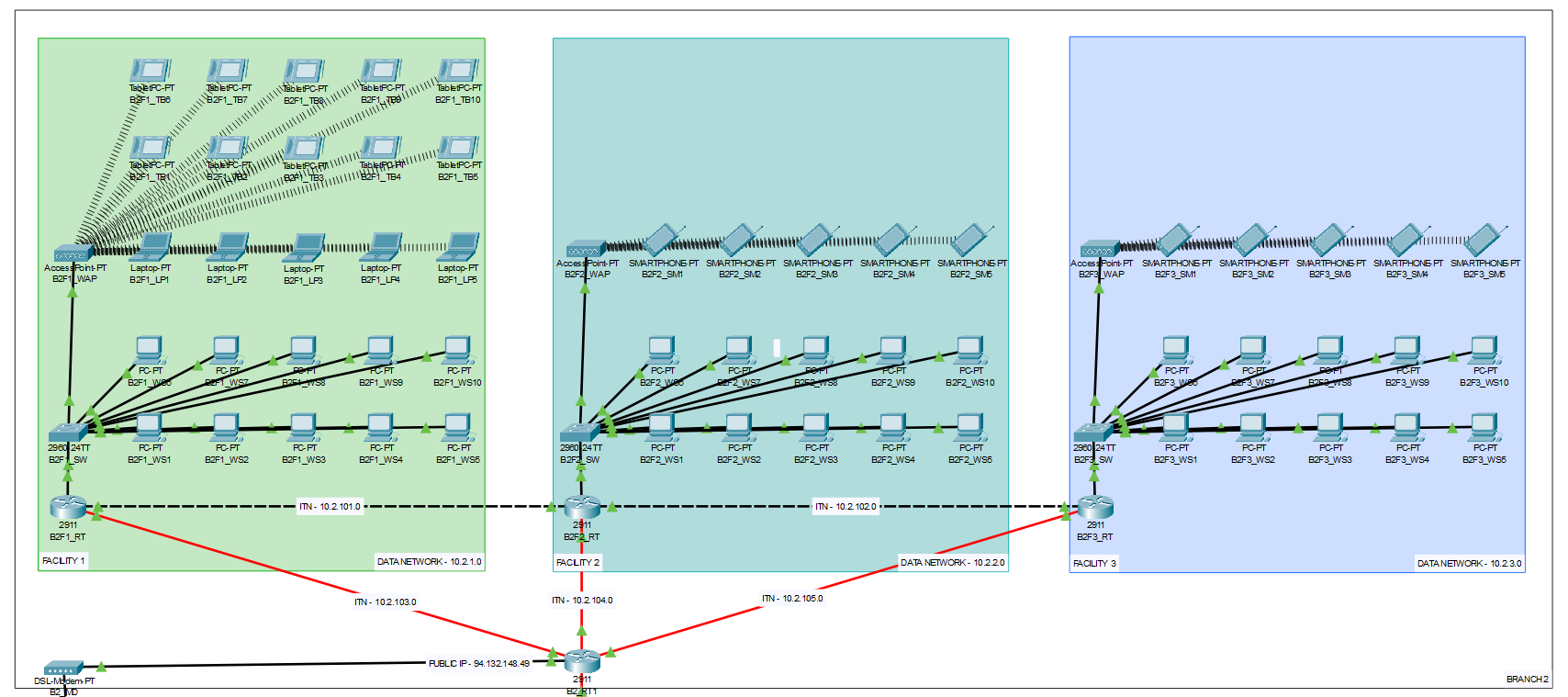


Figure 2.3: Overview of the branch B2’s network’s logical design

Nothing special in terms of network in the B2 branch. These 3 facilities are almost identical to first branch’s first facility.



Figure 2.4: Overview of the ISP’s network’s physical design

ISP’s network is completely fictional. It represents the Internet. We created a higher-level DNS server and a web server which hosts the Google.com

### Protocols Used in Network

* Transmission Control Protocol (TCP) and Internet Protocol (IP)
* User Datagram Protocol (UDP)
* Border Gateway Protocol (BGP)
* Open Shortest Path First (OSPF)
* Simple Network Management Protocol (SNMP)
* Domain Name System (DNS)
* Dynamic Host Configuration Protocol (DHCP)
* Hypertext Transfer Protocol (HTTP)
* Secure Shell (SSH)
* Open Shortest Path First (OSPF)
* Hypertext Transfer Protocol (HTTP)

## Requirement Analysis

In this section, we are going to explore the network’s required use cases and applications. These include but not limited to:

* Web Browsing
* Email Service
* FTP Service
* VoIP Service
* DHCP Service
* DNS Service
* SSH Service

### Web Browsing

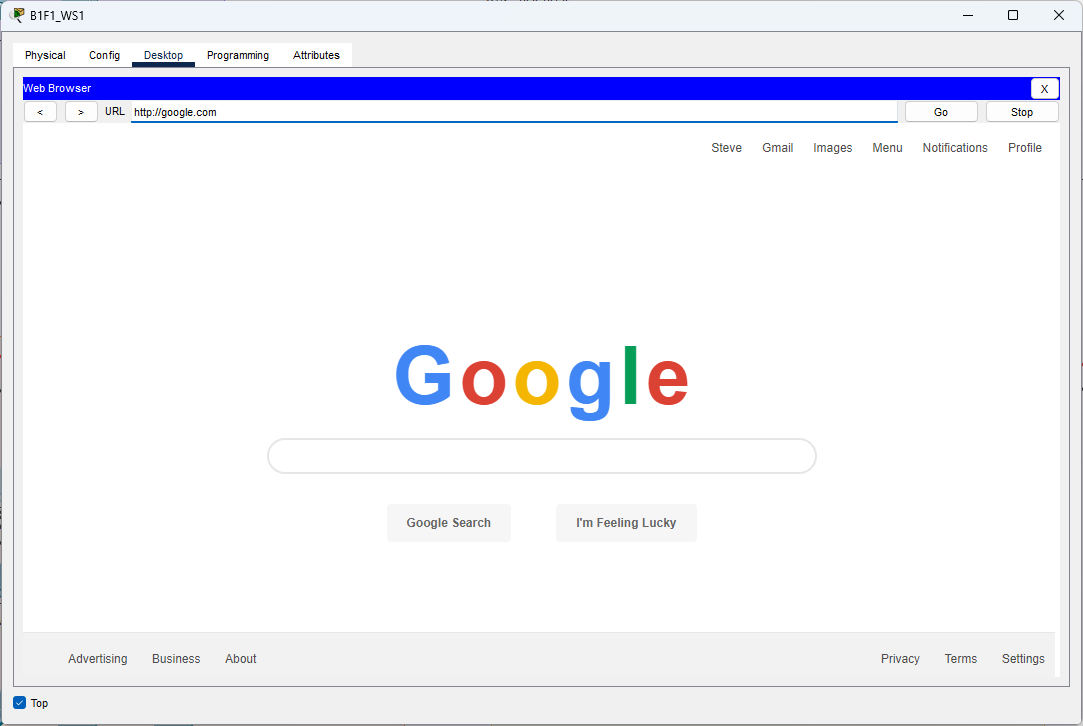


Figure 3.1: Demonstrating the web browsing in the network

Web browsing achieved via ISP’s router that connects our network to the internet. A symbolic Google.com server created to serve the purpose.

To resolve the DNS, we forwarded the request from our local DNS server to ISP’s DNS server.

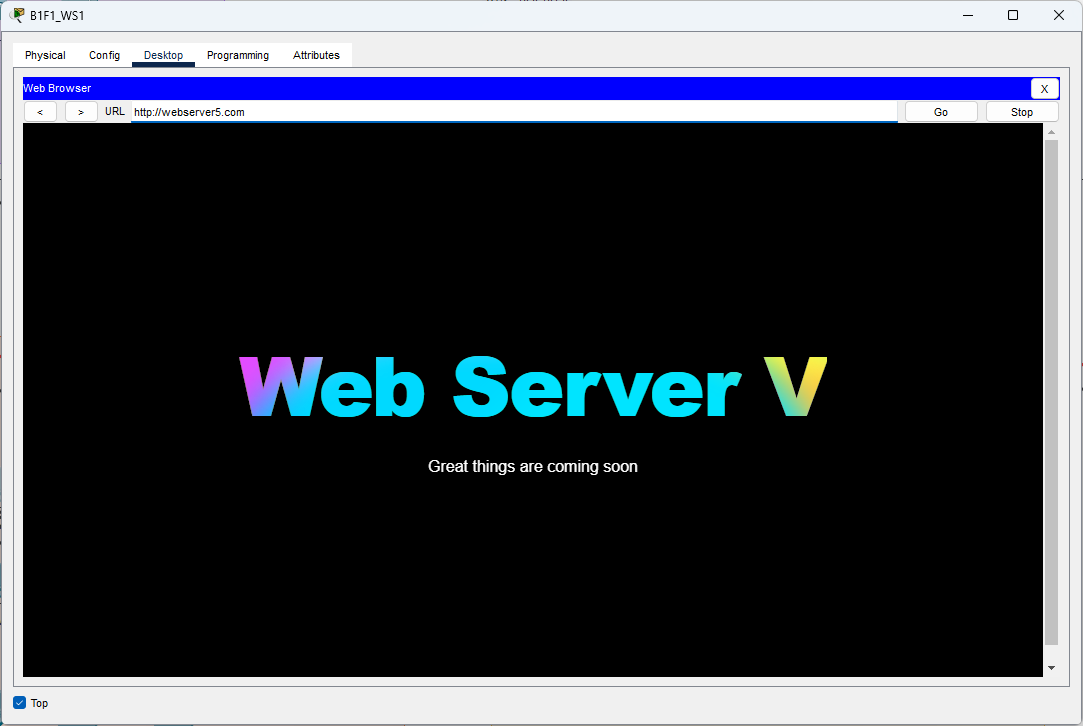


Figure 3.2: Demonstrating the private web servers’ browsing

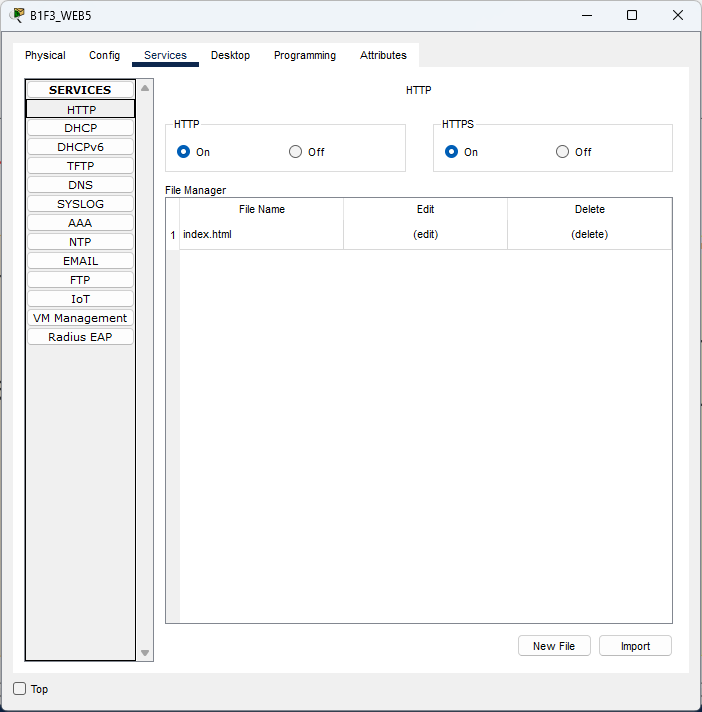


Figure 3.3: Web server configurations

### Email Service

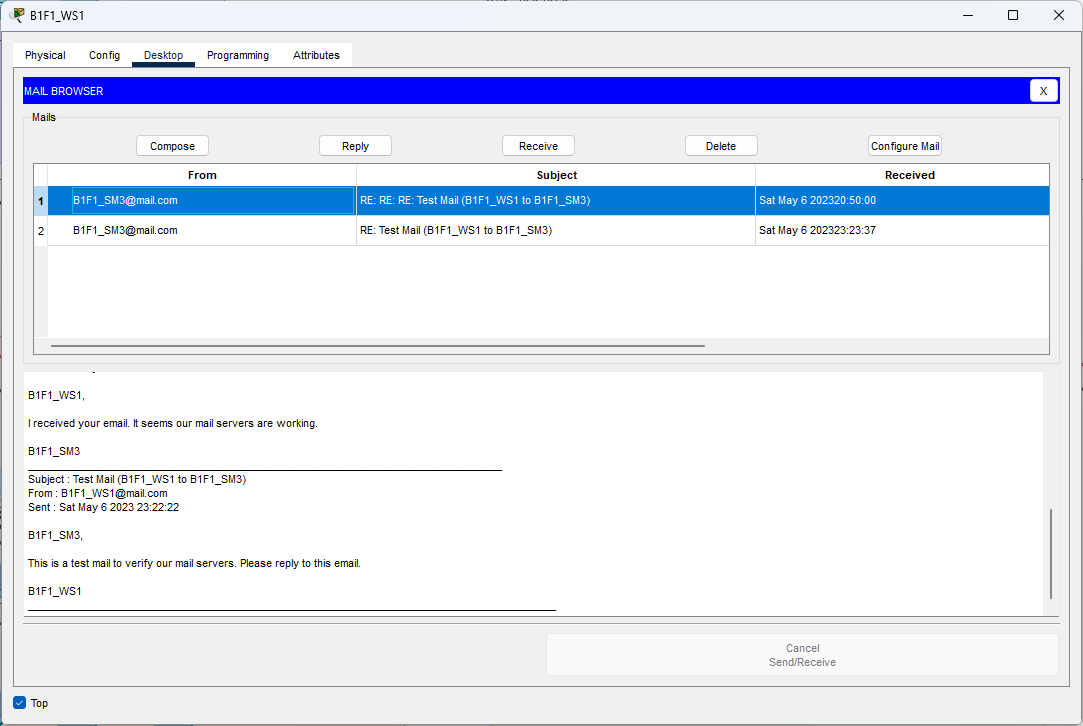


Figure 3.4: Demonstrating the email service

Our email service uses SMTP and POP3 services respectively. Every user who privileged to use the email service given by corporate mail accounts and passwords.

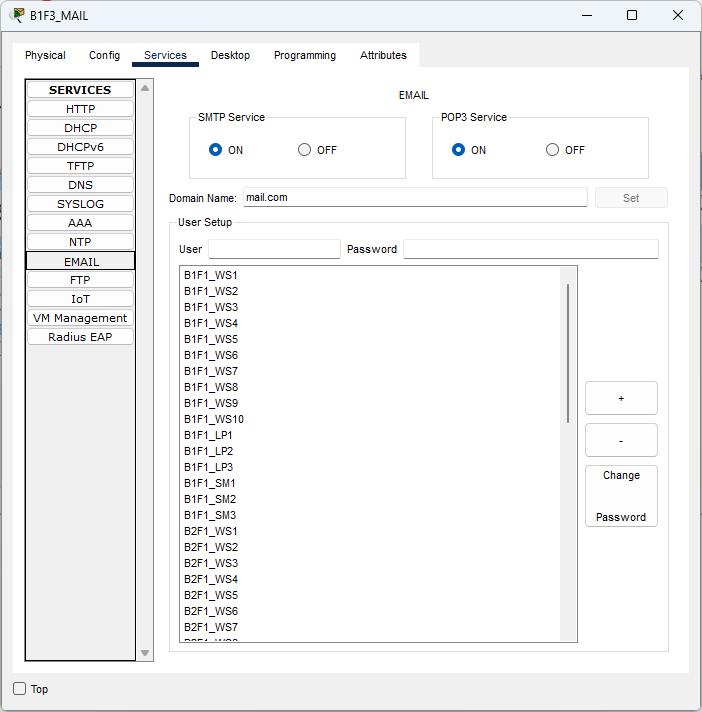


Figure 3.5: Email server configurations

### FTP Service

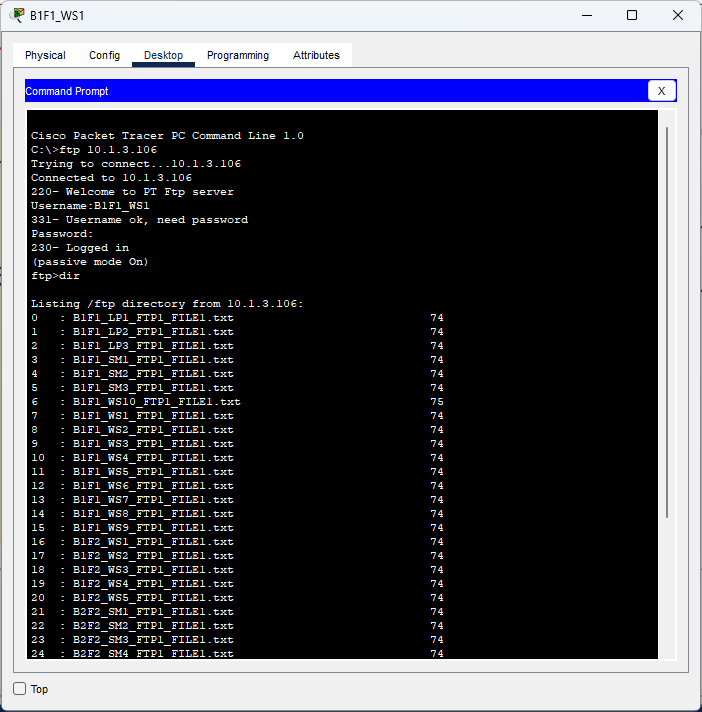


Figure 3.6: Demonstrating the FTP service

FTP servers (2) are configured accordingly to allow users to share files with each other. Every user who privileged to use the service given with the accounts representing their privileges.

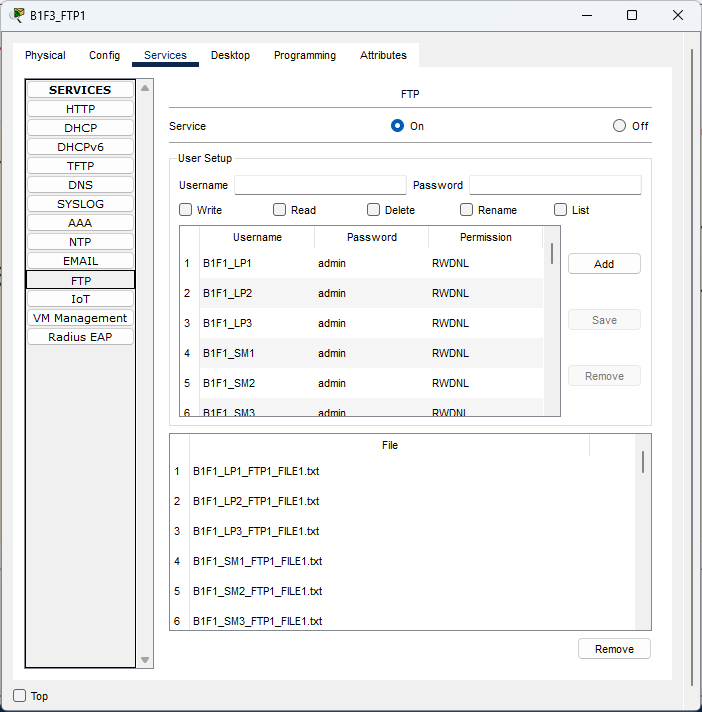


Figure 3.7: FTP server configurations

### VoIP Service

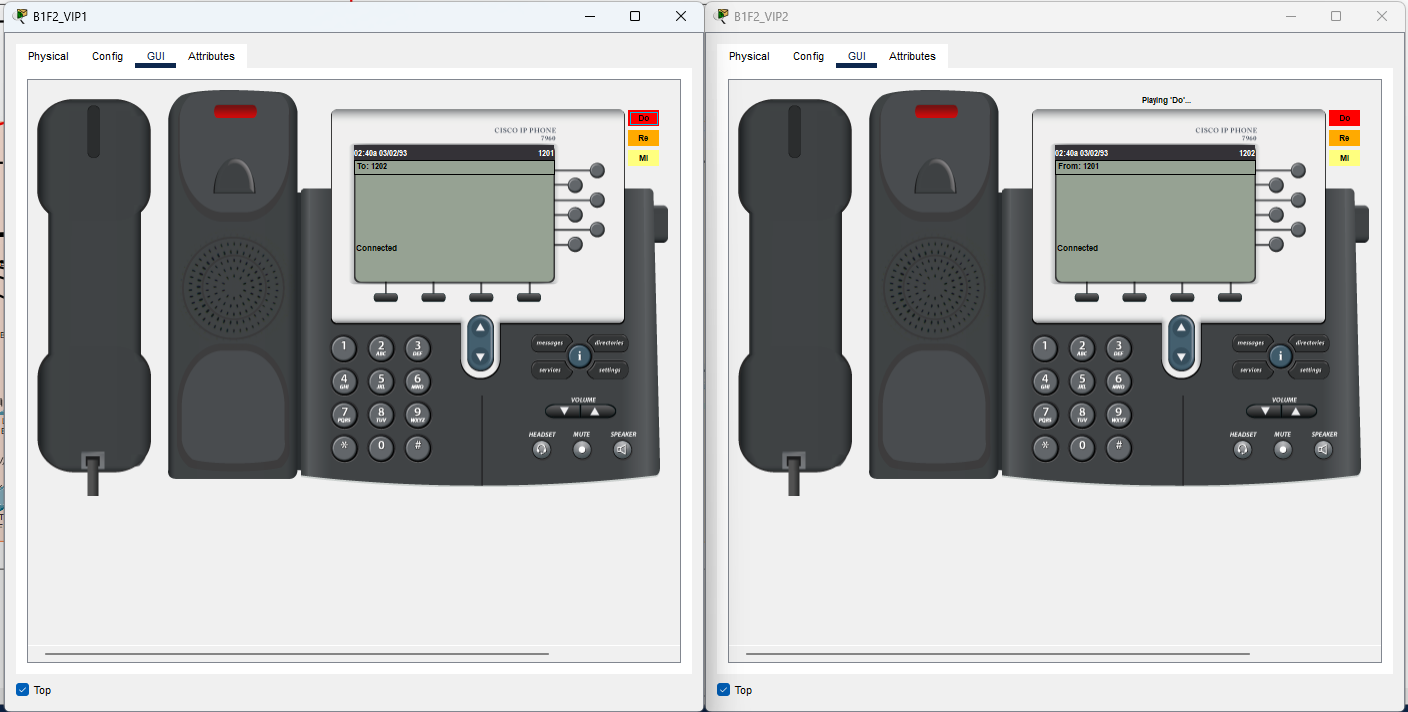


Figure 3.8: Demonstrating the VoIP service

VoIP service was the hardest service to achieve. We needed to create corresponding voice and data VLANs to separate the communication from the data network. We achieve that using these steps:

* Configured switch to provide two virtual networks, VLAN 2 DATA, VLAN 2O2 VOICE.
* Configured router to have sub interfaces to correctly route incoming traffic
* Configured router to encapsulate traffic with the protocol DOT1Q
* Added special router to be our communication manager
* Configured our CUCM to address the IP phones correctly
* Assigned each IP Phone with corresponding numbers

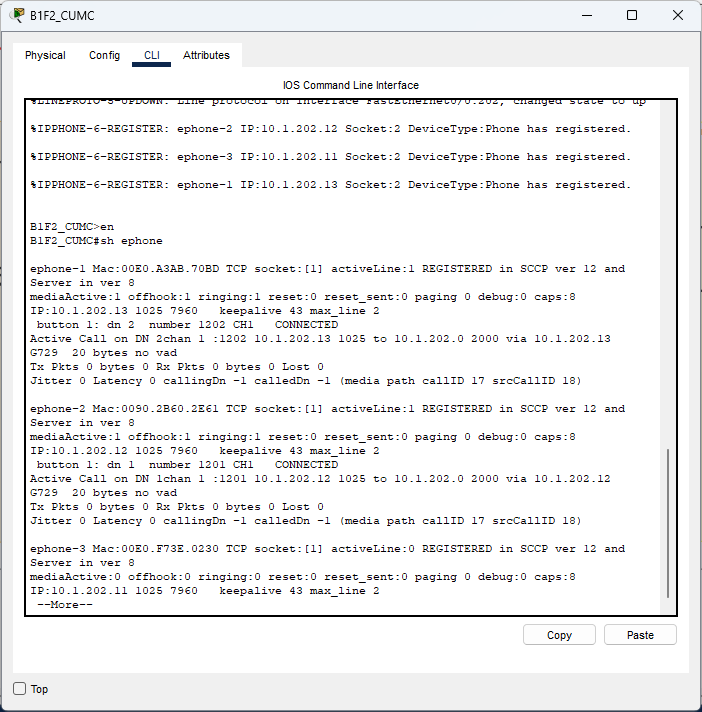


Figure 3.9: Registered ephones on the CUCM

### DHCP Service

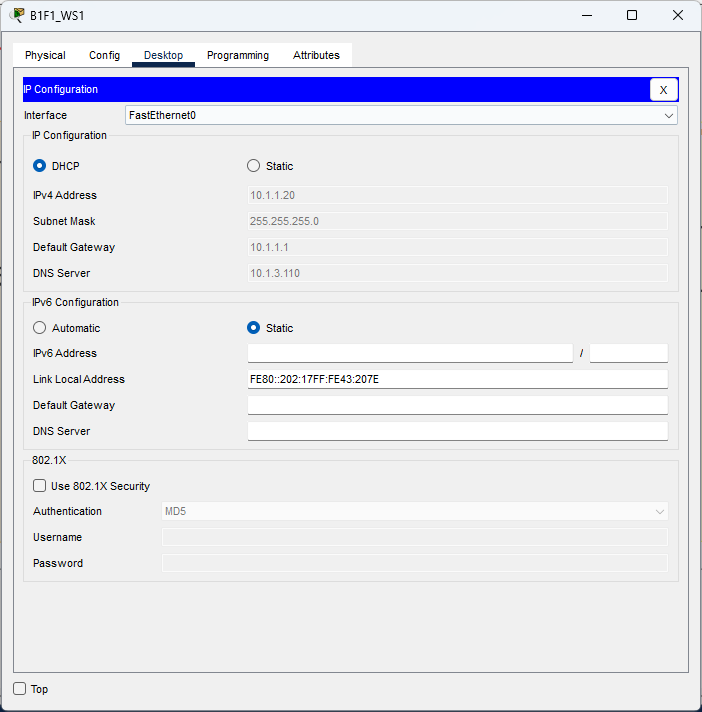


Figure 3.10: Demonstrating the DHCP Service

DHCP server assigns each end-device its IP address. We configured our DHCP server to address each end-device correctly.

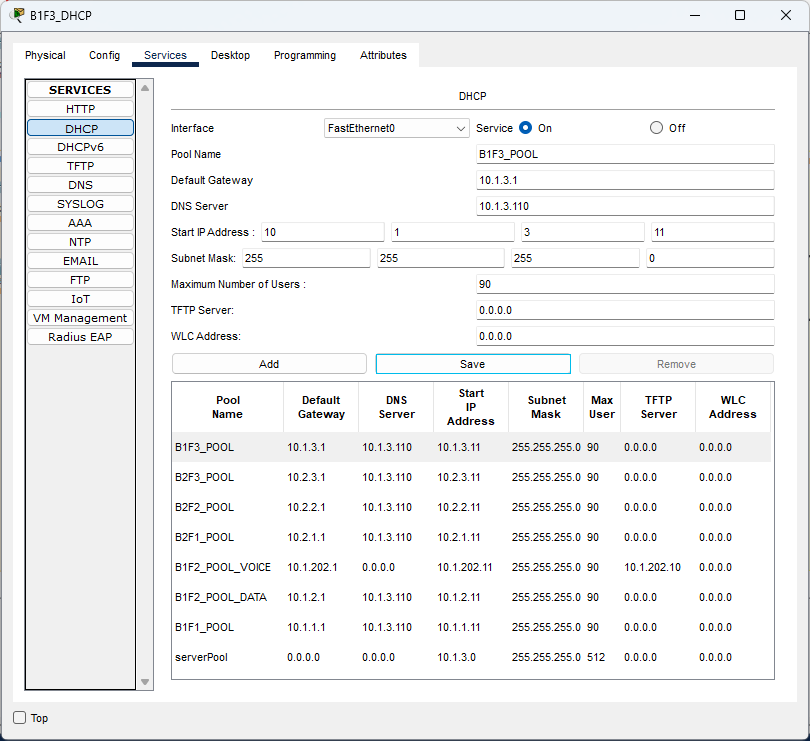


Figure 3.11: DHCP Server configurations

### DNS Service



Figure 3.12: Local DNS server configurations

Our local DNS server is responsible for local domain name resolutions. It is also responsible for forwarding domain names that it can’t resolve. In this case our local DNS server is forwarding requests to Google.com by forwarding to the ISP’s DNS server.

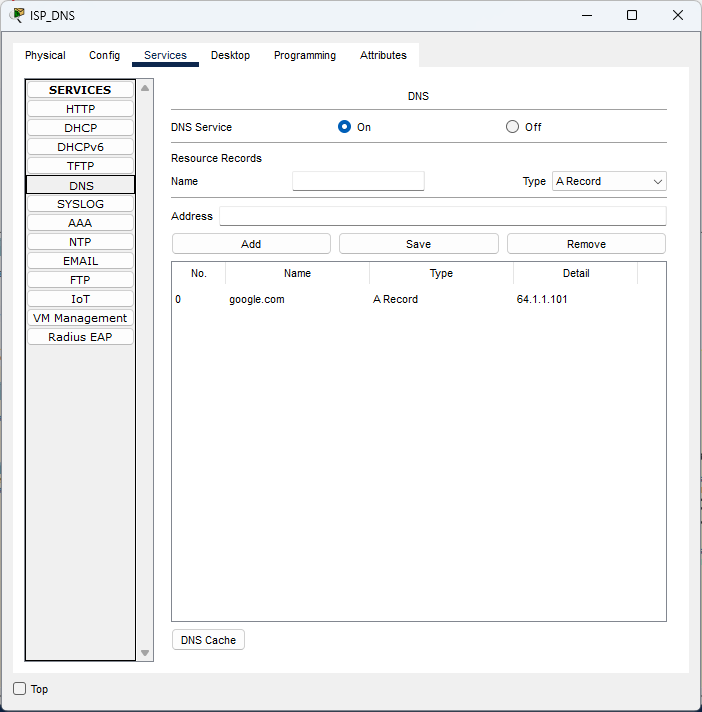


Figure 3.13: ISP’s DNS server configurations

## Definitions of the System/Model

In this section we will discuss the technical specifications, schemas and topologies.

### The Network Topology

* **B1: 10.1.**0.0/24
  + **B1F1: 10.1.1.**0./24
    - **B1F1\_RT:** 10.1.1.1/24
      * **B1F1\_SW**
        + **B1F1\_WS1:** DHCP
        + **B1F1\_WS2:** DHCP
        + **B1F1\_WS3:** DHCP
        + **B1F1\_WS4:** DHCP
        + **B1F1\_WS5:** DHCP
        + **B1F1\_WS6:** DHCP
        + **B1F1\_WS7:** DHCP
        + **B1F1\_WS8:** DHCP
        + **B1F1\_WS9:** DHCP
        + **B1F1\_WS10:** DHCP
        + **B1F1\_WAP**

**B1F1\_LP1:** DHCP

**B1F1\_LP2:** DHCP

**B1F1\_LP3:** DHCP

**B1F1\_SM1:** DHCP

**B1F1\_SM2:** DHCP

**B1F1\_SM3:** DHCP

* + **B1F2: 10.1.2.**0./24
    - **B1F2\_RT: VLAN 2**: 10.1.2.1/24, **VLAN 202**: 10.1.202.1/24
      * **B1F2\_SW:**
        + **B1F2\_CUCM:** 10.1.202.10/24
        + **B1F2\_VIP1:** DHCP

**B1F2\_WS1:** DHCP

* + - * + **B1F2\_VIP1:** DHCP

**B1F2\_WS2:** DHCP

* + - * + **B1F2\_VIP1:** DHCP

**B1F2\_WS3:** DHCP

* + - * + **B1F2\_WS4:** DHCP
        + **B1F2\_WS5:** DHCP
  + **B1F3: 10.1.3.**0./24
    - **B1F3\_RT:** 10.1.3.1/24
      * **B1F3\_SW**
        + **B1F3\_WEB1:** 10.1.3.101/24
        + **B1F3\_WEB2:** 10.1.3.102/24
        + **B1F3\_WEB3:** 10.1.3.103/24
        + **B1F3\_WEB4:** 10.1.3.104/24
        + **B1F3\_WEB5:** 10.1.3.105/24
        + **B1F3\_FTP1:** 10.1.3.106/24
        + **B1F3\_FTP2:** 10.1.3.107/24
        + **B1F3\_DHCP:** 10.1.3.108/24
        + **B1F3\_MAIL:** 10.1.3.109/24
        + **B1F3\_DNS:** 10.1.3.110/24
* **B2: 10.2.**0.0/24
  + **B2F1: 10.2.1.**0./24
    - **B2F1\_RT:** 10.2.1.1/24
      * **B2F1\_SW**
        + **B2F1\_WS1:** DHCP
        + **B2F1\_WS2:** DHCP
        + **B2F1\_WS3:** DHCP
        + **B2F1\_WS4:** DHCP
        + **B2F1\_WS5:** DHCP
        + **B2F1\_WS6:** DHCP
        + **B2F1\_WS7:** DHCP
        + **B2F1\_WS8:** DHCP
        + **B2F1\_WS9:** DHCP
        + **B2F1\_WS10:** DHCP
        + **B2F1\_WAP**

**B2F1\_LP1:** DHCP

**B2F1\_LP2:** DHCP

**B2F1\_LP3:** DHCP

**B2F1\_LP4:** DHCP

**B2F1\_LP5:** DHCP

**B2F1\_TB1:** DHCP

**B2F1\_TB2:** DHCP

**B2F1\_TB3:** DHCP

**B2F1\_TB4:** DHCP

**B2F1\_TB5:** DHCP

**B2F1\_TB6:** DHCP

**B2F1\_TB7:** DHCP

**B2F1\_TB8:** DHCP

**B2F1\_TB9:** DHCP

**B2F1\_TB10:** DHCP

* + **B2F2: 10.2.2.**0./24
    - **B2F2\_RT:** 10.2.2.1/24
      * **B2F2\_SW**
        + **B2F2\_WS1:** DHCP
        + **B2F2\_WS2:** DHCP
        + **B2F2\_WS3:** DHCP
        + **B2F2\_WS4:** DHCP
        + **B2F2\_WS5:** DHCP
        + **B2F2\_WS6:** DHCP
        + **B2F2\_WS7:** DHCP
        + **B2F2\_WS8:** DHCP
        + **B2F2\_WS9:** DHCP
        + **B2F2\_WS10:** DHCP
        + **B2F2\_WAP**

**B2F2\_SM1:** DHCP

**B2F2\_SM2:** DHCP

**B2F2\_SM3:** DHCP

**B2F2\_SM4:** DHCP

**B2F2\_SM5:** DHCP

* + **B2F3: 10.2.3.**0./24
    - **B2F3\_RT:** 10.2.3.1/24
      * **B2F3\_SW**
        + **B2F3\_WS1:** DHCP
        + **B2F3\_WS2:** DHCP
        + **B2F3\_WS3:** DHCP
        + **B2F3\_WS4:** DHCP
        + **B2F3\_WS5:** DHCP
        + **B2F3\_WS6:** DHCP
        + **B2F3\_WS7:** DHCP
        + **B2F3\_WS8:** DHCP
        + **B2F3\_WS9:** DHCP
        + **B2F3\_WS10:** DHCP
        + **B2F3\_WAP**

**B2F3\_SM1:** DHCP

**B2F3\_SM2:** DHCP

**B2F3\_SM3:** DHCP

**B2F3\_SM4:** DHCP

**B2F3\_SM5:** DHCP

This topology is only a high-level topology. We always experimented with our topology in the spare projects in Cisco Packet Tracer.

### IP Addressing Schema

As a team, we have developed a unique IP address schema that offers an effective solution for network addressing needs. We have opted for a customized approach using Class A IP addresses instead of traditional Class C or Class B addresses, which allows us to convey pertinent information about each address's function and location within the network.

Our team's approach to network design reflects our commitment to efficiency and organization. By creating a transparent addressing system, we aim to simplify network management and troubleshooting while improving performance and security.

Our IP address schema aims to be as futureproof as possible. We tried to achieve that by utilizing every bit in the Class A private IP addresses in range 10.0.0.0 to 10.255.255.255, we tried to give meaning to every address we can. We only used private IP ranges. We have utilized our understanding of addressing protocols and best practices to create a system that is tailored to our specific needs and goals. It is our expectation that this system will provide a sturdy foundation for our network infrastructure for years to come.

**Theoretical Metrics:**

**Maximum:**

254 Branches

25,400 Facilities

254,000 Network Devices

1,234,440 IP Phones

1,371,600 Other IP Devices

25,400,000 Servers

25,400,000 End-Devices

1. **Addressing Inside the Facilities**

10.X.Y0.Z0/24

**X:**

**Range:** [1-254]

**Purpose:** BID (Branch Identifier)

**Explanation:** Reserved to represent the branch which this network resides.

**Formula:** X = Branch No

**Example:** 10.**1**.1.1 (This network resides in the first branch of the company)

**Y:**

**Y1:**

**Range:** [1-100]

**Purpose:** FID (Facility Identifier)

**Explanation:** Reserved to represent the facility which this network resides.

**Formula:** Y = Facility No

**Example:** 10.1.**1**.1 (This network resides in the first facility of the branch)

**Y2:**

**Range:** [201-254]

**Purpose:** Telephony service

**Explanation:** Reserved for voice purposed VLANs in facilities that are in range [1-54].

**Formula:** Y = 200 + FID

**Example:** 10.1.**201**.1 (This network is intended for use in a voice purposed VLAN for the first facility of the specified branch)

**Z:**

**Z1:**

**Range:** [1-10]

**Purpose:** Network equipment addressing

**Explanation:** Reserved for network equipment addressing in facilities. (Facilities without specified VLANs can support up to 10 pieces of network equipment that require an IP address)

**Formula:** Z = Assign freely in specified range except address 1

**Example:** 10.1.1.**1** (This IP address belongs to the specified facility’s gateway. Also, Z value of 1 is special to facilities’ gateways and must not be used with other purposes)

**Z2:**

**Range:** [11-100]

**Purpose:** End-device addressing

**Explanation:** Reserved for end-device addressing in facilities. These device types are including but not limited to desktop computers, laptops, smartphones, IP phones and tablets.

**Formula:** Z = Usually assigned by a DHCP server. If not, assign freely in specified range

**Example:** 10.1.1.**11** (This IP address belongs to an end-device that is addressed under the specified facility’s network)

**Z3:**

**Range:** [101-200]

**Purpose:** Server addressing

**Explanation:** Reserved for server addressing in facilities. These server types are including but not limited to Web servers, DNS servers, DHCP servers and Mail servers.

**Formula:** Z = Assign freely in specified range

**Example:** 10.1.1.**101** (This IP address belongs to a server that addressed under the specified facility’s network)

**Z3:**

**Range:** [201-254]

**Purpose:** Uncategorized device addressing

**Explanation:** Reserved for other devices that requires IP addressing in facilities. These device types are including but not limited to IP cameras, NAS devices, SCADA systems and medical devices.

**Formula:** Z = Assign freely in specified range

**Example:** 10.1.1.**201** (This IP address belongs to an IP camera that addressed under the specified facility’s network)

1. **Addressing Between the Facilities (Inner Transit Networks)**

10.X.Y.Z0/24

**X:**

**Range:** [1-254]

**Purpose:** BID (Branch Identifier)

**Explanation:** Reserved to represent the branch which this inner transit network is a part of.

**Formula:** X = Branch No

**Example:** 10.**1**.101.1 (This inner transit network resides in the first branch of the company)

**Y:**

**Range:** [101-200]

**Purpose:** ITNID (Inner Transit Network Identifier)

**Explanation:** Reserved to represent the inner transit network uniquely but provides no specific information about the network being addressed.

**Formula:** Y = Assign freely in specified range

**Example:** 10.1.**101**.1 (This is an ITN and its ITNID is 101)

**Z:**

**Z1:**

**Range:** [1-100]

**Purpose:** SFID (Source Facility Identifier)

**Explanation:** Reserved to represent the source facility’s gateway that is a part of this inner transit network.

**Formula:** Z = Source Facility no

**Example:** 10.1.101.**1** (This IP address represents an ITN and belongs to the first facility’s gateway in the specified branch)

**Z2:**

**Range:** [101-200]

**Purpose:** BGID (Border Gateway Identifier)

**Explanation:** Reserved to represent uniquely the specified branch’s border gateway.

**Formula:** Z = Assign freely in specified range

**Example:** 10.1.101.**101** (This IP address represents an ITN and belongs to the specified branch’s border gateway with the ID 101)

1. **Addressing Between the Branches (Outer Transit Networks)**

10.0.Y.Z/24

**Y:**

**Range:** [1-254]

**Purpose:** OTNID (Outer Transit Network Identifier)

**Explanation:** Reserved to represent the outer transit network uniquely but provides no specific information about the network being addressed.

**Formula:** Y = Assign freely in specified range

**Example:** 10.0.**101**.1 (This is an OTN and its OTNID is 101)

**Z:**

**Range:** [1-254]

**Purpose:** SBID (Source Branch Identifier)

**Explanation:** Reserved to represent the source branch’s border gateway that is a part of this outer transit network.

**Formula:** Z = Assign freely in specified range

**Example:** 10.0.101.**1** (This IP address belongs to the first branch’s border gateway that is a part of this OTN)

Overall, it is so easy to understand the meanings of the IP addresses when seen one. We even considered writing a Python script to give the meaning of any address to the network manager but because the current complexity of the network is not unbearable, we decided to postpone that development.

### Routing

We definitely wanted to use a dynamic routing protocol. We tried RIPv1, RIPv2 but these protocols were classful routing protocols, making our routing almost impossible due to classful nature of our IP addressing specifications. We later researched current standards like BGP and OSPF and we finally decided to use OSPF.

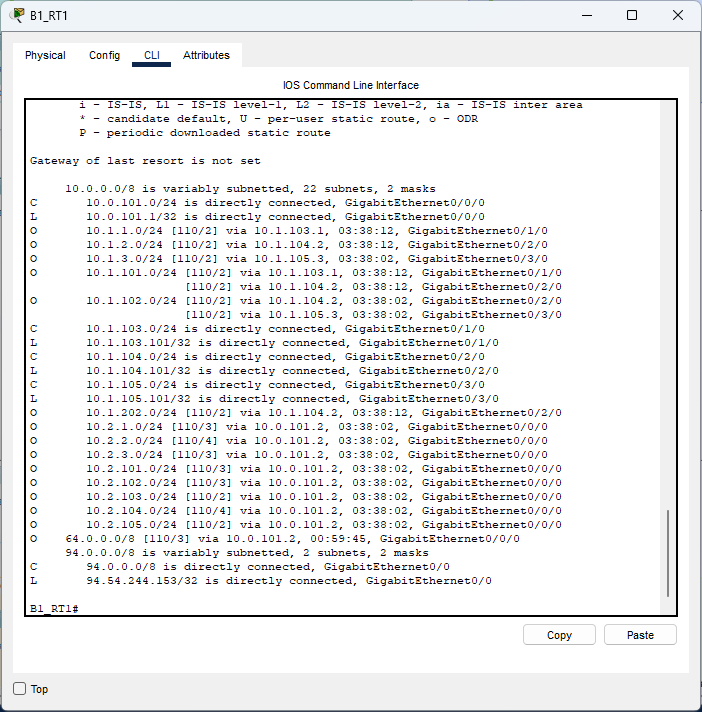


Figure 4.1: `show IP route` command used on B1\_RT

OSPF (Open Shortest Path First) is a popular routing protocol used in metropolitan area networks (MANs) due to its scalability, efficiency, and reliability. In this answer, we will explain why OSPF is a good choice for a MAN and how it is applied in technical detail.

First, let's discuss why OSPF is a good choice for a MAN. OSPF is a link-state routing protocol, which means that each router in the network has a complete map of the entire network topology. This allows OSPF to quickly and efficiently calculate the shortest path between any two routers in the network. Additionally, OSPF uses a hierarchical structure, which allows for easy scalability as the network grows. OSPF also supports load balancing, which allows traffic to be spread across multiple paths, improving network performance.

Now, let's discuss how OSPF is applied in a MAN. The first step in implementing OSPF is to configure OSPF on each router in the network. This involves specifying the network interfaces that OSPF should use to communicate with other routers and assigning each interface to a specific OSPF area. OSPF areas are used to organize the network topology into smaller, more manageable segments.

Once OSPF has been configured on each router, the routers will begin exchanging OSPF packets to build a complete map of the network topology. This process is called the OSPF adjacency process and involves the exchange of OSPF hello packets, which are used to establish and maintain neighbor relationships between routers. Once OSPF adjacency has been established between two routers, they will exchange their link-state information to build a complete map of the network topology.

Once the network topology has been established, OSPF routers use the Dijkstra algorithm to calculate the shortest path between any two routers in the network. OSPF supports multiple metrics for calculating path costs, including bandwidth, delay, and hop count. By default, OSPF uses the shortest path based on the number of hops between routers, but this can be adjusted to use other metrics if desired.

One of the benefits of OSPF is that it supports load balancing, which allows traffic to be spread across multiple paths. OSPF uses equal cost multipath (ECMP) load balancing, which means that if there are multiple paths with the same cost, OSPF will distribute traffic evenly across those paths. This can improve network performance by preventing congestion on any one path.

# Traffic Analysis and Simulation Results

We will analyze and evaluate our network simulation through given scenarios. These scenarios are real-world examples of how users will use our network.

## Scenarios

### Scenario 1

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

#### Receiving The Email

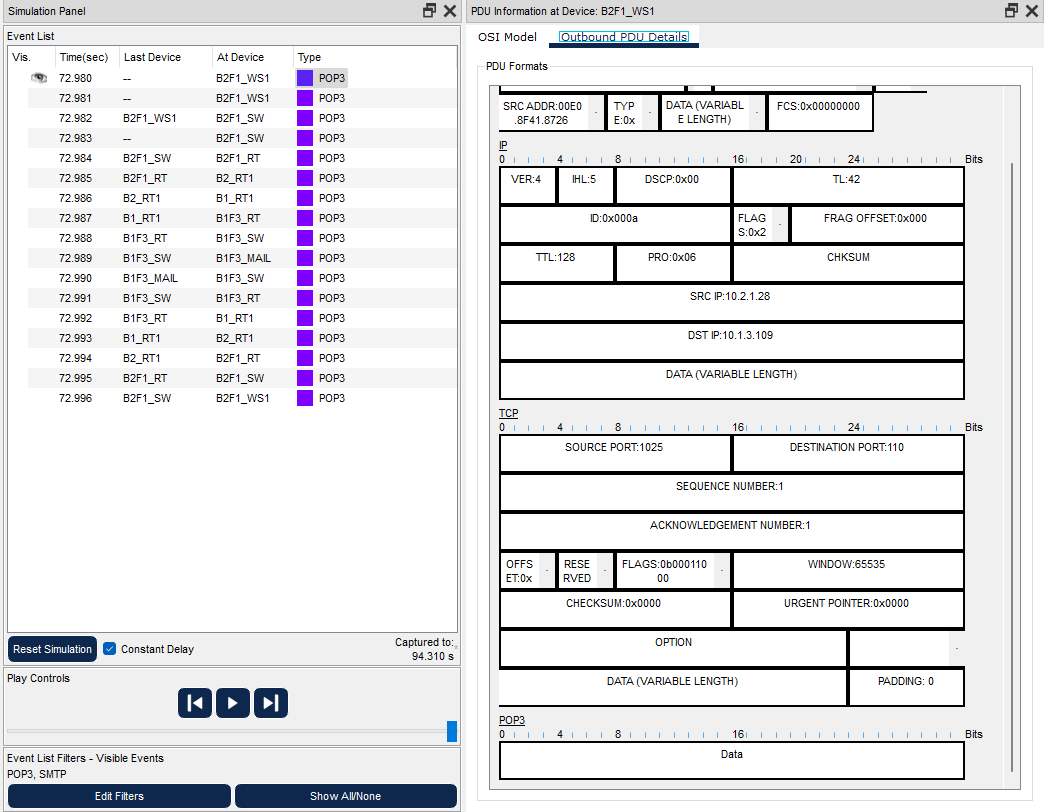


Figure 5.1: User’s computer sends ready to receive message to the mail server

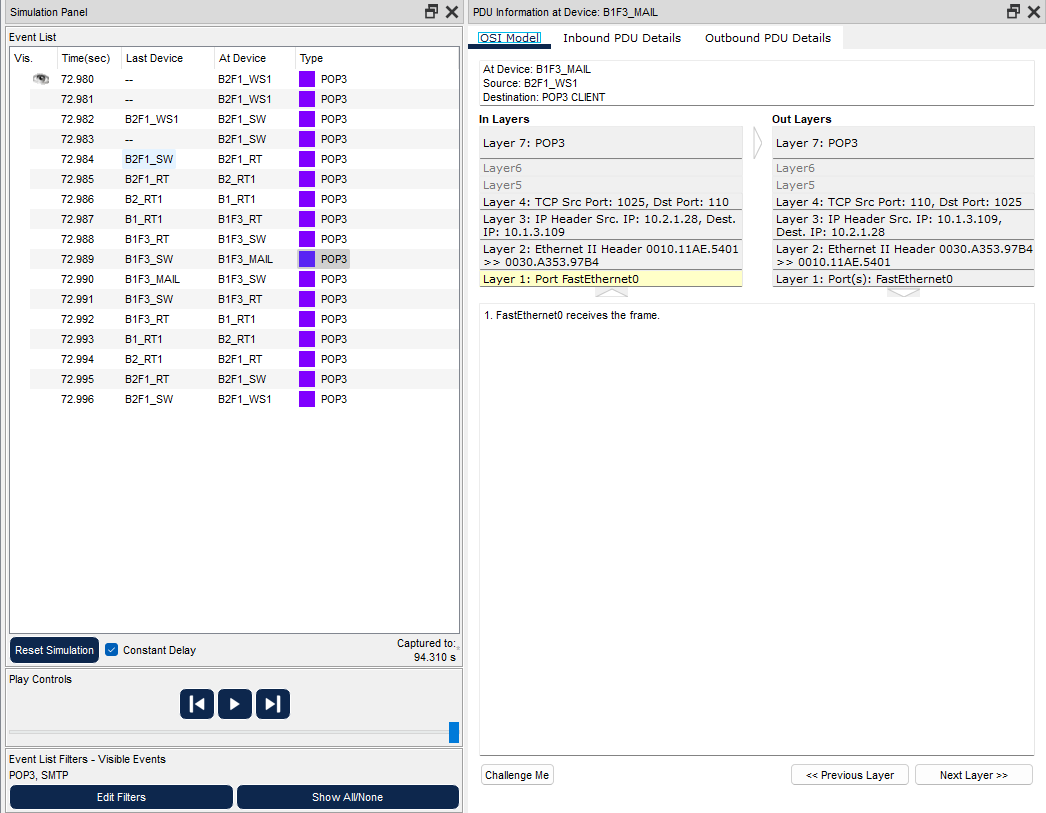


Figure 5.1: Server receives the request

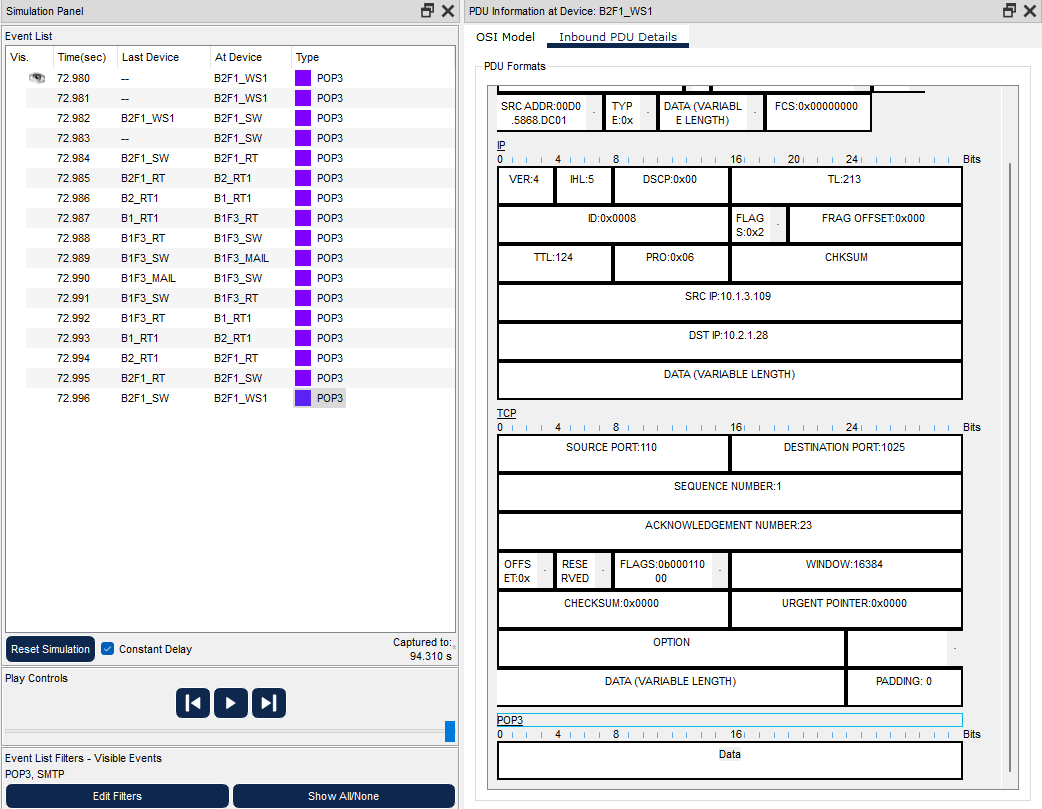


Figure 5.3: User’s PC receives the mail.

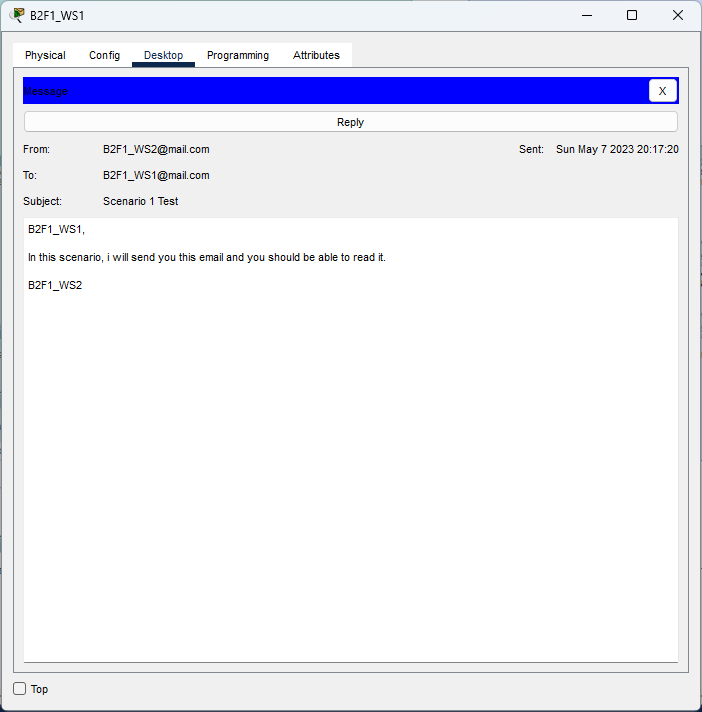


Figure 5.4: Received mail

#### Browsing The Web

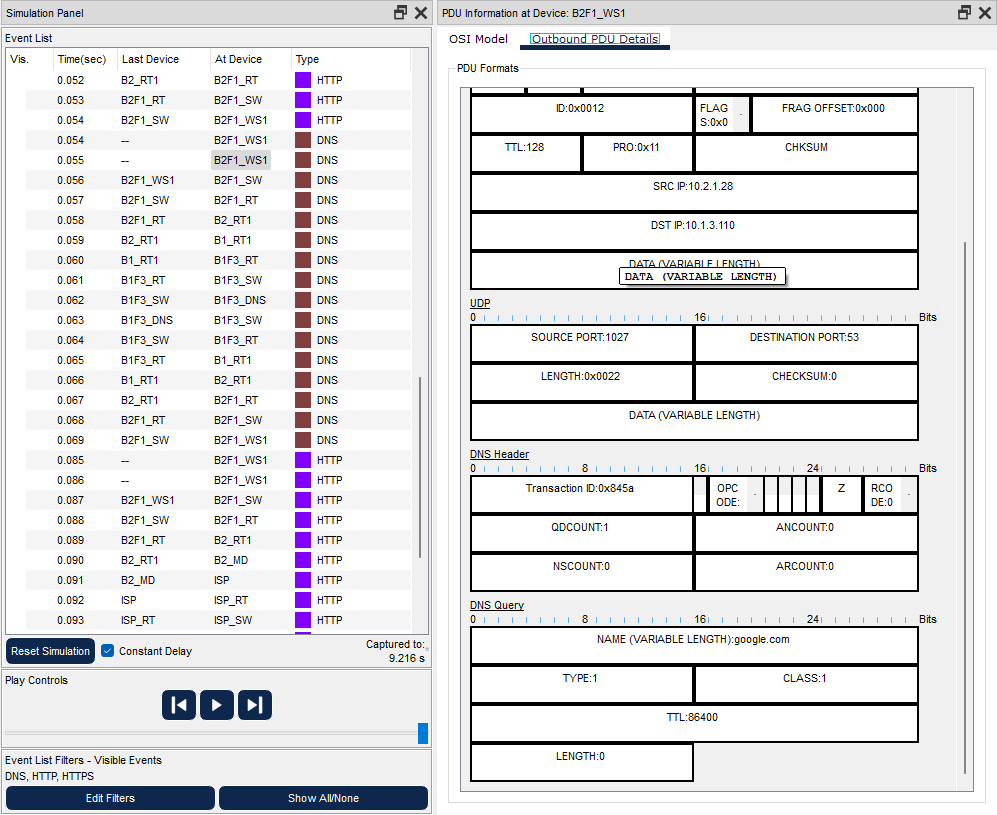


Figure 5.5: DNS query sent from the user’s computer

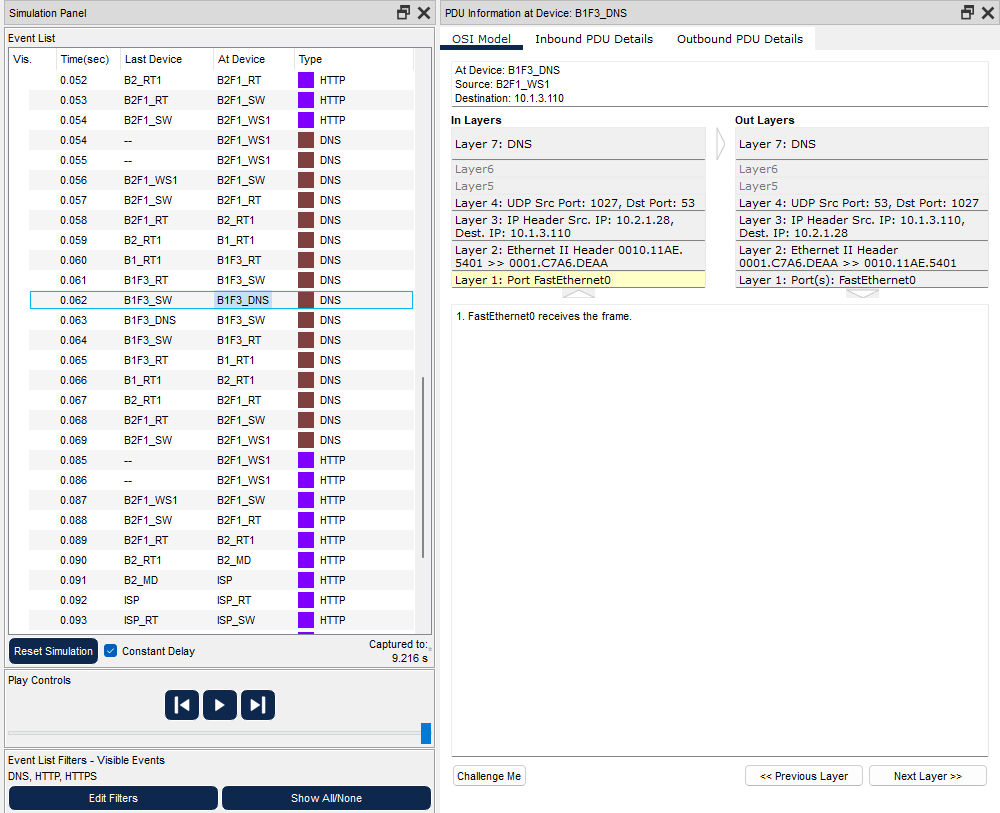


Figure 5.6: DNS server receives the query; queried website is cached thus answers from its cache

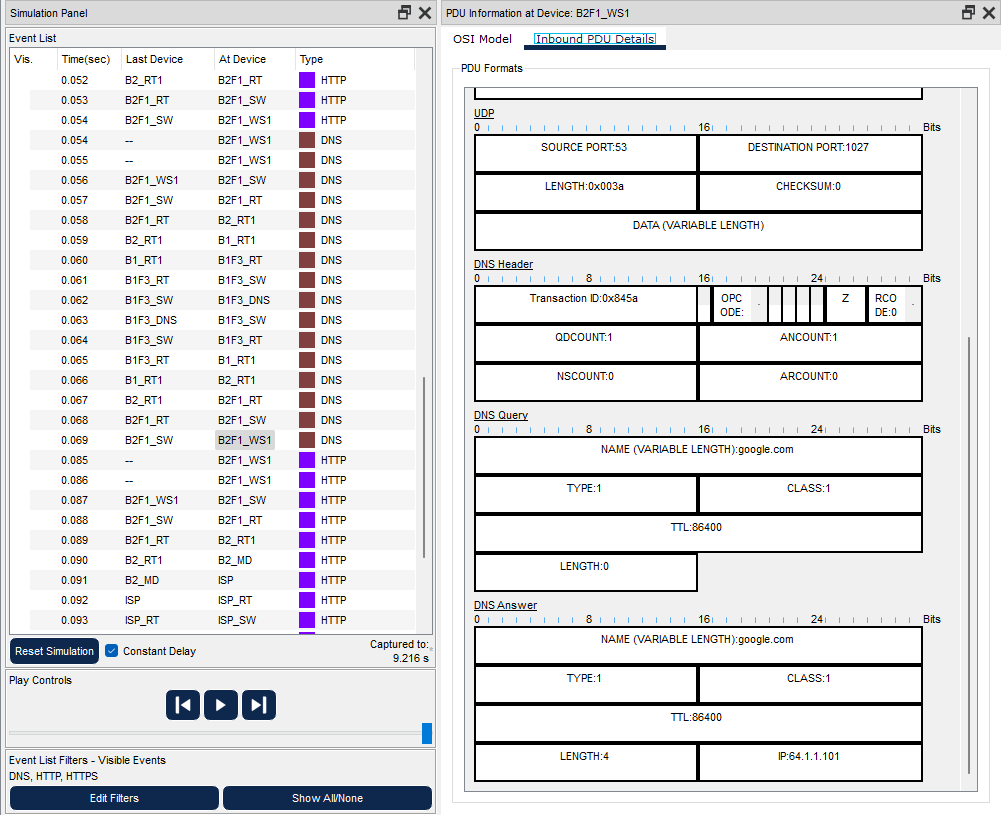


Figure 5.7: DNS query resulted with success and user’s PC receives the IP address

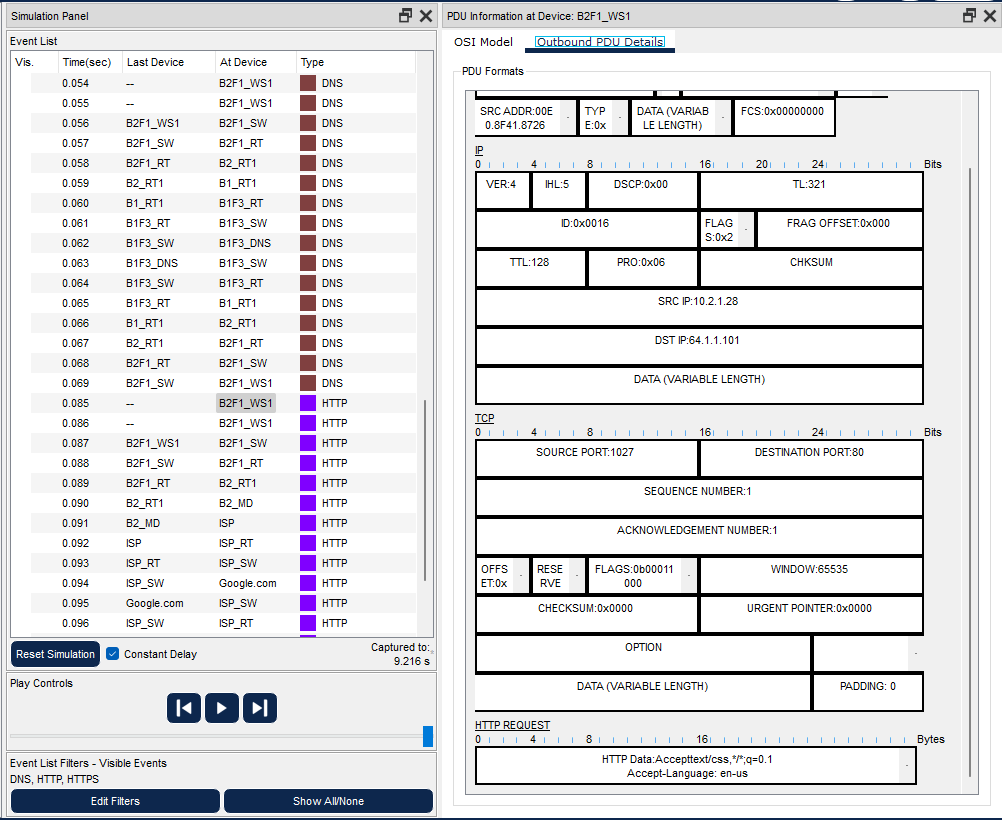


Figure 5.8: User’s PC sends and HTTP request to Google’s server

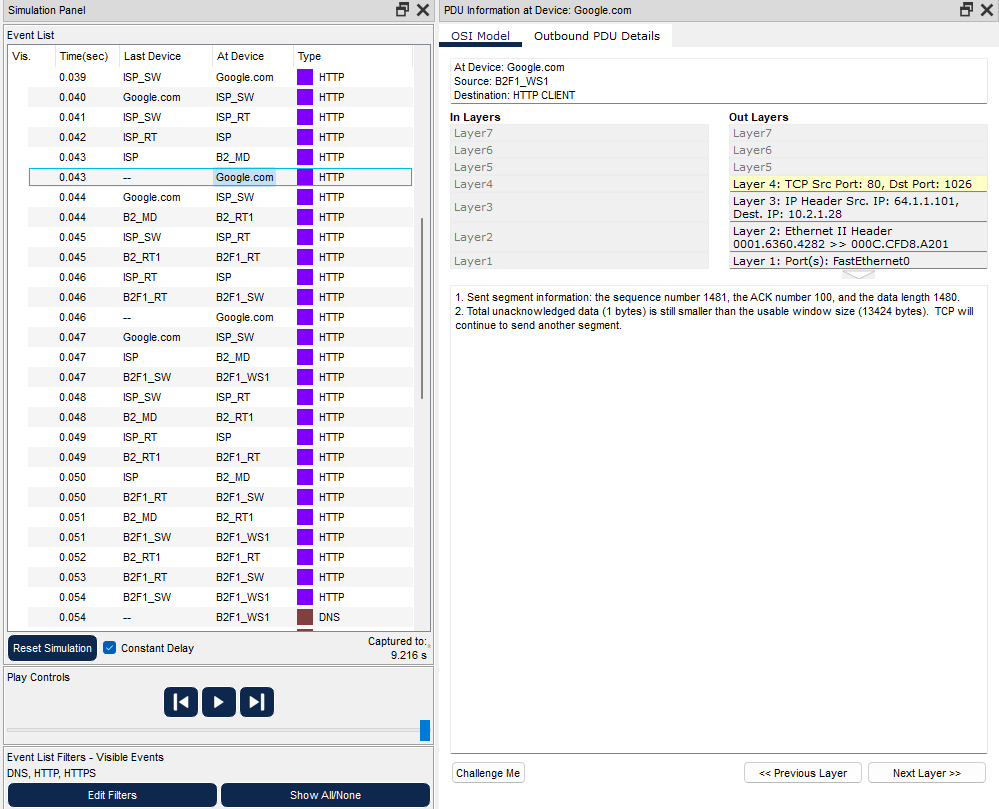


Figure 5.9: Google’s server receives the request

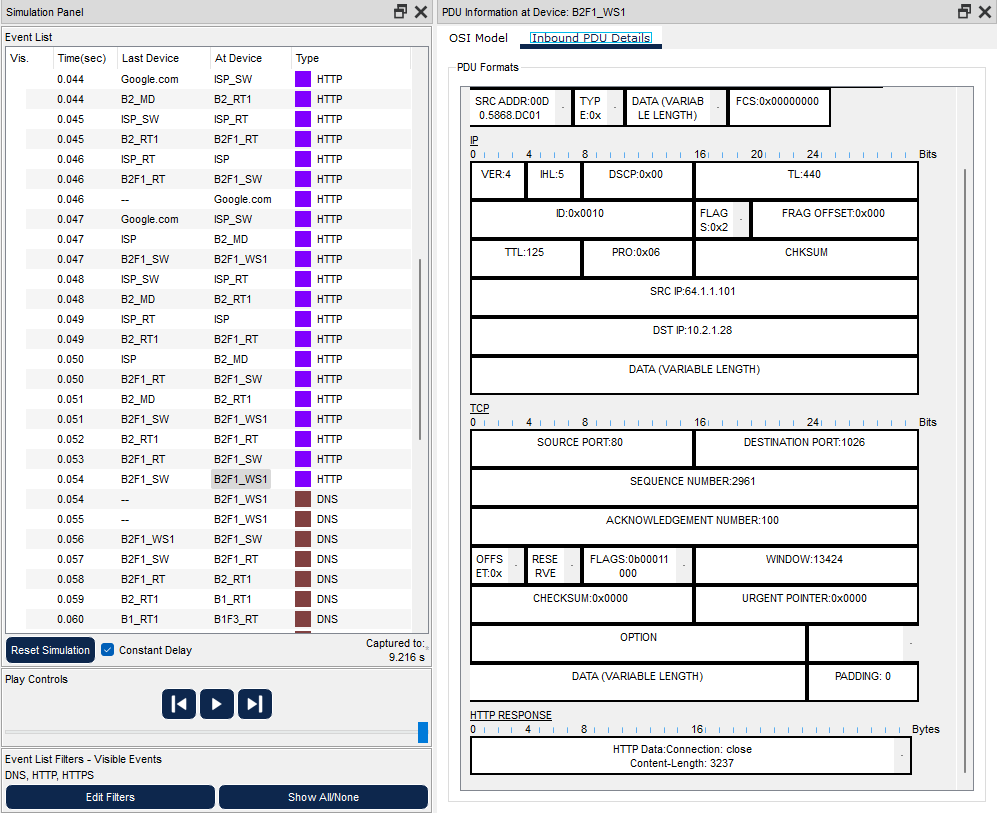


Figure 5.10: Some arbitrary number of requests and answers happen

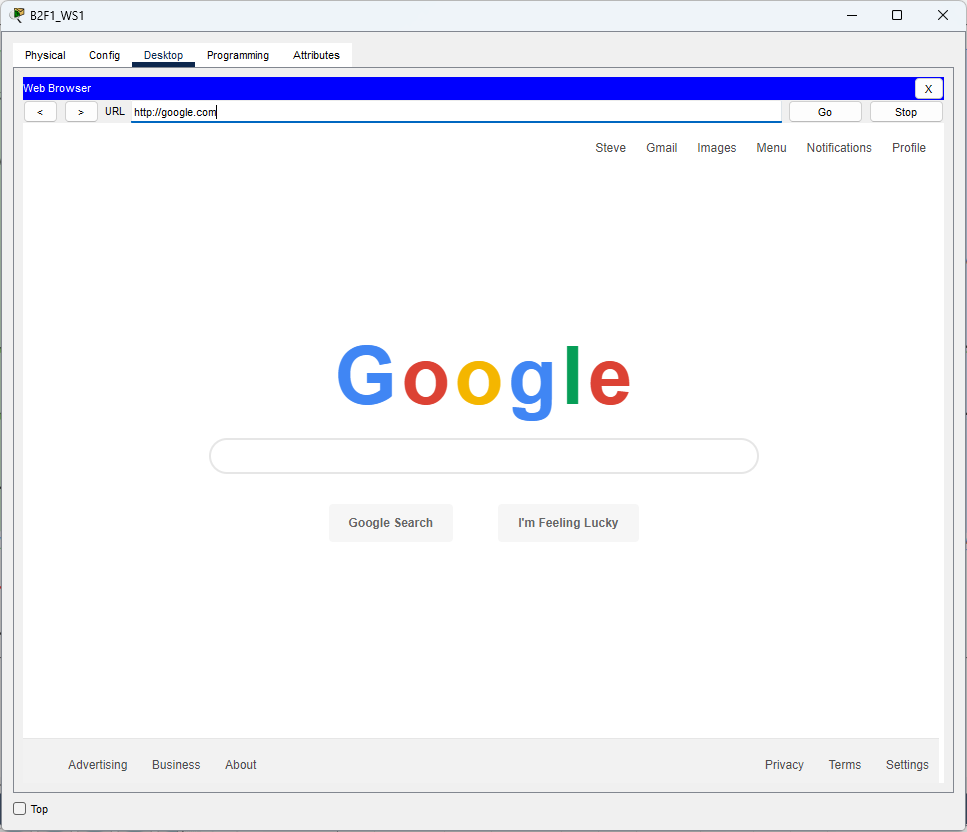


Figure 5.11: User is able to browse the Web

### Scenario 2

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

#### Upload to FTP

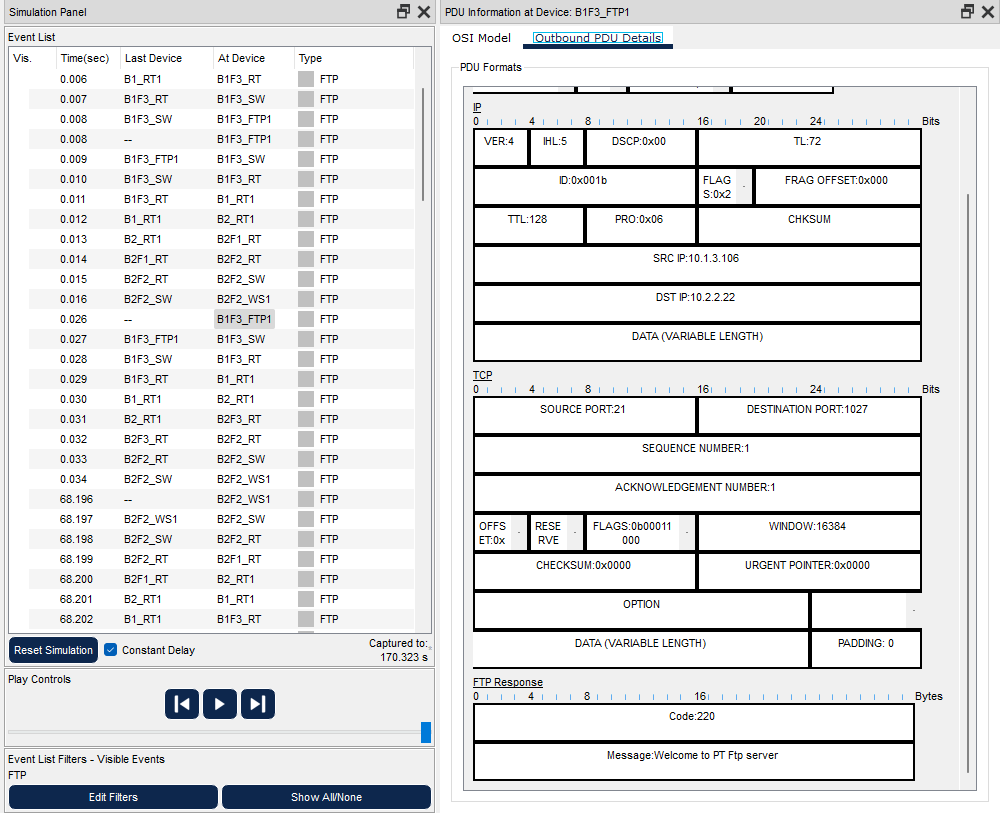


Figure 5.12: FTP Server sends welcome message to the user

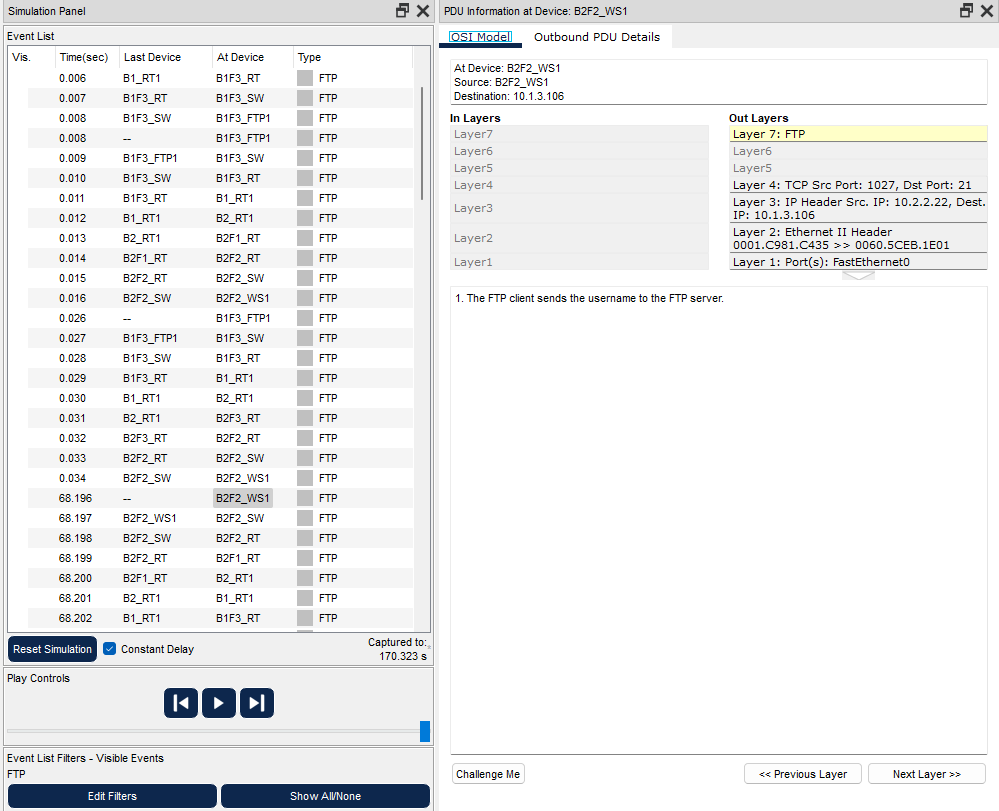


Figure 5.13: User types username

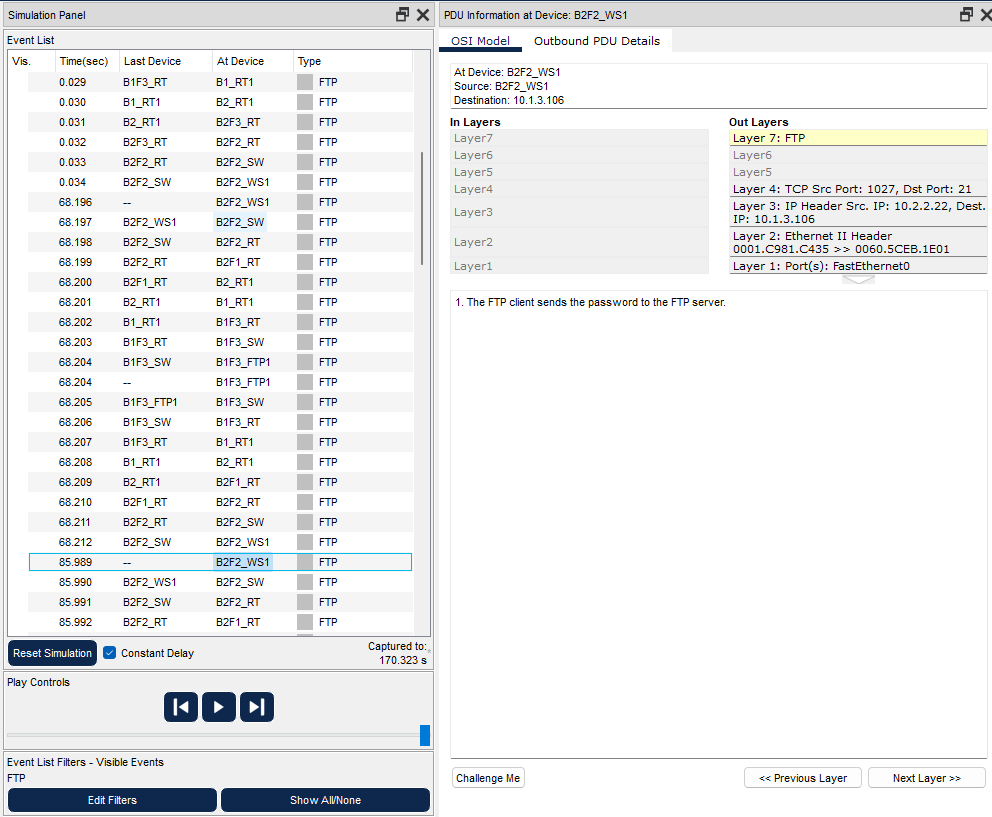


Figure 5.14: User sends password

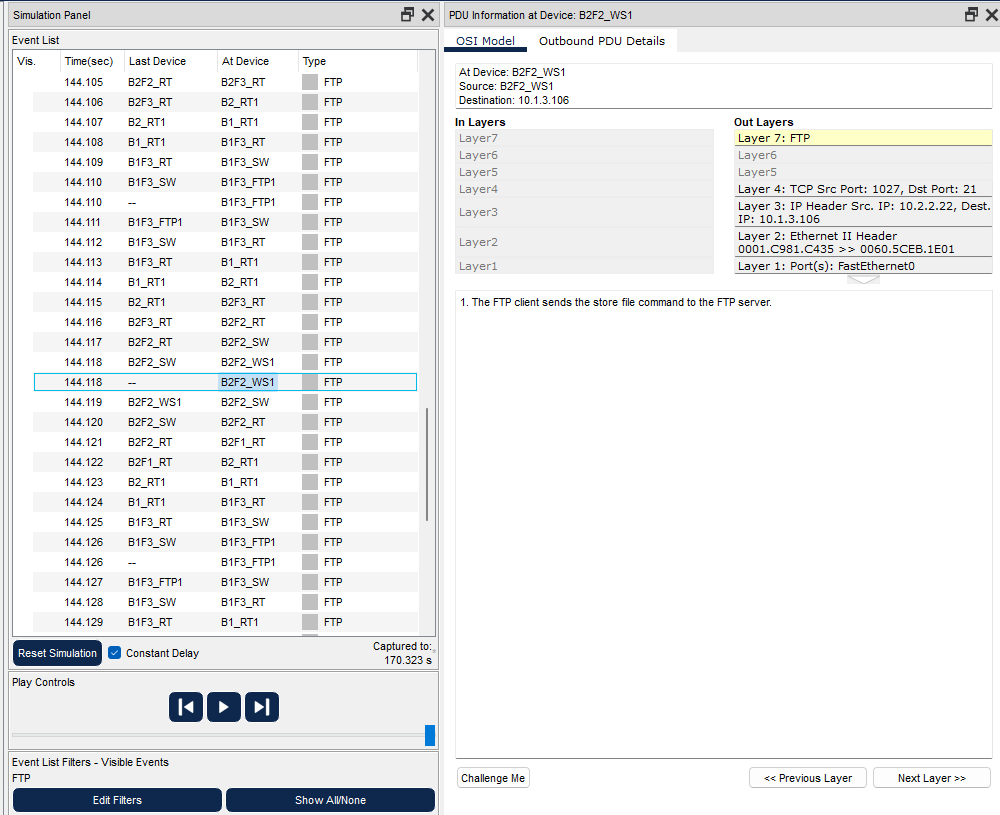


Figure 5.15: User sends the file

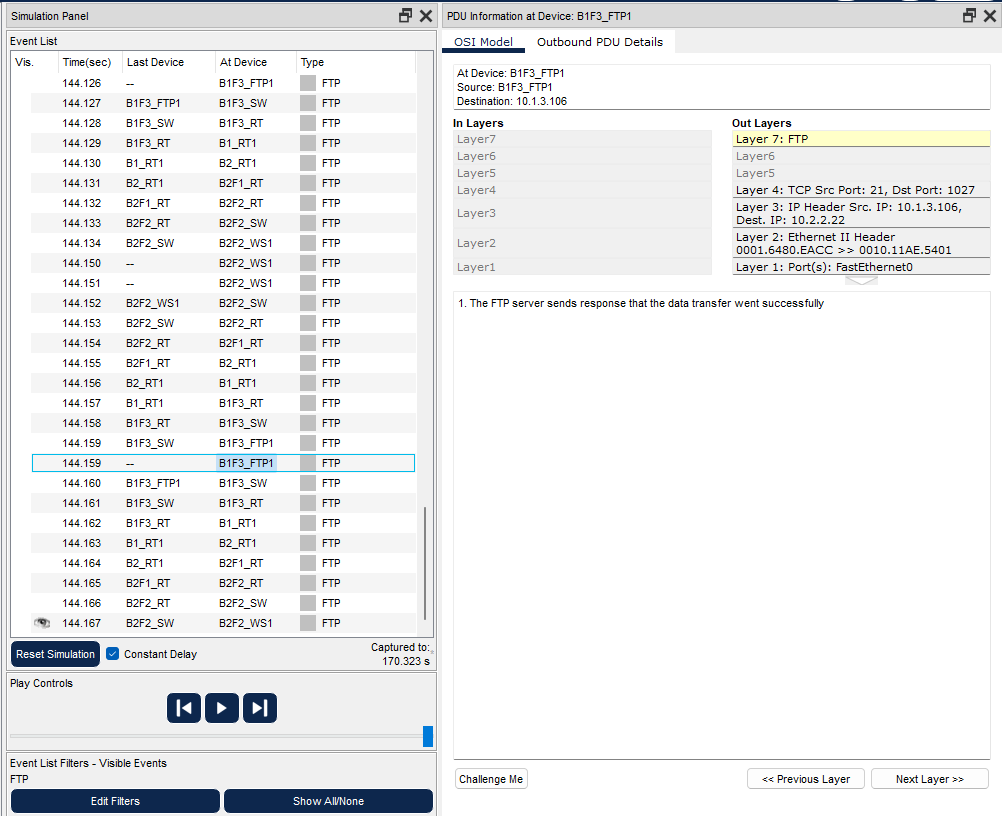


Figure 5.16: Server informs the user that transfer was successful

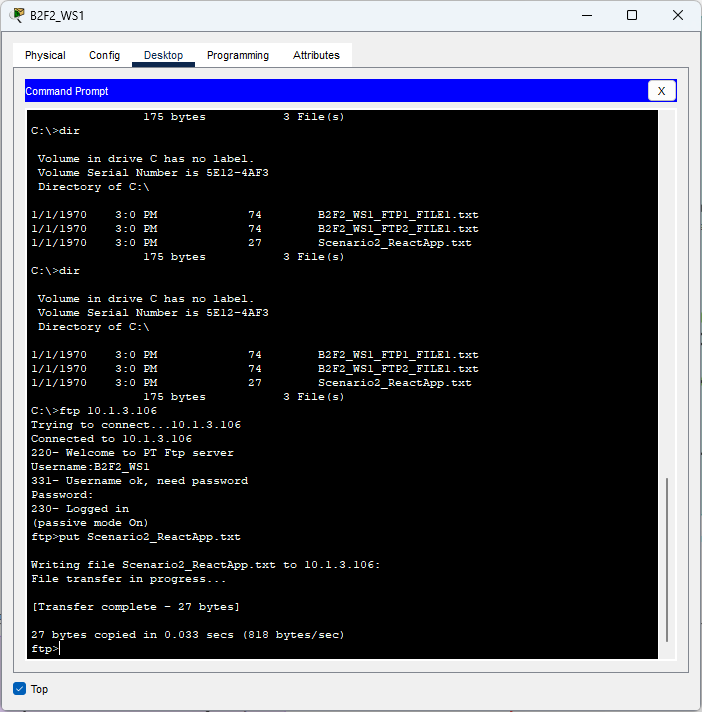


Figure 5.17: User is able to upload a file to the FTP server

### Scenario 3

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

#### VoIP Conference

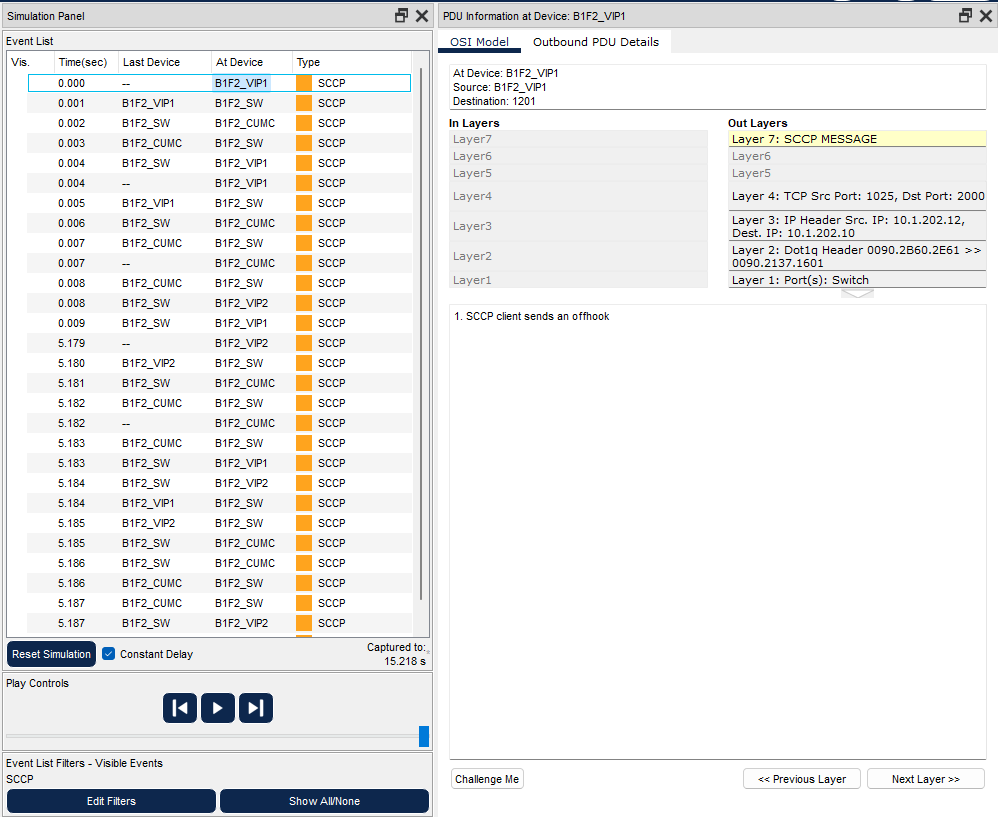


Figure 5.18: First phone sends off hook message

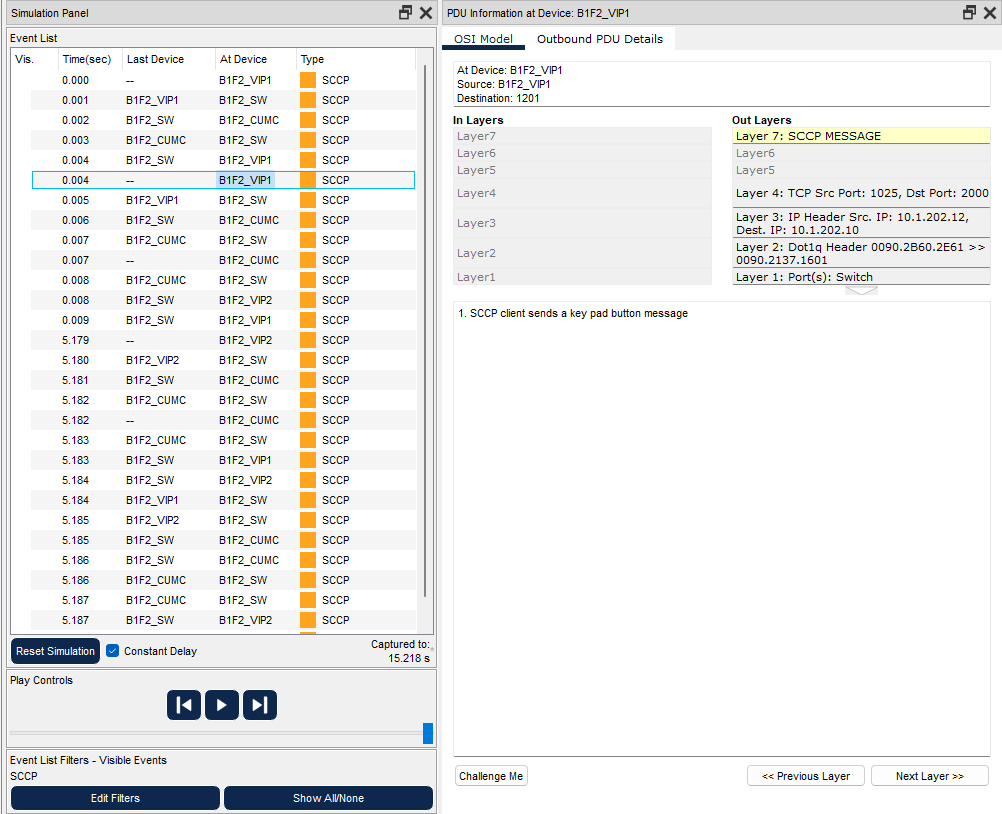


Figure 5.19: First phone sends a key pad button message

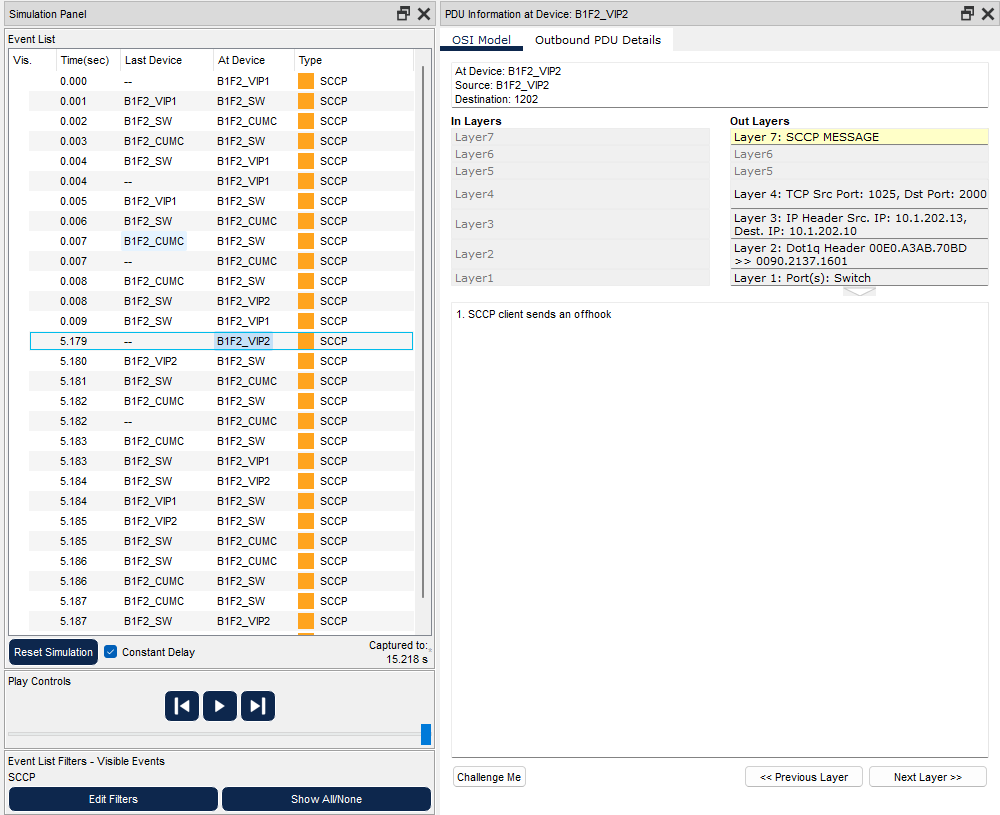


Figure 5.20: Second phone sends off hook message

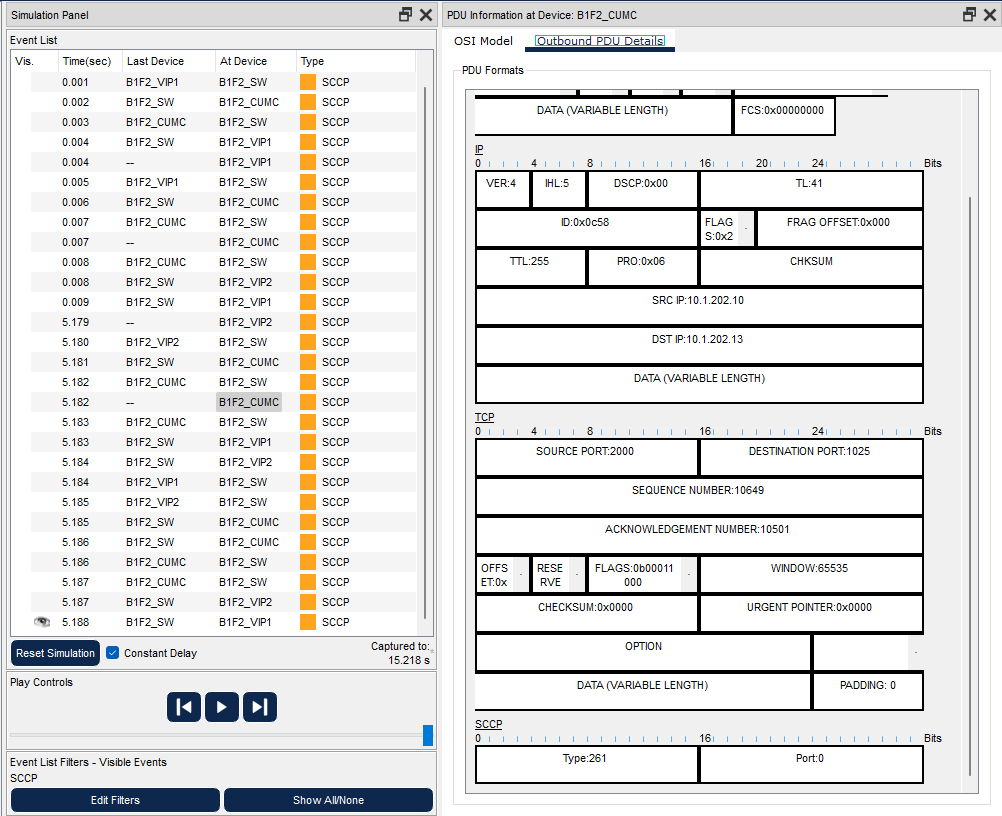


Figure 5.21: CUCM manages the communication

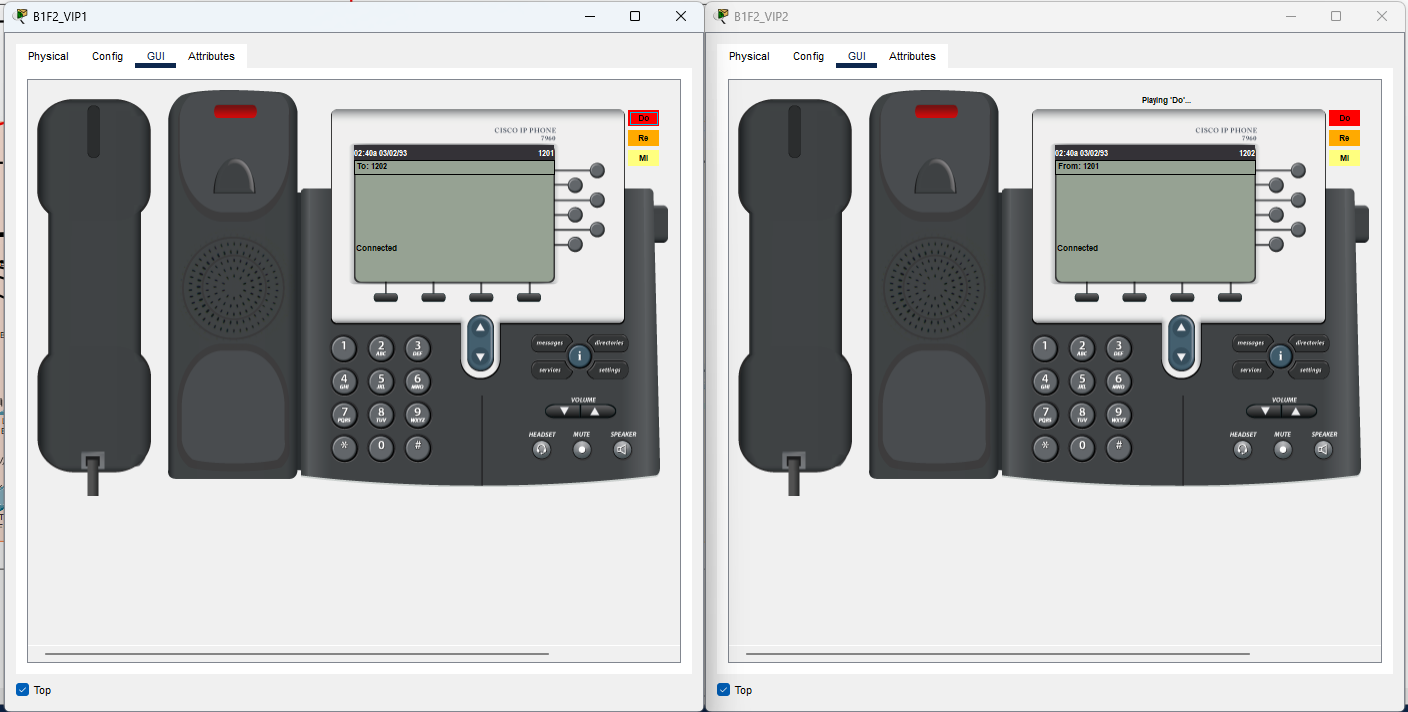


Figure 5.22: VoIP communication is established

### Scenario 4

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

#### Send & Receive Email

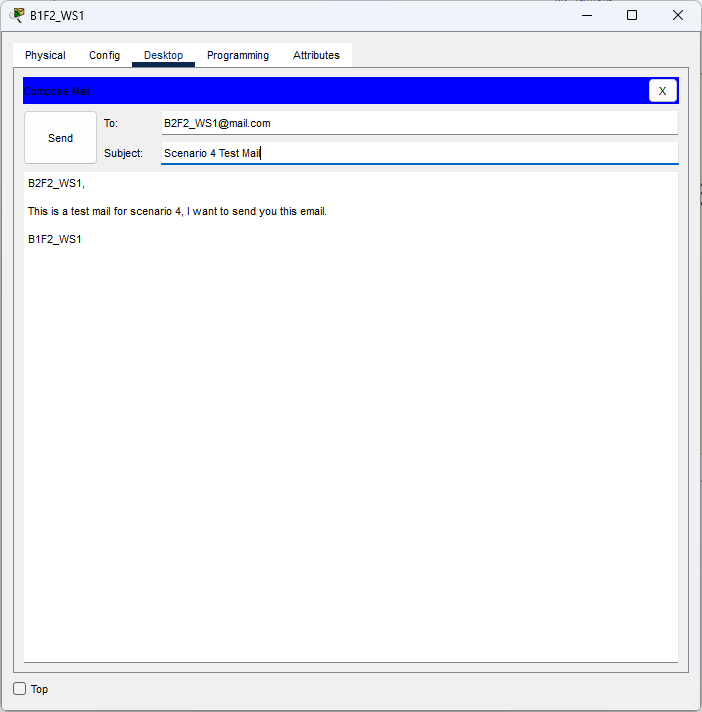


Figure 5.23: First user sends the email



Figure 5.24: SMTP message sent from the first PC

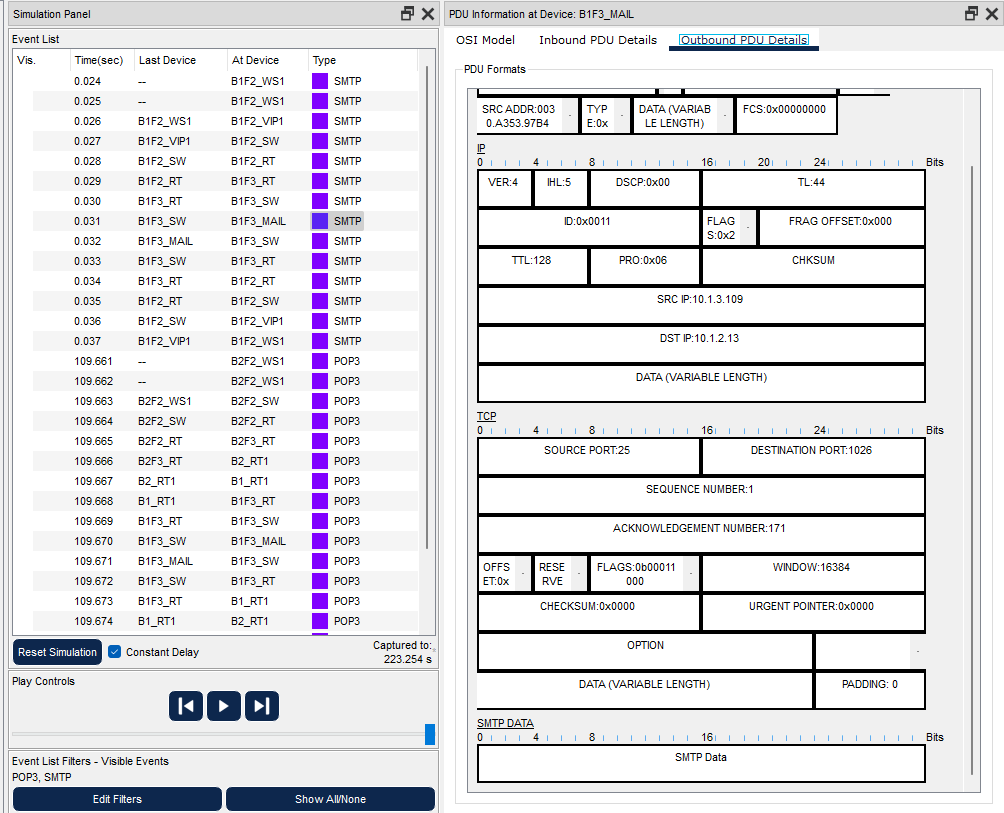


Figure 5.25: Mail server receives the frame

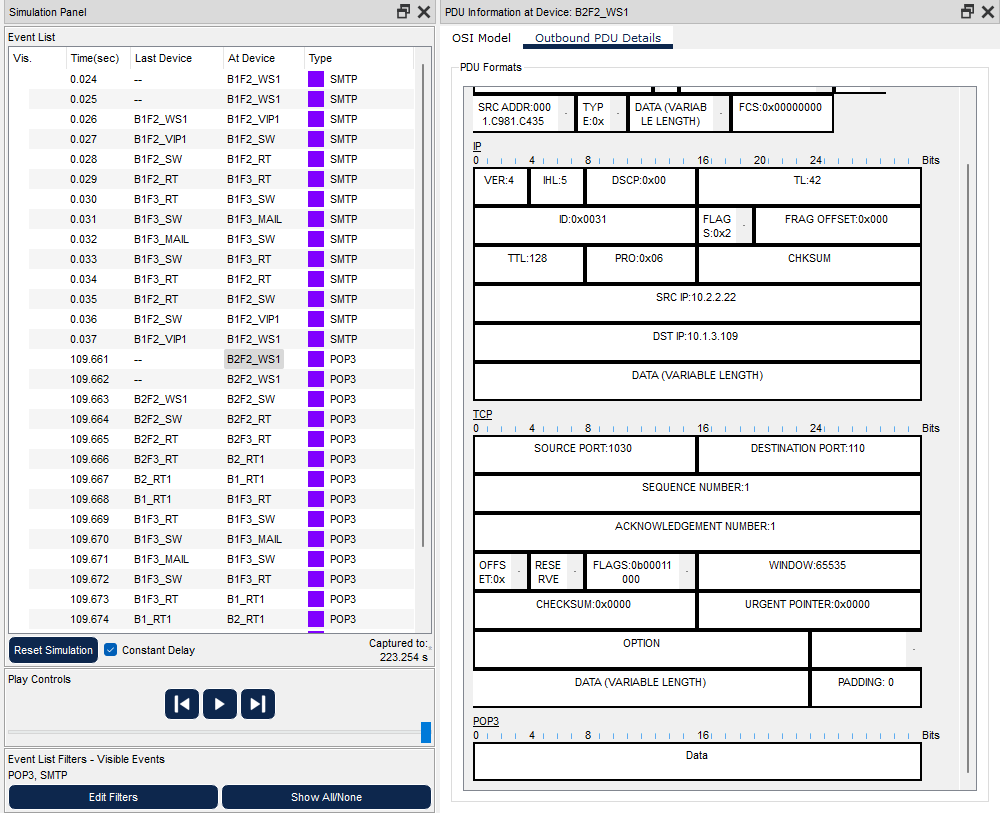


Figure 5.26: Second user presses receive button

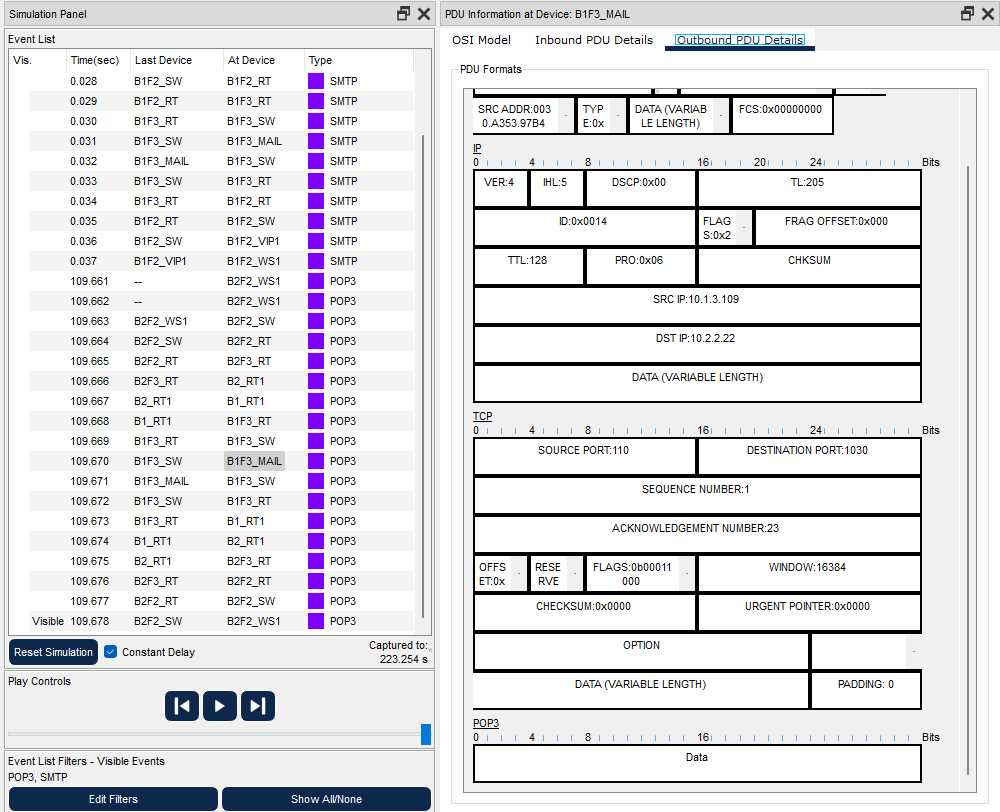


Figure 5.27: Mail server sent the email

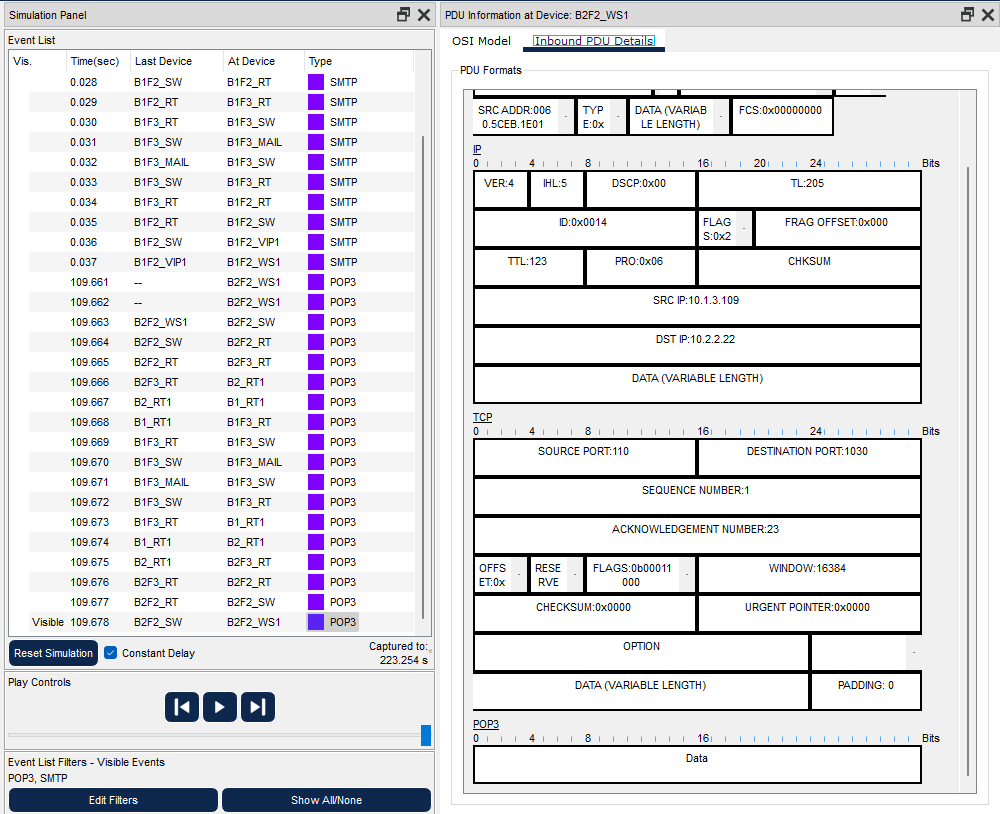


Figure 5.28: Email received by the receiving PC

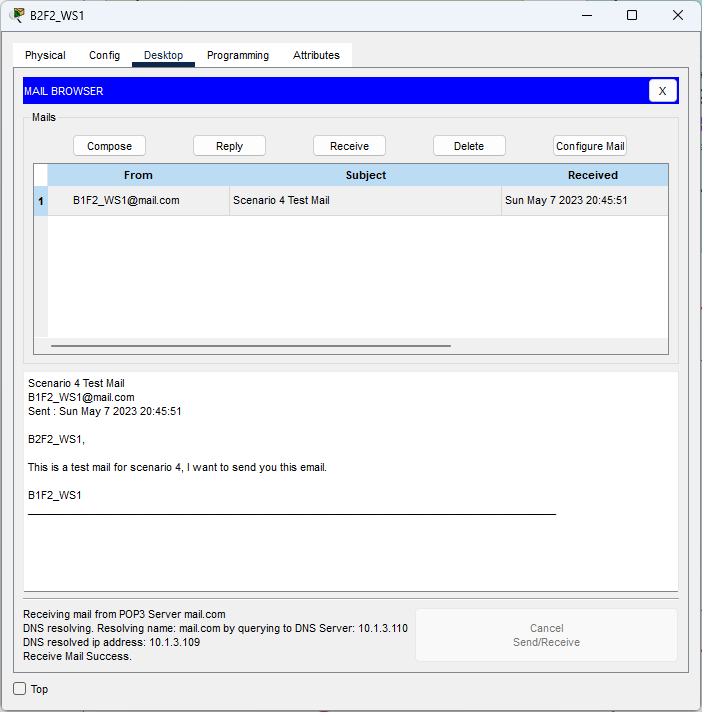


Figure 5.29: User reads the email

### Scenario 5

A user from first facility of second branch pings Web server of second facility of first branch. (There must be an error in the assignment paper, there is no web servers in the second facility of first branch, changed it to third facility of first branch)

#### Pinging

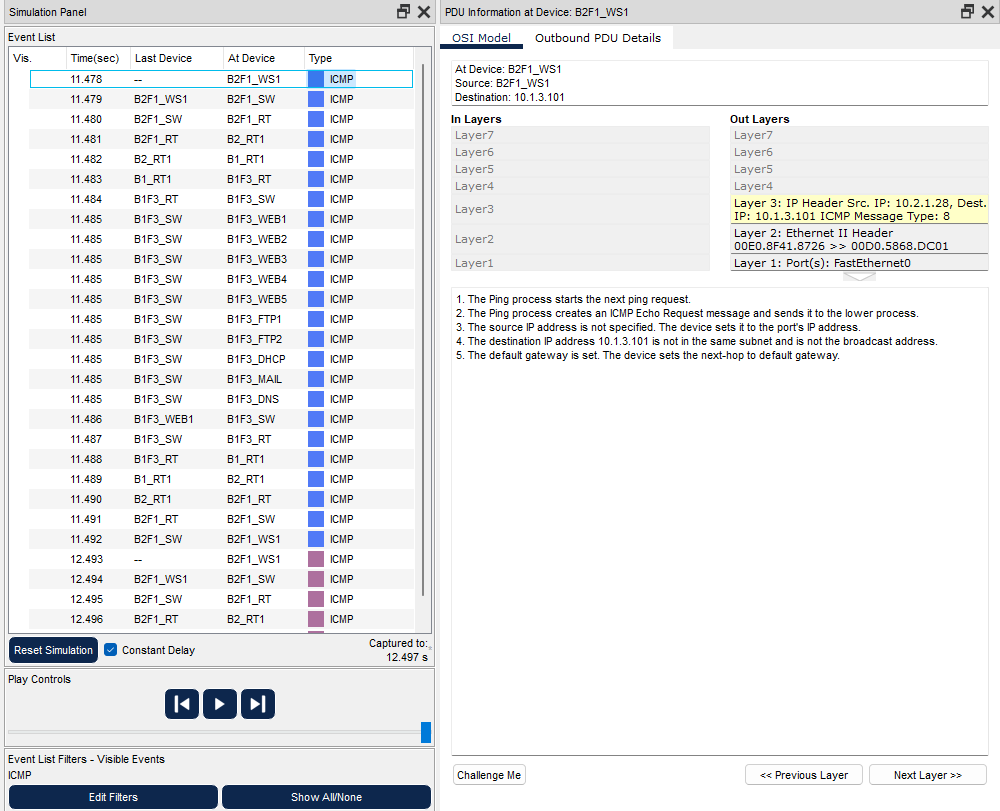


Figure 5.30: ICMP package has been sent from the user’s PC

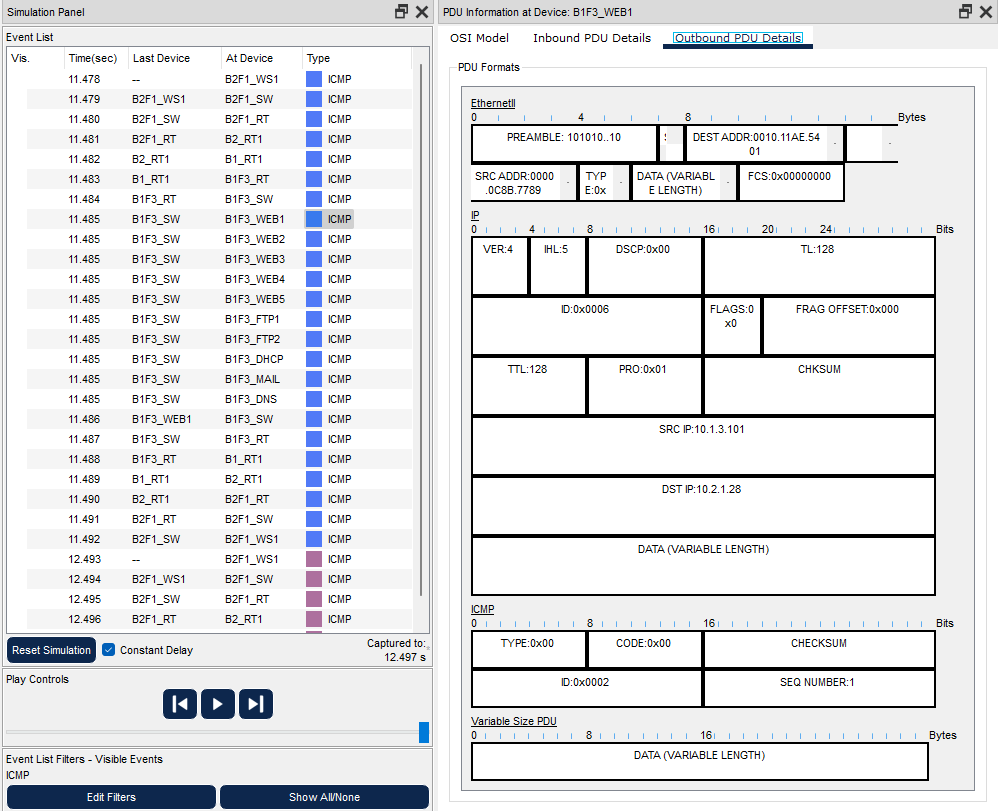


Figure 5.31: ICMP response sent from the web server

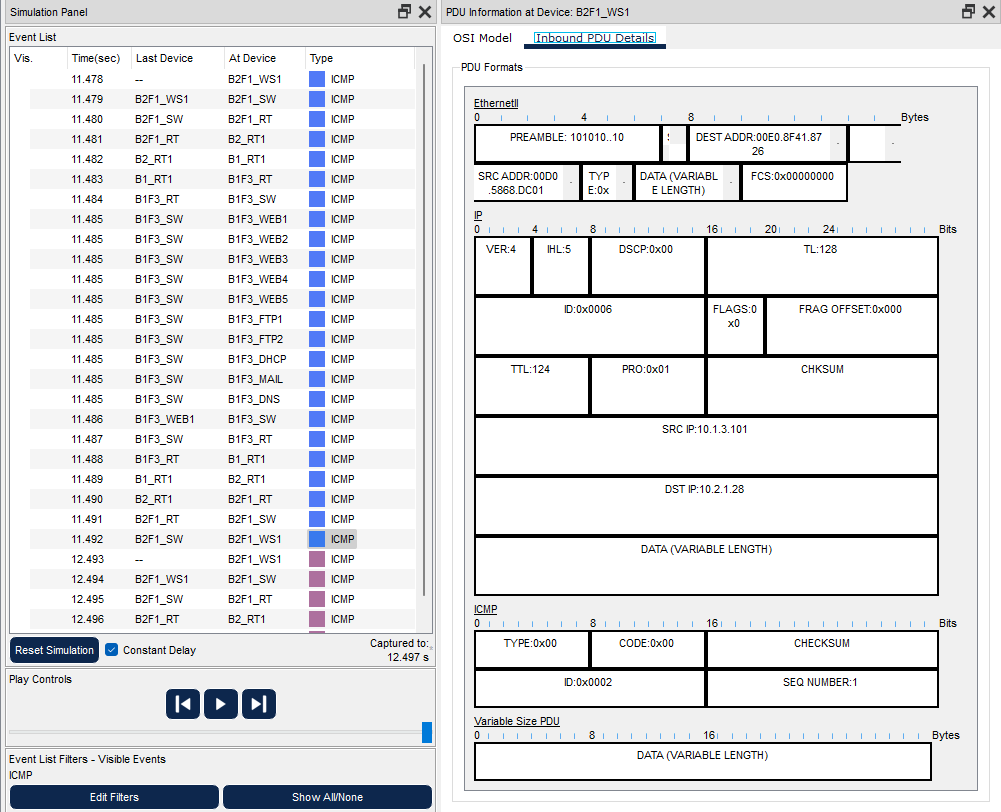


Figure 5.32: ICMP response received in the user’s computer

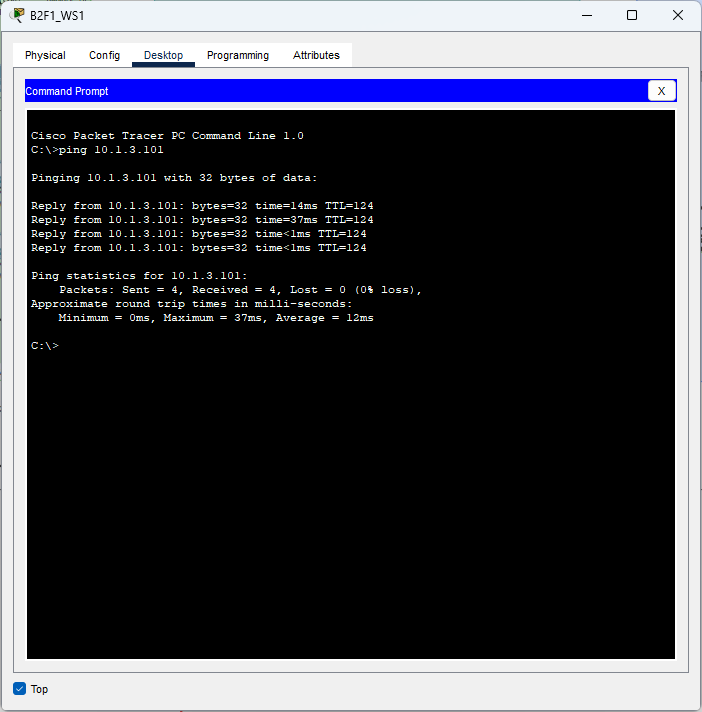


Figure 5.33: Pinging successful

### Scenario 6

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

#### Send Email

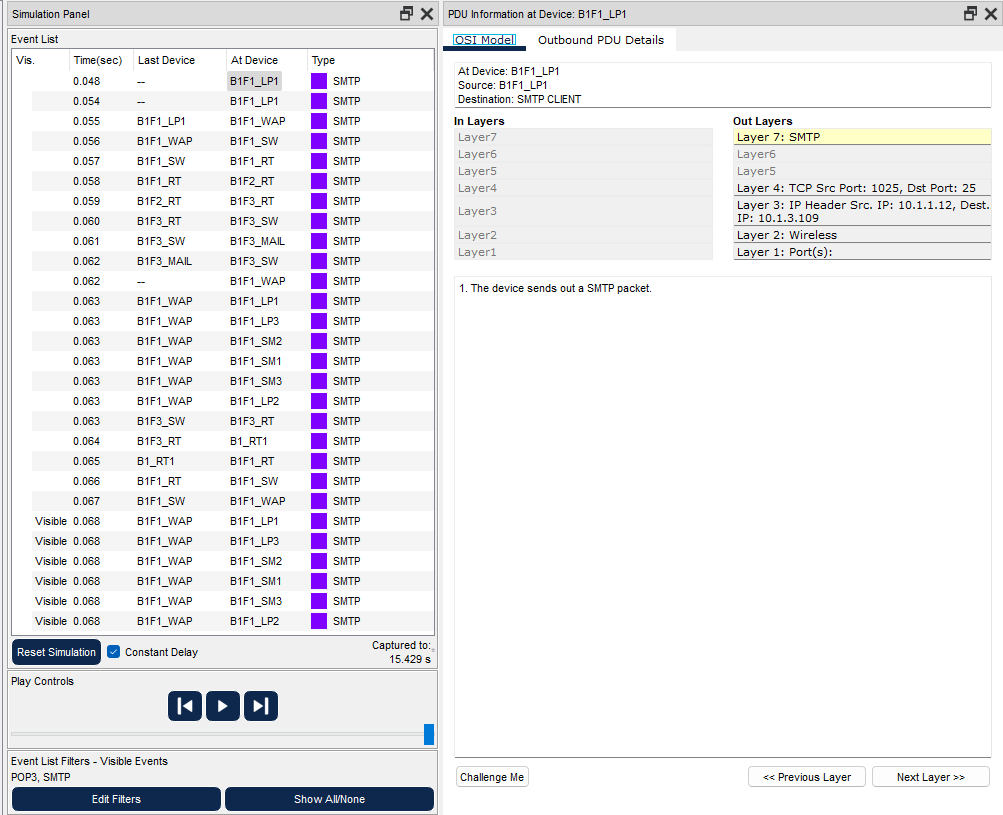


Figure 5.34: User sends the email

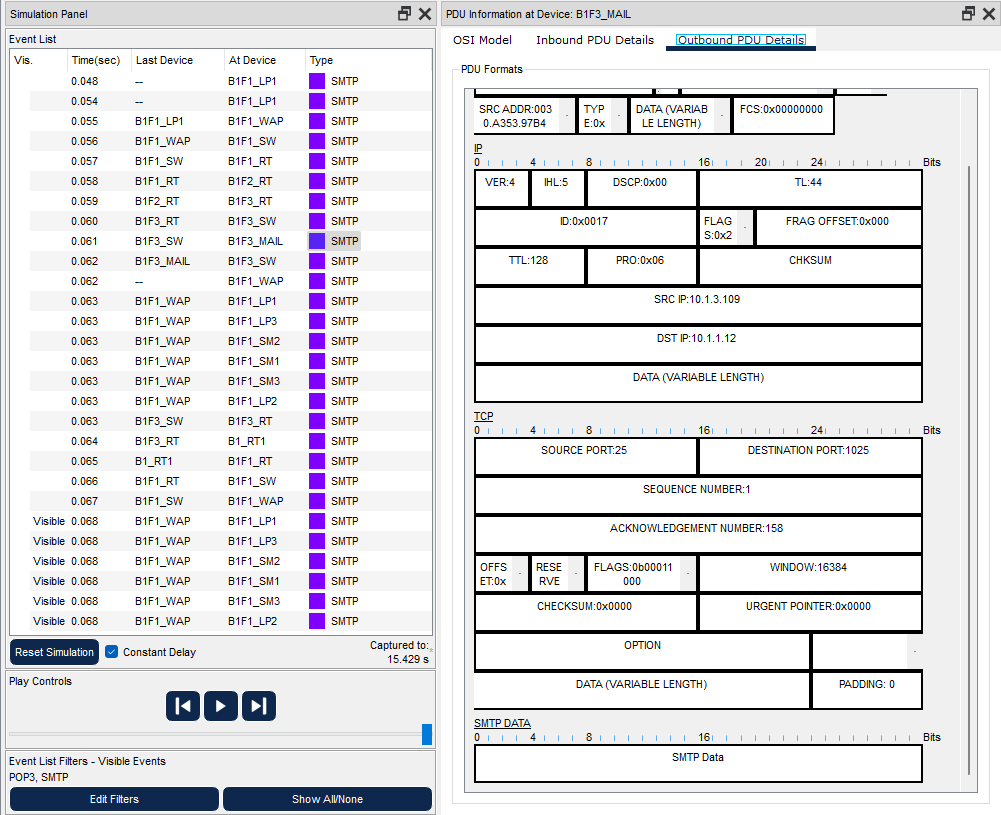


Figure 5.35: Server receives the mail, sends conformation

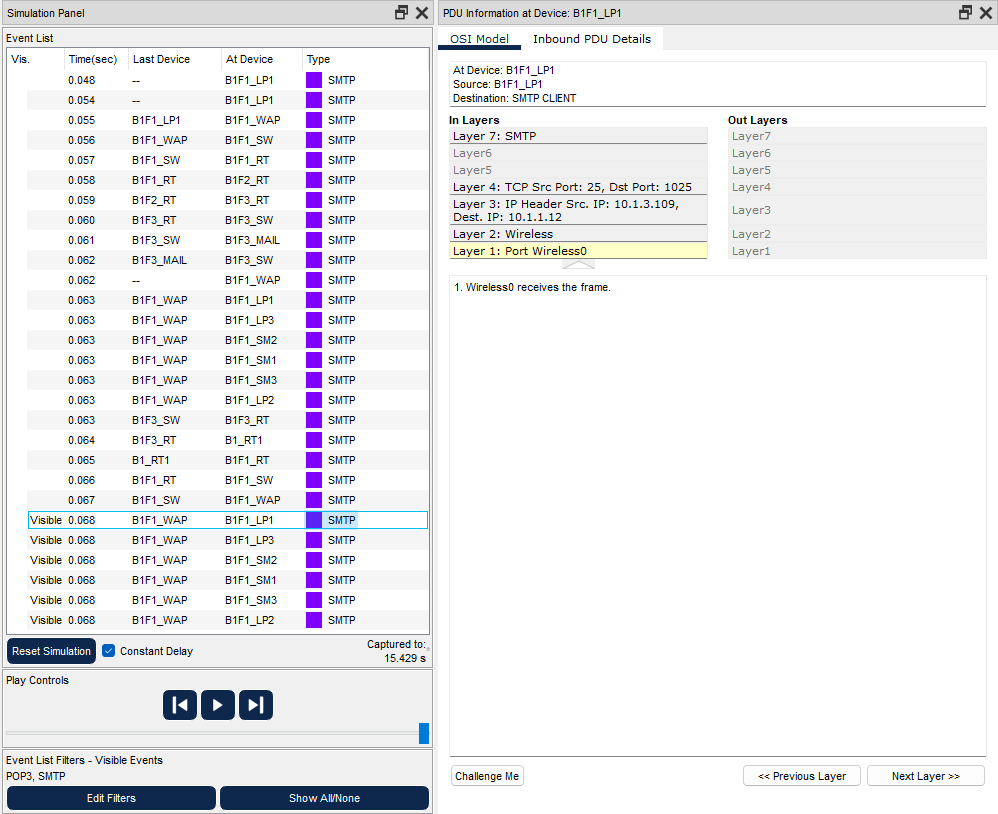


Figure 5.36: PC gets the conformation package

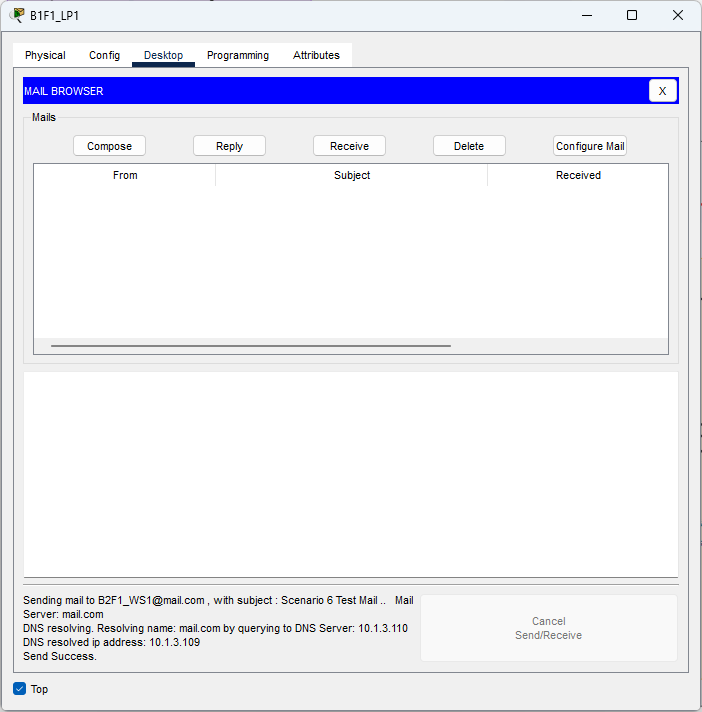


Figure 5.37: User has been informed

### Scenario 7

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 first branch office. (In Packet Tracer, SSH connections to devices other than network devices are not allowed thus We will only show the process.)

#### SSH Connection

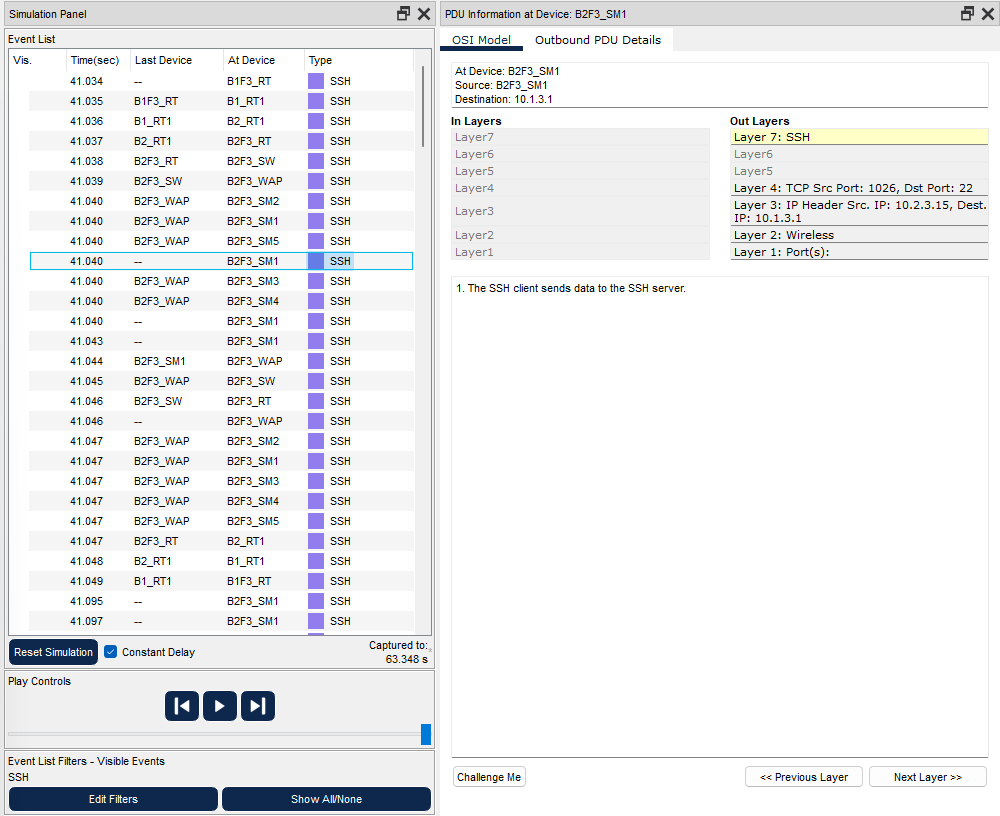


Figure 5.38: User tries to connect Web server via SSH

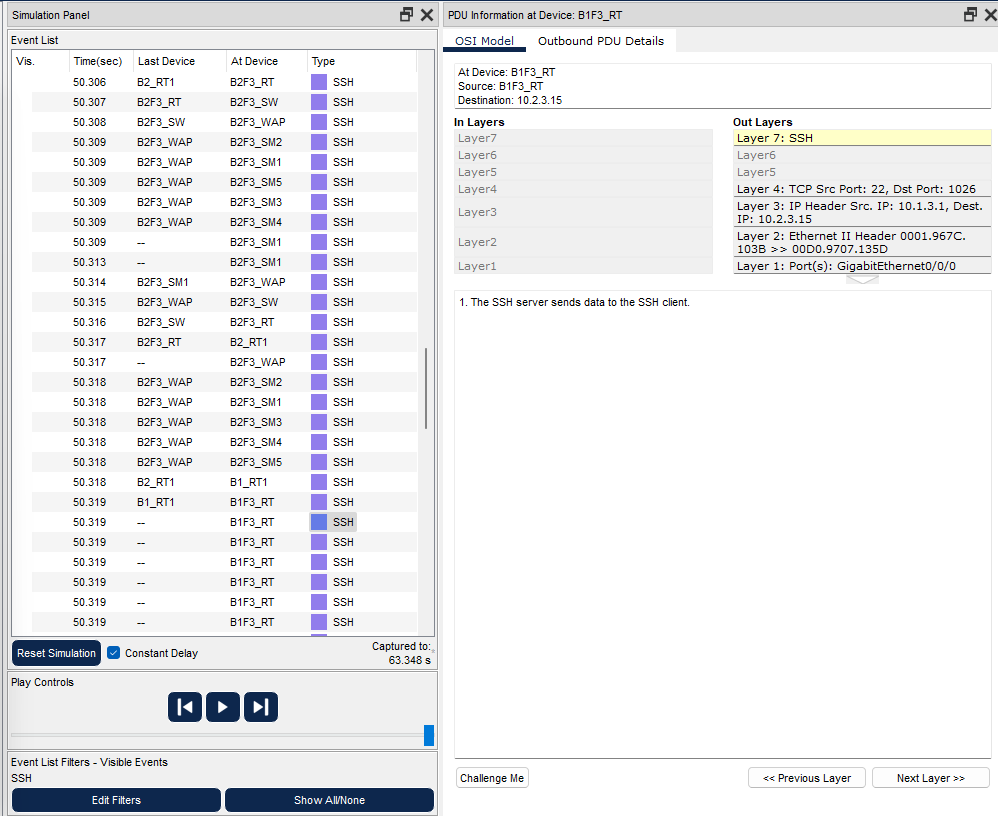


Figure 5.39: Server rejects SSH connection



Figure 5.40: Command prompt

### Scenario 9

A user from the first facility of first branch wants to tracert to Google’s server.

#### Tracert

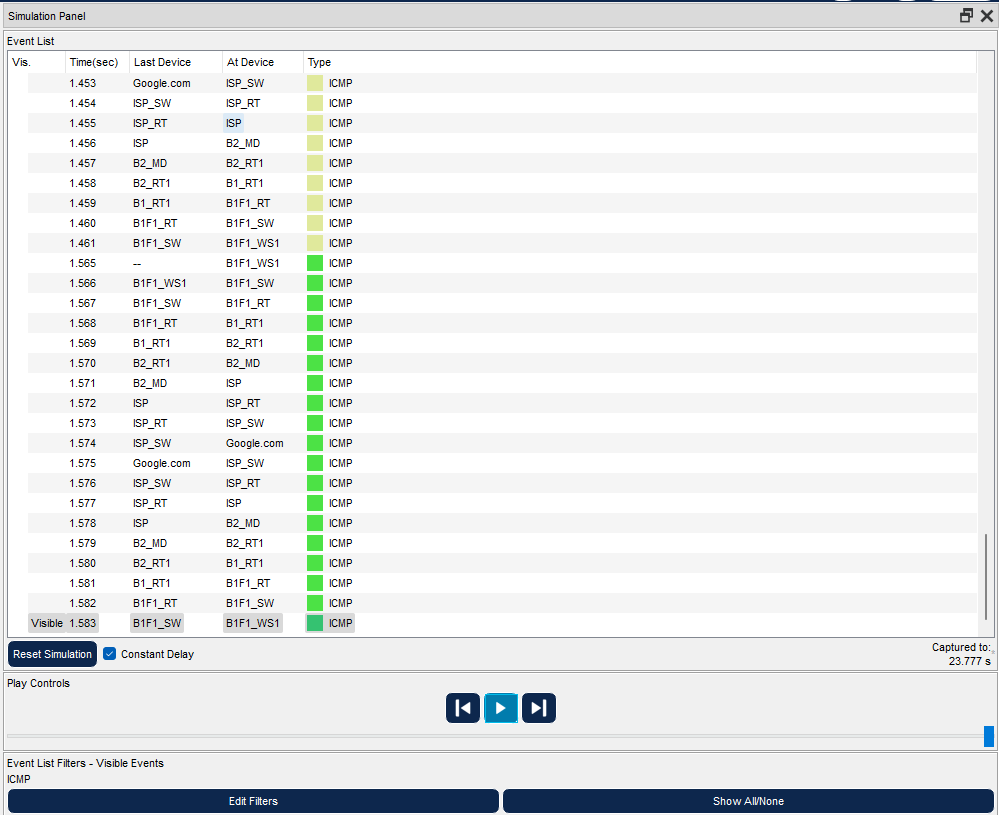


Figure 5.41: Many packages sent during the tracert process

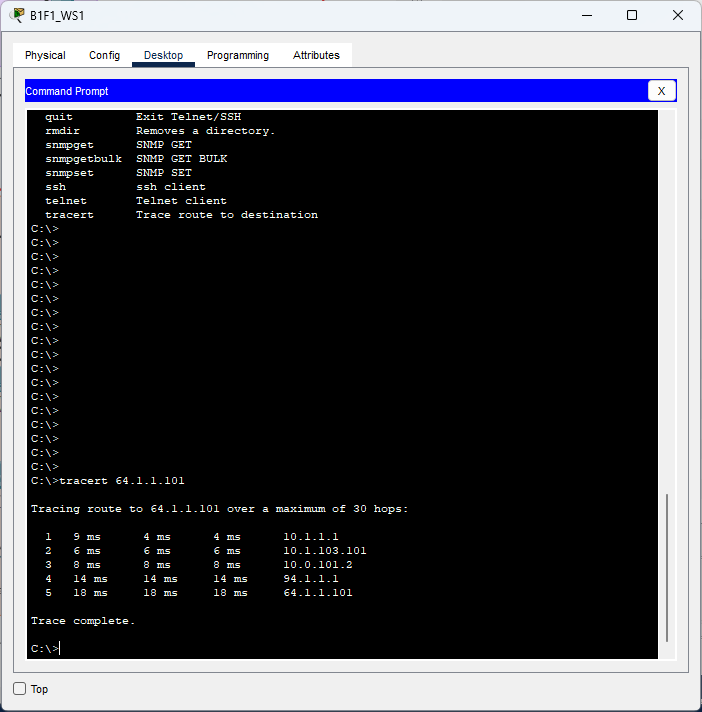


Figure 5.42: Tracert process complete

### Scenario 9

A user from the first facility of the first branch wants to download a file from the ftp server

#### FTP Download

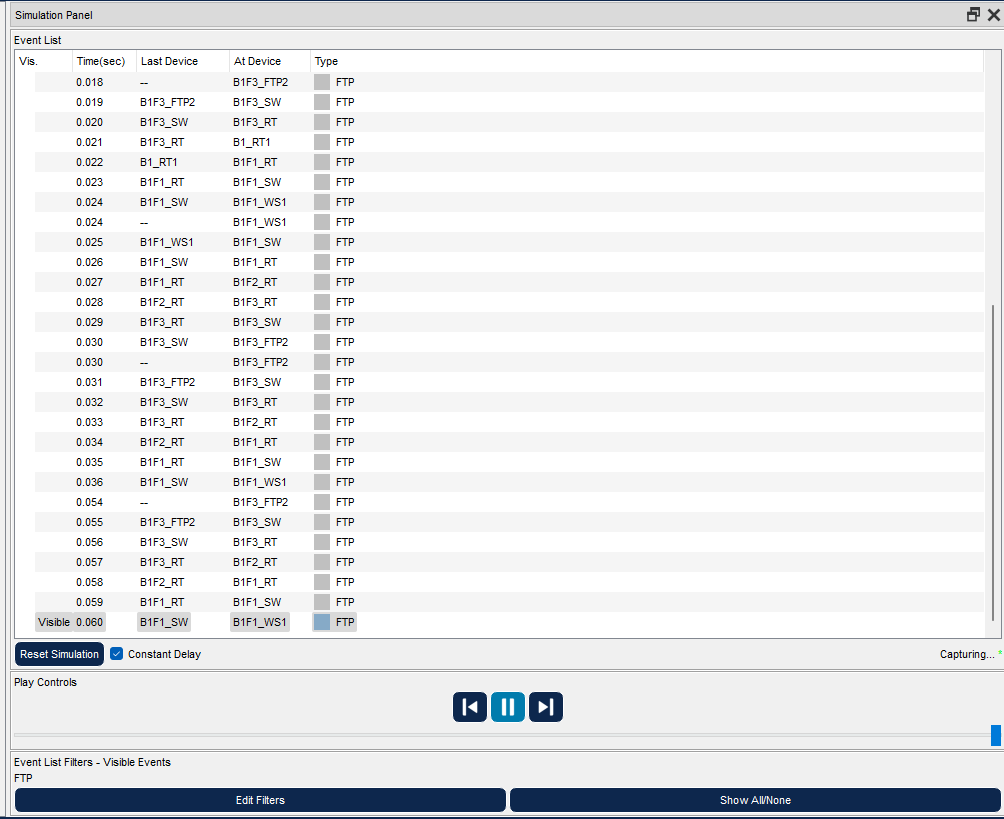
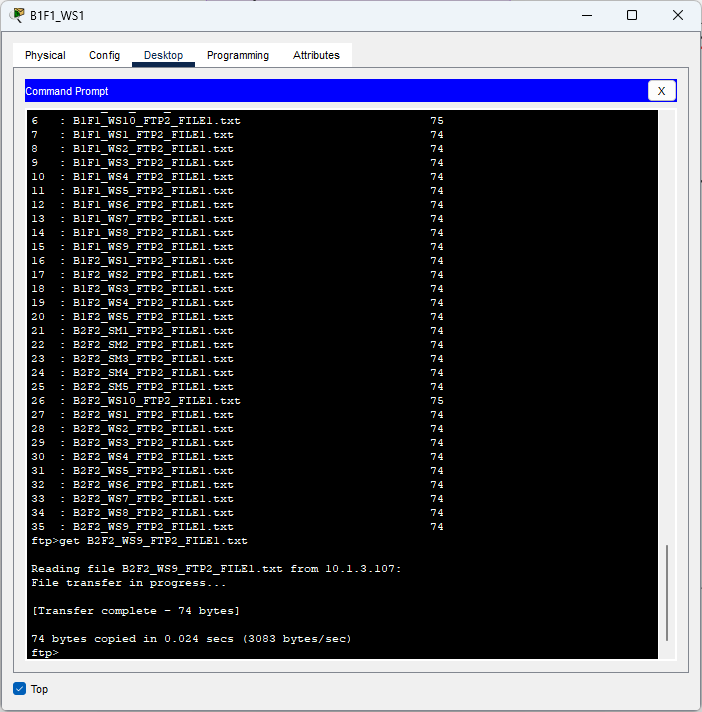


Figure 5.43: Many FTP messages sent during the download process

Figure 5.44: User was able to download the file

## Configurations

B1\_RT

!

version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname B1\_RT1

!

!

!

!

!

!

!

!

no ip cef

no ipv6 cef

!

!

!

!

license udi pid CISCO2911/K9 sn FTX152472R1-

!

!

!

!

!

!

!

!

!

!

!

spanning-tree mode pvst

!

!

!

!

!

!

interface GigabitEthernet0/0

ip address 94.54.244.153 255.0.0.0

duplex auto

speed auto

!

interface GigabitEthernet0/1

no ip address

duplex auto

speed auto

shutdown

!

interface GigabitEthernet0/2

no ip address

duplex auto

speed auto

shutdown

!

interface GigabitEthernet0/0/0

ip address 10.0.101.1 255.255.255.0

!

interface GigabitEthernet0/1/0

ip address 10.1.103.101 255.255.255.0

!

interface GigabitEthernet0/2/0

ip address 10.1.104.101 255.255.255.0

!

interface GigabitEthernet0/3/0

ip address 10.1.105.101 255.255.255.0

!

interface Vlan1

no ip address

shutdown

!

router ospf 1

log-adjacency-changes

network 93.0.0.0 0.255.255.255 area 0

network 10.1.103.0 0.0.0.255 area 0

network 10.1.104.0 0.0.0.255 area 0

network 10.1.105.0 0.0.0.255 area 0

network 94.0.0.0 0.255.255.255 area 0

network 10.0.101.0 0.0.0.255 area 0

!

ip classless

!

ip flow-export version 9

!

!

!

!

!

!

!

line con 0

!

line aux 0

!

line vty 0 4

login

!

!

!

end

B1F2\_RT

!

version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname B1F2\_RT

!

!

!

!

!

!

!

!

ip cef

no ipv6 cef

!

!

!

!

license udi pid CISCO2911/K9 sn FTX1524P73E-

!

!

!

!

!

!

!

!

!

!

!

spanning-tree mode pvst

!

!

!

!

!

!

interface GigabitEthernet0/0

no ip address

duplex auto

speed auto

!

interface GigabitEthernet0/0.2

encapsulation dot1Q 2

ip address 10.1.2.1 255.255.255.0

ip helper-address 10.1.3.108

!

interface GigabitEthernet0/0.202

encapsulation dot1Q 202

ip address 10.1.202.1 255.255.255.0

ip helper-address 10.1.3.108

!

interface GigabitEthernet0/1

ip address 10.1.101.2 255.255.255.0

duplex auto

speed auto

!

interface GigabitEthernet0/2

ip address 10.1.102.2 255.255.255.0

duplex auto

speed auto

!

interface GigabitEthernet0/0/0

ip address 10.1.104.2 255.255.255.0

!

interface Vlan1

no ip address

shutdown

!

router ospf 1

log-adjacency-changes

network 10.1.2.0 0.0.0.255 area 0

network 10.1.101.0 0.0.0.255 area 0

network 10.1.102.0 0.0.0.255 area 0

network 10.1.202.0 0.0.0.255 area 0

network 10.1.104.0 0.0.0.255 area 0

!

router rip

!

ip classless

!

ip flow-export version 9

!

!

!

!

!

!

!

line con 0

!

line aux 0

!

line vty 0 4

login

!

!

!

end

# Conclusion

In conclusion, through the process of designing and simulating a Metropolitan Area Network, we have learned a great deal about computer network planning and design. We have gained practical experience in creating a network architecture that supports a large number of users and traffic load with minimum delay, while also balancing the cost of hardware and system requirements. We have also become proficient in using Cisco Packet Tracer software, which allowed us to create a virtual network environment for testing and analysis.

Furthermore, we have explored various network scenarios, such as wireless connectivity, VoIP conferencing, and email and file transfers between different facilities and branches. By analyzing the traffic flow and performance of our network design, we have identified potential bottlenecks and areas for improvement, such as increasing bandwidth and implementing quality of service protocols.

Overall, this project has provided us with valuable knowledge and skills in the field of data communications and computer networks. We are confident that we can apply what we have learned to real-world situations and continue to develop our expertise in this field.

# References

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

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

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

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

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

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

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

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