DOKUZ EYLUL UNIVERSITY

ENGINEERING FACULTY

DEPARTMENT OF COMPUTER ENGINEERING

METROPOLITAN AREA NETWORK SIMULATION PROJECT

by

Serdar KARACA - 2019510046

Harun Adem TEMUR- 2019510072

YASSER AL HASAN- 2019510006

İZMİR

11.05.2023

**TABLE OF CONTENTS**

CHAPTER 1 – INTRODUCTION.....................................................................................3

1.1 Project Definition and Problem Formulation............................................................3

1.2 The Purpose and Motivation of The Project.............................................................3

1.3 Term Definitions.......................................................................................................4

1.4 Related Work............................................................................................................7

CHAPTER 2 – METHOD AND SIMULATION...............................................................8

2.1 Simulation and Modeling Concepts.........................................................................8

2.2 Simulation Environment/Tool..................................................................................9

2.3 Network Design Requirements..............................................................................10

2.4 Requirement Analysis............................................................................................10

2.5 Definitions of the System/Model...........................................................................11

2.6 Simulation Elements..............................................................................................19

CHAPTER 3 – TRAFFIC ANALYSIS AND SIMULATION RESULTS.......................23

Scenario 1.....................................................................................................................23

Scenario 2.....................................................................................................................31

Scenario 3.....................................................................................................................35

Scenario 4.....................................................................................................................39

Scenario 5.....................................................................................................................40

Scenario 6.....................................................................................................................44

Scenario 7.....................................................................................................................49

Scenario 8.....................................................................................................................53

Scenario 9.....................................................................................................................57

CHAPTER 4 – PROBLEMS ENCOUNTERED.............................................................61

CHAPTER 5 – CONCLUSION.......................................................................................62

CHAPTER 6 – REFERENCES........................................................................................63

CHAPTER 1

INTRODUCTION

1.1.Project Definition and Problem Formulation

A metropolitan area network (MAN) is a computer network that links computers within a metropolitan area, encompassing a large city, multiple cities and towns, or any extensive region with multiple buildings. It serves as an intermediary between a local area network (LAN) and a wide area network (WAN). The term MAN is used to describe the integration of LANs within a city, forming a larger network that facilitates efficient connectivity to a WAN. It also refers to the interconnection of multiple LANs in a metropolitan area through point-to-point connections. This approach involves bridging several LANs with backbone lines.

Our project focuses on designing a MAN to facilitate communication among users in a company that operates two branches within a city. Each branch comprises three facilities, and users within these facilities have distinct roles and responsibilities. Instead of dedicated servers for each facility, there is a single server room where users access shared servers to carry out their tasks. The project aims to achieve process synchronization and effective communication among the branches, facilities, and users by leveraging Internet service providers (ISPs) and appropriate connection methods and tools when required.

1.2. The Purpose and Motivation of The Project

During the project preparation phase for the Metropolitan Area Network (MAN), our objective was to create a network infrastructure that could accommodate a maximum number of users, handle high traffic loads with minimal delay, and provide adequate hardware support for future expansions at a cost-effective level. To achieve this, we utilized widely adopted technologies like fiber optic technology to ensure fast network speeds. The MAN topology we designed focuses on enabling various operations such as email transactions, internet browsing, file transfers, secure protocols like SSH, and voice transfer through protocols like VoIP, all while maintaining low costs and high efficiency.

In this project, the connection between two branches and three facilities will be established via an Internet Service Provider (ISP). Our design aims to optimize performance while minimizing costs, prioritizing maximum efficiency. However, it's important to note that if additional features beyond the initial requirements are desired or expected, it may have a negative impact on costs while positively affecting performance

**1.3.Term Definitions**

**Node:** A node denotes a connection point within a network that can receive, send, create, or store data. To gain access, each node necessitates some form of identification, such as an IP address. Examples of nodes include computers, printers, modems, bridges, and switches. Essentially, a node encompasses any network device capable of recognizing, processing, and transmitting information to other network nodes.

**Packet:** A packet refers to a small unit of data transmitted over a network, such as a Local Area Network (LAN) or the Internet. Similar to a physical package, each packet contains source and destination addresses, as well as the content or data being transferred. Upon reaching their destinations, the packets are reassembled into a single file or a contiguous block of data. While the specific structure of a packet may vary across protocols, a typical packet comprises two sections: a header and a payload. The header stores information about the packet.

**Channel:** A channel refers to either a physical transmission medium, such as a wire, or a logical connection over a multiplexed medium, such as a radio channel in telecommunications and computer networking. Channels are utilized to transmit information signals, such as digital bit streams, from one or more senders or transmitters to one or more receivers.

**Protocol:** A protocol comprises a set of regulations governing the format and handling of data. When it comes to networks, protocols serve as a common language for computers. Even if computers within a network utilize different software and hardware, protocols enable them to communicate with one another seamlessly.

**System:** In telecommunications, a communication system encompasses various individual networks, transmission systems, transfer stations, and data terminal equipment that can be interconnected and operate together as a unified entity. A communication system consists of several essential components, including an information source, input transducer, transmitter, communication channel, receiver, output transducer, and destination.

**Architecture:** Network architecture encompasses the complete framework of a computer network within an organization. The network architecture diagram provides a comprehensive overview of the established network, offering detailed insights into all accessible resources. It includes hardware components used for communication, cabling and device types, network layout and topologies, physical and wireless connections, implemented areas, and future plans. Additionally, network architecture comprises the software rules and protocols that govern the network.

Network: A network refers to a collection of two or more devices or nodes that have the ability to communicate with each other. These devices or nodes can be interconnected through either physical or wireless connections. The fundamental requirement is the presence of at least two distinct components that are linked together.  
  
**Wireless:** Wireless technology pertains to telecommunication and data transmission without the use of physical wires. In a broad sense, wireless encompasses any form of telecommunications or data transfer where electromagnetic waves are employed to carry signals along some or all parts of the communication pathway. This term specifically applies to a type of network that broadcasts an access signal to workstations, enabling the mobility of laptops and tablet PCs while maintaining a continuous network connection.  
  
**Ethernet:** Ethernet represents the standard method for connecting computers within a network through a wired connection. It offers a straightforward interface for linking multiple devices such as computers, routers, and switches. With a single router and a few Ethernet cables, it is possible to establish a Local Area Network (LAN) that enables communication among all connected devices.  
  
**Frame:** In computer networking and telecommunications, a frame serves as a digital data transmission unit. In packet-switched systems, a frame acts as a simple container for a single network packet. In other telecommunications systems, a frame functions as a repeating structure that supports time-division multiplexing.  
  
**Access Point:** An access point is a device responsible for creating a Wireless Local Area Network (WLAN), typically within an office or a large building. It connects to a wired router, switch, or hub via an Ethernet cable and projects a Wi-Fi signal within a designated area.  
  
**Switches:** A switch is a device that connects other devices and manages node-to-node communication within a network. Its role involves ensuring that data packets reach their intended destinations. While a router forwards information between networks, a switch facilitates information transfer between nodes within a single network. In the context of computer networks, "switching" refers to the process of data transfer between devices.  
  
**Router:** A router is a physical or virtual device responsible for forwarding information contained within data packets between networks. Routers analyze the data within packets to determine the optimal path for transmitting information to its ultimate destination. They continue to forward data packets until they reach the intended destination node.  
  
**IP address:** An IP address serves as a unique identifier for a device on the internet or a local network. IP stands for "Internet Protocol," which defines the rules governing data formatting and transmission over the internet or a local network. IP addresses contain location information and enable devices to establish communication. They allow for differentiation between various computers, routers, and websites on the internet.

**Workstation:** A workstation is a high-performance computer system designed primarily for a single user. It possesses advanced graphics capabilities, ample storage capacity, and a powerful central processing unit. Workstations offer more capabilities than personal computers (PCs) but are less advanced than servers. Servers can manage large networks of peripheral PCs or workstations and handle extensive data processing and reporting tasks.  
  
**Server:** A server refers to a piece of computer hardware or software (computer program) that provides functionality for other programs or devices, known as "clients." This architecture is referred to as the client-server model. Servers offer various functionalities, often termed "services," such as data or resource sharing among multiple clients or performing computations on behalf of a client. Examples of servers include database servers, file servers, mail servers, print servers, web servers, game servers, and application servers.  
  
**DNS:** The Domain Name System is a hierarchical and decentralized naming system for computers, services, and other resources connected to the internet or a private network. It associates diverse information with domain names assigned to each participating entity. Most notably, DNS translates easily memorized domain names into numerical IP addresses required to locate and identify computer services and devices using the underlying network protocols.

**TCP:** The Transmission Control Protocol (TCP) is a fundamental component of the Internet protocol suite. It originated as part of the initial network implementation and complements the Internet Protocol (IP). The entire suite is commonly referred to as TCP/IP. TCP plays a crucial role in major internet applications such as the World Wide Web, email, remote administration, and file transfer. It operates within the Transport Layer of the TCP/IP suite.  
  
**FTP:** File Transfer Protocol (FTP) is a set of rules that computers follow when transferring files from one system to another over the internet. Businesses may use FTP to transfer files between computer systems, and websites often utilize FTP to upload or download files from a website's server.  
  
**HTTP:** HTTP is the protocol employed for data transfer over the web. It is part of the Internet protocol suite and defines commands and services used to transmit web page data.  
  
**POP:** A Point of Presence (PoP) serves as an artificial demarcation or interface point between communicating entities. An example is an ISP Point of Presence, which is the local access point enabling users to connect to the internet through their Internet Service Provider (ISP). A typical PoP houses servers, routers, network switches, multiplexers, and other network interface equipment and is typically located in a data center.

**SMTP:** SMTP stands for "Simple Mail Transfer Protocol." It is the protocol used for sending email over the internet. When you send a message from your email client, it utilizes SMTP to transmit the message to the mail server, which in turn relays it to the appropriate receiving mail server.

**1.4.Related Work**

In the completion of this project, we have solely relied on our own original work and have not incorporated any external sources or materials.

CHAPTER 2

**METHOD AND SIMULATION**

**2.1. Simulation and Modeling Concepts**

During the process of establishing the network, we made careful assessments of both logical and physical requirements. Following a bottom-up approach, we initiated the construction phase by assembling smaller units and gradually progressing towards larger units. This alternative approach allowed us to expedite the network setup considerably. Typically, when designing a network from the bottom-up, the focus tends to be primarily on the infrastructure, with applications and services being considered at a later stage. This approach often necessitates a less comprehensive initial analysis, making it easier to implement as a quick solution.  
  
 In our modeling endeavor, we created user profiles for workstation users, wireless users, tablet users, and smartphone users across various branch facilities. As the users connected with each other, successful communication was established through switches, routers, wireless routers, and connecting cables. Additionally, we configured our servers and assigned IP addresses to users at each facility using the DHCP server. We thoroughly examined the network device connections between workstations and network devices, ensuring the accuracy of their physical locations within the facilities. We then proceeded to configure the network devices.  
  
 To establish connections between workstations and other network devices, we utilized packet tracer simulation, automatically selecting the appropriate cable. Facilities within the same branches were interconnected through a main switch utilizing a fast Ethernet port. For communication between different branches, we employed routers equipped with serial Ethernet ports. These routers facilitated connections between routers in different branches through serial Ethernet ports. Furthermore, routers played a crucial role in managing packets. When a workstation intended to send data (such as messages or emails) to another workstation on a different network, the router ensured the proper routing of the packet with the assistance of static routing.  
  
 Finally, at the third facility of the first branch office, we established server farms to enable users to engage in various activities such as email communication, web browsing, file transfers, VoIP services (transmitting voice data over IP between private users or workstations), and automatic IP assignment. Within the server room, we configured web servers, DNS servers, mail servers, FTP servers, and DHCP servers, ensuring their readiness and connection to the main switch of the server farm. The server farm switch was then linked to the server router. Additionally, by connecting the shared connection router of the three facilities in the second branch to the server router via a serial connection, we established a metropolitan area network. Following the establishment of this connection, we conducted thorough tests between workstations to verify its functionality.  
  
 In summary, although we have not delved into the specifics of each phase of the metropolitan area network design, we have provided a brief overview of the undertaken tasks. With the network cables and devices we have employed, all our workstations and devices are now able to perform their designated functions effectively, thereby establishing a functional network spanning two different branches within the same city.

**2.2. Simulation Environment/Tool**

We utilized the Cisco Packet Tracer simulation for our project. Cisco Packet Tracer is a simulation program employed by Cisco to configure essential settings prior to implementing routers, switches, hubs, or security devices on an actual network. This tool facilitates the simulation of both simple and complex networks, offering two operational modes: Real-time and Simulation Mode. With Cisco Packet Tracer, users can work within two distinct workspaces: logical and physical.

The logical workspace allows users to construct logical network topologies by placing, connecting, and grouping virtual network devices. On the other hand, the physical workspace provides a graphical representation of the logical network in a physical dimension, providing a realistic perspective on the placement and scale of network devices, including routers, switches, and hosts. Furthermore, the physical view incorporates geographic representations of networks, featuring multiple cities, buildings, and wiring closets.

It's important to note that the software itself offers only a limited set of features compared to the actual hardware running the Cisco IOS version. Consequently, it is not suitable for modeling production networks, and it may not encompass the complete range of IOS commands required for practice. Primarily, this software caters to Certified Cisco Network Associate Academy students as an educational tool, aiding them in grasping fundamental CCNA concepts.

Cisco Packet Tracer program offers several advantages, including a user-friendly environment. It facilitates the creation of multi-user training laboratories in real-time, allowing for collaborative learning experiences. With the use of virtual equipment, the program allows for the design of network environments and configuration of network devices.

In summary, Cisco Packet Tracer greatly simplifies the process of learning and teaching by enabling multiple users to collaborate and explore within a realistic simulation environment for conducting experiments.

**2.3. Network Design Requirements**

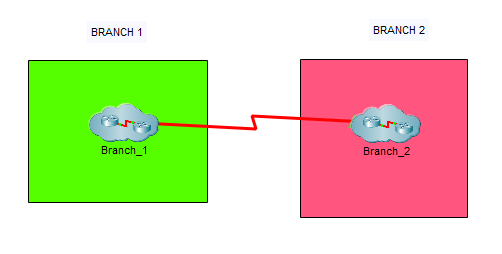
We have implemented a network design that fulfills all the requirements outlined in the project. The project's network design entails the utilization of a server/client architecture, with various communication protocols such as HTTP, DHCP, DNS, FTP, POP3, TCP, SSH, SMTP, and SCCP facilitating device connectivity. The design incorporates 6 switches, 4 access points, 5 routers, 10 servers, 45 workstations, 8 laptops, 13 smartphones, 10 tablets, and 3 IP Phones. The network connections follow a star topology, those are then connected as hybrid topology, resulting in an overall hybrid network structure.

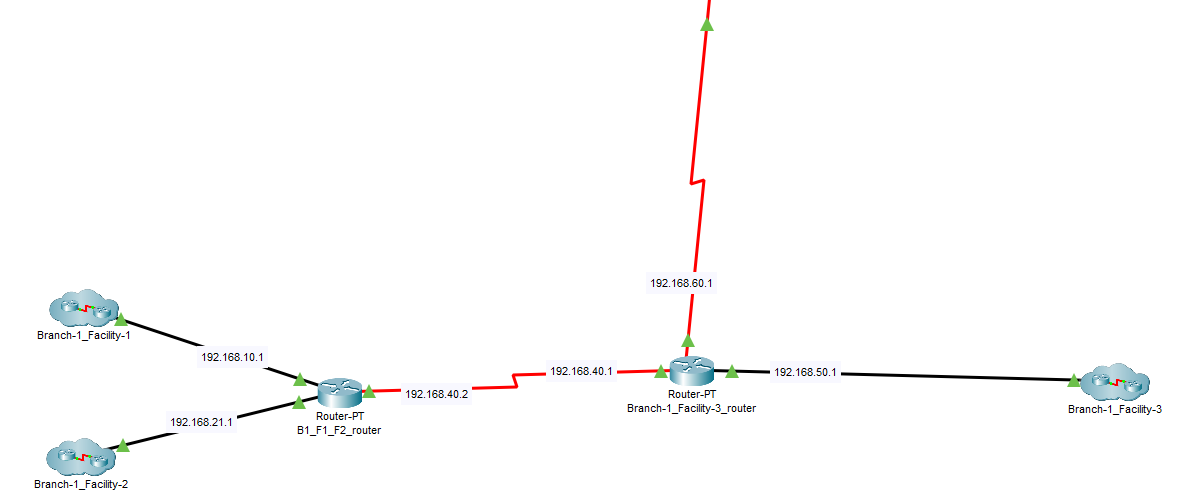
**2.4. Requirement Analysis**

Web browsing should be enabled for all network devices. In the first facility of the first branch and the first and third facilities of the second branch, devices should have the capability to send and receive emails. File transfer support is required for devices in the first facility of the first branch and the first and second facilities of the second branch. Additionally, three devices in the second facility of the first branch should be capable of hosting VoIP conferences. Wireless connectivity is necessary for all devices in the first facility of the second branch.

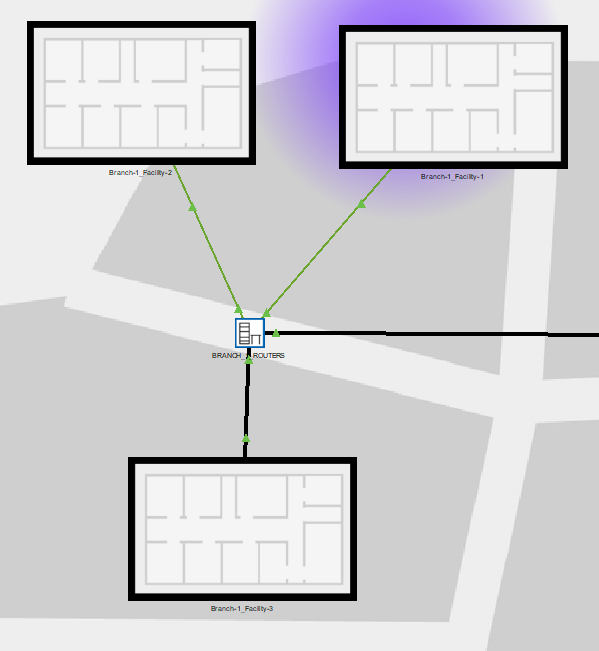
Overall, the network needs to accommodate a maximum of 76 concurrent users. The devices should be capable of downloading at speeds of up to 100 Mbps and uploading at speeds of up to 10 Mbps.

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

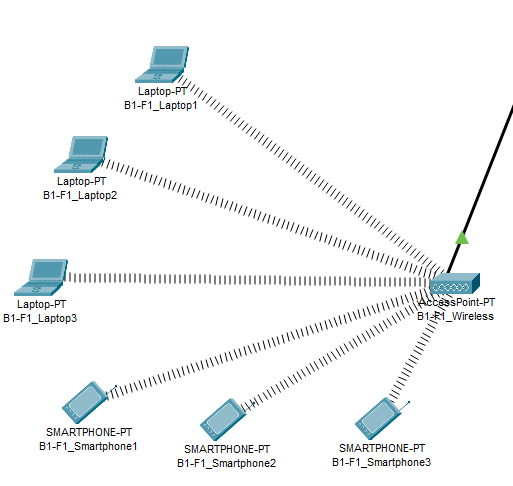
 **Logical View**

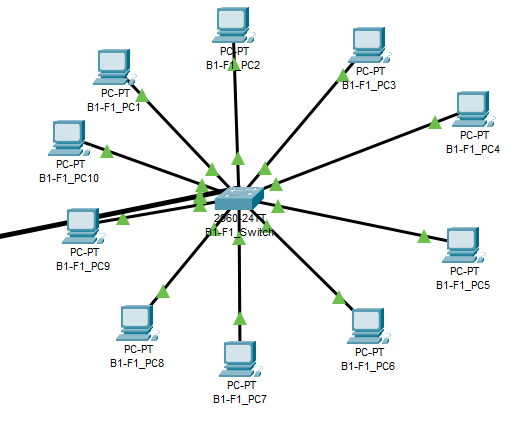
**Physical View** **First Branch Logical View**

**First Branch Physical View**

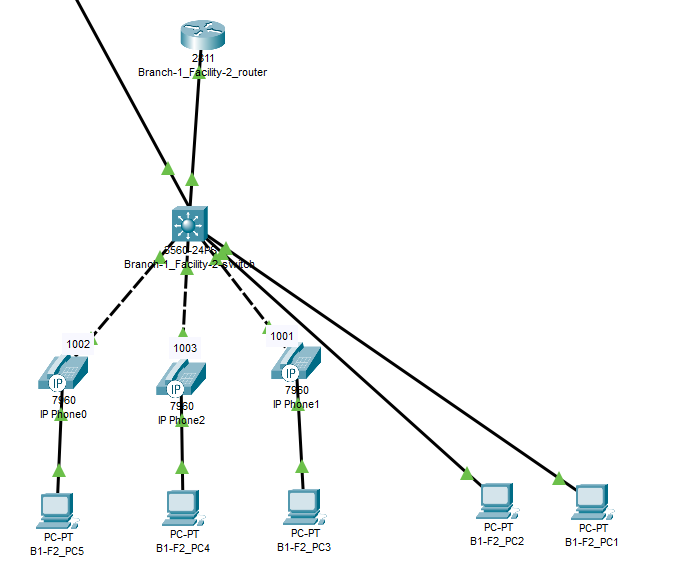
****

**First Facility of First Branch**

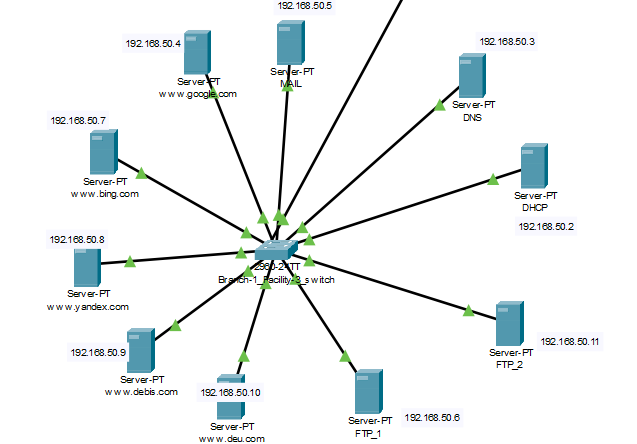




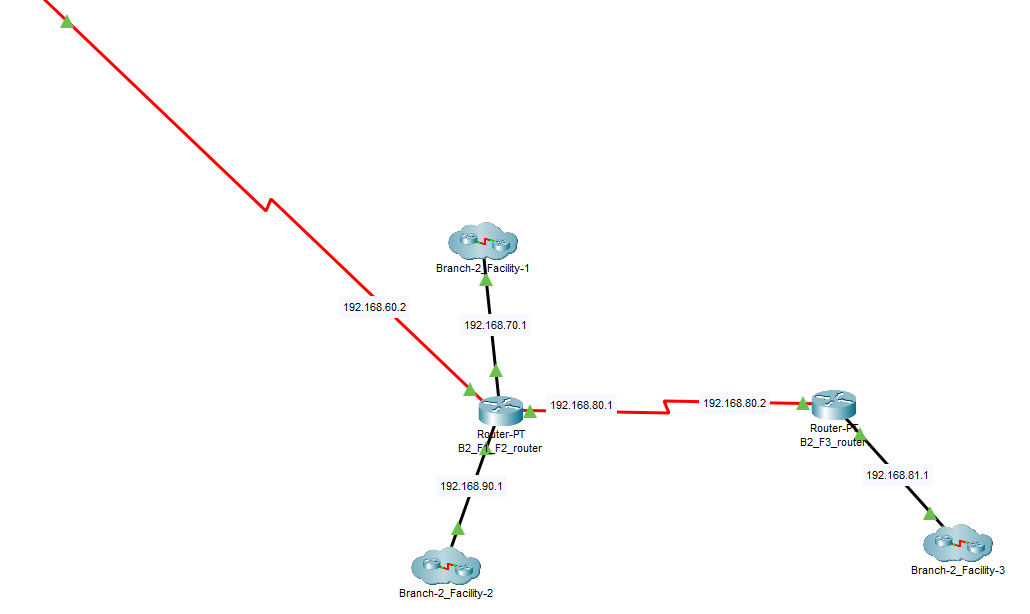
**Second Facility of First Branch**



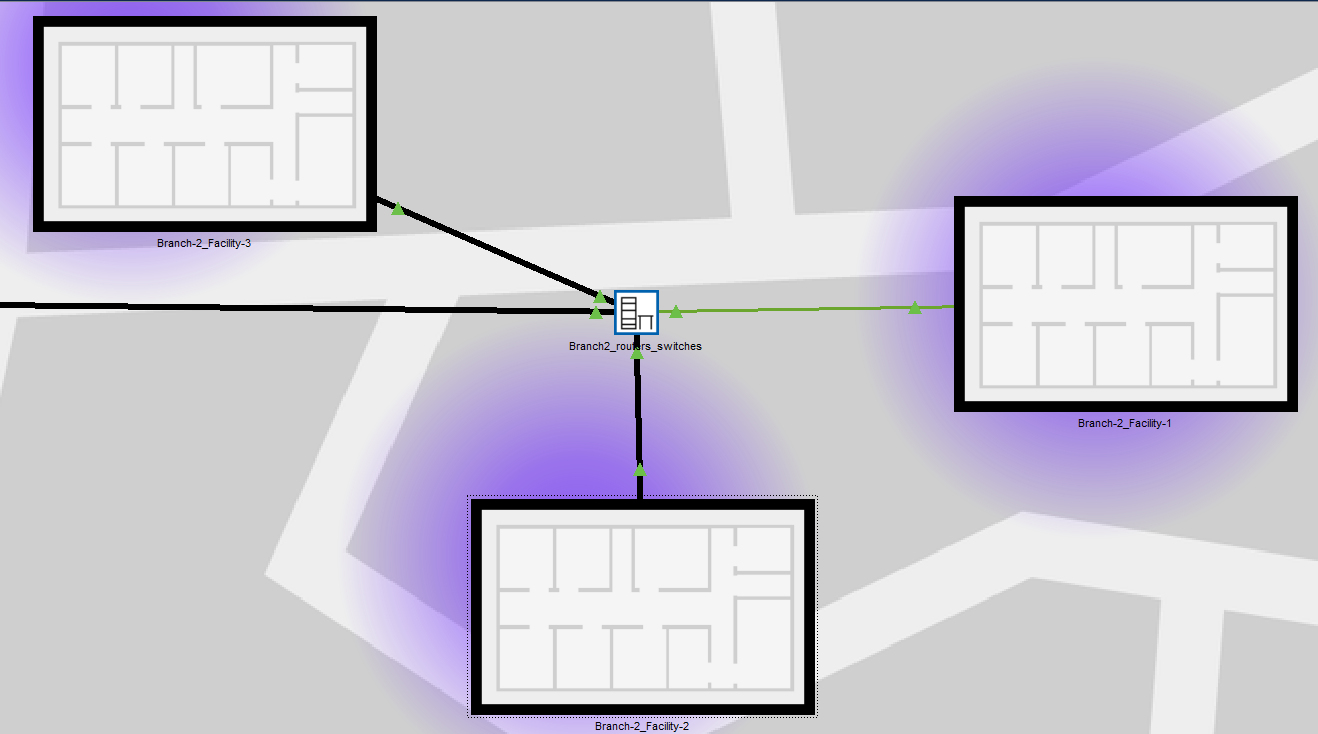
**Third Facility of First Branch**



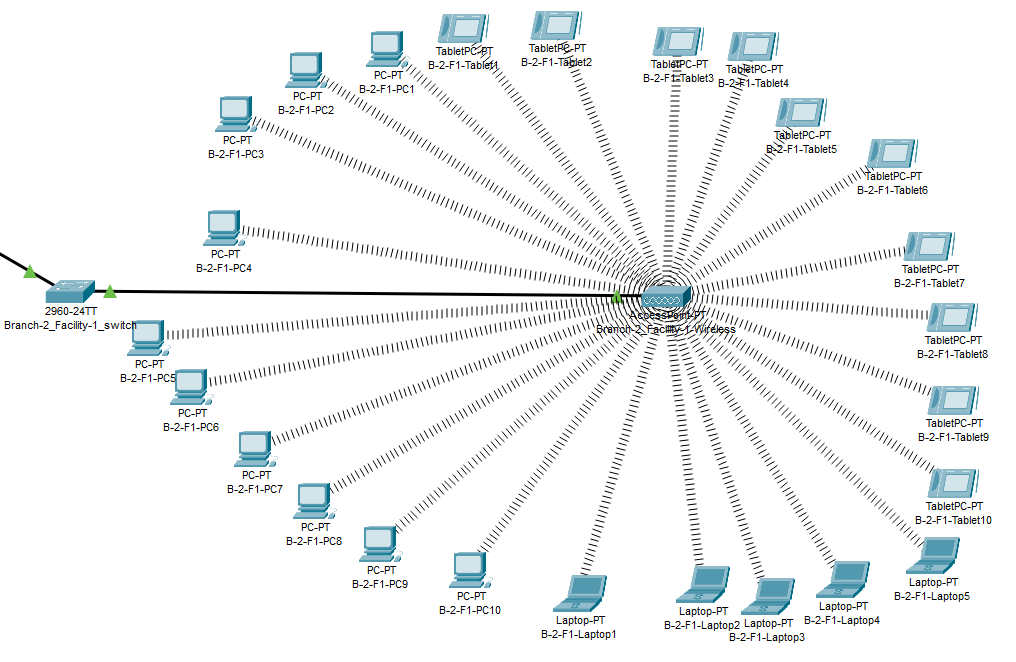
**Second Branch Logical View**



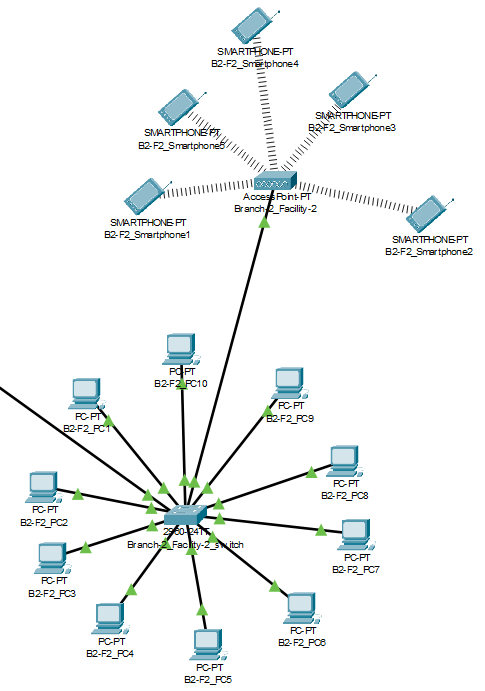
**Second Branch Physical View**

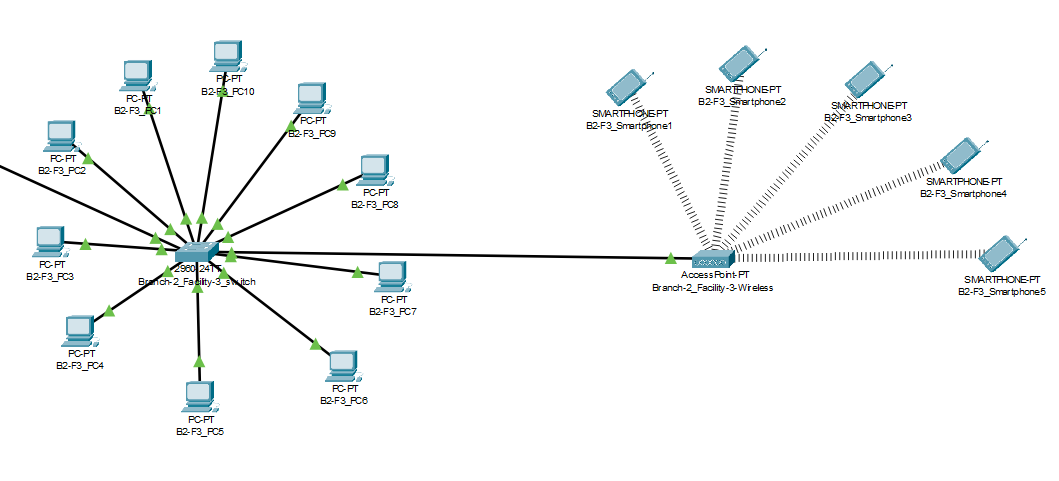
****

**First Facility of Second Branch**

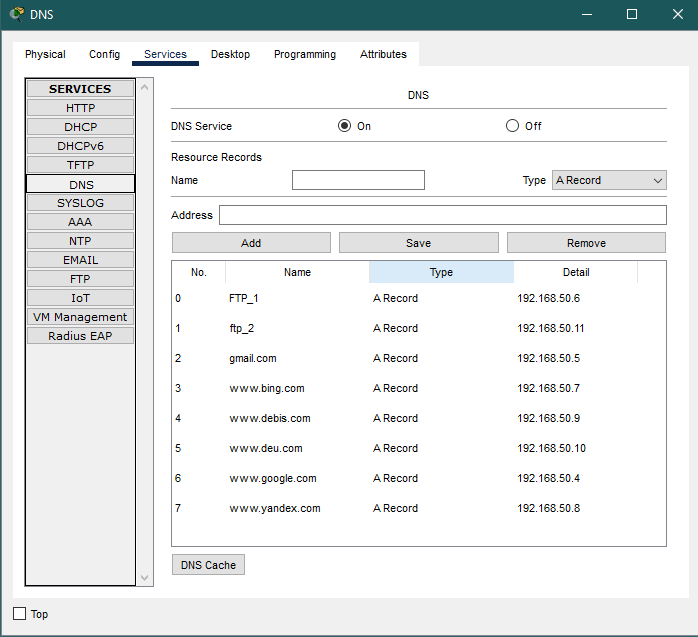
****

**Second Facility of Second Branch**

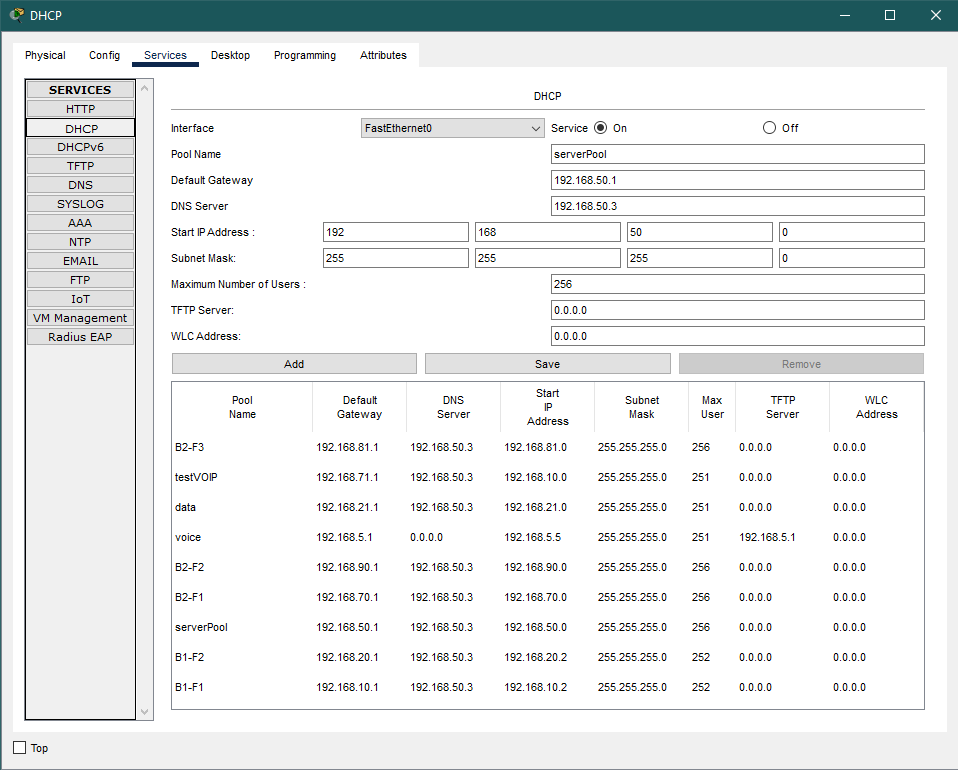
****

** Third Facility of Second Branch**

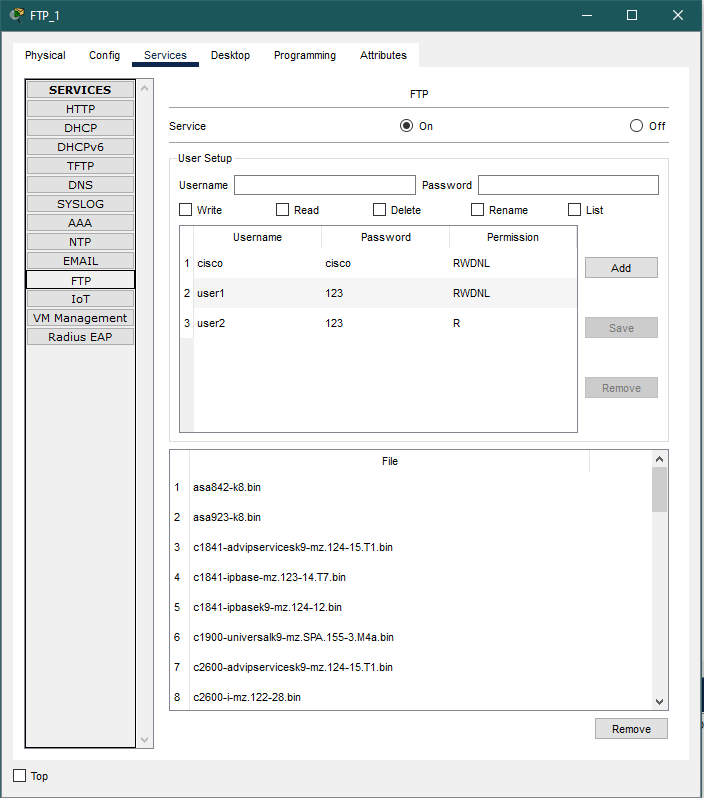
**2.6. Simulation Elements**



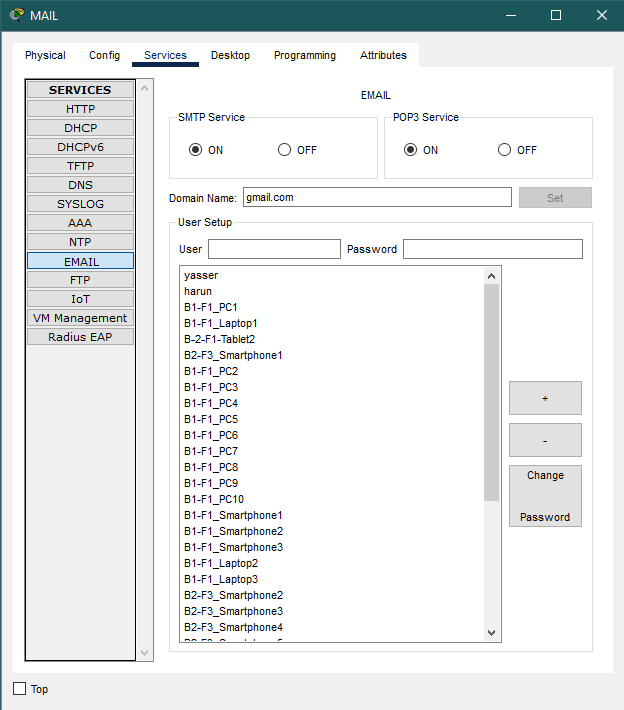
DNS Server



DHCP Server



FTP Server

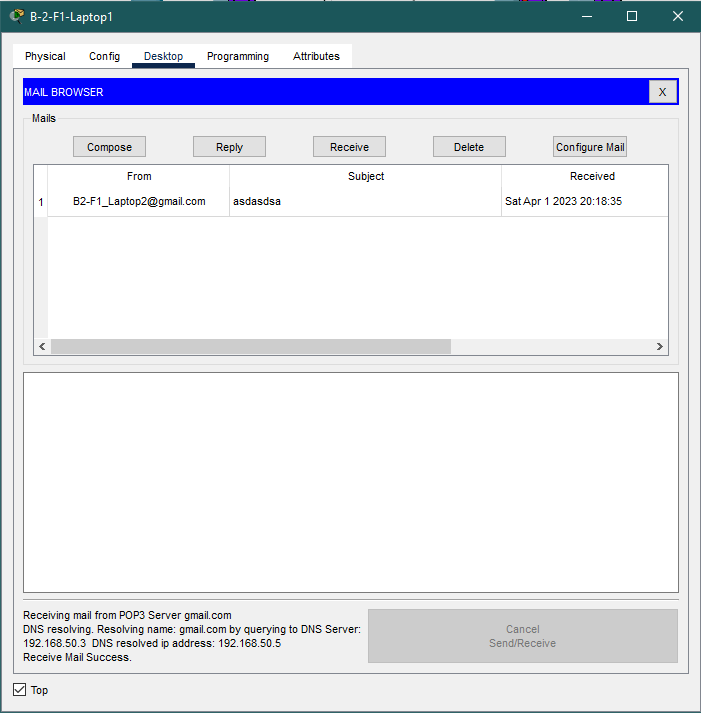


MAIL Server

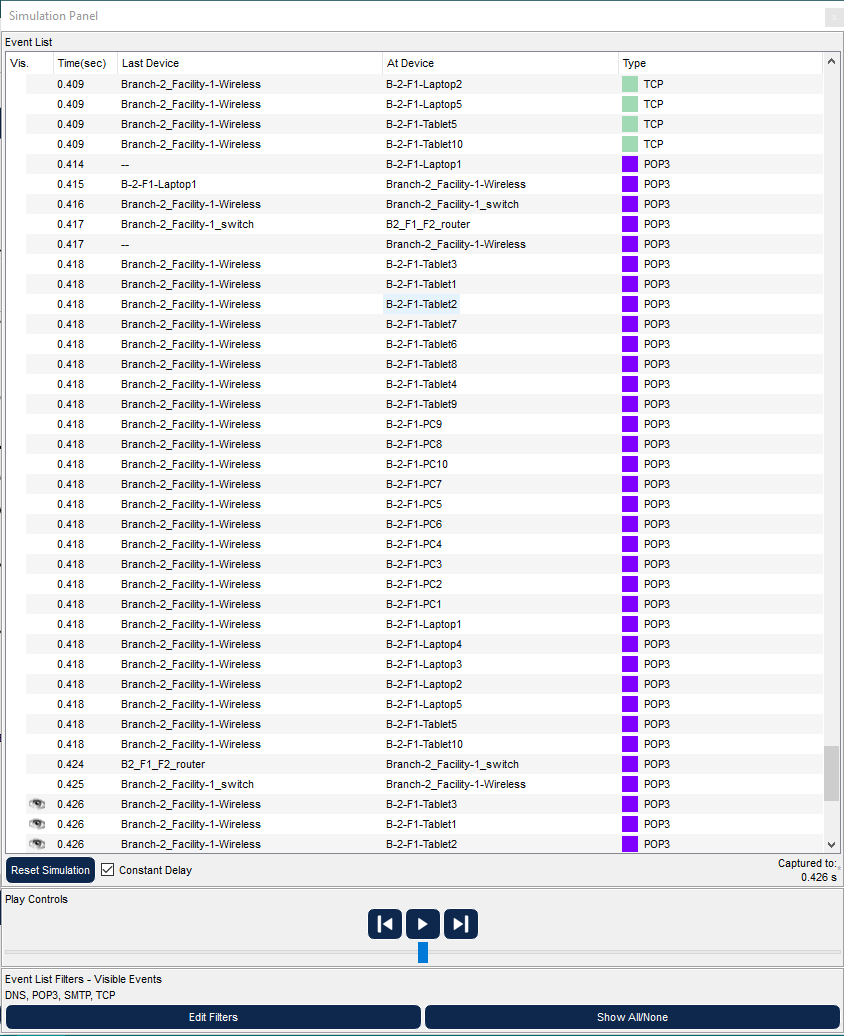
CHAPTER 3

TRAFFIC ANALYSIS AND SIMULATION RESULTS

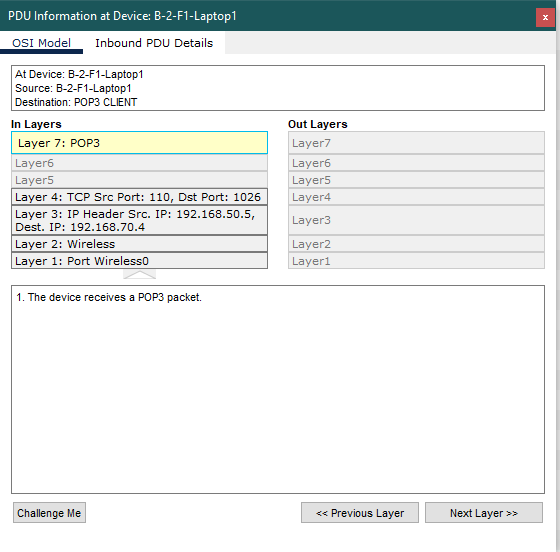
**Scenario 1:** A wireless user from first facility of second branch wants to read emails and browse Web. The user B2-F1\_Laptop1 communicated with the mail server to carry out the process of reading mail. The network path for this scenario is as follows: B2-F1\_Laptop1, Branch-2\_Facility-1-Wireless Access Point, Branch-2\_Facility-1\_Switch, B2\_F1\_F2\_Router, Branch-1\_Facility-3\_Router, Branch-1\_Facility-3\_Switch, Mail Server.



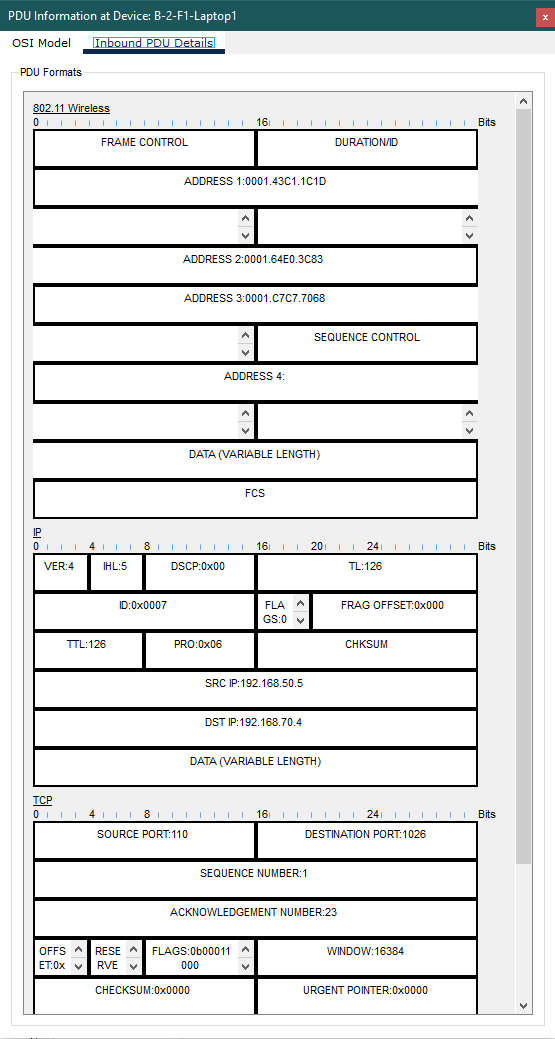
Receive Mail Result



Receive Mail Event List

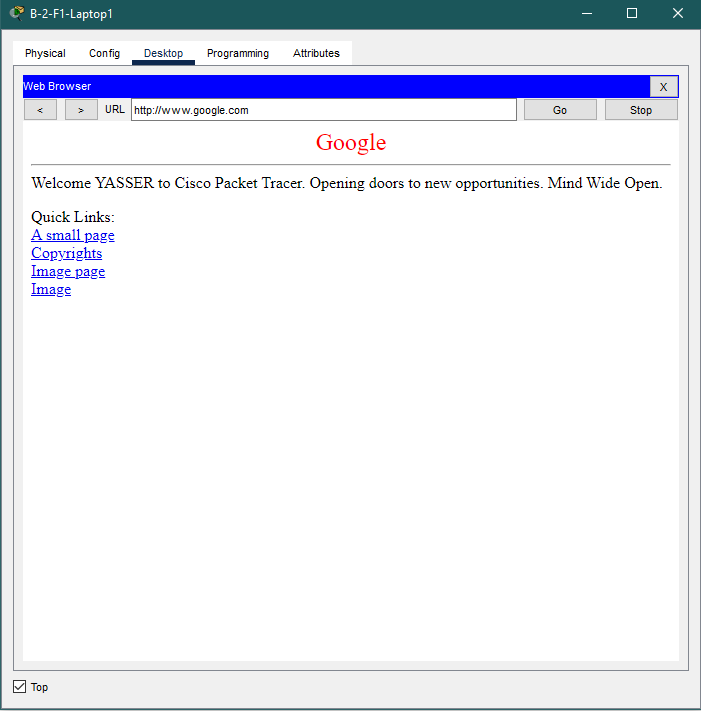


Receive Mail OSI Model

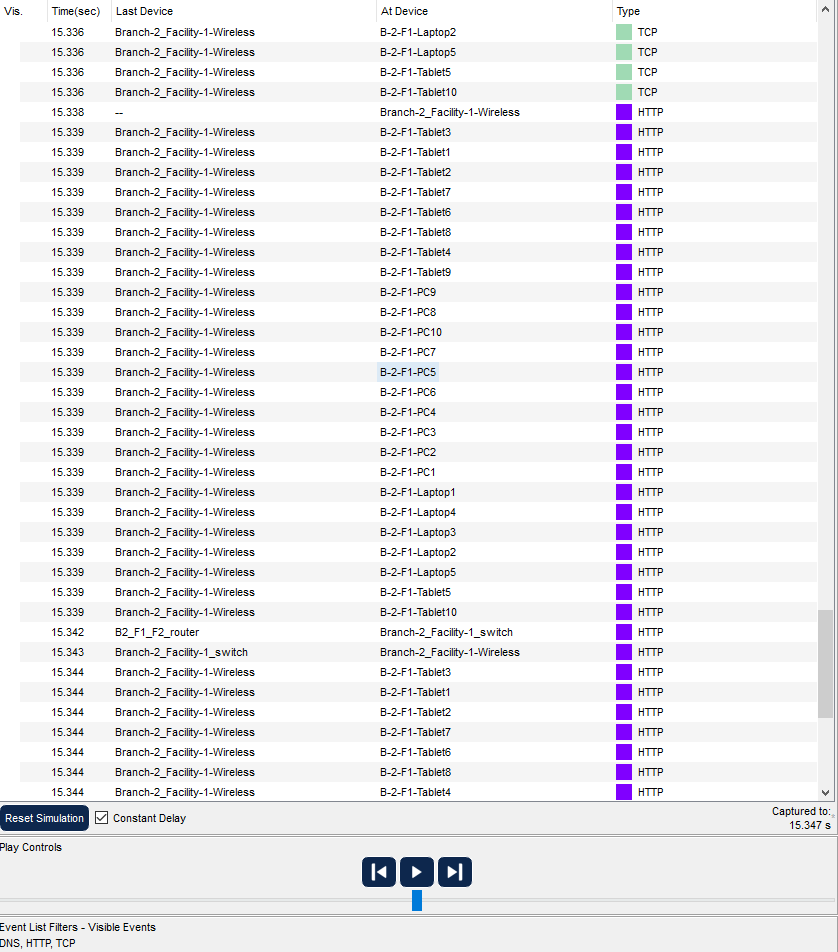


Receive Mail PDU

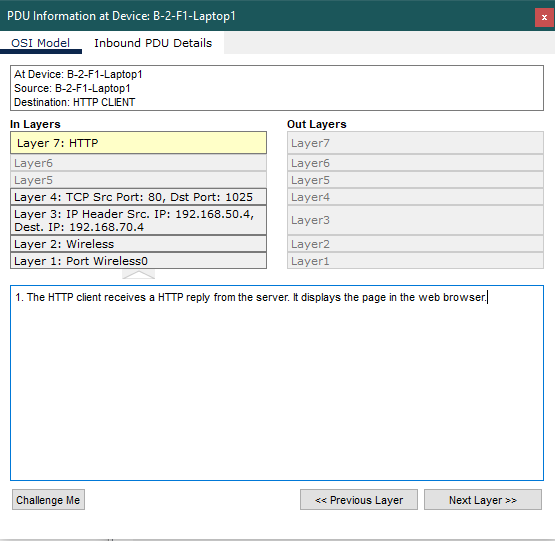
The user of B2-F1\_Laptop1 was able to access the web server by communicating through the browser. The network devices that were involved in this process are listed below:

B2-F1\_Laptop1, Branch-2\_Facility-1-Wireless Access Point, Branch-2\_Facility-1\_Switch, B2\_F1\_F2\_Router, Branch-1\_Facility-3\_Router, Branch-1\_Facility-3\_Switch, Web Server.

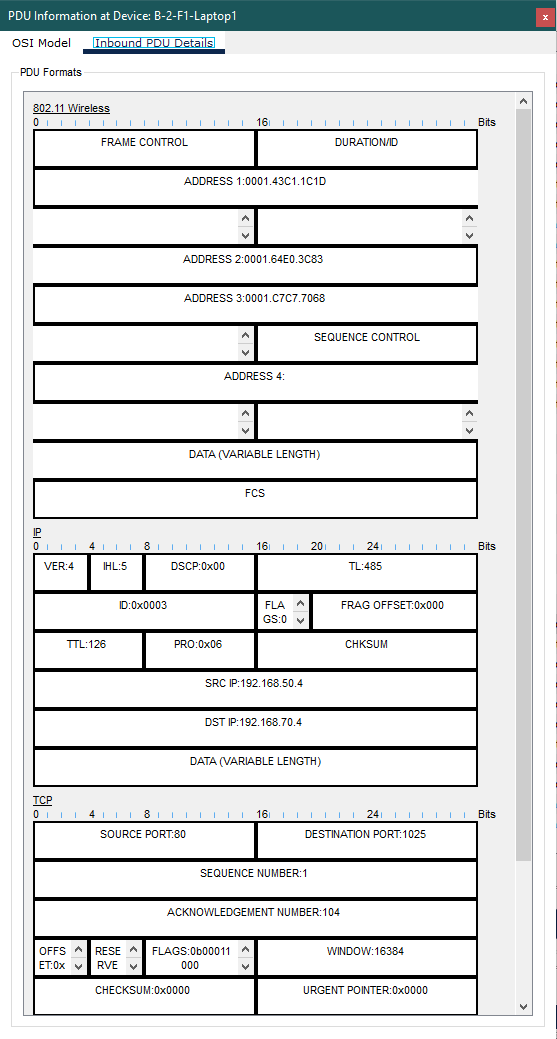
Browse Web Result



Browse Web Event List



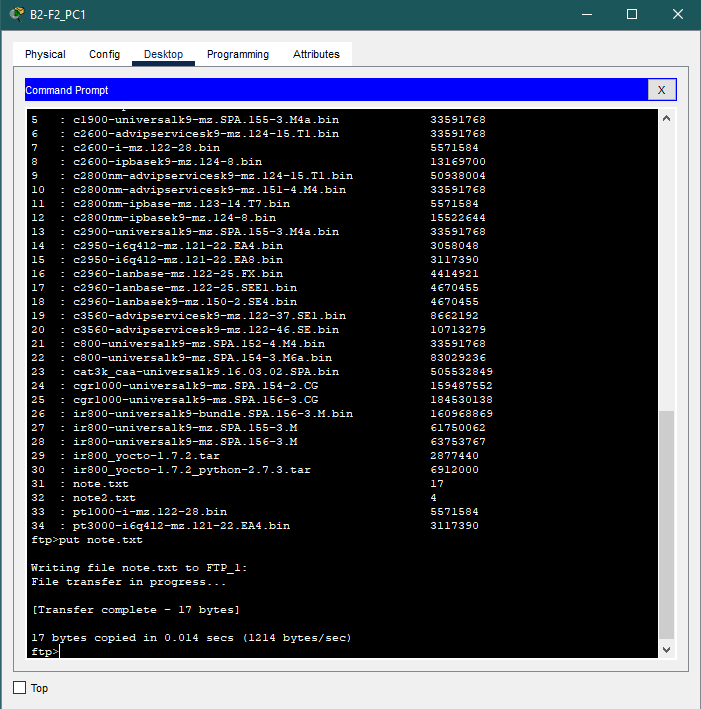
Browse Web OSI Model



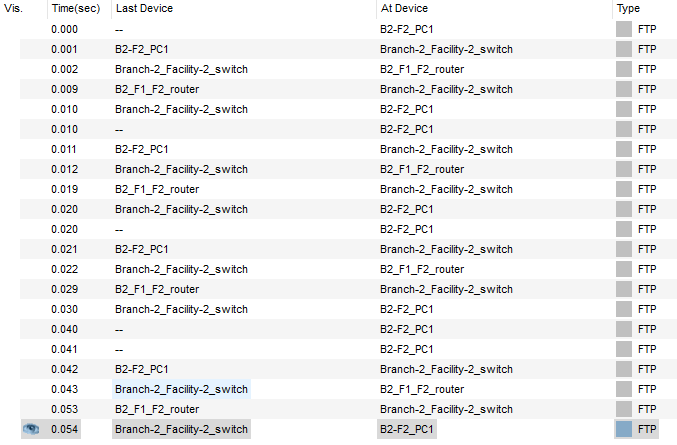
Browse Web PDU Information

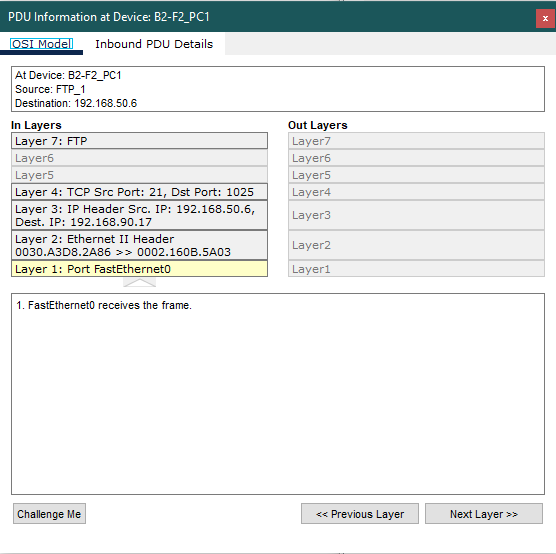
**Scenario 2**: A computer engineer from second facility of second branch developed a web application and wants to send her code files to FTP server in the third facility of first branch.

Established network connectivity between the FTP server and the user B2-F2-PC1. The network route taken when transmitting files to the FTP server from the B2-F2-PC1 user is as outlined below. B2-F2-PC1, Switch at Branch-2\_Facility-2, Router B2\_F1\_F2, Router at Branch-1\_Facility-3, Switch at Branch-1\_Facility-3, and FTP\_1.

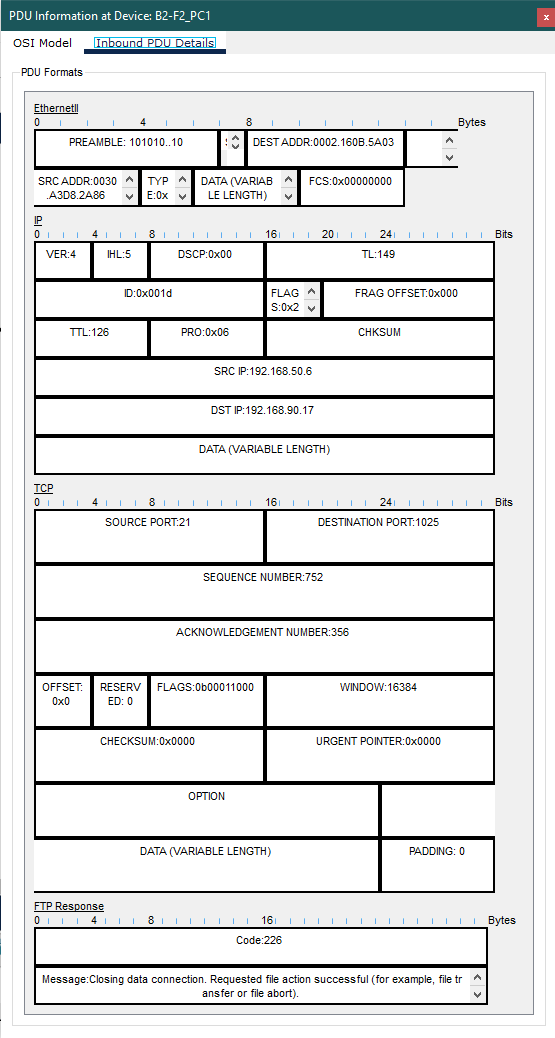


File Upload Result

File Upload Event List



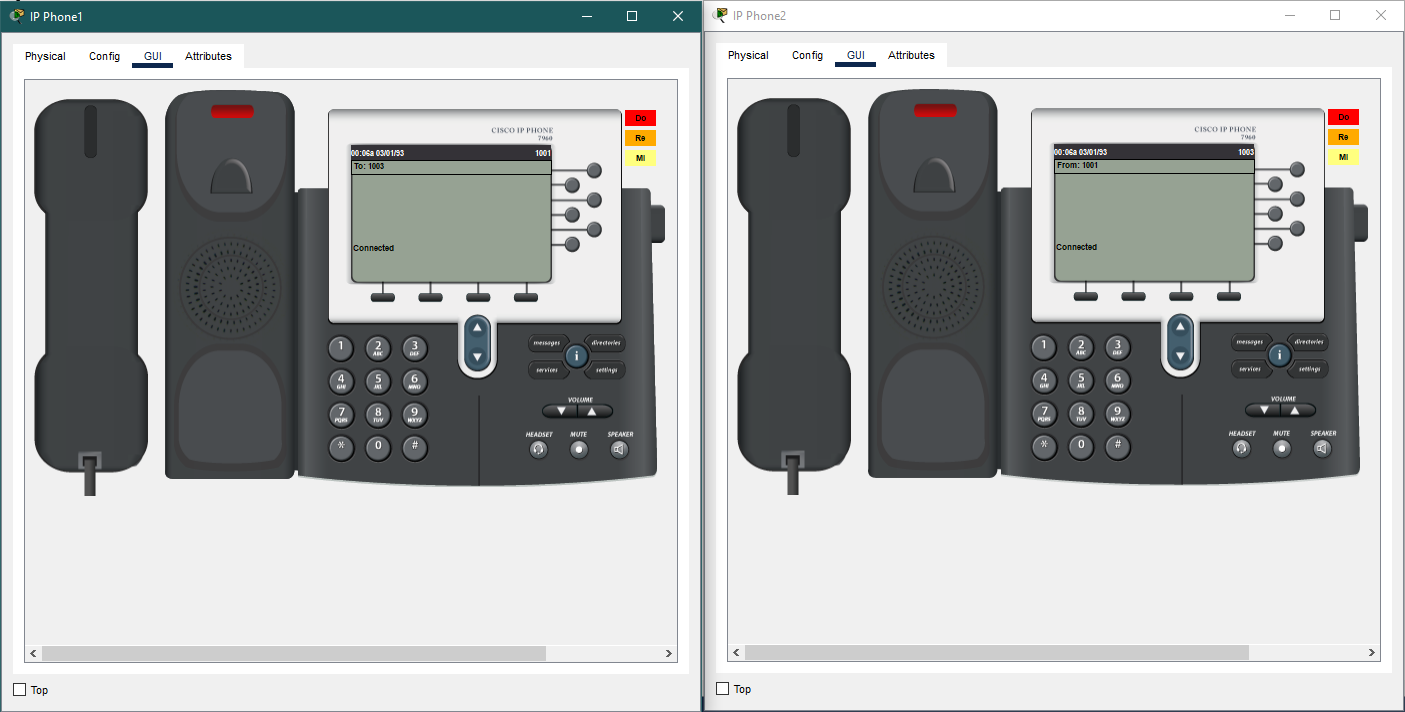
Upload OSI Model



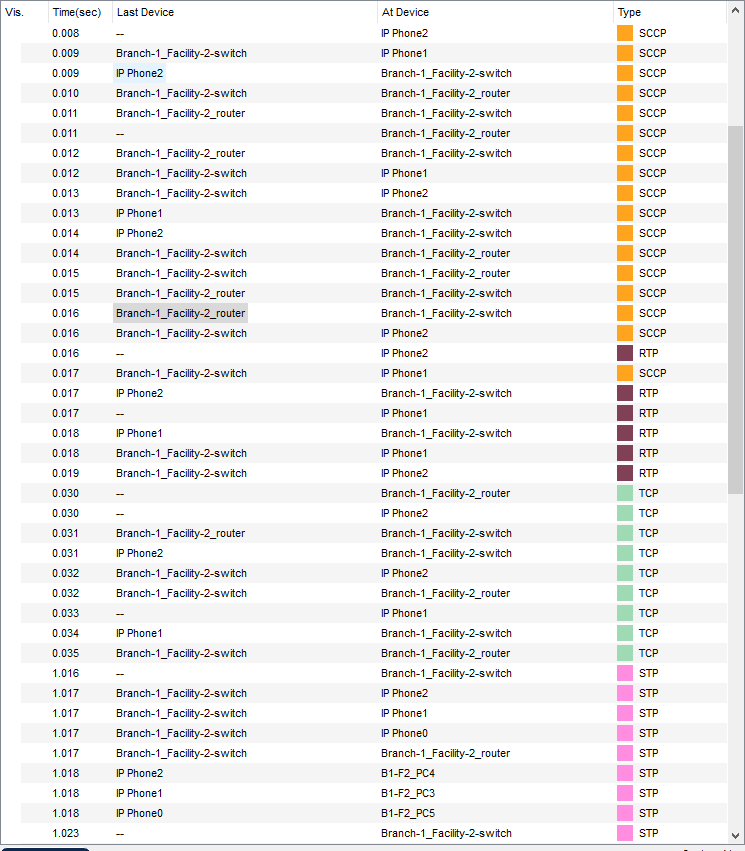
File Upload PDU Information

**Scenario 3:** Two users from second facility of first branch want to talk via VoIP.

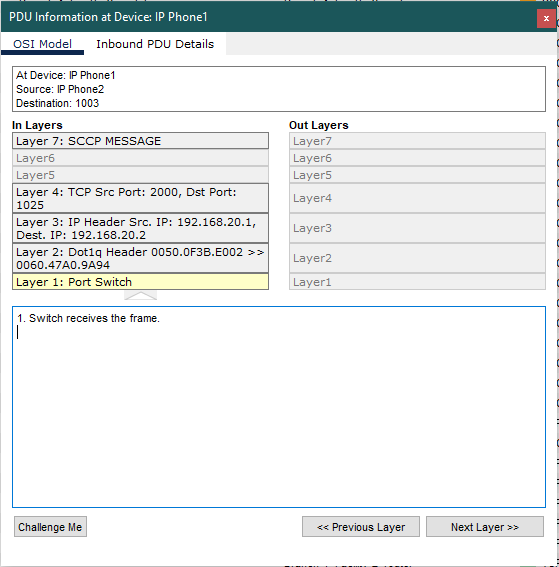
A VoIP conference took place between the user of IP Phone1 and the user of IP Phone2. The network route followed for this situation is as outlined below. Switch at Branch-1\_Facility-2, Router at Branch-1\_Facility-2, Switch at Branch-1\_Facility-2, and IP Phone2.

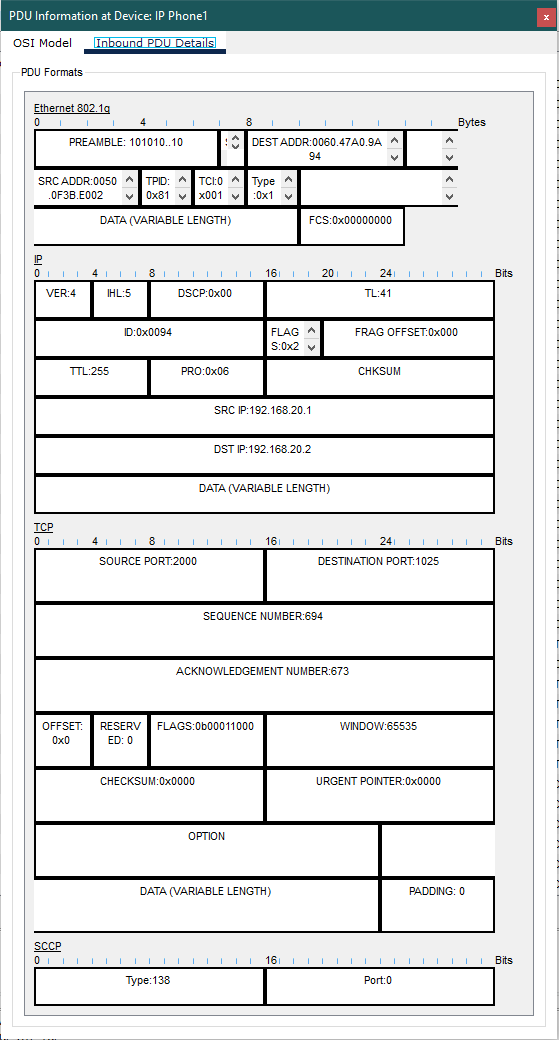


VoIP Conference Result



VoIP Conference Event List

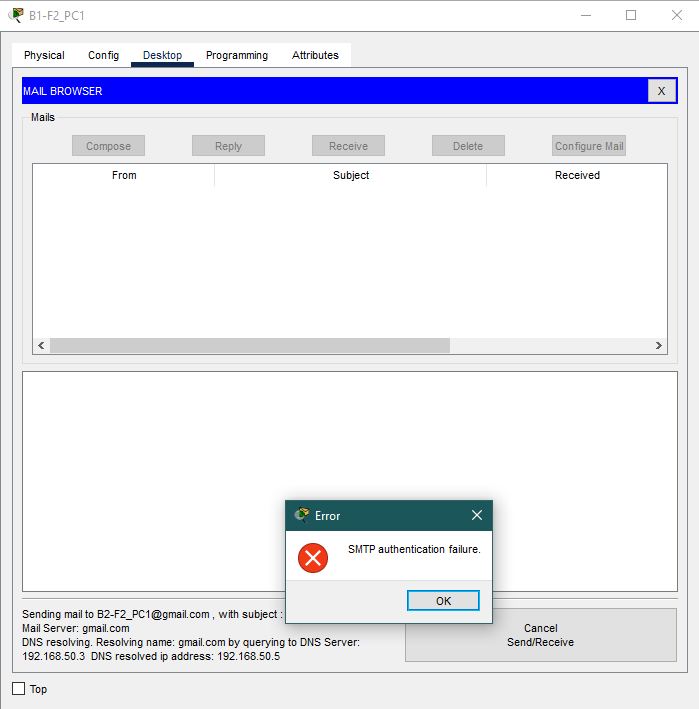
VoIP Conference OSI Model 



VoIP Conference PDU Details

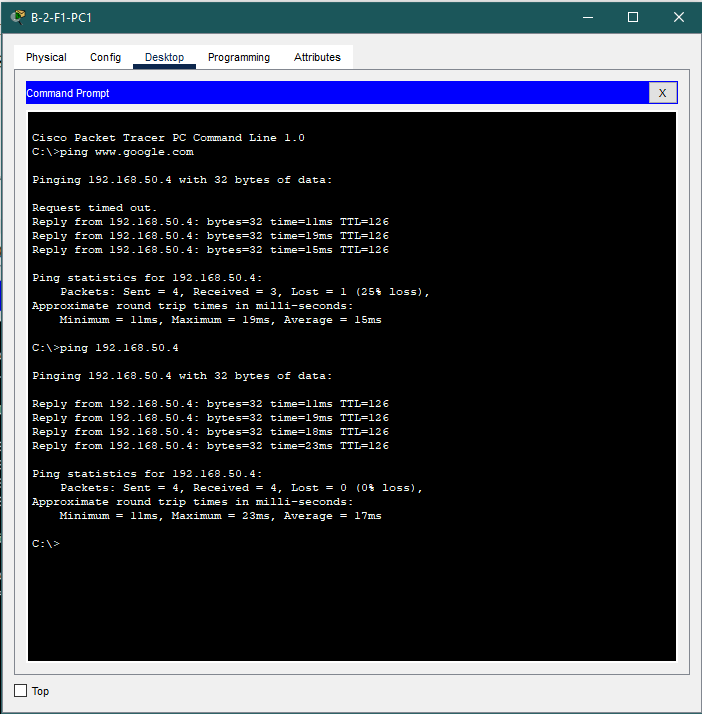
**Scenario 4:** A user in the second facility of first branch wants to send an email message to his friend in the second facility of second branch.

The users in the second facility of the first branch and the second facility of the second branch do not have permission to send or receive emails. Therefore, the workstation user in the second facility of the first branch was unable to send an email to the workstation user in the second facility of the second branch.

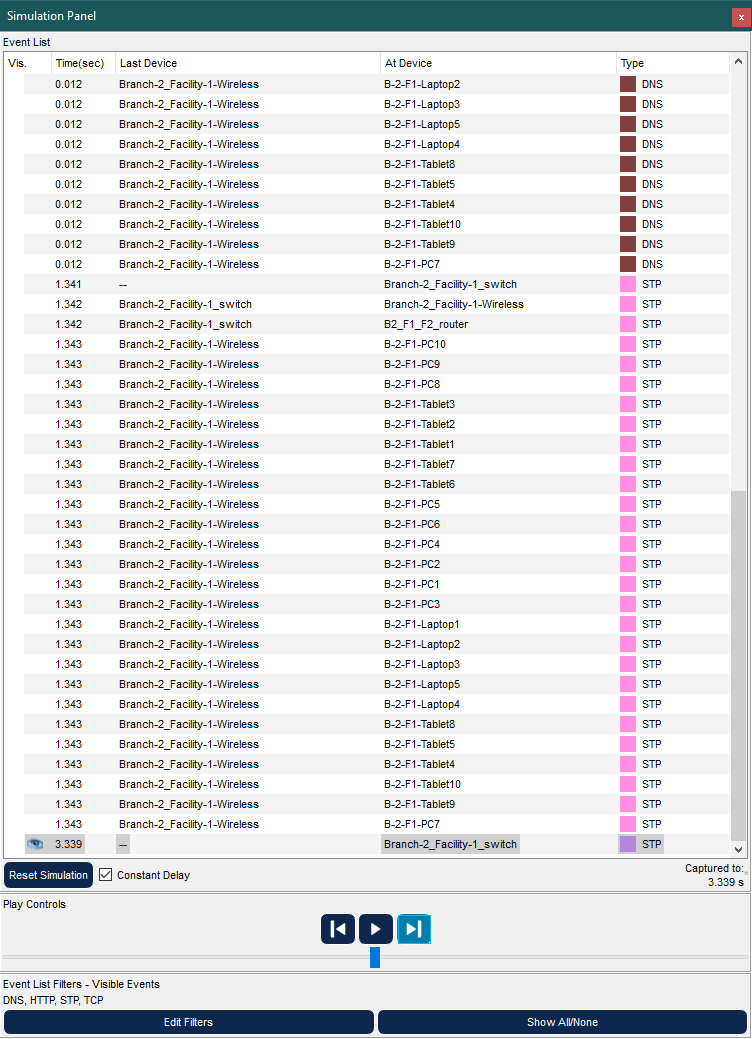


Since the devices in the second facility of either branch are not authorized to send or receive emails, their information is not stored in the mail server. Therefore, there is no way to authenticate the users in this facility, so this action results in SMTP authentication failure.

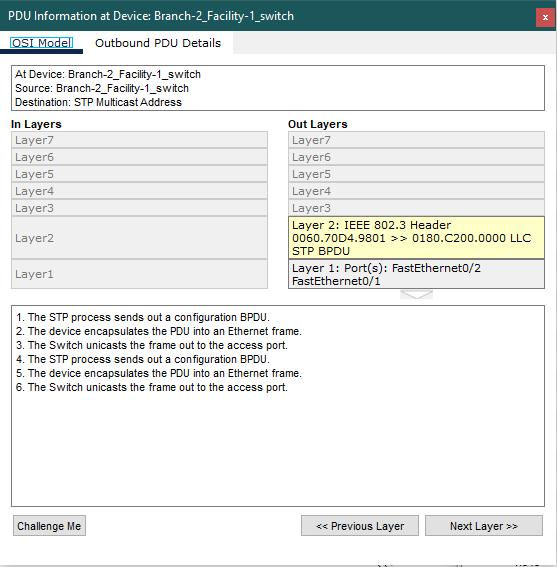
**Scenario 5:** A user from first facility of second branch pings Web server of second facility of first branch.

 A ping test was conducted between the web server and the B-2-F1-PC1 user. The network path taken in this scenario is as outlined below: B-2-F1-PC1, the wireless access point in Branch-2 Facility-1, the switch in Branch-2 Facility-1, the B2\_F1\_F2\_Router, the router in Branch-1 Facility-3, the switch in Branch-1 Facility-3, Google Server.

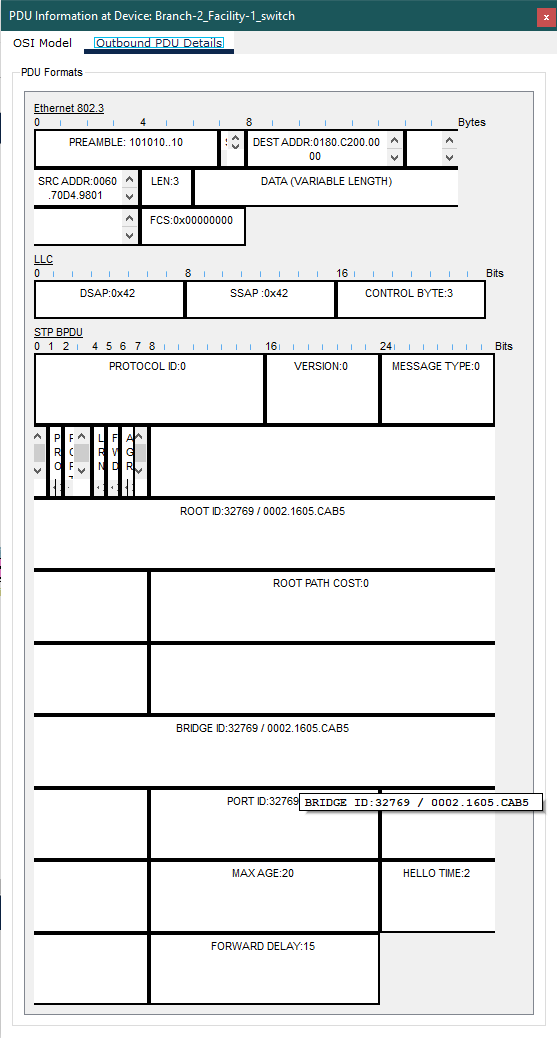
Ping Web Server Result



Ping Web Server Event List



Ping Web Server OSI Model



Ping Web Server PDU Information

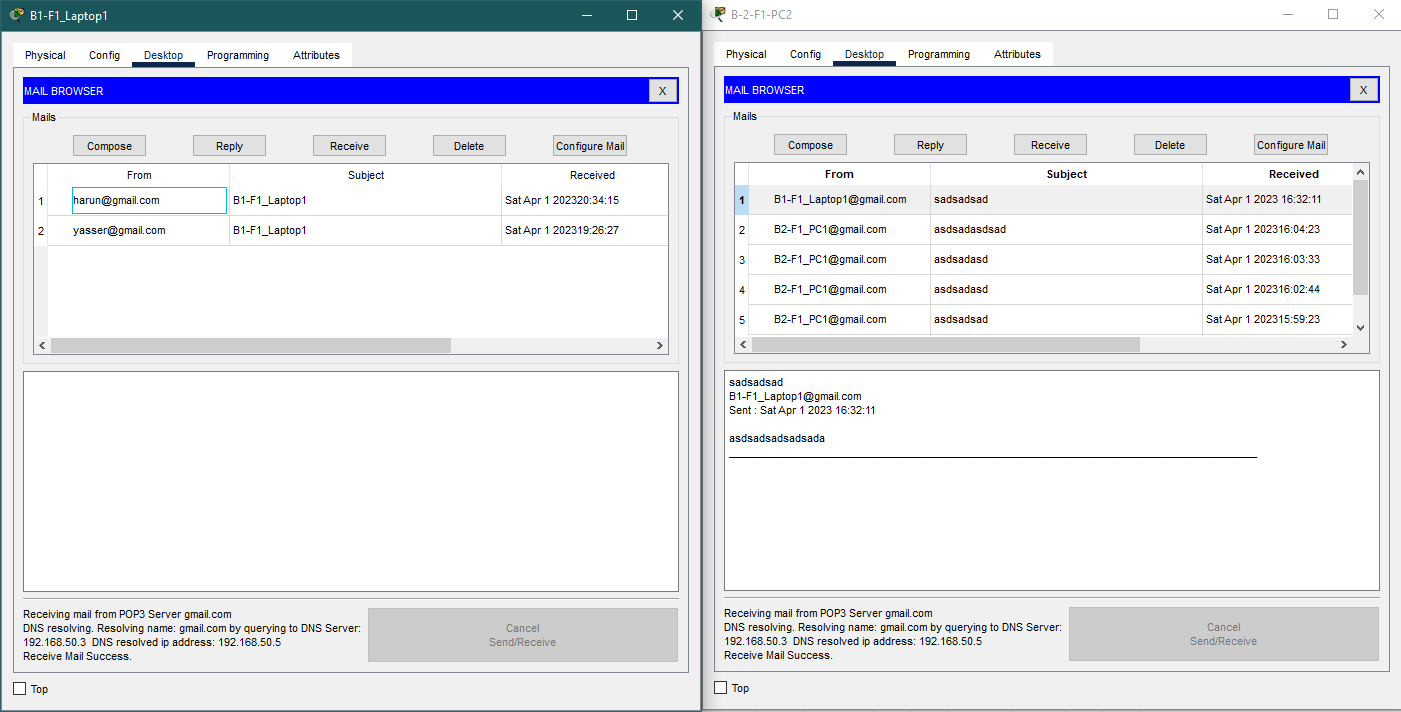
**Scenario 6:** A laptop user from first facility of first branch office wants to send email to her friend in the first facility of second branch office.

The user using B1-F1\_Laptop1 sent an email to B2-F1\_PC2, using the mail server. The path followed in this scenario is:

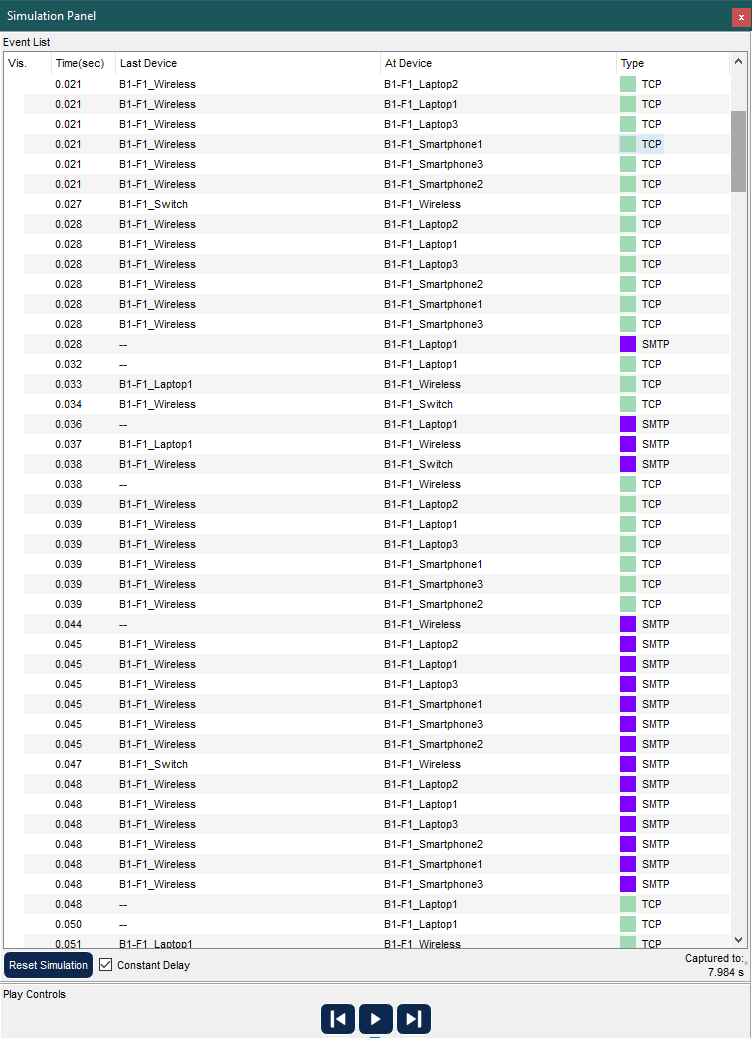
B1-F1\_Laptop1, B1-F1\_Wireless Access Point, B1\_F1\_F2\_Router, Branch-1\_Facility-3\_Router, Branch-1\_Facility-3\_Switch, Mail Server

Later, when the user using B2-F1\_PC2 wants to receive the mails sent, they will receive the mails from the mail server using the following path:

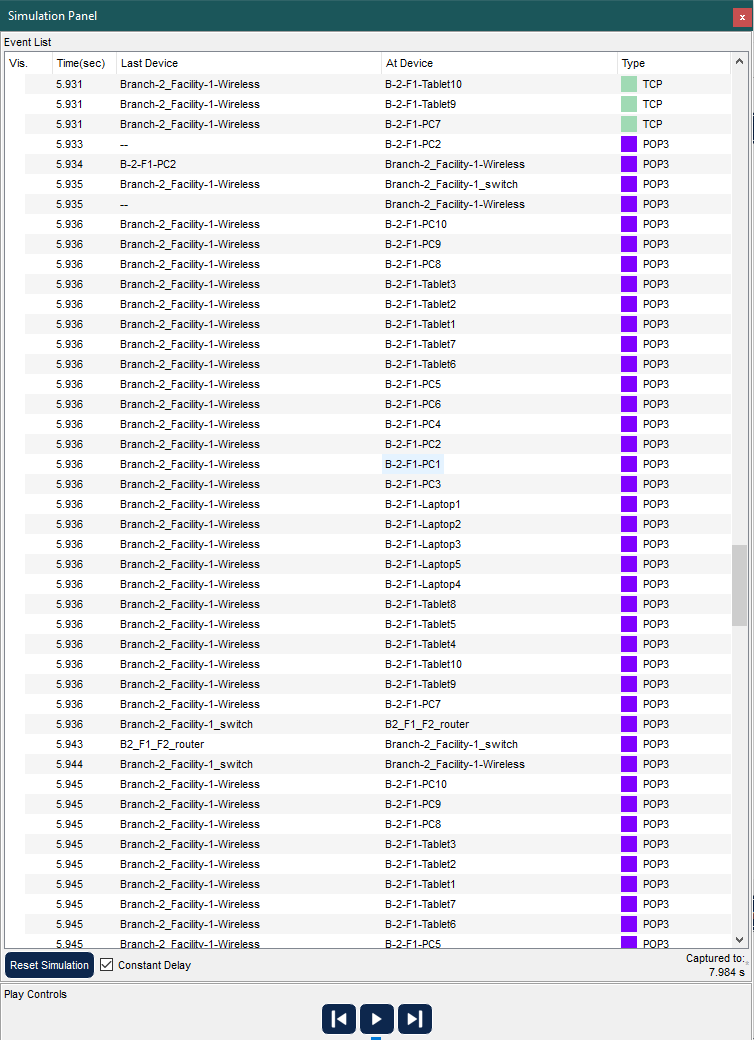
Branch-1\_Facility-3\_Switch, Branch-1\_Facility-3\_Router, B2\_F1\_F2\_router, Branch-2\_Facility-1\_Switch, Branch-2\_Facility-1-Wireless Access Point, B2-F1\_PC2.



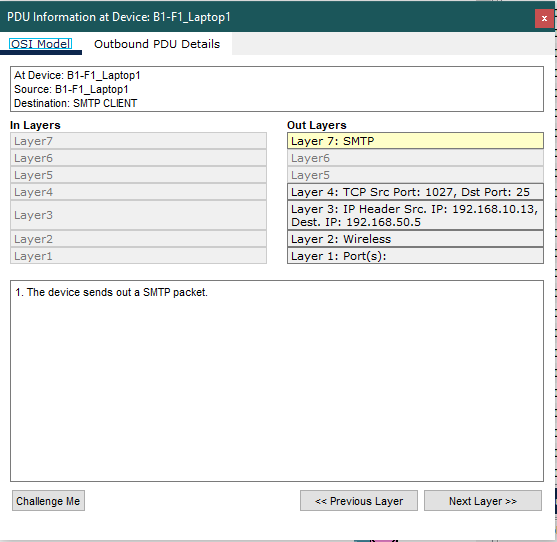
Send-Receive Mail Result



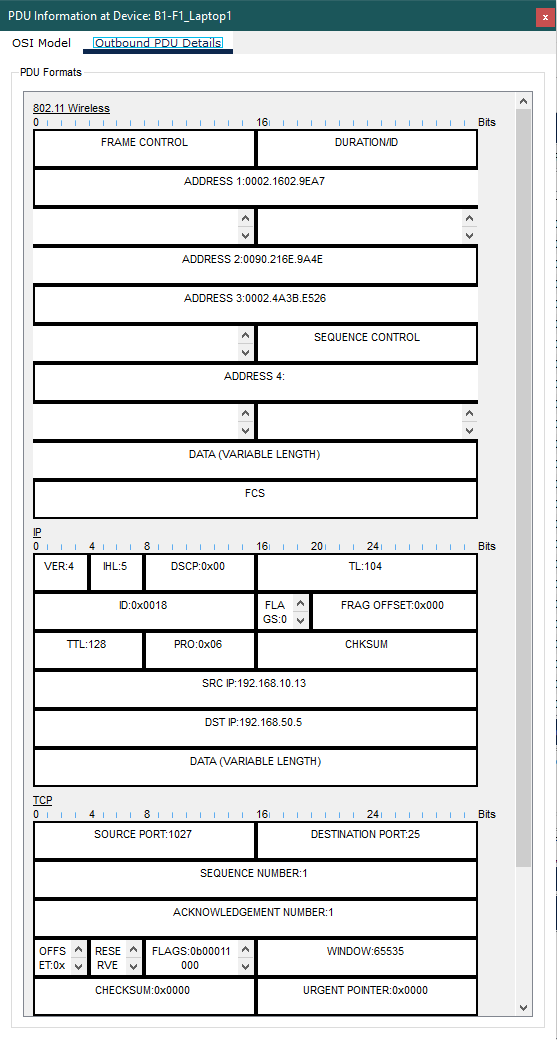
Send Mail Event List



Receive Mail Event List



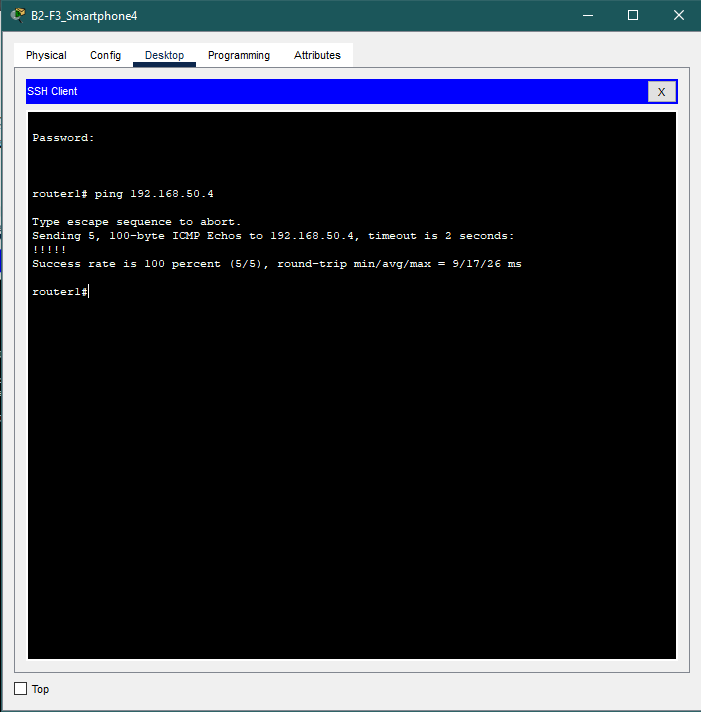
Send Mail OSI Model



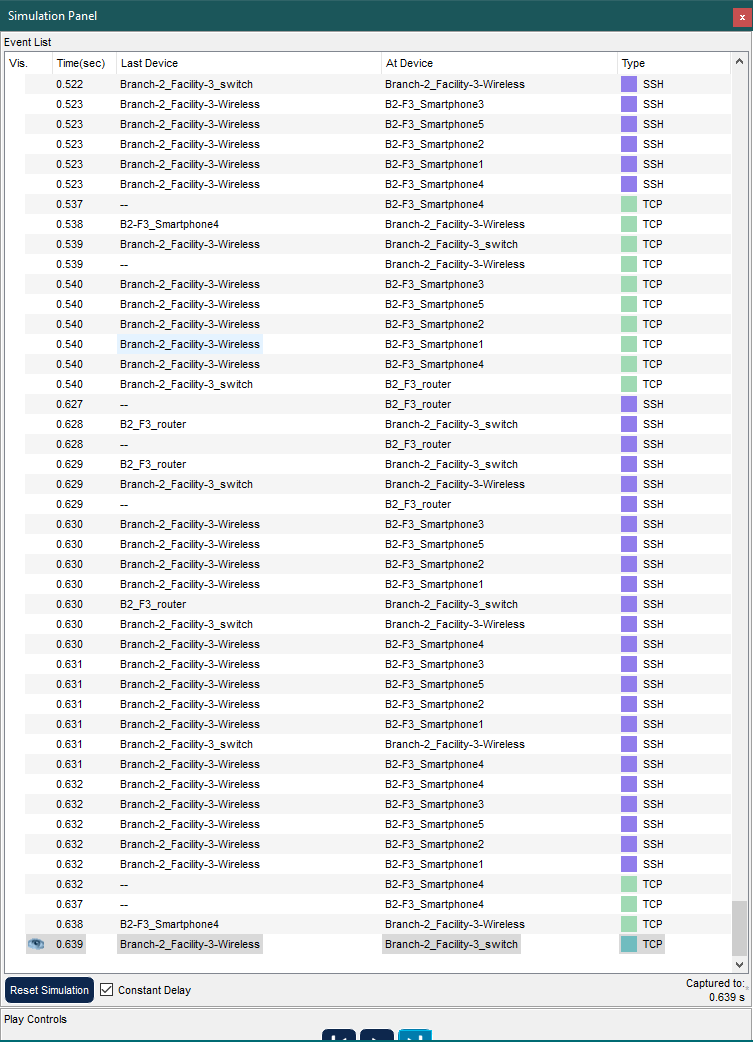
Send Mail PDU Information

**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.

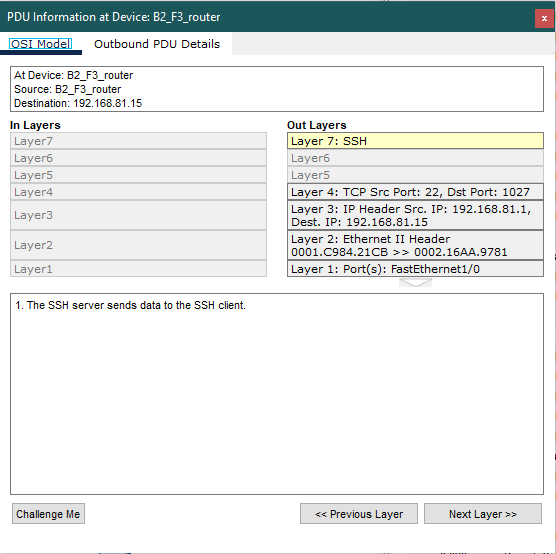
A SSH connection between B2-F3-Smartphone4 and Web Server was created with SSH protocol. The path used is as follows: B2-F3-Smartphone4,Branch-2\_Facility-3-Wireless, Branch-2\_Facility-3\_Switch, B2\_F3\_Router, B2\_F1\_F2\_Router, Branch-1\_Facility-3\_router, Branch-1\_Facility-3\_switch, Web Server.



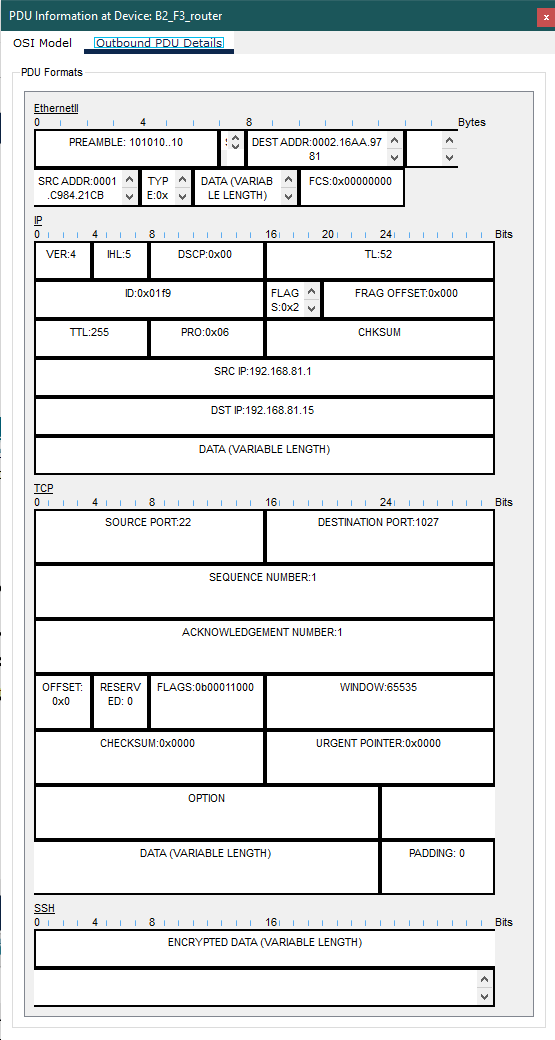
SSH Connection Result



SSH Connection Event List



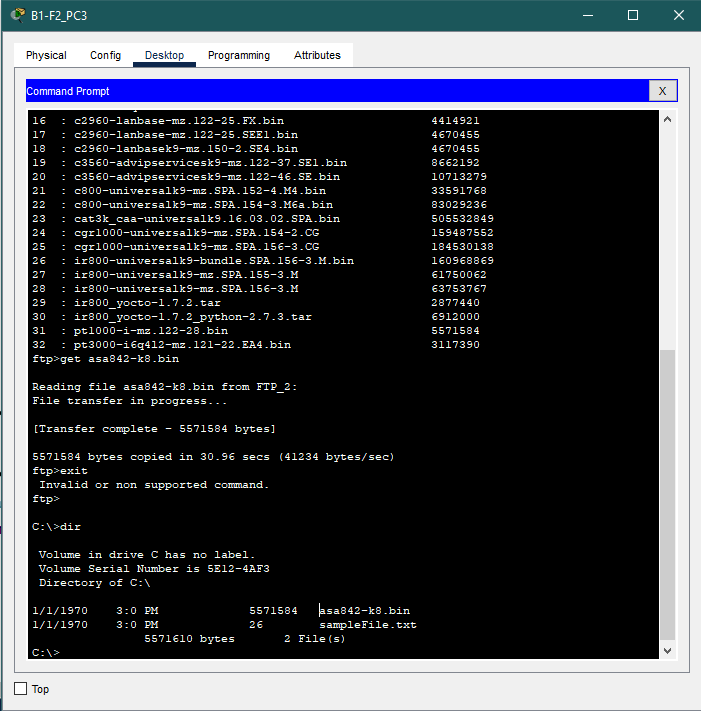
SSH Connection OSI Model



SSH Connection PDU Information

**Scenario 8**: A computer from second facility of first branch wants to download some scripts found in the second FTP server in the third facility of first branch.

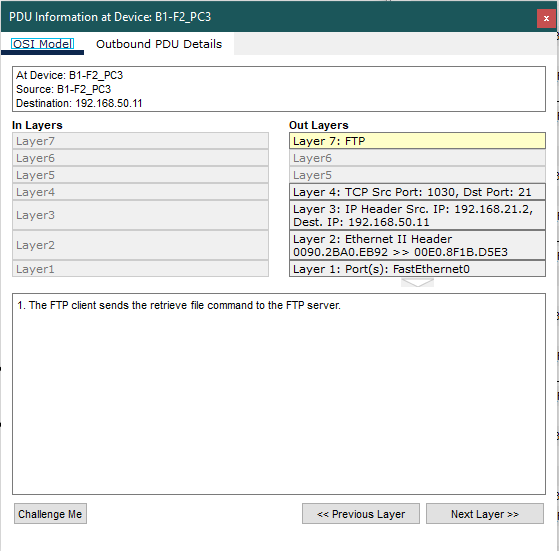
Established network connection between the FTP server and the user B1-F2-PC1. The network route taken when transmitting files to the FTP server from the B1-F2-PC1 user is as outlined below: B1-F2-PC3, Branch-1\_Facility-2-Switch, Branch-1\_Facility-2\_Router, B1\_F1\_F2\_router, Branch-1\_Facility-3\_Router, Branch-1\_Facility-3\_switch and FTP\_2.



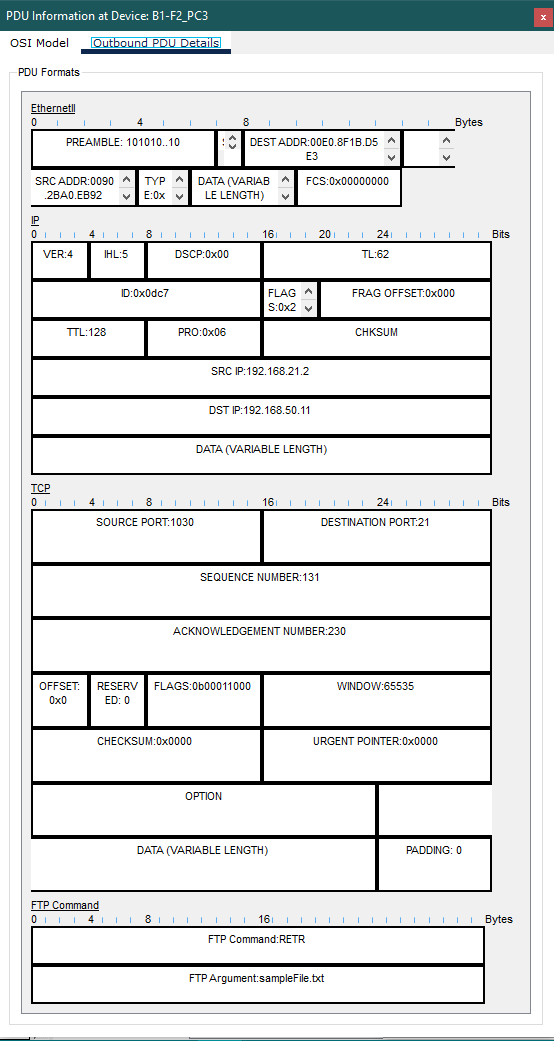
File Download Result



File Download Event List



File Download OSI Model

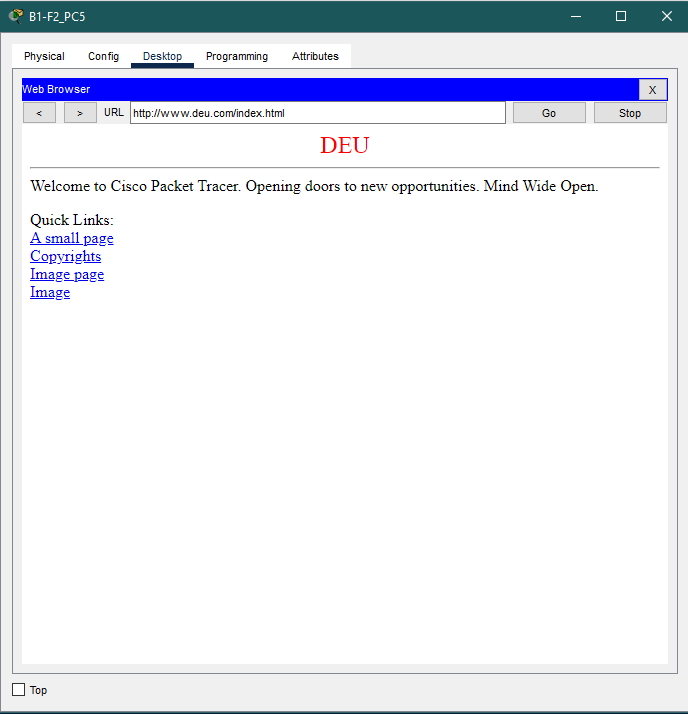


File Download PDU

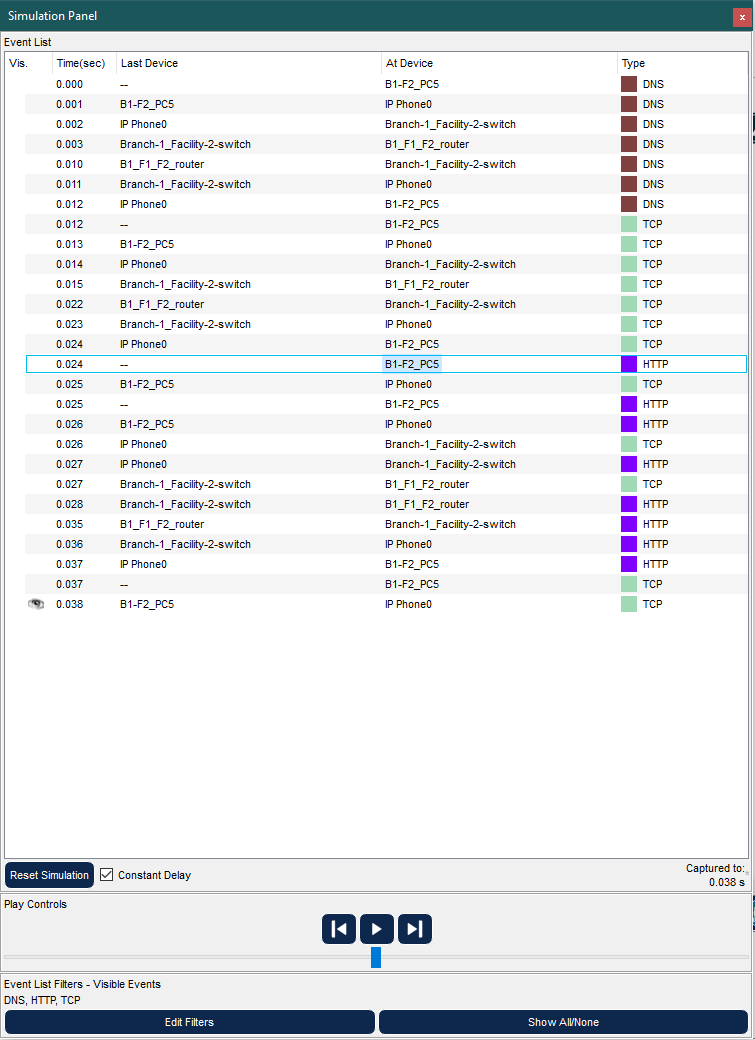
**Scenario 9:** A workstation user from the second facility of first branch wants to browse Web.

The user of B1-F2\_PC5 was able to access the web server by communicating through the browser. The network devices that were involved in this process are listed below:

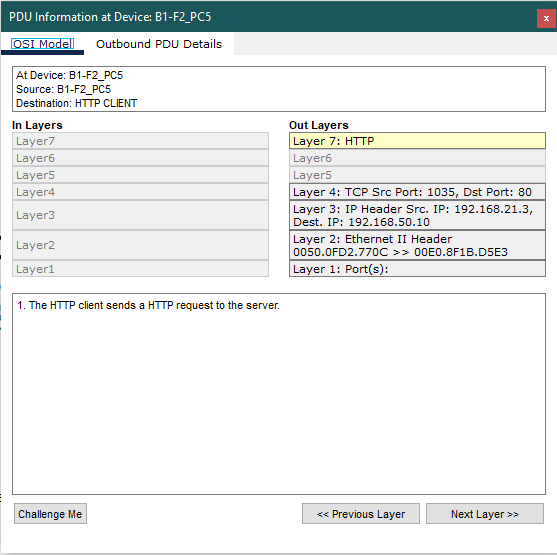
B1-F2\_PC5, Branch-1\_Facility-2-Switch, B1\_F1\_F2\_Router, Branch-1\_Facility-3\_Router, Branch-1\_Facility-3\_Switch, Web Server.



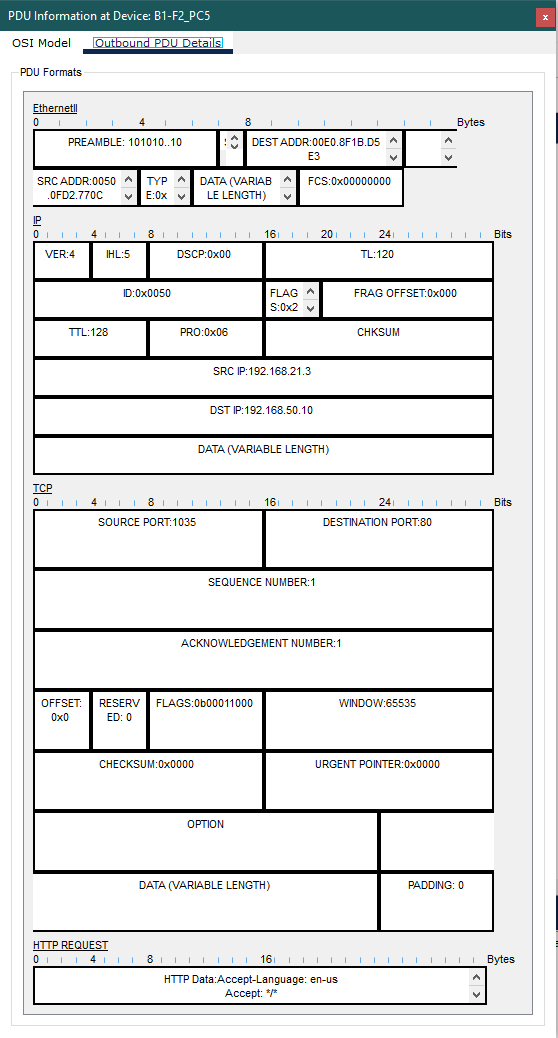
Browse Web Result



Browse Web Event List



Browse Web OSI Model



Browse Web PDU Information

CHAPTER 4

PROBLEMS ENCOUNTERED

**APIPA Error:**

APIPA stands for Automatic Private IP Addressing. It is a feature of Windows operating systems that allows computers to automatically assign themselves an IP address if they cannot find a DHCP server. When you encountered an APIPA error, it meant that the DHCP server was not able to assign IP addresses to the computers in the facilities. To solve this problem, you distributed the generated DHCP Pools via the Router with a few commands. This ensured that all of the computers in the facilities had access to a DHCP server, and that they could be assigned IP addresses automatically.

**“Buffer is full” Error:**

This error message means that the buffer that is used to store events is full. When this happens, new events cannot be added to the buffer, and they are lost. To solve this problem, you filtered the events. This means that you only allowed certain events to be stored in the buffer. By filtering the events, you were able to prevent the buffer from becoming full, and you ensured that all of the important events were stored.

CHAPTER 5

**CONCLUSION**

A Metropolitan Area Network (MAN) simulation was conducted to connect two branches of a company, each with three facilities. The goal of the project was to allow users to communicate, transfer files, and browse the web. To complete the project, the group members had to research the necessary devices and configurations. They also had to observe the desired scenarios, analyze and test them, and select the desired features and tasks for the topology and architecture. The group members successfully completed the project by working accurately, communicating consistently, and being meticulous in each step. They used a metropolitan area network (MAN) instead of a wide area network (WAN) to achieve the desired security and speed. The network successfully provided the requested services using the protocols specified in the report. As a result, users in each facility could perform their tasks, and communication was possible between users in the same facility or different facilities and branches. The servers in the project could also be used collaboratively by both branches. In short, the MAN simulation was a success. It allowed the company to connect its two branches and provide users with the services they needed.

CHAPTER 6

REFERENCES

**[1]** M. Ozdemir, "Cisco Packet Tracer’da VoIP Nasıl yapılır?," Journal of Computer Networks and Communications, vol. 2018, Article ID 1740195, 2018.

**[2]** K. Sharma and A. Saini, "How to configure an FTP server in Packet Tracer," International Journal of Engineering Research and Technology, vol. 7, no. 12, pp. 249-251, 2018.

**[3]** V. B. Yadav and S. K. Singh, "Configuration of SSH on Cisco Switch in Packet Tracer," International Journal of Advanced Research in Computer Science, vol. 8, no. 5, pp. 28-32, 2017.

**[4]** J. N. O. Odeyemi and O. D. Ogunseye, "Web Traffic Simulation using Cisco Packet Tracer," International Journal of Computer Applications, vol. 179, no. 6, pp. 1-5, 2021.

**[5]** S. K. Singh and V. B. Yadav, "Email Server Configuration in Cisco Packet Tracer | Cisco Packet Tracer Email Server | Mail Server," International Journal of Advanced Research in Computer Science, vol. 9, no. 2, pp. 11-14, 2018.

**[6]** M. K. Das, "Packet Tracer – Web and Email," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 7, no. 7, pp. 294-297, 2017.

**[7]** R. Singh and S. K. Singh, "DNS, SMTP, FTP, and WEB Server configuration in packet tracer," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 9, no. 5, pp. 34-37, 2019.

**[8]** M. K. Das and S. K. Mohanty, "Web Server Configuration in Cisco Packet Tracer," International Journal of Computer Science and Mobile Computing, vol. 6, no. 10, pp. 10-13, 2017.

**[9]** A. Khawaja and A. Hussain, "DHCP FAILED APIPA IS USED," Proceedings of the 2017 IEEE Conference on Information and Communication Technologies, pp. 245-248, 2017.

[10] IBM Corporation, "The Fundamentals of Networking," IBM Cloud Learn Hub, 2021. [Online]. Available: <https://www.ibm.com/cloud/learn/networking>. [Accessed: May 11, 2023].

[11] S. K. Singh and V. B. Yadav, "Wireless Router configuration in Cisco Packet Tracer," International Journal of Advanced Research in Computer Science, vol. 8, no. 2, pp. 19-22, 2017.