# DOKUZ EYLUL UNIVERSITY

# ENGINEERING FACULTY

# DEPARTMENT OF COMPUTER ENGINEERING

## CME3204 DATA COMMUNICATIONS AND COMPUTER NETWORKS

## METROPOLITAN AREA NETWORK REPORT


| | |
|---|---|
| **Sena Yurtseven** | **2017510001** |
| **Burcu Ağdar** | **2017510014** |
| **Emirhan Bilge Bulut** | **2017510020** |

# 1. INTRODUCTION

## 1.1 Project Definition and Problem Formulation

Before starting the project, we watched cisco packet tracer training videos and made simple experiments. Afterwards, we set up the communications and communication within the first building itself. Here we discussed whether we should give DHCP or give our IPs as static. We decided that it would be more logical to give static IP so that we could access them from different branches.

For the 3rd Facility of the 1st Branch, we created the servers and their structure, and tested the communications within them. Then we tried to access the servers with the 1st Facility and tested the servers. We made DNS settings for the communication of servers with 1.Facilty. We directly gave Static IP assignments of the servers, saying that they should be similar to the real world. We realized that the servers should be static while the IPs of the end users can be assigned by DHCP. In 1.Branchin 2.Facility, we tried to understand how VoIP communication is and vlan structure. While we were communicating with vlan here, we could not communicate with the outside world because of the vlan structure and because we gave the gateway as the vlan gateway. Another problem we have here is that we initially added a router for the PCs next to the VoIP structure, and we used 2 routers within the facility to communicate with each other over Serial ports. Then, in the first Branch, we made routing operations on serial ports for the routers to communicate among themselves. The first branch was communicating among themselves, but VoIP could not reach other computers or servers in its own branch.For this, we arranged the gateway according to the vlan settings and we did the routing operations over the vlan ips for the communication of serial ports and routers.

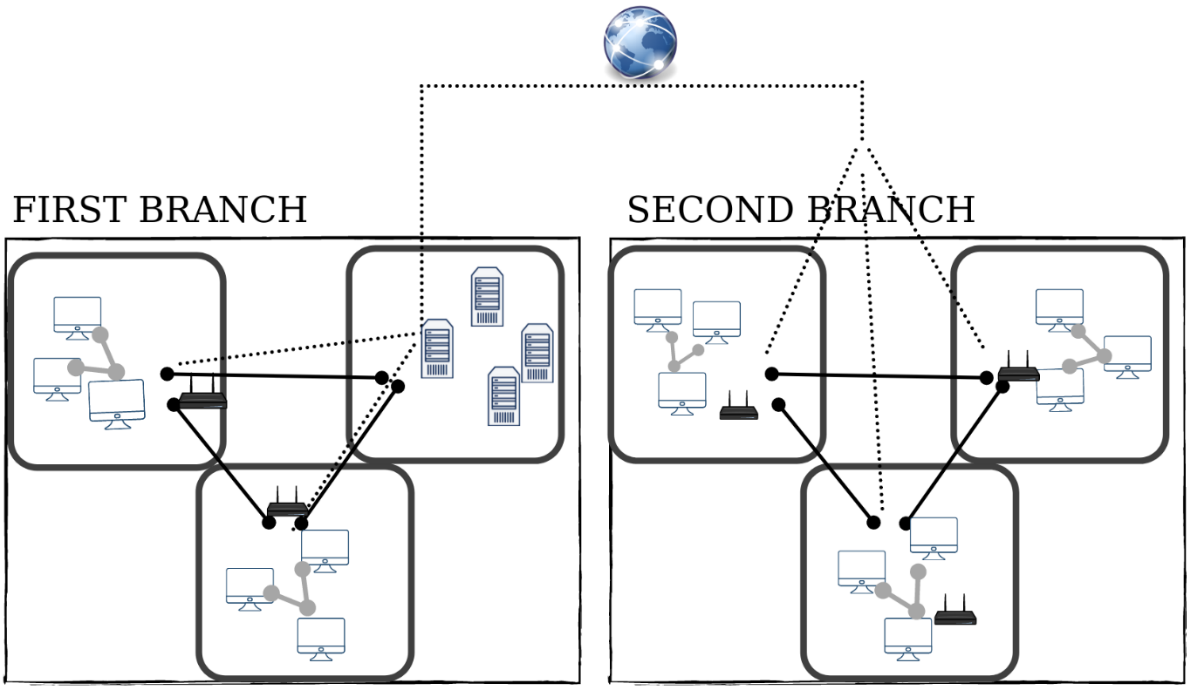
When we moved to the second branch, we quickly created a structure that communicates using 1 router and 1 switch for each facility, since there is no special structure such as VoIP or a special structure such as servers. Since they need to be connected to the ISP here, we researched how to design that structure and tried to make a few applications. Here at the same time, we tried to give what is required by writing code on an application that can run on the web, on computers or any device. By writing code in Python language, we installed an application that can be used by all computers on a client basis. By connecting the routers in a triangle shape, we ensured that in case of a connection failure (between facilites), the communication continues and the whole system does not crash. By using separate modems for each facility to connect to the ISP, we aimed to distribute all the connection to the ISP in this way, and in case of a problem in any facility, the other facility would not have a problem.

The modem we used here was a DSL modem, and we looked at which would be the fastest port for the modem we used to have a fast internet connection. Here, we saw that the FastEthernet port has 100mbs speed support, and when we added the Gigabit port, we had problems in the system and that the gigabit port is only 1 in our router model and we could not add it. Thinking that 100mbs would be enough for each facility, we decided that we would connect both to each other and to the ISP via FastEthernet ports. Here, we realized that when we want to use gigbait ethernet ports in other router models, we cannot use it due to the lack of ports.

Since the ISP will communicate between 2 branches, we connected the servers that I was going to communicate with in the first branch to the ISP in the 1st branch.This is how we connected and communicated the 2. Branch with the ISP. Here we tried to set the authentication and sync settings on the ISP and they did not connect initially. We re-adjusted our DNS settings and the 1st Branch Servers to connect to the ISP by removing the IPs that I gave at the beginning, and we created a vlan structure and allowed them to be customized within themselves.

In order for the first branch to be able to connect to the servers and send mail, we also connected the parts of the first branch to the modems and made them go to the servers. Here, we had to change the DNS settings and ip settings we made at first. At the same time, since 2 branches will communicate through the ISP, we removed the routers so that the ISP settings were correct, and we provided this process with new IPs and different ports that we added to the router, as in the 2nd Branch.

We tested whether the communication between the two branches could be established, file sending operations and mail operations. We removed this build because it had problems getting to the outside world and ISP in VoIP. We came to a decision by discussing the gateway and vlan settings necessary for VoIP to open up to the outside world and to make calls within itself,and we implemented it. We tested things like routing and file operations in system operation and added information about connections through notes.




**Model of MAN**

## 1.2 The purpose and motivation of the project

Our motivation in this project was to learn how to set up the real network, what problems we might encounter before directly designing the system, and how we can overcome them. Our main motivation was to learn this tool, which enables us to overcome problems faster in terms of material and time, and by seeing through simulation, without directly adapting it to real life in the design of a network. After installing the system in real life, encountering and overcoming errors will be more difficult, more costly and time-consuming. We can quickly set up, test and see the errors on the simulation, which will take the time we spend to set up and test a system. In addition, it is more difficult to detect a problem in real life. The disadvantage of simulation is that sometimes some problems may arise due to environmental conditions and unexpected environmental conditions in real life. Our system, which is correct in simulation and theory, may not work in real life due to environmental conditions and some factors, may fail, and may not perform as expected. Also, while things like wiring are easy to do in simulation and in the project, they can be difficult to set up in real life or problems like cable clutter can occur. Considering the general framework, using simulations and models will be a logical choice, as in this project, if the affordability of the risk factor is also evaluated.

## 1.3 Term Definition

*IP*: An IP address is a unique address that identifies a device on the internet or a local network.

*SERVER*: A computer or computer program which manages access to a centralized resource or service in a network.

*SWITCH* : A **switch** is a device in a computer **network** that connects other devices together.

*ROUTER* : A **router** is a switching device for **networks**, which is able to route **network** packets, based on their addresses, to other **networks** or devices.STP : **Spanning Tree** Protocol (**STP**) is a Layer 2 protocol that runs on bridges and switches

*MODEM* : Modem is short for "Modulator-Demodulator." It is a hardware component that allows a computer or another device, such as a router or switch, to connect to the Internet.

*PROTOCOL* : A **network protocol** is an established set of rules that determine how data is transmitted between different devices in the same **network**.

*NETWORK* : A network, in computing, is a group of two or more devices or nodes that can communicate. The devices or nodes in question can be connected by physical or wireless connections. The key is that there are at least two separate components, and they are connected.

*DNS* :The Domain Name System (**DNS**) turns domain names into IP addresses, which browsers use to load internet pages.

*FTP* :File transfer protocol (**FTP**) is a set of rules that computers follow for the transferring of files from one system to another over the internet.

*DHCP* : A **DHCP** Server is a **network** server that automatically provides and assigns IP addresses, default gateways and other **network** parameters to client devices.

*LOCAL AREA NETWORK* :A **local area network** (**LAN**) is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building.

*METROPOLITAN AREA NETWORK :* A metropolitan area **network** (**MAN**) is similar to a local area **network** (LAN) but spans an entire city or campus.

*CLOUD* :**Cloud networking**, or **cloud**-based **networking**, gives users access to **networking** resources through a centralized third-party provider operating inter-connected servers.

*ISP* : An Internet service provider (ISP) is an organization that provides a myriad of services for accessing, using, or participating in the Internet. Internet service providers can be organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned.

*ACCESS POINT* : An access point is a device that creates a wireless local area network, or WLAN, usually in an office or large building.

*SSH* :SSH, also known as Secure Shell or Secure Socket Shell, is a network protocol that gives users, particularly system administrators, a secure way to access a computer over an unsecured network

*VoIP* : Voice over Internet Protocol (VoIP) is a proven technology that lets anyone place phone calls over an internet connection.

*PACKET* : In networking, a packet is a small segment of a larger message.

*NODE*: In telecommunications networks, a node (Latin: nodus, ‘knot’) is either a redistribution point or a communication endpoint.

*CHANNEL* : channel is a communication medium, the path that data takes from source to destination.

*NETWORK ARCHITECTURE* :Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data.

*NETWORK TOPOLOGY* : The configuration, or topology, of a network is key to determining its performance. Network topology is the way a network is arranged, including the physical or logical description of how links and nodes are set up to relate to each other.

*PDU* : Stands for "Protocol Data Unit." A PDU is a specific block of information transferred over a network.

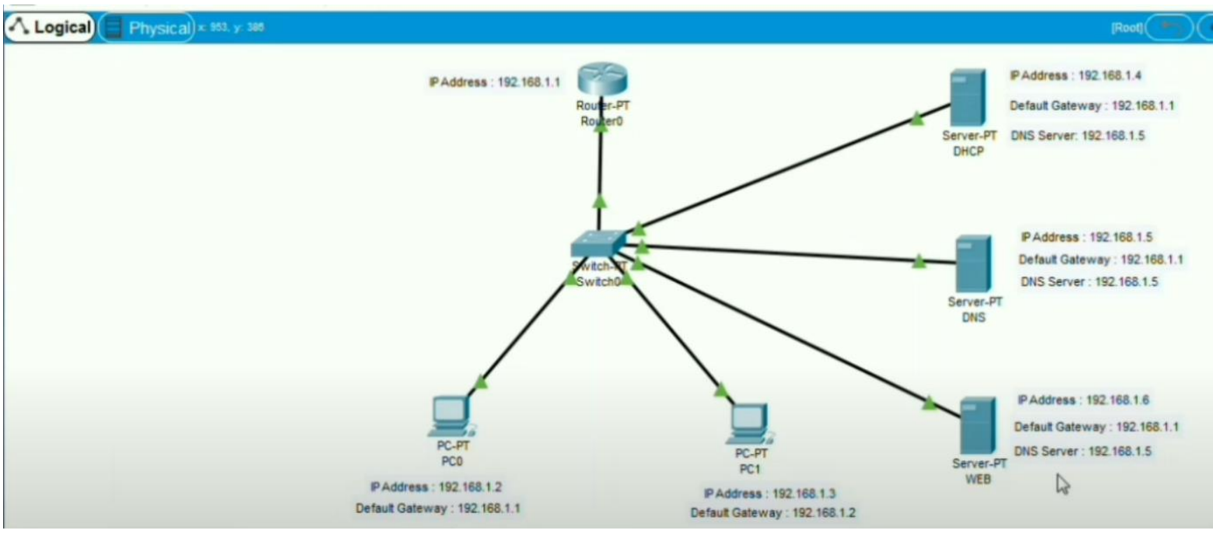
*OSI* : The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network.

*FRAME* : In networking, a frame is a unit of data. A frame works to help identify data packets used in networking and telecommunications structures.

*MOBILE DEVİCE* :A mobile device is a handheld tablet or other device that is made for portability, and is therefore both compact and lightweight.

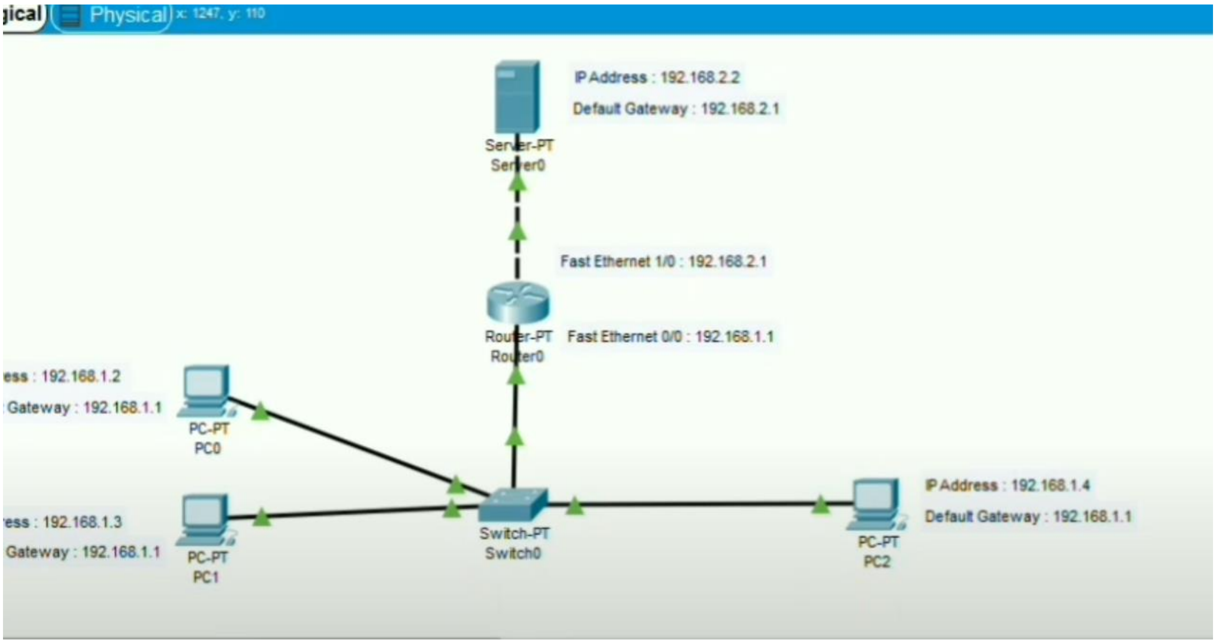
### 1.4 Related Work

- [1] Reference ( Web Server Configuration )



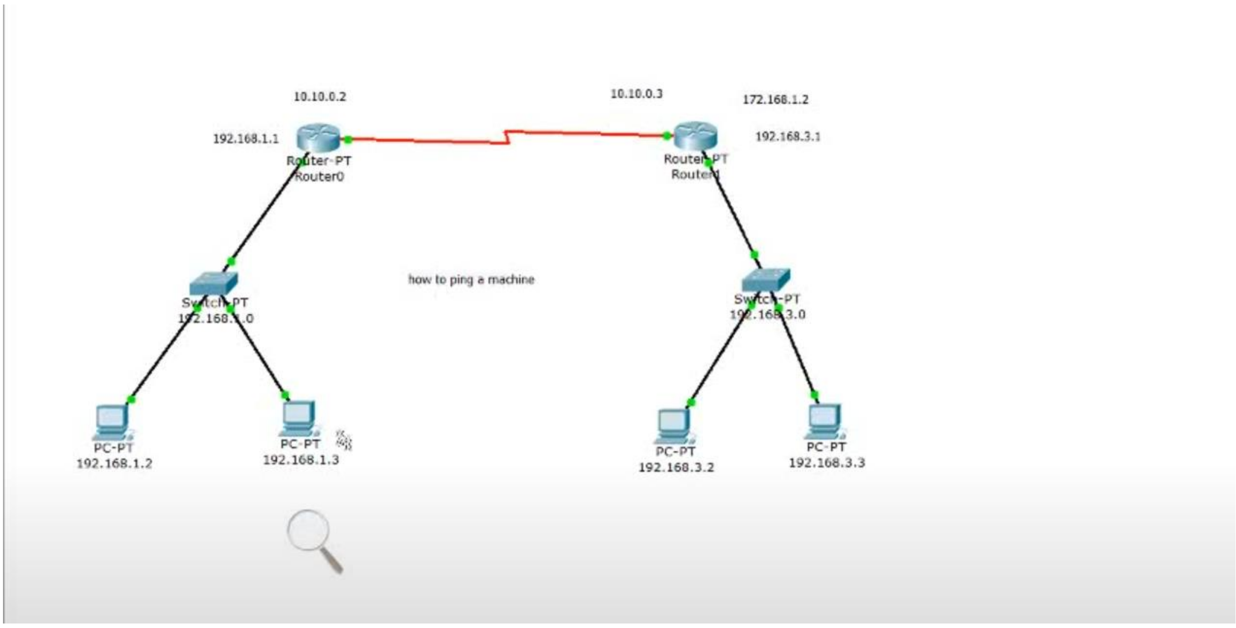

The design shown above can be seen as a **web server** modeling designed for a simple office. Three servers were used in modelling. DHCP server is the server that we use to distribute IP addresses quickly and automatically, DNS to provide double conversion between machine domain names and IP addresses, and Web server to access a web server. We are building a local network system consisting of servers and computers using a switch. The router seen here is used to establish a relationship with a different network structure.

- [2] Reference ( Email Server Configuration )



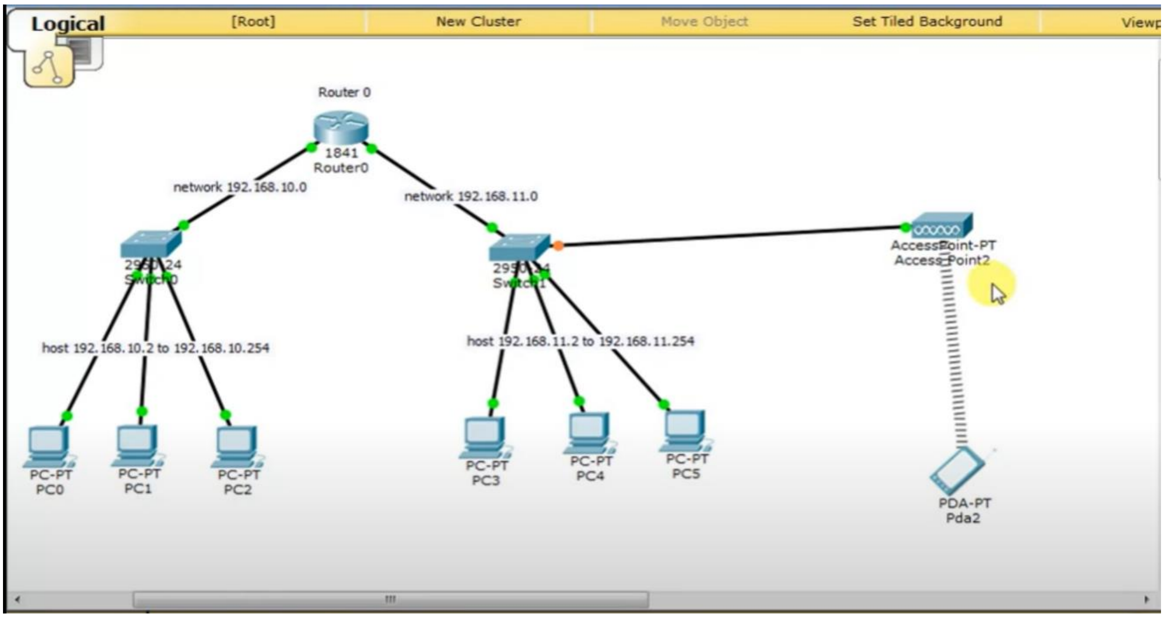

The design shown is a simple network model designed to send **e-mail between computers**. In the modeling shown, two different networks were created via a router. 1. A local network structure has been created between computers with the help of a switch in the network. The second network structure hosts a mail server. This server has kept the e-mail messages of the computers and made it accessible for every computer.

- [3] Reference ( Ping )



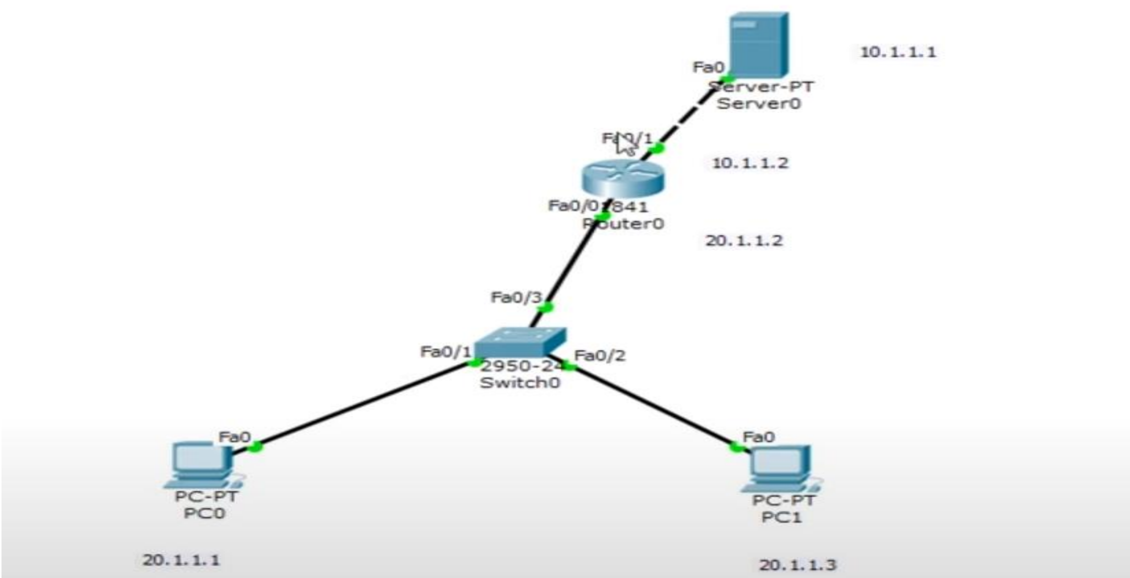

The design is a simple model of two **networks communicating via routers**. In the modeling seen, the first network has a local network with two computers in itself, and as it can be seen, the second network network structure also has a local network structure with two computers. These two routers are connected to each other with a serial structure and directing them correctly has allowed us to establish communication between computers.

- [4] Reference ( Wireless Device )



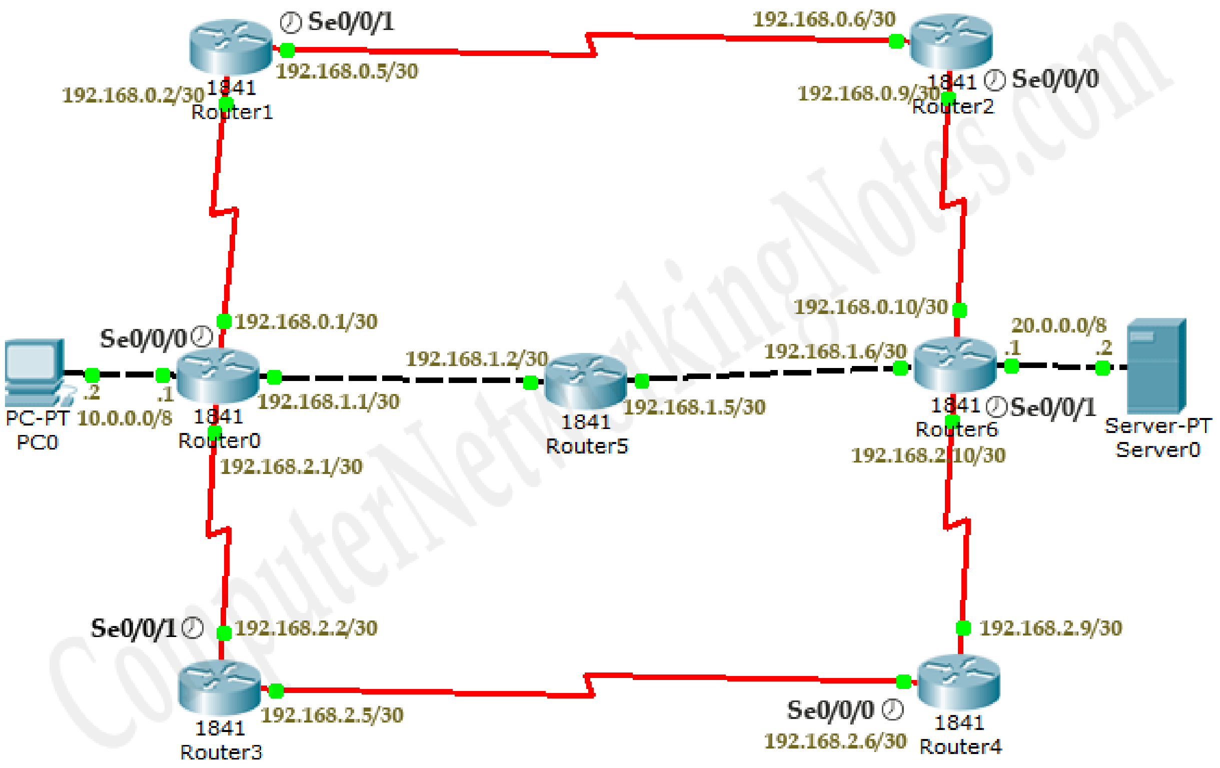

In the design seen, we see that there are two switches created over the router. These switches create local networks between computers for each network. We see that there is an access point connected to the second of the created networks. The access point here has enabled devices that cannot be connected via cable to connect wirelessly and enable them to participate in communication within the network.

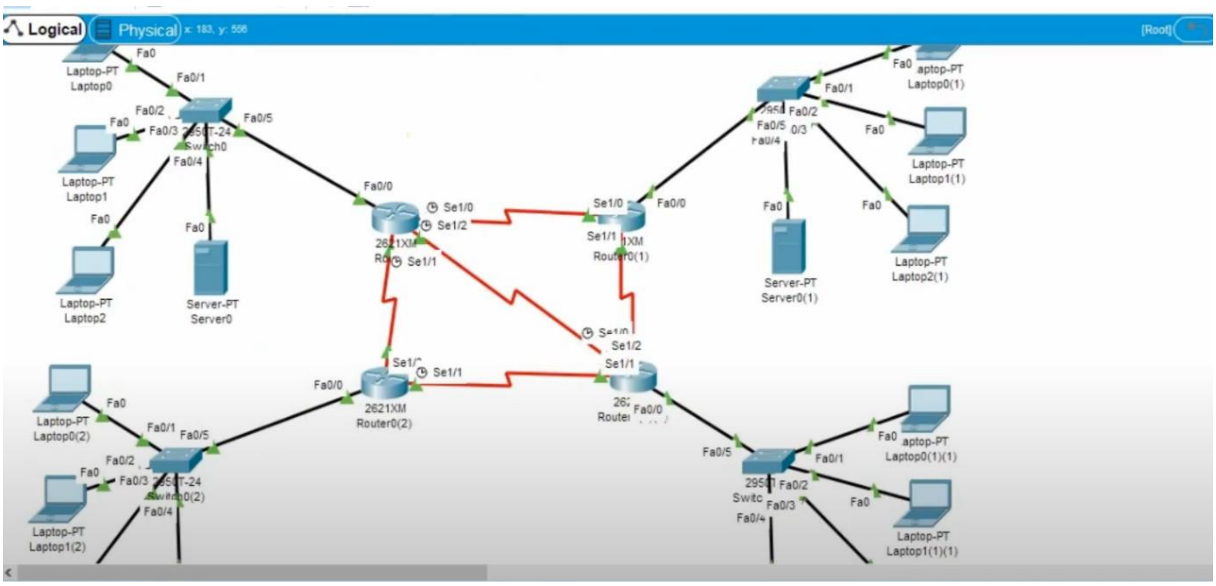
- [7] Reference (File Transfer Protocol)



Our visible design is an example of an **FTP server**. This example is very similar to reference two. Users and their permissions are determined in the FTP server, which is used differently.

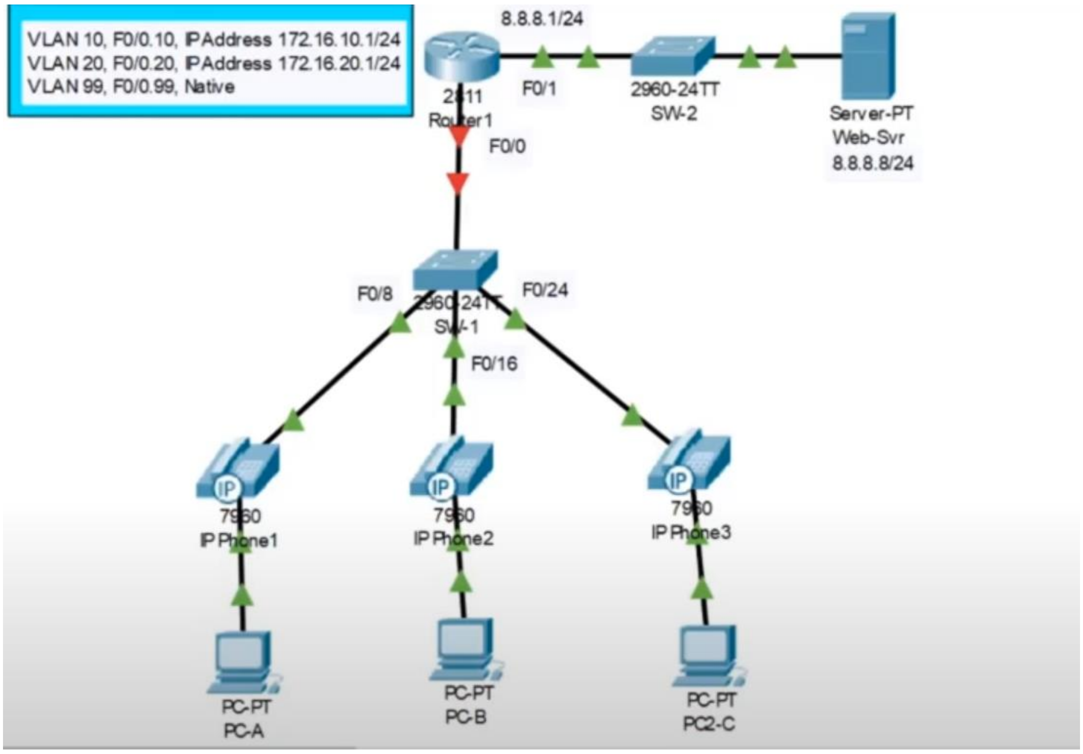
- [5] – [6] Reference ( OSPF Topology )



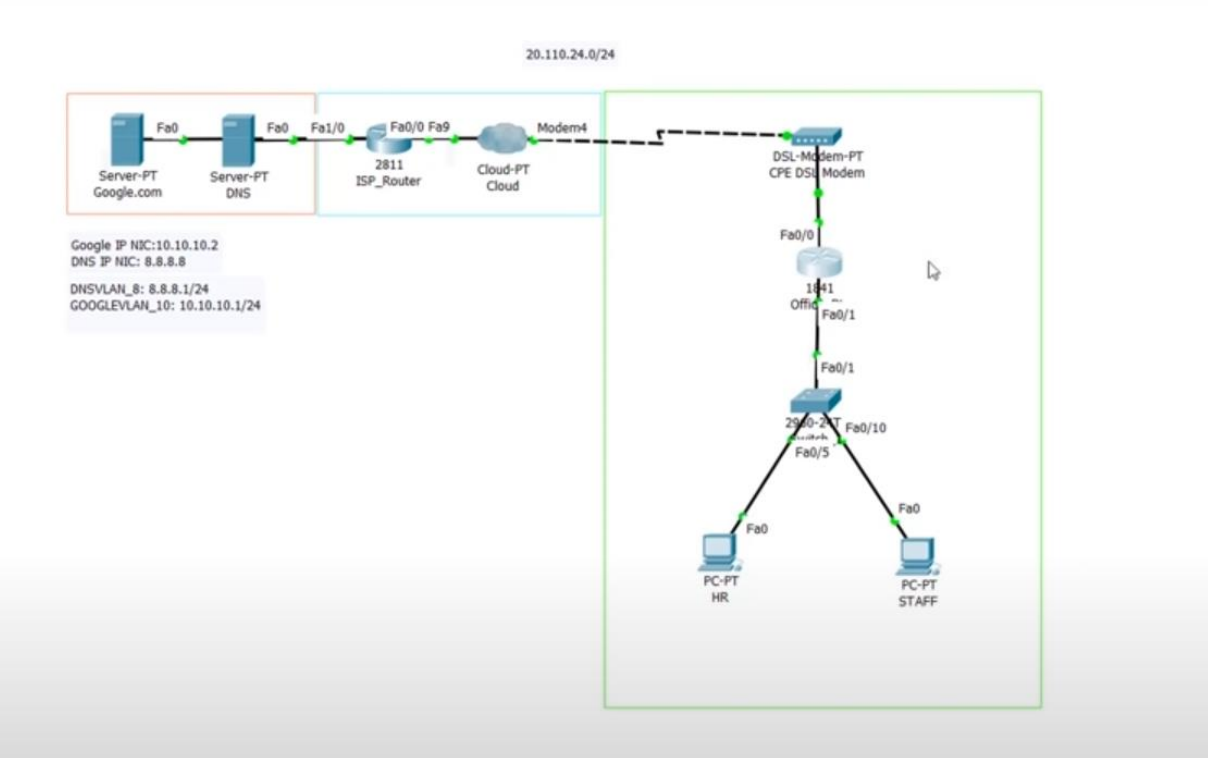
The above design was one of the most ideal examples to be used in a network structure model. It is the creation of different networks through routers using ospf topolgy. Accordingly, it offers us a different perspective for our own design.

- [8] VOIP




- The network seen is established with a structure very similar to the networks mentioned above. A router has created two different networks. A local network has been created for the server part through a switch. On the other hand, it creates a local network for computers and phones used for voip conferencing. In order to use voip in this network, a vlan structure has been set up on the switch. Each vlan undertakes a different task. By providing access to each fast ethernet cable on the switch, only these five computers were able to communicate among themselves. Of course, here it is necessary to assign numbers and make adjustments for each phone.

- [9] Reference ( ISP )




If we briefly examine the modeling of the isp structure that forms the basis of this project in its simplest form and the design that helped us in our project;

-There is an ISP router to which our servers are connected. This router allows incoming requests to reach the servers. This isp router has a ip before it passes to the servers, and when we reach this ip, the ip decides whether to allow us to pass to the servers or not.

-Other structures will be able to access the servers via a modem. The place that connects with these modems is the clouds.

- An IP is assigned to the router to which our computers are connected via modems, through which it can connect with an ISP.

- With the help of a switch, it is possible to set the access permissions and restrictions of the computers.

# 2. Method and Simulation

## 2.1 Simulation and Modeling Concepts

A discrete-event simulation (DES) models the operation of a system as a (discrete) sequence of events in time. Each event occurs at a particular instant in time and marks a change of state in the system.[1] Between consecutive events, no change in the system is assumed to occur; thus the simulation time can directly jump to the occurrence time of the next event, which is called next-event time progression.
Components
In addition to the logic of what happens when system events occur, discrete event simulations include the following:

Priority queue,
Animation event handler, and
Time re-normalization handler (as simulation runs, time variables lose precision. After a while all time variables should be re-normalized by subtracting the last processed event time).

State
A system state is a set of variables that captures the salient properties of the system to be studied. The state trajectory over time S(t) can be mathematically represented by a step function whose value can change whenever an event occurs.

Clock
The simulation must keep track of the current simulation time, in whatever measurement units are suitable for the system being modeled. In discrete-event simulations, as opposed to continuous simulations, time 'hops' because events are instantaneous – the clock skips to the next event start time as the simulation proceeds.

Our system is Discrete-event simulation( DES for short) because there are processes such as waiting for packets in a ping operation, or when multiple packets are traveling to a common point, or when multiple packets are passing over a line, and are directed by the first come router.For example, if we start the simulation and keep a packet waiting in one place for a long time, the packet may time out and be interrupted, or a packet may go with a high latency value from the first time, and then the time of the packet may be reduced by hop. According to the density of a line, the duration of the packets or the sending priorities can be arranged by the router and may take different times.

In the system we use, we can see whether the packets have arrived or where they were interrupted. And each of these steps can differ in discrete time values and in different time intervals. In addition, we can see the packets passing through the layers or the arrival of the packet to the users, and we can understand the changes in time, the density of the packets and the hop operations of the packets, we can test the model without installing it, and we can predict how it will follow and what the estimated time intervals will be. At the same time, we can notice in advance how packets hop in our design in case of a disconnection or blockages in the hop operations of packets in a busy packet sending process.

Benefits:

We can predict possible errors and test the accuracy of the connection between the systems. This saves both time and money. The accuracy of the transmissions and design of the packets can be seen. It allows us to predict the deficiencies and traffic congestion in our system, and which devices will be affected in case of ruptures that may occur. It greatly reduces the cost. It allows us to test test scenarios without installing systems. It allows us to test and close possible security vulnerabilities. It allows us to make it better, efficient and cost-free.

Challenges:

Systems that always work in simulation cannot be expected to respond and operate in the same way in real life. In real life, unexpected problems may arise due to things such as cable density, magnetic field, infrastructure, and the system that we see working in the simulation may not work. At the same time, the traffic densities or delay values in the system may not give the expected values when we adapt them to the real world, and delays and traffic congestion may occur due to noise. In terms of cost, the devices in the system we have installed may not be found, their accessibility may be low, or problems in the necessary infrastructure may be detected. There is no accuracy guaranteed by the simulation. In the real world, failure of the system due to external factors, infrastructure, some physical reasons can cause a great loss of labor, an additional burden in terms of time and cost.

## 2.2 Simulation Environment/Tool

Simulation is the modeling of a project on the computer in accordance with the reality before it is done. It contains all the details of the project, allowing to see all possible situations before starting. It enables to foresee how the system will behave, which events will be interconnected, which event will occur after which operation. It usually allows for experimentation in costly and large projects without using real products. It allows the mistakes made during the design or the mistakes that may occur spontaneously to be seen in the virtual environment without the project. This situation causes the high cost and labor force to be caused by the pre-detected errors during the construction phase. There are many advantages such as seeing the reactions of the system in changing conditions, detecting the deficiencies in advance, making the cost calculation easier. If it is necessary to make the calculation in advance, if an error during the construction process will affect the system too much, simulation tools are preferred. . A good simulation tool should be easily understandable by users, be complete, and be updatable. The simulation modeling processes are as follows:

Description of the System

Formulation of the Model

Data Compilation

Formulating the Computer Program

Checking the Validity of the Model

Strategic and Tactical Planning

Trial and Sensitivity Analysis

Implementation and Documentation

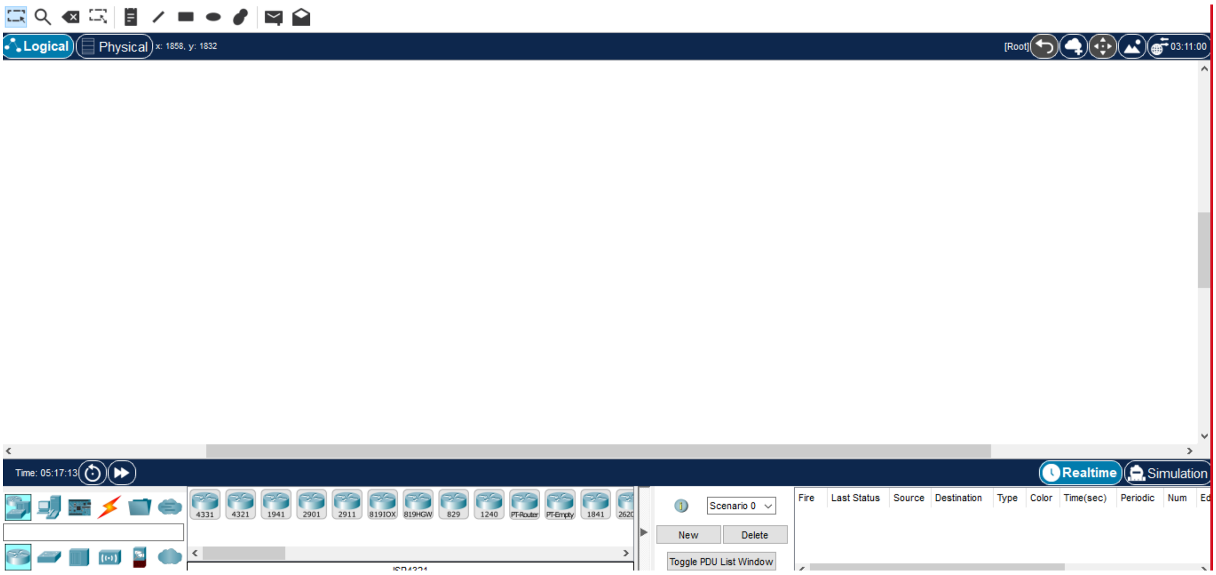
In this project we used cisco packet tracer to model a network. Cisco packet tracer enables creating network models without the need for real materials. It contains virtually router, switch, modem, computer, telephone etc. It also allows you to make changes in the settings of these tools.

Advantages:

- -It reduces the cost as it enables designing without the need for real tools.
    - Ensures that potential errors are found and corrected before the product actually goes into production.
- -We can see how a packet behaves in layers within the network structure. This reduces the number of errors on the real line.
- Being a portable application provides a great advantage.
- -Simulation mode allows us to experience real life.
- It is possible to create and design different logical network topologies by modeling in cisco packet tracer.
- Thanks to the -cisco packet tracer, it is possible to demonstrate and integrate our models with buildings and cabling cabinets in the city.

Disadvantages:

- -No debugging available.
- If the spanning tree procedure (stp) is used too often, it will get into some loops and throw an error.
- -In the simulation mode, our first attempts usually fail. However, this is a misleading result for us. Afterwards, it is seen that the design made is correct.
- -Although it has an Undo feature, its functionality is very limited. Only one step can be taken back.
- -When the system stays in the simulation mode for a long time, it gives an error for an inexplicable reason and closes without saving the last changes.
- Although the system has the above advantages, different results may occur in its real-life application. As a result, cisco packet tracer is an application, it continues to evolve. But what it can do is limited only by the elements inside and their settings.When the network modeling is designed on cisco packet tracer, it shows all the paths that the packet follows until it reaches its destination by pressing the button in the picture below (simulation mode).



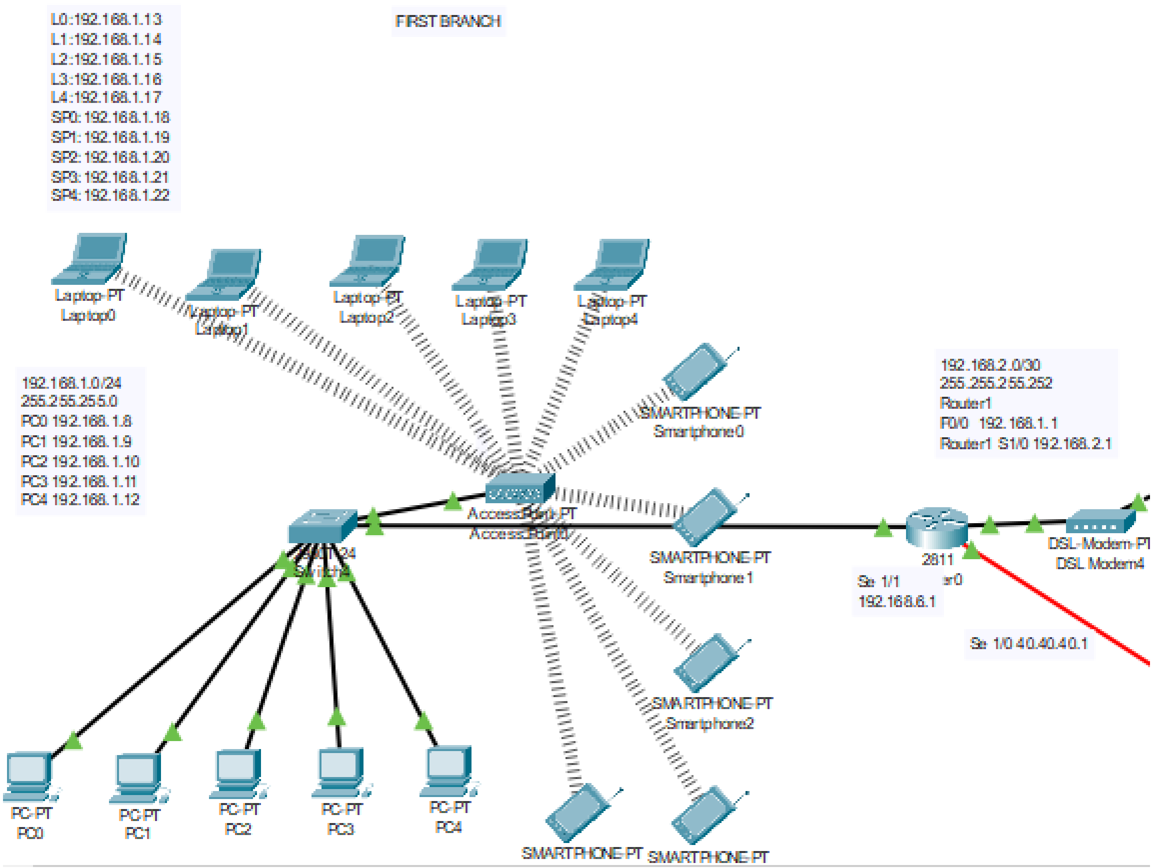

Among the tools in Cisco Packet tracer, the components we use for the project are as follows:

- Computer
- Telephone
- laptop
- Tablet
- Modem
- VoIP device
- cloud
- access point
- switch
- router
- server

## 2.3 Network Design Requirements

There are two main branches in our design. Each branch contains three separate facilities. These two main branches communicate via isp. Below, each facility will be explained within itself.

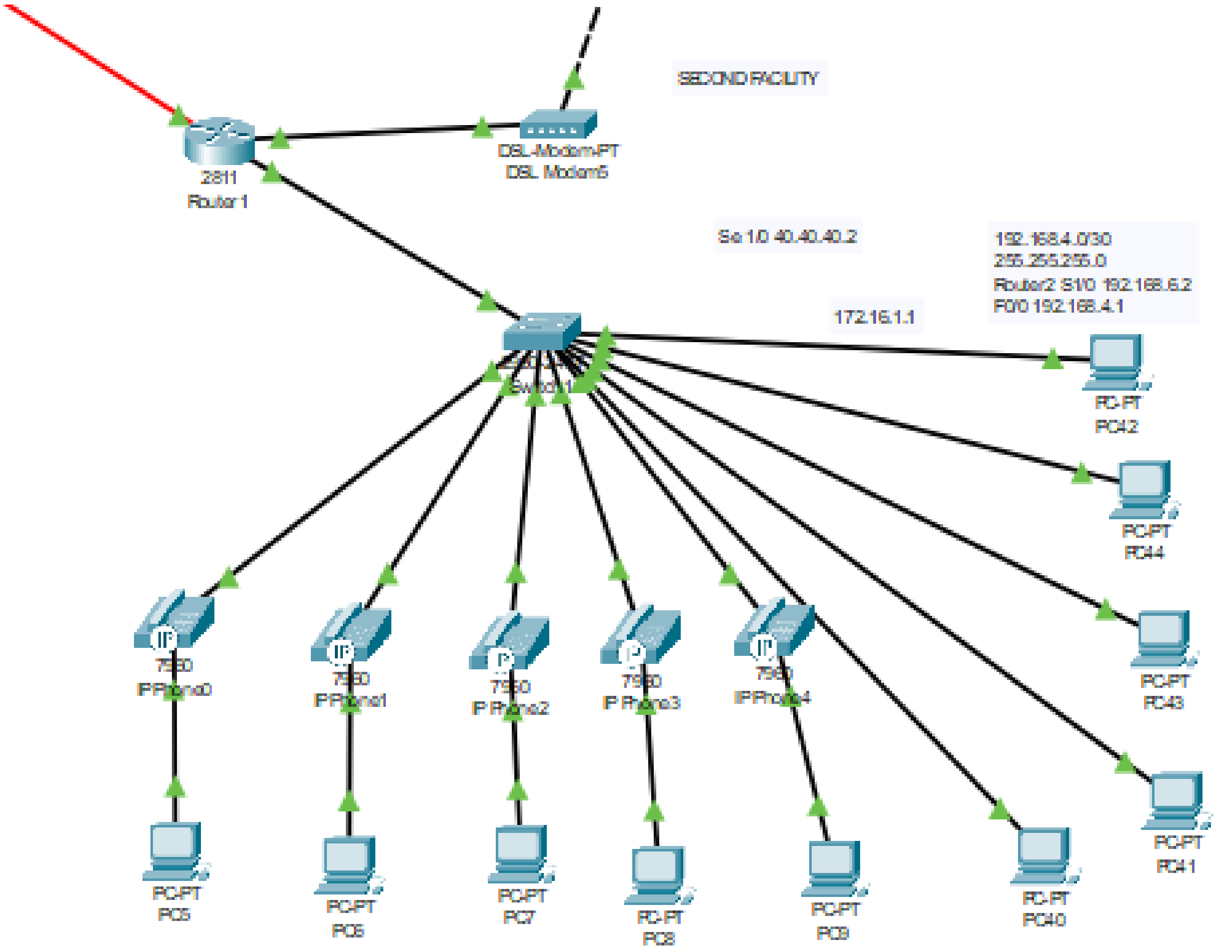
2.3.1- First Facility of First Branch




There are 5 workstation users, 5 laptop , 5 smartphone users, 1switch , 1 router , 1 access point in the first facility of the first branch. These users can browse the internet, send emails and transfer files. The router on the far right above connects the network in this facility to other networks. The router connects to the DSL modem and reaches the servers via isp, so it can browse the internet, send e-mails and transfer files. The switch connected to the router creates a local network for the first facility. While workstations that can be connected to the switch with a cable can make a direct connection, devices such as laptops and smartphones use access points to provide wireless connection. Different access points are also available in other facilities. In order to prevent some unwanted connections, a username and a password are assigned to the access point. We make these routings with the help of some configurations (ip route) we wrote in the router. It defines an ip address so that it can be connected to the

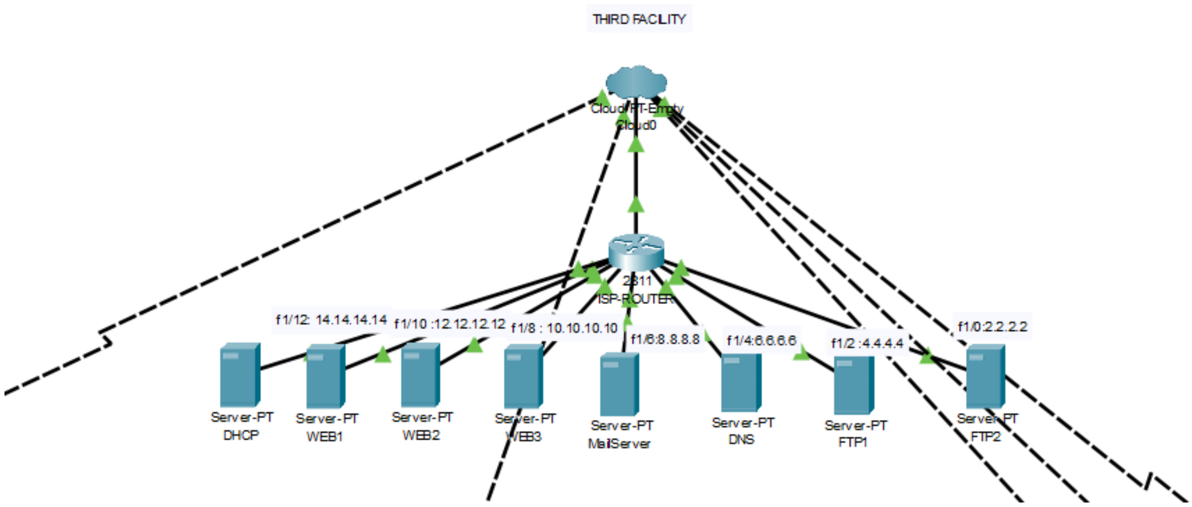
DSL modem facility with the ip router. With this defined IP address, a connection is established with the servers.

2.3.2 Second Facility of First Branch



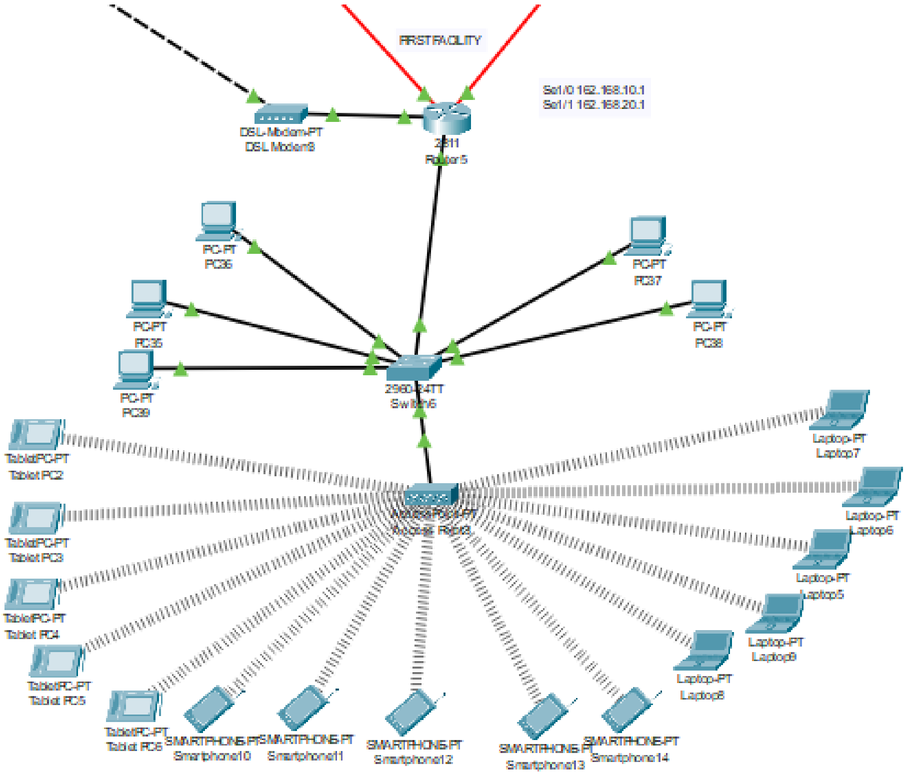

There are 10 workstations, 5 VoIP phones, 1 router and 1 DSL modem in the second facility of the first branch. In the second branch, the expected 5 workstations can make VoIP conferences within themselves, browse the internet and transfer files. For this, we provided the connection of 5 workstations and 5 VoIP devices. and we connected the remaining 5 workstations directly to the switch. We made certain configurations in the switch for VoIP devices. Some of them we use to activate telephony-service, to create virtual networks and to communicate with each other by creating a local network. We connect the switch to the router to communicate with other networks. The router connects to the DSL modem and reaches the servers via isp, so that it can browse the internet and transfer files.

2.3.3 Thirth Facility of First Branch




The third facility of the first branch consists of servers. These servers are 3 web, 2 FTP, 1 DHCP, 1 mail and 1 DNS. These servers are connected to an IP address outside the facility. This isp connects the modems to the servers via the cloud. Isp implements the stp protocol on other routers connected to it. Isp has its own private ip address. All routers that want to connect to itself request an appropriate ip adder via the modem. Isp provides an access to the servers as well as providing the connection between all branches. It performs this access via vlan. In order to provide Ispn access to all these modems, the modem must be defined in the cloud.

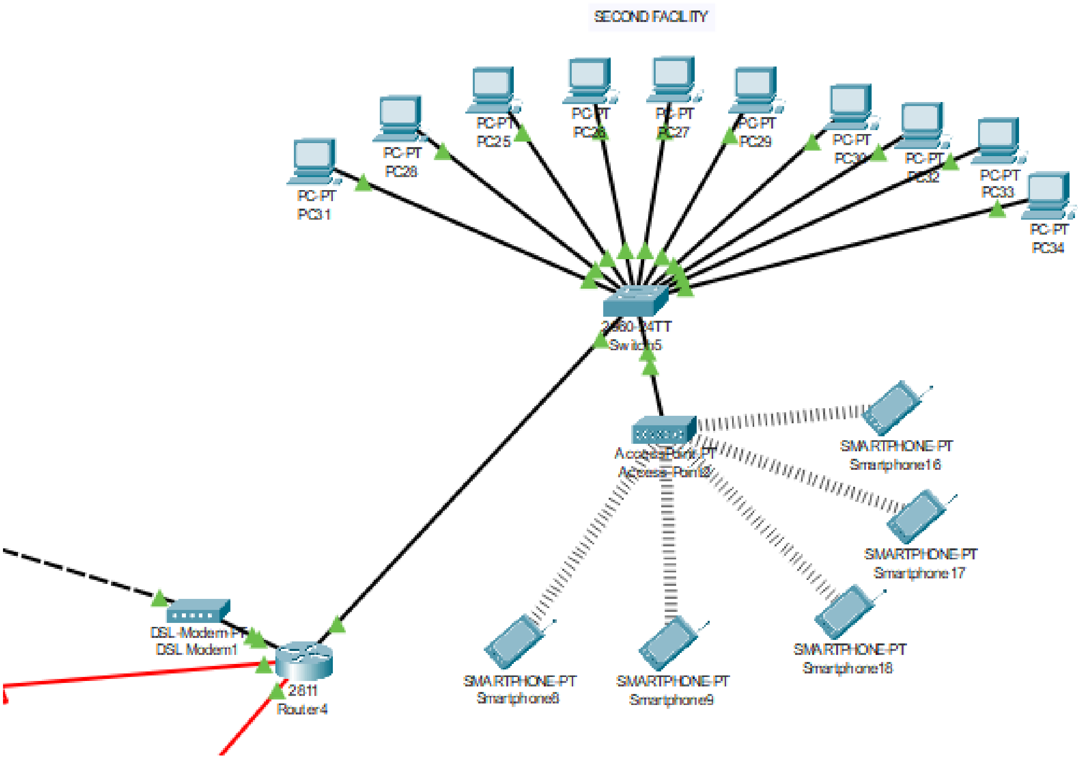
2.3.4 First Faciliy of Second Branch



In the first facility of the second branch, there are 5 workstation users, 10 wireless users (5 laptops, 5 smartphones), 5 tablets, 1 switch, 1 access point, 1 router, 1 DSL modem. Users

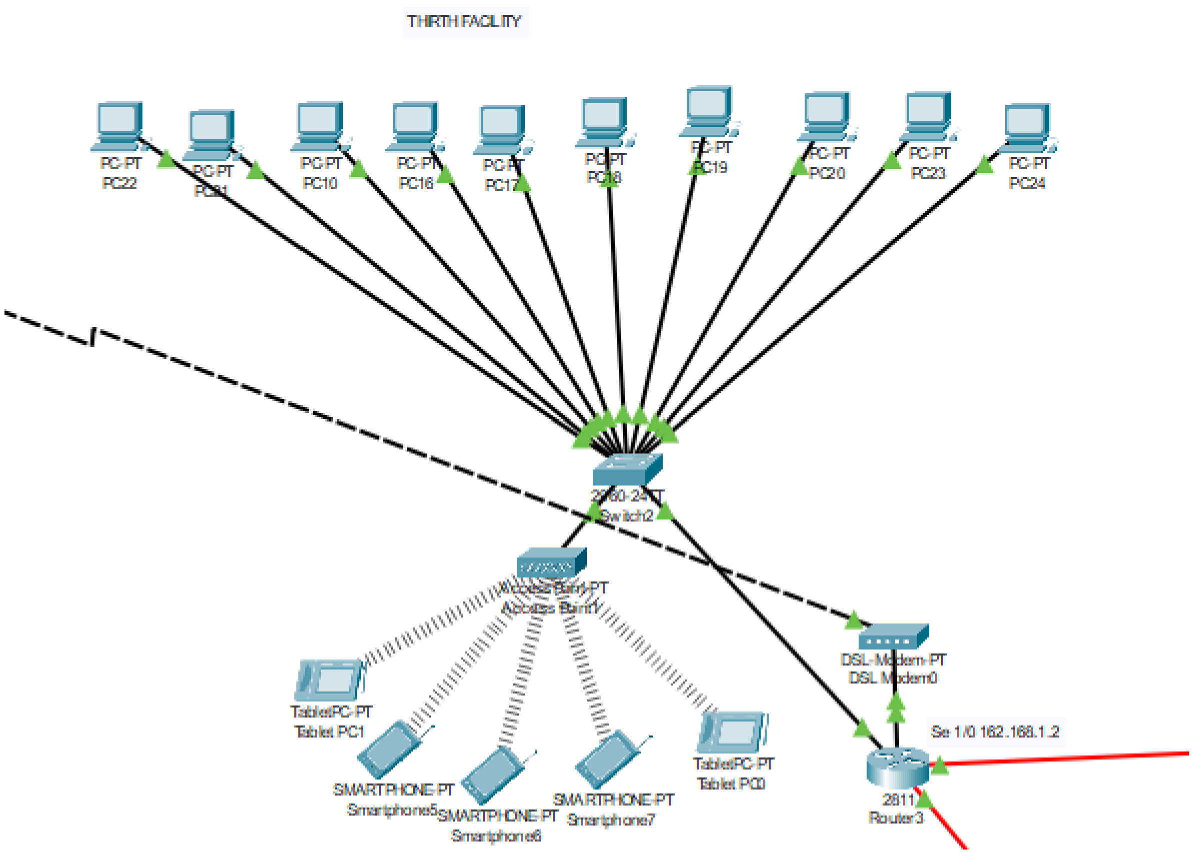
here should be able to connect to the internet using a wireless connection, browse the internet, and use email applications. Wireless devices are connected to the switch via an access point. Workstations are connected directly to the switch with a cable. The router provides the connection of these devices with different networks. In addition, it can access the servers via isp over the internet by connecting with the router modem. In this way, it is possible to gamble on the web and use e-mail applications.

2.3.5 Second Facility of Second Branch




In the second facility of the second branch, there are 10 workstation users, 5 smartphones, 1 switch, 1 access point, 1 router, 1 DSL modem. Users here should be able to browse the internet, use editing applications and transfer files. Wireless devices are connected to the switch via an access point. Workstations are connected directly to the switch with a cable. The router provides the connection of these devices with different networks. In addition, it can access the servers via isp over the internet by connecting with the router modem. In this way, you can browse the web and transfer files.

2.3.6 Thirth Facility of Second Branch




In the third facility of the second branch, there are 10 workstation users, 5 mobile devices, 1 switch, 1 access point, 1 router, 1 DSL modem. Users here should be able to browse the internet and send and receive emails. Wireless devices are connected to the switch via an access point. Workstations are connected directly to the switch with a cable. The router provides the connection of these devices with different networks. In addition, it can access the servers via isp over the internet by connecting with the router modem. In this way, you can browse the web and send and receive e-mails.

## 2.4 Requirement Analysis

The Switches we will use should have more than 20 fast Ethernet lines as ports, because the number of devices in most of our buildings is expected to be a minimum of 10 and a maximum of 30. That's why our switches need to be large and have good vlan manageability. On the other hand, we decided that our routers should have SerialPorts to communicate with each other in a closed network and that there should be at least 4 of them on average. Here, we aimed to ensure the flow of traffic even in the event of a line break by connecting the 2nd Branchte routers in a triangle with each other. We decided that the routers should also have FastEthernet ports and that there should be at least 3 of them. The 2 connections here could be for the switch and the other branch, and since a 3rd branch may be needed in some requirements, we left 1 port empty and used it in some structures.

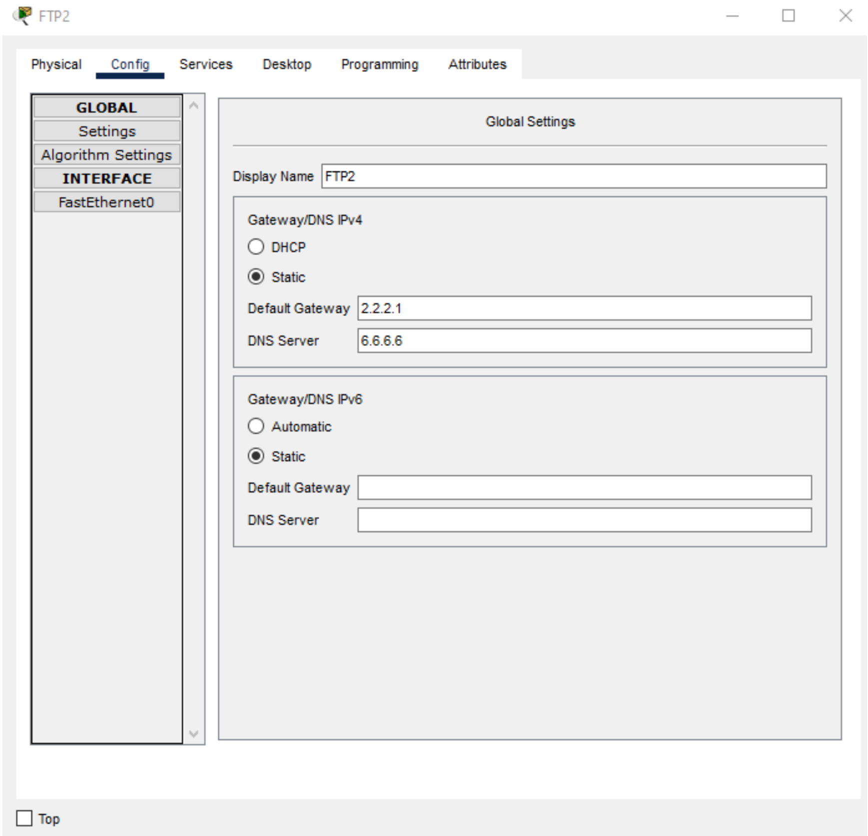
Routers need to include Serial and Fast Ethernet ports, and we chose the FastEthernet line for the line to which they will be connected to the modems, due to its speed. We chose our modems as VDS. The reason we chose VDS was because we thought that cable modems are hard to find in our country. Since we could not use gigabit Ethernet because we chose VDS, we chose FastEthernet, which we can communicate with the fastest, and its speed is 100mbs. When we looked at the number of users, we did not see any limit on our AccessPoints and we did not need to make a special choice. In switches, we preferred models with 10 to 20 Fastethernet ports so that we can establish as many connections as possible. Here, the user capacity remained as the capacities of the switches and access points themselves. Since 100mbs internet speed will be divided when more users are connected, we thought that the numbers given were sufficient, so we left only the ports that need to be connected open.

In our VoIP phones, we designed using the 7960 model and this selection must be made. We have not specifically tested whether it will work in any model case, but the 7960 model is used for VoIPs. A special reason for choosing our router 2811 is that we have problems with connection and routing in some models, so we chose the 2811 model as the router so that the whole system works in harmony. We had some problems with routing between different modems. We set up vlan structures for VoIP and ISP, and we did the necessary permission and routing with vlans. Here for VoIP, we set up structures as DATA, VOICE and NATIVE as vlans and set the ports of the switch accordingly, while we set up vlan CUSTOMERS for the ISP and made a vlan system that allows users or customers to connect to the ISP, checking whether they have access.

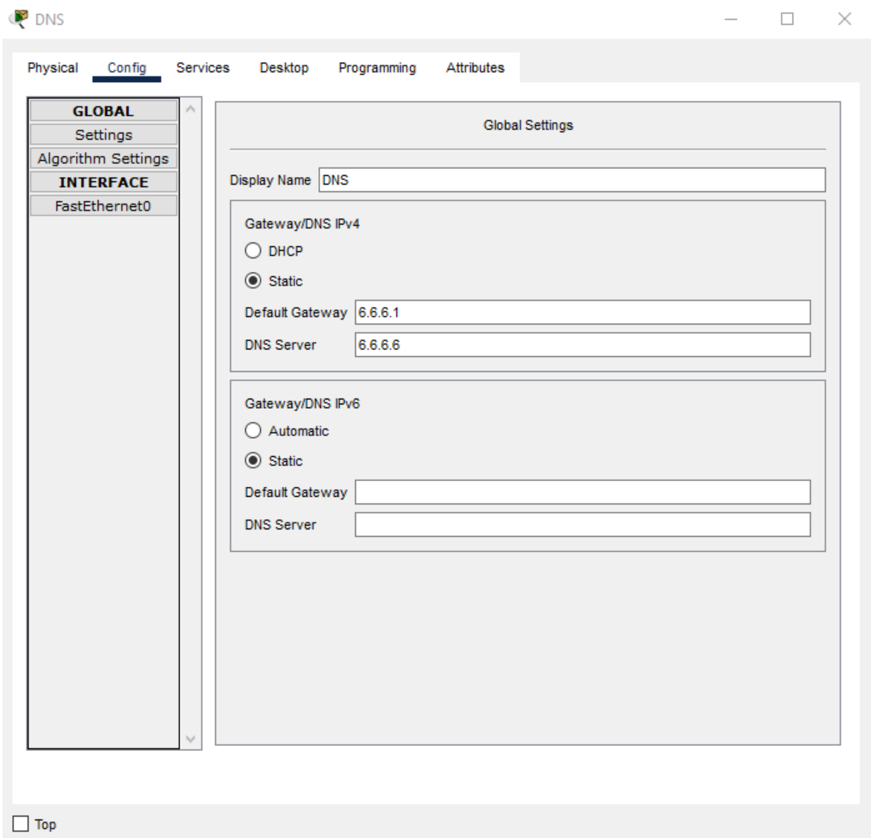
## 2.5 Definitions of the System/Model

There are two branches connected to each other via Isp. At this point, we can clearly say that the structure that enables us to communicate is the ISP router. Each branch has 3 networks within itself and each network has local networks within itself. Although these two branches communicate with the ISP router, the branches communicate within themselves through routers. If we make an assumption for this system, the system works consistently within itself. Computers reach the desired places and realize all expected scenarios. The network topologies we use in the system are extended star, mesh and star. The network topology in the most general view of our system is an extended star and each facility has stars within itself. Only in the second facility, mash topology was used between the routers. In the pictures below, you can see some of our routing and equipment configurations. There are main computers in our system. These computers can access and manage servers remotely.

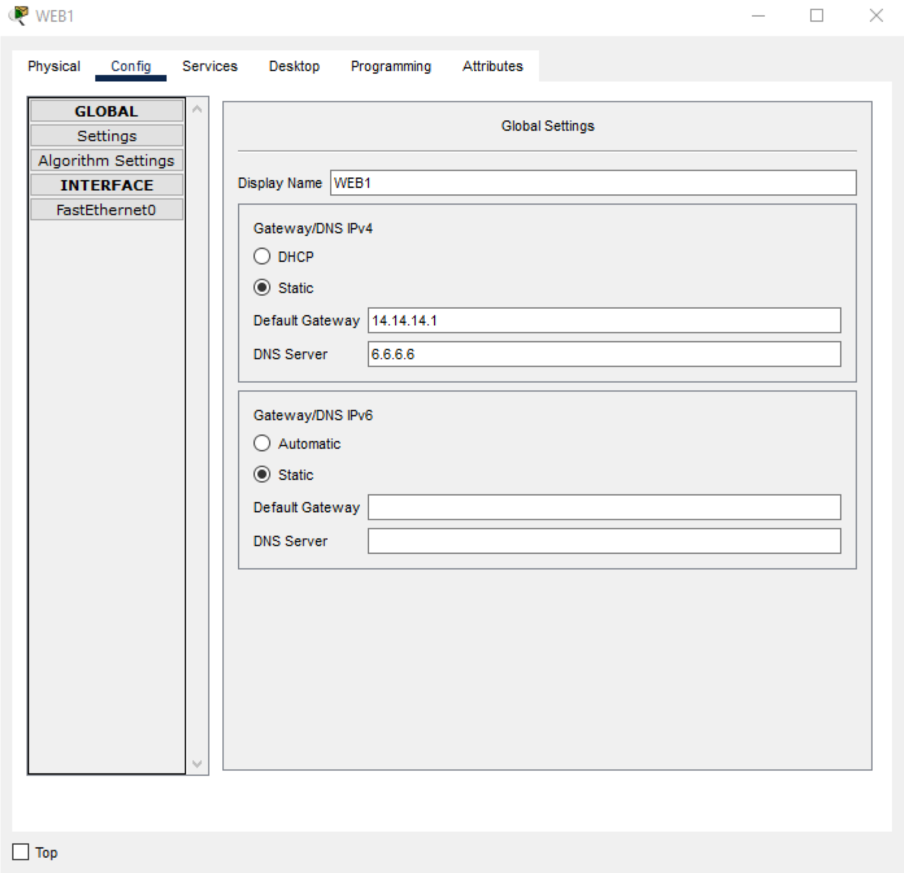
There are approximately 15-20 users in each facility. Our goal is to provide an effective connection to every user that may be included in the system.



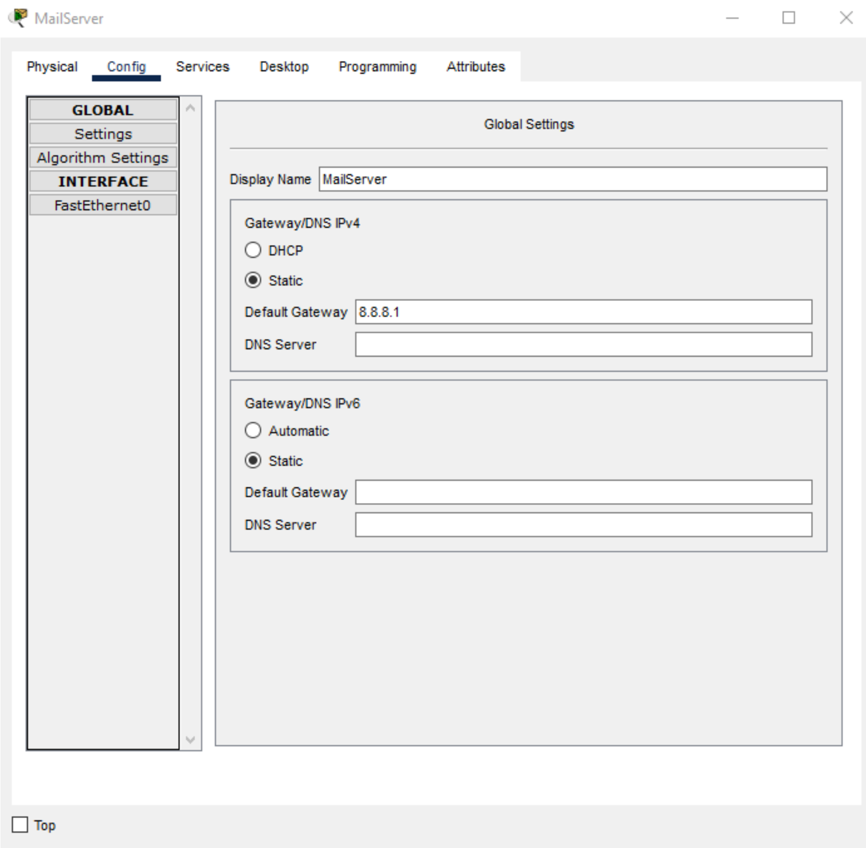

Config of FTP2 server




Config of DNS server




Config of WEB server




Config of Mail server

## 2.6 Simulation Elements

*System entities

Computer Nodes: Computers that have the ability to communicate with other computers in the network are called 'Node computers'. Having the ability to communicate here is the ability to connect to other networks through routers other than the closed network. In this way, the network we call the Internet may have been created. DNS servers can be given as the biggest example of these. But all computers can become Nodes if necessary settings and connections are made. In addition, it can be said that the developing blockchain is the node structure directly visited by every computer.

Server: Computers connected to a specialized network that are assigned for certain purposes and that accept and respond to connection requests from other computers.

Queue : Packet flows in the network are made in a certain order and if there is a heavy traffic or if there is a continuous traffic, they form a queue. This is called a queue.

Packets: Each packet of information flowing in the network is called a 'packet'. They contain various information.

Flows of Packets: The flow of packets tries to go to the destination in the packets according to the forwarding authority of the routers. These packets try to reach their destination by being routed through routers. If packet flows are not allowed, packets may be lost on the way and may not reach their destination.

*System state variables

Although there may be more than one type of this, in general, devices such as routers or servers are in standby mode in an asynchronous network and this situation is called 'idle'. If there is a heavy traffic and the device on which the package is located cannot respond to new arrivals or if it is performing a transaction, it is in 'busy' mode.

* Input variables

It can have multiple types. Inputs can be on the network in different protocols or in different formats.

* Resources

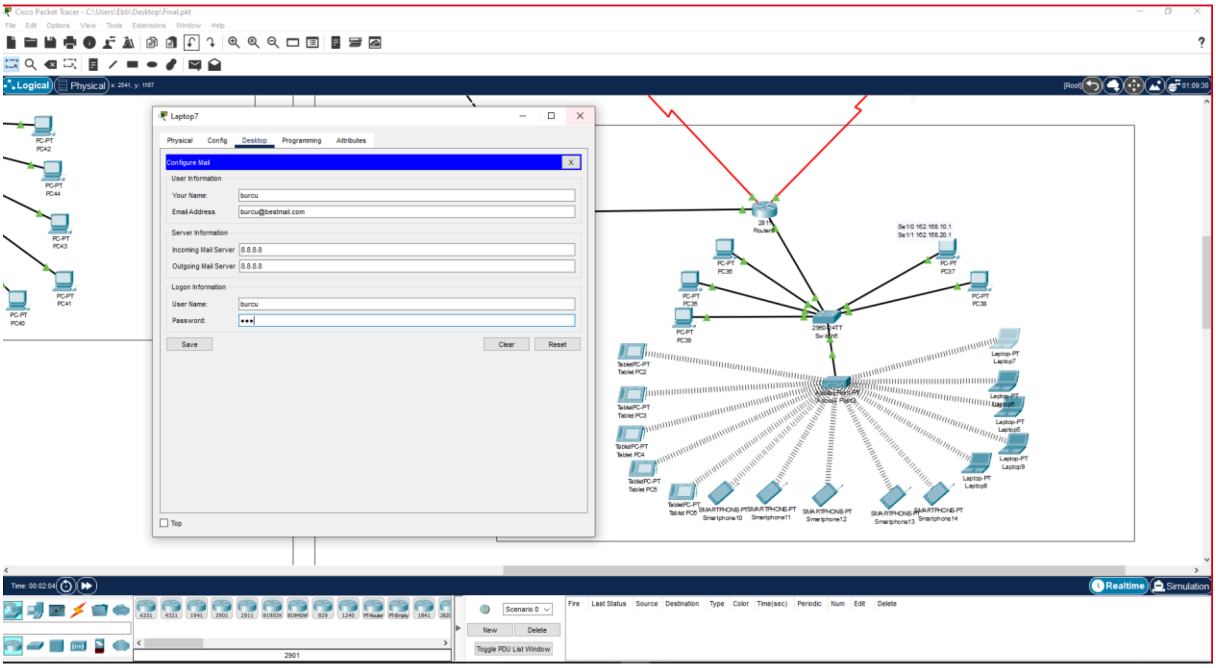
The number of bits that resources can pass over (for example: seconds) is called 'bandwith', and this is important where traffic needs to be heavy and high. This is a resource because when different computers use the same line, the number of bits to be transferred over this cable is a resource and each computer consumes as many bits of this resource as it uses. Servers are also a resource because a data stream or connection request goes there from different computers. This request also consumes the capacity of the server. Transmission time, on the other hand, has a time interval that must pass and consume in the transmission of packets.

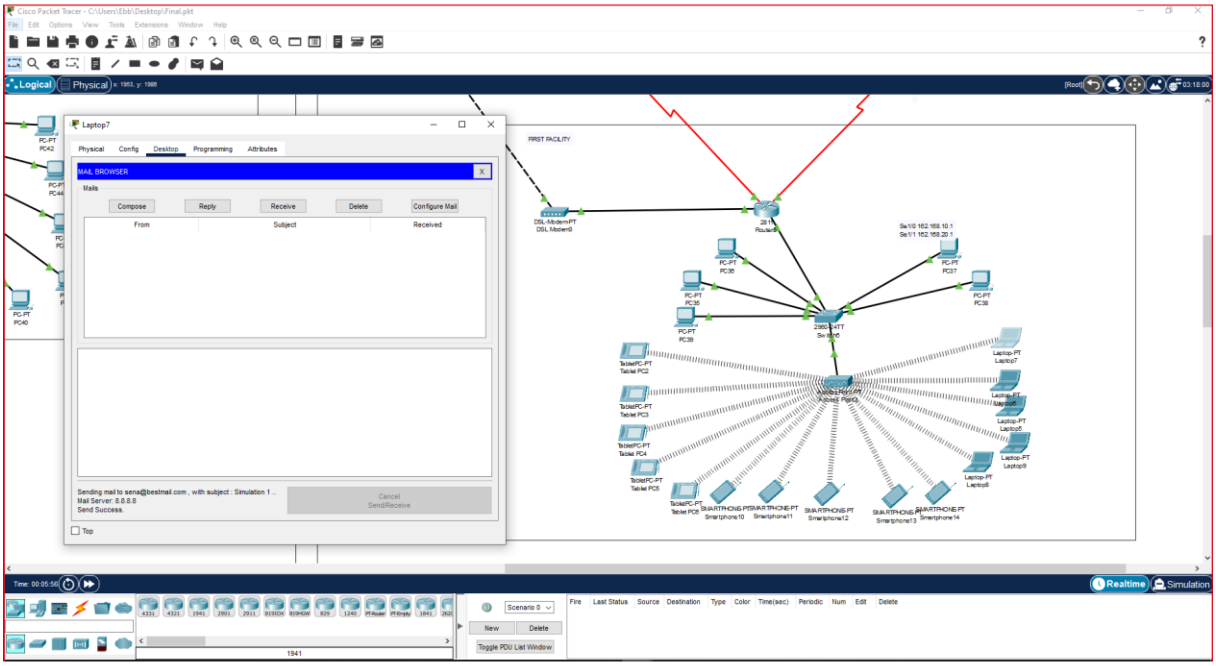
*Activities and events

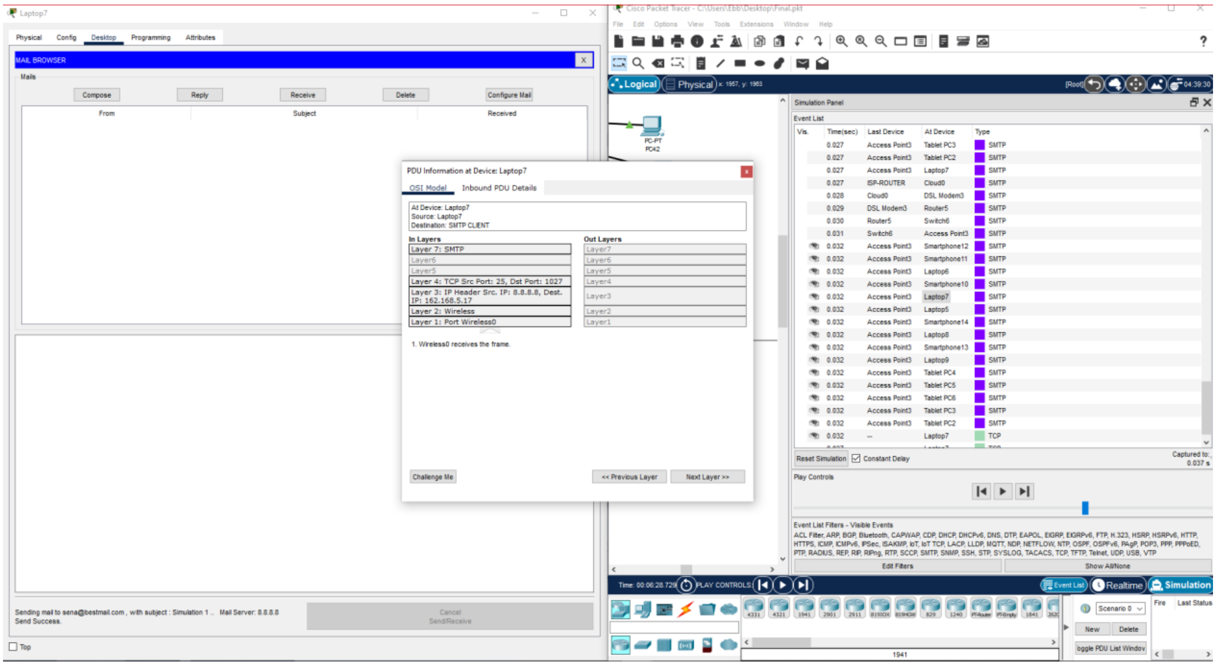
There may be situations where a packet waits in a certain place, skips, or when the traffic is heavy, the router puts it in a queue (queue). Packets can arrive or go from one place to another.

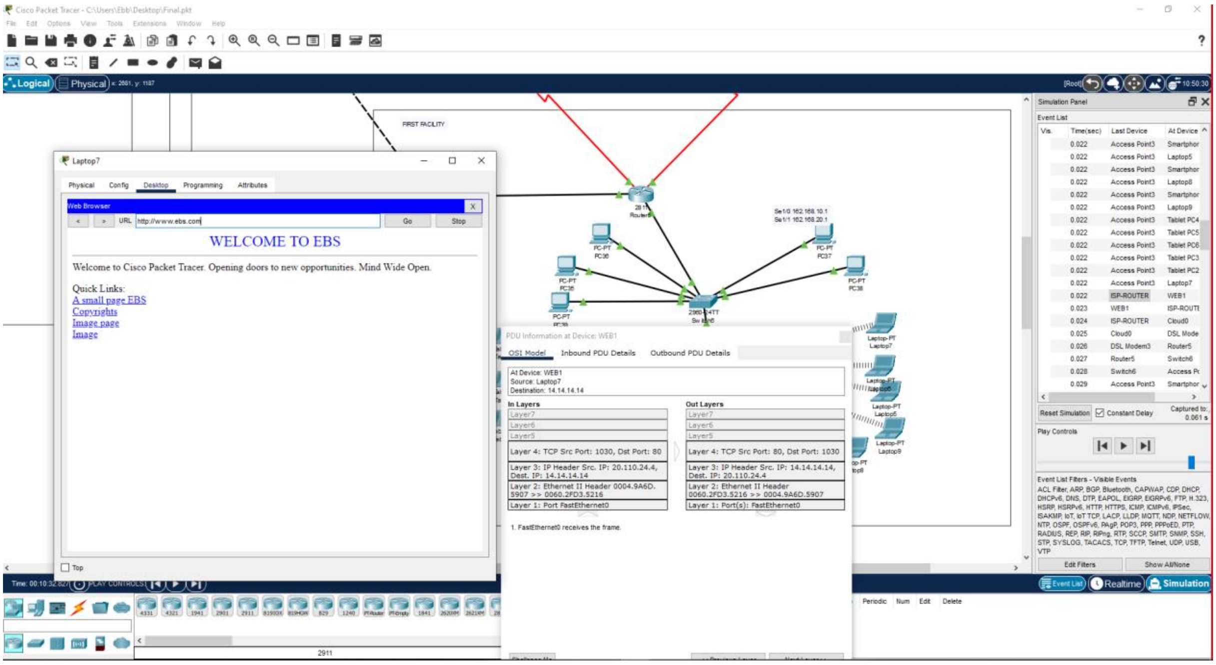
# 3. Traffic Analysis and Simulation Results

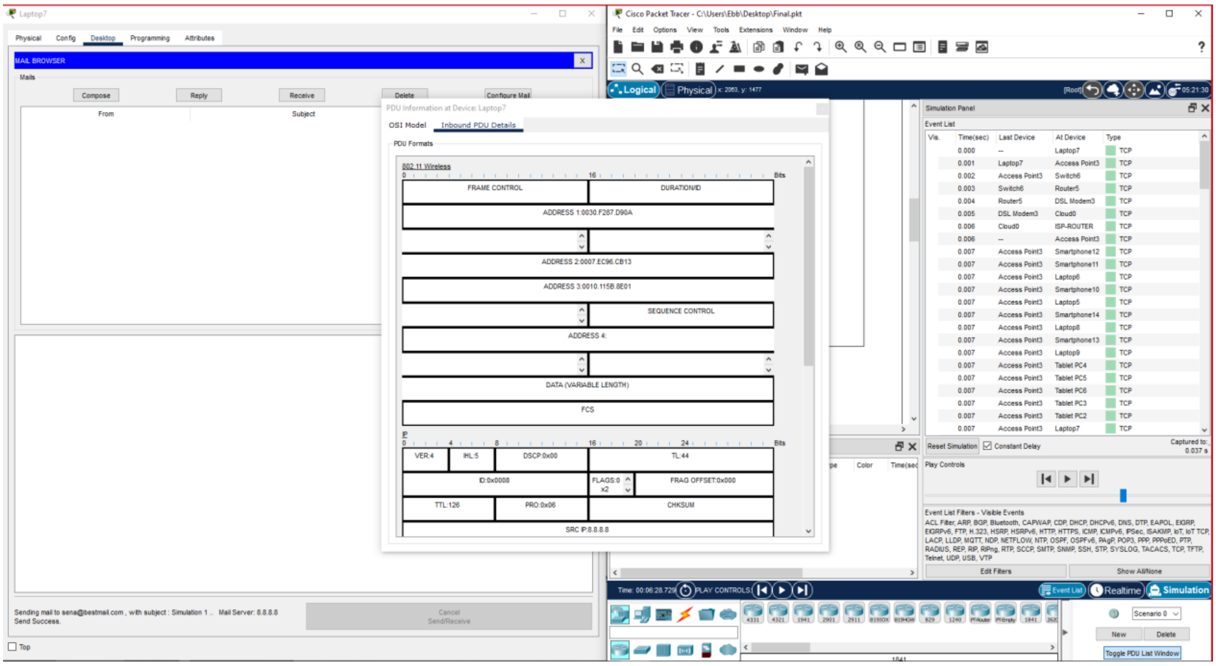
**Scenario 1:** A wireless user from first facility of second branch wants to read emails and browse Web.



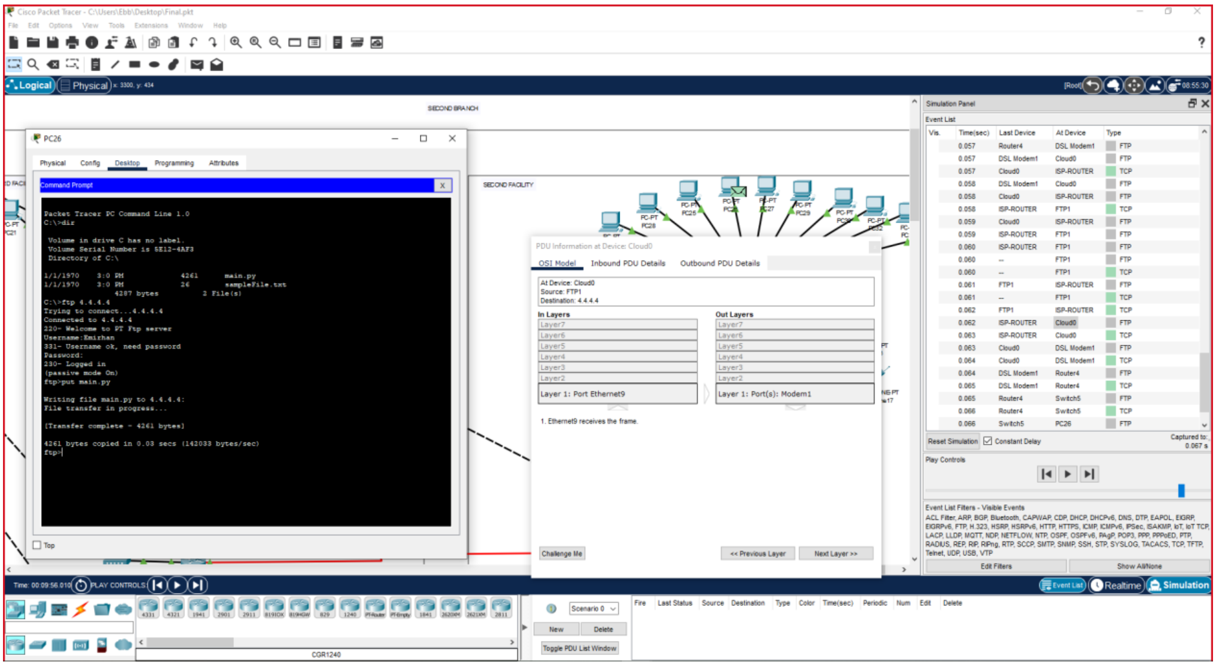


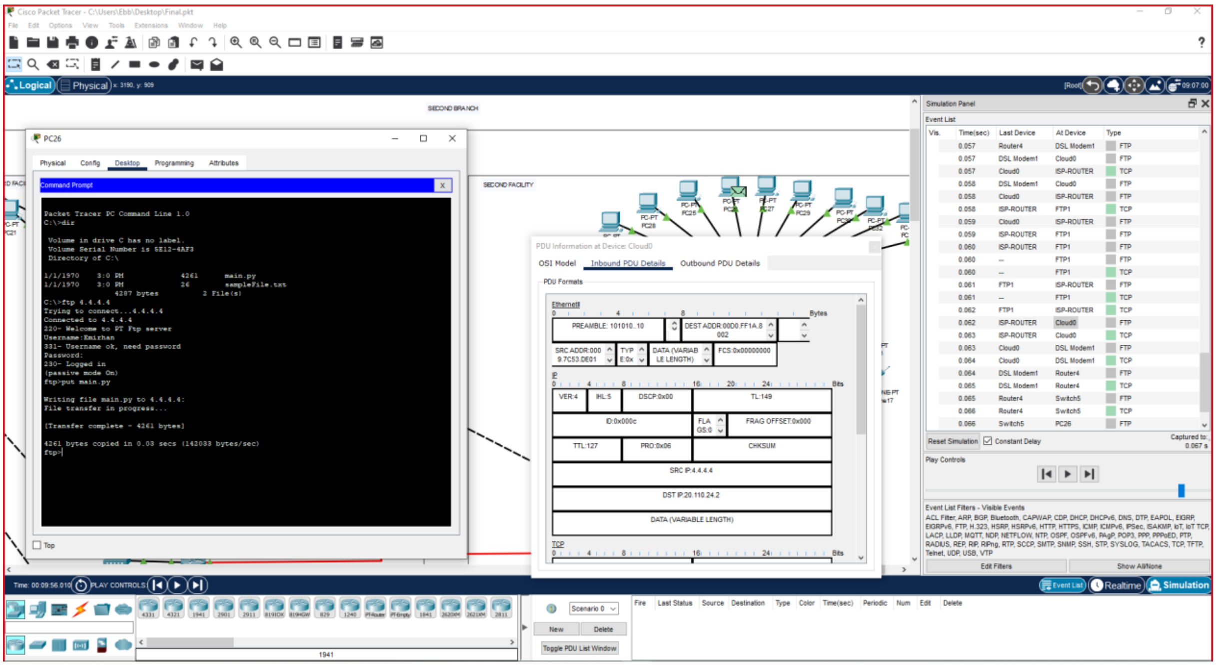

MAIL BROWSER
Compose
Reply
Receive
Delete
Configure Mail
From
Subject
Received
PDU Information at Device: Laptop7
OSI Model
Inbound PDU Details
At Device: Laptop7
Source: Laptop7
Destination: SMTP CLIENT
In Layers
Layer 7: SMTP
Layer 4: TCP Src Port: 25, Dst Port: 1027
Layer 3: IP Header Src. IP: 8.8.8.8, Dest. IP: 162.168.5.17
Layer 2: Wireless
Layer 1: Port Wireless0
Out Layers
1. Wireless0 receives the frame.
Sending mail to sena@bestmail.com , with subject : Simulation 1 ... Mail Server: 8.8.8.8
Send Success.
Simulation Panel
Event List

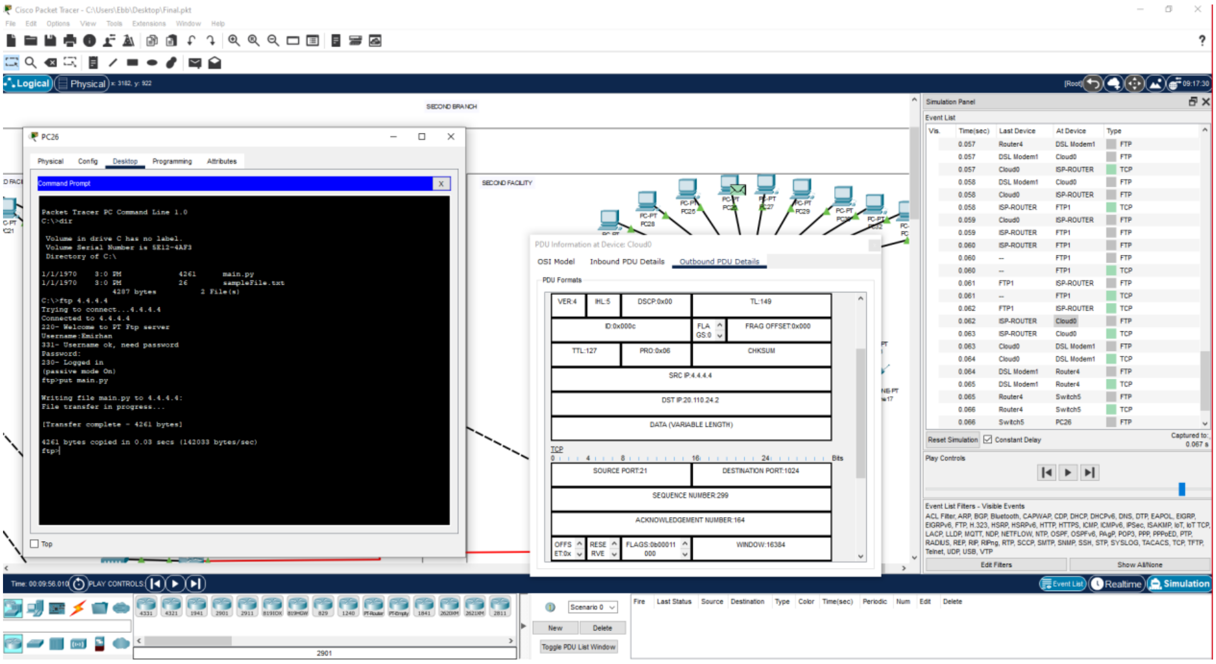

Web Browser
URL http://www.ebs.com
WELCOME TO EBS
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page EBS
Copyrights
Image page
Image
PDU Information at Device: WEB1
OSI Model
Inbound PDU Details
Outbound PDU Details
At Device: WEB1
Source: Laptop7
Destination: 14.14.14.14
In Layers
Layer 4: TCP Src Port: 1030, Dst Port: 80
Layer 3: IP Header Src. IP: 20.110.24.4, Dest. IP: 14.14.14.14
Layer 2: Ethernet II Header 0004.9A6D.5907 >> 0060.2FD3.5216
Layer 1: Port FastEthernet0
Out Layers
Layer 4: TCP Src Port: 80, Dst Port: 1030
Layer 3: IP Header Src. IP: 14.14.14.14, Dest. IP: 20.110.24.4
Layer 2: Ethernet II Header 0060.2FD3.5216 >> 0004.9A6D.5907
Layer 1: Port(s): FastEthernet0
1. FastEthernet0 receives the frame.
FIRST FACILITY



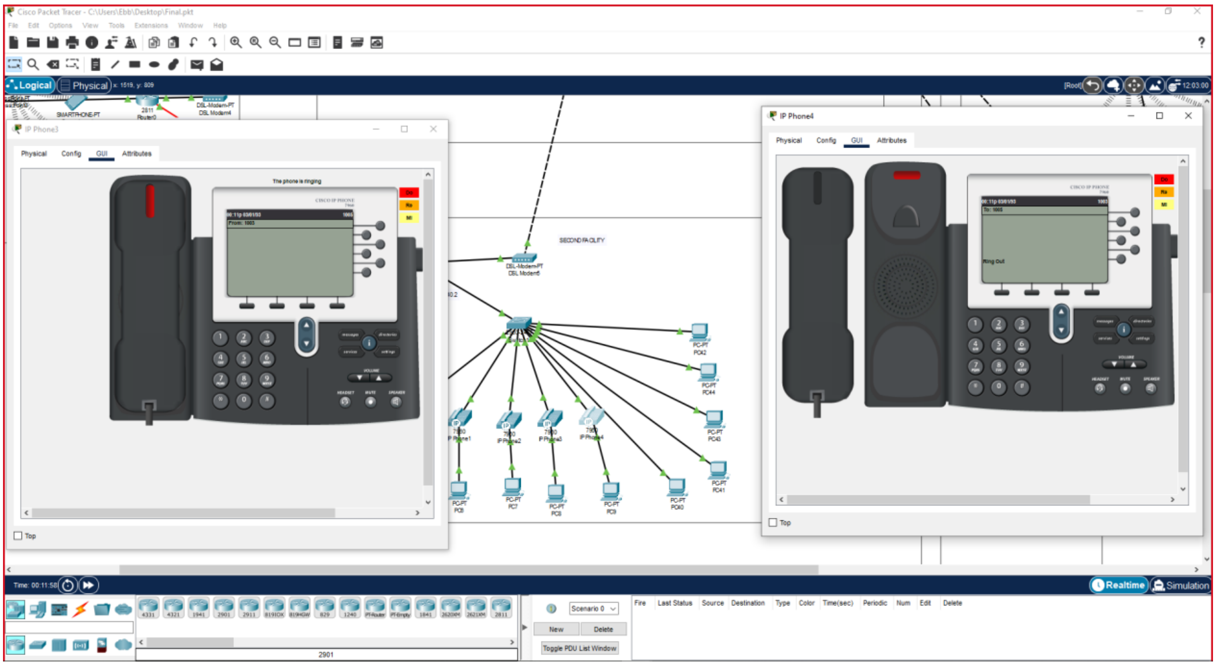
**Scenario 2:** A computer engineer from second facility of second branch developed a web application and wants to send her code files to FTP server in the third facility of first branch.

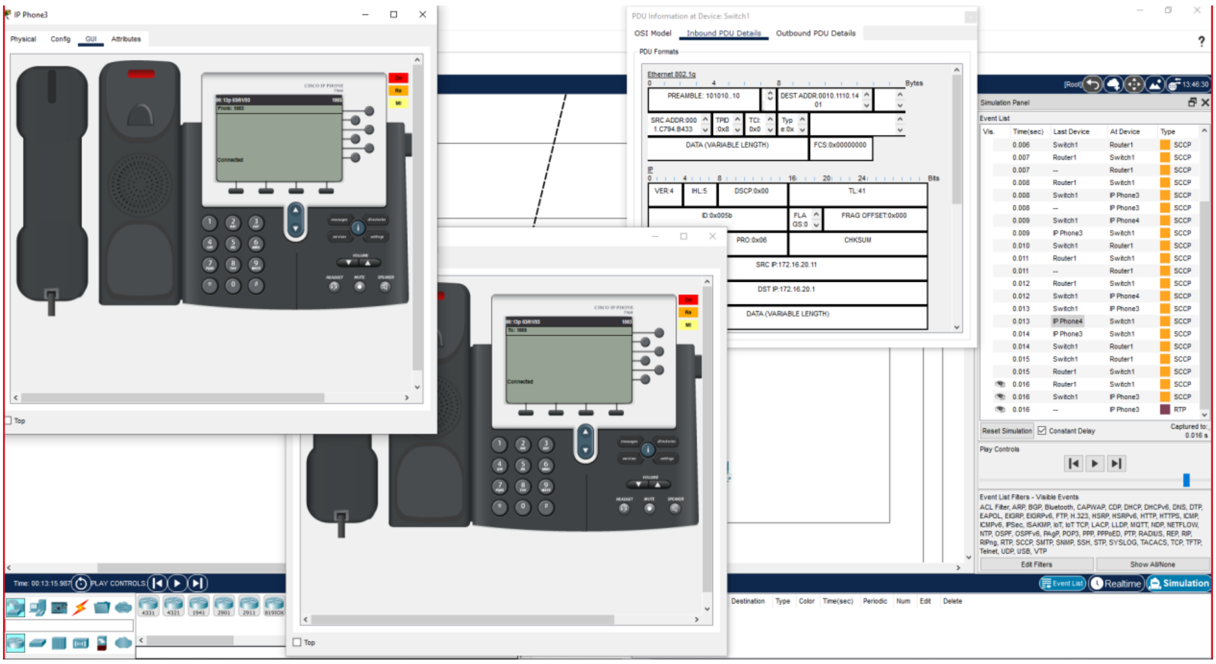


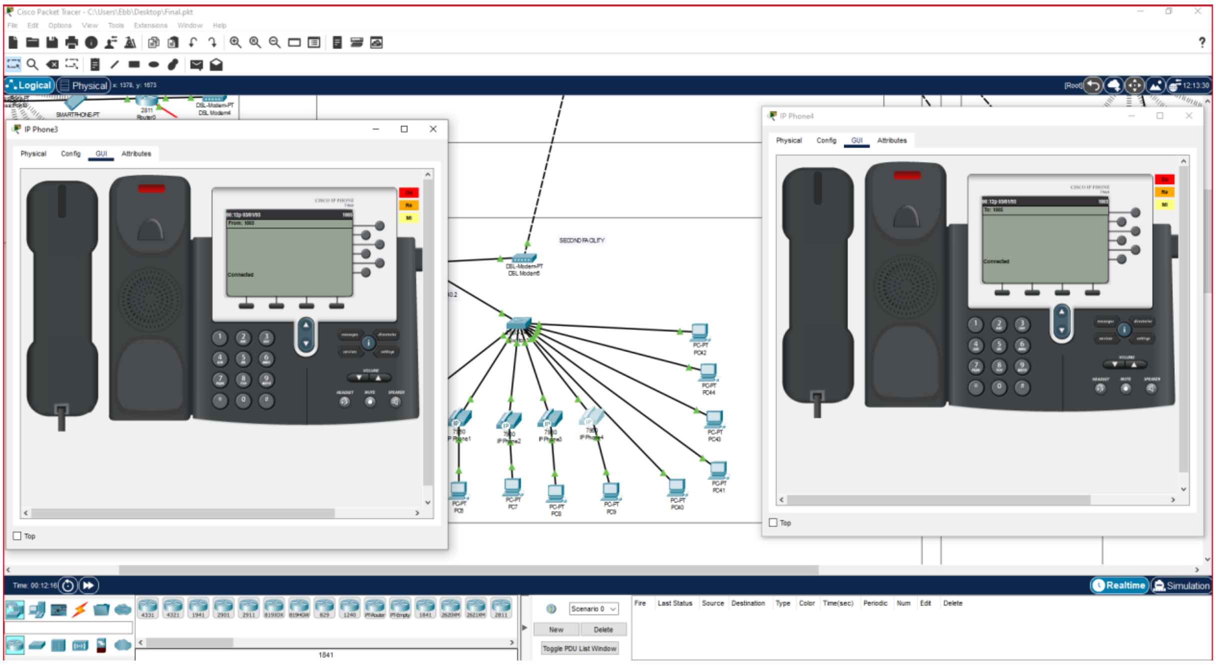




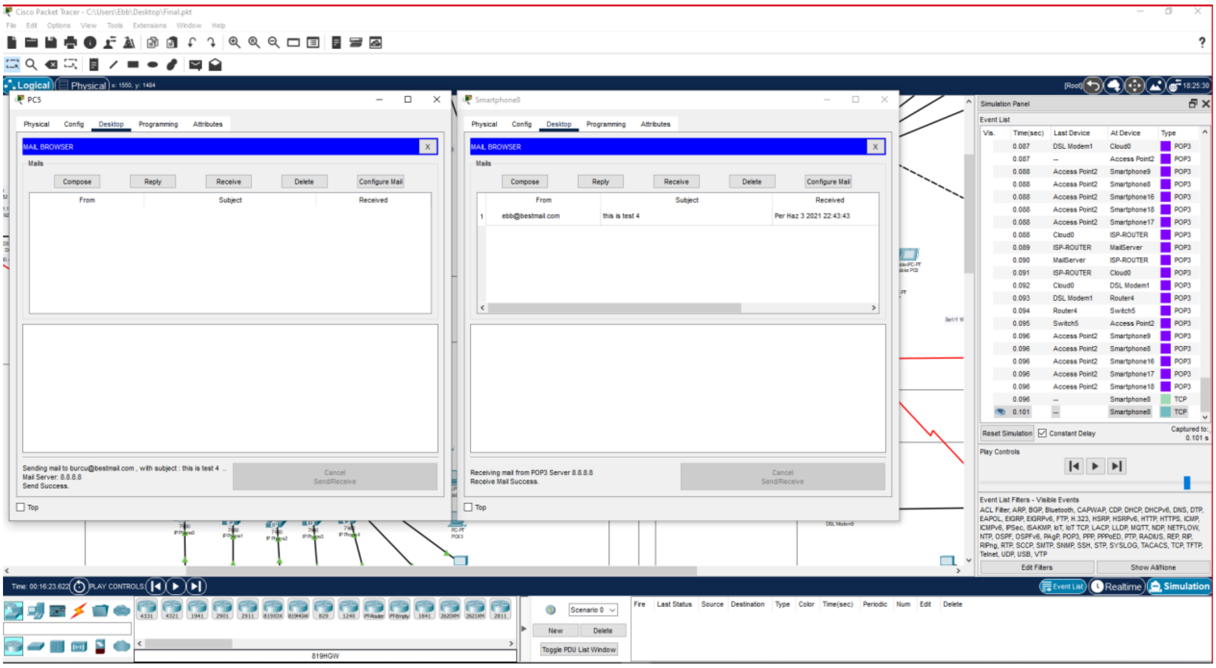
**Scenario 3:** Two users from second facility of first branch want to talk via VoIP.

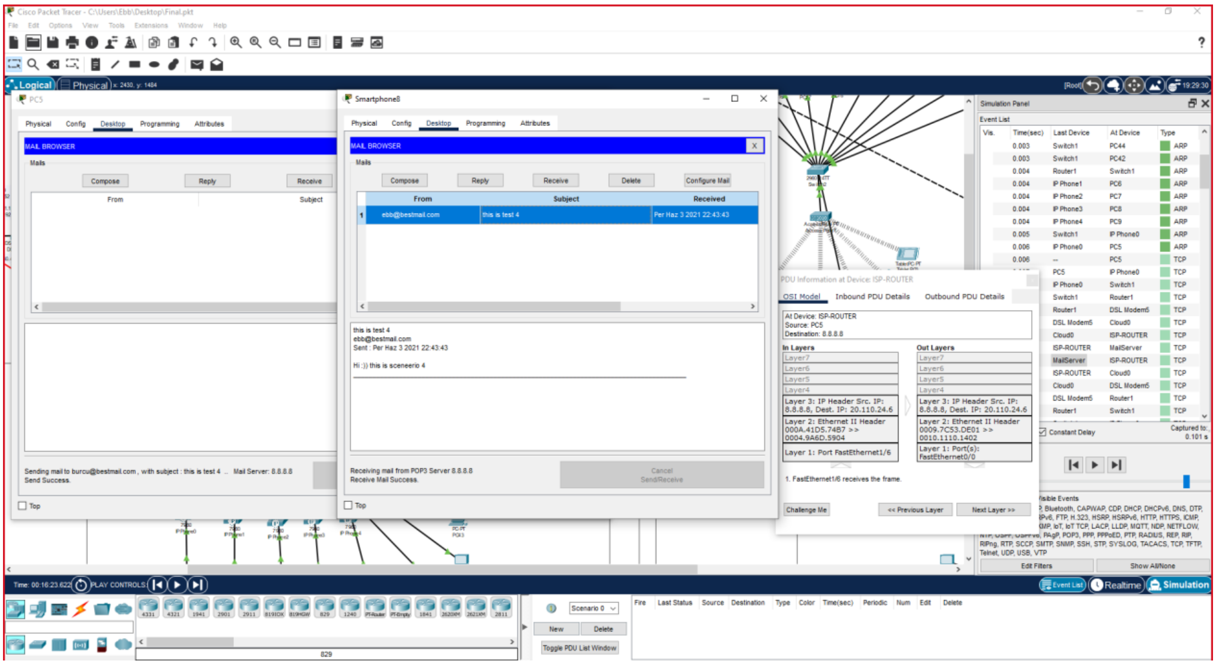




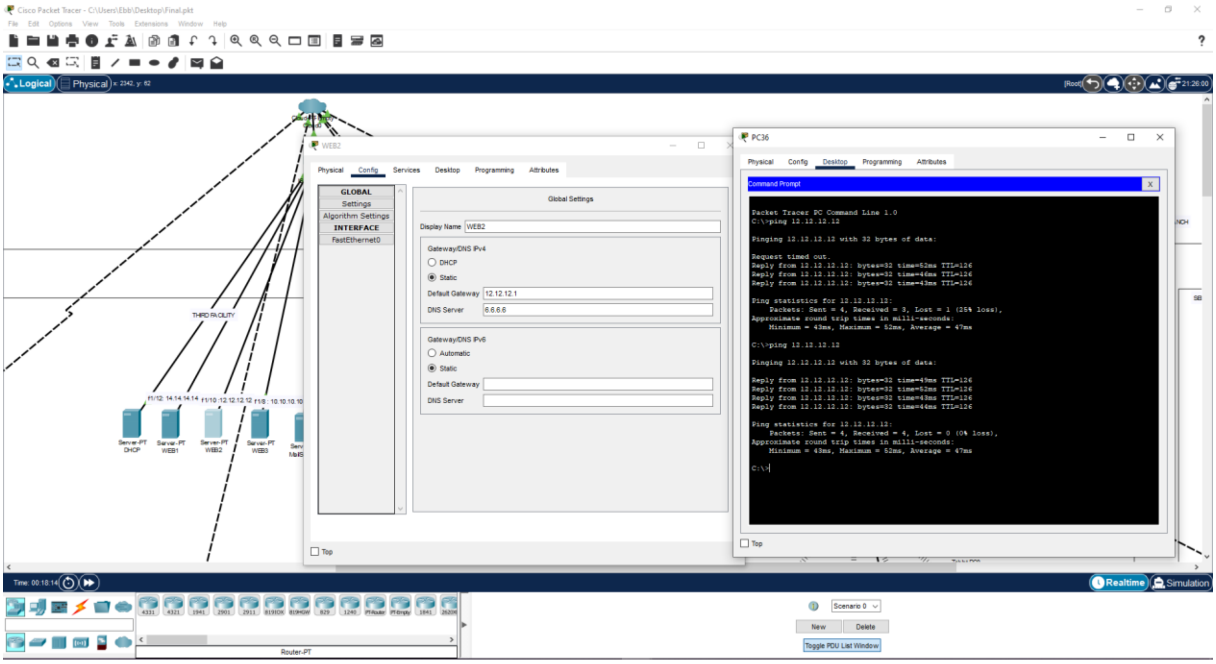


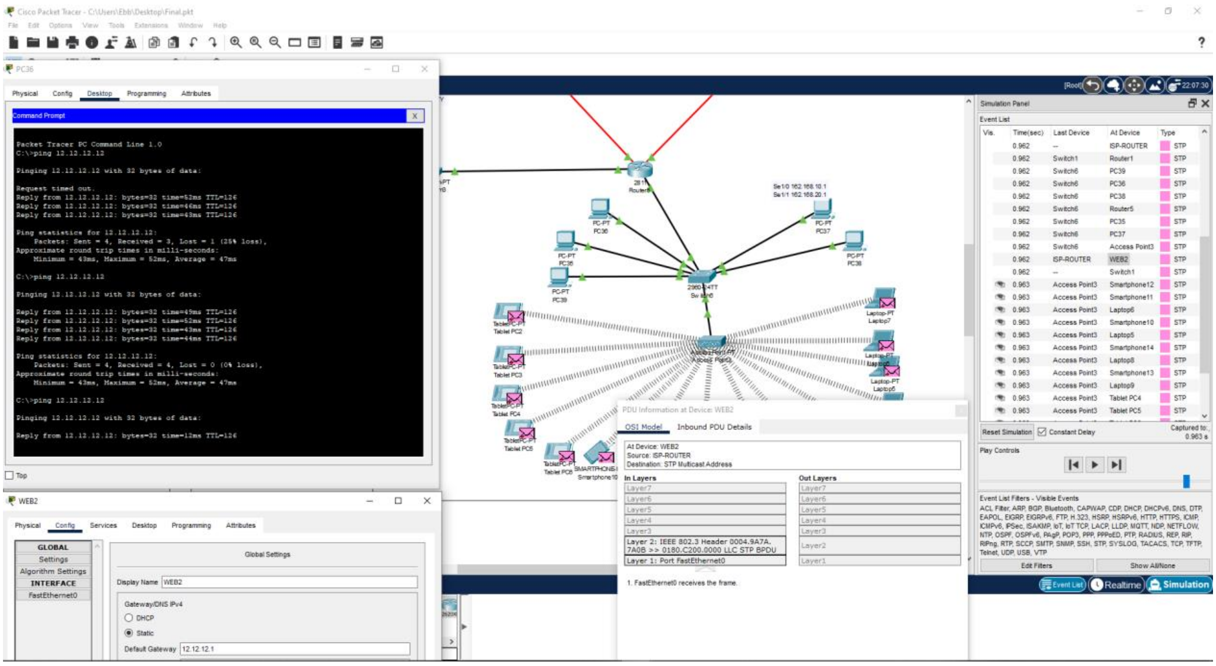
**Scenario 4:** A user in the second facility of first branch wants to send an email message to his friend in the second facility of second branch.

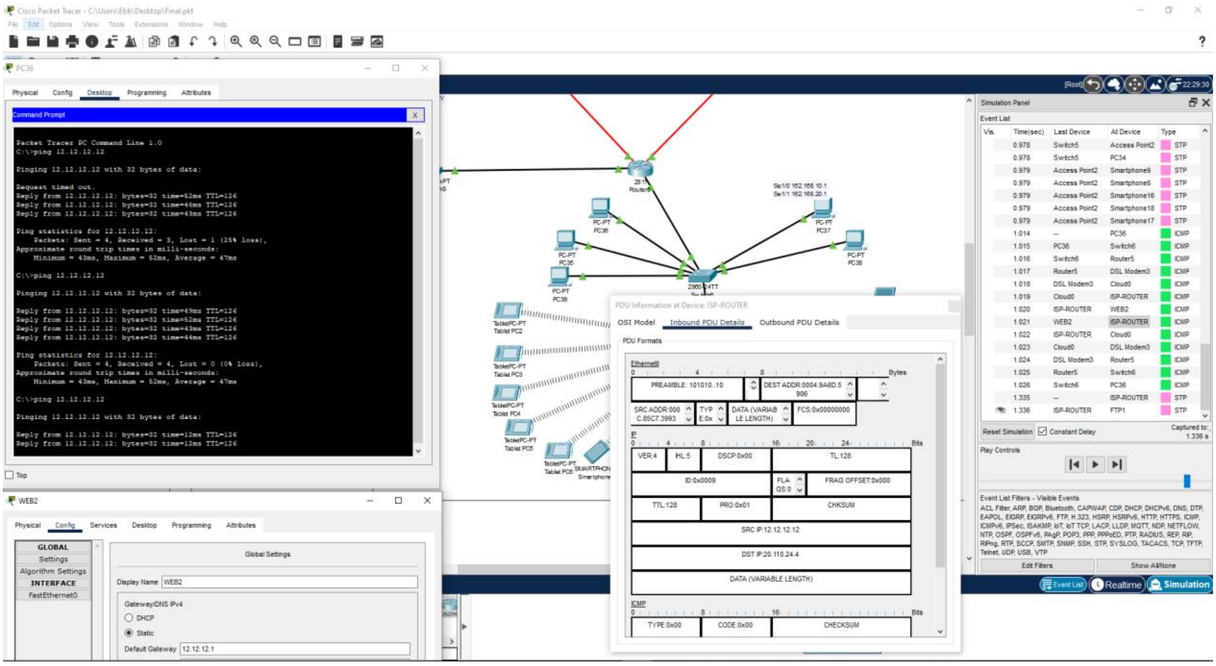




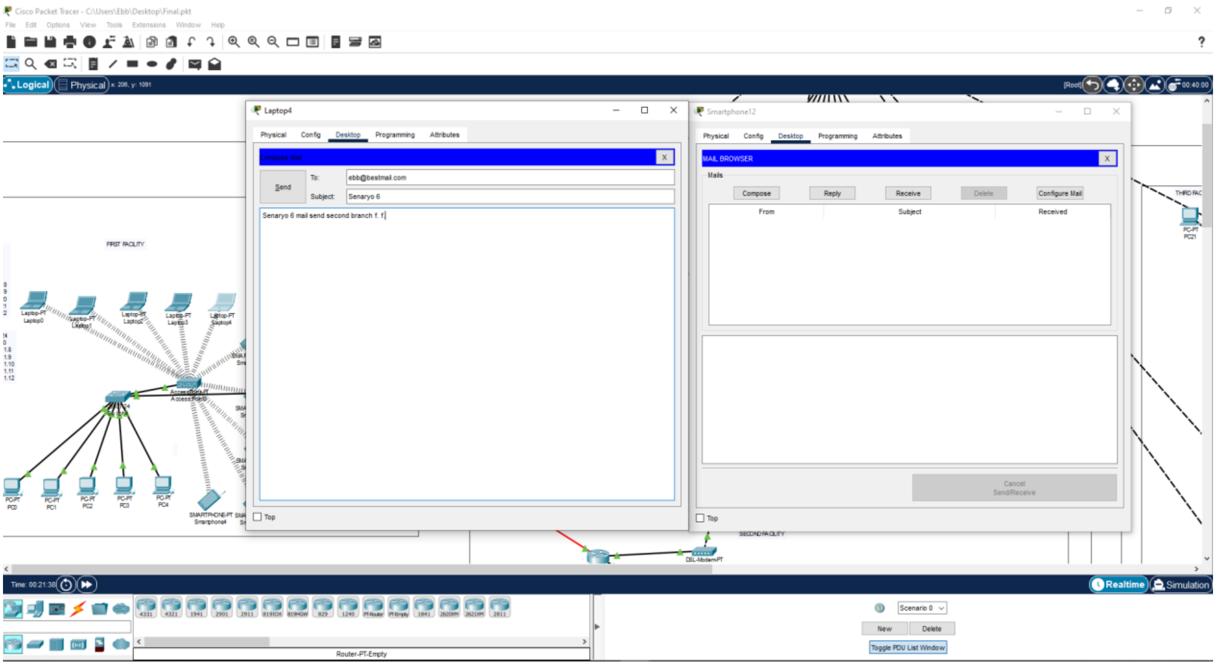
**Scenario 5:** A user from first facility of second branch pings Web server of third facility of first branch.

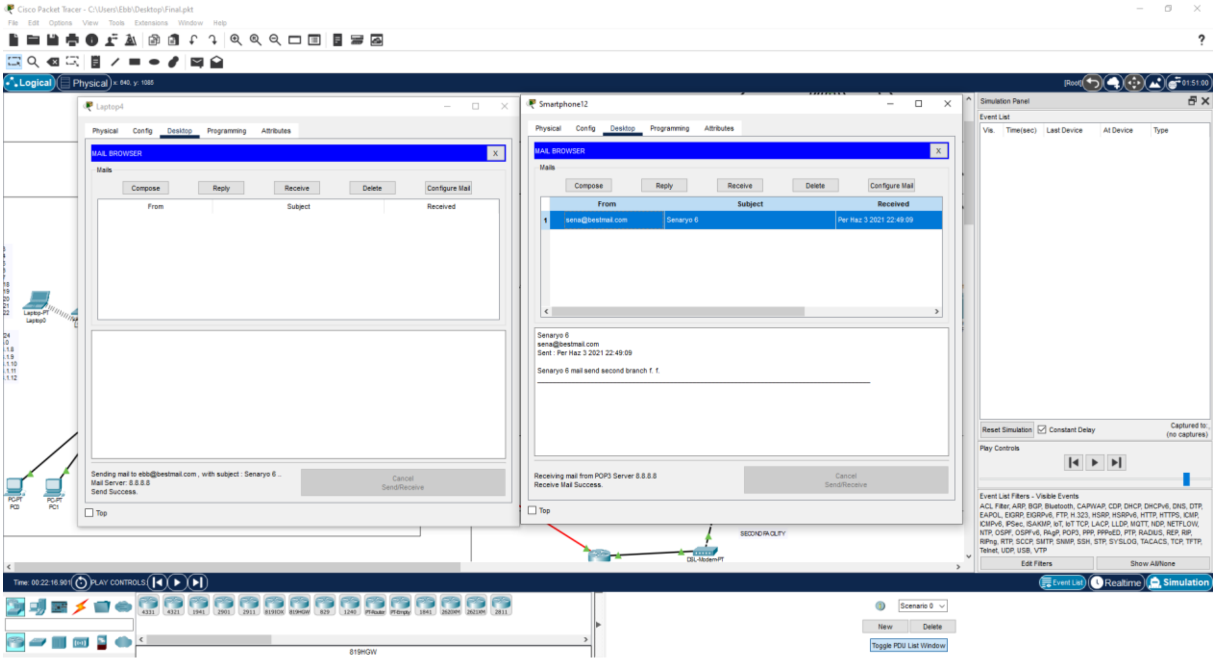




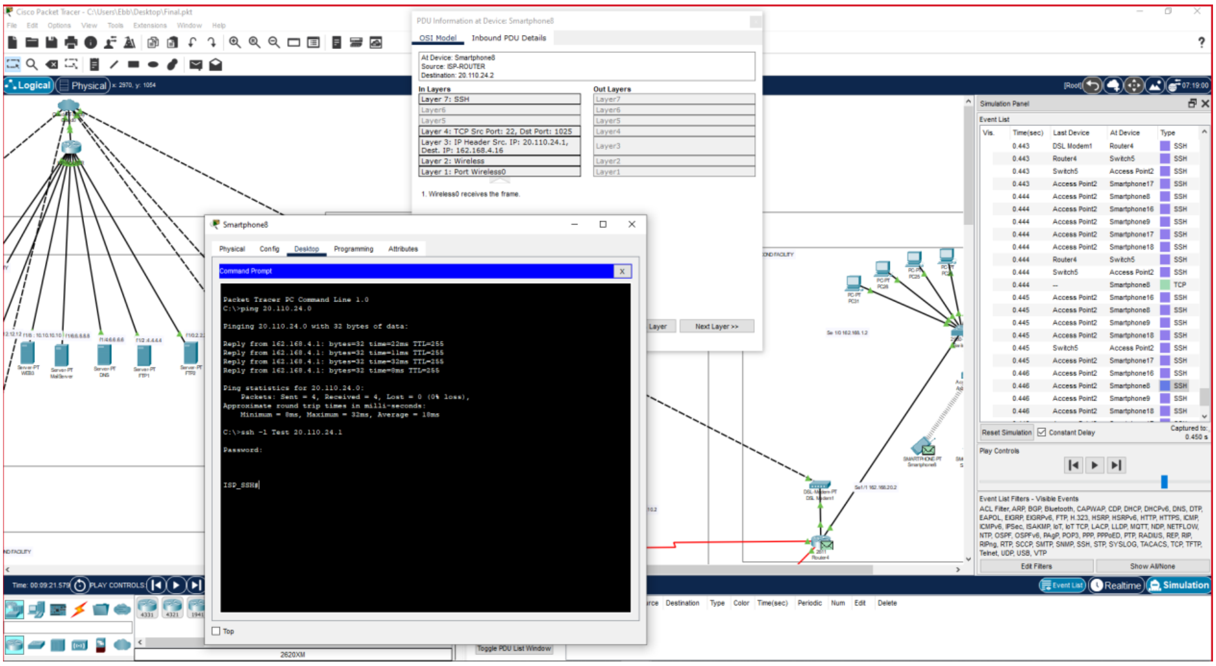


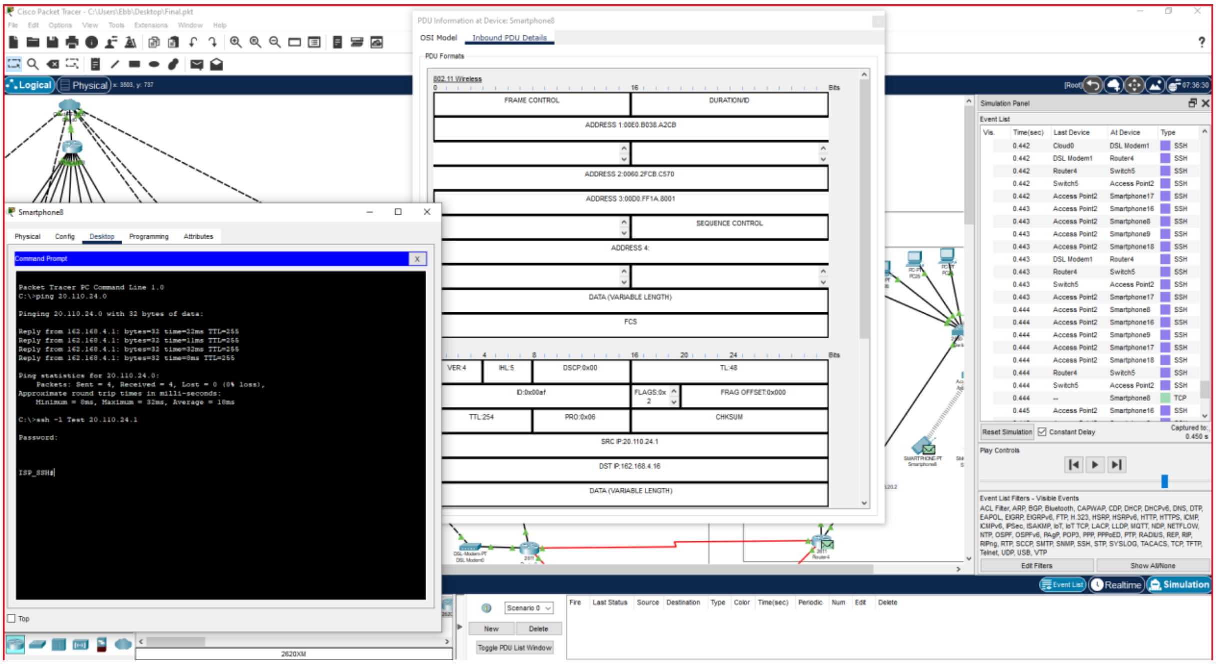
**Scenario 6:** A laptop user from first facility of first branch office wants to send email to her friend in the first facility of second branch office.



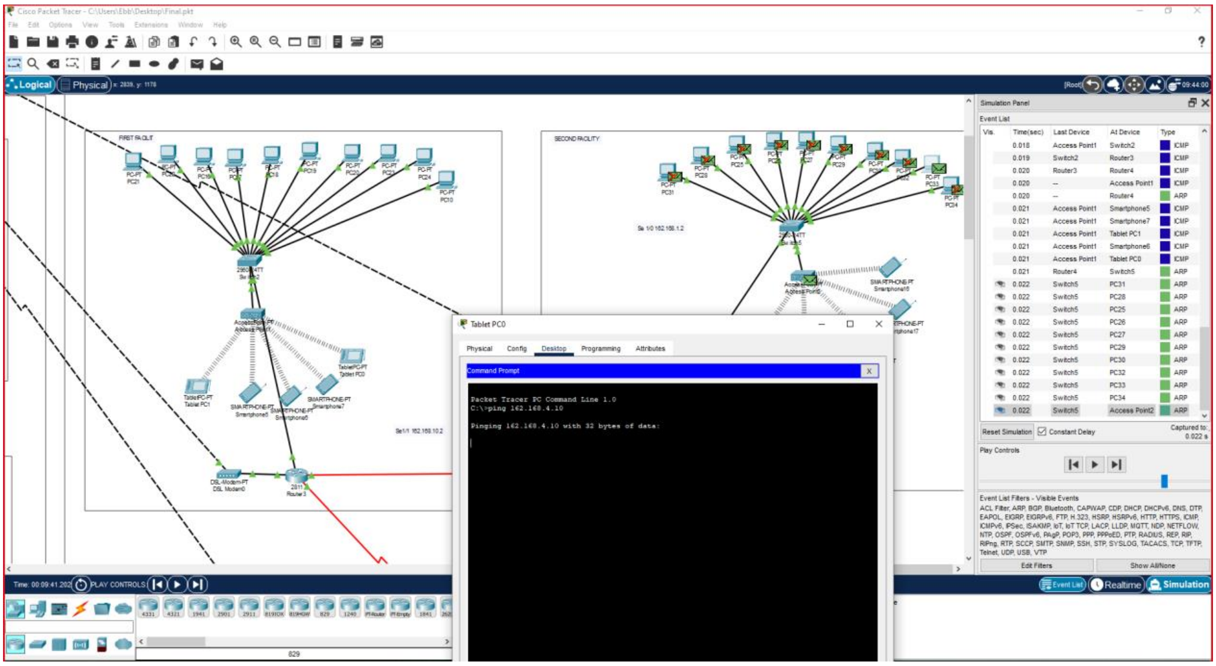


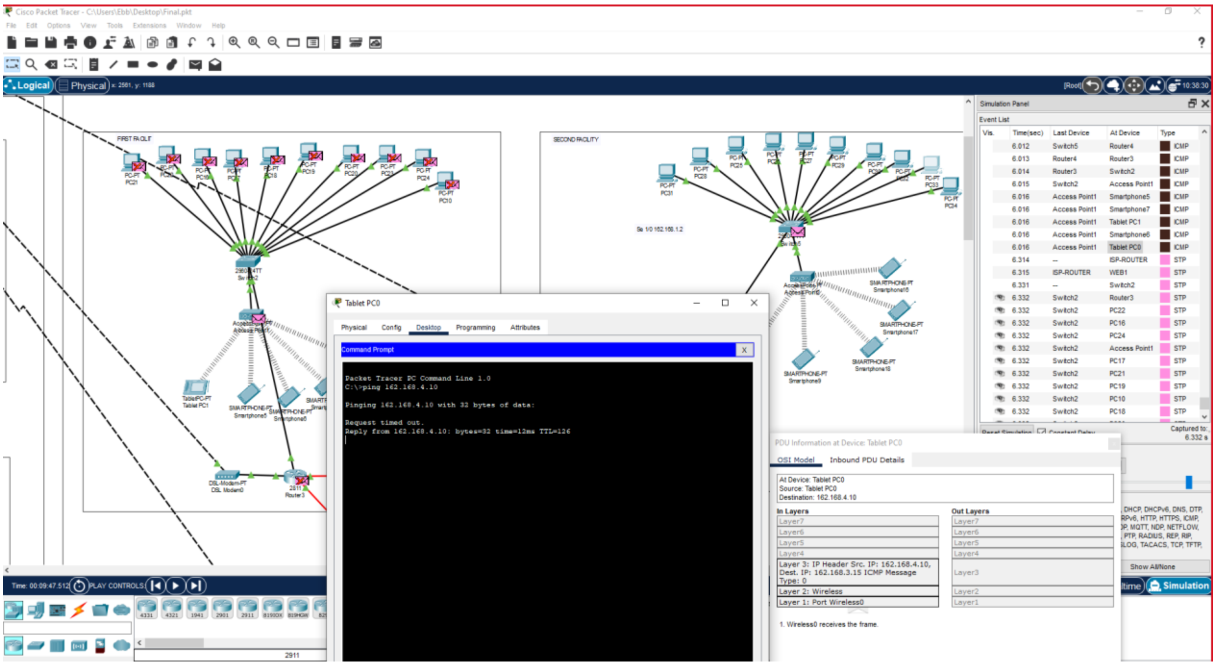

**Scenario 7:** A smartphone user from third facility of second branch office wants to use ssh to connect to a Web server in the third facility of first branch office.

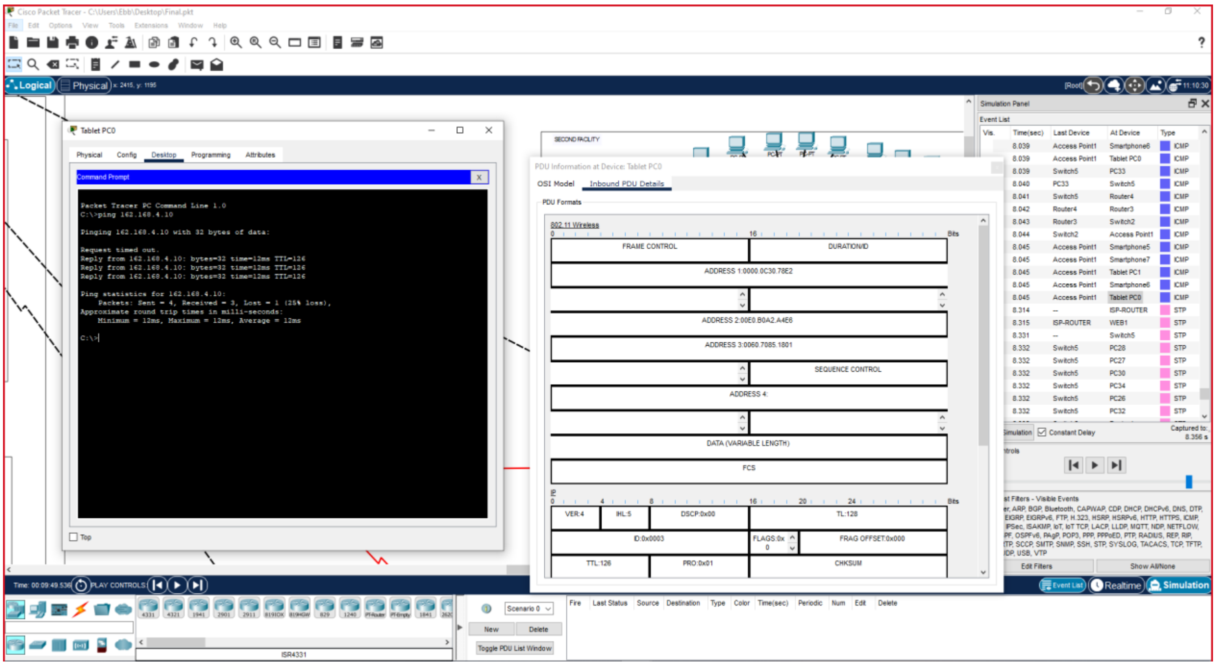




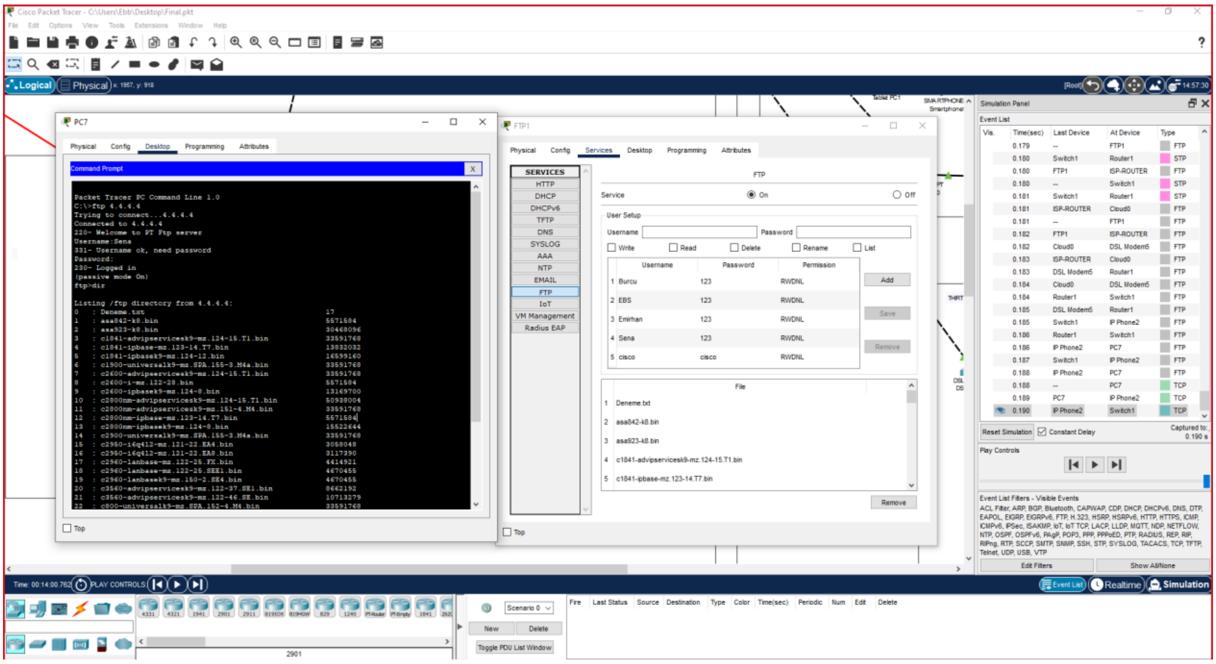
**Scenario 8:** A mobil device user from first facility of  second branch  pings second facility of second branch.

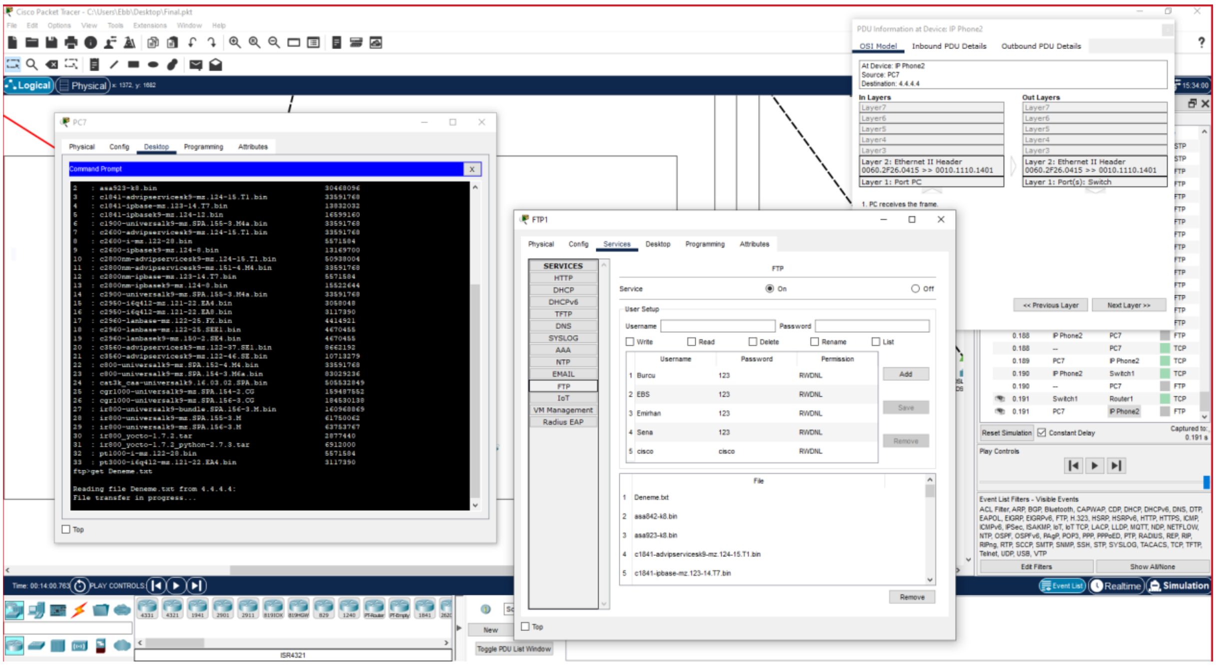


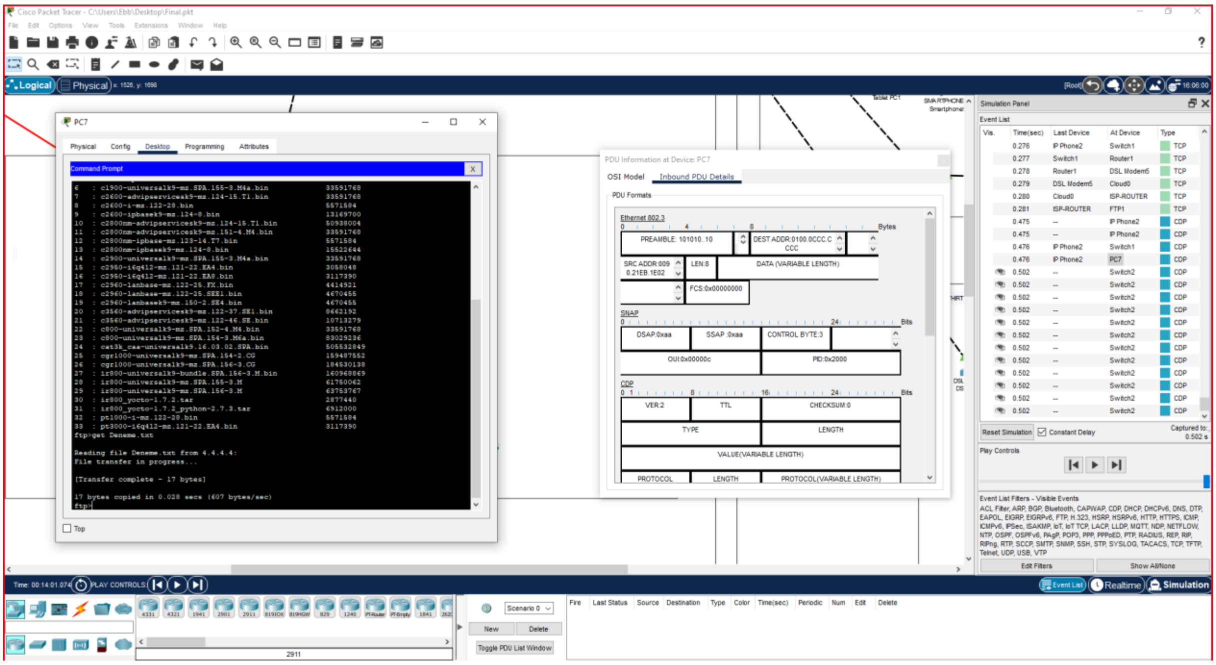

Cisco Packet Tracer - C:\Users\Ebb\Desktop\Final.pkt
Tablet PC0
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 162.168.4.10
Pinging 162.168.4.10 with 32 bytes of data:
Request timed out.
Reply from 162.168.4.10: bytes=32 time=12ms TTL=126
PDU Information at Device: Tablet PC0
OSI Model
Inbound PDU Details
At Device: Tablet PC0
Source: Tablet PC0
Destination: 162.168.4.10
In Layers
Out Layers
Layer 3: IP Header Src. IP: 162.168.4.10, Dest. IP: 162.168.3.15 ICMP Message Type: 0
Layer 2: Wireless
Layer 1: Port Wireless0
1. Wireless0 receives the frame.
Simulation Panel
Event List


Cisco Packet Tracer - C:\Users\Ebb\Desktop\Final.pkt
Tablet PC0
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 162.168.4.10
Pinging 162.168.4.10 with 32 bytes of data:
Request timed out.
Reply from 162.168.4.10: bytes=32 time=12ms TTL=126
Reply from 162.168.4.10: bytes=32 time=12ms TTL=126
Reply from 162.168.4.10: bytes=32 time=12ms TTL=126
Ping statistics for 162.168.4.10:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 12ms, Maximum = 12ms, Average = 12ms
C:\>
PDU Information at Device: Tablet PC0
OSI Model
Inbound PDU Details
PDU Formats
802.11 Wireless
FRAME CONTROL
DURATION/ID
ADDRESS 1:0000.0C30.78E2
ADDRESS 2:00E0.B0A2.A4E6
ADDRESS 3:0060.7085.1801
SEQUENCE CONTROL
ADDRESS 4:
DATA (VARIABLE LENGTH)
FCS
VER:4
IHL:5
DSCP:0x00
TL:128
ID:0x0003
FRAG OFFSET:0x000
TTL:126
PRO:0x01
CHKSUM
Simulation Panel
Event List

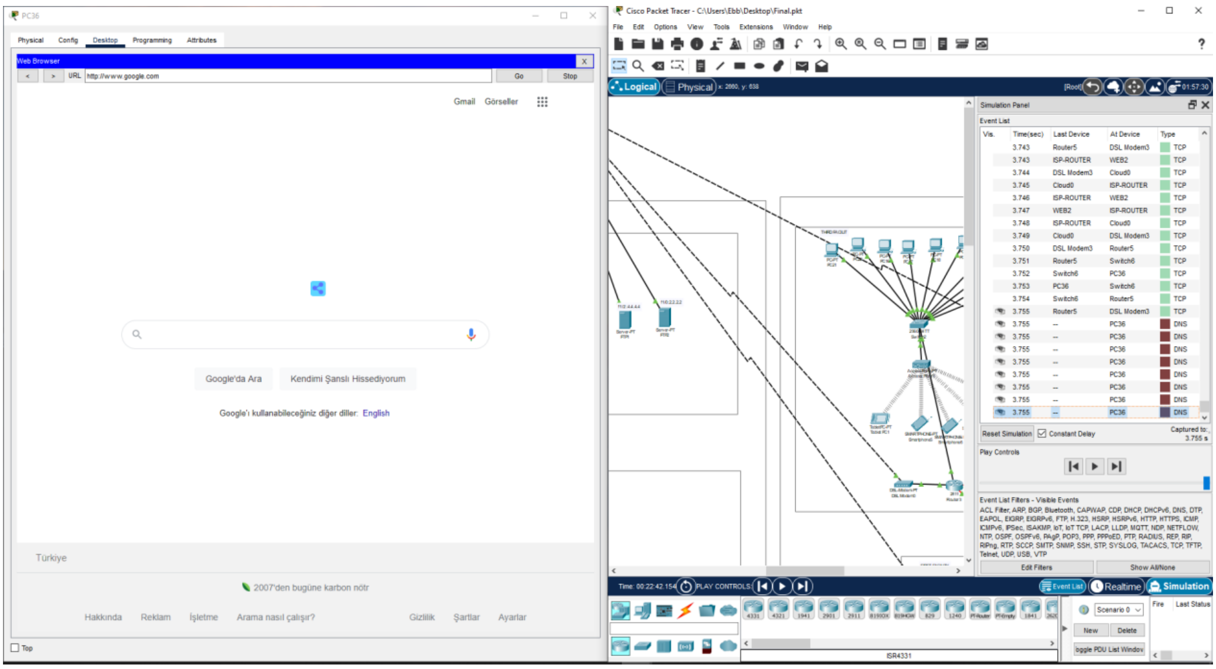
**Scenario 9:** A computer user from second facility of first branch get file from FTP server.

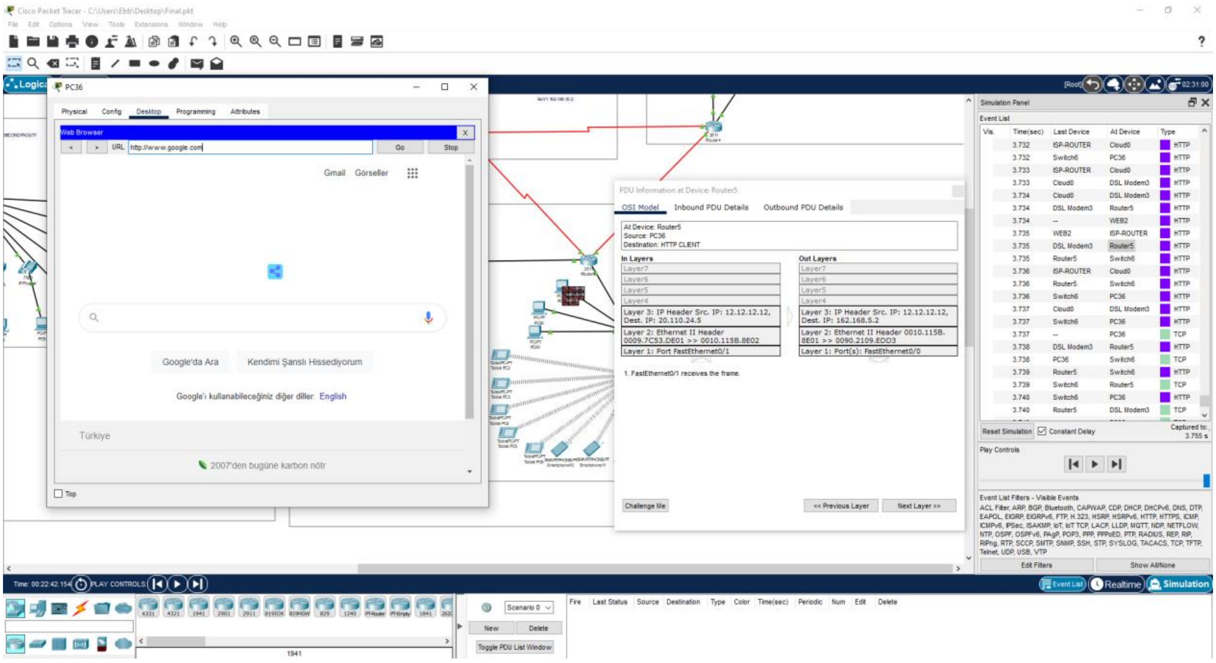


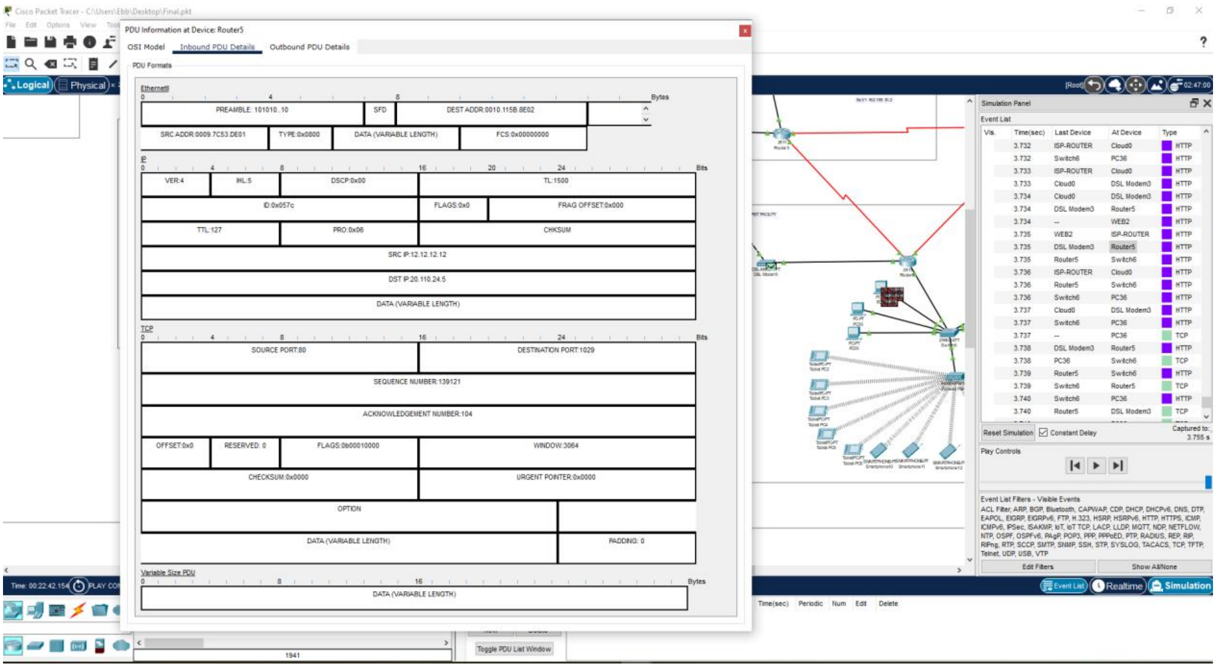




**Scenario 10:** A workstation from first facility of second branch want to browse WEB.






**Notes on Simulation: When we first turn on Cisco Packet Tracer, the system takes some time to recover, but due to the application, it may be 'faild' at the first connections. After one or two tries, the system starts to work stably and the errors disappear. This is because of Cisco Packet Tracer. In the SSH scenario, we did not connect directly to WEBServer, so we connected to the Router via SSH. We were asked for the web server, but when we couldn't do this, we connected to the web server's router via SSH.**

# 4. Conclusion

Analysis and tests on simulation show that topology and architecture selection is done correctly according to requirements.We designed the communication between the 2 branches and the communication and rules between the branches themselves, tested their work and the communication of different protocols and carried out the simulation.
We tried to optimize our design between 2 branches and inside buildings by experimenting with different network topologies and designs. We tested the accuracy and operation of the flow in the network with simulation scenarios. We have a better understanding of the working mechanism of the network by displaying the scenarios in case of heavy traffic and the modeling of the packets in OSI layers in simulation. We tried to fix the errors in the network by developing different solutions, taking into account the loss of communication between branches and buildings. We have understood where and how different connection types and ports are used by connecting them . We have made sure that we have successfully designed our network by meeting the
requirements in the project, trying out its tests and simulation scenarios.

# 5. REFERENCES


[1] https://www.youtube.com/watch?v=HWZ6_Z8bi2c&t=141s
[2] https://www.youtube.com/watch?v=otAZaqjjwl0&t=289s
[3] https://www.youtube.com/watch?v=8LwViEbJZLU
[4] https://www.youtube.com/watch?v=OlX8RfmdANk&t=112s
[5] https://www.computernetworkingnotes.com/ccna-study-guide/ospf-configuration-step-by-step-guide.html
[6] https://www.youtube.com/watch?v=TqWLJMt1dtQ&t=548s
[7] https://www.youtube.com/watch?v=rCKBV3rCHhI&t=57s
[8] https://www.youtube.com/watch?v=hcNqBxQbZs4&t=1055s
[9] https://www.youtube.com/watch?v=MXNM7_Kykaw&t=739s
[10] https://my.kualo.com/knowledgebase/?kbcat=0&article=890
[11] https://linoxide.com/how-use-ssh-commands-windows-10-command-prompt/
[12] https://www.youtube.com/watch?v=_D7V6oWtSnI
[13] https://www.youtube.com/watch?v=-5PWBQPIe9I
[14] https://blog.router-switch.com/2011/11/cisco-catalyst-switch-how-to-create-and-delete-vlan-on-it/
[15] https://www.youtube.com/watch?v=hcNqBxQbZs4
[16] https://www.youtube.com/watch?v=_MxWcnNcCdE
[17] https://www.youtube.com/watch?v=U2Z61gkYoFs
[18] https://www.youtube.com/watch?v=HWZ6_Z8bi2c
[19] https://www.cisco.com/c/en/us/td/docs/switches/wan/mgx/mgx_8850/software/mgx_r3/rpm/rpm_r1-1/configuration/guide/appc.html
[20] https://serverfault.com/questions/415309/dhcpd-multiple-domain-name-servers
[21] http://www.networksorcery.com/enp/protocol/bootp/option006.htm
[22] https://static-course-assets.s3.amazonaws.com/IntroNet50ENU/files/10.2.2.8%20Packet%20Tracer%20-%20DNS%20and%20DHCP%20Instructions.pdf
[23] https://serverfault.com/questions/951435/which-name-server-will-be-chosen-to-handle-dns-query-if-multiple-name-servers-ar
[24] https://www.youtube.com/watch?v=0i3POPmXpP0
[25] https://www.computernetworkingnotes.com/ccna-study-guide/vlan-configuration-commands-step-by-step-explained.html
[26] https://community.cisco.com/t5/small-business-switches/sx500-how-to-add-secondary-dns-server-ip-address-in-dhcp-pool/td-p/2613295
[27] https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-2_2_e/consolidated_guide/configuration_guide/b_1522e_consolidated_2960x_cg/b_consolidated_152ex_2960-X_cg_chapter_0100110.pdf
[28] https://www.cisco.com/c/en/us/support/docs/ip/domain-name-system-dns/24182-reversedns.html
[29] https://systemzone.net/computer-network-topology-outline/

[30] https://www.youtube.com/watch?v=U2Z61gkYoFs
[31] https://www.youtube.com/watch?v=_MxWcnNcCdE&t=472s
[32] https://en.wikipedia.org/wiki/Discrete-event_simulation