DOKUZ EYLUL UNIVERSITY

ENGINEERING FACULTY

DEPARTMENT OF COMPUTER ENGINEERING

CME 3204 DATA COMMUNICATIONS AND COMPUTER NETWORKS

Term Project – Metropolitan Area Network

By

2019510042 Gufran Güneş

2019510050 Selim Eren Karar

Lecturers

Prof.Dr. Yalçın ÇEBİ

Res.Asst. İbrahim Atakan Kubilay

Izmir

12.05.2023

TABLE OF CONTENTS

1. Introduction

This report is the final report of the Metropolitan Area Network project, which is the term paper of the CME3204 Data Communications course. At the same time, this project was made using Cisco Packet Tracer and includes the following structures:

The mission of this Project is to provide the following requirements of a Metropolitan Area Network (two branches, each branch consists of three facilities):

a. Browse web
b. Send and receive emails
c. Transfer files (FTP)
d. VoIP conference
e. Edit applications
f. Wireless connection through internet

1. First branch's network is comprised of 3 distinct facilities and each facility has different units and requirements.

   All specification for the first branch office is as following:

   a) First facility has 10 workstation (PC) users, 3 wireless users (laptop) and 3 smartphone users. All the users in this facility can browse web, send e-mails andtransfer files by using their devices.
   b) Second facility has 5 workstation users who can use Web and FTP. 3 of workstations are used for VoIP conference events.
   c) Third facility has a server farm including 5 Web servers, 2 FTP servers, 1 DHCP server, 1 mail server and 1 domain name server (DNS).

2. Second branch includes 3 distinct facilities, and each facility includes different units and requirements.
   a) First facility has 10 workstation users, 5 wireless users and 10 tablet users, who can connect to the Internet using wireless connection, browse Web and use e-mail applications.
   b) Second facility has ten workstation users and 5 smartphone users. They can browse the web, edit applications, and transfer files.
   c) Third facility has ten workstations and 5 mobile devices that are used to browse Web, send and receive emails.

1.1. Project Definition and Problem Formulation

The project's description is to create a computer network that connects people to computer resources in an area the size of a metropolitan area. One of the project's major issues is that it has too many gadgets, all of which must work together. Otherwise, users will be unable to send emails from one branch to another, indicating that the Metropolitan Area Network is not operational. There are numerous configurations.

Any problems that occur while adjusting the devices to be created may result in improper connections and errors. As a result, the project necessitates careful planning, extensive research, and accurate designs.

1.2. The purpose and motivation of the project

The purpose of this project is to link people with the appropriate people, to create a long-lasting solution using this system without the use of any physical document transfer, and to apply our theoretical knowledge while working on this project.

This project's main goal is to use Cisco Packet Tracer to design a Metropolitan Area Network (MAN). A metropolitan area network (MAN) is a type of computer network that links computers in an area with many buildings, such as a single large metropolis, several smaller cities, or any other sizeable area. The size of a MAN is more than that of a LAN but less than that of a WAN. The name "metropolitan" emphasizes the scale of the network, not the demographics of the area it covers, hence MANs not need to be in urban areas.[14] MAN often joins networks of various organizations, but in this case, it joins two branches, each of which has three facilities.

The major improvements that this project has given us, a group of computer engineering students who will graduate next year, are knowing how to use servers, routers, protocols, packages, and servers in hardware, arranging them effectively, and developing high-quality systems. Additionally, because it is a group project, it directly strengthened our ability to work in groups and communicate with one another. The project currently functions flawlessly based on the scenarios that were successfully finished prior to the completion date, but since this is a final report, there are no more mistakes.

1.3. Term Definitions

i) Protocol: A protocol is a common set of guidelines that enables communication between electronic devices. These guidelines specify the permitted types of data transmission, the commands used to send and receive data, and the procedures for verifying data transfers. There are protocols for numerous applications. Examples include Internet communication (e.g., IP), wireless networking (e.g., 802.11ac), and wired networking (e.g., Ethernet). There are numerous protocols in the Internet protocol suite, which is used to send data across the Internet. These protocols can be divided into four groups:

- ~ Link layer - PPP, DSL, Wi-Fi, etc.
- ~ Internet layer - IPv4, IPv6, etc.
- ~ Transport layer - TCP, UDP, etc.
- ~ Application layer - HTTP, IMAP, FTP, etc.

ii) Packet: A packet is a brief message conveyed through a network, like a LAN or the Internet. Each packet contains the content (or data) being transported as well as a source and destination, just like a real-world package would. The packets are put back together into a single file or other contiguous block of data when they arrive at their destination.

While each protocol has its own unique packet form, most packets consist of a header and a payload. The header contains data that relates to the packet. For instance, the following fields are present in an IPv6 header:

- ~ Source address (128 bits) - IPv6 address of the packet origin
- ~ Destination address (128 bits) - IPv6 address of the packet destination
- ~ Version (4 bits) - "6" for IPv6
- ~ Traffic class (8 bits) - priority setting for the packet
- ~ Flow label (20 bits) - optional ID that labels the packet as part of a specific flow; used to distinguish between multiple transmissions from a single origin
- ~ Payload length (16 bits) - size of the data, defined in octets
- ~ Next header (8 bits) - ID of the header following the current packet; may be TCP, UDP, or another protocol
- ~ Hop limit (8 bits) - maximum number of network hops (between routers, switches, etc.) before the packet is dropped; also known as "TTL" in IPv4

iii) IMAP is an acronym for "Internet Message Access Protocol" and is pronounced "eye-map." It is a technique for getting access to email messages that are stored on a server without having to download them to your personal computer. The fundamental distinction between IMAP and the well-known "POP3" email system is this. To access messages sent using POP3, users must first download them to their hard drive. Using an IMAP mail server has the benefit of allowing users to view their mail on several machines and always see the same messages. This is because, unless the user decides to download them to a local drive, the messages remain on the server.

iv) POP is an acronym for "Post Office Protocol." POP3, also known as just "POP," is a straightforward, standardized approach to sending emails. Emails are received by a POP3 mail server, which filters them into the proper user folders. The messages are downloaded to the user's hard drive when the user connects to the mail server to collect his mail.

When you configure your e-mail client, such as Outlook (Windows) or Mail (Mac OS X), you will need to enter the type of mail server your e-mail account uses. This will typically be either a POP3 or IMAP server.

v) DNS: Stands for "Domain Name System." Domain names serve as memorizable names for websites and other services on the Internet. However, computers access Internet devices by their IP addresses. DNS translates domain names into IP addresses, allowing you to access an Internet location by its domain name.

vi) FTP: Stands for "File Transfer Protocol." FTP is a protocol designed for transferring files over the Internet. Files stored on an FTP server can be accessed using an FTP client, such as a web browser, FTP software program, or a command line interface.
An FTP server can be configured to enable different types of access. For example, an "anonymous FTP" configuration allows anyone to connect to the server. However, anonymous users may only be allowed to view certain directories and may not be able to upload files. If anonymous FTP access is disabled, users are required to log in to view and download files.

vii) HTTP: Stands for "Hypertext Transfer Protocol." HTTP is the protocol used to transfer data over the web. It is part of the Internet protocol suite and defines commands and services used for transmitting webpage data.
HTTP uses a server-client model. A client, for example, may be a home computer, laptop, or mobile device. The HTTP server is typically a web host running web server software, such as Apache or IIS. When you access a website, your browser sends a request to the corresponding web server, and it responds with an HTTP status code. If the URL is valid and the connection is granted, the server will send your browser the webpage and related files.

Some common HTTP status codes include:

- ~ 200 - successful request (the webpage exists)
- ~ 301 - moved permanently (often forwarded to a new URL)
- ~ 401 - unauthorized request (authorization required)
- ~ 403 - forbidden (access is not allowed to the page or directory)
- ~ 500 - internal server error (often caused by an incorrect server configuration)

viii) TCP: Stands for "Transmission Control Protocol." TCP is a fundamental protocol within the Internet protocol suite — a collection of standards that allow systems to communicate over the Internet. It is categorized as a "transport layer" protocol since it creates and maintains connections between hosts.

TCP compliments the Internet protocol (IP), which defines IP addresses used to identify systems on the Internet. The Internet protocol provides instructions for transferring data while the transmission control protocol creates the connection and manages the delivery of packets from one system to another. The two protocols are commonly grouped together and referred to as TCP/IP.

ix) ICMP: The "Internet Control Message Protocol." Computer systems use the TCP/IP protocol to send and receive data while transferring data over the Internet. If there is a problem with the connection, ICMP, a component of the Internet protocol, is used to send error and connection status messages.

It may appear to be a simple and rapid operation when one computer connects to another system over the Internet (for example, a home computer connecting to a Web server to access a webpage). Even though the connection might be made in a matter of seconds, it frequently takes several different connections for the computers to successfully communicate with one another. In fact, it could surprise you that Internet connections are successful so frequently if you were to track every stage of a connection using the traceroute command. This is because the network must be operational and able to receive requests from your computer for each "hop" along the route.

x) Server: A server is a computer that makes data available to other computers. It may use the Internet to provide data to systems connected to a local area network (LAN) or a wide area network (WAN).

There are many kinds of servers, such as web servers, mail servers, and file servers. Each type runs software designed specifically for the server's function. For instance, a Web server might run Microsoft IIS or Apache HTTP Server, both of which offer access to websites over the Internet. An application like Exim or iMail, which offers SMTP capabilities for sending and receiving email, may be running on a mail server. To distribute files over a network, a file server may use Samba or the built-in file sharing features of the operating system.

xi) Router: This is a hardware device that routes data (hence the name) from a local area network (LAN) to another network connection. A router acts like a coin sorting machine, allowing only authorized machines to connect to other computer systems. Most routers also keep log files about the local network activity.

xii) Switch: A switch is used to network multiple computers together. Switches made for the consumer market are typically small, flat boxes with 4 to 8 Ethernet ports. These ports can connect to computers, cable or DSL modems, and other switches. High-end switches can have more than 50 ports and often are rack mounted.

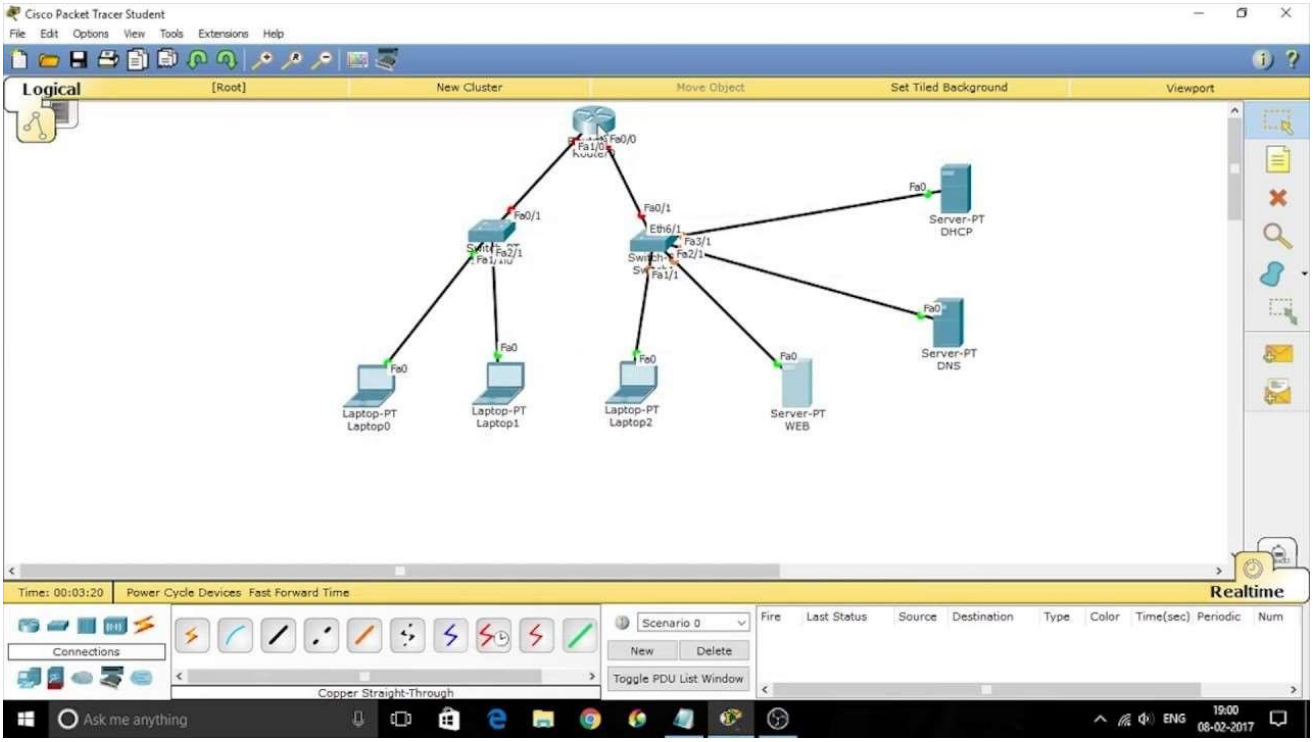
Switches are more advanced than hubs and less capable than routers. Unlike hubs, switches can limit the traffic to and from each port so that each device connected to the switch has enough bandwidth. For this reason, you can think of a switch asa "smart hub." However, switches don't provide the firewall and logging capabilities that.

routers do. Routers can often be configured by software (typically via a Web interface), while switches only work the way the hardware was designed.

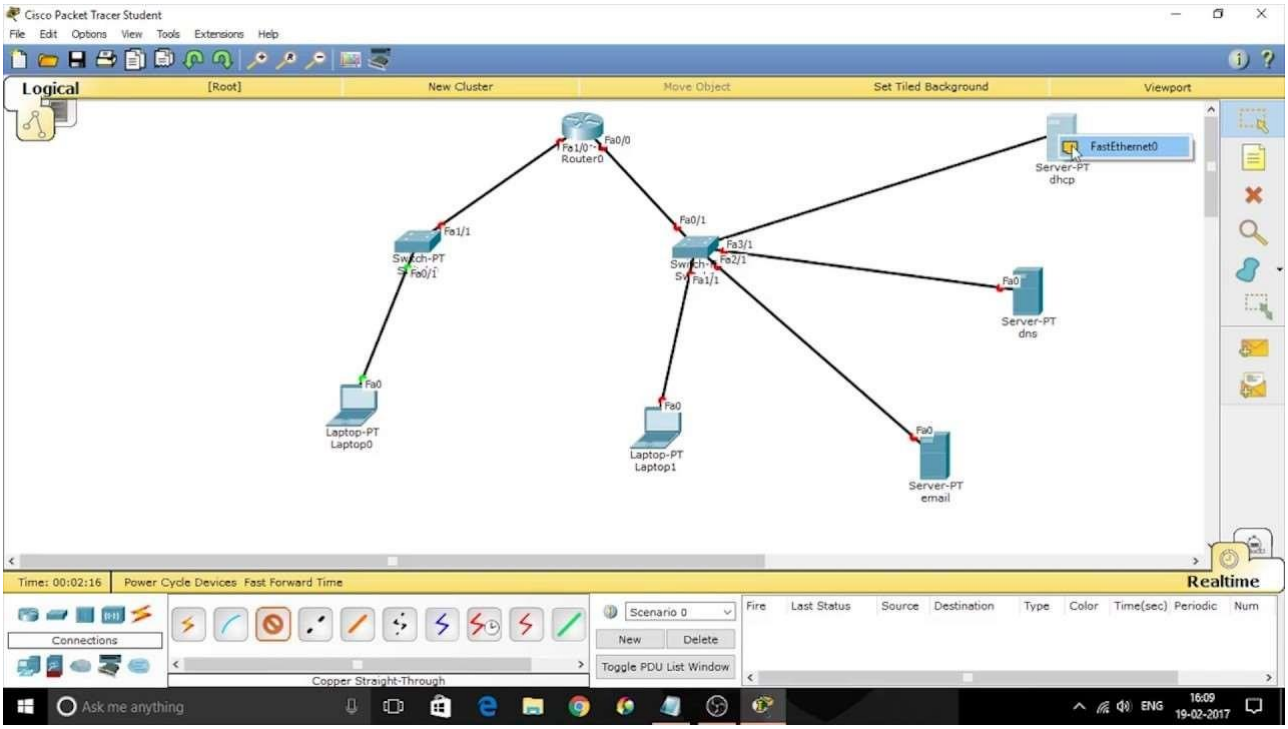
In addition to a small lever or button found on computer hardware, the word "switch" can also apply to those items. In skating and snowboarding, "riding switch" refers to moving backwards while on the snow, although having nothing to do with computers.

xiii) DHCP: This acronym stands for "Dynamic Host Configuration Protocol." DHCP is a protocol that automatically allocates each device that connects to a network a unique IP address. There is no need to manually assign IP addresses to new devices when using DHCP. Therefore, no user configuration is necessary to connect to a DHCP-based network. Because of its ease of use and widespread support, DHCP is the default protocol used by most routers and networking equipment.

1.4. Related Work

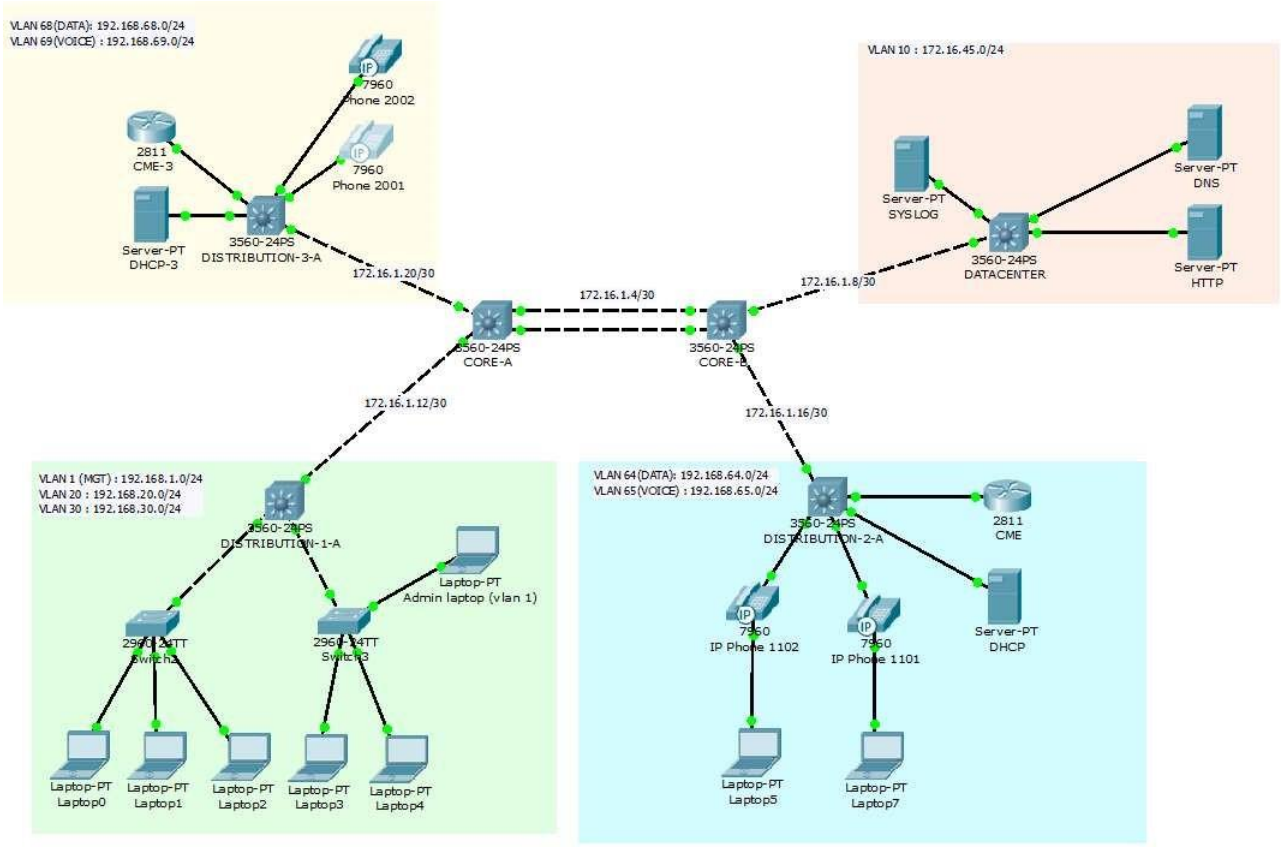


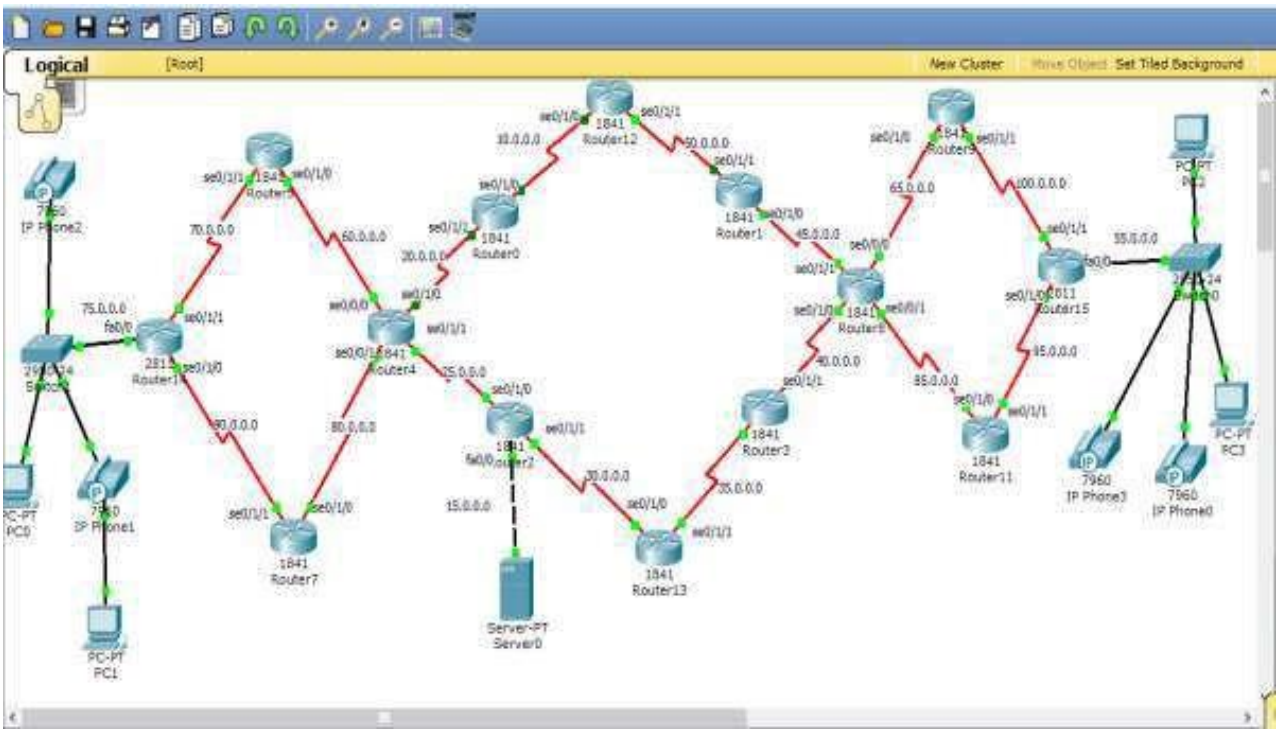
(Example of Web Server System which had been found while surfing the net)



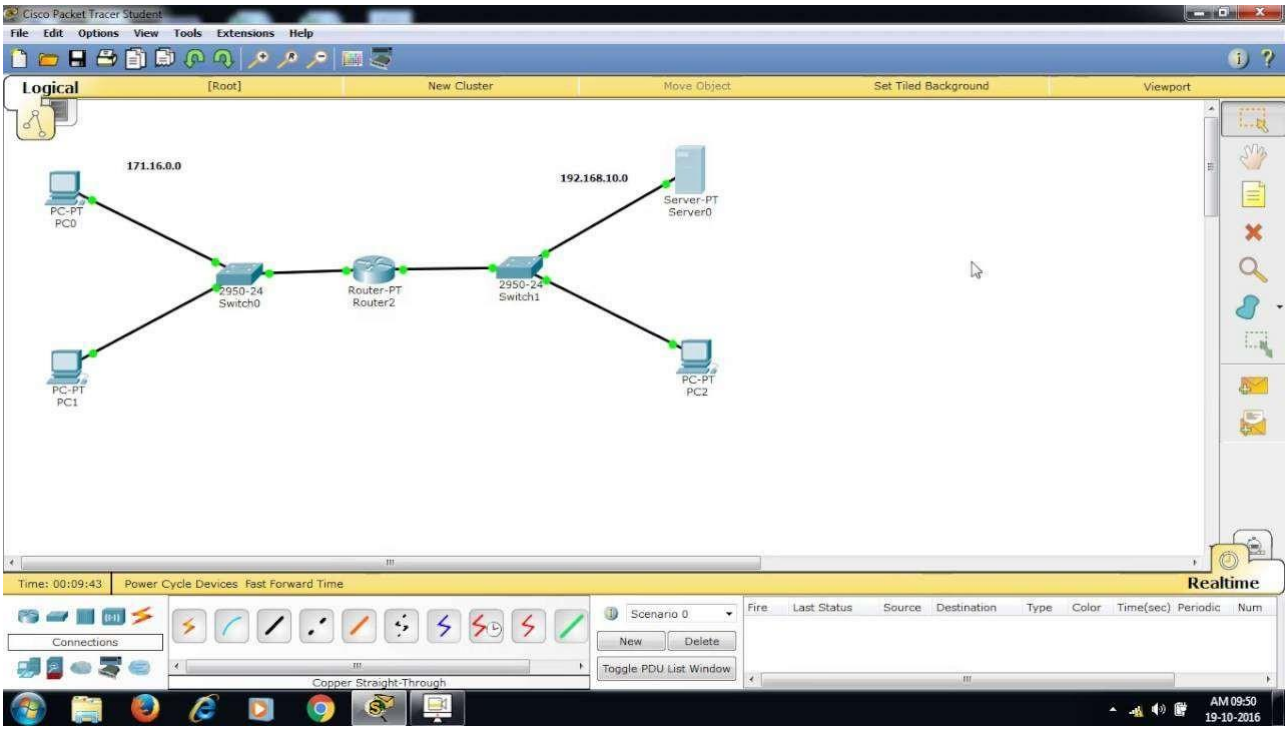
(Example of Mail Server System which had been found while surfing the net)

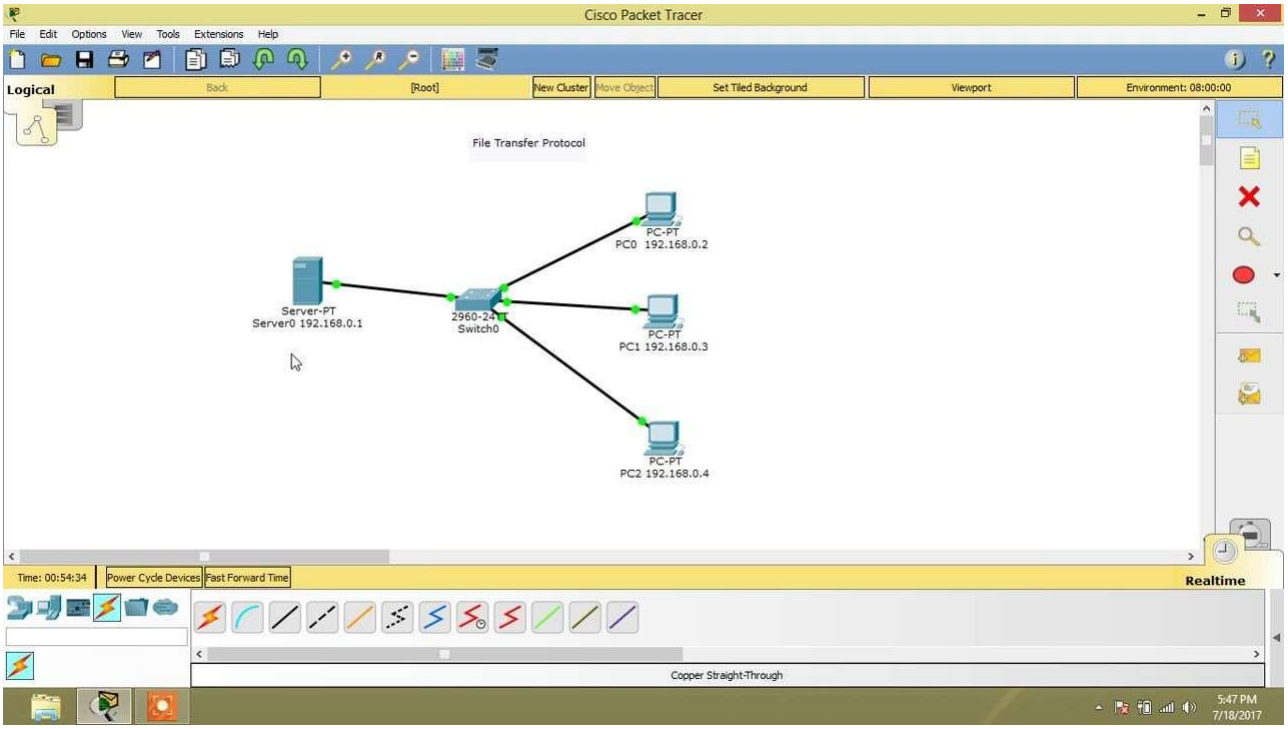
Example of VoIP Conference Calls which only the main ideas were the same as in our project (Image links in order)



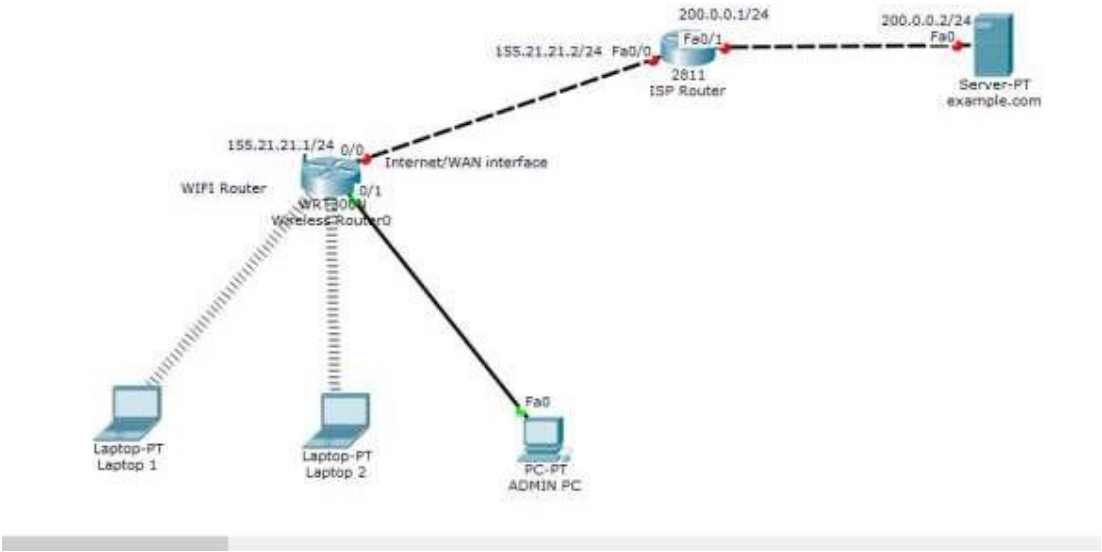


FTP Server Usage





Wireless router Configuration



The examples provided above encouraged us as we began our quest for examples and assisted us in drawing connections for our project. Most of the projects were smaller ones like LANs and PANs (Personal Area Networks). Therefore, we had to develop our own solution and apply it using Cisco Packet Tracer.

2. Method and Simulation

2.1. Simulation and Modeling Concepts

A Discrete Event Simulation (DES) example is the Metropolitan Area Network. A discrete series of occurrences in time is used in discrete event simulations (DES) to study system design. This simulation aids in creating adaptable and diverse answers to issues. It offers the chance and capacity to develop ambiguous components. Additionally, the DES makes it simple and inexpensive to apply new project limitations and changes.

The use of simulation helps us to adjust for probable semantic and configuration issues before the project is launched, while its cost impact is smaller. Detailed reviews and tests on the design are great opportunities to see how the system works and how we can make it more efficient. Because executing the project without employing simulation in network projects covering a vast geographical region such as the Metropolitan Area Network may lead to serious cost problems and the inability to complete the project. The large size of the project may lead to forgetting to test whether the devices at two different ends can send, for example, emails to each other. That is a reason for dissatisfaction for the customer.

Despite all these benefits, employing simulation could postpone the project's transition to reality because it allows for frequent adjustments. Engineers should, therefore, produce the best design possible within the time constraints. While it's possible that this design isn't the best option for the given issue, it should be investigated to see if it's the best one that can be found right now.

2.2. Simulation Environment/Tool

The project's planning has made use of Cisco Packet Tracer. It is a program that is often used to create networks. Large initiatives like the Metropolitan Area Network show that such simulation systems are essential for the network field, even when the positive effect is not very important in small-scale projects. Before executing projects in real life, it is verified by using this application that the design is generated entirely and that tests are applied using a variety of techniques.

At any point during the project's design phase, no extra modules were utilized. The Cisco Packet Tracer's built-in features were utilized.

2.3. Network Design Requirements

End Devices:

- ~ 45 PC
- ~ 8 Laptops
- ~ 13 smartphones
- ~ 10 tablets
- ~ 5 Web servers
- ~ 2 FTP servers
- ~ 1 DHCP server
- ~ 1 mail server
- ~ 3 IP Phones
- ~ 1 domain name server (DNS)

Network Devices:

- ~ 6 access points
- ~ 5 switches
- ~ 5 routers

*Bus and Star topologies had been used so this means this is a **hybrid topology**.*

2.4. Requirement Analysis

There are two branches that are connected.

Each branch has 3 different facilities.

For the first branch:

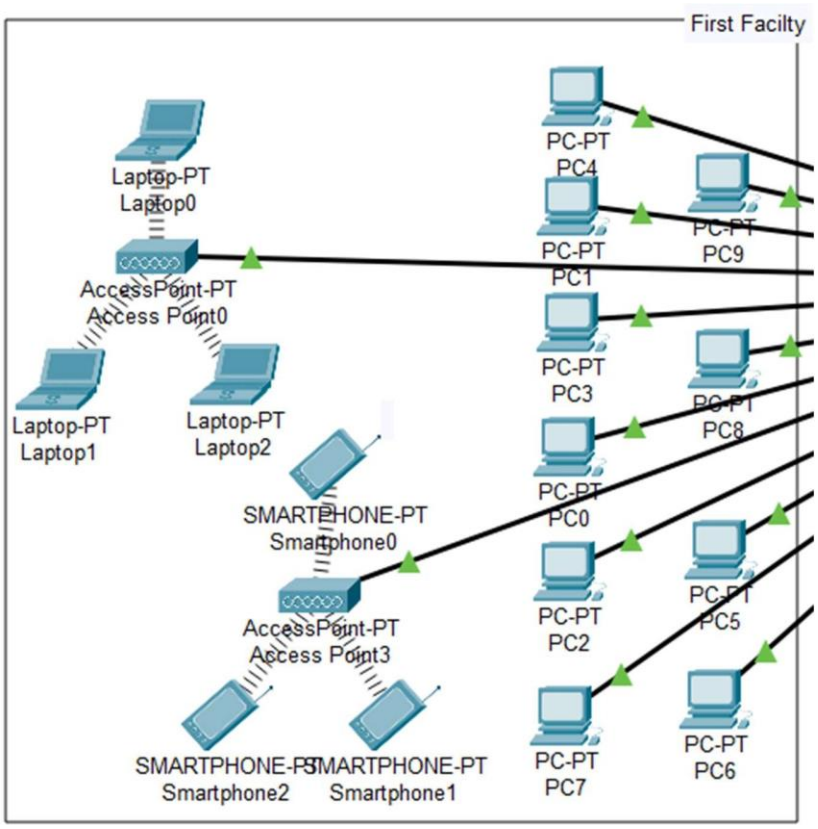
- Devices of first facility should apply web browsing, sending emails and transfer files functions.
- Devices of second facility should apply web browsing and transfer files. 3 of them are used for VoIP conference events.
- Third facilty of first branch consists of servers. It is a server farm. There are web servers, FTP servers, DHCP server, mail server and Domain Name Server (DNS).

For the second branch:

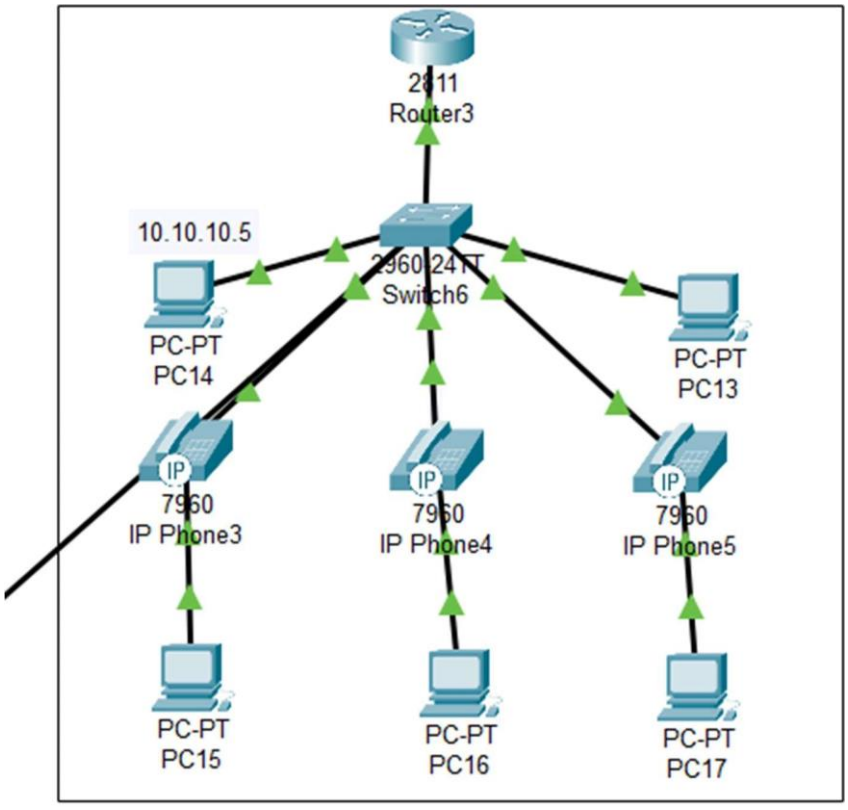
- Devices from first facilty should apply web browsing and use emails. There should be wireless connection.
- Second facilty of second branch should be available for web browsing and edit applications and transfer files.
- Third facility is used for web browsing, sending, and receiving emails.

2.5. Definitions of the System/Model

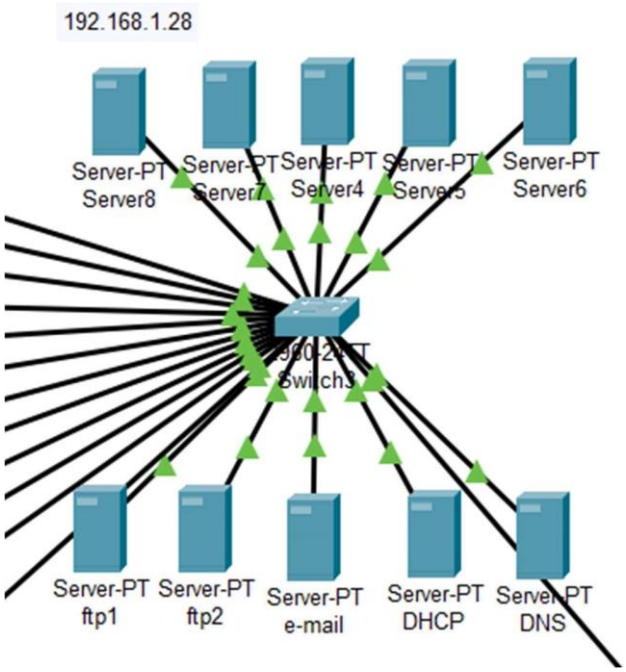
i) 1.Branch 1. Facility:



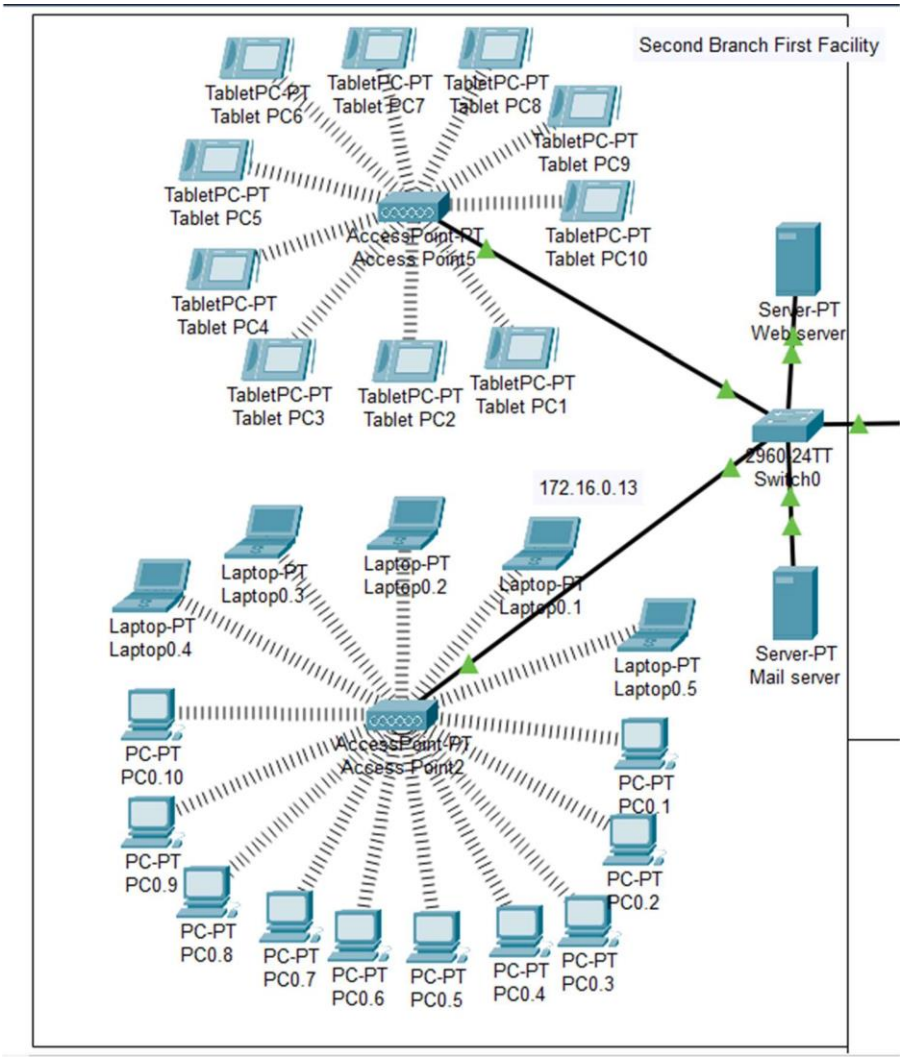
ii) 1.Branch 2. Facility:



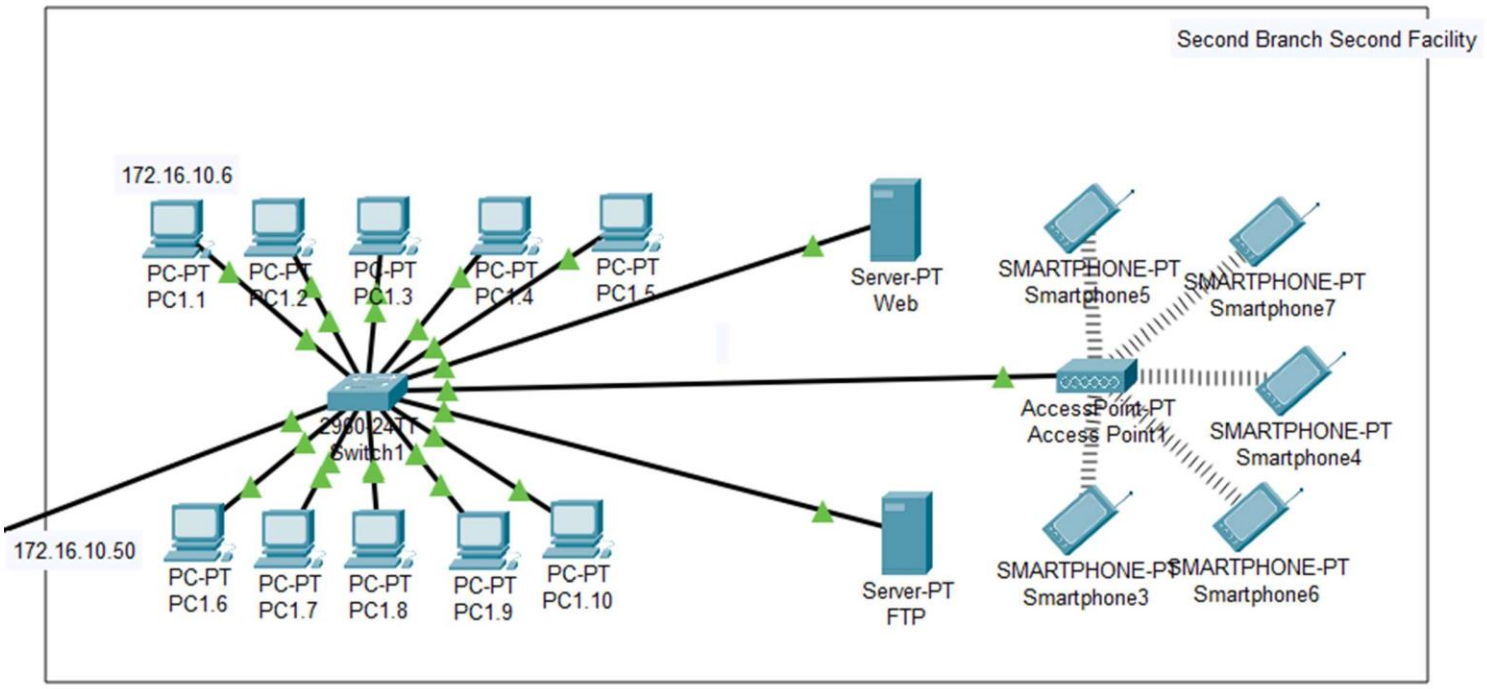
iii) 1.Branch 3. Facility



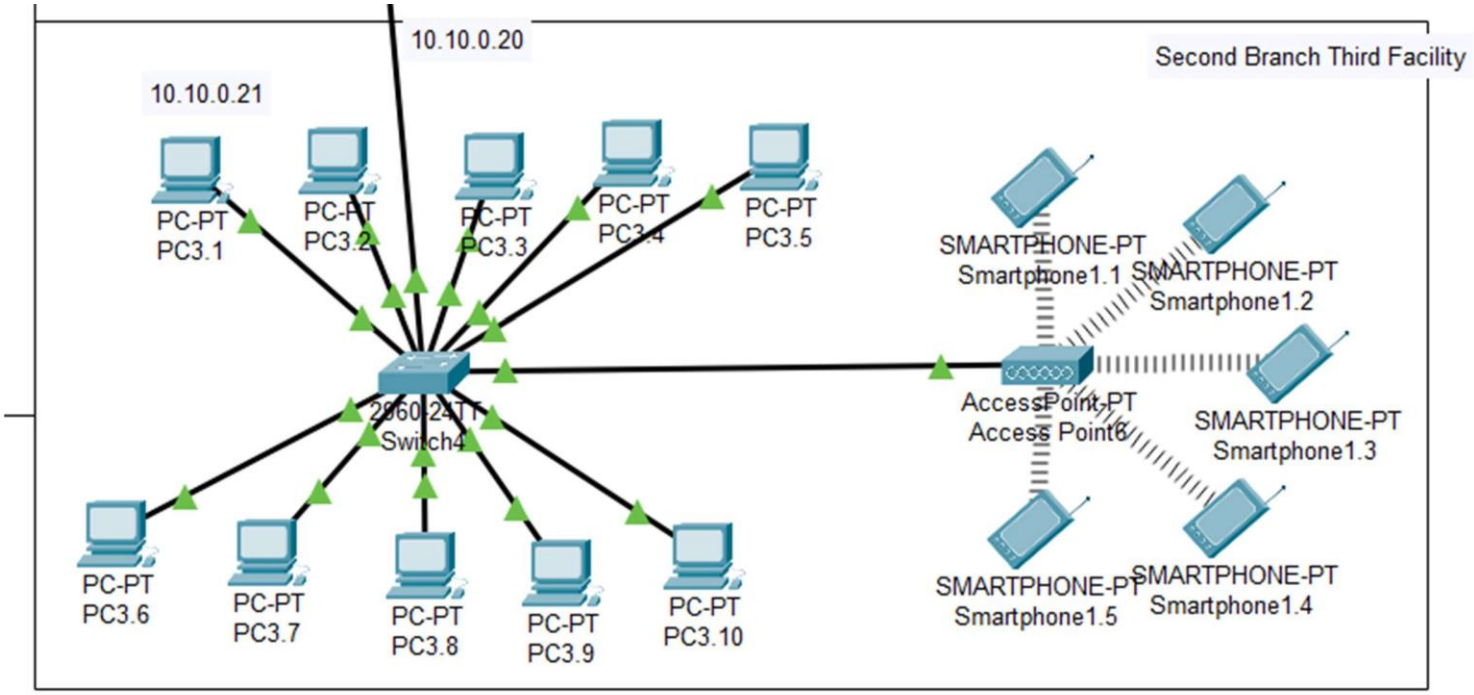
iv) 2. Branch 1. Facility:



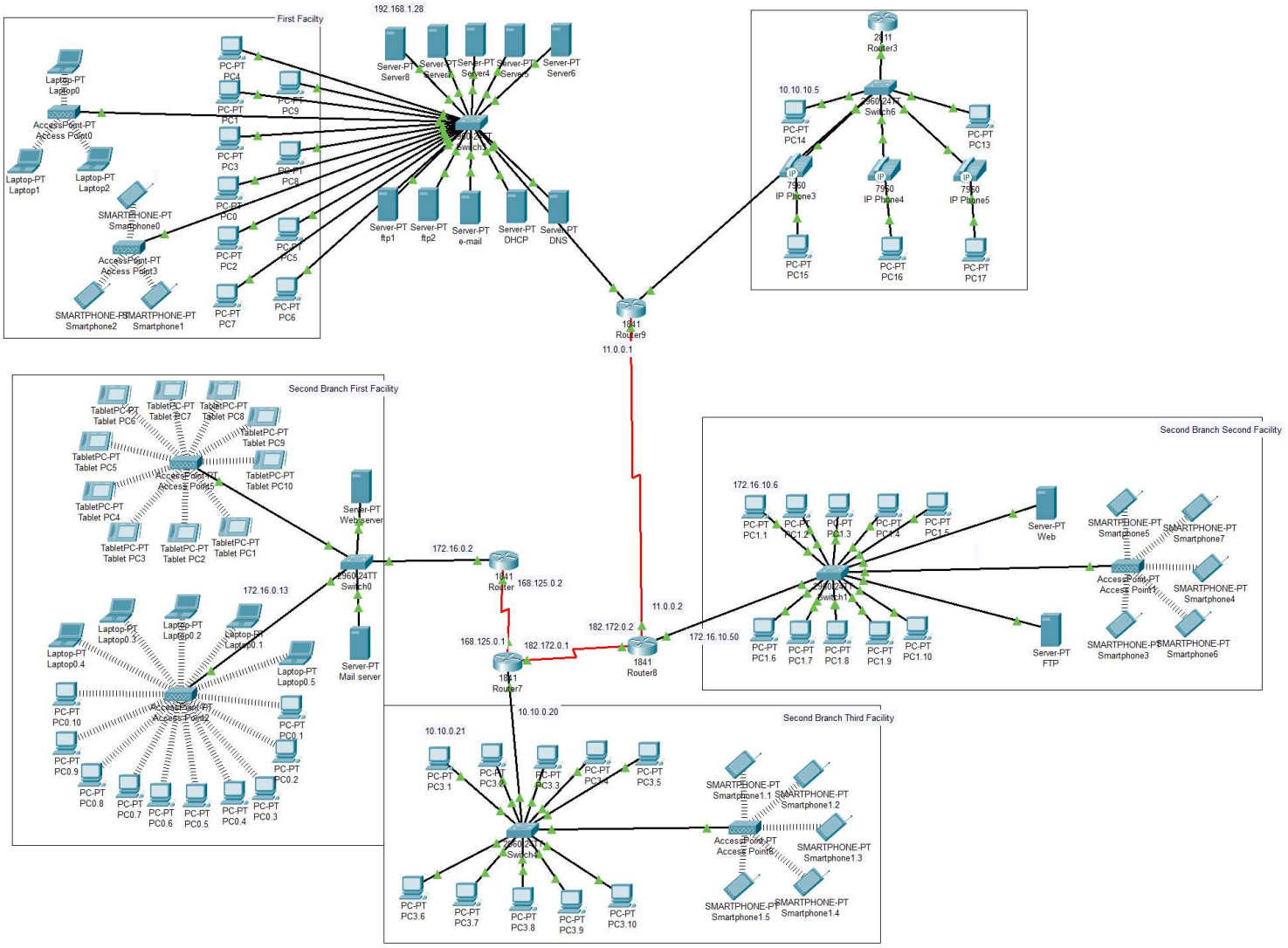
v) 2. Branch 2. Facility



vi) 2. Branch 3. Facility



vii) Whole Facilities and Branches

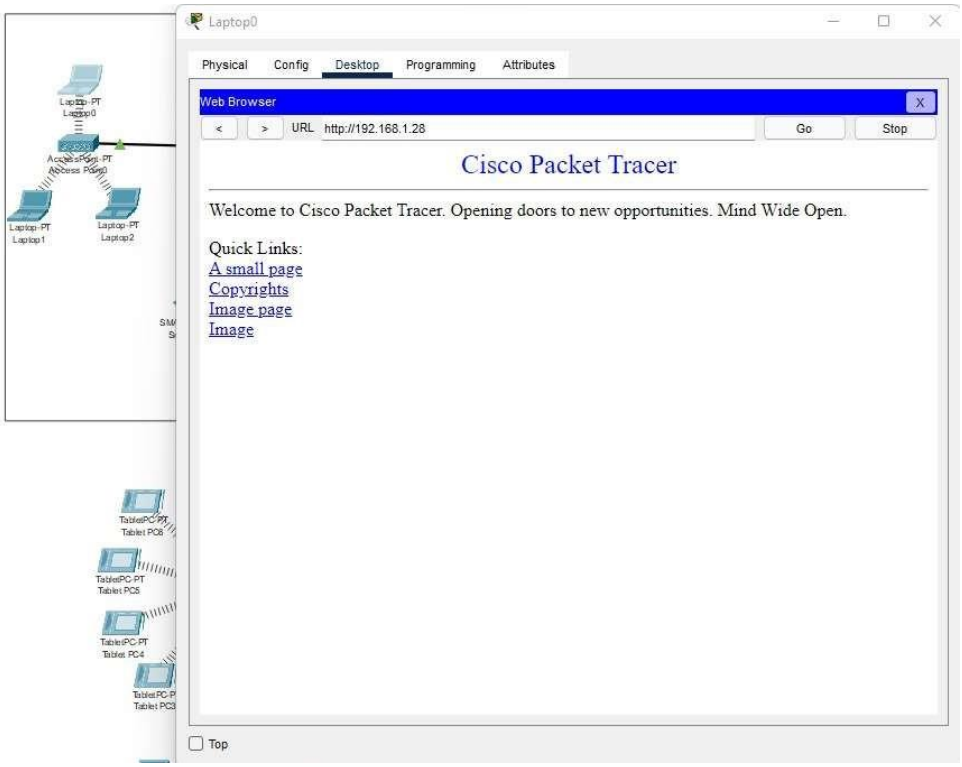


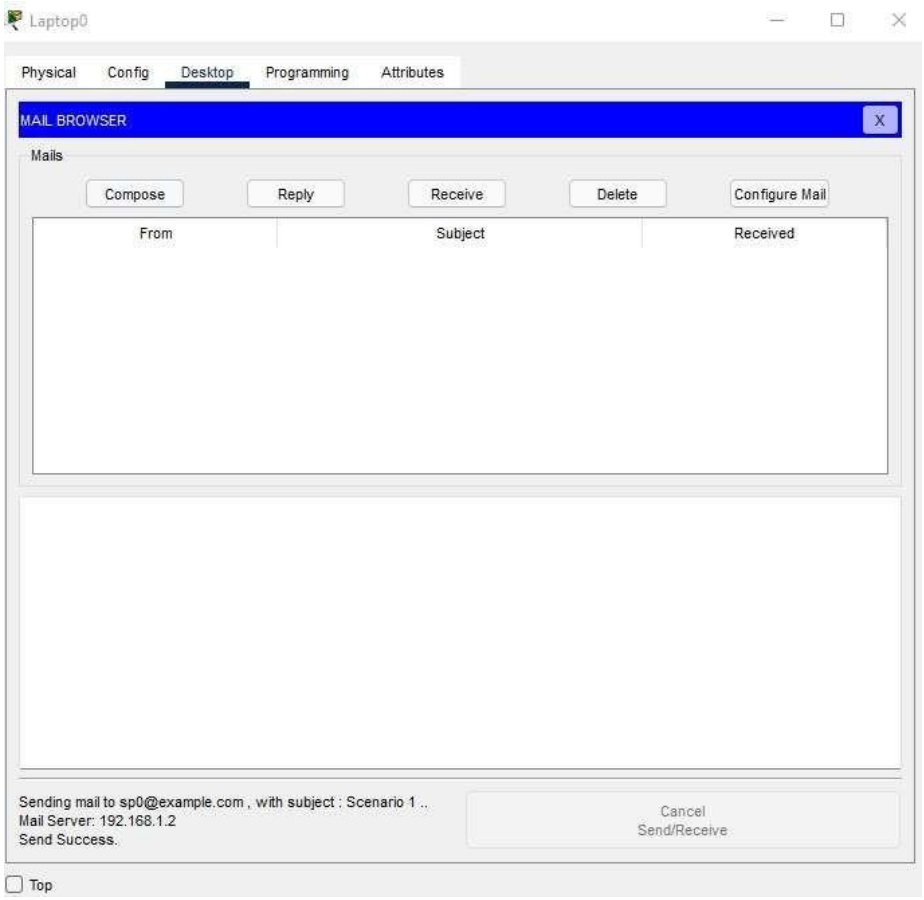
The structure of this system had been given by the pictures above (inside chapter 2.5)

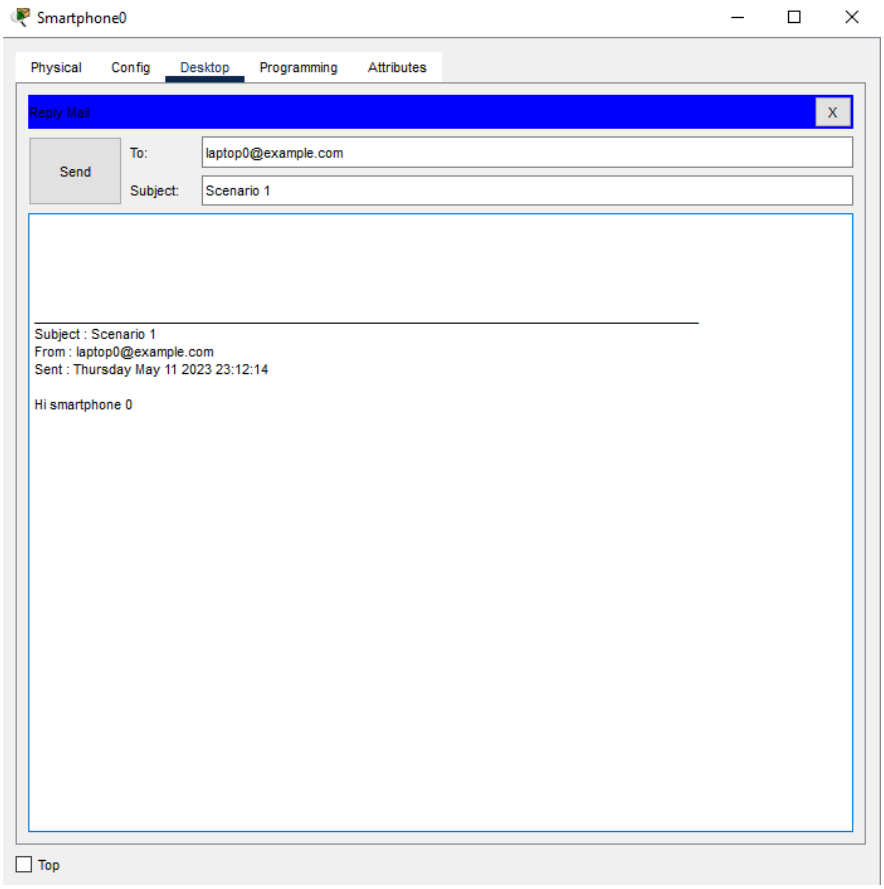
3. Simulation Elements

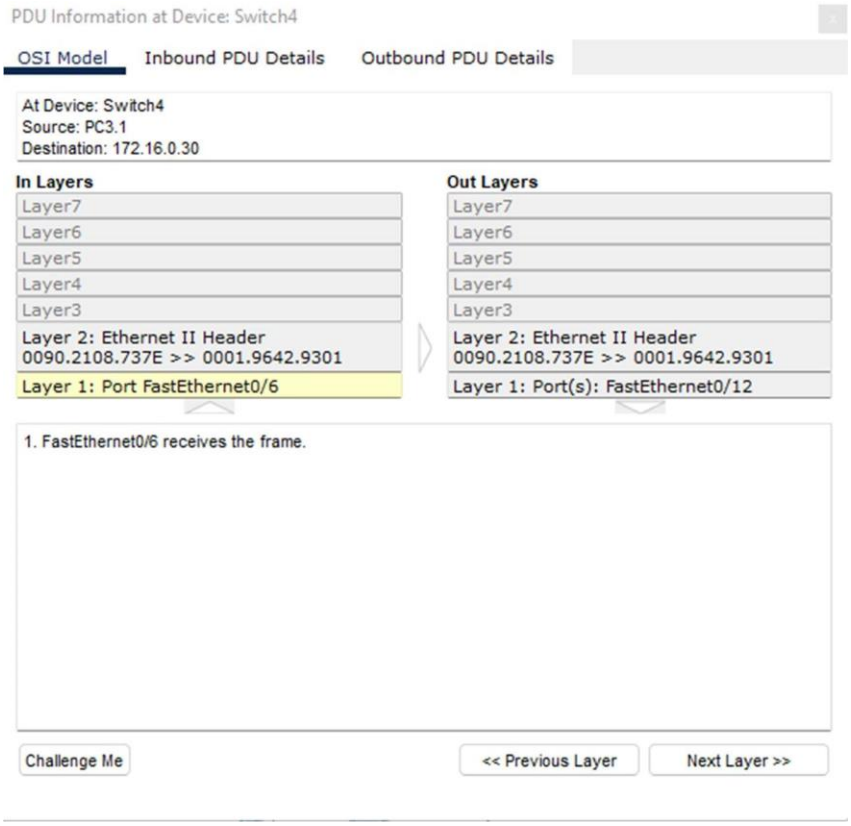
3.1. Traffic Analysis and Simulation Results

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



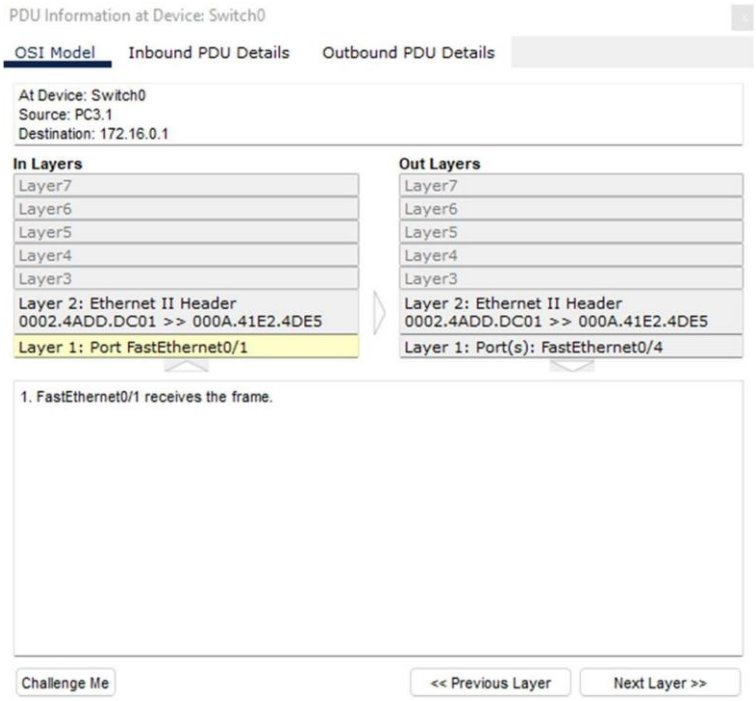

Laptop0
Physical
Config
Desktop
Programming
Attributes
MAIL BROWSER
X
Mails
Compose
Reply
Receive
Delete
Configure Mail
From
Subject
Received
Sending mail to sp0@example.com , with subject : Scenario 1 ..
Mail Server: 192.168.1.2
Send Success.
Cancel
Send/Receive
Top


Smartphone0
Physical
Config
Desktop
Programming
Attributes
Reply Mail
X
Send
To:
laptop0@example.com
Subject:
Scenario 1
Subject : Scenario 1
From : laptop0@example.com
Sent : Thursday May 11 2023 23:12:14
Hi smartphone 0
Top



Event List

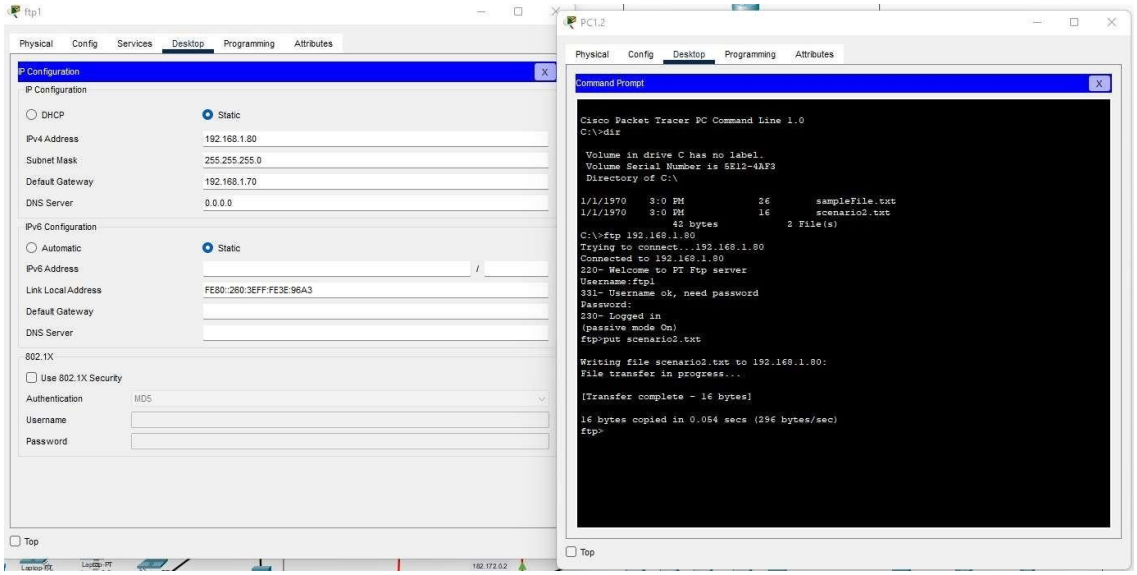
Vis.	Time(sec)	Last Device
	0.010	--
	0.011	PC3.1
	0.011	--
	0.012	PC3.1
	0.012	Switch4
	0.013	Switch4
	0.013	Router7
	0.014	Router7
	0.014	Router6
	0.015	Router6
	0.015	Switch0
	0.016	Switch0
	0.017	Mail server
	0.018	Switch0
	0.019	Router6
	0.020	Router7
	0.021	Switch4
	0.021	--
	0.022	PC3.1
	0.023	Switch4

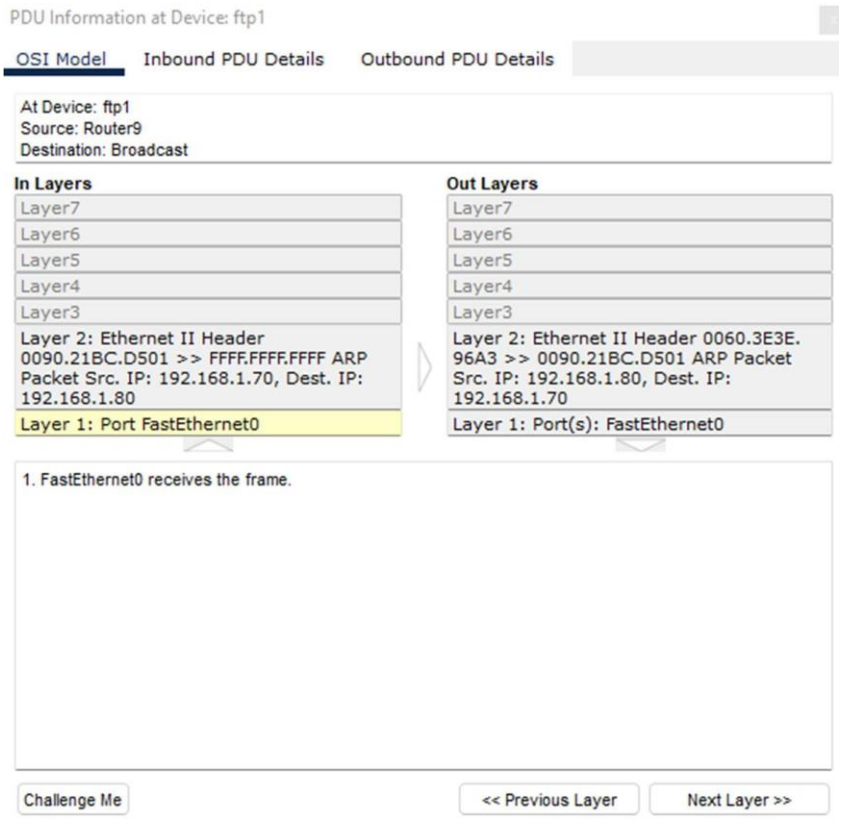


Event List

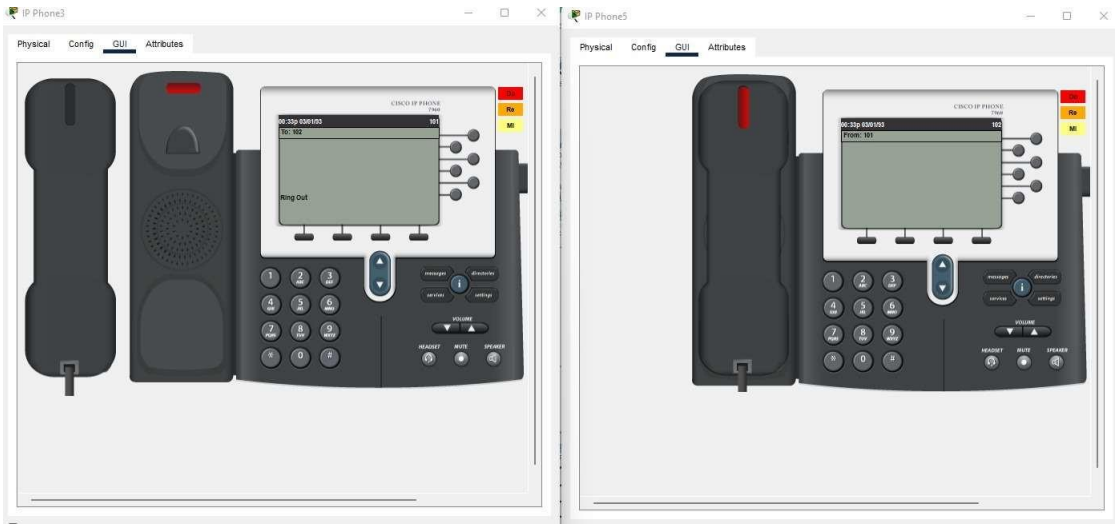
Vis.	Time(sec)	Last Device
	0.003	Access Point5
	0.003	Router7
	0.004	Switch4
	0.004	Router7
	0.004	Router6
	0.005	Router7
	0.005	Router6
	0.005	Switch0
	0.005	--
	0.006	Router6
	0.006	Switch0
	0.006	Web server
	0.006	--
	0.007	Switch0
	0.007	--
	0.007	Switch0
	0.007	Switch0
	0.007	Switch0
	0.007	Switch0
	0.007	--

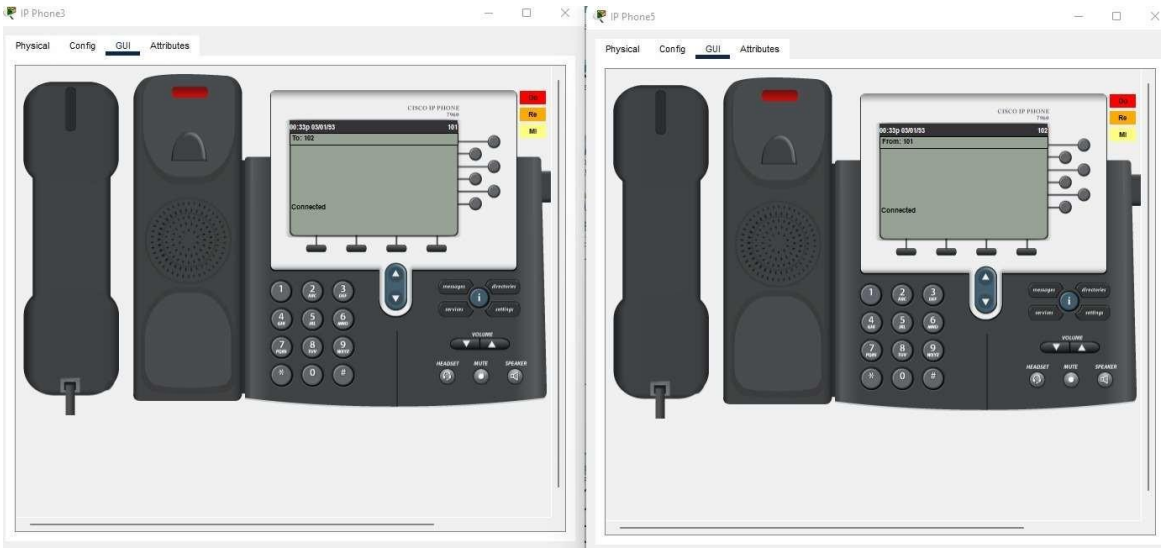
Scenario 2: A computer engineer from second facility of second branch developed a web application and wants to send his/her code files to FTP server in the third facility of first branch.

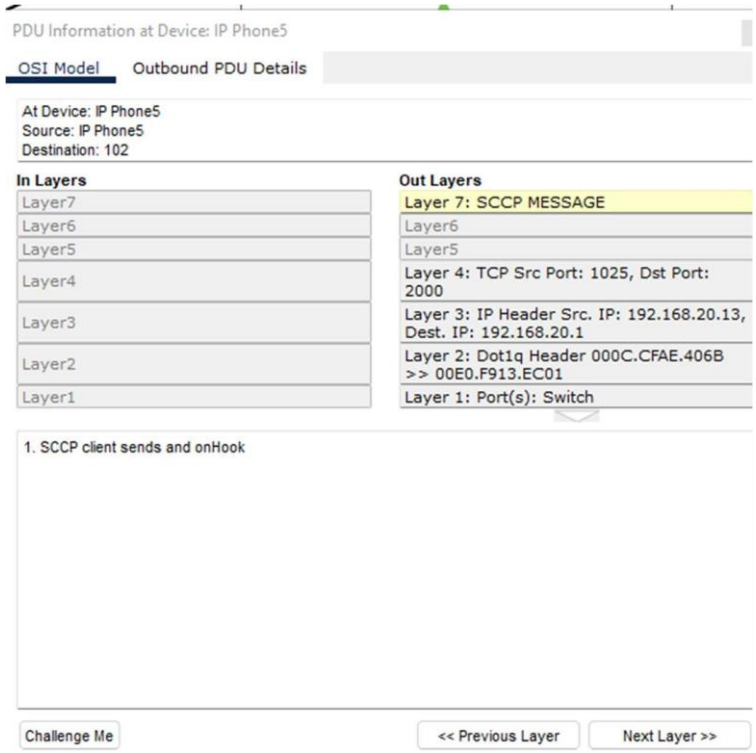


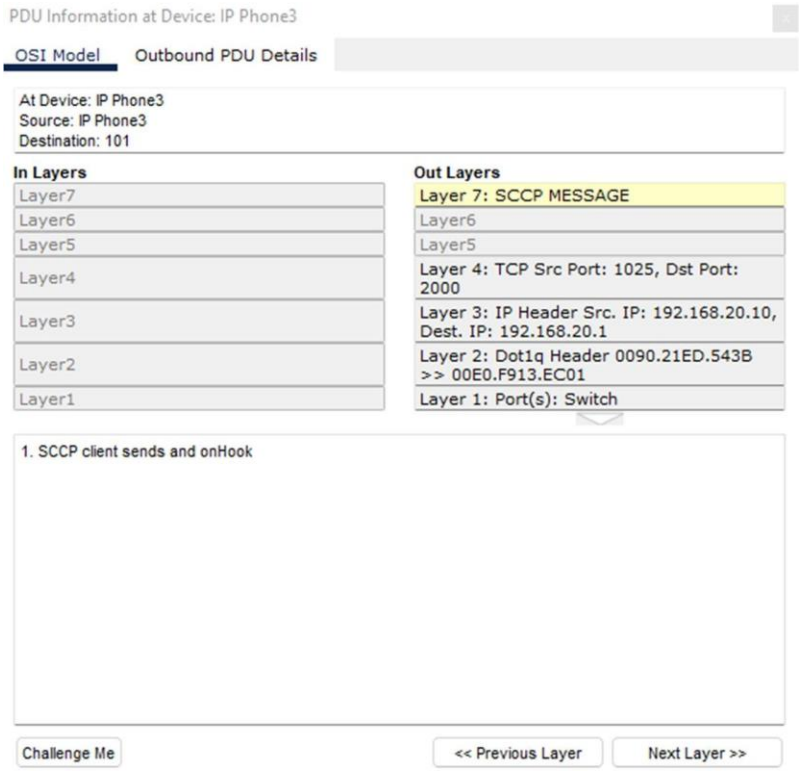


Scenario 3: Two users from second facility of first branch want to talk via VoIP.





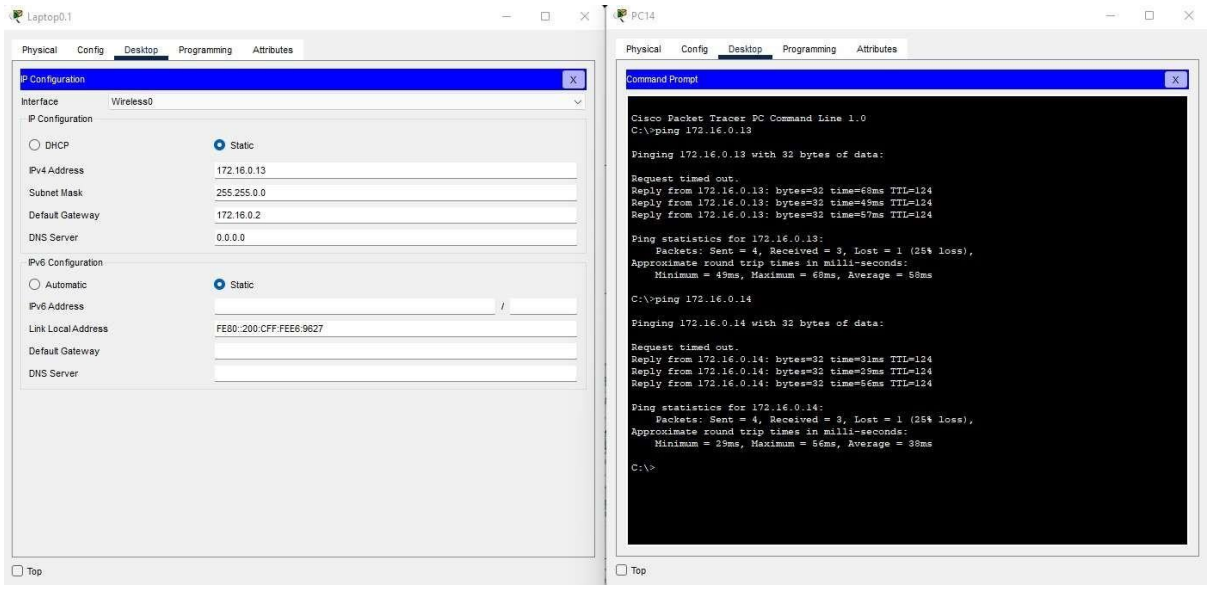

PDU Information at Device: IP Phone5
OSI Model
Outbound PDU Details
At Device: IP Phone5
Source: IP Phone5
Destination: 102
In Layers
Out Layers
Layer7
Layer 7: SCCP MESSAGE
Layer6
Layer6
Layer5
Layer5
Layer4
Layer 4: TCP Src Port: 1025, Dst Port: 2000
Layer3
Layer 3: IP Header Src. IP: 192.168.20.13, Dest. IP: 192.168.20.1
Layer2
Layer 2: Dot1q Header 000C.CFAE.406B >> 00E0.F913.EC01
Layer1
Layer 1: Port(s): Switch
1. SCCP client sends and onHook
Challenge Me
<< Previous Layer
Next Layer >>

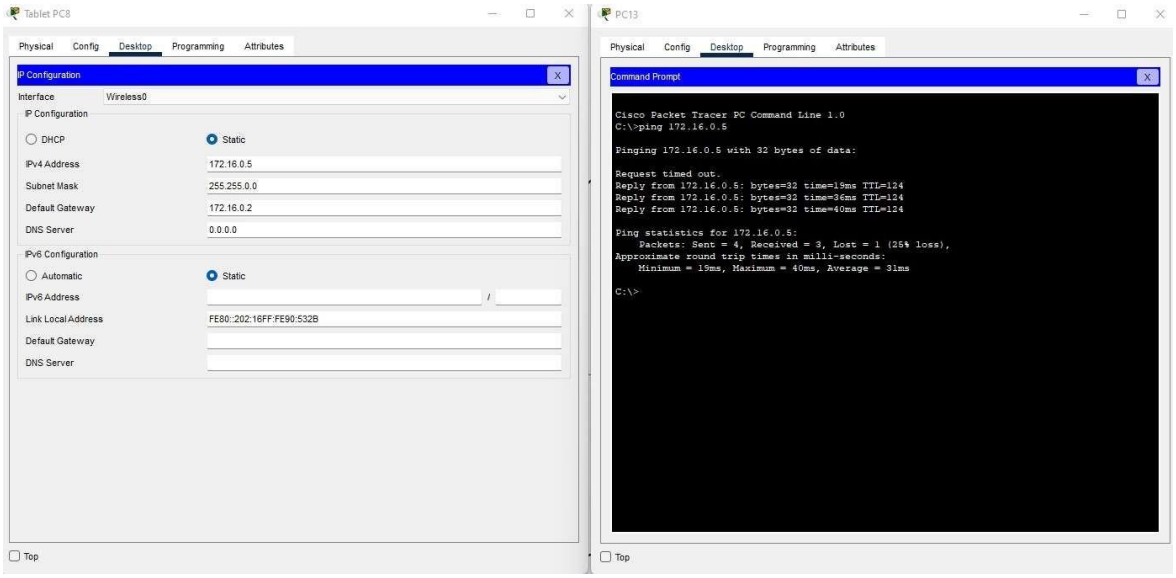

PDU Information at Device: IP Phone3
OSI Model
Outbound PDU Details
At Device: IP Phone3
Source: IP Phone3
Destination: 101
In Layers
Out Layers
Layer7
Layer 7: SCCP MESSAGE
Layer6
Layer6
Layer5
Layer5
Layer4
Layer 4: TCP Src Port: 1025, Dst Port: 2000
Layer3
Layer 3: IP Header Src. IP: 192.168.20.10, Dest. IP: 192.168.20.1
Layer2
Layer 2: Dot1q Header 0090.21ED.543B >> 00E0.F913.EC01
Layer1
Layer 1: Port(s): Switch
1. SCCP client sends and onHook
Challenge Me
<< Previous Layer
Next Layer >>

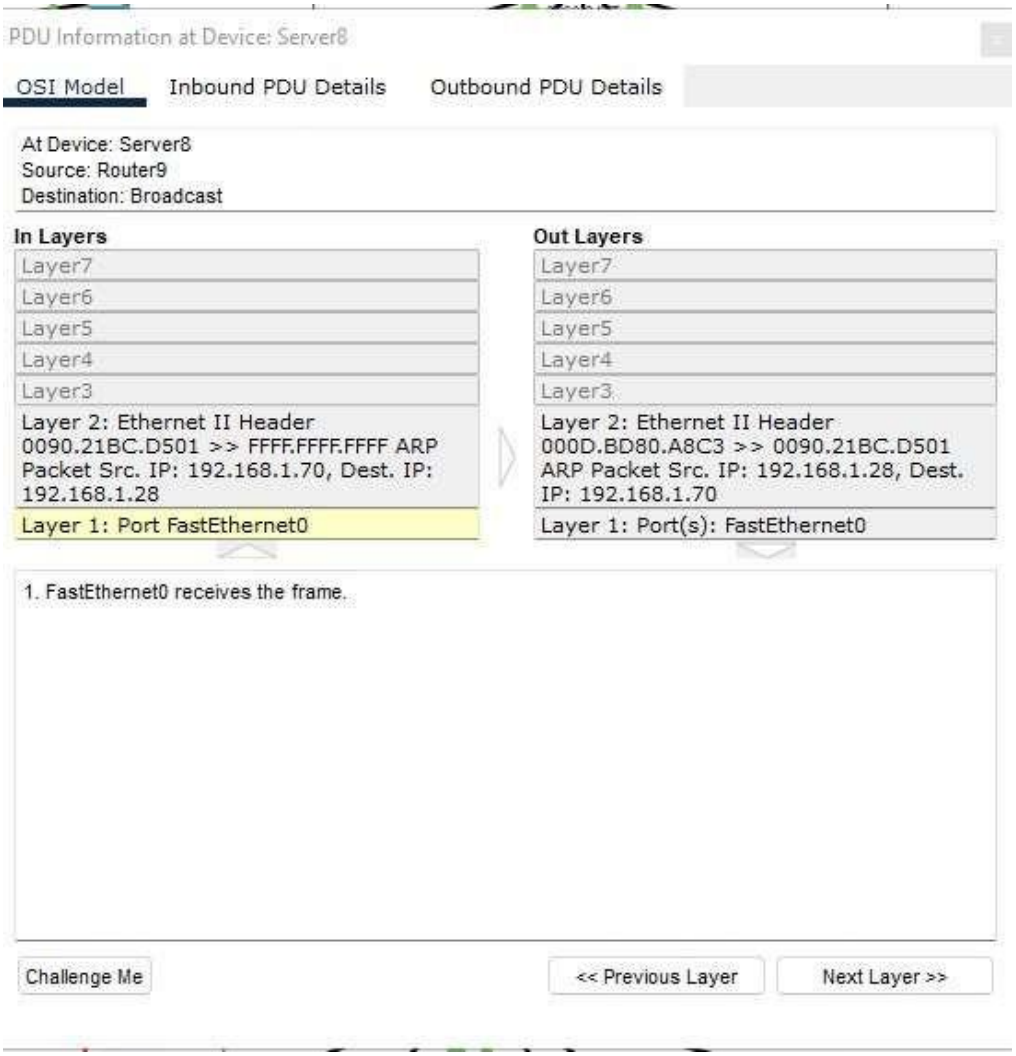
Scenario 4:

The second facility of the second branch is expected to receive e-mail. But the devices in this facility do not have this function according to the information in the project document. That's why this scenario was skipped while trying the others.

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

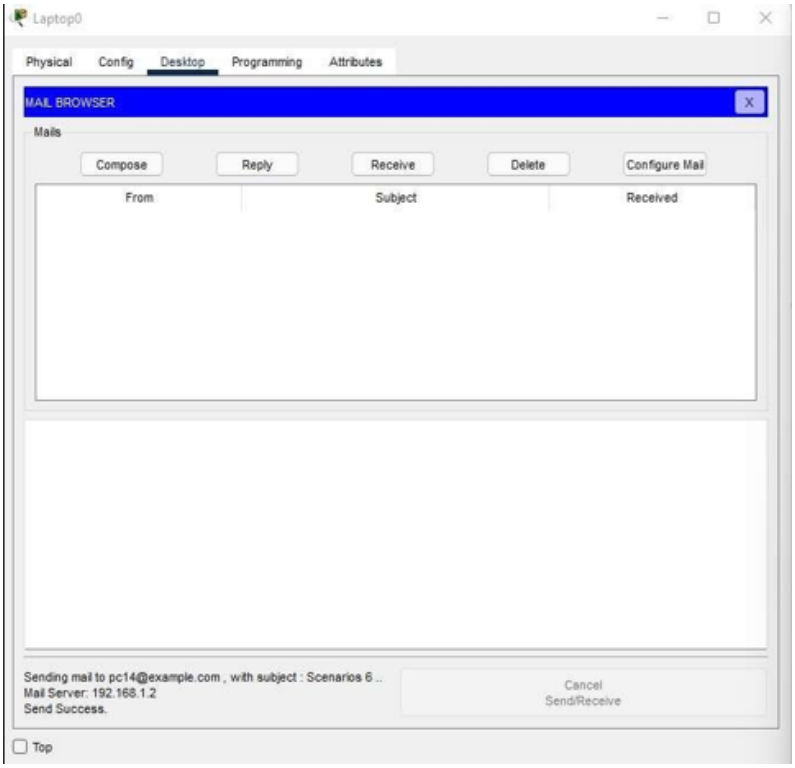


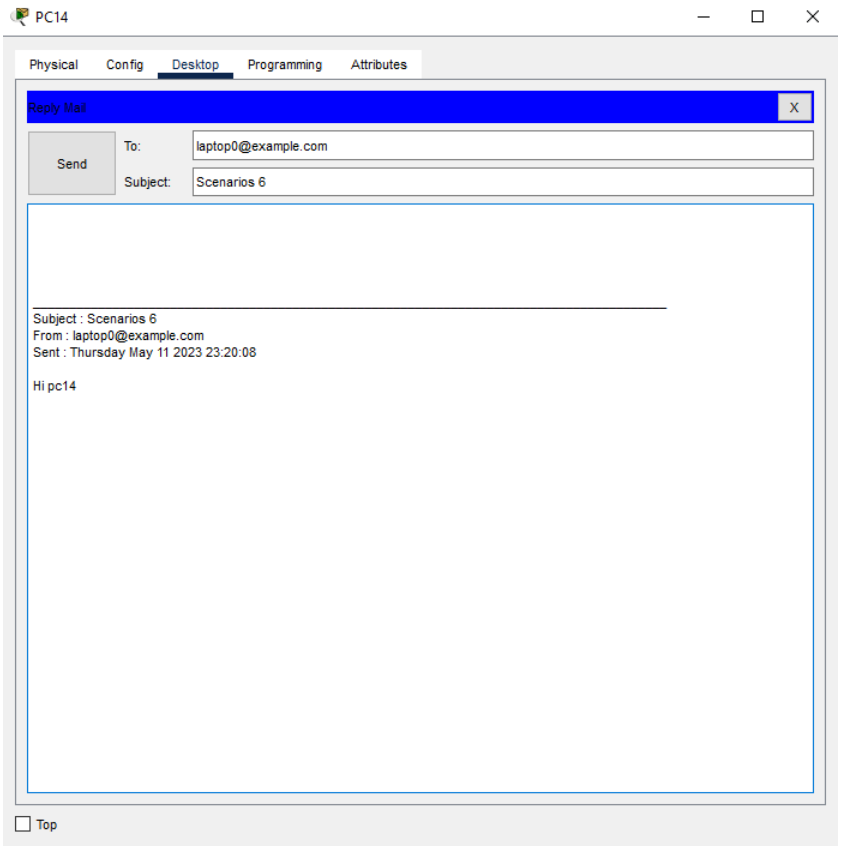


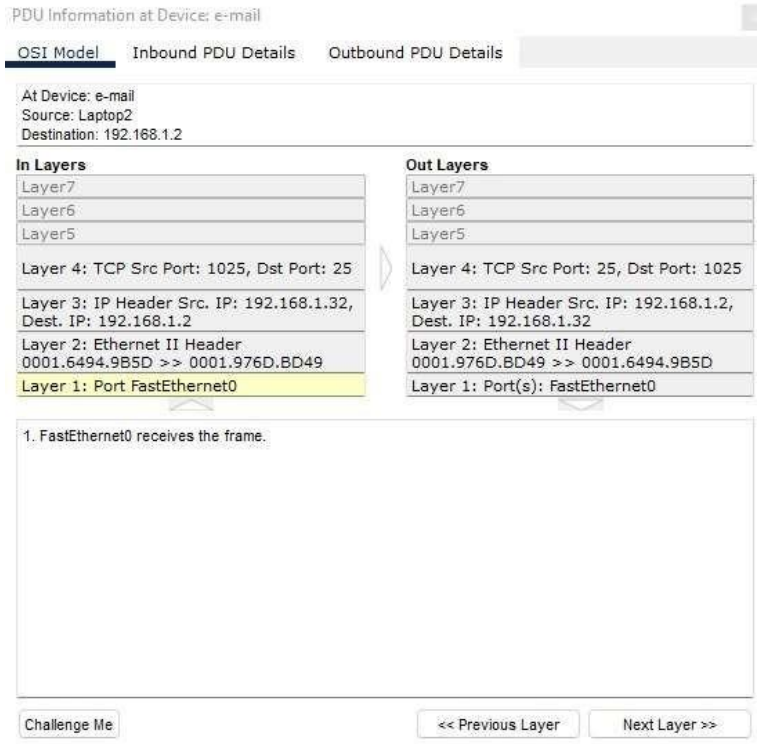


0.015	Tablet PC8	Access Point5	ICMP
0.016	Access Point5	Switch0	ICMP
0.017	Switch0	Router6	ICMP
0.018	Router6	Router7	ICMP
0.019	Router7	Router8	ICMP
0.019	--	Access Point5	ICMP
0.020	Access Point5	Tablet PC2	ICMP
0.020	Access Point5	Tablet PC3	ICMP
0.020	Access Point5	Tablet PC4	ICMP
0.020	Access Point5	Tablet PC5	ICMP
0.020	Access Point5	Tablet PC1	ICMP
0.020	Access Point5	Tablet PC9	ICMP
0.020	Access Point5	Tablet PC7	ICMP
0.020	Access Point5	Tablet PC6	ICMP
0.020	Access Point5	Tablet PC8	ICMP
0.020	Access Point5	Tablet PC10	ICMP
0.020	Router8	Router9	ICMP
0.020	--	Router9	ARP
0.021	Router9	Switch3	ARP
0.022	Switch3	ftp1	ARP
0.022	Switch3	ftp2	ARP
0.022	Switch3	e-mail	ARP

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.






PDU Information at Device: e-mail
OSI Model
Inbound PDU Details
Outbound PDU Details
At Device: e-mail
Source: Laptop2
Destination: 192.168.1.2
In Layers
Layer7
Layer6
Layer5
Layer 4: TCP Src Port: 1025, Dst Port: 25
Layer 3: IP Header Src. IP: 192.168.1.32, Dest. IP: 192.168.1.2
Layer 2: Ethernet II Header 0001.6494.9B5D >> 0001.976D.BD49
Layer 1: Port FastEthernet0
Out Layers
Layer7
Layer6
Layer5
Layer 4: TCP Src Port: 25, Dst Port: 1025
Layer 3: IP Header Src. IP: 192.168.1.2, Dest. IP: 192.168.1.32
Layer 2: Ethernet II Header 0001.976D.BD49 >> 0001.6494.9B5D
Layer 1: Port(s): FastEthernet0
1. FastEthernet0 receives the frame.
Challenge Me
<< Previous Layer
Next Layer >>

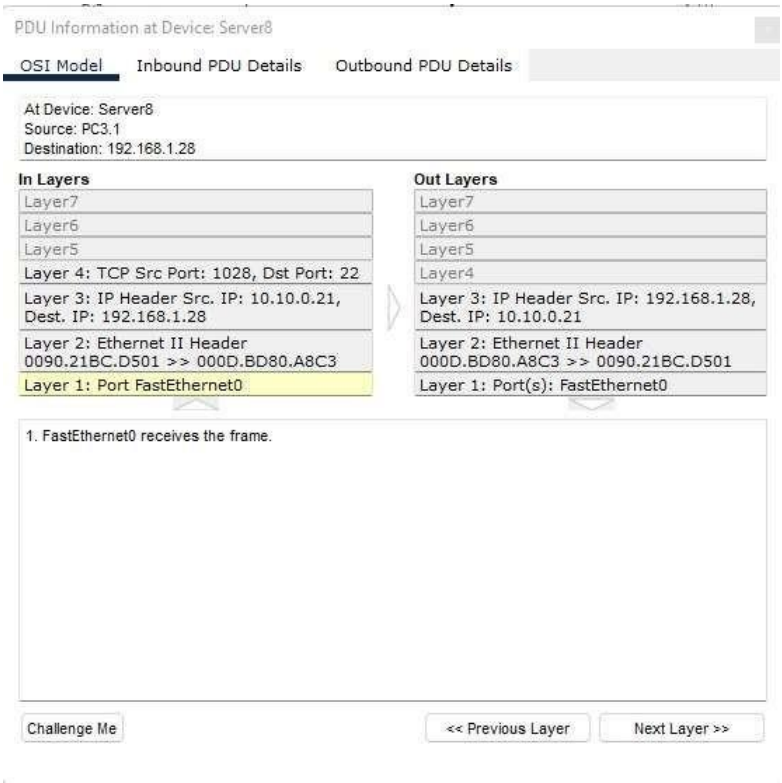
	0.057	Access Point0	Laptop1	ARP
	0.057	Access Point0	Laptop0	ARP
	0.057	Access Point0	Switch3	TCP
	0.057	Access Point0	Laptop2	ARP
	0.058	Switch3	e-mail	TCP
	0.059	e-mail	Switch3	TCP

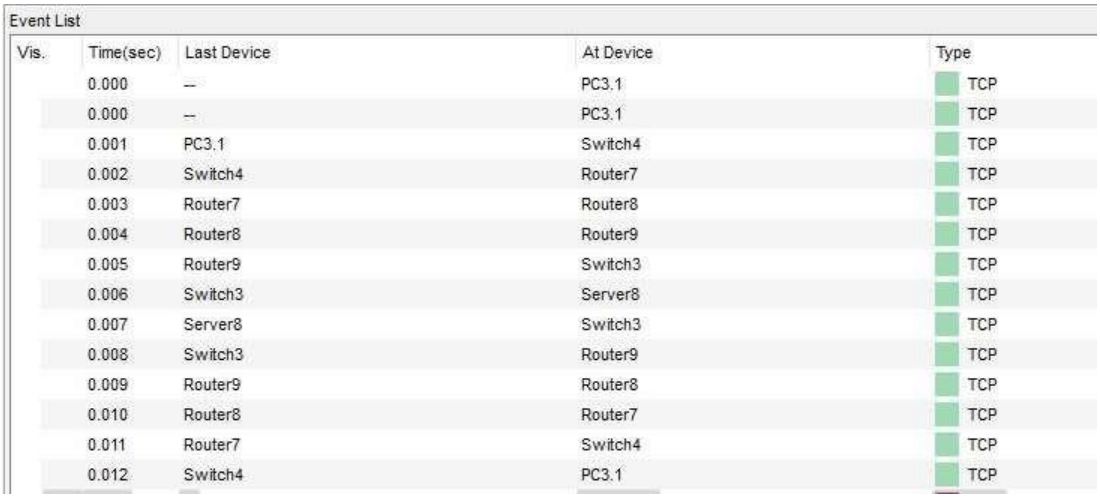
PC3:1

Physical Config Desktop Programming Attributes

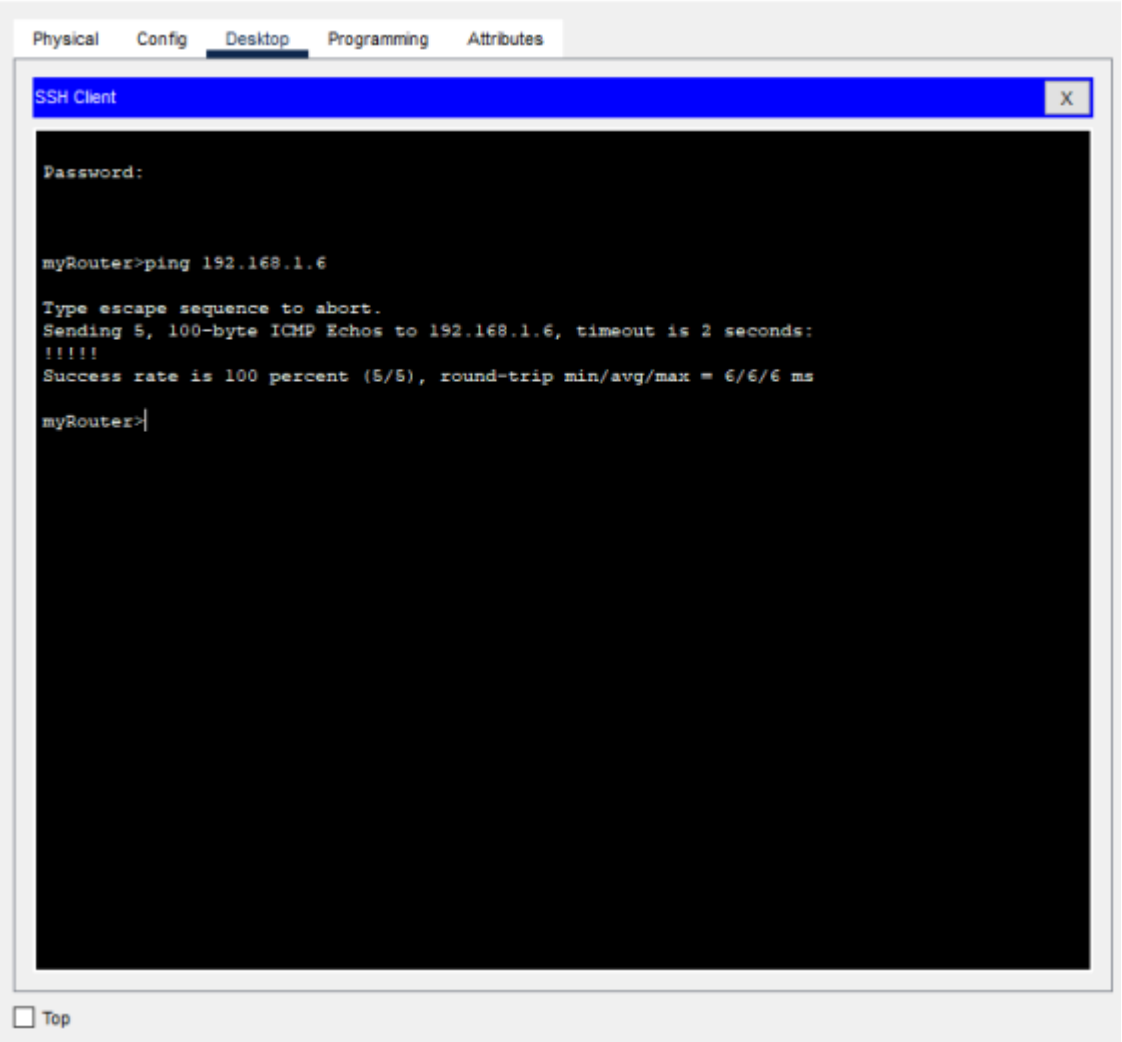
Command Prompt

```
% Login invalid

[Connection to 10.10.0.20 closed by foreign host]
C:\>co
Invalid Command.

C:\>ping 192.168.1.28

Pinging 192.168.1.28 with 32 bytes of data:

Reply from 192.168.1.28: bytes=32 time=2ms TTL=125
Reply from 192.168.1.28: bytes=32 time=10ms TTL=125
Reply from 192.168.1.28: bytes=32 time=5ms TTL=125
Reply from 192.168.1.28: bytes=32 time=4ms TTL=125

Ping statistics for 192.168.1.28:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 10ms, Average = 5ms

C:\>ssh -l admin 192.168.1.28

% Connection refused by remote host
C:\>SSH -l admin 10.10.0.20

Password:



R1>ping 192.168.1.28

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.28, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/21/53 ms

R1>
```



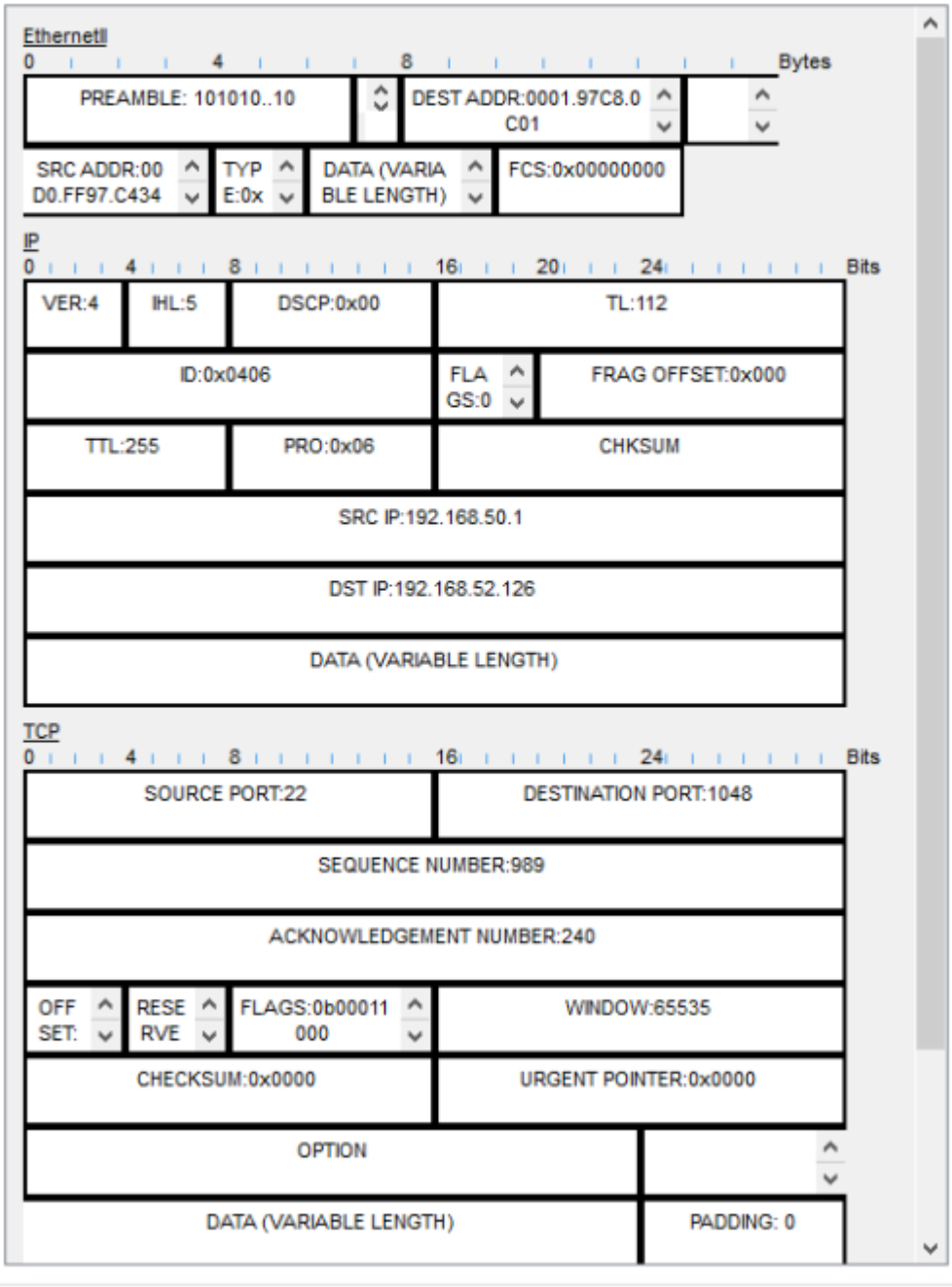


Scenario 7: A smartphone user from third facility of second branch office wants to use ssh to connect to a Web server in the third facility of first branch office.


Physical
Config
Desktop
Programming
Attributes
SSH Client
X
Password:
myRouter>ping 192.168.1.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/6 ms
myRouter>
Top

OSI Model | Outbound PDU Details

PDU Formats



4. Conclusion

The design included all the project's specifications. Applying scenarios yields exact and accurate outcomes. The two branches and their amenities were made to operate in line with a Metropolitan Area Network, which is described in detail in the document.

The IP addresses of cellphones 1 and 2 from the first facility of the first branch are lost when the user closes and reopens the Cisco Packet Tracer program, which is a concern. It has to do with the Cisco Packet Tracer program and has nothing to do with the design.

5. References

[1] *Protocol Definition*. (2019, March 29). Protocol Definition. https://techterms.com/definition/protocol

[2] *Packet Definition*. (2018, May 31). Packet Definition. https://techterms.com/definition/packet

[3] *MAP (Internet Message Access Protocol) Definition*. (2011, June 25). IMAP (Internet Message Access Protocol) Definition. https://techterms.com/definition/imap

[4] POP3 (Post Office Protocol) Definition. "POP3 (Post Office Protocol) Definition," January 1, 2006. https://techterms.com/definition/pop3

[5] DNS (Domain Name System) Definition. "DNS (Domain Name System) Definition," August 30, 2014. https://techterms.com/definition/dns

[6] *Server Definition*. (2014, April 16). Server Definition. https://techterms.com/definition/server

[7] https://www.cloudflare.com/learning/network-layer/what-is-a-metropolitan-area-network/

[8] S., & complete profile, V. M. (n.d.). *DHCP FAILED APIPA IS USED*. DHCP FAILED APIPA IS USED. http://sharanitcomputer.blogspot.com/2015/12/dhcp-failed-apipa-is-used.html