DOKUZ EYLUL UNIVERSITY

ENGINEERING FACULTY

DEPARTMENT OF COMPUTER ENGINEERING

CME 3204

Data Communications and Computer Networks

Midterm Project

2024-2025 Spring

Metropolitan Area Network Simulation

By

Fatih Boz - 2022510106

Taha Furkan Cengiz - 2021510136

Melih Altın - 2021510004

IZMIR

23.05.2025

Table of Contents

1. Introduction

1.1. Project Definition and Problem Formulation

At the start, we took time to learn how to use the Cisco Packet Tracer software by studying relevant training videos and running small experiments. These first exercises gave us a good idea about networking such as how to connect hardware, assign IP addresses to it, set up routers and switches and verify networking using special modes and command-line tools. After gaining the basic knowledge, we started working to build a practical Metropolitan Area Network (MAN) that links the branch offices in the city.

The first thing we did was build the internal network at First Branch, keeping our attention on First Facility. We faced the decision early on if DHCP should give out IP addresses to machines or if we would manually set them. After going over the pros and cons, we decided that at this facility, static IPs make more sense. This selection helped us handle IPs more easily and kept the connection process the same across all branches or with centralized servers.

After that, we focused on the Third Facility within the First Branch that features a server farm. As this phase of the project, we set up and adjusted various servers: 10 Web servers, 4 FTP servers, a DNS server, a mail server and a DHCP server. We looked at how servers communicated with each other and confirmed that devices in the test facility could reach the services. We used static IPs on each server because this matches how enterprises often need their servers to be stable and be accessed directly from a fixed address. Nevertheless, for end-user devices we plan to support DHCP where needed and where there will be big numbers of wireless or mobile devices, although these plans have not yet moved beyond setting.

We looked at VoIP and DNS in the second part of the First Branch. We first encountered challenges in talking to each other inside the company.. We understood that VoIP configuration is different the rest of them so in many attempts in command prompt we achieved to make communicate phones with each other inside the facility.

At this point, we also started building the link between the branches and the ISP and began to plan the modems and port setups. We tied the DSL modem to the testing server and tested each port to find the best configuration. Our results showed that FastEthernet ports, allowed up to 100 Mbps, gave us the most stable and compatible connection. Since our simulation could perform well with 100 Mbps, we chose to use FastEthernet ports for all interconnections among each facility and with the ISP.

The ISP was used to connect the third facility of the First Branch to itself and then we linked the Second Branch’s corresponding facility by making a connection through the ISP. Early on, we found that authentication and DNS synchronization between the different locations were connecting us. In order to fix this, we made changes to the DNS and gave some devices new IP addresses rather than their original static ones.

In order for the First Branch to successfully send and receive emails and connect to internal servers, we reconfigured DNS settings, checked IP assignments, and ensured each branch was properly connected to the modems, so ISP. We then mirrored this setup on the Second Branch by reassigning IPs, adding appropriate ports to the routers, and aligning the routing settings with the updated LANs and ISP structure. We tested inter-branch communication, file transfers, and email operations to ensure everything was functioning as expected.

While testing the VoIP functionality again, we noticed issues when trying to connect to the outside world and the ISP. We reviewed the gateway and settings of VoIP devices, discussed how they should be adjusted to allow VoIP to communicate both internally and externally, and implemented the necessary changes. These adjustments resolved the issue, allowing VoIP calls to function properly and connect through the ISP. Throughout the project, we took notes on key configurations such as IP schemes, routing setups, and server connections, which helped us debug and fine-tune the network design efficiently.

In summary, this project helped us understand the process of designing a real-world MAN network from the ground up. It involved configuring internal LANs, setting up and testing servers, and troubleshooting various communication challenges. We gained practical experience with both hardware configurations and logical networking concepts, laying a solid foundation for future work in network administration and design.

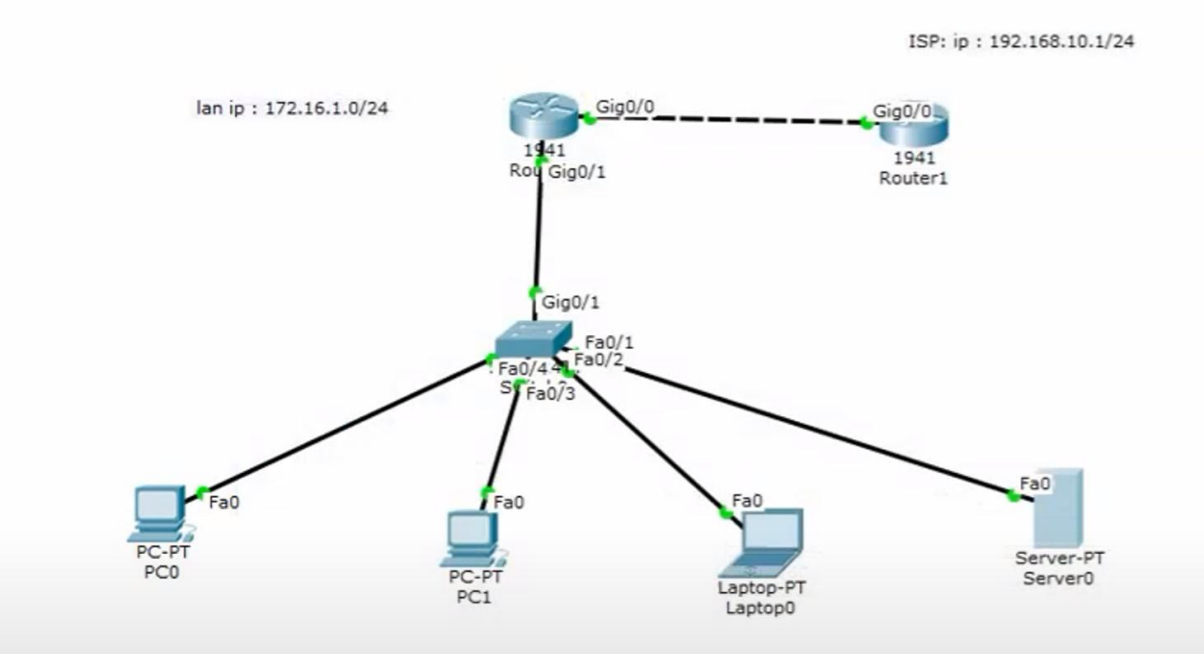
1.2. The purpose and motivation of the project

This project aims to come up with a detailed design and simulation of a Metropolitan Area Network (MAN) that supports the communication and connectivity of two branch offices in a city that are not close to each other. With Cisco Packet Tracer, we plan to simulate a reliable and efficient network solution to handle all the application and user needs in each branch.

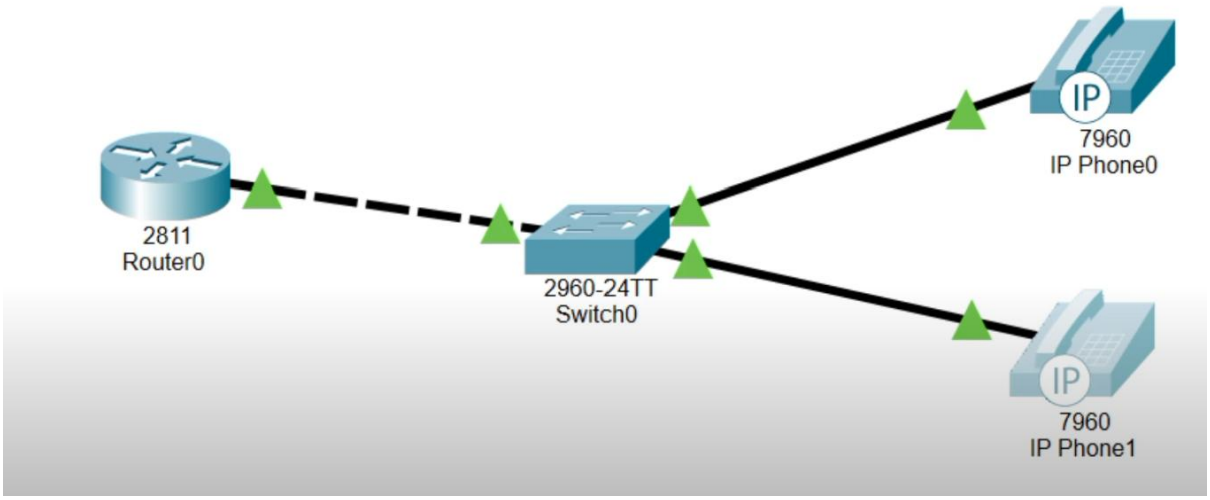
We chose to focus on this project because of how vital dependable and capable network infrastructure is to the success and efficient running of companies now. As digital communication and data-heavy apps become essential for businesses, well-designed and scalable networks have become more urgent. With this project, we are taught how to apply what we learn about networking in real-life, learning what is needed to design and set up these networks. Simulation also allows us to check and confirm our designs safely, optimizing performance and keeping problems to a minimum before anything goes live. Using network simulation tools such as Cisco Packet Tracer directly helps individuals build the important skills required in network engineering and management.

1.3. Related Work

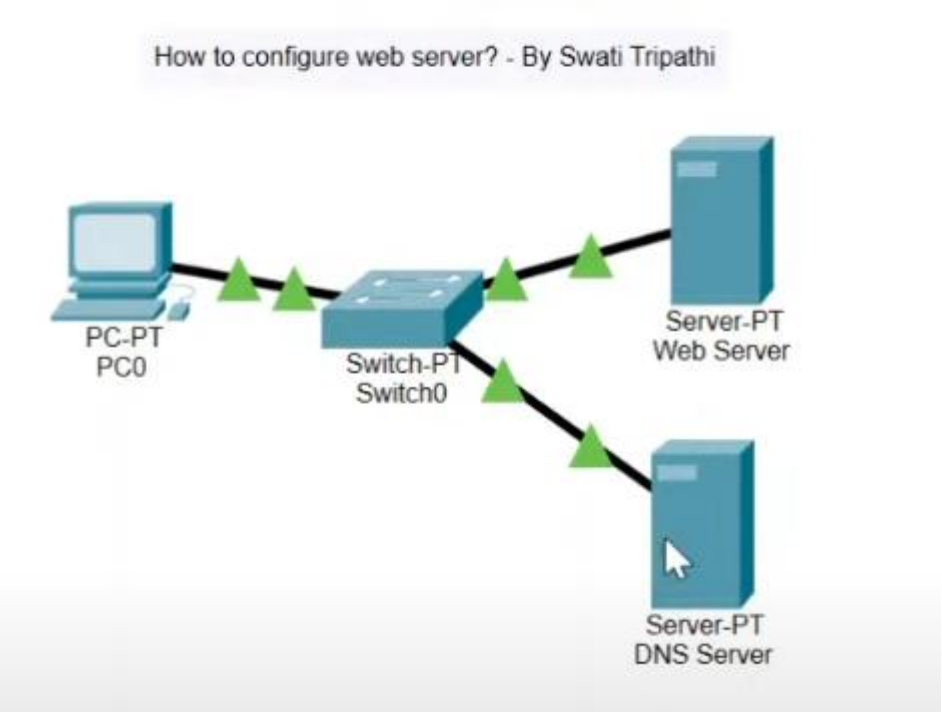
[1] ISP Router Configuration Reference



[2] VoIP Configuration Reference



[3] Configuration of Web Server Reference



2. Method and Simulation

2.1. Simulation and Modeling Concepts

The first branch's initial facility saw devices chosen and the wiring for cabled devices and the SSID setup for wireless connections were completed through access points. All of the devices were given the required IP addresses and subnet masks. A server farm was put into place at the Third Facility, so the hardware could perform its expected duties for HTTP, DNS, email, FTP, DHCP and others. The designated functions were possible because the router joined the devices in the First Facility to the servers. Just as with the First Facility, the Second Facility had telephones that used a computer for VoIP through a router. Switches of attached devices in these three facilities were tied to the main router, so packets could be routed successfully using IP-Routing.

The jobs in the first branch were repeated for the second branch. Steps were taken to check that routing between the main router in our branch and the router in the first branch was working correctly. The objective was met by modifying IP-Routing settings on the principal routers.

For the simulation, the ping method was used to examine how devices were connected within the branch over the network. Various simulations were carried out using web servers, emails, VoIP calls, FTP file moving and so on.

2.2. Simulation Environment/Tool

The project carried out all its simulations using Cisco Packet Tracer. 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 any router, switch, modem, computer, telephone etc. It also allows you to make changes in the settings of these tools. With Packet Tracer, users may experience meaningful simulation, clear visuals, advanced assessment support, powerful activity creation and the ability to collaborate in a community. With Cisco Packet Tracer, learning and teaching is made much simpler thanks to support for groups working together and a realistic environment to explore and test ideas.

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

The first facility has 3 workstation (PC) users, 3 wireless (laptop) users, and 3 smartphone users. All of the users in this facility can browse the web, send e-mails, and transfer files using their devices.

Facility Overview and User Requirements

The First Facility of the First Branch is designed to support a total of **9 users**, which include:

- **3 Workstation (PC) users**
- **3 Wireless (Laptop) users**
- **3 Smartphone users**

All users in this facility are required to perform basic network activities such as:

- Web browsing (HTTP/HTTPS)
- Email communication (SMTP/IMAP)
- File transfer (FTP or file sharing across LAN)

Network Architecture and Topology

The network architecture for this facility follows a **hybrid topology**, combining **wired** and **wireless** components connected to a central switch and wireless access point. This design allows flexibility for different types of users while maintaining performance and manageability.

Topology Components:

- **1 Router** (Cisco 1941)
- **1 Switch** (Cisco 2960)
- **1 Wireless Router or Access Point** (Linksys or Cisco WAP)
- **3 Desktop PCs** (wired)
- **3 Laptops** (wireless)
- **3 Smartphones** (wireless)
- **1 DSL Modem** (connected to simulate external ISP link)

Interconnection and Physical Design:

- The **DSL Modem** connects to the **Router** using a **FastEthernet port** (since we found FastEthernet sufficient for simulation and compatible with our router model).
- The **Router** connects to the **Switch** using another FastEthernet port.
- All **wired desktop PCs** are connected to the **Switch** via FastEthernet cables.
- The **Wireless Access Point** connects to the **Switch** to provide wireless coverage to laptops and smartphones.
- Wireless devices are configured to connect to a **WPA2-secured SSID**, ensuring network security.

2.3.2 Second Facility of First Branch

The second facility has 6 workstation users who can access the Web and FTP. Two of the workstations are used for VoIP conference events.

Facility Overview and User Requirements

The Second Facility of the First Branch is designed to support **6 workstation users** with the following capabilities:

- All users can access **Web services** (HTTP/HTTPS) and **FTP servers** for downloading and uploading files.

- Out of the 6 users, **2 workstations** are also configured for **VoIP (Voice over IP)** communication to participate in conference events within the facility and potentially with other parts of the network.

This setup required us to design both a data and a voice network within the same physical infrastructure, which added complexity but also provided an opportunity to implement VLANs and IP telephony.

Network Architecture and Topology

The network for this facility uses a **star topology**, with all devices connected to a central switch. A router connects the facility to the rest of the First Branch and the ISP. The design ensures scalability and centralized management.

Topology Components:

- **1 Router**

- **1 Switch**

- **6 Desktop PCs**

- **2 IP Phones**

Note: The 2 PCs used for VoIP are connected **through IP phones**, meaning that each phone sits between the switch and the PC, enabling voice and data traffic to share the same port using different VLANs.

Interconnection and Physical Design:

- The **Router** is connected to the **Switch** via **FastEthernet.**

- **6 PCs** are connected to the switch via Ethernet cables.

- **2 of the PCs** are connected **through IP Phones**, which are in turn connected to the switch. These phones are configured with **voice VLANs**.

Testing and Troubleshooting

We tested the following to verify functionality:

- **Web and FTP Access:** All PCs successfully accessed the web and transferred files to/from FTP servers.
- **VoIP Calling:** Phones were configured to call each other internally using their extension numbers. We verified call connectivity.
- **Ping and Traceroute:** Used to test routing across VLANs and to ISP.
- **Connectivity with the First and Third Facility:** Verified that data VLAN devices could reach DNS and FTP servers in the third facility.

2.3.3 Thirth Facility of First Branch

The third facility has a server farm that includes 10 Web servers, 4 FTP servers, 1 DHCP server, 1 mail server, and 1 domain name server (DNS).

Facility Overview and Purpose

The **Third Facility** of the First Branch serves as the **central server farm** for the entire Metropolitan Area Network (MAN). This facility hosts all the critical services required for the network to operate efficiently. These include:

- **10 Web Servers** – Hosting internal and external websites
- **4 FTP Servers** – Handling file uploads and downloads
- **1 DHCP Server** – Distributing IP addresses dynamically to client devices in other facilities
- **1 Mail Server** – Managing internal and external email communication
- **1 DNS Server** – Resolving domain names to IP addresses for all users in the network

This facility is vital for supporting core business operations, user access to online services, and inter-branch communications.

Network Architecture and Topology

This facility is designed as a **centralized server network** using a **hierarchical topology**. All servers are connected to a **switch**, which is then connected to the branch **router**. The router provides connectivity to other branch and the ISP.

Topology Components:

- **1 Router**
- **1 Switch**
- **10 Web Servers**
- **4 FTP Servers**
- **1 DHCP Server**
- **1 Mail Server**
- **1 DNS Server**
- **1 DSL Modem**

Total of **17 servers** directly connected to the switch.

The **Switch** used the default VLAN for simplicity, as all servers are within the same subnet and broadcast domain.

Server Configuration Details

Each server was configured manually in Packet Tracer:

- **Web Servers:**
    - HTTP and HTTPS services enabled
    - Different websites hosted for load balancing simulation
- **FTP Servers:**
    - FTP service enabled
    - Credentials and directories created for testing file transfers
- **Mail Server:**
    - SMTP and POP3 services enabled

    - Test email accounts created

- **DNS Server:**
    - Hostnames mapped to all critical servers and test devices
    - DNS entries tested with web and mail clients

Interconnectivity and Testing

We conducted several test scenarios to ensure everything worked as expected:

- **Web Access:** From First and Second Facility to each of the 10 web servers using browser tool and DNS resolution
- **FTP Transfer:** Uploading and downloading files from FTP clients on workstations
- **Email Testing:** Emails sent between users across both branches using the Mail Server
- **DNS Lookup:** Tested domain resolution using the simulated DNS client tool

2.3.4 First Facility of Second Branch

The first facility has 5 workstation users, 5 wireless users, and 5 tablet users. These users can connect to the Internet using wireless connections, browse the Web, and use e-mail applications The first facility has 5 workstation users, 5 wireless users, and 5 tablet users. These users can connect to the Internet using wireless connections, browse the Web, and use email applications

Facility Overview and User Requirements

The **First Facility** of the **Second Branch** is designed to serve a total of **15 users**, broken down as follows:

- **5 Workstation (PC) users**
- **5 Wireless (Laptop) users**
- **5 Tablet users**

This facility primarily emphasizes **wireless connectivity**, making it essential to build a secure, stable, and high-performing wireless network infrastructure.

Network Architecture

The facility uses a **hybrid topology**, combining both wired and wireless connectivity. However, the **majority of devices rely on wireless access**, so most design and configuration efforts were focused on optimizing wireless performance and ensuring correct, DNS, and routing behavior.

Topology Components:

- **1 Router**
- **1 Switch**
- **1 Wireless Access Point**
- **5 PCs**
- **5 Laptops** (wireless)
- **5 Tablets** (wireless)

Interconnection and Physical Design

- The **DSL Modem** connects to the **Router** via FastEthernet.
- The **Router** is connected to the **Switch** via FastEthernet.
- The **Wireless Access Point** is connected to the switch and provides access to wireless devices.
- **Laptops and tablets** connect wirelessly via the access point.

Wireless signal coverage and bandwidth were considered to ensure stable access for all 10 wireless devices.

Wireless Device Settings:

- Devices were configured to connect to the access point using the correct SSID and WPA2 credentials.
- IP addresses were assigned statically.
- DNS settings verified through successful domain resolution using the DNS server from the Third Facility.

Testing and Verification

We tested several core functionalities to ensure the facility met all user requirements:

- **Web Browsing:** All devices successfully accessed external websites using DNS resolution
- **Email Communication:** Devices connected to the mail server in the third facility, and emails were sent/received
- **Connectivity:** Wireless connectivity was stable and secure with WPA2K encryption
- **Ping Tests:** Successful pings to external DNS, web servers, and mail servers verified proper routing

2.3.5 Second Facility of Second Branch

The second facility has 5 workstation users and 2 smartphone users. They can browse the web, edit applications, and transfer files.

Facility Overview and User Requirements

The **Second Facility** of the **Second Branch** supports a total of **7 users**, consisting of:

- **5 Workstation (PC) users**
- **2 Smartphone users**

These users are expected to perform the following tasks:

- **Browse the Web** (HTTP/HTTPS)
- **Transfer files** across the network or using FTP services

The facility has a mixed-use environment where **stable wired access for PCs** is required, and **wireless access for mobile devices** (smartphones) is essential. The network is designed to provide both secure and efficient access to internal resources (like FTP servers) and external internet services.

Network Architecture and Topology

The topology here is a **star topology** that includes both **wired and wireless segments**, connected through a central **switch** and a **router**. The facility is part of the larger Metropolitan Area Network (MAN).

Topology Components:

- **1 Router**
- **1 Switch**
- **1 Wireless Access Point**
- **5 PCs**
- **2 Smartphones** (wireless)

Interconnection and Physical Layout

- The **DSL Modem** connects to the **Router via FastEthernet.**
- The **Router** connects to the **Switch** for internal LAN distribution.
- **Wired PCs** are connected to the switch via Ethernet cables.
- **Smartphones** connect wirelessly through the Access Point.
- The **Access Point** is wired to the switch and configured with secure wireless settings (WPA2K).

This configuration ensures reliable internet access for all users and allows file transfer operations to and from the **FTP servers** located in the **Third Facility of the First Branch**.

Device and Functional Testing

We performed extensive testing for functionality and network performance:

- **PCs accessed FTP servers** using command-line FTP client tools and transferred test files.
- **Smartphones browsed internal and external web pages** using the Web Browser tool in Packet Tracer.
- **All devices successfully resolved DNS queries** and sent ICMP pings to test network reachability.
- We simulated **application editing** as cloud-based interaction via web browsers (e.g., document tools hosted on web servers in the Third Facility).

2.3.6 Thirth Facility of Second Branch

The third facility has 5 workstations, and 2 mobile devices used to browse the Web and send and receive emails

Facility Overview and User Requirements

The **Third Facility** of the **Second Branch** includes:

- **5 Workstation users**
- **2 Mobile device users** (wireless)

All users in this facility are expected to:

- **Browse the web** (HTTP/HTTPS)
- **Send and receive emails** (SMTP and POP3)

This is a relatively small user group, but it's critical that users experience **reliable connectivity**, **fast web access**, and **secure and consistent email communication**, especially from mobile devices.

Network Architecture and Topology

This facility uses a **hybrid network topology**, combining **wired and wireless segments**. All devices are interconnected through a central switch and router, with access to an ISP via a

DSL modem. The design supports secure wireless access for mobile users while maintaining robust Ethernet connections for the workstations.

Topology Components:

- **1 Router**
- **1 Switch**
- **1 Wireless Access Point**
- **5 Desktop PCs**
- **2 Smartphones** (wireless)
- **1 DSL Modem**

Physical and Logical Topology Design

- The **DSL Modem** connects to the **Router via Ethernet.**
- The **Router** connects to a **Switch**, which distributes the local network.
- **5 PCs** are connected directly to the switch using Ethernet cables.
- A **Wireless Access Point** is also connected to the switch to serve the 2 mobile devices.

This physical design ensures a **centralized, efficient star topology**, which simplifies future scalability or troubleshooting.

Testing and Verification

We performed a full suite of connectivity and service tests:

- **Web Browsing:** Verified that all 7 devices could access external websites.
- **Email Access:** Smartphones and PCs successfully sent and received emails using the internal Mail Server.
- **Ping Tests:** Validated reachability to the DNS and Mail servers from all devices.

- **Security Checks:** Verified WPA2 encryption on wireless access.

2.4. Requirement Analysis

Before beginning the design and implementation of the Metropolitan Area Network (MAN) in Cisco Packet Tracer, we conducted a thorough analysis of the system requirements. This section outlines the **functional requirements**, **performance expectations**, and **constraints** that influenced our design decisions across all facilities and branches.

2.4.1 Functional Requirements

The functional requirements define the core services and applications that the network must support for each facility. These are directly derived from user needs and operational goals across the two branch offices.

- **Internet Connectivity:** All users in every facility must be able to access the internet reliably for general browsing and communication purposes.
- **Web Access:** Every device (wired or wireless) across the network must be able to connect to internal and external web servers through HTTP and HTTPS.
- **Email Services:** Email communication must be supported by connecting users to an internal Mail Server using SMTP and POP3.
- **FTP File Transfer:** Facilities with workstation users require FTP services for put and get files to/from the FTP servers.
- **VoIP Communication:** VoIP must be supported for two dedicated workstations in the First Branch – Second Facility to allow voice calls and conferencing.
- **Wireless Access:** Wireless connectivity is required in most facilities (especially where laptops, tablets, and smartphones are used) and must be secured with encryption (WPA2K).
- **DHCP Services:** DHCP must be used to assign IP addresses automatically to user devices in most facilities, (if want to) while servers must have static IP addresses.
- **Name Resolution:** DNS services must be available across the entire network for domain name resolution, allowing users to connect to web services by hostname rather than IP.

2.4.2 Performance Requirements

The performance requirements were identified based on the expected number of users and the types of applications being used:

- **User Support:** The network must support approximately 50+ devices, including:
    - 19 Workstation PCs
    - 13 Wireless Laptops
    - 7 Smartphones
    - 5 Tablets
    - 17 Servers
- **Network Speed:** The network must support a minimum of **100 Mbps** per wired connection using FastEthernet. **GigabitEthernet** was not used, but FastEthernet provides sufficient bandwidth for browsing, file transfer, and VoIP communication.
- **Latency and Reliability:** VoIP communication requires low-latency, reliable links, which influenced our use of direct router-to-router serial connections and VLAN-aware routing.
- **Server Response:** The central server facility (First Branch – Facility 3) must handle concurrent access from both branches without performance degradation.
- **Wireless Capacity:** Wireless Access Points must support simultaneous connectivity for up to 5–10 devices per facility with secure and stable performance.

2.5. Definition of the System/Model

2.5.1 Structure of the System

Each facility structured as a star topology, with a switch at the center and devices connected to it.

2.5.2 Hypotheses on Input Parameters

Bandwidth: The network is designed to support typical office bandwidth requirements.

Latency: Internal latency is minimal; however, latency between branches could vary.

Traffic: Expected to have a mix of web, email, FTP, and VoIP traffic.

2.5.3 Specifications

Network Applications/Services: HTTP (web services), DNS, email, FTP, DHCP for dynamic addressing, and VoIP services.

Network Configuration:

Addressing: Used private IP address ranges with subnetting to separate network segments.

Routing: Static or dynamic routing with proper route summarization to ensure efficient traffic management between branches.

Equipment Configuration: Routers and switches configured with VLANs, QoS for VoIP, and security features (ACLs, firewall rules).

Data Types/Sources: Data originating from user activities, servers, and external internet sources.

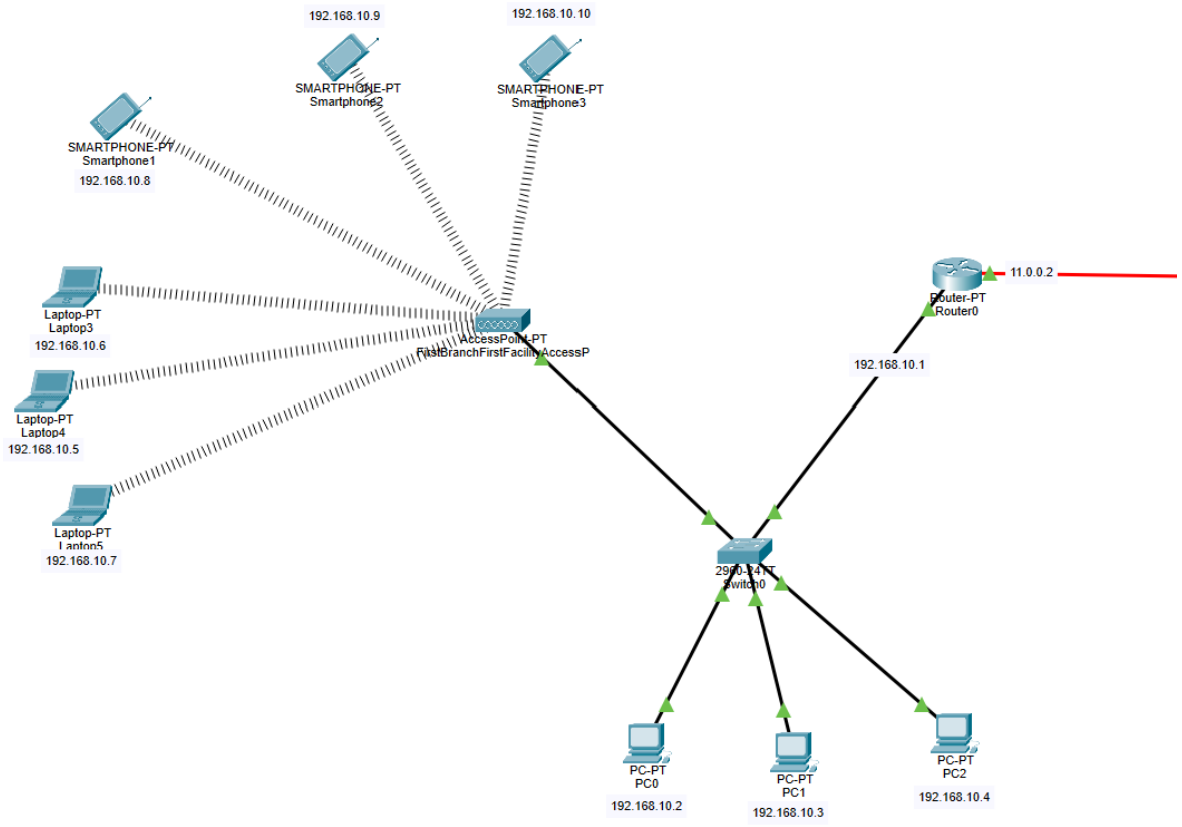
Device Types:

Hosts: Computers and servers providing and consuming network services.

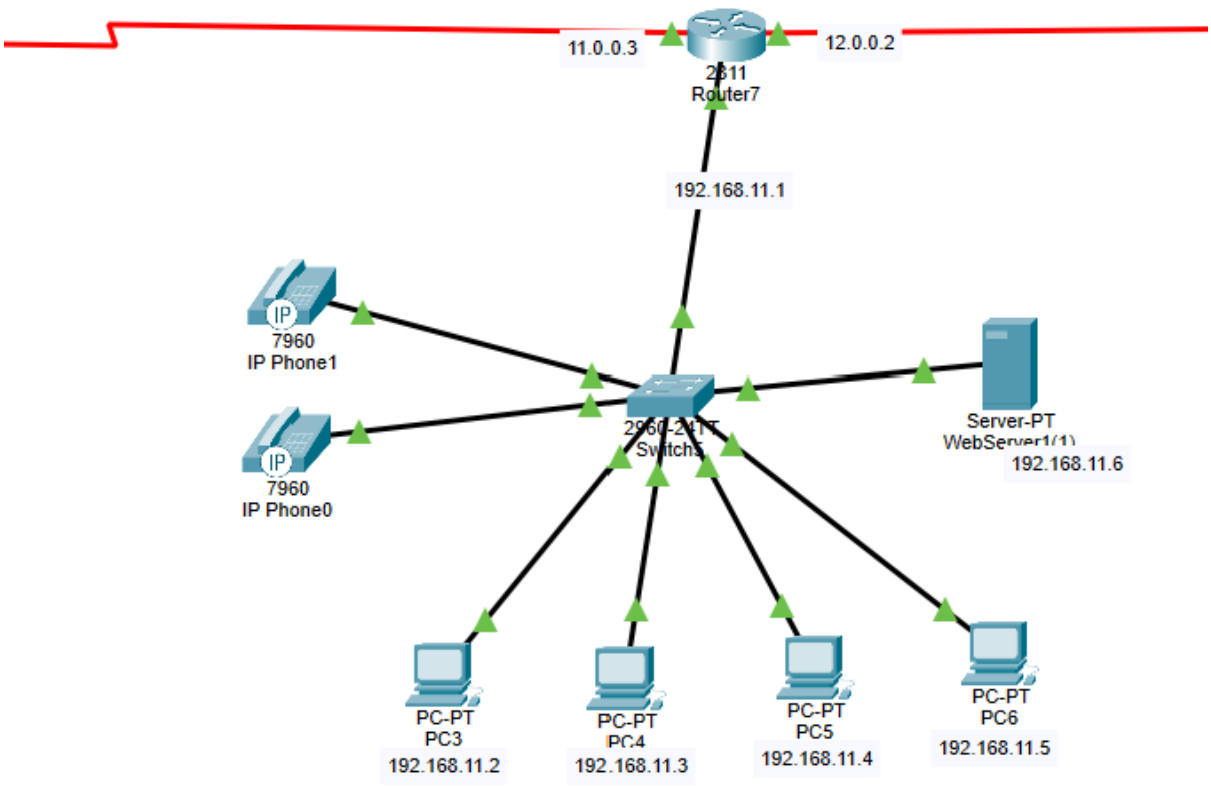
Managed Devices: Routers and switches that are likely SNMP-enabled for network management.

2.6. Simulation Elements

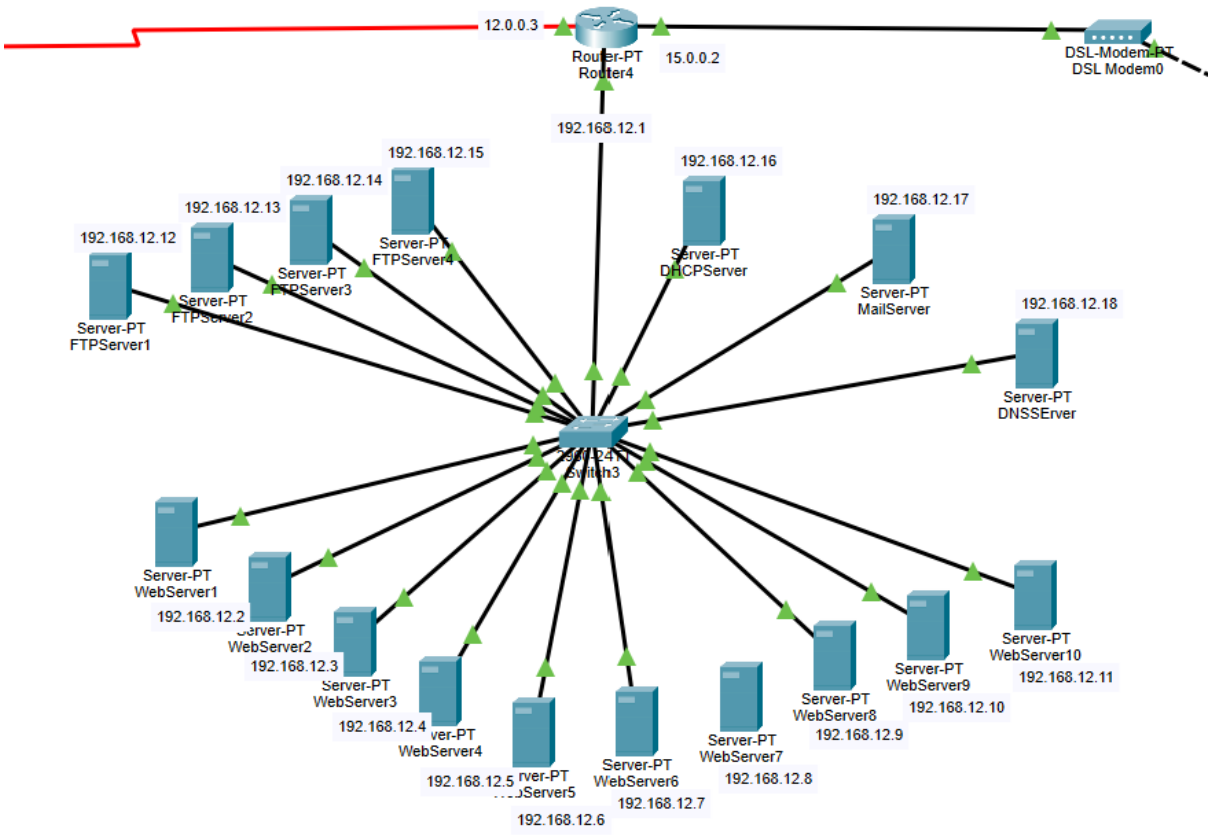
First Facility of First Branch:



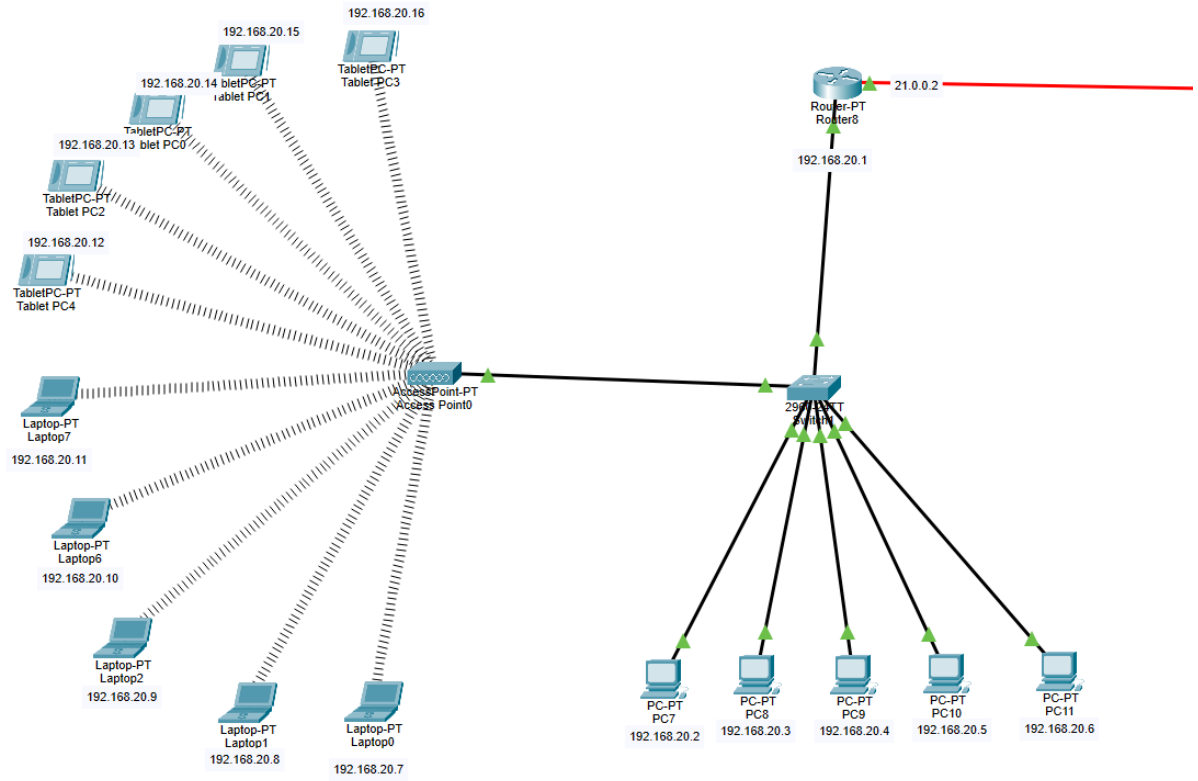
Second Facility of First Branch:



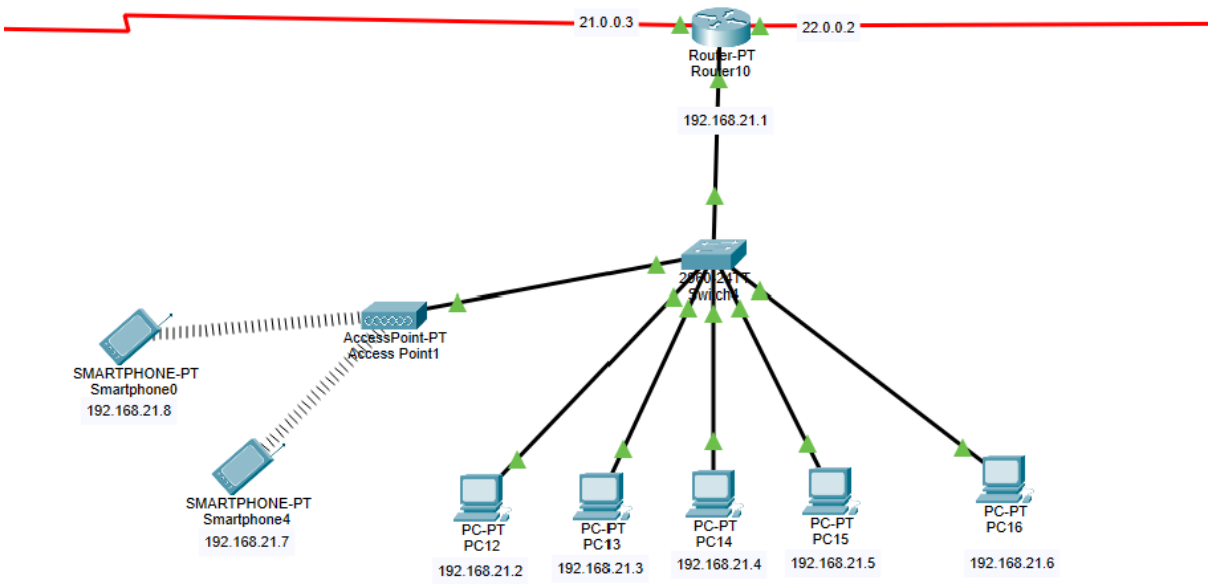
Third Facility of First Branch:


12.0.0.3
Router-PT
Router4
15.0.0.2
DSL-Modem-PT
DSL Modem0
192.168.12.1
192.168.12.15
192.168.12.14
192.168.12.13
192.168.12.12
192.168.12.16
192.168.12.17
192.168.12.18
Server-PT
FTPServer1
Server-PT
FTPServer2
Server-PT
FTPServer3
Server-PT
FTPServer4
Server-PT
DHCPServer
Server-PT
MailServer
Server-PT
DNSSErver
Switch3
Server-PT
WebServer1
192.168.12.2
Server-PT
WebServer2
192.168.12.3
Server-PT
WebServer3
192.168.12.4
Server-PT
WebServer4
192.168.12.5
Server-PT
WebServer5
192.168.12.6
Server-PT
WebServer6
192.168.12.7
Server-PT
WebServer7
192.168.12.8
Server-PT
WebServer8
192.168.12.9
Server-PT
WebServer9
192.168.12.10
Server-PT
WebServer10
192.168.12.11

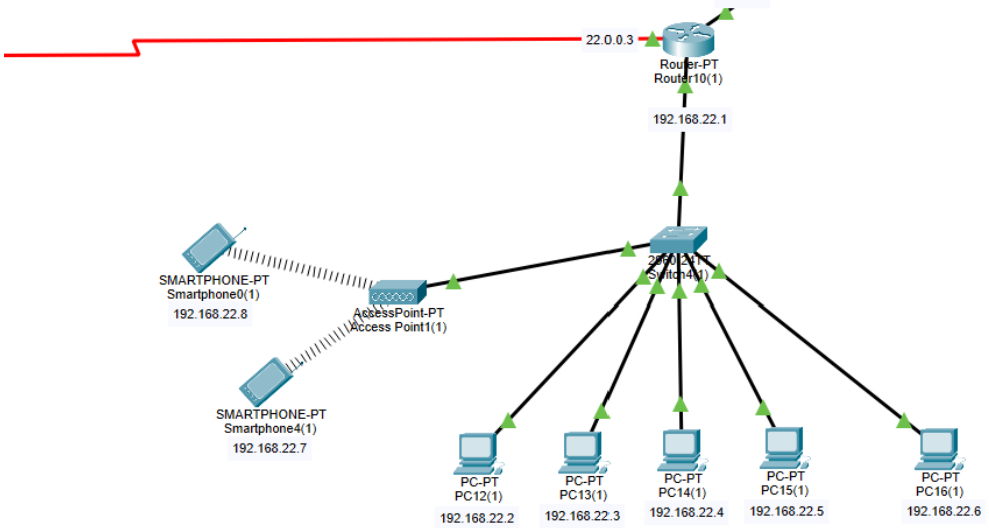
First Facility of Second Branch:



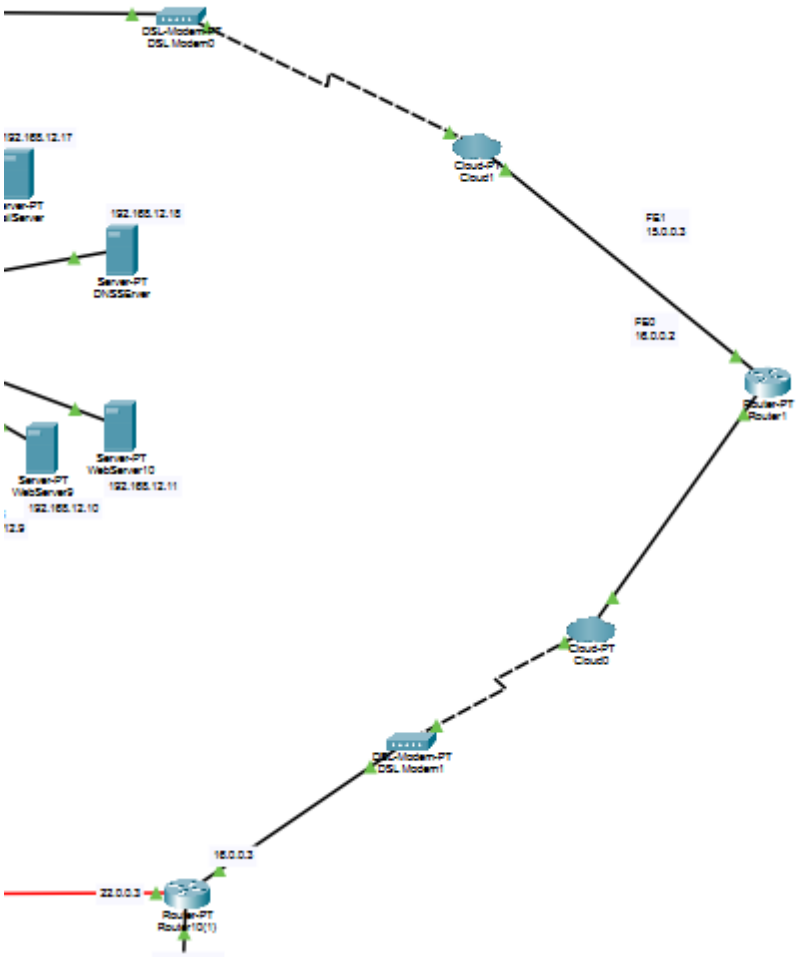
Second Facility of Second Branch:



Third Facility of Second Branch:



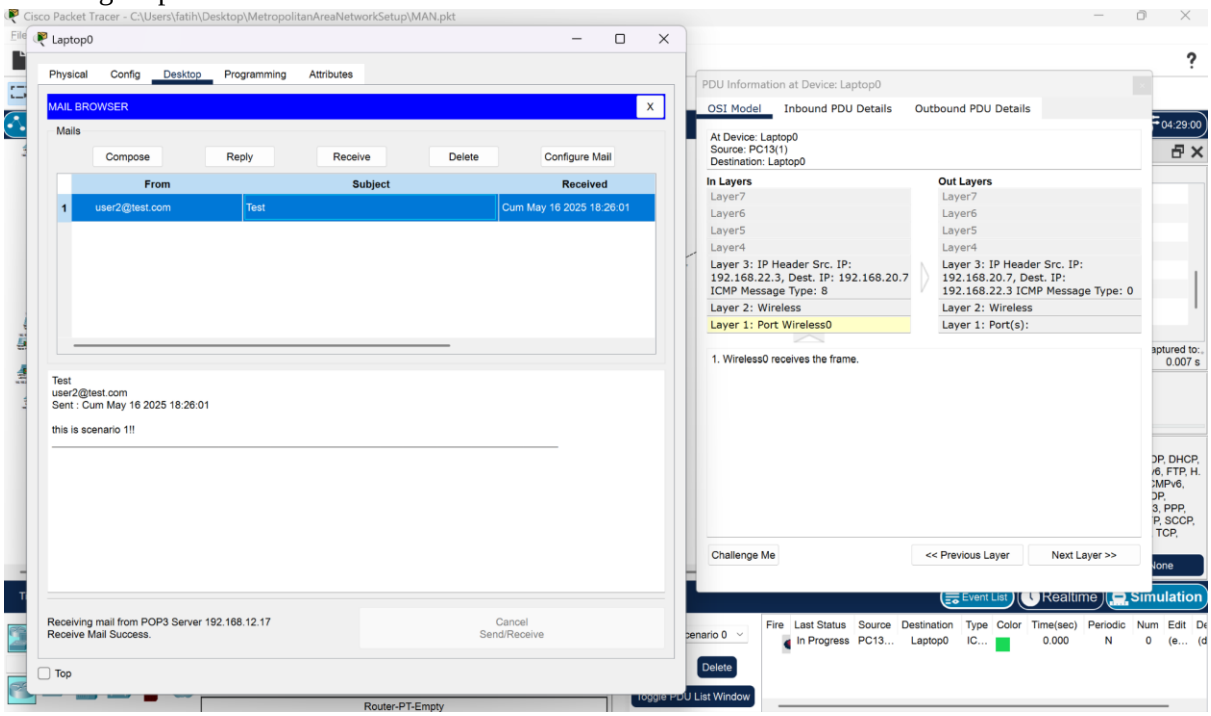
Internet Service Provider:

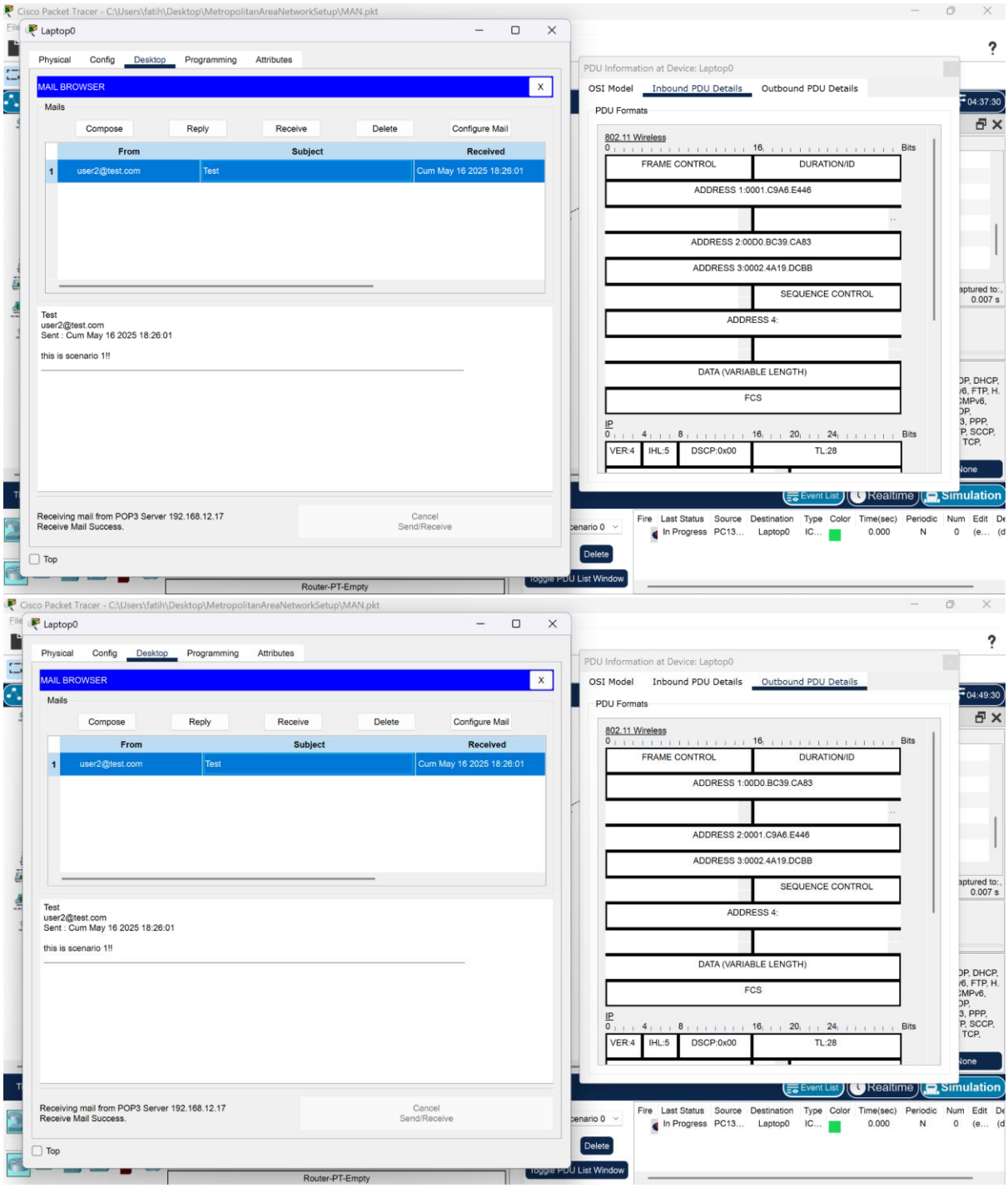


3. Traffic Analysis and Simulation Results

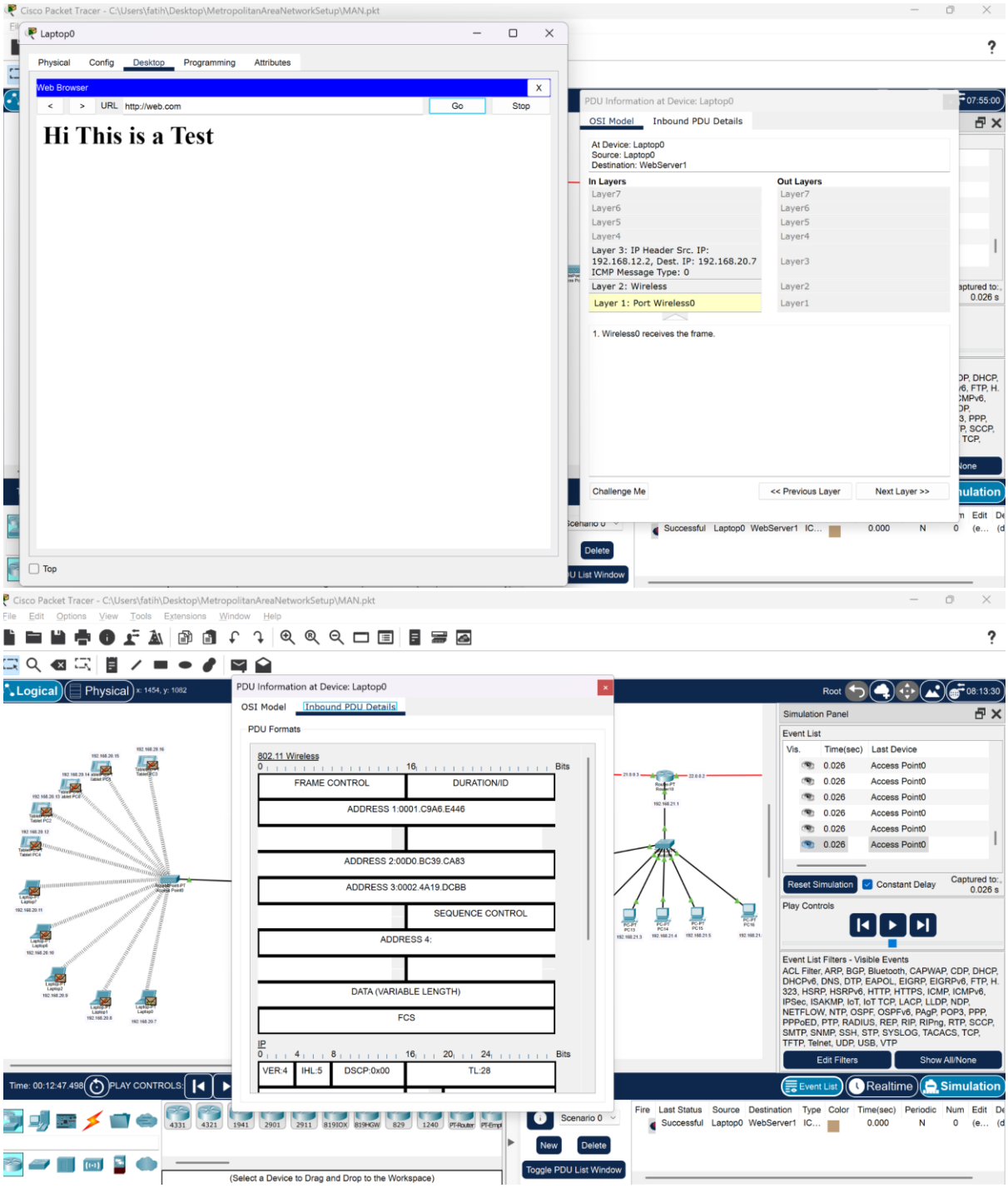
Simulation1: A wireless user from first facility of second branch wants to read emails and browse Web.

Firstly we create mail users from mail server and domain name from DNS server. Then assigning users to devices properly. Then sent email one to another via switches-routers (if in different branches, ISP)
to receive mails.
For browsing web, we again create a domain name in DNS server and put some files in web server for browsing output.



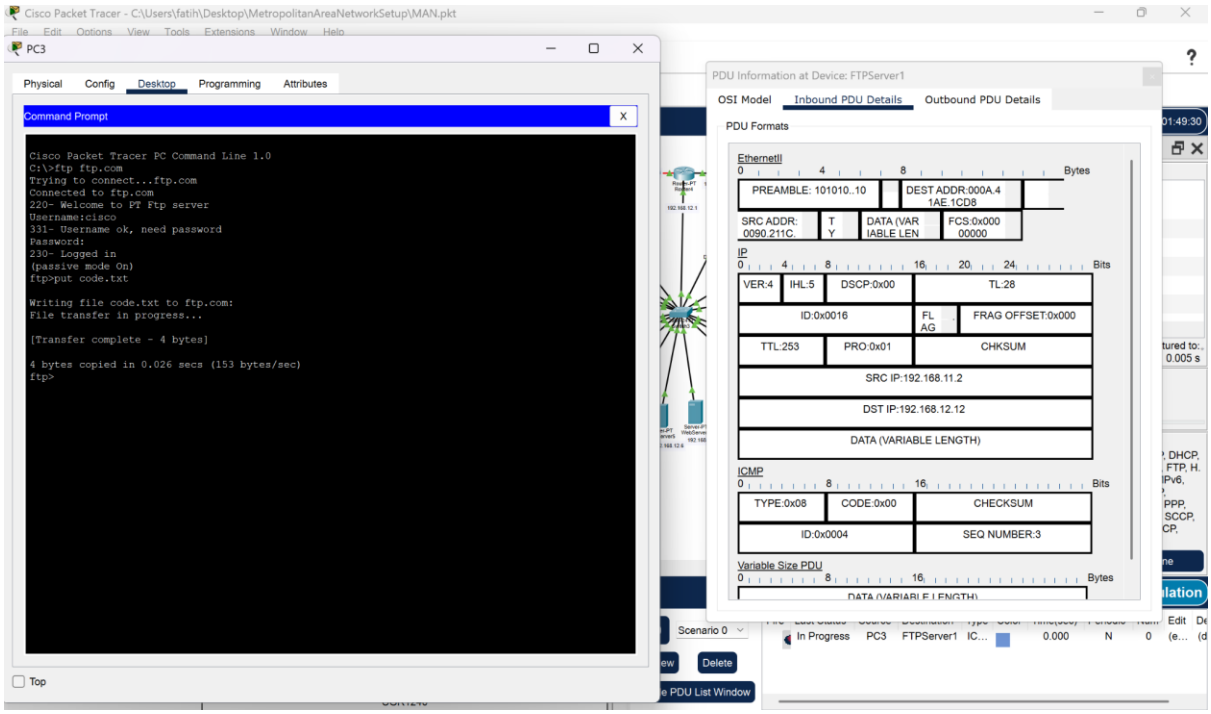

Cisco Packet Tracer - C:\Users\fatih\Desktop\MetropolitanAreaNetworkSetup\MAN.pkt
Laptop0
Physical
Config
Desktop
Programming
Attributes
MAIL BROWSER
Mails
Compose
Reply
Receive
Delete
Configure Mail
From
Subject
Received
1
user2@test.com
Test
Cum May 16 2025 18:26:01
Test
user2@test.com
Sent : Cum May 16 2025 18:26:01
this is scenario 1!!
Receiving mail from POP3 Server 192.168.12.17
Receive Mail Success.
Cancel
Send/Receive
Top
PDU Information at Device: Laptop0
OSI Model
Inbound PDU Details
Outbound PDU Details
PDU Formats
802.11 Wireless
FRAME CONTROL
DURATION/ID
ADDRESS 1:0001.C9A6.E446
ADDRESS 2:00D0.BC39.CA83
ADDRESS 3:0002.4A19.DCBB
SEQUENCE CONTROL
ADDRESS 4:
DATA (VARIABLE LENGTH)
FCS
IP
VER:4
IHL:5
DSCP:0x00
TL:28
Router-PT-Empty
Delete
Realtime
Simulation

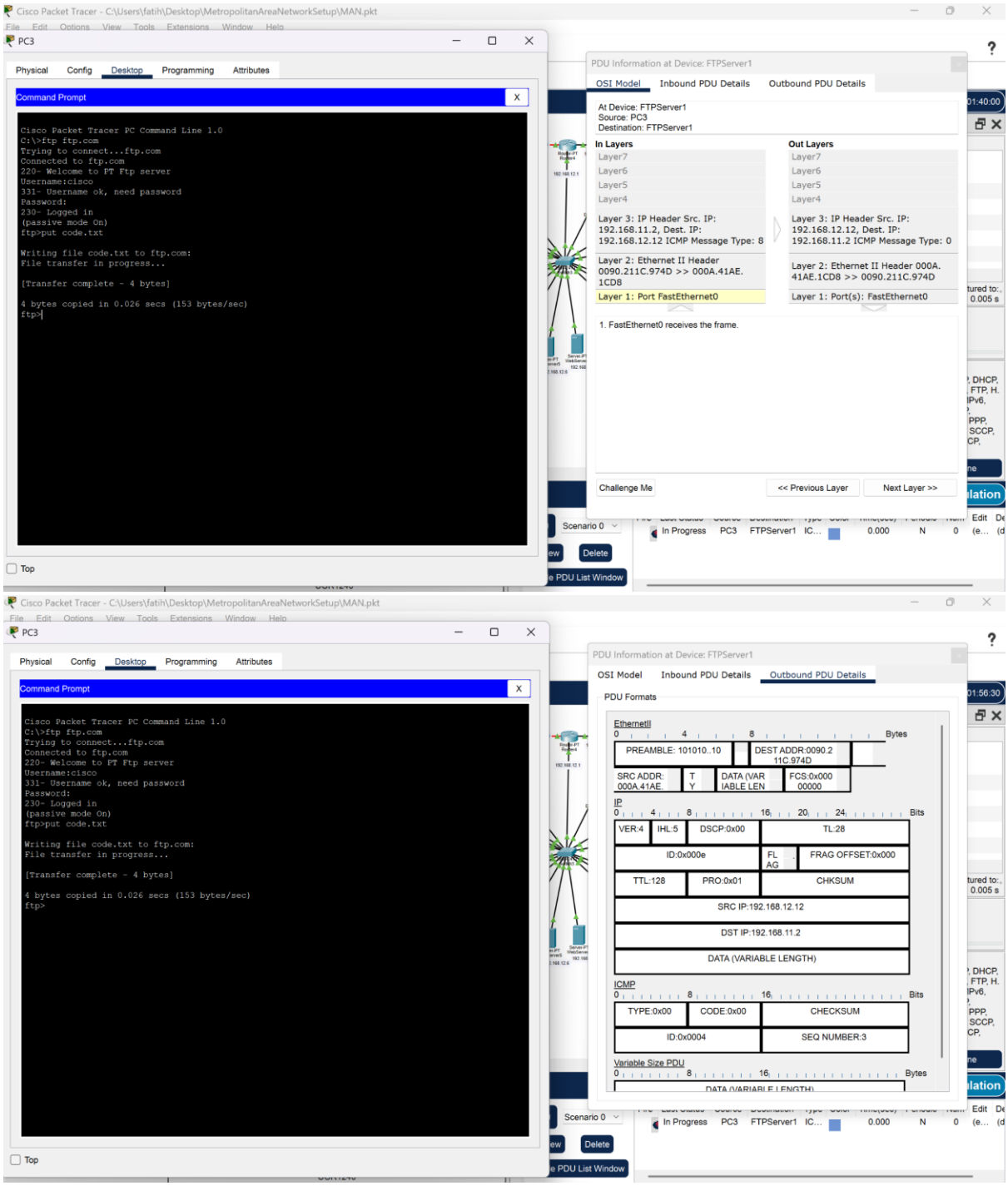
Cisco Packet Tracer - C:\Users\fatih\Desktop\MetropolitanAreaNetworkSetup\MAN.pkt
Laptop0
Physical
Config
Desktop
Programming
Attributes
MAIL BROWSER
Mails
Compose
Reply
Receive
Delete
Configure Mail
From
Subject
Received
1
user2@test.com
Test
Cum May 16 2025 18:26:01
Test
user2@test.com
Sent : Cum May 16 2025 18:26:01
this is scenario 1!!
Receiving mail from POP3 Server 192.168.12.17
Receive Mail Success.
Cancel
Send/Receive
Top
PDU Information at Device: Laptop0
OSI Model
Inbound PDU Details
Outbound PDU Details
PDU Formats
802.11 Wireless
FRAME CONTROL
DURATION/ID
ADDRESS 1:00D0.BC39.CA83
ADDRESS 2:0001.C9A6.E446
ADDRESS 3:0002.4A19.DCBB
SEQUENCE CONTROL
ADDRESS 4:
DATA (VARIABLE LENGTH)
FCS
IP
VER:4
IHL:5
DSCP:0x00
TL:28
Router-PT-Empty
Delete
Realtime
Simulation


Cisco Packet Tracer - C:\Users\fatih\Desktop\MetropolitanAreaNetworkSetup\MAN.pkt
Laptop0
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL http://web.com
Go
Stop
Hi This is a Test
Top
PDU Information at Device: Laptop0
OSI Model
Inbound PDU Details
At Device: Laptop0
Source: Laptop0
Destination: WebServer1
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 192.168.12.2, Dest. IP: 192.168.20.7 ICMP Message Type: 0
Layer3
Layer 2: Wireless
Layer2
Layer 1: Port Wireless0
Layer1
1. Wireless0 receives the frame.
Challenge Me
<< Previous Layer
Next Layer >>
Delete
U List Window
Successful Laptop0 WebServer1 IC...
0.000
N
0
Cisco Packet Tracer - C:\Users\fatih\Desktop\MetropolitanAreaNetworkSetup\MAN.pkt
File Edit Options View Tools Extensions Window Help
Logical
Physical
PDU Information at Device: Laptop0
OSI Model
Inbound PDU Details
PDU Formats
802.11 Wireless
Bits
FRAME CONTROL
DURATION/ID
ADDRESS 1:0001.C9A6.E446
ADDRESS 2:00D0.BC39.CA83
ADDRESS 3:0002.4A19.DCBB
SEQUENCE CONTROL
ADDRESS 4:
DATA (VARIABLE LENGTH)
FCS
IP
VER:4
IHL:5
DSCP:0x00
TL:28
Root
08:13:30
Simulation Panel
Event List
Vis.
Time(sec)
Last Device
0.026
Access Point0
Reset Simulation
Constant Delay
Captured to:
0.026 s
Play Controls
Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP
Edit Filters
Show All/None
Time: 00:12:47.498
PLAY CONTROLS:
Event List
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
(Select a Device to Drag and Drop to the Workspace)

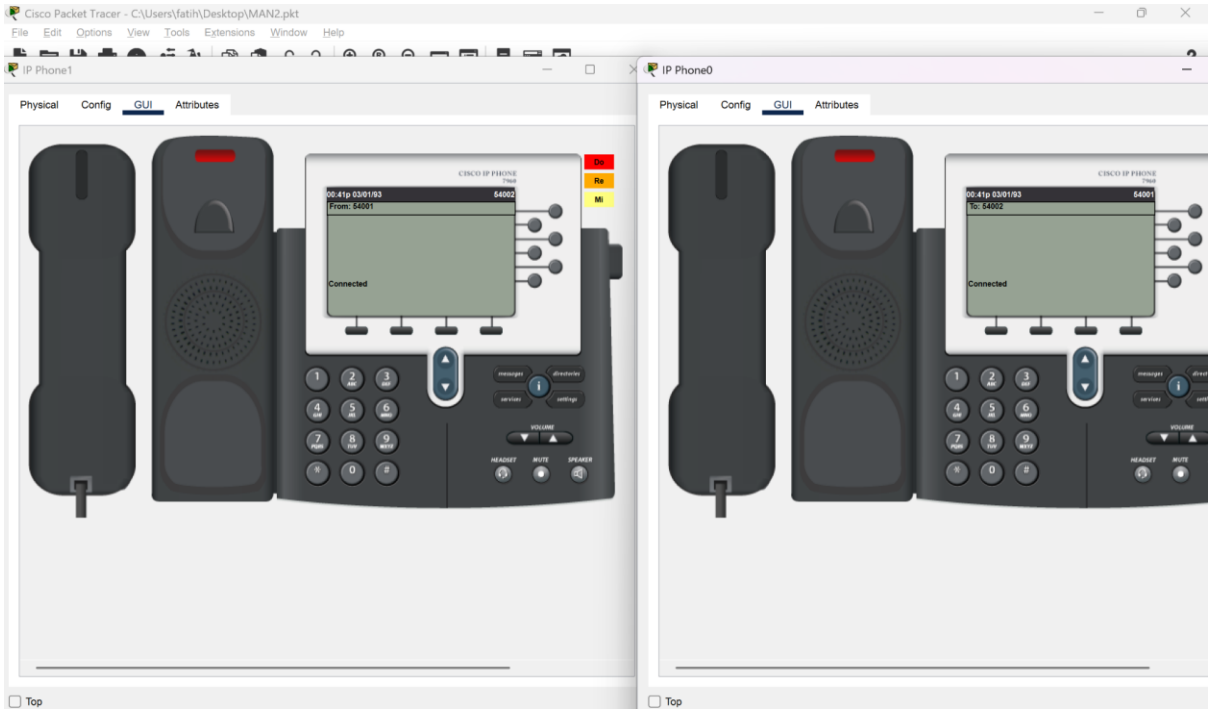
Simulation2: A computer engineer from second facility of second branch developed a web application and wants to send his/her code files to FTP server in the third facility of first branch.

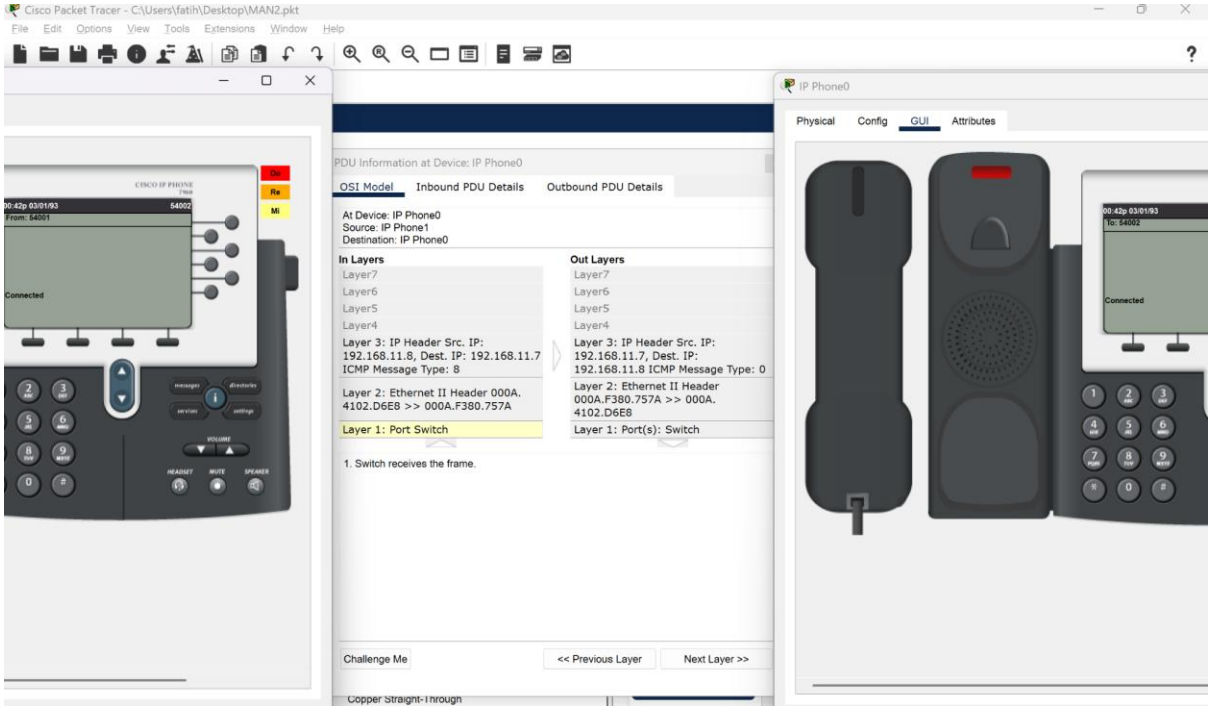
We create a domain name for ftp server and some files in device to send. Then reaching the ftp server by domain name and sent the file successfully.

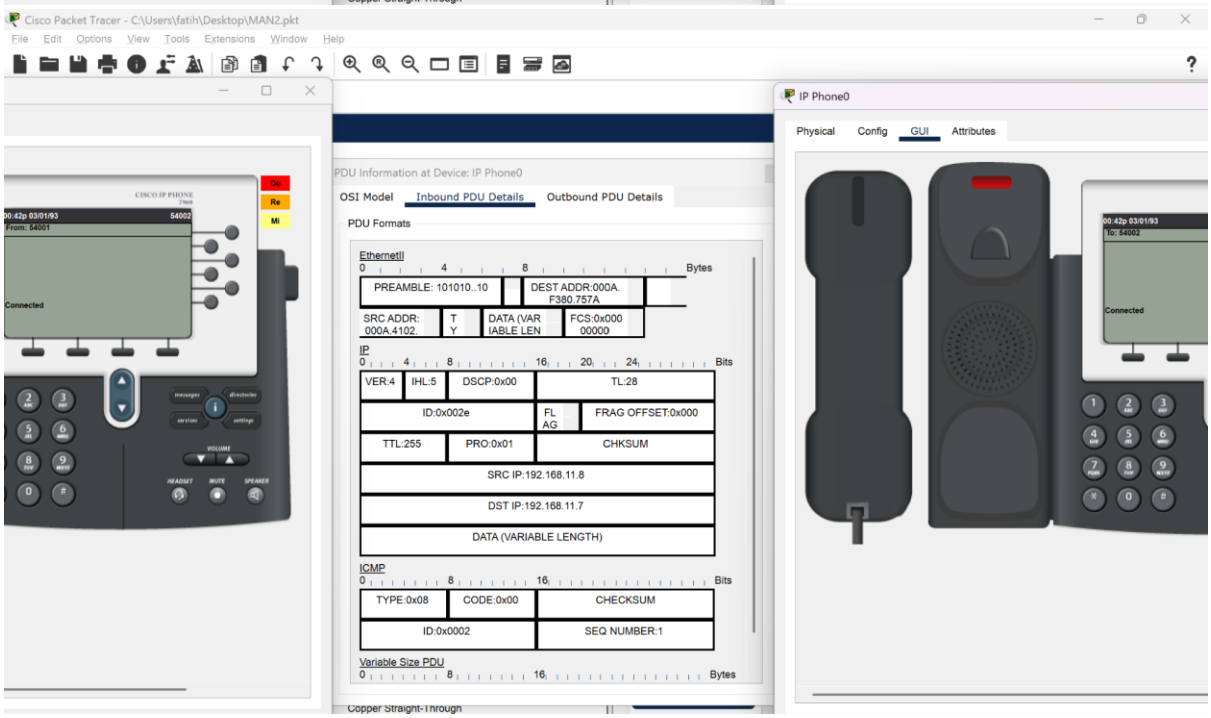


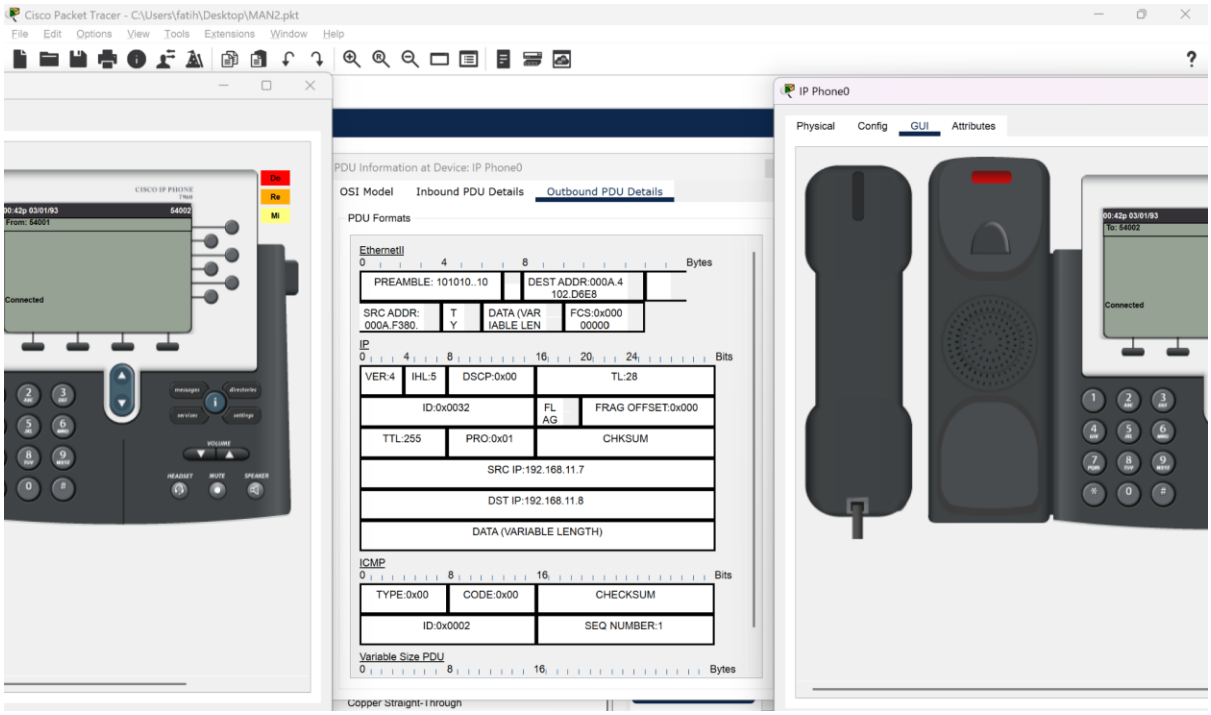


Simulation3: Two users from second facility of first branch want to talk via VoIP.
We needed to assign IPs via DHCP then enter their line numbers to call each other. After a few command prompts they can call and receive call from each other.

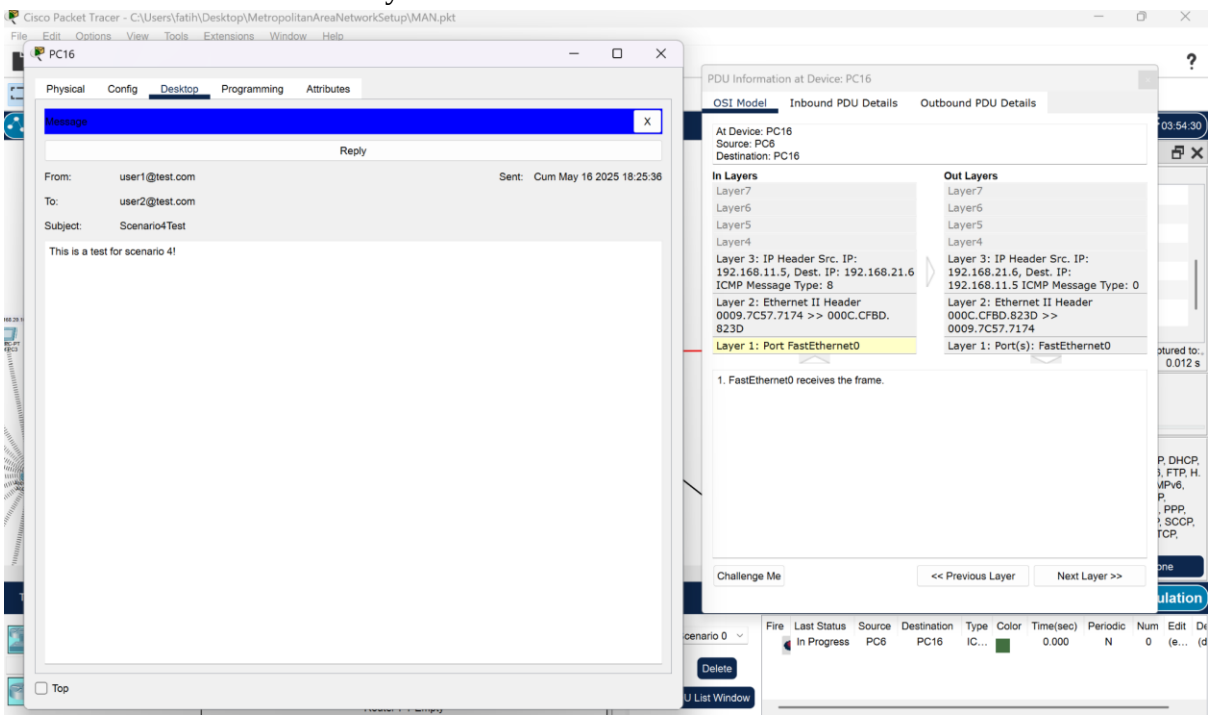

Cisco Packet Tracer - C:\Users\fatih\Desktop\MAN2.pkt
File Edit Options View Tools Extensions Window Help
IP Phone1
Physical Config GUI Attributes
Do
Re
Mi
00:41p 03/01/93 54002
From: 54001
Connected
Top
IP Phone0
Physical Config GUI Attributes
00:41p 03/01/93 54001
To: 54002
Connected
Top

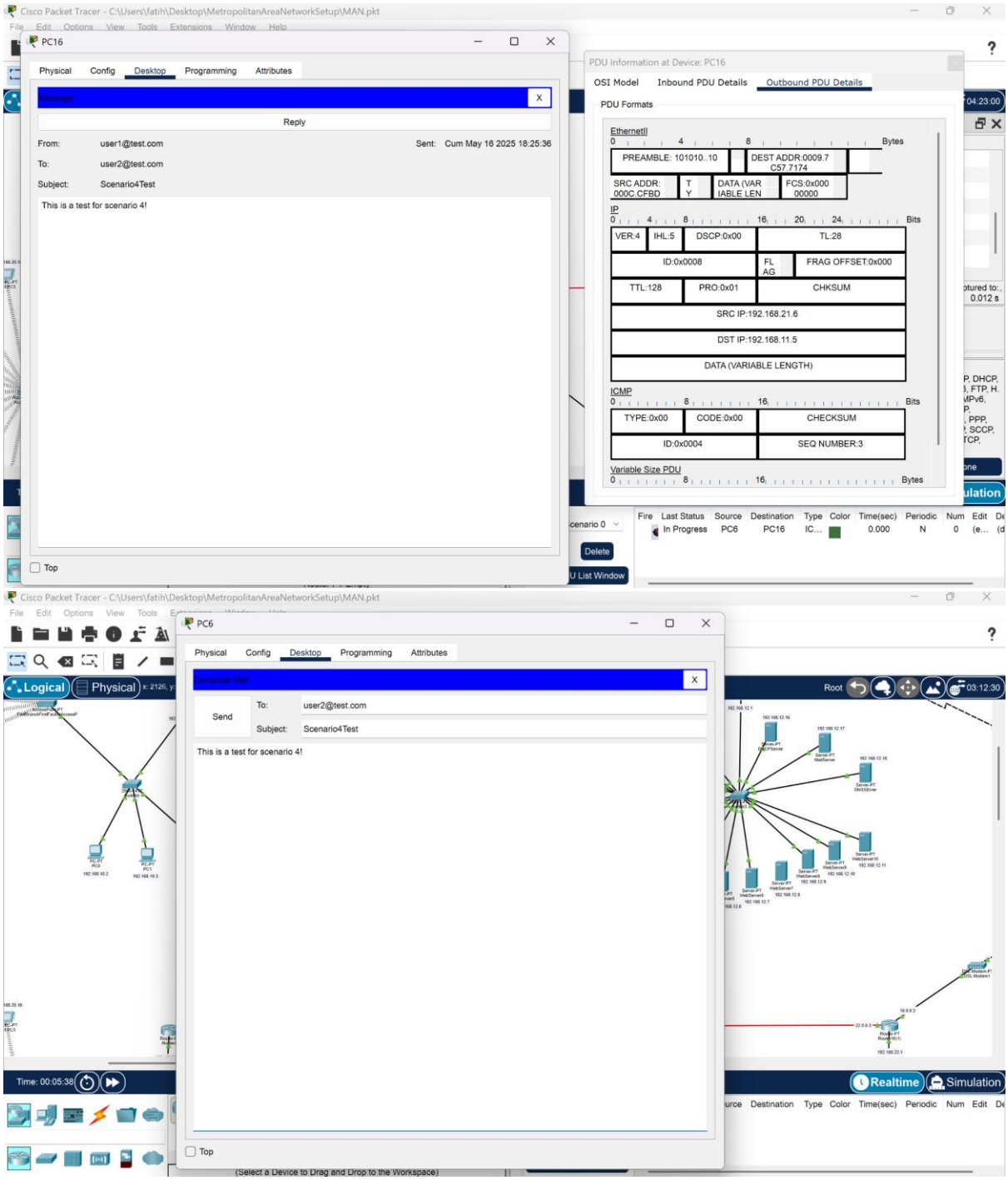

Cisco Packet Tracer - C:\Users\fatih\Desktop\MAN2.pkt
File Edit Options View Tools Extensions Window Help
PDU Information at Device: IP Phone0
OSI Model Inbound PDU Details Outbound PDU Details
At Device: IP Phone0
Source: IP Phone1
Destination: IP Phone0
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 192.168.11.8, Dest. IP: 192.168.11.7 ICMP Message Type: 8
Layer 3: IP Header Src. IP: 192.168.11.7, Dest. IP: 192.168.11.8 ICMP Message Type: 0
Layer 2: Ethernet II Header 000A.4102.D6E8 >> 000A.F380.757A
Layer 2: Ethernet II Header 000A.F380.757A >> 000A.4102.D6E8
Layer 1: Port Switch
Layer 1: Port(s): Switch
1. Switch receives the frame.
Challenge Me
<< Previous Layer
Next Layer >>
Copper Straight-Through
IP Phone0
Physical Config GUI Attributes

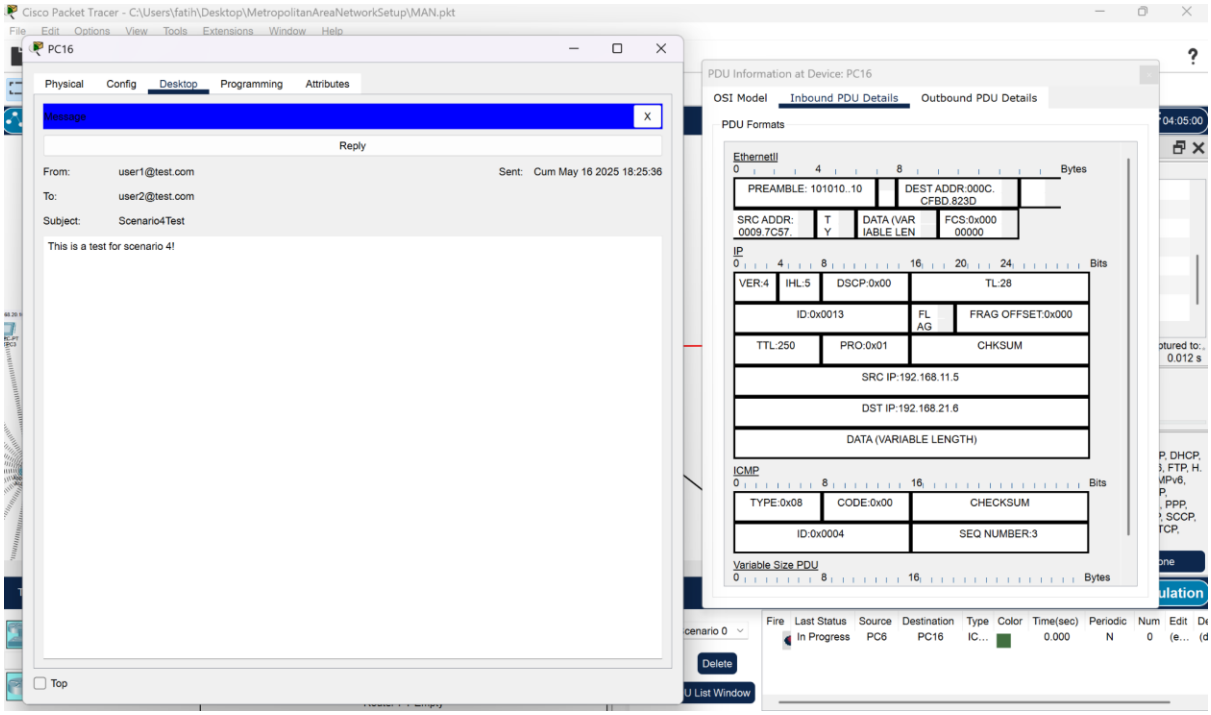

Cisco Packet Tracer - C:\Users\fatih\Desktop\MAN2.pkt
File Edit Options View Tools Extensions Window Help
PDU Information at Device: IP Phone0
OSI Model Inbound PDU Details Outbound PDU Details
PDU Formats
EthernetII
PREAMBLE: 101010..10
DEST ADDR:000A.F380.757A
SRC ADDR: 000A.4102.
DATA (VARIABLE LEN
FCS:0x00000000
IP
VER:4
IHL:5
DSCP:0x00
TL:28
ID:0x002e
FLAG
FRAG OFFSET:0x000
TTL:255
PRO:0x01
CHKSUM
SRC IP:192.168.11.8
DST IP:192.168.11.7
DATA (VARIABLE LENGTH)
ICMP
TYPE:0x08
CODE:0x00
CHECKSUM
ID:0x0002
SEQ NUMBER:1
Variable Size PDU
Copper Straight-Through
IP Phone0
Physical Config GUI Attributes



Simulation4: 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.

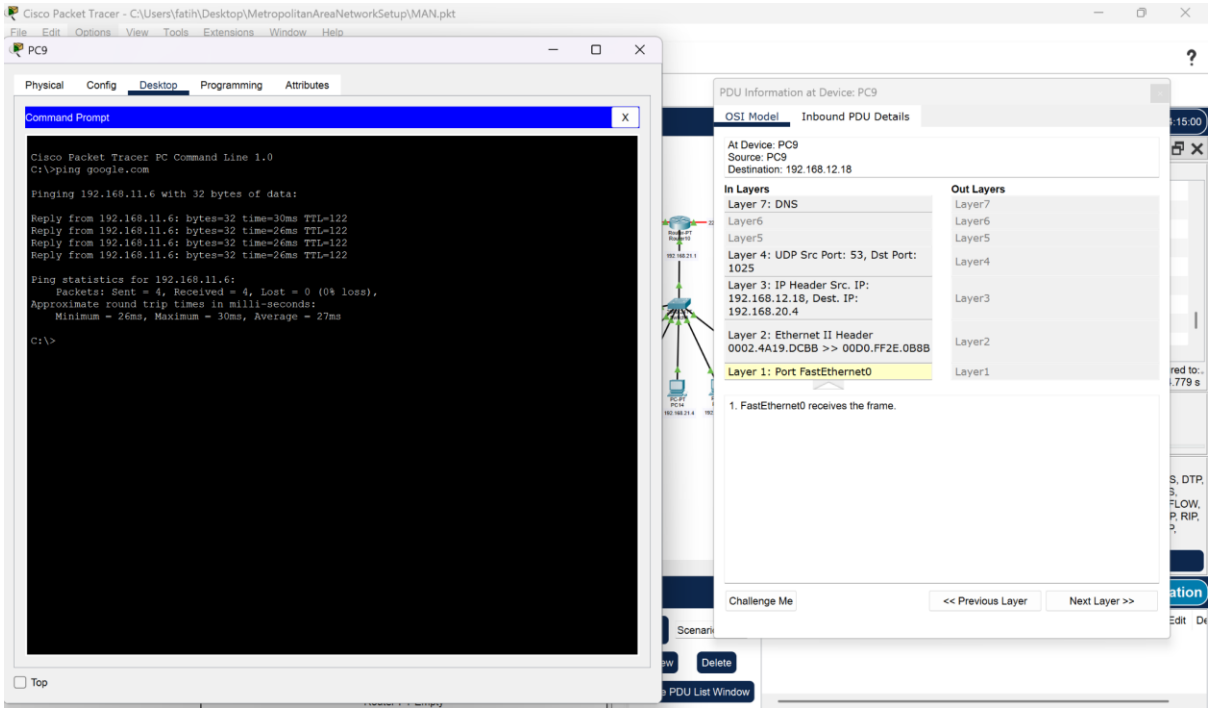


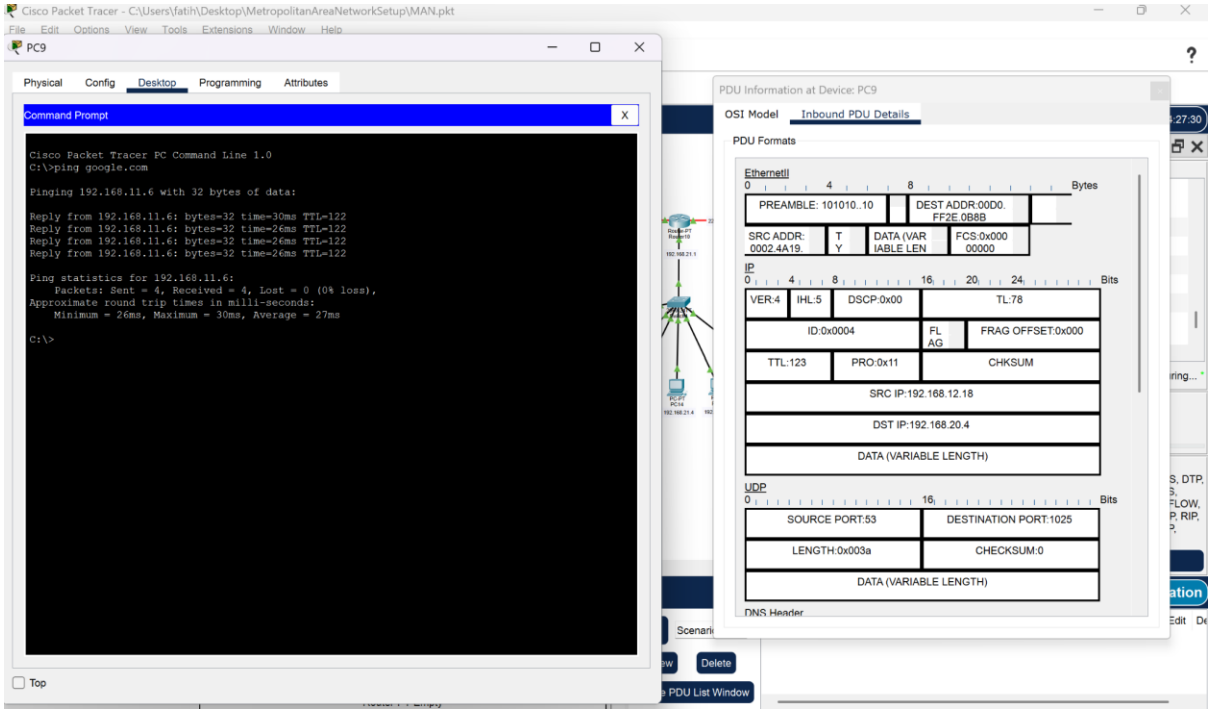

PC16
Physical
Config
Desktop
Programming
Attributes
Reply
From: user1@test.com
Sent: Cum May 16 2025 18:25:36
To: user2@test.com
Subject: Scenario4Test
This is a test for scenario 4!
Top
PDU Information at Device: PC16
OSI Model
Inbound PDU Details
Outbound PDU Details
PDU Formats
Ethernetll
PREAMBLE: 101010..10
DEST ADDR:0009.7
C57.7174
SRC ADDR:
000C.CFBD
DATA (VAR
IABLE LEN
FCS:0x000
00000
IP
VER:4
IHL:5
DSCP:0x00
TL:28
ID:0x0008
FRAG OFFSET:0x000
TTL:128
PRO:0x01
CHKSUM
SRC IP:192.168.21.6
DST IP:192.168.11.5
DATA (VARIABLE LENGTH)
ICMP
TYPE:0x00
CODE:0x00
CHECKSUM
ID:0x0004
SEQ NUMBER:3
Variable Size PDU
Delete
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
In Progress
PC6
PC16
0.000
PC6
Physical
Config
Desktop
Programming
Attributes
Send
To: user2@test.com
Subject: Scenario4Test
This is a test for scenario 4!
Top
Logical
Physical
Root
Time: 00:05:38
Realtime
Simulation



Simulation5: A user from first facility of second branch pings Web server of second facility of first branch.

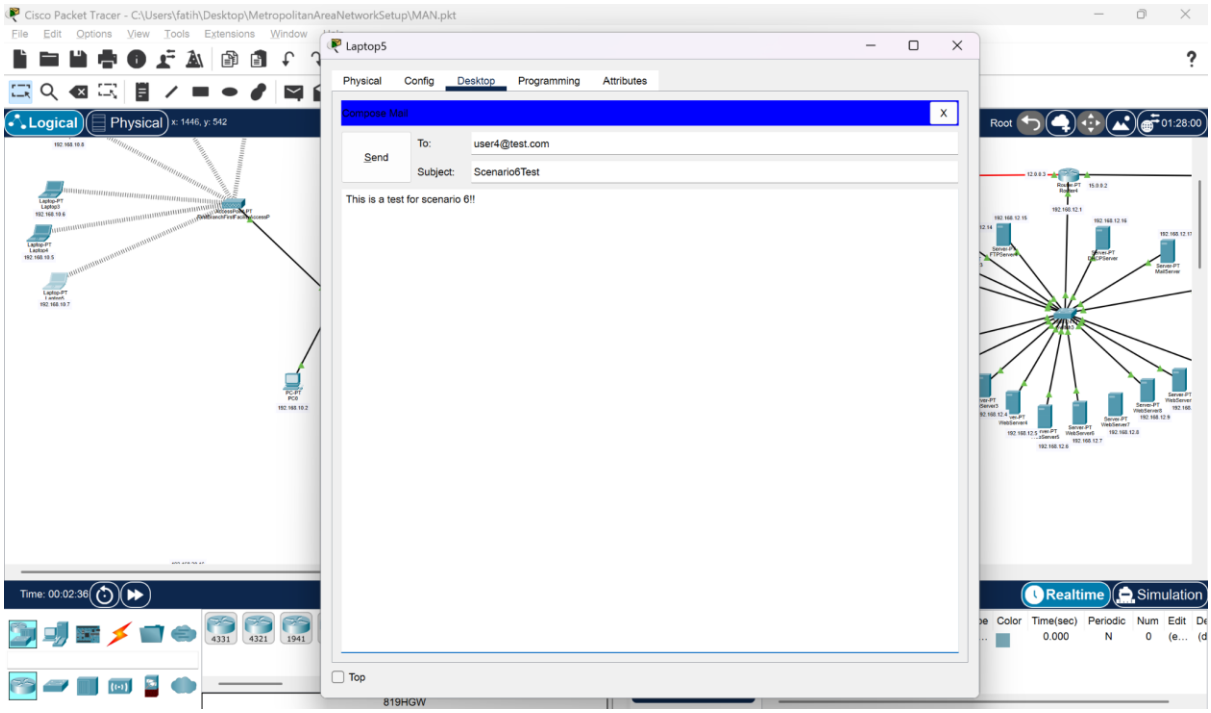
First we created a domain name for the web server in DNS server and ping that domain name via command prompt .

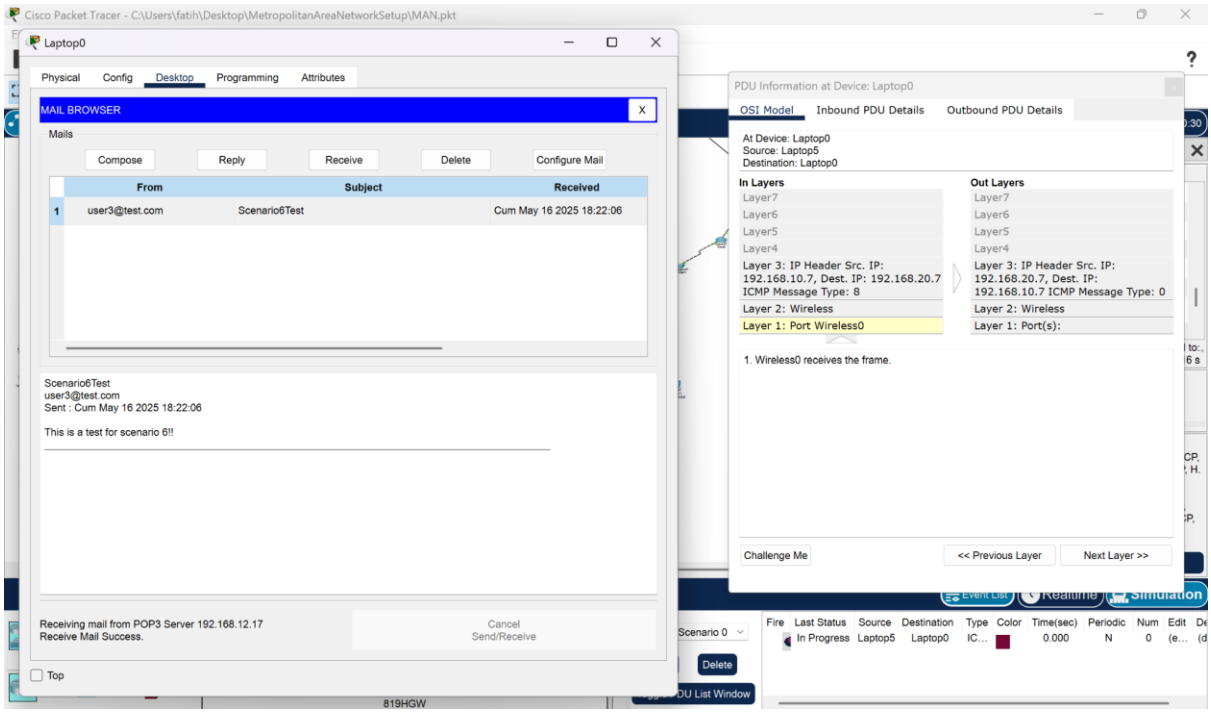


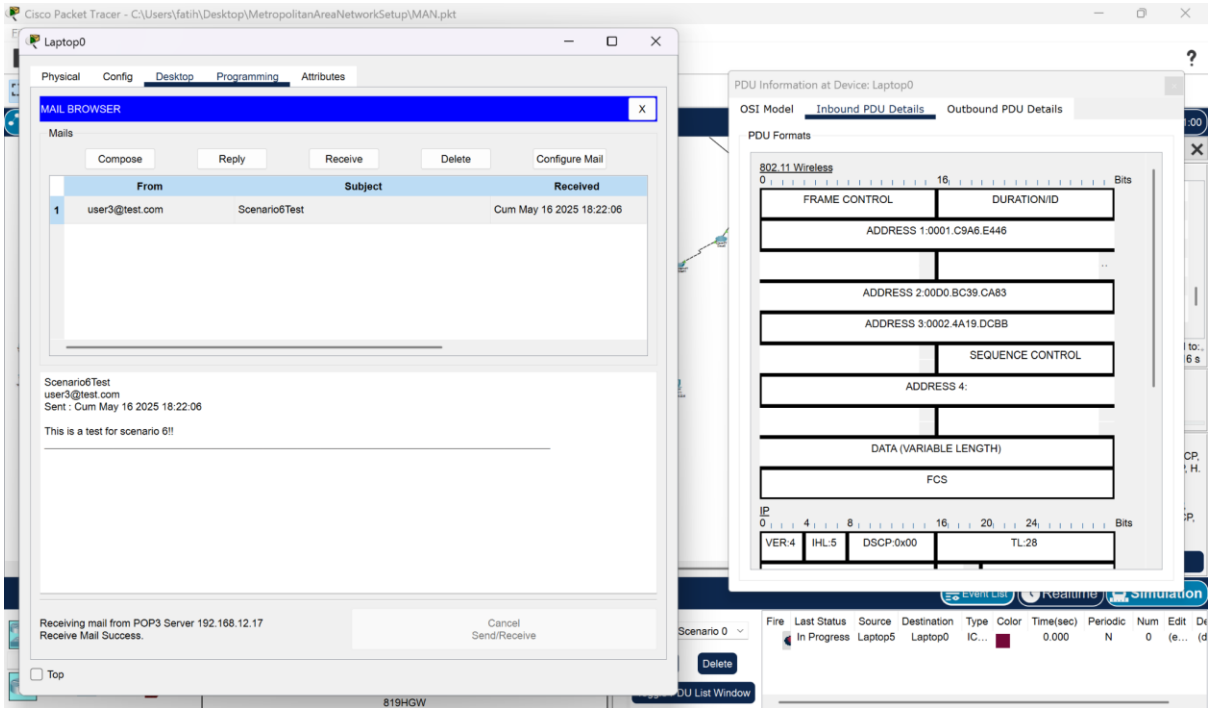


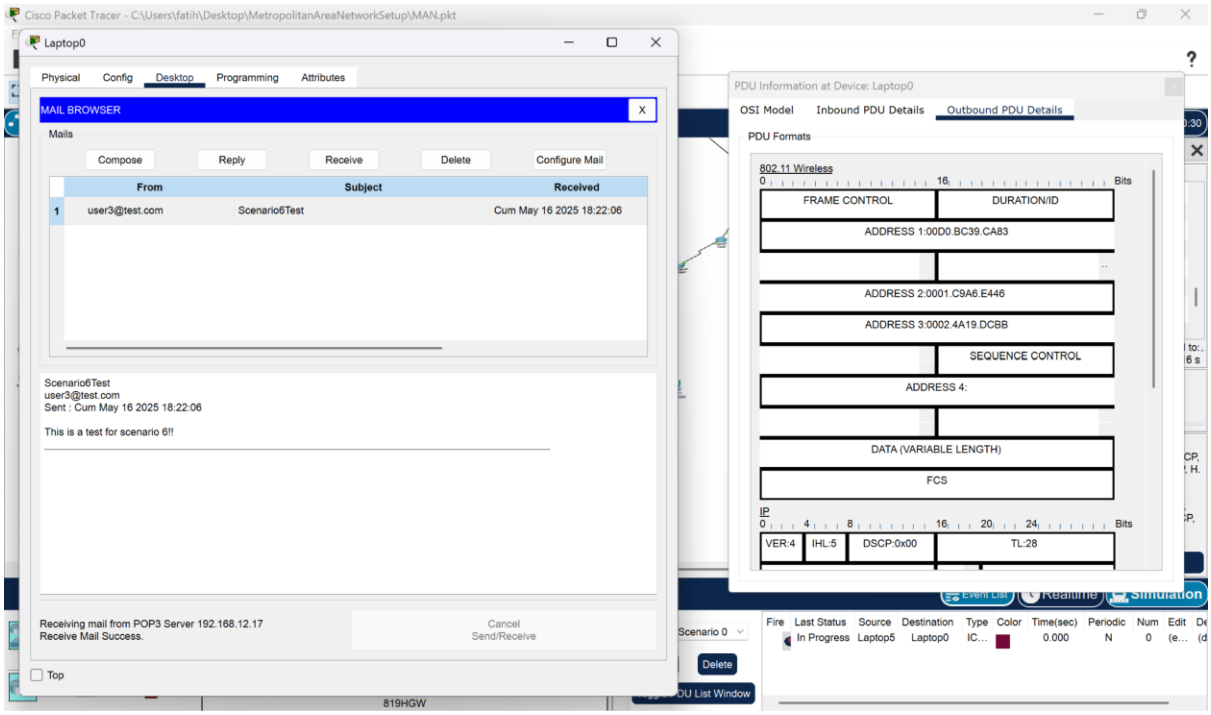
Simulation6: A laptop user from first facility of first branch office wants to send email to her friend in the first facility of second branch office.

We already created domain name for mail server. Just by created 2 more email users from mail server we can send and receive mail by assigning these users to devices.



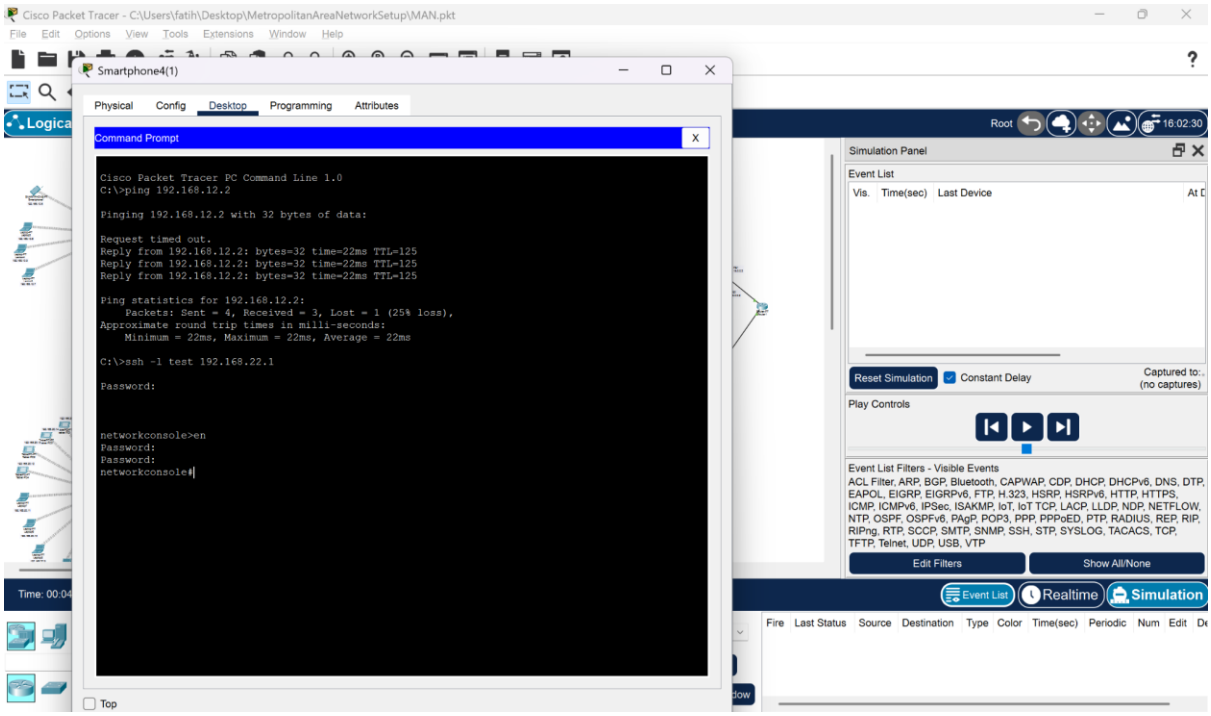

Cisco Packet Tracer - C:\Users\fatih\Desktop\MetropolitanAreaNetworkSetup\MAN.pkt
Laptop0
Physical
Config
Desktop
Programming
Attributes
MAIL BROWSER
Mails
Compose
Reply
Receive
Delete
Configure Mail
From
Subject
Received
1
user3@test.com
Scenario6Test
Cum May 16 2025 18:22:06
Scenario6Test
user3@test.com
Sent : Cum May 16 2025 18:22:06
This is a test for scenario 6!!
Receiving mail from POP3 Server 192.168.12.17
Receive Mail Success.
Cancel
Send/Receive
Top
819HGW
PDU Information at Device: Laptop0
OSI Model
Inbound PDU Details
Outbound PDU Details
At Device: Laptop0
Source: Laptop5
Destination: Laptop0
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 192.168.10.7, Dest. IP: 192.168.20.7 ICMP Message Type: 8
Layer 3: IP Header Src. IP: 192.168.20.7, Dest. IP: 192.168.10.7 ICMP Message Type: 0
Layer 2: Wireless
Layer 1: Port Wireless0
Layer 1: Port(s):
1. Wireless0 receives the frame.
Challenge Me
<< Previous Layer
Next Layer >>
Scenario 0
Delete
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
In Progress
Laptop5
Laptop0
0.000
N
0

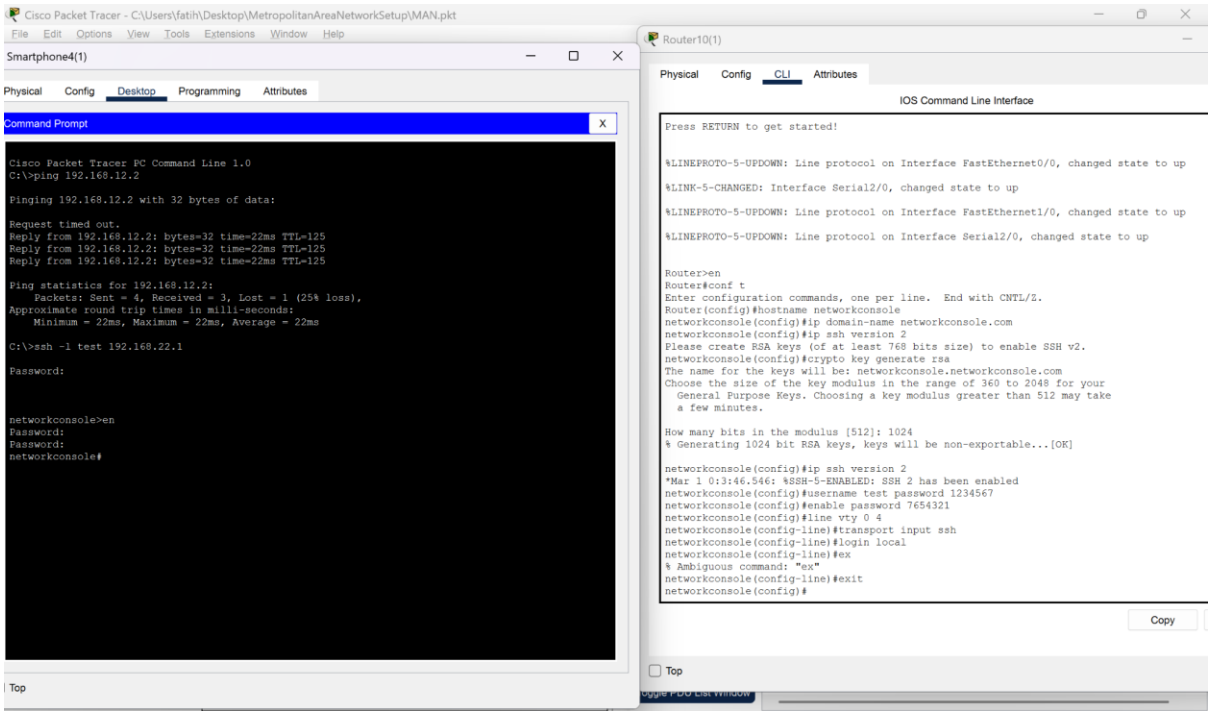

Cisco Packet Tracer - C:\Users\fatih\Desktop\MetropolitanAreaNetworkSetup\MAN.pkt
Laptop0
Physical
Config
Desktop
Programming
Attributes
MAIL BROWSER
Mails
Compose
Reply
Receive
Delete
Configure Mail
From
Subject
Received
1
user3@test.com
Scenario6Test
Cum May 16 2025 18:22:06
Scenario6Test
user3@test.com
Sent : Cum May 16 2025 18:22:06
This is a test for scenario 6!!
Receiving mail from POP3 Server 192.168.12.17
Receive Mail Success.
Cancel
Send/Receive
Top
819HGW
PDU Information at Device: Laptop0
OSI Model
Inbound PDU Details
Outbound PDU Details
PDU Formats
802.11 Wireless
Bits
FRAME CONTROL
DURATION/ID
ADDRESS 1:0001.C9A6.E446
ADDRESS 2:00D0.BC39.CA83
ADDRESS 3:0002.4A19.DCBB
SEQUENCE CONTROL
ADDRESS 4:
DATA (VARIABLE LENGTH)
FCS
IP
VER:4
IHL:5
DSCP:0x00
TL:28
Scenario 0
Delete
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
In Progress
Laptop5
Laptop0
0.000
N
0



Simulation7: A smartphone user from the third facility of the second branch office wants to use SSH to connect to a Web server in the third facility of the first branch office.

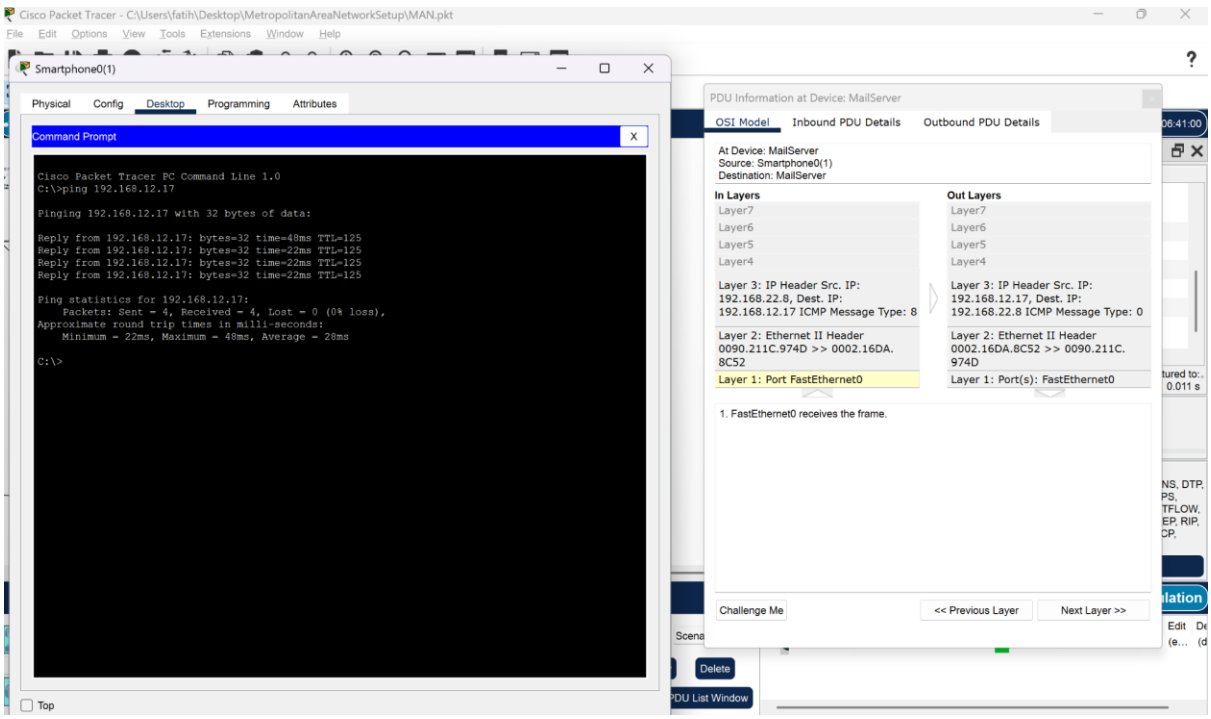
First we ensured the connection between server and device by pinging the server. Then creating a username and password (and an enable password) by selection various options in command prompt we can use ssh in the router.

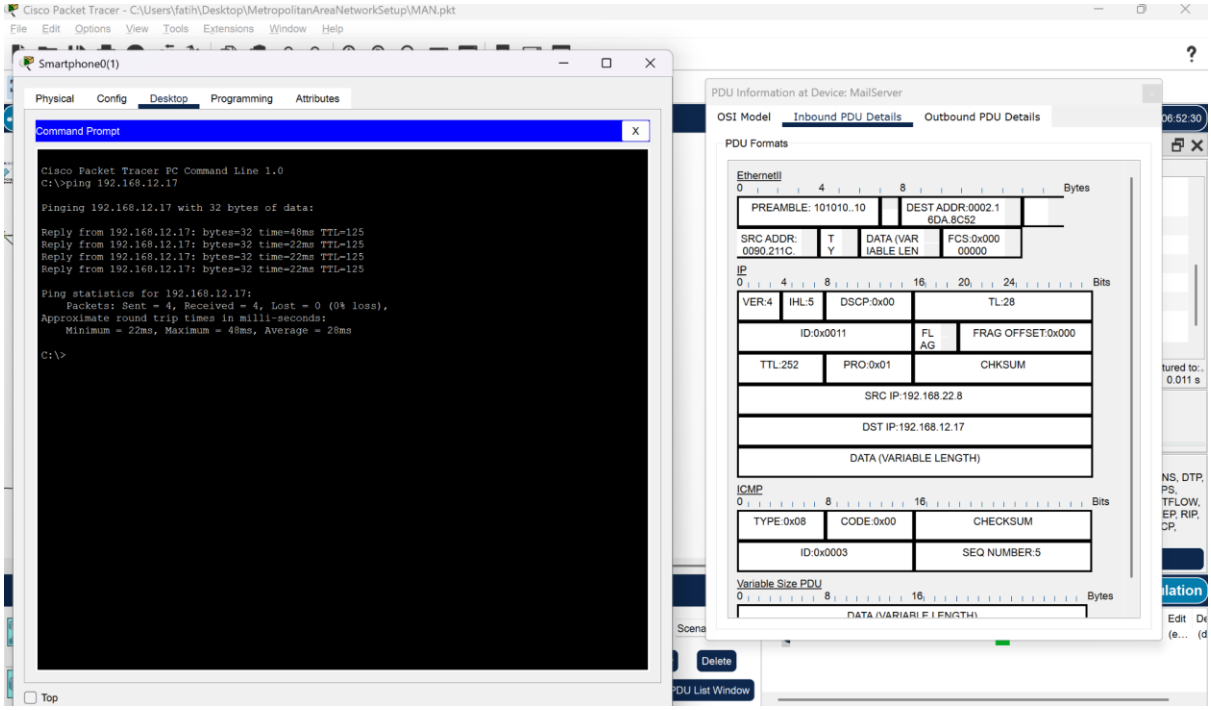


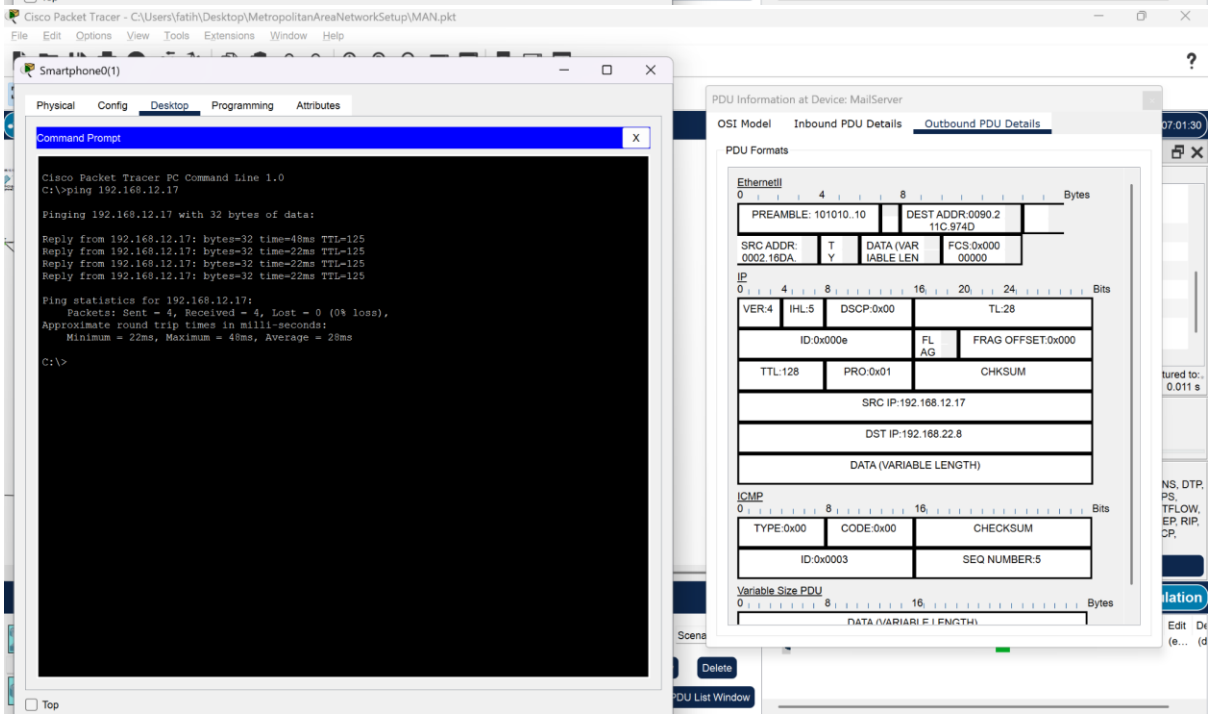


Simulation8: A mobile device user from third facility of second branch pings the email server of third facility of first branch.

This type of communication is explained in the previous simulations

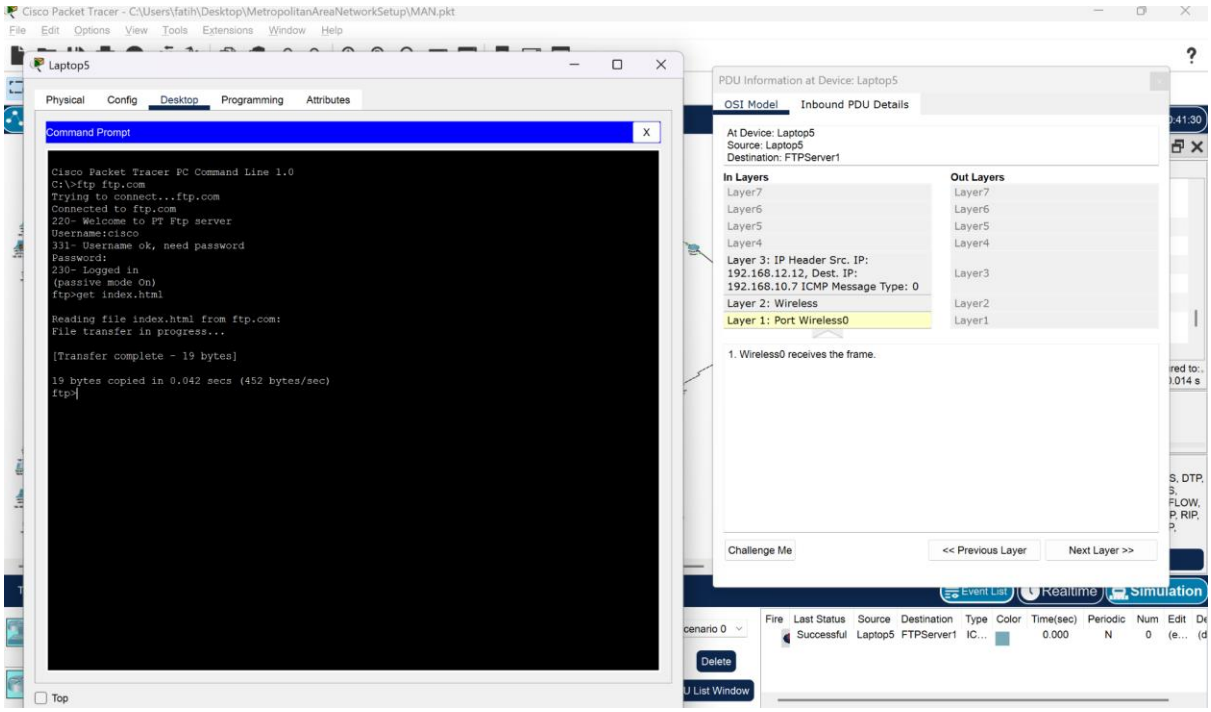


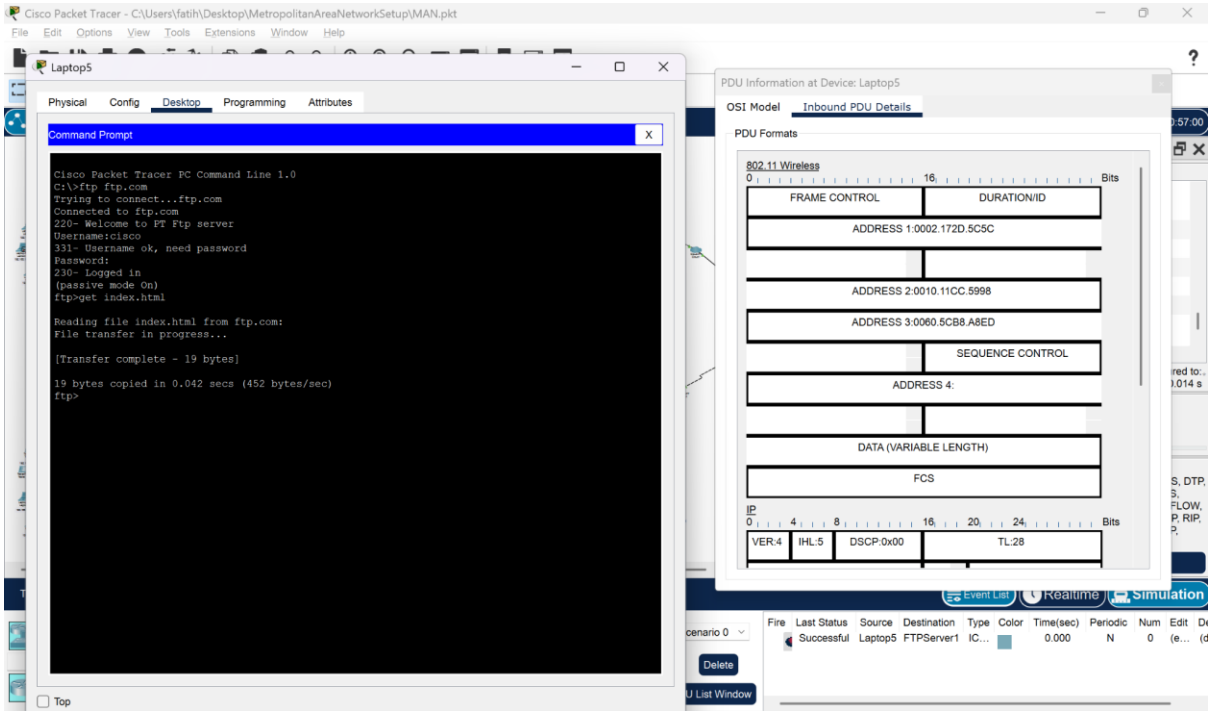

Cisco Packet Tracer - C:\Users\fatih\Desktop\MetropolitanAreaNetworkSetup\MAN.pkt
File Edit Options View Tools Extensions Window Help
Smartphone0(1)
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.12.17
Pinging 192.168.12.17 with 32 bytes of data:
Reply from 192.168.12.17: bytes=32 time=48ms TTL=125
Reply from 192.168.12.17: bytes=32 time=22ms TTL=125
Reply from 192.168.12.17: bytes=32 time=22ms TTL=125
Reply from 192.168.12.17: bytes=32 time=22ms TTL=125
Ping statistics for 192.168.12.17:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 22ms, Maximum = 48ms, Average = 28ms
C:\>
Top
PDU Information at Device: MailServer
OSI Model Inbound PDU Details Outbound PDU Details
PDU Formats
EthernetII
PREAMBLE: 101010..10
DEST ADDR:0002.16DA.8C52
SRC ADDR: 0090.211C.
DATA (VARIABLE LEN
FCS:0x000 00000
IP
VER:4 IHL:5 DSCP:0x00 TL:28
ID:0x0011 FLAG FRAG OFFSET:0x000
TTL:252 PRO:0x01 CHKSUM
SRC IP:192.168.22.8
DST IP:192.168.12.17
DATA (VARIABLE LENGTH)
ICMP
TYPE:0x08 CODE:0x00 CHECKSUM
ID:0x0003 SEQ NUMBER:5
Variable Size PDU
Delete
PDU List Window


Cisco Packet Tracer - C:\Users\fatih\Desktop\MetropolitanAreaNetworkSetup\MAN.pkt
File Edit Options View Tools Extensions Window Help
Smartphone0(1)
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.12.17
Pinging 192.168.12.17 with 32 bytes of data:
Reply from 192.168.12.17: bytes=32 time=48ms TTL=125
Reply from 192.168.12.17: bytes=32 time=22ms TTL=125
Reply from 192.168.12.17: bytes=32 time=22ms TTL=125
Reply from 192.168.12.17: bytes=32 time=22ms TTL=125
Ping statistics for 192.168.12.17:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 22ms, Maximum = 48ms, Average = 28ms
C:\>
Top
PDU Information at Device: MailServer
OSI Model Inbound PDU Details Outbound PDU Details
PDU Formats
EthernetII
PREAMBLE: 101010..10
DEST ADDR:0090.211C.974D
SRC ADDR: 0002.16DA.
DATA (VARIABLE LEN
FCS:0x000 00000
IP
VER:4 IHL:5 DSCP:0x00 TL:28
ID:0x000e FLAG FRAG OFFSET:0x000
TTL:128 PRO:0x01 CHKSUM
SRC IP:192.168.12.17
DST IP:192.168.22.8
DATA (VARIABLE LENGTH)
ICMP
TYPE:0x00 CODE:0x00 CHECKSUM
ID:0x0003 SEQ NUMBER:5
Variable Size PDU
Delete
PDU List Window

Simulation9: A wireless user from the first facility of first branch gets index.html file from the FTP server from third facility of first branch.

Domain name for FTP server was already created in DNS server. So by creating a file in the ftp server and connect it by using that domain name, we can get the file with -get- keyword in command prompt.





4. Conclusion

Analysis and tests on simulation show that topology and architecture selection is done correctly according to requirements. We note that the simulation has established the necessary networks for both local and global facilities in the tested Metropolitan Area Network. Overall, it has become clear that forming network architecture is not easy and often causes errors, whether in simulation or real life and that even a small mistake in real applications is not acceptable. If accidents take place, the possible problems and expenses have been understood. 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.

5. References

[1] Cisco, "Configuring VoIP phones using Cisco packet tracer (IP Telephony)" *YouTube*, Apr. 13, 2020. [Online]. Available: https://www.youtube.com/watch?v=TGMzUDE9XiU

[2] Tech Academy, "Cisco Packet Tracer Tutorial -Part 01 | Switch & end device connection," *YouTube*, Sep. 30, 2021. [Online]. Available: https://www.youtube.com/watch?v=YZRQpZPp4E4

[3] Network Kings, “Build a Basic Network - A Cisco Packet Tracer Tutorial" *YouTube*, Nov. 6, 2020. [Online]. Available: https://www.youtube.com/watch?v=TqWLJMt1dtQ

[4] Ajay Yadav, "How to Configure a Web Server in Cisco Packet Tracer," *YouTube*, Aug. 24, 2021. [Online]. Available: https://www.youtube.com/watch?v=qZB_biPOBwA

[5] DSR Network Solutions, "How to Configure DNS Server in Cisco Packet Tracer," *YouTube*, Jun. 18, 2021. [Online]. Available: https://www.youtube.com/watch?v=Iefd4BUcsLs

[6] DSR Network Solutions, "How to Configure HTTP and HTTPS in Cisco Packet Tracer," *YouTube*, Jun. 14, 2021. [Online]. Available: https://www.youtube.com/watch?v=lQ0AXwELLLM

[7] GeekyShows, "How to Configure FTP Server in Cisco Packet Tracer," *YouTube*, May 19, 2019. [Online]. Available: https://www.youtube.com/watch?v=_MxWcnNcCdE

[8] Tech Gurukul, "How to Configure Telnet in Cisco Packet Tracer," *YouTube*, May 13, 2020. [Online]. Available: https://www.youtube.com/watch?v=vyzvdbnOTXY

[9] DSR Network Solutions, "How to Configure SSH in Cisco Packet Tracer," *YouTube*, Jun. 15, 2021. [Online]. Available: https://www.youtube.com/watch?v=-_UabFPUVSo

[10] Network Kings, "How to Configure VLAN in Cisco Packet Tracer," *YouTube*, Nov. 12, 2020. [Online]. Available: https://www.youtube.com/watch?v=UrzKYKi8NEM

[11] Network Kings, "How to Configure Inter VLAN Routing in Cisco Packet Tracer," *YouTube*, Nov. 22, 2020. [Online]. Available: https://www.youtube.com/watch?v=rZw_b0wpQ00

[12] computernetworking747640215, "How to Configure an FTP Server in Packet Tracer," *WordPress*, Nov. 22, 2019. [Online]. Available: https://computernetworking747640215.wordpress.com/2019/11/22/how-to-configure-an-ftp-server-in-packet-tracer/

[13] GeeksforGeeks, "File Transfer Protocol (FTP) Server Configuration using Cisco Packet Tracer," *GeeksforGeeks*. [Online]. Available: https://www.geeksforgeeks.org/file-transfer-protocol-server-configuration-using-cisco-packet-tracer/