DE LA SALLE UNIVERSITY
GOKONGWEI COLLEGE OF ENGINEERING
DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING

Computer Networks and Security Lecture
(CONETSC)

Final Project Documentation

Title:

Enterprise Network of a Huawei IT Service Office

April 10, 2024
DATE PERFORMED

April 15, 2024
DATE SUBMITTED

Group No. 6

BONCODIN, CARL PATRICK Q.
CHUA, KENDRICK DAYLE J.
EVARISTO, GIER BRYANT J.
ONG, BRYCE ERWIN D.
SACDALAN, RAPHAEL CARLOS D.

Section: EQ1

ENGR. JUNE LORENZ E. CAPIN, ECT, MSc.
- Instructor -

I. Introduction

Network security and computer networks are major areas of relevance for the Enterprise Network project of the Huawei IT Service Office located in Makati City. The network created plays a pivotal role in enabling smooth communication across diverse departments by acting as a center for software development, IT consulting, project management, and technical support. Protecting sensitive data and maintaining network integrity requires implementing strong security measures due to the growing number of cyberattacks and data breaches. The project intends to create a robust digital ecosystem by balancing network efficiency and security. Optimizing organizational operations and reducing risk of unauthorized access are the primary goals of this project. It seeks to reinforce the resilience of the Huawei IT Service Office in an increasingly interconnected world.

II. Understanding Design Problem and Boundaries

Background Scenario

The Huawei building is a one-story building located in Makati City. It contained multiple departments inside the office. The company specializes in software development and IT services. With that, the primary departments included in the office were IT Network, Data Science, Human Resources, Sales, Quality Assurance, and Product Design. The office had approximately 150 employees who were scattered through the different departments mentioned above. Regarding the devices inside the whole office, it contained PCs, which were mostly in the IT consulting department so each room had separate access to a PC and the server while accommodating a customer. In the software development department, laptops were utilized. Through the network that was designed below, routers, wired and wireless, and servers were located in an efficient way, and connections and cabling were designed in each department.

Objectives

1. Configure Network Intermediary Devices (NIDs) while applying security best practices and device hardening features.
2. Implement an appropriate IPv4 addressing scheme (static and dynamic) and subnetting in both wireless and wired configurations.
3. Create VLANs and ensure trunking and InterVLAN connectivity across networks.
4. Construct Redundant Network Switching through STP & EtherChannel
5. Apply Static and Dynamic Routing, applying Load Balancing across multiple routes.
6. Configure Dedicated Servers (Web – DNS & HTTP, FTP, & Mail – SMTP & POP3) for Enterprise Use.

III. Approach Formulation

A. 20 PCs and 10 Mobile Devices (e.g. Laptops & Smartphones)

To accommodate a floor plan with at least 20 PCs, and 10 mobile devices, the group found a large floor plan with multiple rooms and tables that could accommodate the required number of PCs and Laptops.

B. 8 Layer 2 Switches & 2 Layer 3 Switches

The group divided the office floor plan into six departments where each department would contain at least one layer 2 switch. Since the project required the project to contain ether channels, the group was able to design a network where two departments would contain a total of three layer 2 switches and one layer 3 switch.

C. 5 Routers

As for the routers, two departments would contain, three-layer 2 switches which are in EtherChannel that is connected to the layer 3 switch. The group then decided that a router would be connected to the layer 3 switch. A total of four routers would be connected in a loop where one router would act as the backup router for IP routing. Another router that is connected to the servers would be connected to one of the routers.

D. 3 Wireless Routers/WAPs & 3 Servers

As for the wireless routers and servers, the group did not have a hard time as the only thing needed was to connect 3 servers to a router which would be connected to the departments while at least 2 or 3 wireless routers are placed in each department depending on the floor plan. The wireless routers are placed in conference rooms or the hallway.

IV. Network Design

A. Physical Topology

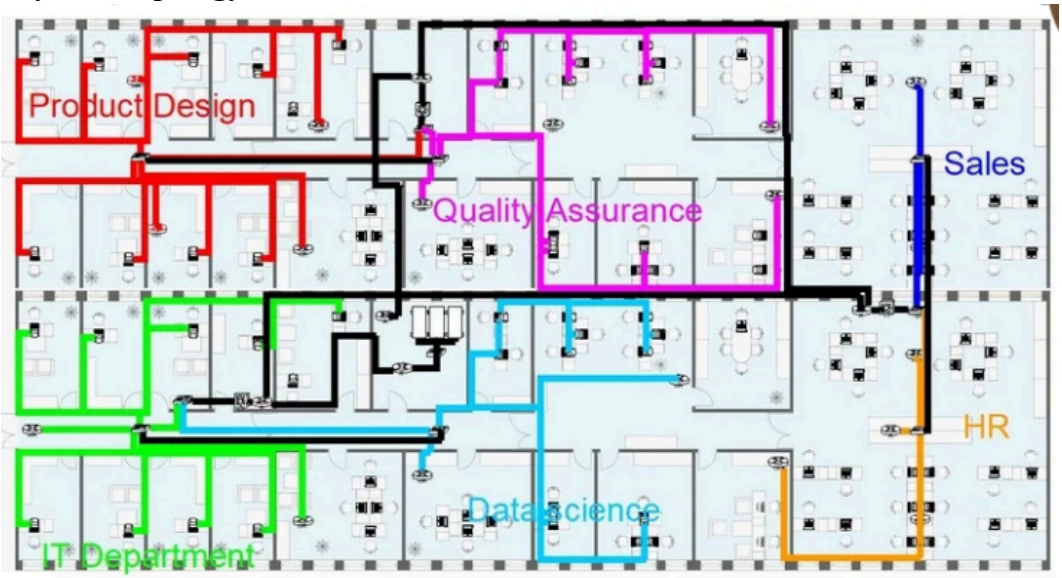

Figure 1. Physical Topology of the Network

The enterprise network's physical topology encompasses several departments: product design, quality assurance, sales, human resources, data science, and IT, with switches forming connections through the Internet or servers. All PCs and wireless connections are linked to switches, each delineated by distinct colors for ease of identification

B. Logical Topology

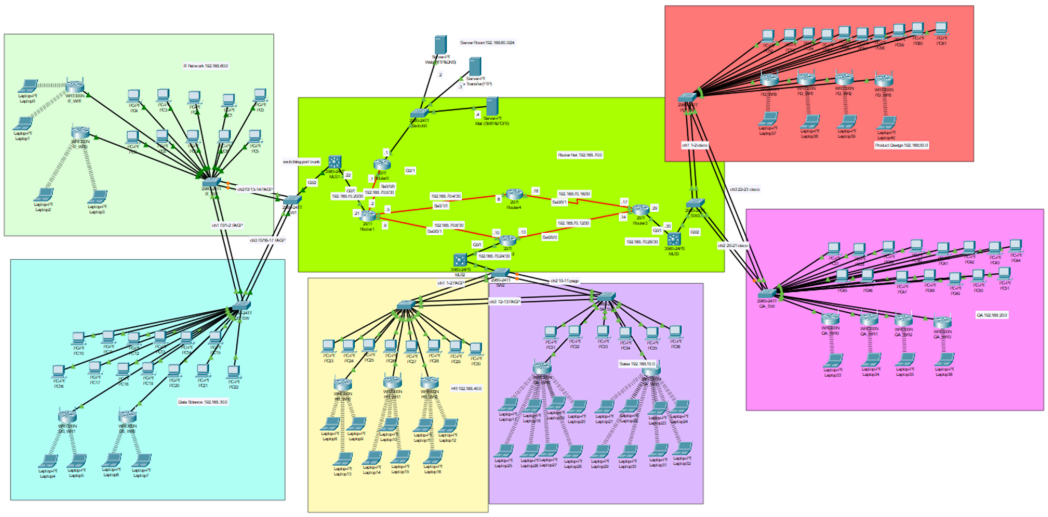

Figure 2. Logical Topology of the Network

Illustrating the network's logical topology, the IT department occupies the upper left, followed by the data science department in the lower left quadrant. The HR department is situated at the bottom-left corner, adjacent to the sales

department. Quality assurance finds placement in the bottom-right quadrant, while the product design department resides in the upper right. Routers occupy the middle, with servers positioned at the top.

C. Subnet Table and IP Addressing Tables

Subnet Description	# Hosts Needed	Network Address/CIDR	First Usable	Last Usable Host	Broadcast Address
Sales	24	192.168.10.0/24	192.168.10.1	192.168.10.254	192.168.10.255
QA	23	192.168.20.0/24	192.168.20.1	192.168.20.254	192.168.20.255
Data Science	20	192.168.30.0/24	192.168.30.1	192.168.30.254	192.168.30.255
HR	20	192.168.40.0/24	192.168.40.1	192.168.40.254	192.168.40.255
Product Design	18	192.168.50.0/24	192.168.50.1	192.168.50.254	192.168.50.255
IT Department	16	192.168.60.0/24	192.168.60.1	192.168.60.254	192.168.60.255
Router Net	12	192.168.70.0/24	192.168.70.1	192.168.70.254	192.168.70.255
Server Room	5	192.168.80.0/24	192.168.80.1	192.168.80.254	192.168.80.255

Figure 3. Subnet Table of the Network

Router 0	Se0/0/0	192.168.70.1	255.255.255.252	NA
	G0/1	192.168.80.1	255.255.255.0	NA
Router 1	Se0/0/0	192.168.70.2	255.255.255.252	NA
	Se0/0/1	192.168.70.9	255.255.255.252	NA
	Se0/1/1	192.168.70.5	255.255.255.252	NA
	G0/1	192.168.70.21	255.255.255.252	NA
Router 2	Se0/0/0	192.168.70.13	255.255.255.252	NA
	Se0/0/1	192.168.70.10	255.255.255.252	NA
	G0/1	192.168.70.25	255.255.255.252	NA
Router 3	Se0/0/0	192.168.70.14	255.255.255.252	NA
	Se0/0/1	192.168.70.17	255.255.255.252	NA
	G0/1	192.168.70.29	255.255.255.252	NA
Router 4	Se0/0/1	192.168.70.18	255.255.255.252	NA
	Se0/1/1	192.168.70.6	255.255.255.252	NA
Web		192.168.80.2	255.255.255.0	192.168.80.1
FTP		192.168.80.3	255.255.255.0	192.168.80.1
Mail		192.168.80.4	255.255.255.0	192.168.80.1
MLSW1	G0/1	192.168.70.22	255.255.255.252	NA
	VLAN30	192.168.30.1	255.255.255.0	NA
	VLAN60	192.168.60.1	255.255.255.0	NA
MLSW2	G0/1	192.168.70.26	255.255.255.252	NA
	VLAN40	192.168.40.1	255.255.255.0	NA
	VLAN10	192.168.10.1	255.255.255.0	NA
MLSW3	G0/1	192.168.70.30	255.255.255.252	NA
	VLAN20	192.168.20.1	255.255.255.0	NA
	VLAN50	192.168.50.1	255.255.255.0	NA

Figure 4. Addressing Table of Server Room and Router

PC0	NIC	192.168.60.2	255.255.255.0	192.168.60.1
PC1	NIC	192.168.60.3	255.255.255.0	192.168.60.1
PC2	NIC	192.168.60.4	255.255.255.0	192.168.60.1
PC3	NIC	192.168.60.5	255.255.255.0	192.168.60.1
PC4	NIC	192.168.60.6	255.255.255.0	192.168.60.1
PC5	NIC	192.168.60.7	255.255.255.0	192.168.60.1
PC6	NIC	192.168.60.8	255.255.255.0	192.168.60.1
PC7	NIC	192.168.60.9	255.255.255.0	192.168.60.1
PC8	NIC	192.168.60.10	255.255.255.0	192.168.60.1
PC9	NIC	192.168.60.11	255.255.255.0	192.168.60.1
IT_WR0	LAN	192.168.60.12	255.255.255.0	192.168.60.1
IT_WR1	LAN	192.168.60.43	255.255.255.0	192.168.60.1
Laptop 0	NIC	192.168.60.13	255.255.255.0	192.168.60.1
Laptop 1	NIC	192.168.60.14	255.255.255.0	192.168.60.1
Laptop 2	NIC	192.168.60.15	255.255.255.0	192.168.60.1
Laptop 3	NIC	192.168.60.16	255.255.255.0	192.168.60.1
VLAN 60	NIC	192.168.60.254	255.255.255.0	192.168.60.1

Figure 5. Addressing Table of IT Department

PC10	NIC	192.168.30.2	255.255.255.0	192.168.30.1
PC11	NIC	192.168.30.3	255.255.255.0	192.168.30.1
PC12	NIC	192.168.30.4	255.255.255.0	192.168.60.1
PC13	NIC	192.168.30.5	255.255.255.0	192.168.60.1
PC14	NIC	192.168.30.6	255.255.255.0	192.168.60.1
PC15	NIC	192.168.30.7	255.255.255.0	192.168.60.1
PC16	NIC	192.168.30.8	255.255.255.0	192.168.60.1
PC17	NIC	192.168.30.9	255.255.255.0	192.168.60.1
PC18	NIC	192.168.30.10	255.255.255.0	192.168.60.1
PC19	NIC	192.168.30.11	255.255.255.0	192.168.60.1
PC20	NIC	192.168.30.12	255.255.255.0	192.168.60.1
PC21	NIC	192.168.30.13	255.255.255.0	192.168.60.1
PC22	NIC	192.168.30.14	255.255.255.0	192.168.60.1
DS_WR0	LAN	192.168.30.15	255.255.255.0	192.168.60.1
DS_WR1	LAN	192.168.30.46	255.255.255.0	192.168.60.1
Laptop 4	NIC	192.168.30.16	255.255.255.0	192.168.60.1
Laptop 5	NIC	192.168.30.17	255.255.255.0	192.168.60.1
Laptop 6	NIC	192.168.30.18	255.255.255.0	192.168.60.1
Laptop 7	NIC	192.168.30.19	255.255.255.0	192.168.60.1
VLAN 30	NIC	192.168.30.254	255.255.255.0	192.168.60.1

Figure 6. Addressing Table of Data Science Department

PC23	NIC	192.168.40.2	255.255.255.0	192.168.40.1
PC24	NIC	192.168.40.3	255.255.255.0	192.168.40.1
PC25	NIC	192.168.40.4	255.255.255.0	192.168.40.1
PC26	NIC	192.168.40.5	255.255.255.0	192.168.40.1
PC27	NIC	192.168.40.6	255.255.255.0	192.168.40.1
PC28	NIC	192.168.40.7	255.255.255.0	192.168.40.1
PC29	NIC	192.168.40.8	255.255.255.0	192.168.40.1
PC30	NIC	192.168.40.9	255.255.255.0	192.168.40.1
HR_WR0	LAN	192.168.40.10	255.255.255.0	192.168.40.1
HR_WR1	LAN	192.168.40.41	255.255.255.0	192.168.40.1
HR_WR2	LAN	192.168.40.72	255.255.255.0	192.168.40.1
Laptop 8	NIC	192.168.40.11	255.255.255.0	192.168.40.1
Laptop 9	NIC	192.168.40.12	255.255.255.0	192.168.40.1
Laptop 10	NIC	192.168.40.13	255.255.255.0	192.168.40.1
Laptop 11	NIC	192.168.40.14	255.255.255.0	192.168.40.1
Laptop 12	NIC	192.168.40.15	255.255.255.0	192.168.40.1
Laptop 13	NIC	192.168.40.42	255.255.255.0	192.168.40.1
Laptop 14	NIC	192.168.40.43	255.255.255.0	192.168.40.1
Laptop 15	NIC	192.168.40.44	255.255.255.0	192.168.40.1
Laptop 16	NIC	192.168.40.45	255.255.255.0	192.168.40.1
VLAN 40	NIC	192.168.40.254	255.255.255.0	192.168.40.1

Figure 7. Addressing Table of HR Department

PC31	NIC	192.168.10.2	255.255.255.0	192.168.40.1
PC32	NIC	192.168.10.3	255.255.255.0	192.168.40.1
PC33	NIC	192.168.10.4	255.255.255.0	192.168.40.1
PC34	NIC	192.168.10.5	255.255.255.0	192.168.40.1
PC35	NIC	192.168.10.6	255.255.255.0	192.168.40.1
PC36	NIC	192.168.10.7	255.255.255.0	192.168.40.1
SA_WR0	LAN	192.168.10.8	255.255.255.0	192.168.40.1
SA_WR1	LAN	192.168.10.39	255.255.255.0	192.168.40.1
Laptop 17	NIC	192.168.10.9	255.255.255.0	192.168.40.1
Laptop 18	NIC	192.168.10.10	255.255.255.0	192.168.40.1
Laptop 19	NIC	192.168.10.11	255.255.255.0	192.168.40.1
Laptop 20	NIC	192.168.10.12	255.255.255.0	192.168.40.1
Laptop 21	NIC	192.168.10.13	255.255.255.0	192.168.40.1
Laptop 22	NIC	192.168.10.14	255.255.255.0	192.168.40.1
Laptop 23	NIC	192.168.10.15	255.255.255.0	192.168.40.1
Laptop 24	NIC	192.168.10.16	255.255.255.0	192.168.40.1
Laptop 25	NIC	192.168.10.40	255.255.255.0	192.168.40.1
Laptop 26	NIC	192.168.10.41	255.255.255.0	192.168.40.1
Laptop 27	NIC	192.168.10.42	255.255.255.0	192.168.40.1
Laptop 28	NIC	192.168.10.43	255.255.255.0	192.168.40.1
Laptop 29	NIC	192.168.10.44	255.255.255.0	192.168.40.1
Laptop 30	NIC	192.168.10.45	255.255.255.0	192.168.40.1
Laptop 31	NIC	192.168.10.46	255.255.255.0	192.168.40.1
Laptop 32	NIC	192.168.10.47	255.255.255.0	192.168.40.1
VLAN 10	NIC	192.168.10.254	255.255.255.0	192.168.40.1

Figure 8. Addressing Table of Sales Department

PC 37	NIC	192.168.20.2	255.255.255.0	192.168.20.1
PC 38	NIC	192.168.20.3	255.255.255.0	192.168.20.1
PC 39	NIC	192.168.20.4	255.255.255.0	192.168.20.1
PC 40	NIC	192.168.20.5	255.255.255.0	192.168.20.1
PC 41	NIC	192.168.20.6	255.255.255.0	192.168.20.1
PC 42	NIC	192.168.20.7	255.255.255.0	192.168.20.1
PC 43	NIC	192.168.20.8	255.255.255.0	192.168.20.1
PC 44	NIC	192.168.20.9	255.255.255.0	192.168.20.1
PC 45	NIC	192.168.20.10	255.255.255.0	192.168.20.1
PC 46	NIC	192.168.20.11	255.255.255.0	192.168.20.1
PC 47	NIC	192.168.20.12	255.255.255.0	192.168.20.1
PC 48	NIC	192.168.20.13	255.255.255.0	192.168.20.1
PC 49	NIC	192.168.20.14	255.255.255.0	192.168.20.1
PC 50	NIC	192.168.20.15	255.255.255.0	192.168.20.1
PC 51	NIC	192.168.20.16	255.255.255.0	192.168.20.1
QA_WR0	LAN	192.168.20.17	255.255.255.0	192.168.20.1
QA_WR1	LAN	192.168.20.48	255.255.255.0	192.168.20.1
QA_WR2	LAN	192.168.20.79	255.255.255.0	192.168.20.1
QA_WR3	LAN	192.168.20.110	255.255.255.0	192.168.20.1
Laptop 33	NIC	192.168.20.18	255.255.255.0	192.168.20.1
Laptop 34	NIC	192.168.20.19	255.255.255.0	192.168.20.1
Laptop 35	NIC	192.168.20.20	255.255.255.0	192.168.20.1
Laptop 36	NIC	192.168.20.21	255.255.255.0	192.168.20.1
VLAN 20	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Figure 9. Addressing Table of Quality Assurance Department

PC 52	NIC	192.168.50.2	255.255.255.0	192.168.20.1
PC 53	NIC	192.168.50.3	255.255.255.0	192.168.20.1
PC 54	NIC	192.168.50.4	255.255.255.0	192.168.20.1
PC 55	NIC	192.168.50.5	255.255.255.0	192.168.20.1
PC 56	NIC	192.168.50.6	255.255.255.0	192.168.20.1
PC 57	NIC	192.168.50.7	255.255.255.0	192.168.20.1
PC 58	NIC	192.168.50.8	255.255.255.0	192.168.20.1
PC 59	NIC	192.168.50.9	255.255.255.0	192.168.20.1
PC 60	NIC	192.168.50.10	255.255.255.0	192.168.20.1
PC 61	NIC	192.168.50.11	255.255.255.0	192.168.20.1
PD_WR0	LAN	192.168.50.12	255.255.255.0	192.168.20.1
PD_WR1	LAN	192.168.50.43	255.255.255.0	192.168.20.1
PD_WR2	LAN	192.168.50.74	255.255.255.0	192.168.20.1
PD_WR3	LAN	192.168.50.105	255.255.255.0	192.168.20.1
Laptop 37	NIC	192.168.50.13	255.255.255.0	192.168.20.1
Laptop 38	NIC	192.168.50.14	255.255.255.0	192.168.20.1
Laptop 39	NIC	192.168.50.15	255.255.255.0	192.168.20.1
Laptop 40	NIC	192.168.50.16	255.255.255.0	192.168.20.1
VLAN 50	NIC	192.168.50.254	255.255.255.0	192.168.20.1

Figure 10. Addressing Table of Product Design Department

IT_SW	VLAN 99	192.168.99.1	255.255.255.0	
SW1	VLAN 99	192.168.99.2	255.255.255.0	
DS_SW	VLAN 99	192.168.99.3	255.255.255.0	
MLS1	VLAN 99	192.168.99.4	255.255.255.0	
HR_SW	VLAN 99	192.168.99.5	255.255.255.0	
SA_SW	VLAN 99	192.168.99.6	255.255.255.0	
SW2	VLAN 99	192.168.99.7	255.255.255.0	
MLS2	VLAN 99	192.168.99.8	255.255.255.0	
QA_SW	VLAN 99	192.168.99.9	255.255.255.0	
PD_SW	VLAN 99	192.168.99.10	255.255.255.0	
SW3	VLAN 99	192.168.99.11	255.255.255.0	
MLS3	VLAN 99	192.168.99.12	255.255.255.0	

Figure 11. Addressing Table of VLAN 99

IP addressing involves assigning unique numerical labels to network devices to facilitate communication, while subnetting partitions a larger network into smaller, manageable subnetworks. There are a total of eight subnets, one for each department, one for the network of routers, and one for the servers.

D. EtherChannel

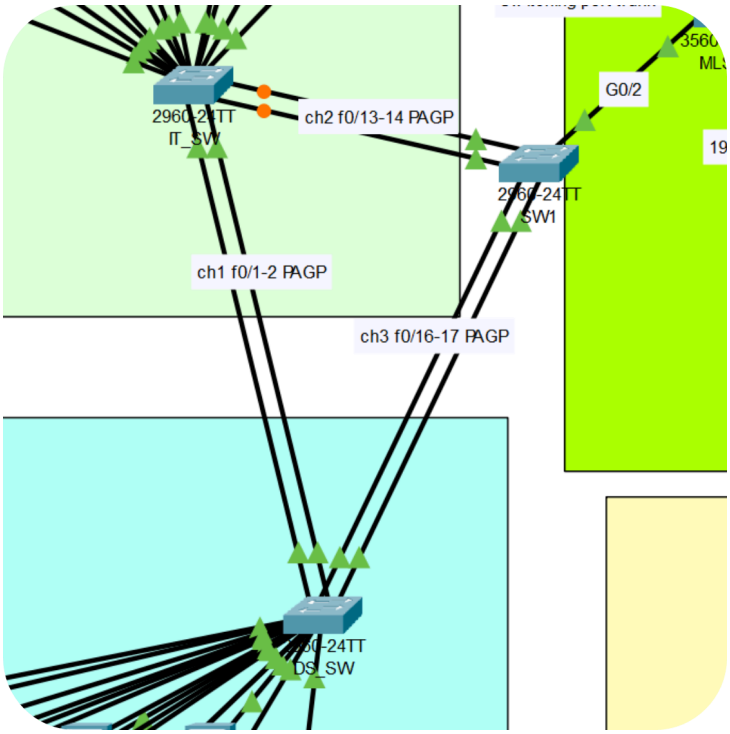

Figure 12. EtherChannel of the Network

EtherChannel, also known as port bundling or link aggregation, is a networking technology that allows multiple physical Ethernet links to be combined into a single logical interface. This aggregated link offers increased bandwidth, higher availability, and improved load balancing across the member links. Additionally, it provides redundancy and fault tolerance, as if one link fails, traffic can automatically fail over to the remaining active links in the bundle, ensuring continuous connectivity. PAgP (Port Aggregation Protocol), a Cisco proprietary protocol, was used to aggregate interfaces to form EtherChannels in the STP network.

E. Spanning-Tree Protocol

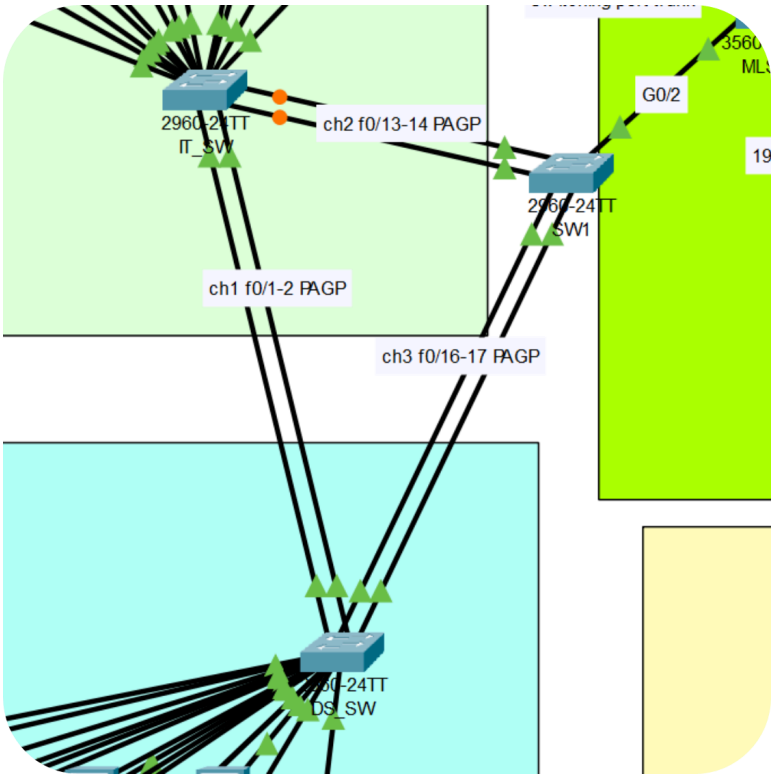

Figure 13. Spanning-Tree Protocol used in EtherChannel

Spanning Tree Protocol (STP) is a network protocol used to prevent loops in Ethernet networks by dynamically shutting down redundant paths while maintaining a loop-free topology. PVST is the STP protocol used. Per-VLAN Spanning Tree (PVST) creates a separate spanning tree instance for each VLAN, allowing for finer control over network traffic and redundancy while ensuring that loops are prevented at the VLAN level. As seen in Figure 13, the switch for the Data Science department was chosen as the root bridge which resulted in channel 2 being blocked. The Bridge ID was then set to 4096 to set the switch was a root bridge.

F. Inter-VLAN Routing

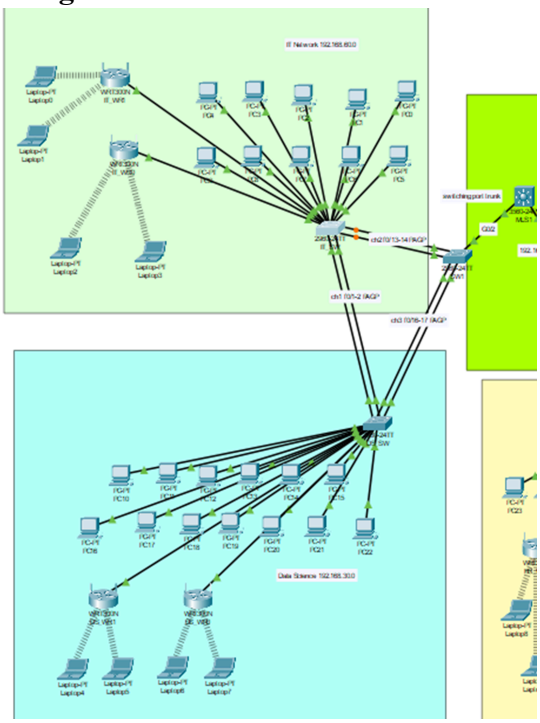

Figure 14. Inter-VLAN Routing on VLANs 30 and 60

Inter-VLAN routing is the process of forwarding traffic between different VLANs (Virtual Local Area Networks) within a network. MLS (Multilayer Switching) is a Cisco technology that enables high-performance routing between VLANs directly within a Layer 3 switch. A Multi-layer Switch was connected to the L2 switch which was used for the two VLANs for IT and Data Science. The segment connected to the switch was set to a trunk while the segment connected to the Router acted like a L3 switch due to IP routing being enabled.

G. Static and Dynamic Routing

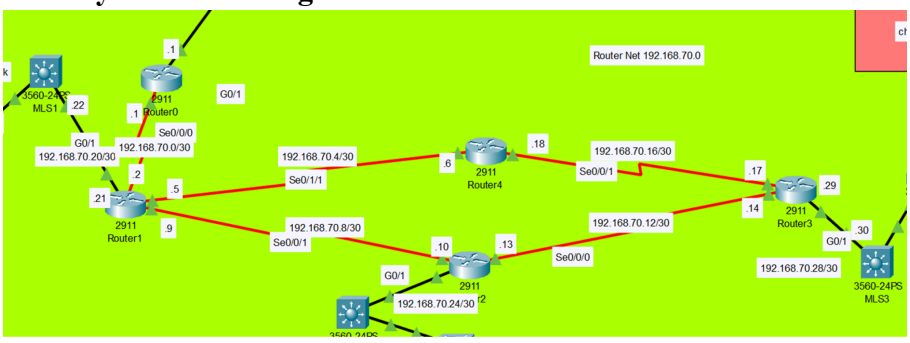

Figure 15. Implementation of Static and Dynamic Routing on Routers

Static routing involves manually configuring the routing table on routers or network devices to specify the paths that packets should follow. Dynamic routing protocols automate the process of updating routing tables by allowing

routers to communicate with each other to share information about network topology and determine the best paths for packet forwarding. OSPF (Open Shortest Path First), a dynamic routing protocol, was used on top of static routing.

H. Server Room

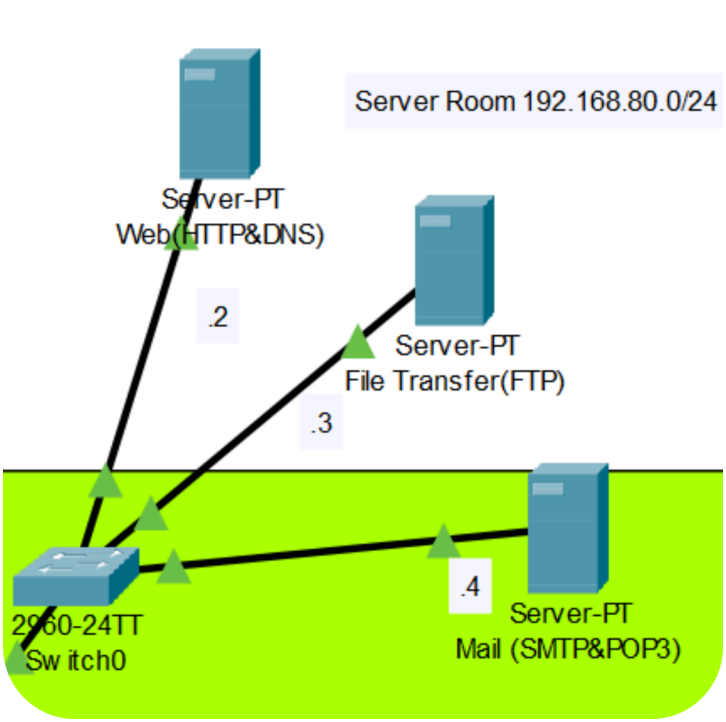

Figure 16. HTTP & DNS, FTP, and SMTP Servers

HTTP is the protocol used for transmitting hypermedia documents, such as web pages, over the internet. DNS is used to translate human-readable domain names into IP addresses. FTP (File Transfer Protocol) is a standard network protocol used for transferring files between a client and a server. SMTP is a protocol used for sending outgoing emails from a client to a mail server or between mail servers. POP3 is a protocol used for retrieving incoming emails from a mail server to a client device.

V. Attainment of Objectives

A. Configure Network Intermediary Devices (NIDs) while applying security best practices and device hardening features.

To enhance security in the system. all routers and switches are configured with passwords and these are implemented for both the console line and privileged mode. When the *show run* command is executed, these passwords are encrypted, to protect them from unauthorized viewing. Additionally, a MOTD or message of the day will be displayed upon accessing the device stating “This is a secure system. Authorized Access Only!”. the console password for all devices is

set as *consoleAdmin*, while *consoleEnable* serves as the password for privileged mode. Any unused ports on routers and switches are disabled to apply device hardening features.

B. Implement an appropriate IPv4 addressing scheme (static and dynamic) and subnetting in both wireless and wired configurations.

In setting up the IPv4 addressing scheme, all PC or wired connection devices are configured to static IP addresses, while for the laptops or wireless devices, dynamic IP addresses or DHCP are utilized. Referring to the addressing table provided in the previous section, each device is allocated to a specific IP address and subnet mask. In configuring the wireless router, the SSID is appropriately named after the router itself. The SSID of the router becomes visible when a wireless device attempts to connect to the router. Additionally, each wireless router is set up with a password to ensure that only authorized users can connect to the router. The password for all routers is *ciscoPass*. All wireless routers can connect to a maximum of 30 numbers of users dynamically. This means that the router will dynamically assign the IP addresses of the connected devices.

C. Create VLANs and ensure trunking and InterVLAN connectivity across networks.

In the network enterprise, there are 6 VLANs for the departments, ranging 10-60. VLAN 70 is set for the router network, VLAN 80 for servers, and VLAN 99 for native trunking. The IT network department and data science share one inter-VLAN, while HR and sales are grouped within another inter-VLAN. Similarly, QA and product design are categorized under a single inter-VLAN. The multilayer switches will act as a router and will be trunked and connected to the primary switch in order for the inter-vlan to connect.

D. Construct Redundant Network Switching through STP & EtherChannel

In implementing the STP and EtherChannels, it is important to make sure that the layer three switches are connected to the primary switch of the loop. They must be configured as trunks. Each channel in the loop are connected with 2 copper straight-through cables and all modes of channel groups in the switches are set to desired. The switch that is opposite to the primary switch will have the channel groups configured as passive. This ensured that STP and EtherChannels were implemented. Testing can be done through the simulation where data packets can be traced when sent and received.

E. Apply Static and Dynamic Routing, applying Load Balancing across multiple routes.

In our network setup, we use both static and dynamic routing across routers and multilayer switches for efficient traffic management. Static routing provides precise control over predetermined paths, while dynamic protocols like OSPF adapt to changes in network topology, enhancing scalability. Multilayer switches operate at both Layer 2 and Layer 3, combining routing and switching functions for optimized performance. We configure static routes for specific network segments like IT, Data Science, etc., and maintain IP addresses of adjacent hops in each switch for efficient packet forwarding.

F. Configure Dedicated Servers (Web – DNS & HTTP, FTP, & Mail – SMTP & POP3) for Enterprise Use.

For Web services, both DNS and HTTP have been enabled. The DNS server is assigned the IP address 192.168.80.2 and is named packettracer.com. This ensures efficient domain name resolution within the network. The HTTP service is also enabled, allowing users to access web content hosted on the servers. FTP (File Transfer Protocol) has been set up on every PC from PC0 to PC61. Users can access the FTP servers using the password "1234" for easy testing. They are granted privileges for writing, reading, deleting, renaming, and listing files, ensuring smooth file transfer operations. Furthermore, Mail services including SMTP (Simple Mail Transfer Protocol) and POP3 (Post Office Protocol version 3) have been enabled. The domain name for email communication is set to packettracer.com. This facilitates efficient email exchange within the enterprise network.

VI. Network Simulation

Configuration of Network Intermediary Devices (NIDs) and application security best practices and device hardening features.

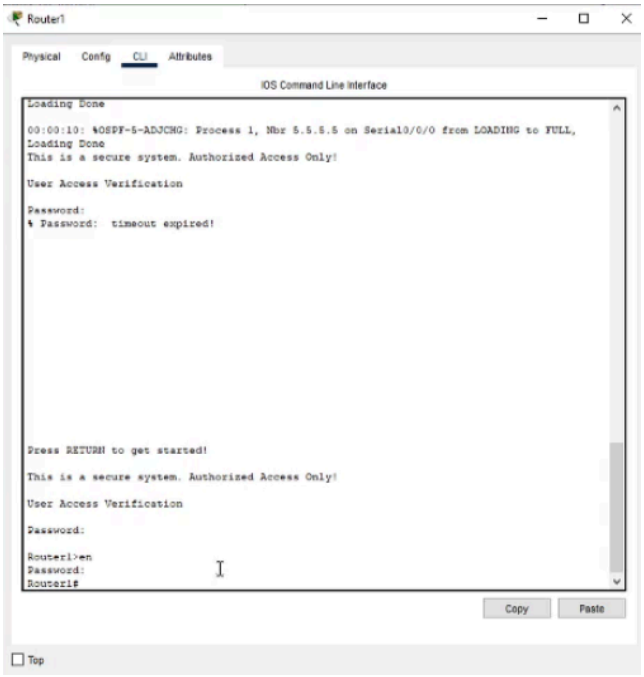

Figure 17. Simulation of line console and privileged mode password

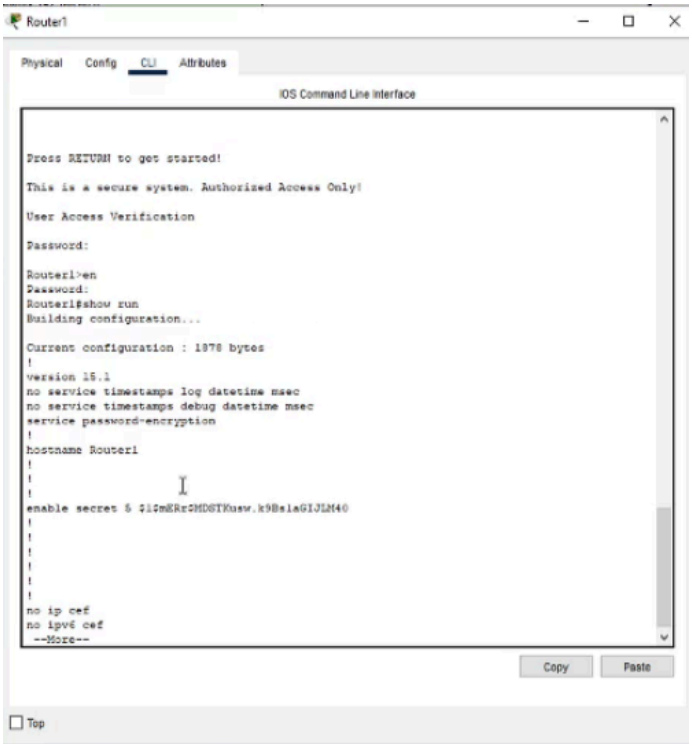

Figure 18. Simulation of encryption of passwords

The first objective of applying security measures to the routers and switches is demonstrated, with Router 1 serving as an illustration. The router password, "console Admin", is already configured. Additionally, a password is required to access the privilege mode, set as "console enable". Both passwords are encrypted for added security, as evidenced by the command show run.

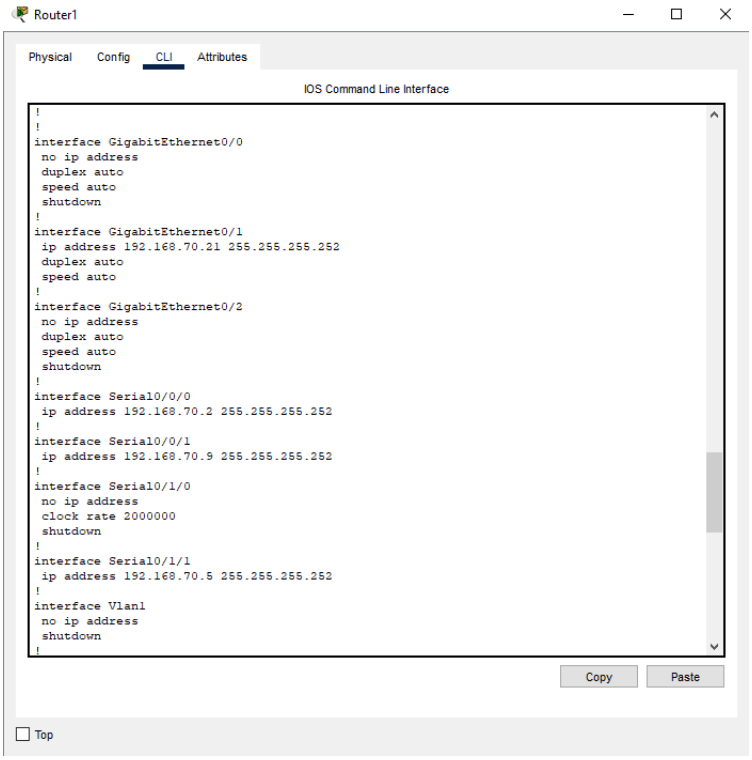

Figure 19. Shut Down Unused Ports

To ensure device hardening, all unused ports of the routers and switches are deactivated or shut down as evident in the command show run.

Implementation of an appropriate IPv4 addressing scheme (static and dynamic) and subnetting in both wireless and wired configurations.

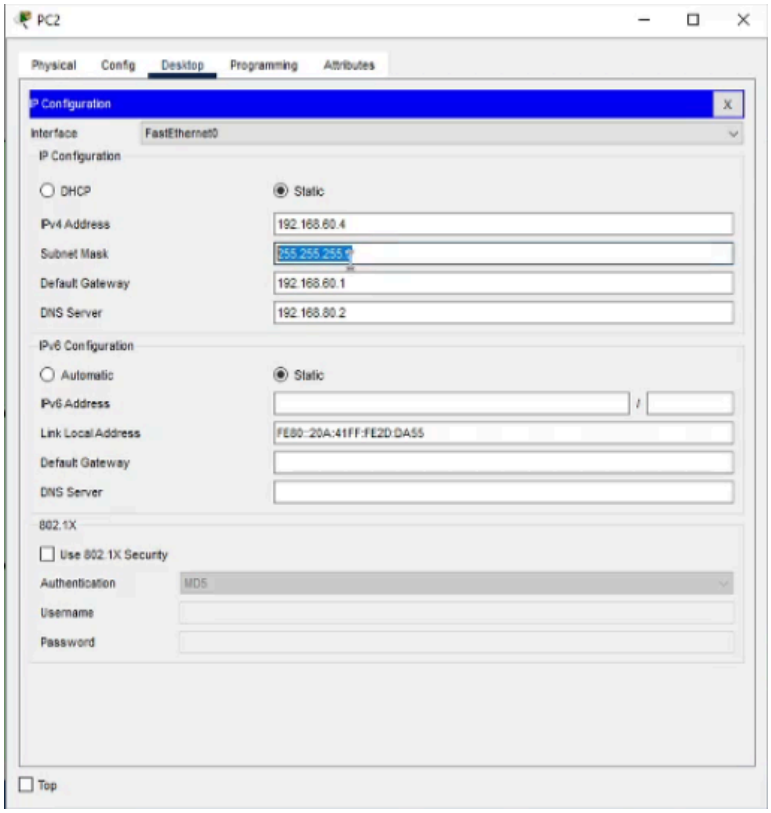

Figure 20. PC2 Subnet Mask

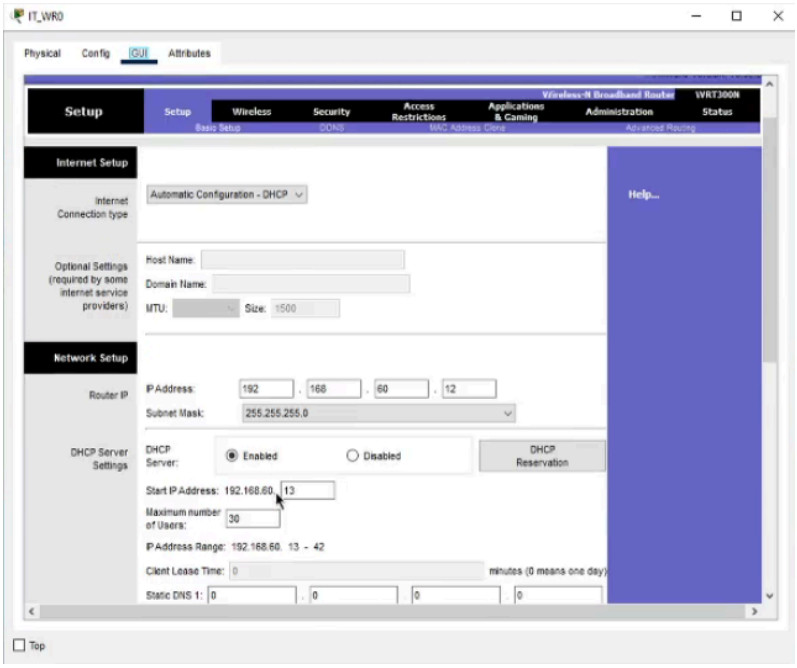

Figure 21. Wireless Configuration Setup

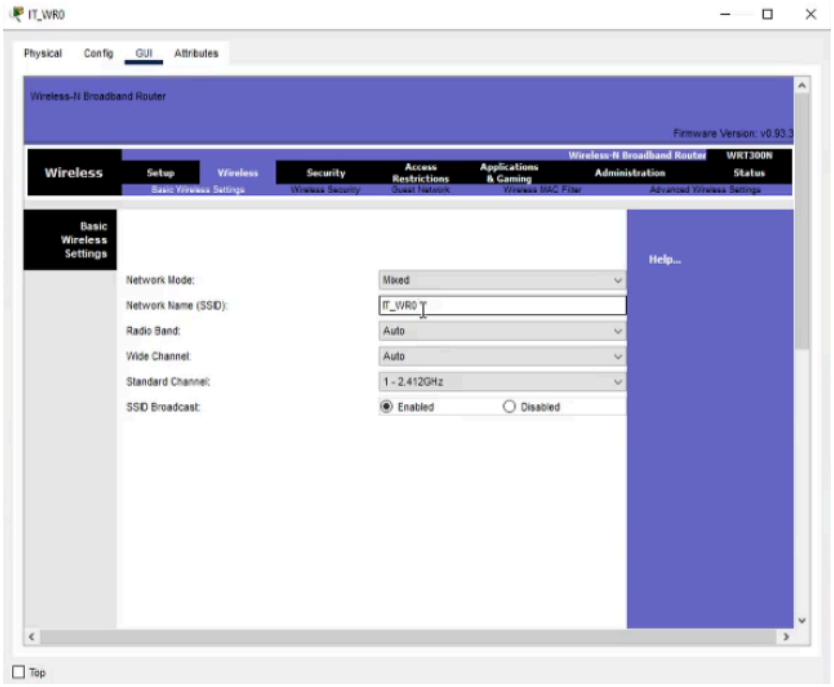

Figure 22. Wireless Configuration

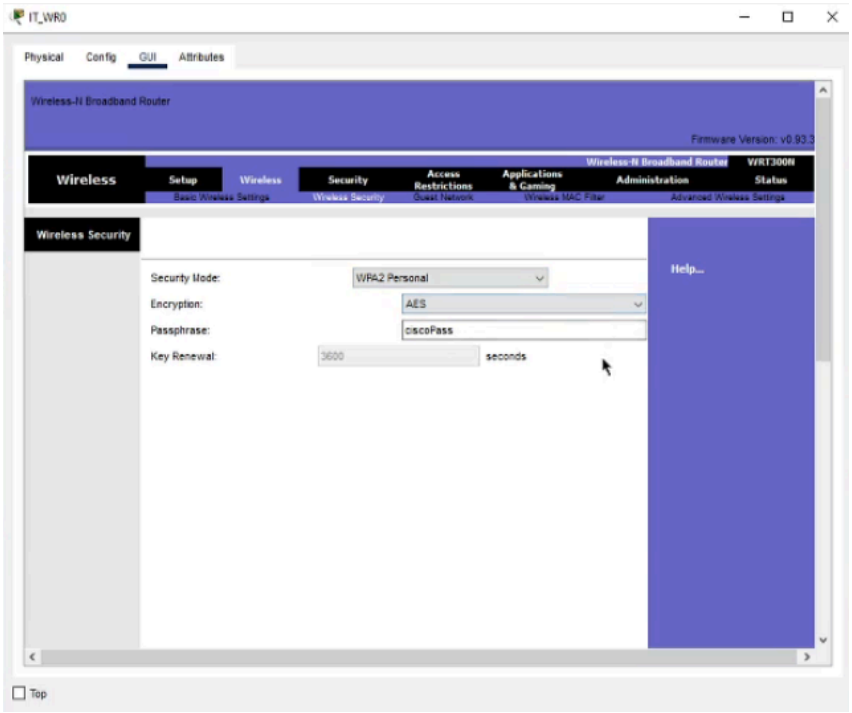

Figure 23. Wireless Configuration

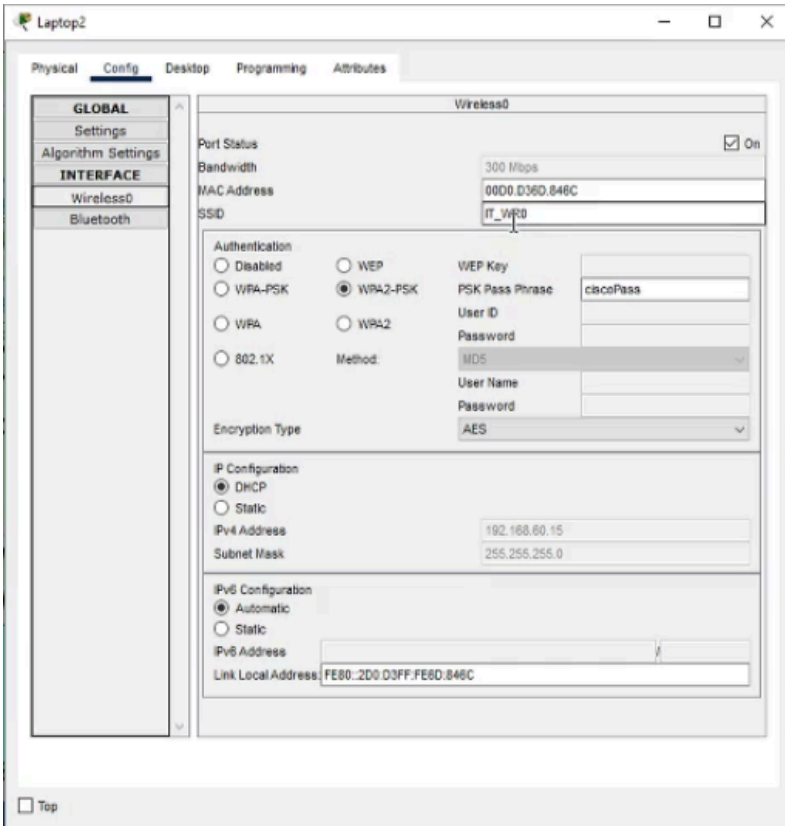

Figure 24. Laptop 2 wireless Configuration

The implementation of an IPv4 addressing scheme involves both static and dynamic addressing, as well as subnetting, in both wired and wireless configurations. In our enterprise setup, PCs are configured with static addresses, while laptops and wireless devices utilize dynamic addressing through DHCP. As an example, setting the IP address for PC2 to 192.168.60.4 with a subnet mask of 255.255.255.0.

In the wireless configuration, the students adopted a dynamic IP addressing scheme, also known as DHCP. They configured a wireless router with the IP address 192.168.60.12, with DHCP server functionality enabled. Subsequently, wireless devices connecting to this router are assigned IP addresses within the range of 192.168.60.13 to 192.168.60.42. Upon connection establishment, the router dynamically allocates IP addresses to the associated wireless devices within this specified range.

Development of VLANs and implementation of trunking and InterVLAN connectivity across networks.

VLAN	NAME	INTERFACE
VLAN 10	Sales	PD_SW: VLAN 10
VLAN 20	Quality Assurance	QA_SW: VLAN 20
VLAN 30	Data Science	DS_SW: VLAN 30
VLAN 40	Human Resources	HR_SW: VLAN 40
VLAN 50	Product Design	PD_SW: VLAN 50
VLAN 60	IT Network	IT_SW: VLAN 60
VLAN 99	Native	N/A

Figure 14. VLAN Table

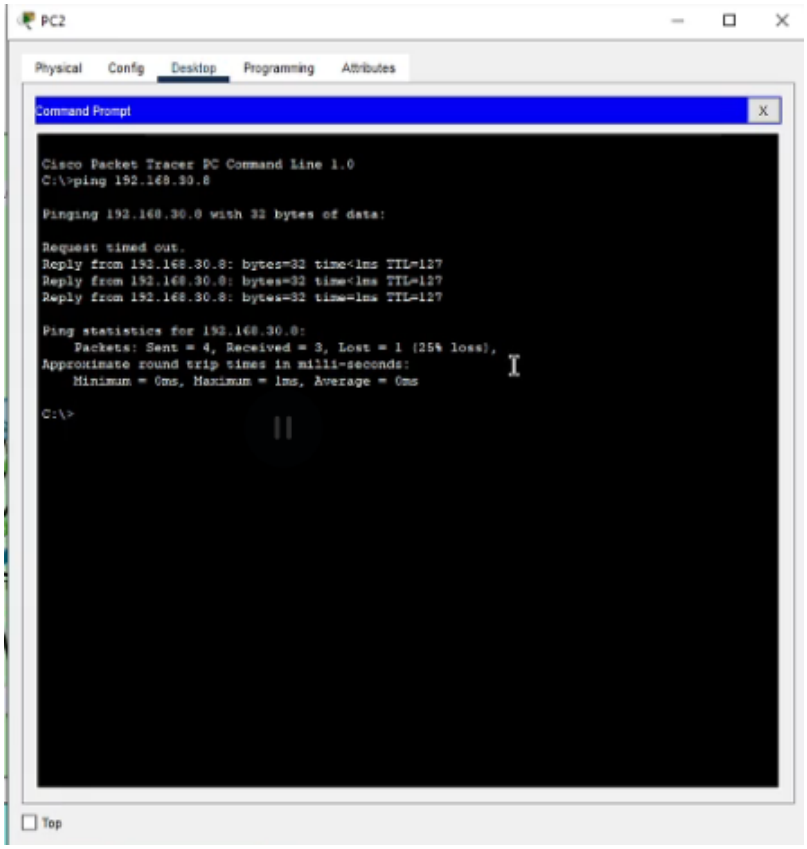

Figure 25. Inter-VLAN Testing

The next objective involves the creation of Virtual Local Area Networks (VLANs) to segregate network traffic and ensure efficient network management. Additionally, trunking and inter-VLAN connectivity across distinct network segments are prioritized. Each department within the network infrastructure is assigned to a specific VLAN, delineating network segmentation.

The IT network department corresponds to VLAN 60, data science to VLAN 30, HR to VLAN 40, sales to VLAN 10, QA to VLAN 20, and product design to VLAN 50. To validate the efficacy of inter-VLAN connectivity, the students attempt to ping a PC from the IT network department to a PC from the data science department. This objective serves as a demonstration of seamless communication across VLANs. The process commences with the acquisition of the IP address of a PC within the data science department. Utilizing PC2 as an example, the students simulated ping communication with PC16, located within the data science department.

Implementation of Redundant Network Switching through STP & EtherChannel

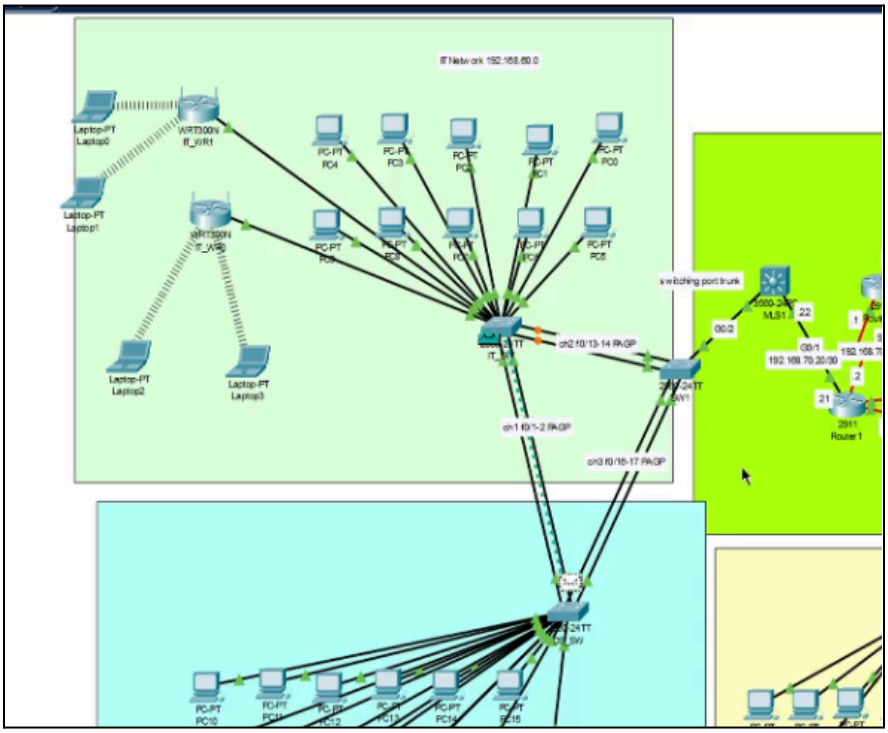

Figure 26. Logical Topology Simulation

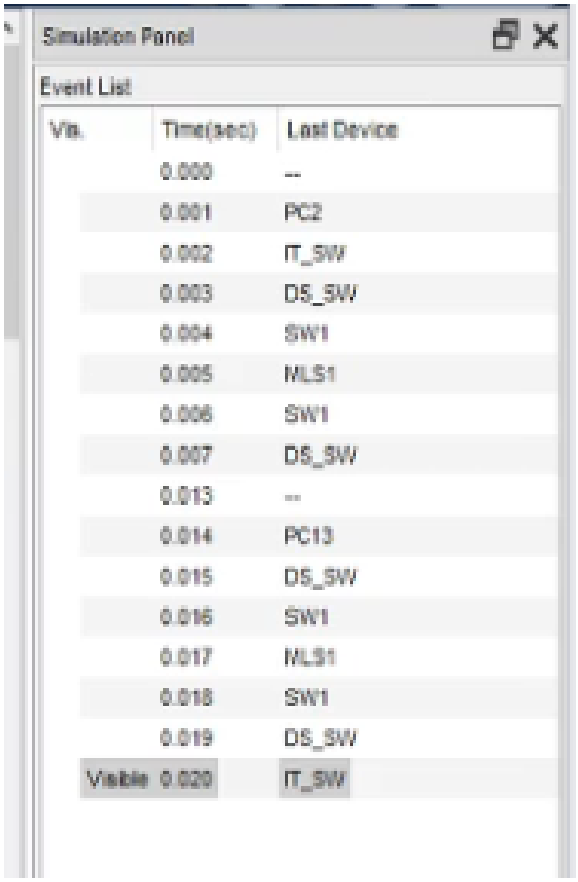

Figure 27. Simulation Panel

The deployment of redundant network switching, facilitated by Spanning Tree Protocol (STP) and EtherChannel, ensures robust network resilience. In the network topology illustrated, the orange interface denotes the alternative port, currently in a blocked state, designated as channel 2. Notably, EtherChannel configuration enables the aggregation of multiple physical links into a single logical channel, optimizing bandwidth utilization and enhancing network reliability. Subsequently, a simulation is conducted to show the packet propagation through the EtherChannels. This simulation serves to determine the operational dynamics of EtherChannel configuration in the network environment.

Implementation of Static and Dynamic Routing and application Load Balancing across multiple routes.

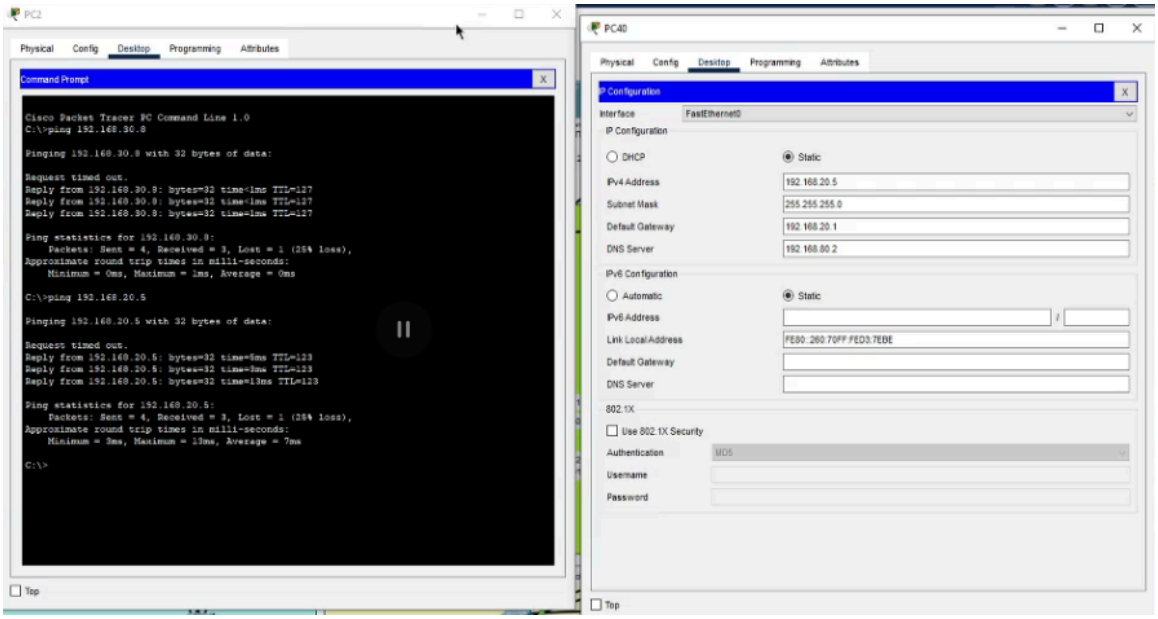

Figure 28. Pinging PC40 using PC2

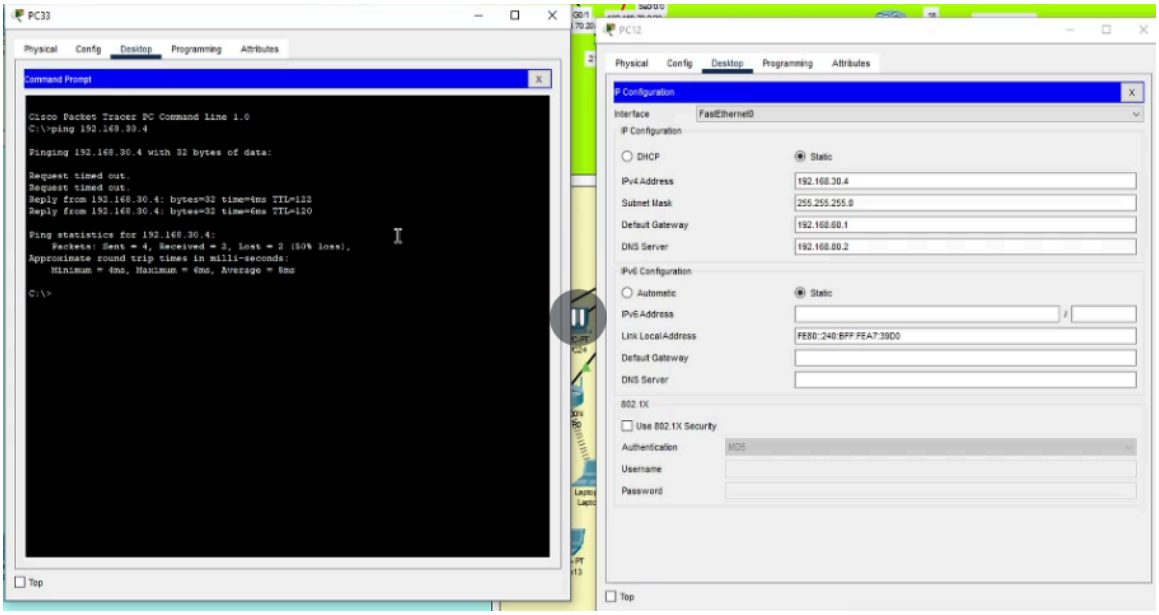

Figure 29. Pinging PC12 using PC33

The next objective entails the implementation of static and dynamic routing mechanisms alongside load-balancing strategies across diverse routes. To demonstrate this, any PC within the IT network department can be utilized to ping any PC within the QA department. This simulation illustrates the ability of PCs within the IT network department to establish communication with other departments, necessitating

connectivity via the router. Initially, the IP address of a PC within the QA department is obtained, such as PC40. Afterward, a ping operation is initiated, targeting the IP address 192.168.20.5 associated with PC40. Upon successful completion of the ping operation, confirming connectivity with PC40, the students proceed to utilize a PC from the sales department, specifically PC33, to initiate a similar ping operation.

Configuration of dedicated Servers (Web – DNS & HTTP, FTP, & Mail – SMTP & POP3) for Enterprise Use.

For the web server, HTTP and HTTPS must be enabled, as well as the DNS Service. All website names are recorded under the DNS tab with their website name, tab, and IP address details, as shown in the figure below.

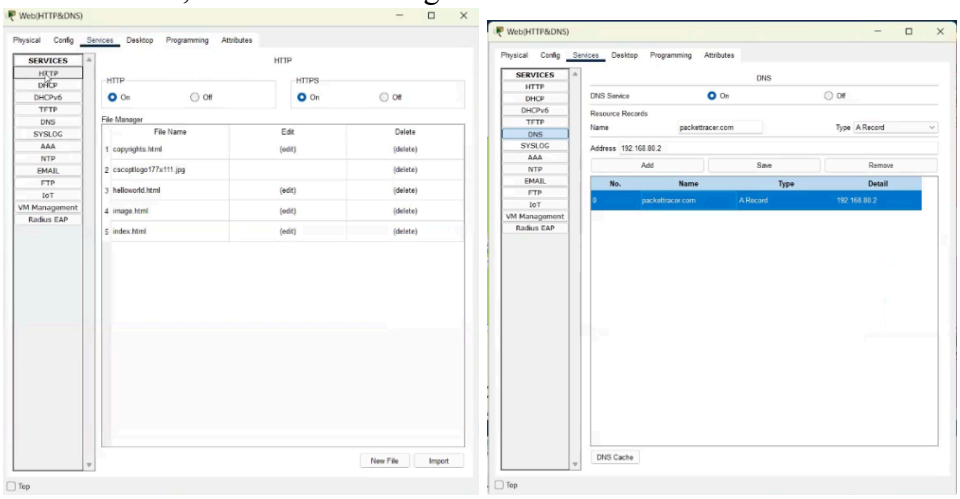

Figure 30. HTTP and DNS Configuration

To test the functionality of the Web (HTTP and DNS) server, a sample website that is listed in the DNS list of websites in the server can be searched on any web browsing computer. In this case, PC55 is used to test the connectivity of the website "packettracer.com". As seen in the figure below, PC55 was able to load the website as expected.

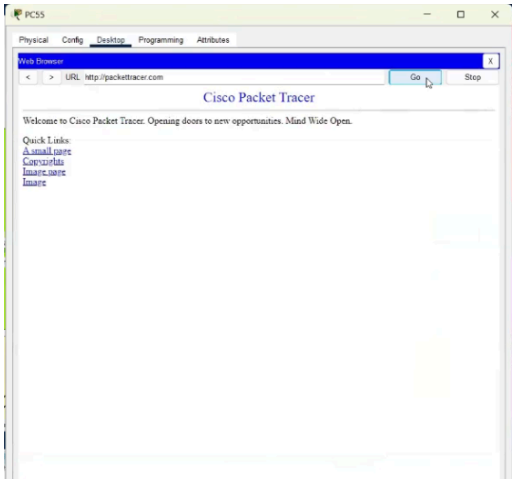

Figure 31. Accessing packettracer.com

For the FTP server, the service under FTP is be enabled. All usernames of the PC, passwords, and permission are listed in the FTP lists. The password for all PCs is set to "1234". The permission for all PCs is set to RWDNL (Read, Write, Delete, Rename, and List). The configuration of the FTP tab is shown below.

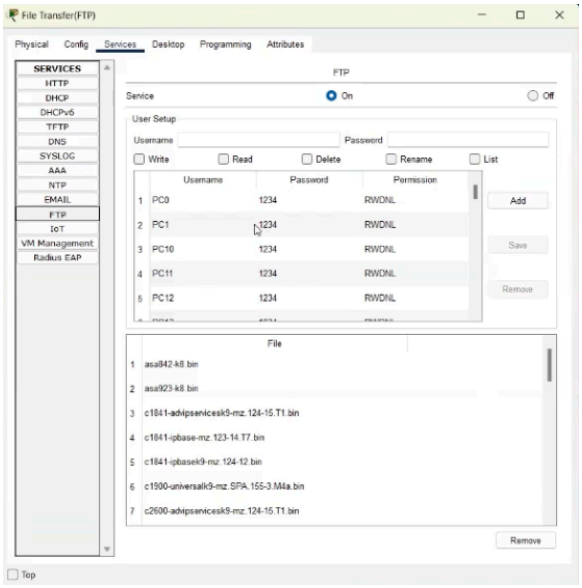

Figure 32. FTP Configuration

To test the functionality of the server, transfer files from each PC were performed. The first is to check if a sample file is present in the PC by entering "dir". If the file is present, file transfer can be initiated by using the command "ftp 192.168.80.3" or the address of the FTP server. Next is to choose which PC to transfer the file to. In this case, PC47 is used. The program will ask for the username and password of the desired PC to transfer the file. To transfer the file to the PC, the command "put" is used followed by the filename. In this case, the code used is "put sampleFile.txt". The transfer has been successful, as shown in the figure below.

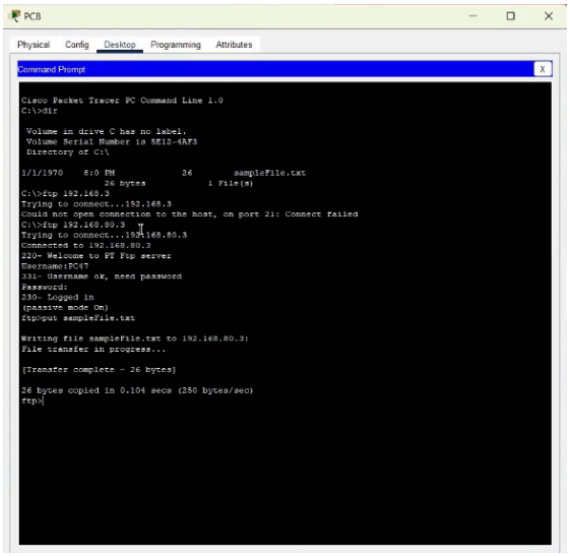

Figure 33. PC8 Command Prompt Writing File

For the Mail Server (SMTP and POP3), the SMTP service and POP3 service are enabled under the email tab. All users are listed in the user setup tab with their username and password. The passwords used are also set to "1234," as similar to the configuration of the previous server discussed.

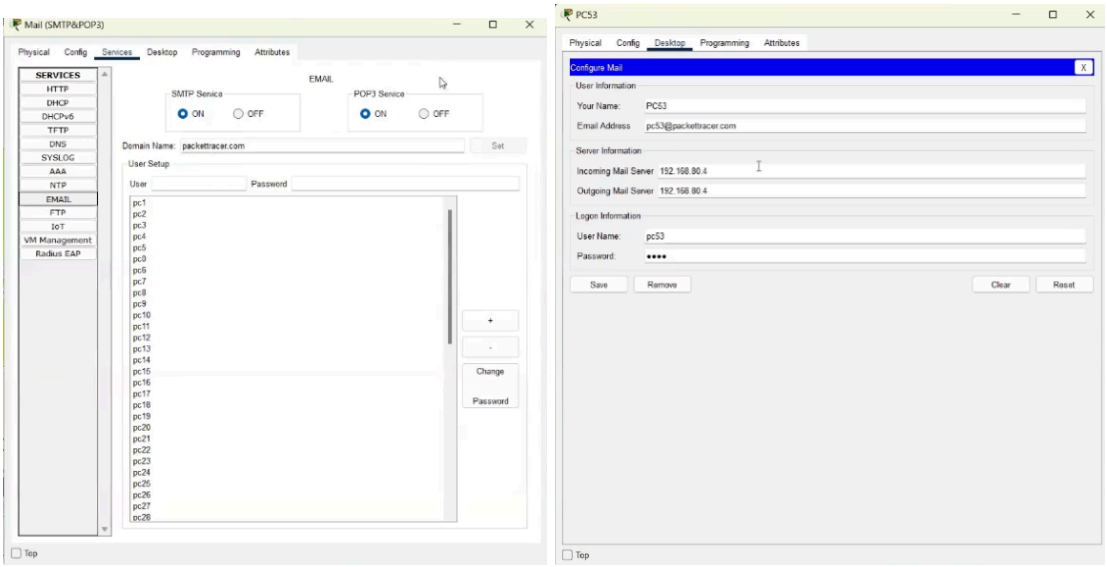

Figure 34. PC53 Configure Email

All PCs are configured with a unique email address. To test the functionality of the server, PC5 will be used to send email to PC53. In PC5, the email address of the designated PC, the desired subject, and the body header are entered. In the testing, the email address of PC53 is "pc53@packettracer.com". After the send button is clicked in PC5 and the receive button is clicked in PC53, the PC will receive the email from PC5. PC53 was also tested by sending an email to PC5. The successful implementation of the FTP server is shown in the figure below.

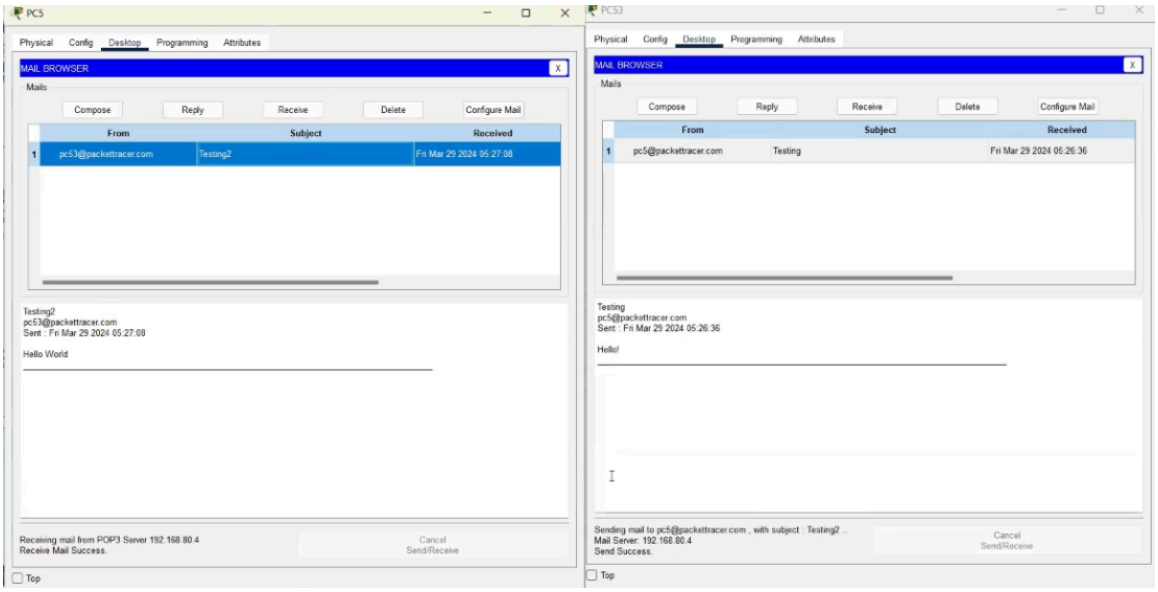

Figure 35. Communication between PC5 and PC53 using Email