ABSTRACT

A secure and efficient Wide Area Network (WAN) is fundamental to the operations of any geographically distributed organization, enabling vital communication, data transfer, and resource sharing across multiple locations. While foundational WAN designs connect disparate Local Area Networks (LANs) using routers and switches, modern networks demand greater intelligence, adaptability, and security to handle complex traffic patterns and protect sensitive information. This project presents an enhanced WAN architecture, simulated in Cisco Packet Tracer, which builds upon a standard multi-office topology.

The baseline model for this project, inspired by existing research, establishes a functional WAN connecting a central headquarters with several branch offices. However, that design relies on static routing, a method that is manually intensive, prone to human error, and inefficient at scaling or adapting to network changes, such as link failures.

Our primary contribution is the modernization of this architecture through the implementation of an advanced dynamic routing protocol, specifically OSPF (Open Shortest Path First) / EIGRP (Enhanced Interior Gateway Routing Protocol). Unlike static routing, this protocol allows routers to automatically discover the network topology, calculate the most efficient paths for data, and dynamically reconverge traffic to alternative routes if a primary link fails. This shift significantly enhances the network's fault tolerance, scalability, and administrative efficiency.

Furthermore, to address modern security challenges, this project integrates Access Control Lists (ACLs) into the network design. These precisely configured rule sets are applied to router interfaces to filter traffic, providing granular control over which devices or subnets are permitted or denied access to specific network resources. This implementation secures critical servers at the headquarters from unauthorized access by guest networks at branch offices, demonstrating a practical and essential layer of network security.

The final implemented network was rigorously tested within the Cisco Packet Tracer simulation environment. Testing confirmed successful end-to-end connectivity, proper route advertisement and convergence via the dynamic protocol, and the successful enforcement of security policies defined by the ACLs. This project successfully demonstrates a scalable, resilient, and secure WAN design that is more aligned with industry best practices and real-world enterprise requirements.

Table of Contents

List of the figures

Chapter-1

Introduction

Introduction (of the project, and the flow of different chapters)

1.1 Background of the project topic

Contemporary organizations heavily depend on strong data communication networks to provide hassle-free communication between geographically scattered offices. A Wide Area Network (WAN) provides the backbone for such communication by linking various Local Area Networks (LANs) across remote locations. WANs facilitate the sharing of data, resources, and services critical to contemporary businesses, government agencies, and schools. As enterprise networks become more complicated, planning and implementing a WAN requires a thorough knowledge of routing protocols, addressing, and network security.

Cisco Packet Tracer, a popular simulation tool, offers an efficient virtual platform to design and simulate WAN topologies without spending money on physical hardware. It enables emulation of routers, switches, servers, and end devices while traffic flow and protocol behavior are being examined. The project is based on the research paper "A Wide Area Network Design and Architecture using Cisco Packet Tracer" (IEEE IC3I 2022) [21]. But this project goes further than the initial architecture by including Dynamic Routing (RIP) and Access Control Lists (ACL) in order to enhance flexibility and network security, creating a more practical and scalable model of enterprise networks.

1.2 Motivation and scope of the report

Organizations need high-performance, secure, and expandable networks that can adapt to changes in topologies frequently in today's digital age. Although static routing is easy, it becomes inefficient and cumbersome when the network is large or paths are down. To counter such limitations, this project incorporates dynamic routing (RIP), which periodically updates routing tables and provides trustworthy data transmission paths.

A further significant motivation is guaranteeing data security and traffic management, which are critical in WAN infrastructures. The use of Access Control Lists (ACL) improves network security by specifying rules that limit unauthorized communication among devices, logically partitioning the network, and avoiding data abuse.

The scope of the project is to design a multi-branch WAN topology on Cisco Packet Tracer, setting up routers, servers, and PCs based on RIP-based routing and implementing ACLs for controlled access. Layered services of DHCP, DNS, FTP, and HTTP are also set up for simulating real-world applications and to check end-to-end connectivity.

1.3 Salient contribution

The project builds upon a given WAN simulation framework by adding two key technical enhancements — Dynamic Routing (RIP) and Access Control Lists (ACL) — thus enhancing the applicability of the design and making it commensurate with actual enterprise network practices.

Notable contributions are:

- Developing and simulating a multi-branch WAN structure consisting of routers, switches, and servers interconnected over multiple LANs.
- Installing RIP routing protocol to automatically control the routing updates and provide dynamic connectivity between every branch.
- Setting ACLs to increase network security by restricting unauthorized inter-network access based on protocol-level and IP-based rules.
- Testing network performance via successful test cases for DNS, DHCP, FTP, and HTTP simulations.
- Examining routing efficiency, packet loss, and throughput to ensure system reliability.

With these additions, the project not only simulates actual WAN environments but also establishes a learning standard for adaptive and secure network simulation.

1.4 Organization of report

The report is organized into five chapters as follows:

- Chapter 1 presents the introduction, background, motivation, and main innovations (RIP and ACL) that make this project stand out.
- Chapter 2 addresses the literature survey, contrasting this work with prior studies and the reference IEEE paper.
- Chapter 3 is about the setup process for RIP and ACL through the WAN topology in terms of methodology, tools, and configuration.
- Chapter 4 is given for the results of simulation, screenshots, and performance checks to validate the functionality of the network.
- Chapter 5 is about the compilation of source code, conclusion, and possible future development like OSPF integration, VPNs, and cloud-based systems.

Chapter-2

Literature survey

2.1 Introduction to the Field

The proliferation of digital services and distributed workforces has made the Wide Area Network (WAN) an indispensable component of modern enterprise infrastructure. A WAN facilitates the interconnection of multiple Local Area Networks (LANs), enabling organizations to expand their operations globally and allowing for the essential transfer of data and access to resources across geographical boundaries. As network traffic increases due to mobile and smart devices, traditional WANs have faced significant challenges in terms of cost, complexity, and security.

This has led to the development of Software-Defined Wide Area Networks (SD-WANs), a virtualized service that offers a more cost-effective, secure, and flexible alternative. Research in this area, such as [1], explores simulation frameworks for interconnecting distributed datacenters using SD-WAN, highlighting its advantages in performance and management. Concurrently, the rise of the Internet-of-Things (IoT) has spurred research into Low-Power Wide Area Networks (LPWANs). These technologies are crucial for supporting massive deployments of low-power devices over long distances, with studies comparing technologies like LoRaWAN and Sigfox and proposing methods to manage network load and service efficiency.

Modern research addresses a wide spectrum of network challenges. This includes managing traffic in inter-cloud communications , enhancing reliability through replicated network topologies , and improving resilience against link failures using protocols like MPTCP. Further studies focus on optimizing network performance by analyzing traffic in network slices , developing algorithms for virtual network embedding , and securing e-healthcare data transmissions. Simulation tools like Network-on-Chip (NoC) are also used to model and analyze network architectures. This collective body of research underscores a continuous drive toward networks that are not only faster and more expansive but also more intelligent, reliable, and secure.

2.2 Exhaustive Literature Survey and Gap Analysis

A review of contemporary research reveals a strong focus on optimizing and extending network capabilities to meet specialized demands. Several studies concentrate on the advancement of SD-WAN and LPWAN. For instance, [1] provides a simulation framework for SD-WANs connecting datacenters, emphasizing bandwidth allocation and traffic flow. This is complemented by [5], which introduces dynamic traffic management (DTM) for SD-WAN inter-cloud communication, aiming to minimize traffic in inter-domains.

A significant portion of the literature is dedicated to the challenges of IoT and LPWANs. [2] offers a comparative review of LPWAN technologies, focusing on improving receiver sensitivity and data flow rates. [3] and [7] both tackle scalability and efficiency in LPWANs; [3] uses K-means and NP-complete methods to improve QoS, while [7] uses an LSTM-EKF model to predict and manage data collisions in LoRa systems. Similarly, [4] and [6] explore multichannel LPWANs and hybrid mesh topologies, respectively, to reduce errors and improve data rates for IoT applications. [9] proposes a dynamic, non-centric approach using virtual gateways to improve transmission performance in LPWA systems.

Performance, reliability, and optimization form another critical research cluster. [8] investigates reliable multicasting using replicated shuffle-exchange networks to mitigate link and switch failures. [10] directly addresses WAN link failures by using Multi-Path Transmission Control Protocol (MPTCP) to achieve fast failure recovery. On the optimization front, [11] models traffic data within network slices to improve performance, while [12] presents an embedding algorithm to enhance the acceptance rate of network requests.

While this body of work addresses advanced topics in network virtualization, IoT, and high-level traffic optimization, it largely overlooks the foundational implementation and security of a standard, traditional enterprise WAN. A recent conference paper by Bhola et al. (2022), "A Wide Area Network Design and Architecture using Cisco Packet Tracer," provides a clear and functional baseline model for this exact scenario. Their work successfully demonstrates the design of a multi-branch WAN, connecting three offices and a headquarters using Cisco Packet Tracer. They validate their network's effectiveness in data transfer, emailing, and achieving high network efficiency with zero packet loss.

However, the implementation by Bhola et al. (2022) relies entirely on static routing. While effective for their specific, unchanging topology, static routing is manually intensive, does not scale, and is not resilient to link failures, as it cannot dynamically reroute traffic. Furthermore, their approach to security is passive, mentioning only the use of a packet sniffer to monitor traffic rather than implementing active security policies to control it.

This analysis identifies a clear research gap: the need to advance the practical, foundational WAN model from a static and passively monitored design to a dynamic, resilient, and actively secured architecture. The existing literature focuses on high-level SD-WAN or niche LPWAN problems, while the foundational simulation model lacks the practical features required by a real-world enterprise[1].

2.3 Problem Statement

The reliance of the established baseline model by Bhola et al. (2022) on static routing presents a significant limitation in terms of scalability, fault tolerance, and administrative overhead. Moreover, the model lacks a robust, configurable security framework to control inter-network traffic.

Therefore, the problem this project seeks to address is: How can the foundational WAN simulation model be enhanced using industry-standard dynamic routing protocols (like OSPF or EIGRP) and layered security policies (via Access Control Lists) to create a more resilient, scalable, and secure enterprise network architecture suitable for practical deployment?

Chapter 3 Methodology / Implementation/ Flowchart /Algorithm

3.1 Software Description:

Cisco Packet Tracer is a powerful network simulation software developed by Cisco Systems, designed to help students, educators, and network professionals learn, design, and test networking concepts in a virtual environment. It provides a realistic platform to simulate complex networks without requiring physical hardware. Users can create both simple and advanced network topologies by integrating routers, switches, servers, PCs, and other networking devices. Packet Tracer supports various networking protocols such as TCP/IP, DHCP, DNS, FTP, HTTP, SMTP, and more, allowing users to analyse real-world data communication and troubleshoot network issues effectively.

Cisco Packet Tracer is particularly effective in simulating Wide Area Networks (WANs), where multiple Local Area Networks (LANs) are interconnected through routers to represent geographically separated offices or organizations. It enables users to configure static and dynamic routing, assign IP addresses, and implement communication between remote sites using protocols like RIP, OSPF, or EIGRP. The software's simulation mode allows observation of data packets as they travel between distant networks, helping analyse bandwidth, latency, and packet delivery. By using Packet Tracer for WAN simulation, learners can visualize how real-world WAN architecture’s function, understand inter-network communication, and gain hands-on experience in managing large-scale network infrastructures in a safe and interactive environment[4].

3.2 Block diagram:

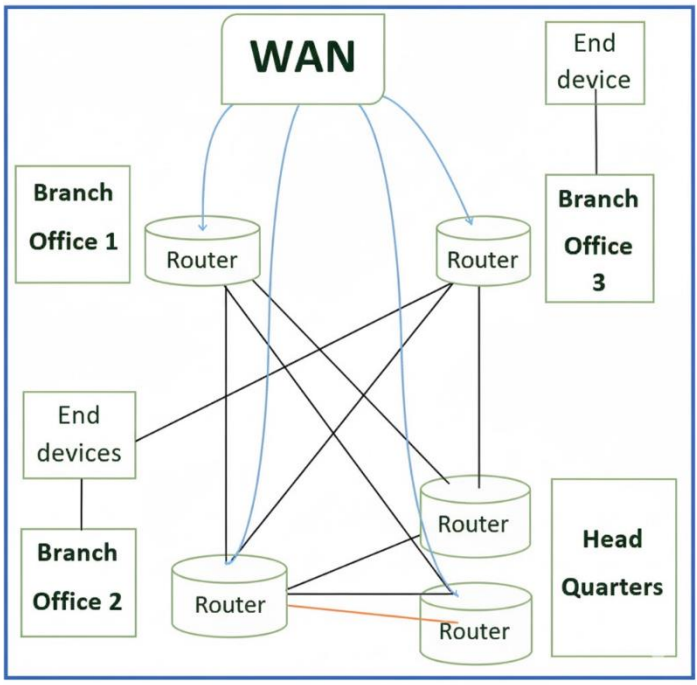


Fig. 1. WAN Architecture of Proposed Work

The provided image presents a high-level block diagram of a Wide Area Network (WAN), detailing the connectivity between a central "Head Quarters" and three distinct remote sites: "Branch Office 1," "Branch Office 2," and "Branch Office 3." The architecture is visualized as a hybrid model, utilizing multiple connection types and redundant pathways to ensure network resilience[2].

The "Head Quarters" functions as the primary hub of this network. It uniquely utilizes two separate "Router" devices for its connectivity. One of these routers acts as a central distribution point, establishing direct, point-to-point links (shown as black lines) to the primary routers at "Branch Office 1," "Branch Office 2," and "Branch Office 3." This main HQ router is also linked to the second HQ router, ensuring internal redundancy at the central site[5].

Beyond the primary hub-and-spoke links from the main HQ router, the network forms a partial-mesh topology. For instance, the router at "Branch Office 1" has a direct link to the router at "Branch Office 2." Furthermore, the router at "Branch Office 2" has a separate connection (distinguished by an orange line) to the second router at the "Head Quarters." The router for "Branch Office 3" also connects back to this second HQ router. This intricate web of interconnections suggests a design focused on resilience, allowing data to take alternative paths if a primary link fails[10].

Separate from these direct inter-router links, a central block labeled WAN provides an alternative, overarching connectivity layer. This WAN block, likely representing a public internet or private MPLS cloud, has its own connections (blue lines) extending to the routers at "Branch Office 1" and "Branch Office 3," as well as to the main router at the "Head Quarters." Notably, "Branch Office 2" is not shown to be connected to this central "WAN" block, relying instead on its direct router-to-router links

Finally, the diagram illustrates the purpose of the branch networks by showing their local connections. The router at "Branch Office 2" provides connectivity to a group of "End devices," while the router at "Branch Office 3" is shown connecting to a single "End device"[6].

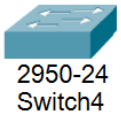
3.3 Hardware description:

1. Routers (A, B, and C)

Routers are the primary hardware used to create the Wide Area Network (WAN) by interconnecting the three separate Local Area Networks (LANs): Location A, Location B, and Location C. In this topology, each router (Router A, Router B, Router C) functions as the default gateway for its respective LAN, with devices like PCs and servers being configured with the router's IP address[3].

The connection between the routers is established using serial connections, and a WAN Interface Card (WIC) was added to the routers to provide the necessary ports for these connections, as they typically only have two. To enable communication between devices on different networks (e.g., Location A to Location C), static routing was configured. This process involves manually adding the IP addresses and "next hops" for the other networks to each router's configuration. This configuration allows a packet from one LAN to be successfully forwarded to the correct destination router and LAN[12].

2. Switches (0, 1, 2, and 3)



Switches are used as the central connecting node within each LAN. The network design employs a star topology, where all end devices (such as PCs and servers) in a LAN are directly connected to a single central switch. When a device sends data, it first passes to the switch; the switch then forwards it, either to another device within the same LAN or to the router if the destination is on the WAN[14].
The implementation uses full-duplex communication, which allows data to be transmitted in both directions simultaneously. This is a key advantage as it helps to "overcome collision during data transmissions". In Location C, two switches are used: Switch 2 connects the main end devices (PC2, PC3), while Switch 3 is part of a dedicated block for the DHCP server[19].

3. PCs (End Devices)

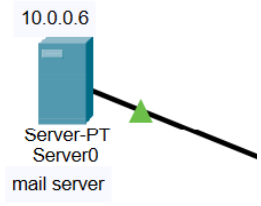
The PCs (Personal Computers) are the end devices used by operators like "USER ALICE" (PC0) and "USER BOB" (PC2). They are used to test the functionality and efficiency of the network. Their primary functions in this project are to initiate connectivity tests and use the network services[14].
For example, PCs are used to ping other devices across the WAN to verify connectivity and check for packet loss . The results in Figure 6 show a successful ping from PC3 to PC2 (50.0.0.11) with 0% loss, confirming correct network configuration. PCs are also configured as email clients (e.g., 'admin@gmail.com' on PC1 and 'admin@gmail.com' on PC2). This allows for testing the mail server by sending emails between PCs in different geographical locations, as shown in Figure 4[17].

4. Server Descriptions

Servers are configured with static IP addresses and provide specific services to the network.

1. Mail Server (Server0)

The Mail Server, labeled 'gmail.com', is hosted in Location A and is responsible for handling email services for the network. It was implemented to test the WAN's ability to facilitate communication between users in different LANs. The paper details a successful test where PC1 (in Location B) sends an email to PC2 (in Location C). The data packet travels from PC1 to Router B, then to Router A, to the Mail Server, which then forwards it via Router A and Router C to PC2 . The successful reply, shown in Figure 4, confirms the server and WAN routing are functioning correctly[17].

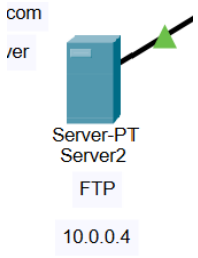


2. DNS Server (Server4)

The Domain Name System (DNS) server is a critical component, also located in Location A. Its function is to map human-readable domain names (like 'gmail.com') to their corresponding IP addresses (like 10.0.0.6), "without the help of remembering the IP address of each device". The server is configured by adding these domain name and IP address records. All other end devices in the network are then configured with the DNS server's IP address, allowing them to use web browsers to access services by name rather than IP[18].

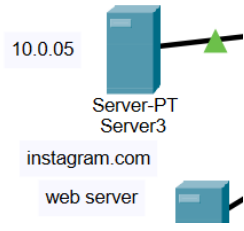
3. FTP Server (Server1)

The File Transfer Protocol (FTP) server, located in Location A, is included to "handle the data transferred between computers". This protocol is specifically noted for its utility in "sending large files". Its implementation demonstrates that the network is configured to support bulk data transfer, a common requirement for a WAN. To ensure its functionality, all necessary protocols (including HTTP) were enabled on the server.



4. Web Server (Server2)

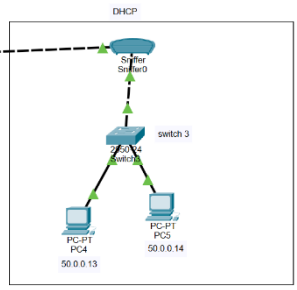
This server, labeled 'instagram.com' in the diagram, is implemented to host "web app services". Its purpose is to demonstrate that the network can successfully support standard web traffic. For this server to function, all HTTP protocols were required to be turned "ON". Users on the network can access this web server by typing its domain name into a browser, a process made possible by the DNS server, which resolves 'instagram.com' to the server's static IP address (10.0.0.15)[19].



5. NTP Server (Server6)

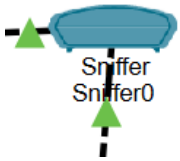
The Network Time Protocol (NTP) server is located in Location B. This server provides an essential utility service for the entire WAN. NTP is defined as a set of rules used for "clock sync between packet-switched systems in data networks and devices". By providing a central time source, the NTP server ensures that all devices across the different geographic locations (A, B, and C) can maintain a synchronized clock, which is crucial for accurate logging, security, and timestamping of events[15].

6. DHCP Server (Server8)



The Dynamic Host Configuration Protocol (DHCP) server is implemented in Location C. Unlike the static IP addressing used in Locations A and B , the DHCP server's role is to "automatically assigns the IP to the devices". This server is shown in a separate block connected to Switch 3 (along with PC4 and PC5) and is also linked to Switch 2 (via a dashed line in Fig 2). This indicates it provides dynamic IP addresses, subnet masks, and default gateway information to all end devices in Location C, including PC2 and PC3, simplifying network management for that branch[20].

5. Packet Sniffer



A packet sniffer, also referred to as a packet analyzer, was a software tool used in this project "to monitor network traffic". This component is not a physical device in the topology but a utility used for analysis. Its function is to "examine streams of data packets that pass between computers on a network". In this implementation, the sniffer was used to analyze the data passing through the network to "ensure the network's security". The simulation panel shown in Figure 5, which logs the step-by-step flow of TCP and DNS packets from device to device, is an example of the analysis provided by this tool[21].

3.4 implementation of project:

The proposed project focuses on the design and implementation of a Wide Area Network (WAN) using Cisco Packet Tracer, which serves as a simulation platform for creating, configuring, and testing real-world networking scenarios. The WAN is designed to interconnect multiple branch offices located in different geographical areas through a central headquarters. Each branch and the headquarters maintain its own Local Area Network (LAN) consisting of routers, switches, servers, and end devices such as PCs. All branch routers are connected to the central router at the headquarters to enable inter-branch communication. This topology effectively represents how multinational organizations or institutions link remote offices for data sharing and collaboration.

The implementation begins with the logical design of the network in Cisco Packet Tracer. Devices such as routers, switches, PCs, and servers are placed and interconnected using appropriate cables. Each LAN is configured using a star topology, where all end devices connect to a central switch. The switches are then linked to routers that act as gateways between LANs and the WAN. For WAN connectivity, routers are connected using serial interfaces with DCE/DTE cables to simulate long-distance communication links[15].

The next step involves IP address configuration. A proper IP addressing scheme is designed using both static and dynamic methods. Each LAN is assigned a unique subnet to avoid address conflicts and to allow efficient routing. The headquarters router acts as a core point that interconnects all branch routers using serial links. End devices in some LANs are configured using static IP addresses, while others use Dynamic Host Configuration Protocol (DHCP) for automatic IP allocation. This ensures scalability, as new devices can join the network without manual configuration.

Once the IP addressing is complete, routing is configured to enable communication between networks. In this project, Dynamic Routing is implemented using the Routing Information Protocol (RIP**)**. RIP allows routers to automatically learn and update routes based on changes in the network topology, reducing manual configuration efforts and enhancing flexibility. The use of RIP ensures that if one link fails, the routers can automatically discover an alternative path, maintaining consistent network connectivity. RIP also simplifies management in multi-branch WAN environments by periodically exchanging routing information between routers to keep the routing tables updated[17].

To further enhance the project's functionality and security, Access Control Lists (ACLs) are implemented on routers. ACLs are used to control network traffic and restrict unauthorized access to sensitive resources. For instance, specific IP addresses or subnets can be permitted or denied access to servers or devices in other networks. In this WAN design**,** standard ACLs are used to filter traffic based on source IP addresses, while extended ACLs are applied to control traffic based on both source and destination addresses as well as protocols. This ensures that only legitimate users and devices can access network resources, thereby increasing security and reducing the risk of data breaches[13].

Additional configurations such as Domain Name System (DNS)**,** File Transfer Protocol (FTP)**,** and Email (SMTP/POP3) services are implemented on servers to simulate real-world applications. The DNS server translates hostnames into IP addresses, simplifying communication between devices without needing to remember numeric IP addresses. The FTP server allows file sharing between networks, and the email server enables communication between users in different LANs through Gmail-like interfaces[15].

After configuring all devices and services, the network's performance is tested using ping commands and packet simulation mode in Cisco Packet Tracer. Packets are successfully transferred between PCs located in different LANs, showing 0% packet loss**,** which verifies proper configuration and high network efficiency. The packet sniffer tool within Packet Tracer is also used to analyze data flow, monitor performance, and verify that ACLs are effectively filtering traffic[8].

The enhanced WAN design demonstrates the benefits of integrating dynamic routing using RIP and ACLs. Dynamic routing ensures continuous communication and adaptability to network changes, while ACLs provide an additional layer of security by regulating data flow. Together, these enhancements make the WAN more intelligent, secure, and resilient compared to a traditional static WAN[12].

In conclusion, the project successfully simulates a fully functional WAN using Cisco Packet Tracer, integrating multiple LANs across different locations. The implementation achieves a scalable and secure WAN architecture that supports efficient data transmission, inter-network communication, and real-world applications - an essential model for organizations and academic institutions seeking to understand and apply WAN concepts in practice[9].

3.5 Working of Project:

The Wide Area Network (WAN) developed in this project aims to establish efficient and secure communication between multiple branch offices and a central headquarters using **Cisco Packet Tracer**. The design reflects a real-world enterprise setup where different offices are interconnected through routers, allowing data exchange, file sharing, and email communication over long distances. The project follows the core principles discussed in the IEEE paper *"A Wide Area Network Design and Architecture using Cisco Packet Tracer"* and includes additional enhancements such as **Dynamic Routing (RIP)**, **Access Control Lists (ACLs)**, **DHCP**, **DNS**, **FTP**, and **Packet Sniffer analysis** to improve automation, scalability, and security[19].

Each branch office in the network has its own **Local Area Network (LAN)** consisting of switches, servers, routers, and PCs. These LANs are connected to the headquarters router using **serial DCE/DTE connections**, forming the complete WAN. A **star topology** is used within each LAN, ensuring centralized communication and reduced data collisions. The routers are assigned unique IP addresses, and addressing is managed using both **static and dynamic methods**. Static IPs are used for routers and servers, while the **Dynamic Host Configuration Protocol (DHCP)** automatically assigns IP addresses to end devices, minimizing manual configuration[6].

Routing Information Protocol (RIP) is implemented to enable **dynamic routing**, allowing routers to automatically share and update route information. This ensures that data packets always find the best available path and that communication continues even if one link fails. The **Domain Name System (DNS)** is configured to resolve hostnames to IP addresses, enabling users to access services easily without memorizing IPs. Services like **File Transfer Protocol (FTP)** and **Email (SMTP and POP3)** simulate real-world data transfer and communication across different LANs[18].

To enhance network security, **Access Control Lists (ACLs)** are configured on routers to control and restrict network traffic. ACLs define which users or networks can access specific resources, providing an extra layer of protection. The **Packet Sniffer tool** is used to capture and analyze network packets, verifying that data is transmitted efficiently with no losses or retransmissions[20].

After configuration, several tests were conducted, including connectivity, DHCP allocation, DNS resolution, packet efficiency, and ACL functionality. Results showed **0% packet loss**, successful hostname resolution, and proper enforcement of access restrictions. Overall, the WAN operates efficiently with secure communication between all branch offices, proving that Cisco Packet Tracer can effectively simulate a real-world, high-performance WAN architecture[11].

Chapter 4: Screenshots of the Project/Test

4.1 Screenshots:

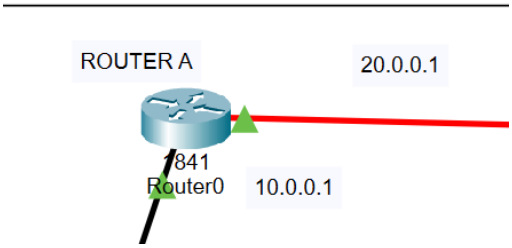


Fig. 1. Router A

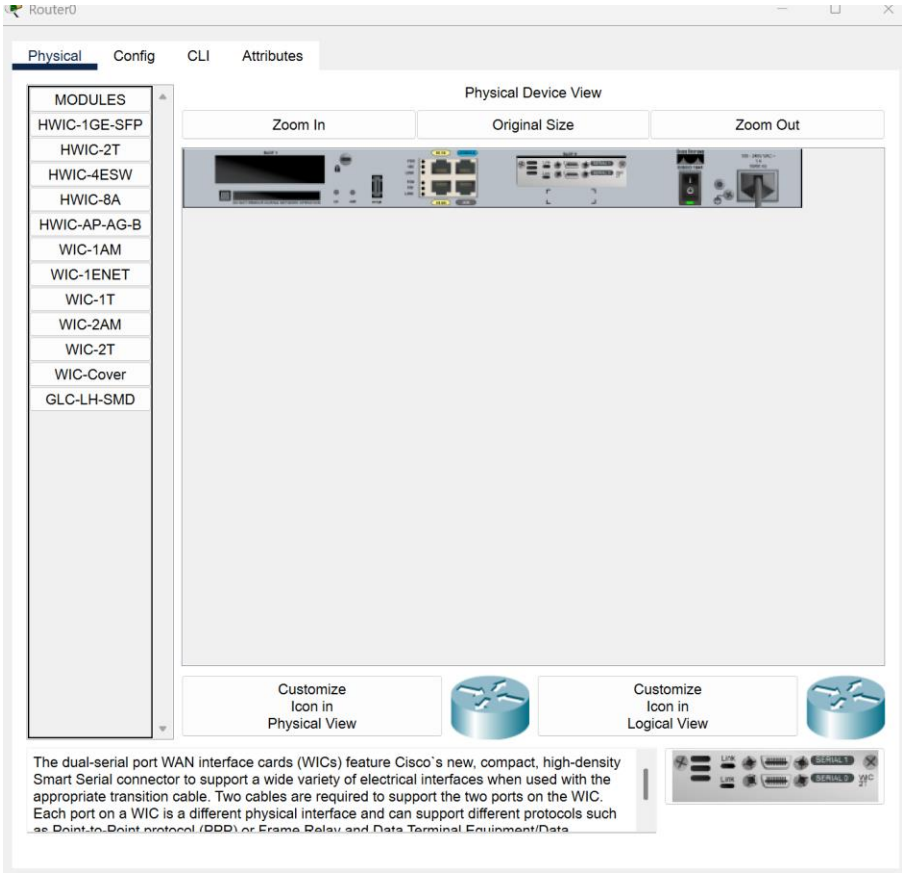


Fig. 2. Router-A- configured WIC-2T

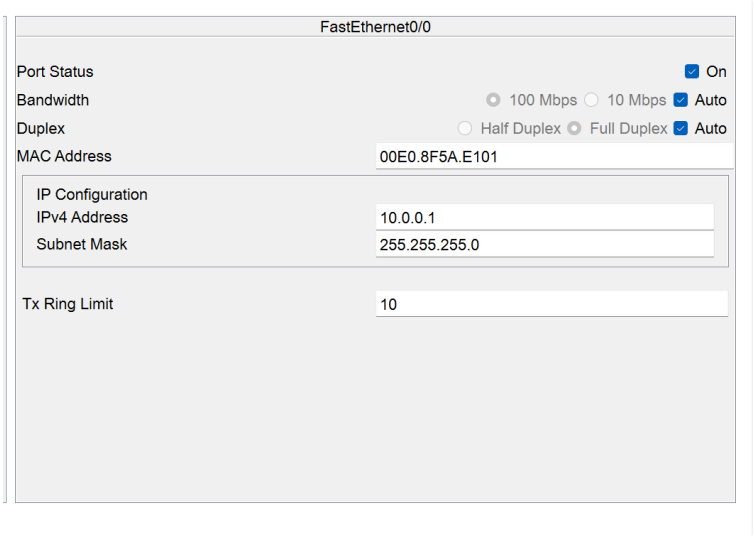


Fig. 1. Router-A- fast ethernet0/0 ipconfig

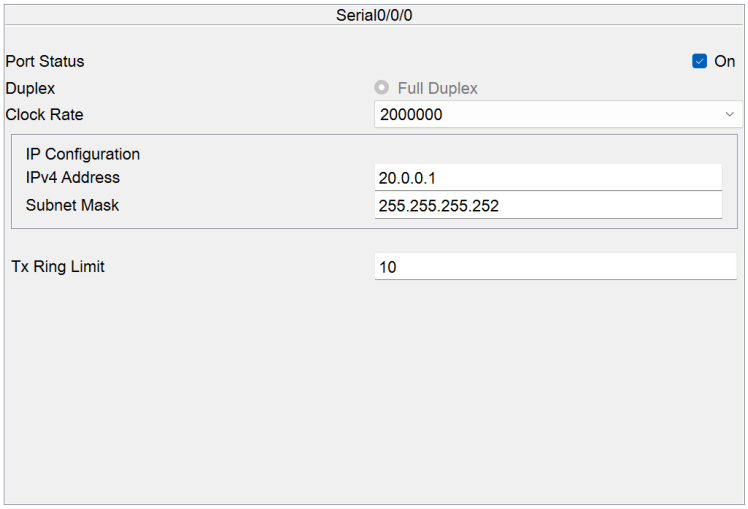


Fig. 1. Router-A- serial0/0 ipconfig

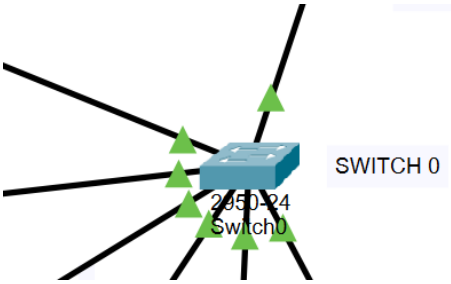


Fig. 1. Location A Switch

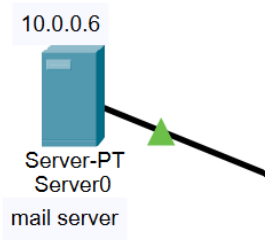


Fig. 1. Server0: Mail router

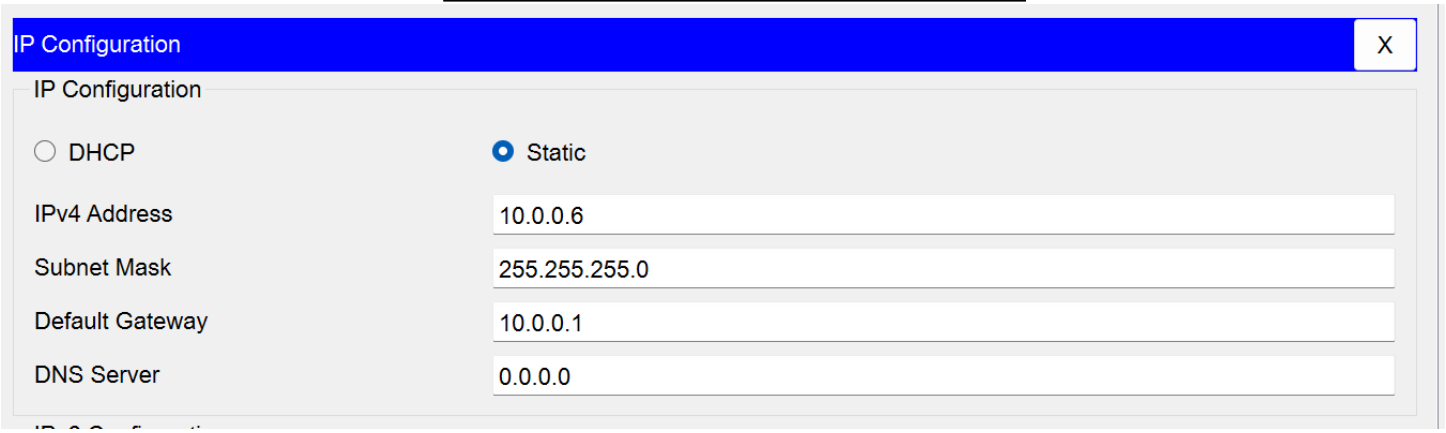


Fig. 1. Mail server ip config

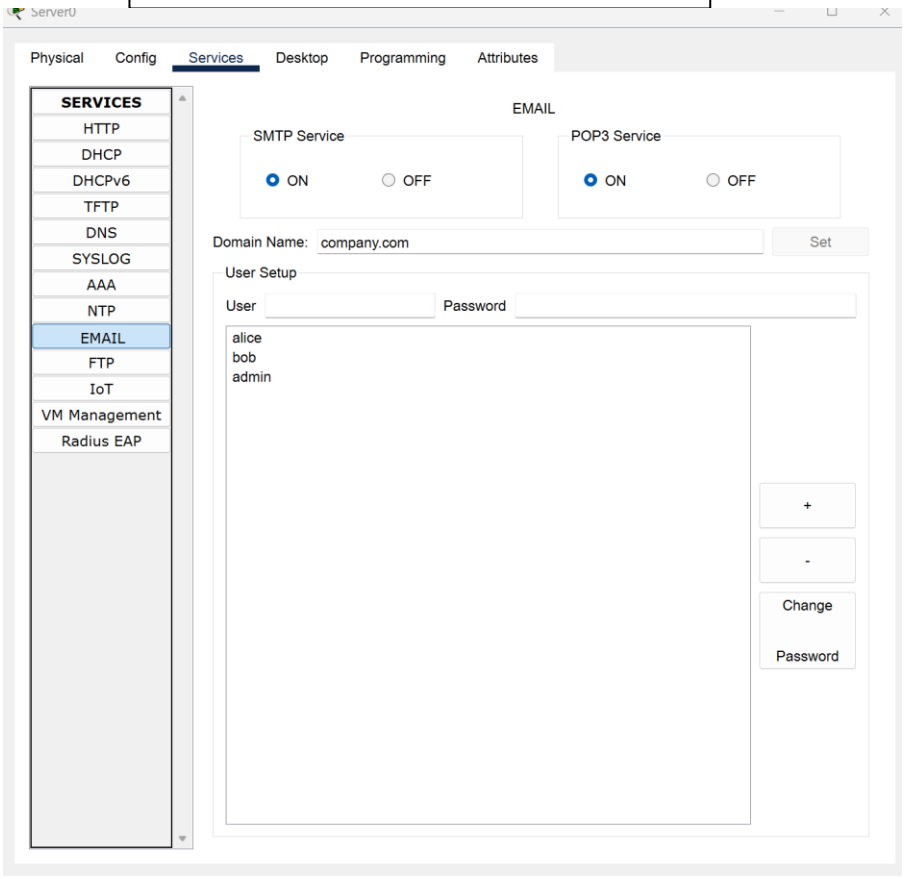
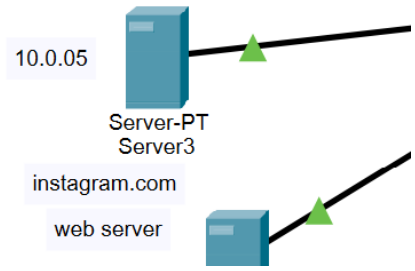
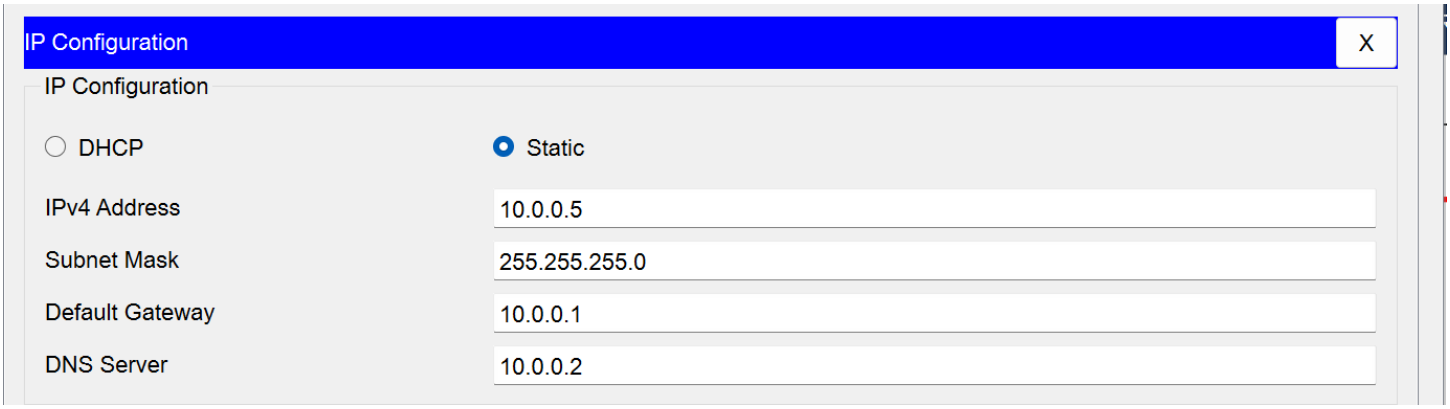
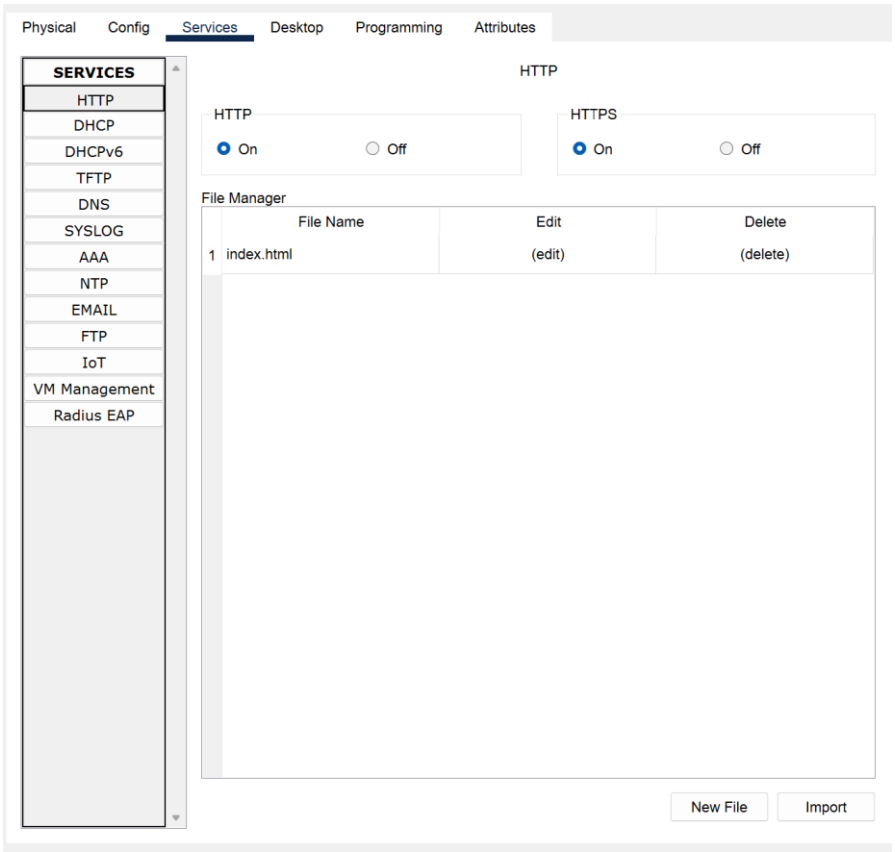


Fig. 1. Router-A- fast ethernet0/0 ipconfig

Location- A

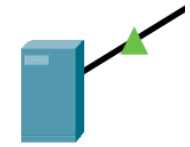

10.0.05
Server-PT
Server3
instagram.com
web server


IP Configuration
X
IP Configuration
DHCP
Static
IPv4 Address
10.0.0.5
Subnet Mask
255.255.255.0
Default Gateway
10.0.0.1
DNS Server
10.0.0.2


Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
HTTP
HTTP
On
Off
HTTPS
On
Off
File Manager
File Name
Edit
Delete
1
index.html
(edit)
(delete)
New File
Import

com

ver



Server-PT
Server2

FTP

10.0.0.4

IP Configuration

IP Configuration

IP Configuration

DHCP

Static

IPv4 Address 10.0.0.4

Subnet Mask 255.255.255.0

Default Gateway 10.0.0.1

DNS Server 0.0.0.0

Physical Config Services Desktop Programming Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

FTP

Service On Off

User Setup

Username Password

Write Read Delete Rename List

	Username	Password	Permission
1	alice	123	RWDNL
2	bob	123	RW
3	cisco	cisco	RWDNL

Add

Save

Remove

	File
1	asa842-k8.bin
2	asa923-k8.bin
3	c1841-advipservicesk9-mz.124-15.T1.bin
4	c1841-ipbase-mz.123-14.T7.bin
5	c1841-ipbasek9-mz.124-12.bin
6	c1900-universalk9-mz.SPA.155-3.M4a.bin

Remove

Server-PT
Server4

DNS

10.0.0.2

IP Configuration

IP Configuration

DHCP

Static

IPv4 Address 10.0.0.2

Subnet Mask 255.255.255.0

Default Gateway 10.0.0.1

DNS Server 0.0.0.0

Physical Config Services Desktop Programming Attributes

SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP

DNS

DNS Service On Off

Resource Records

Name Type A Record

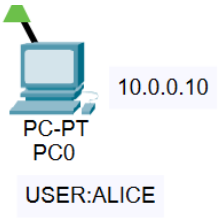
Address

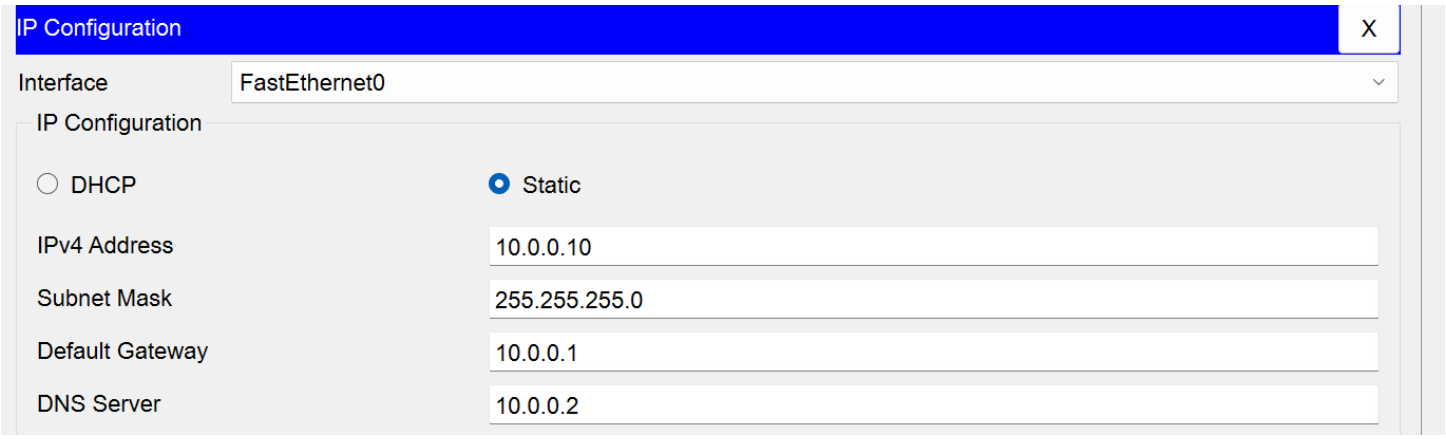
Add Save Remove

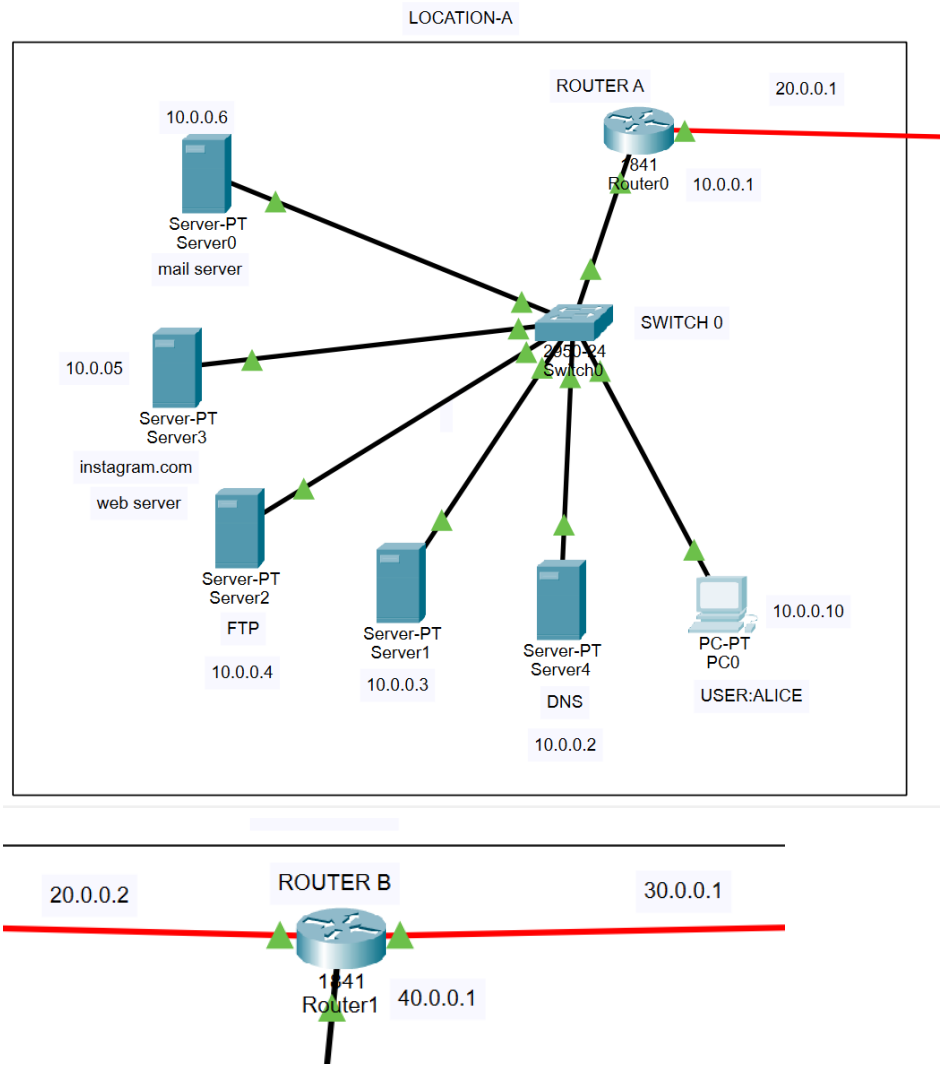
No.	Name	Type	Detail
0	instagram.com	A Record	10.0.0.5
1	mail.company.com	A Record	10.0.0.6

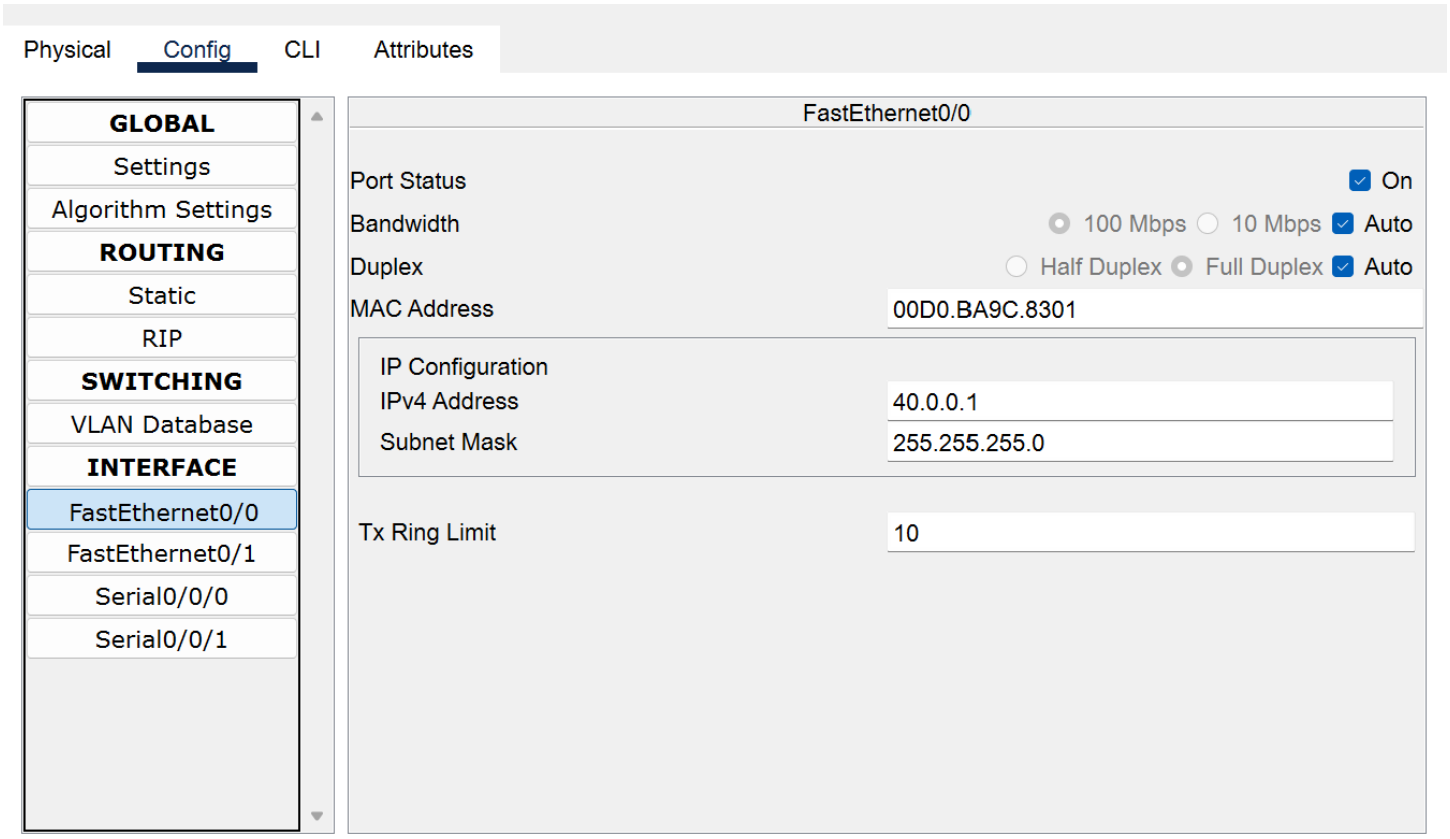
DNS Cache

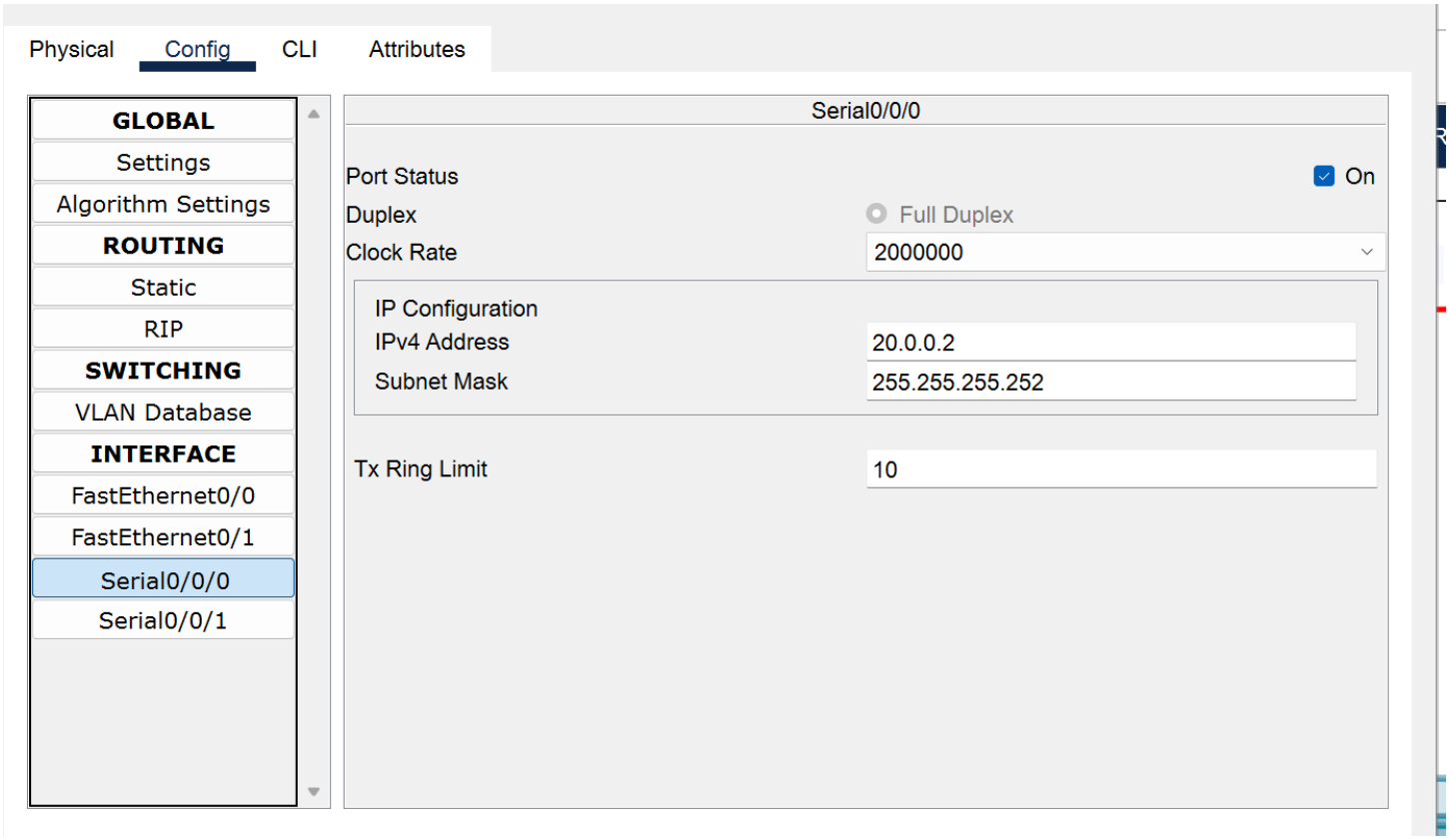
Location B


10.0.0.10
PC-PT
PC0
USER:ALICE


IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
10.0.0.10
Subnet Mask
255.255.255.0
Default Gateway
10.0.0.1
DNS Server
10.0.0.2


LOCATION-A
ROUTER A
20.0.0.1
10.0.0.6
1841
Router0
10.0.0.1
Server-PT
Server0
mail server
SWITCH 0
2950-24
Switch0
10.0.05
Server-PT
Server3
instagram.com
web server
Server-PT
Server2
FTP
10.0.0.4
Server-PT
Server1
10.0.0.3
Server-PT
Server4
DNS
10.0.0.2
PC-PT
PC0
USER:ALICE
10.0.0.10
20.0.0.2
ROUTER B
30.0.0.1
1841
Router1
40.0.0.1


Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
FastEthernet0/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00D0.BA9C.8301
IP Configuration
IPv4 Address
40.0.0.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10


Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/0/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
20.0.0.2
Subnet Mask
255.255.255.252
Tx Ring Limit
10

Location-B

Physical | Config | CLI | Attributes

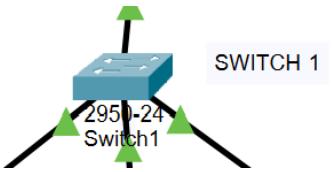
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1

Serial0/0/1

Port Status: On
Duplex: Full Duplex
Clock Rate: 2000000

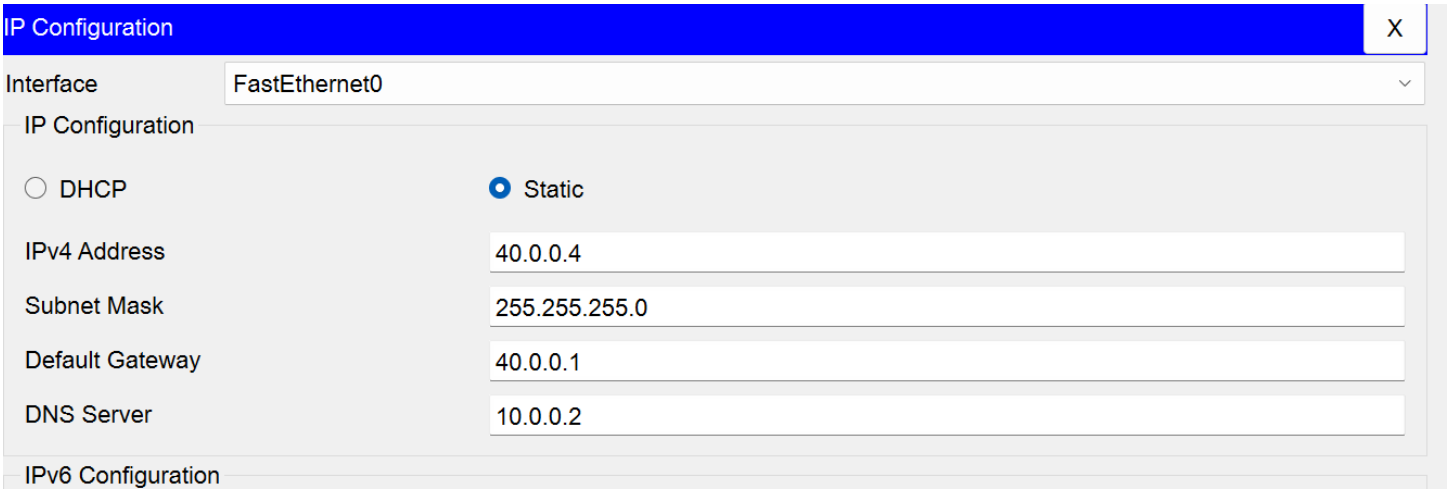
IP Configuration
IPv4 Address: 30.0.0.1
Subnet Mask: 255.255.255.252

Tx Ring Limit: 10



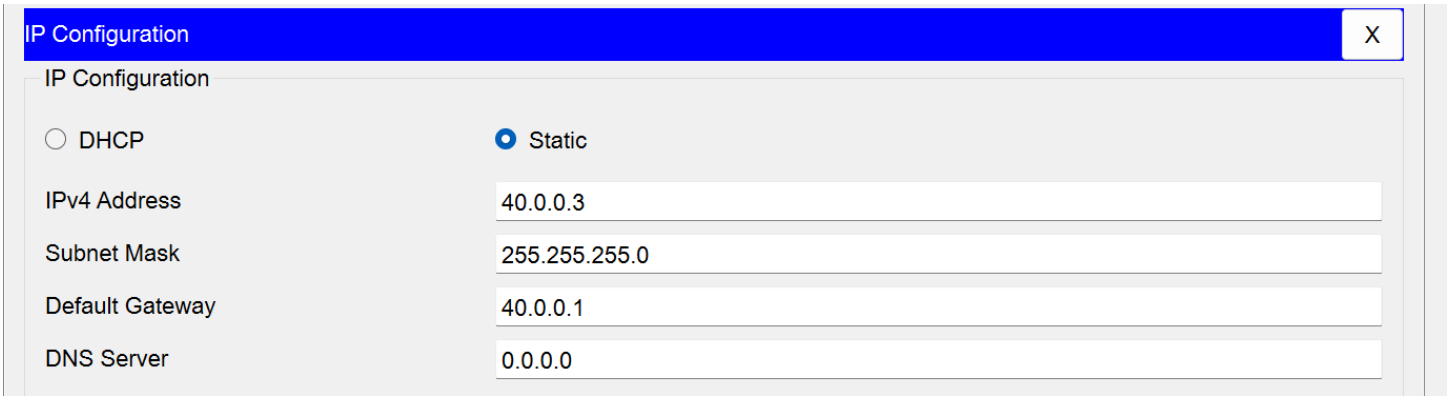
admin@company.com

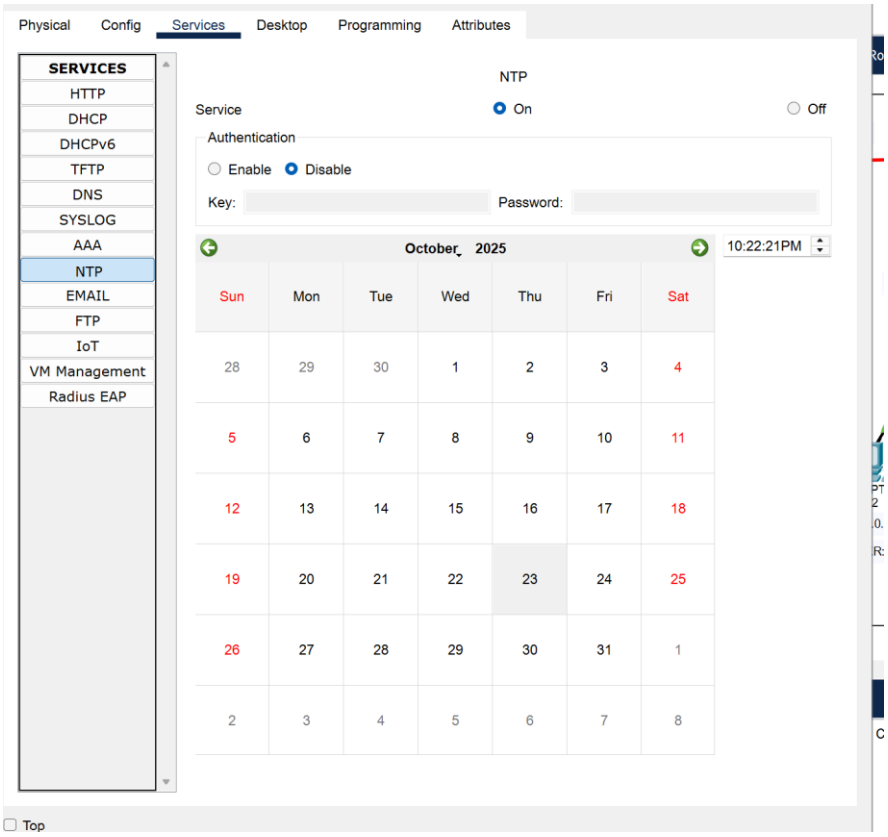
40.0.0.4

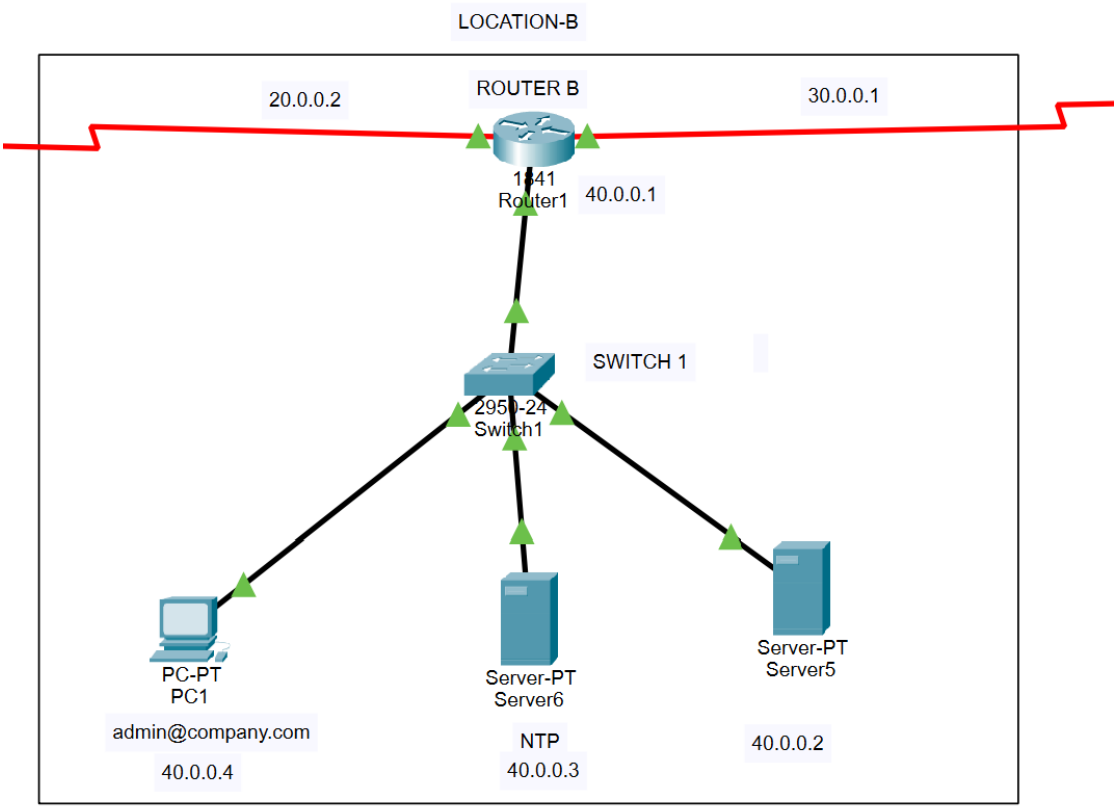

IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
40.0.0.4
Subnet Mask
255.255.255.0
Default Gateway
40.0.0.1
DNS Server
10.0.0.2
IPv6 Configuration

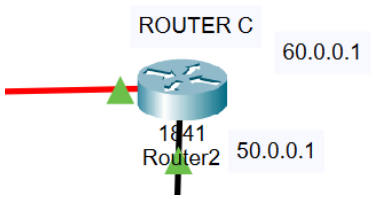
Location-B


Server-PT
Server6
NTP
40.0.0.3


IP Configuration
X
IP Configuration
DHCP
Static
IPv4 Address
40.0.0.3
Subnet Mask
255.255.255.0
Default Gateway
40.0.0.1
DNS Server
0.0.0.0


Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
NTP
Service
On
Off
Authentication
Enable
Disable
Key:
Password:
October 2025
10:22:21PM
Sun Mon Tue Wed Thu Fri Sat
28 29 30 1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 31 1
2 3 4 5 6 7 8
Top


LOCATION-B
20.0.0.2
ROUTER B
30.0.0.1
1841
Router1
40.0.0.1
SWITCH 1
2950-24
Switch1
PC-PT
PC1
admin@company.com
40.0.0.4
Server-PT
Server6
NTP
40.0.0.3
Server-PT
Server5
40.0.0.2

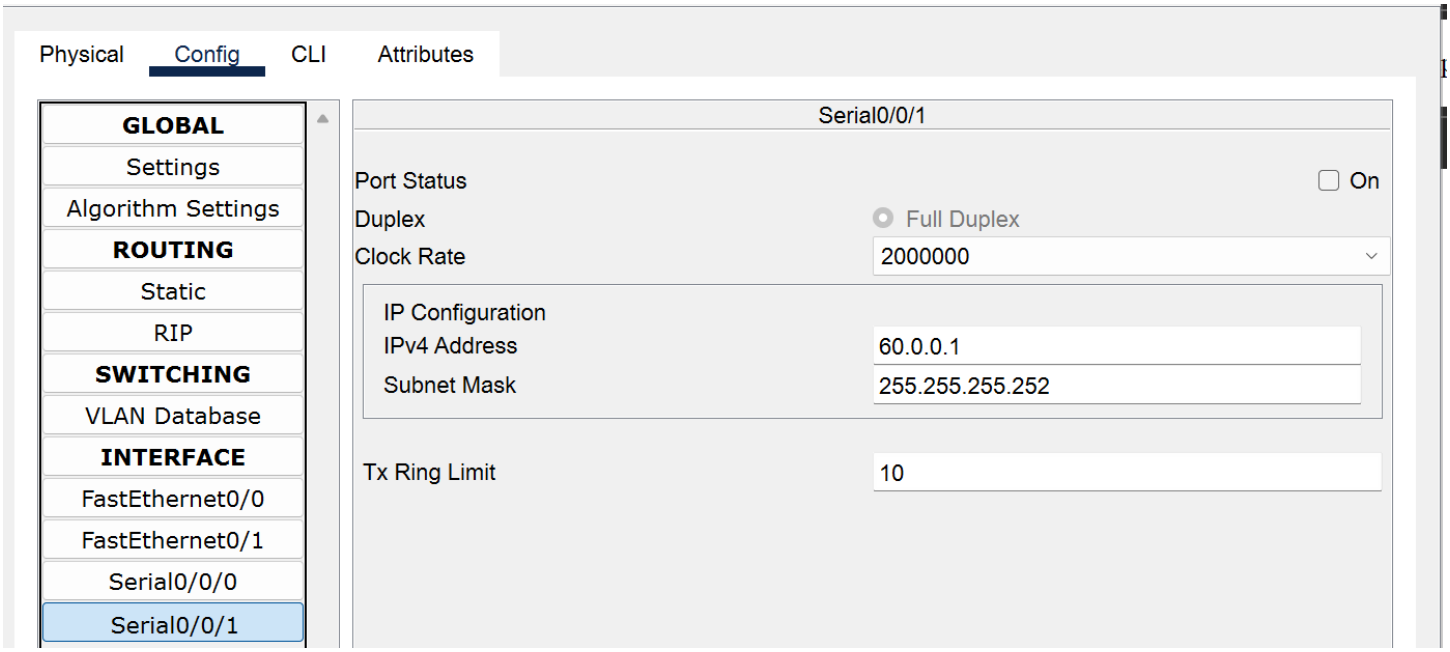


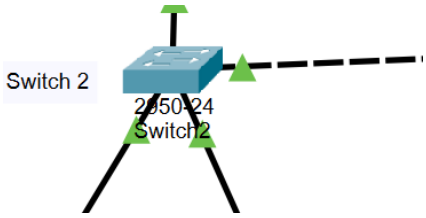
FastEthernet0/0

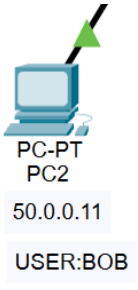
Port Status	On
Bandwidth	100 Mbps / 10 Mbps / Auto
Duplex	Half Duplex / Full Duplex / Auto
MAC Address	0001.42D9.5301
IP Configuration	
IPv4 Address	50.0.0.1
Subnet Mask	255.255.255.0
Tx Ring Limit	10

Serial0/0/0

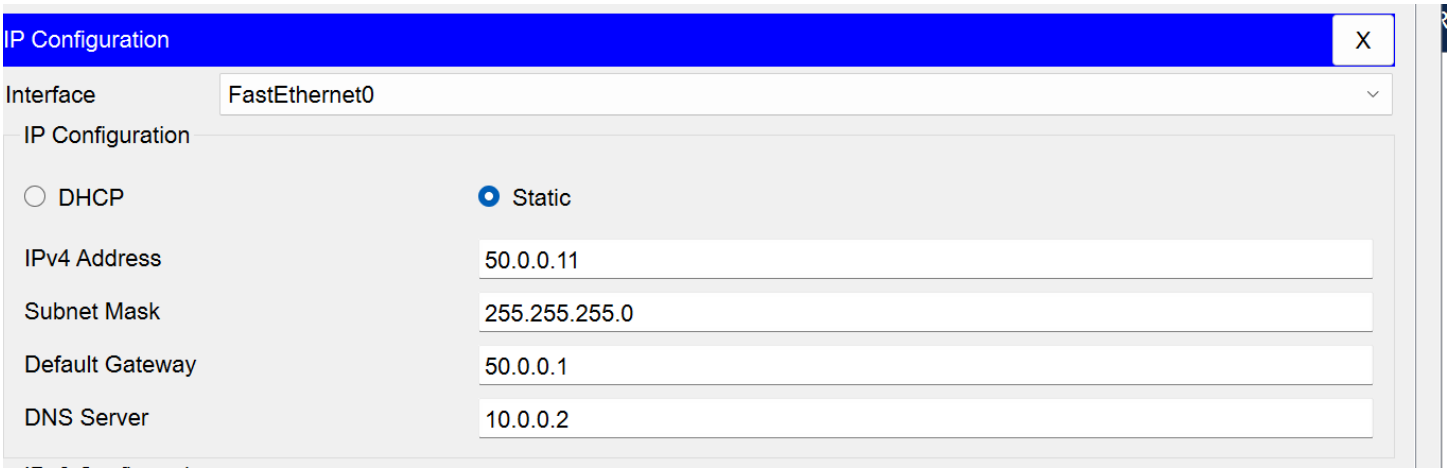
Port Status	On
Duplex	Full Duplex
Clock Rate	2000000
IP Configuration	
IPv4 Address	30.0.0.2
Subnet Mask	255.255.255.252
Tx Ring Limit	10

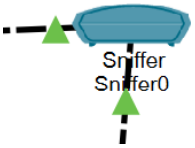

Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/0/1
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
60.0.0.1
Subnet Mask
255.255.255.252
Tx Ring Limit
10

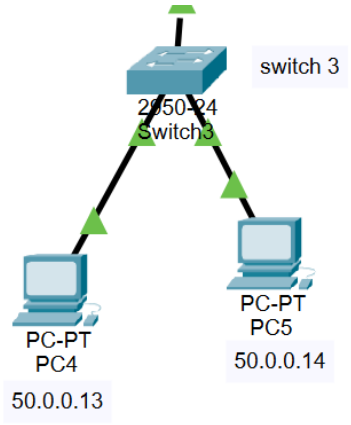

Switch 2
2950-24
Switch2

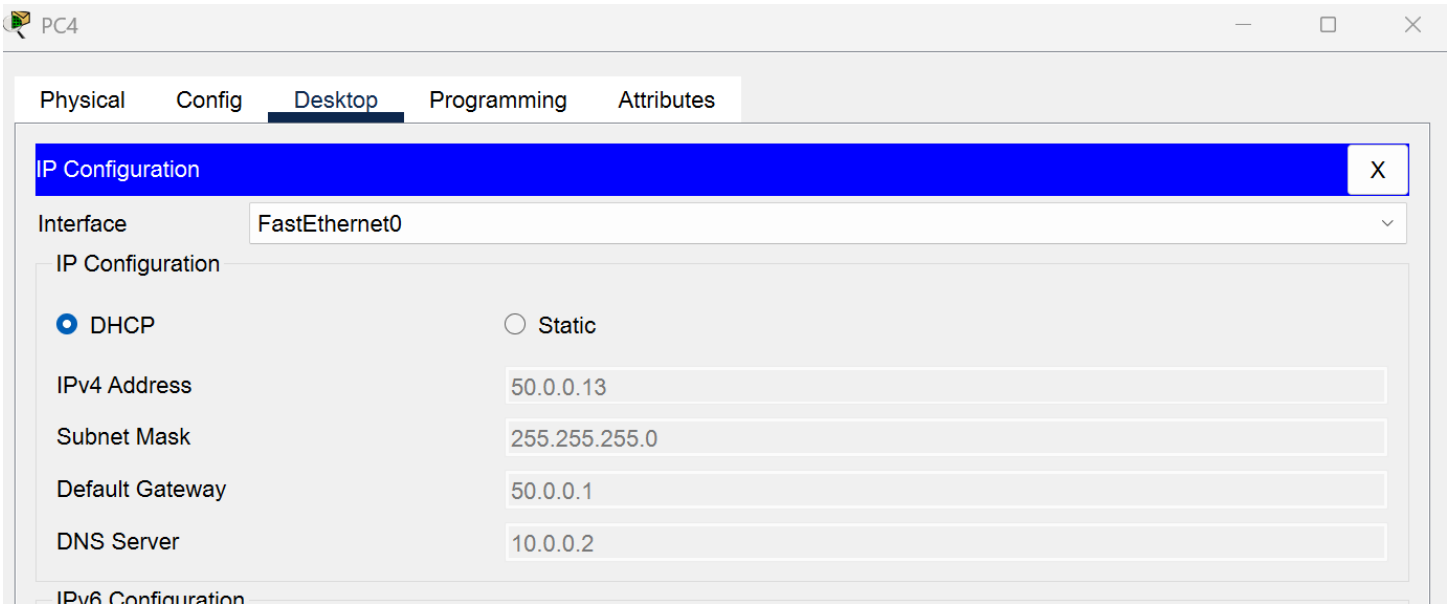

PC-PT
PC2
50.0.0.11
USER:BOB

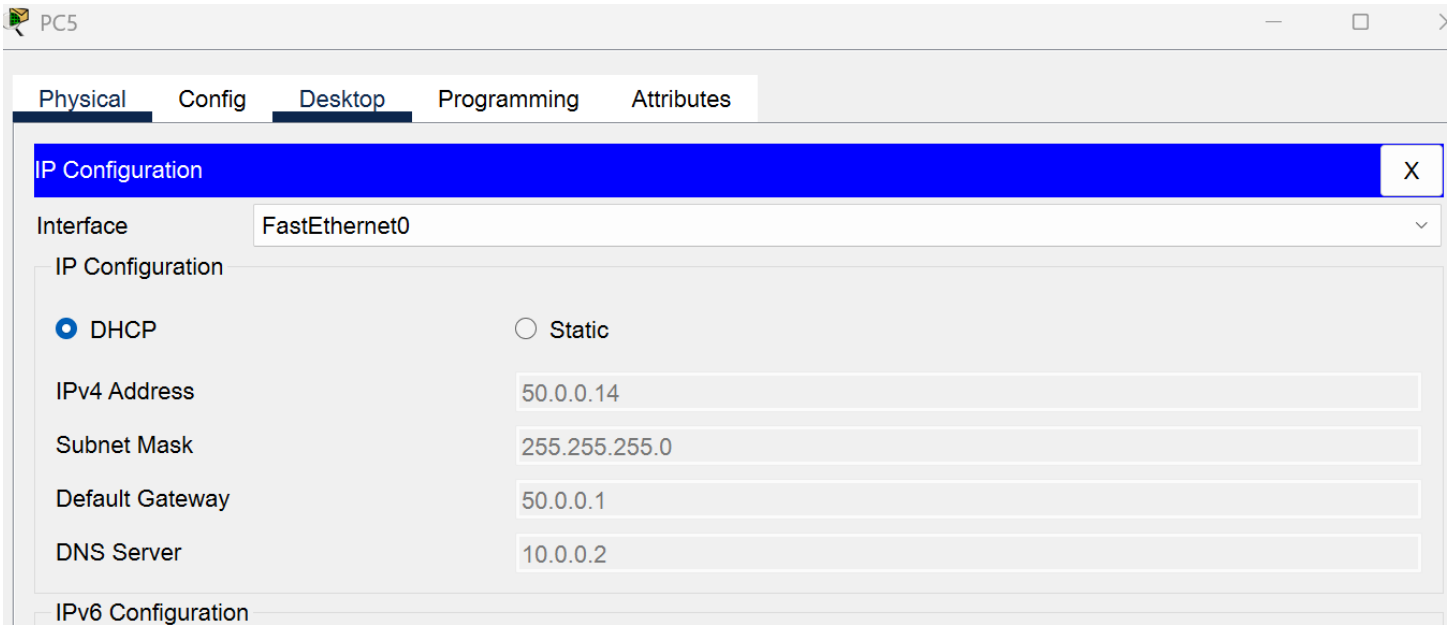
Location-C


IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
50.0.0.11
Subnet Mask
255.255.255.0
Default Gateway
50.0.0.1
DNS Server
10.0.0.2


Sniffer
Sniffer0


switch 3
2950-24
Switch3
PC-PT
PC4
50.0.0.13
PC-PT
PC5
50.0.0.14


PC4
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
50.0.0.13
Subnet Mask
255.255.255.0
Default Gateway
50.0.0.1
DNS Server
10.0.0.2
IPv6 Configuration


PC5
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
50.0.0.14
Subnet Mask
255.255.255.0
Default Gateway
50.0.0.1
DNS Server
10.0.0.2
IPv6 Configuration

Attributes

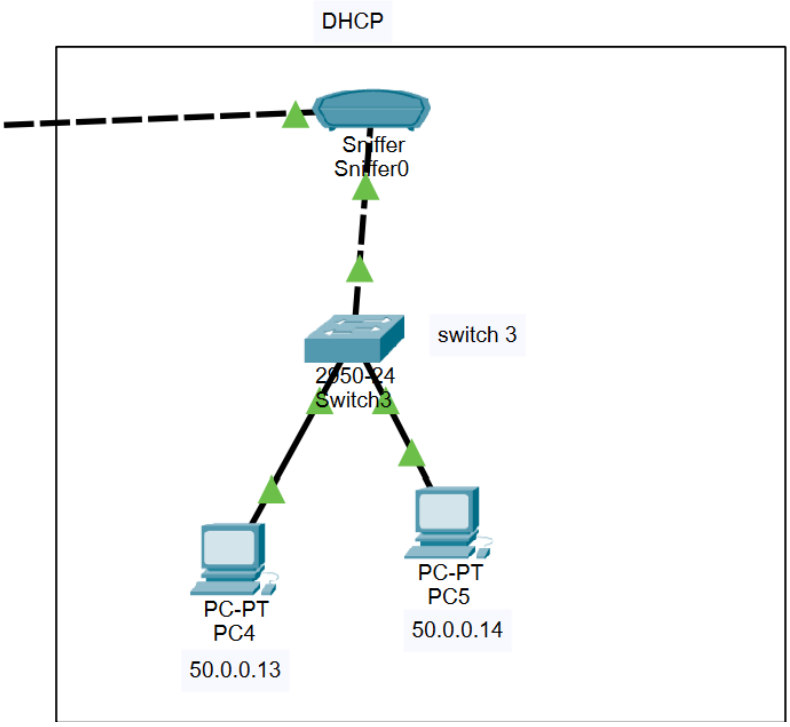
RIP Routing (v2)

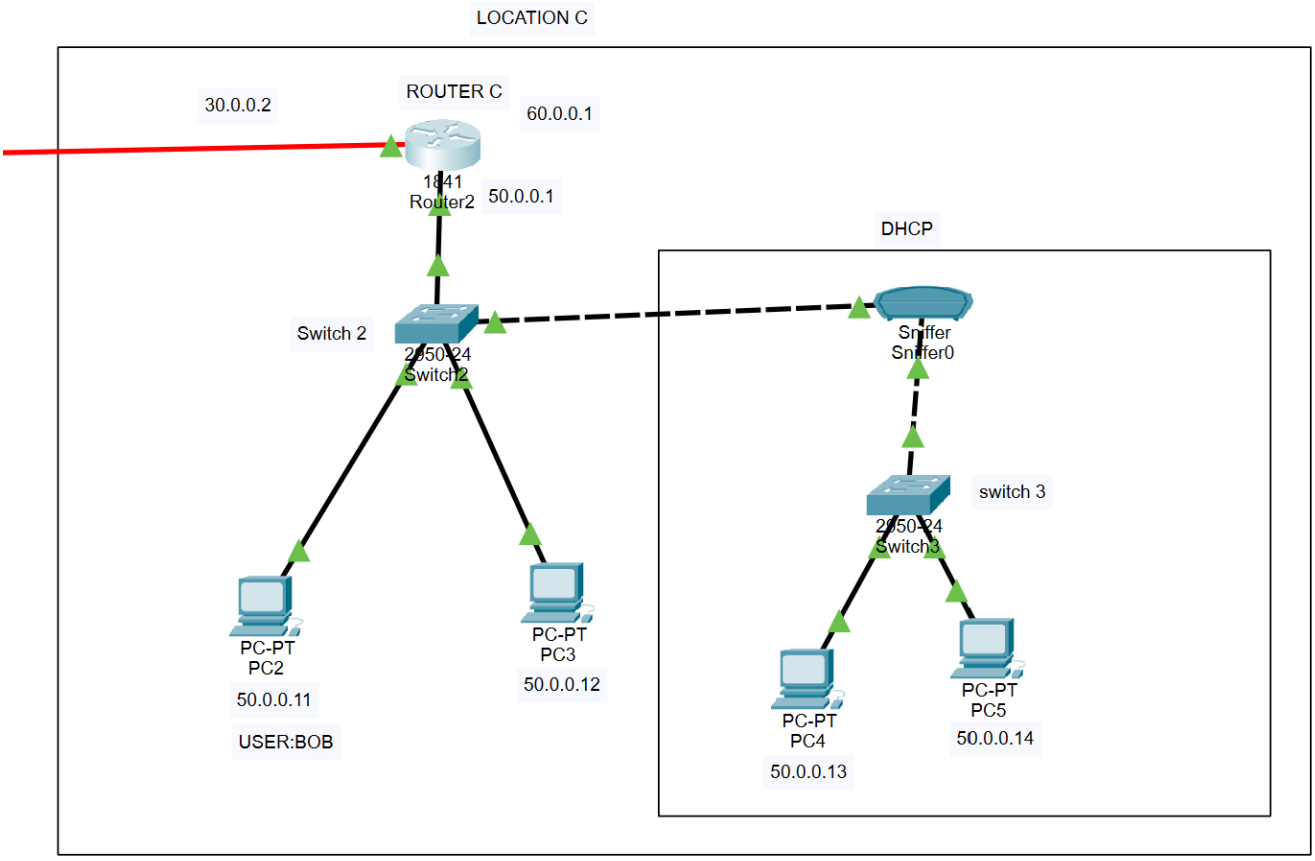
Network

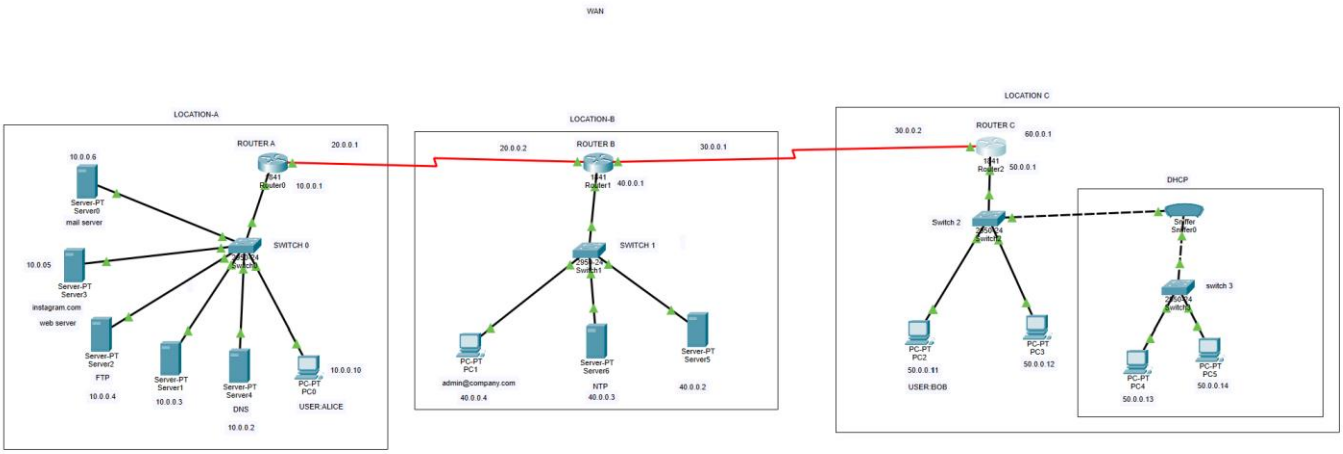
Add

Network Address
10.0.0.0
20.0.0.0
30.0.0.0
40.0.0.0
50.0.0.0

Remove

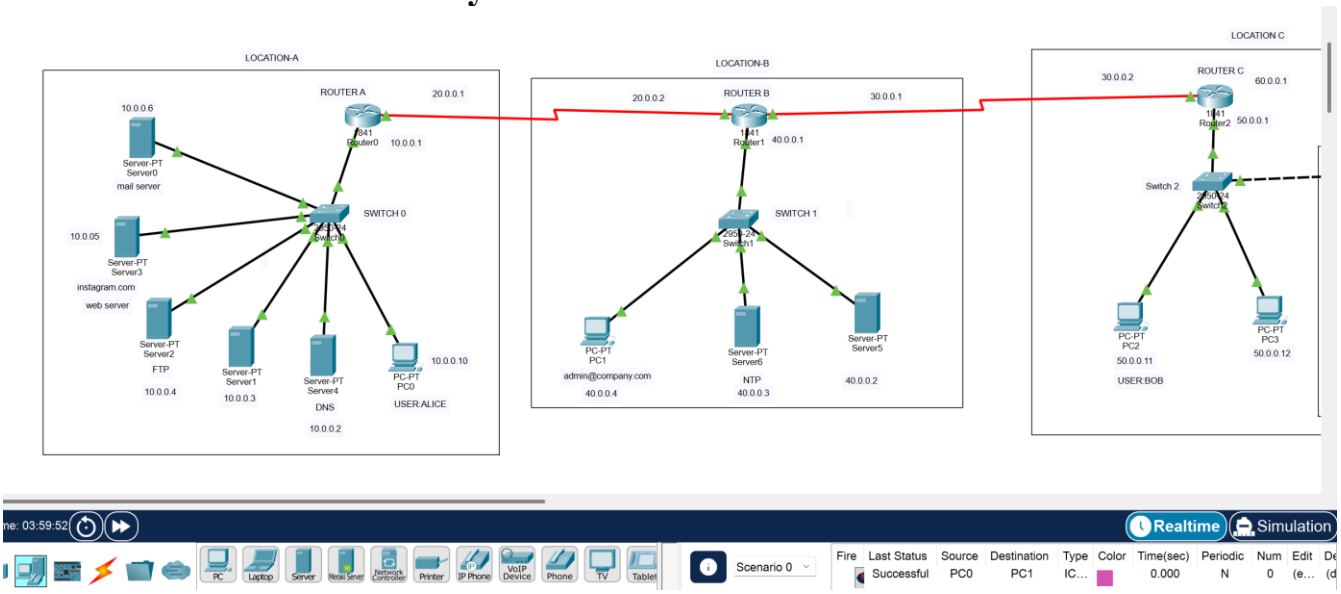


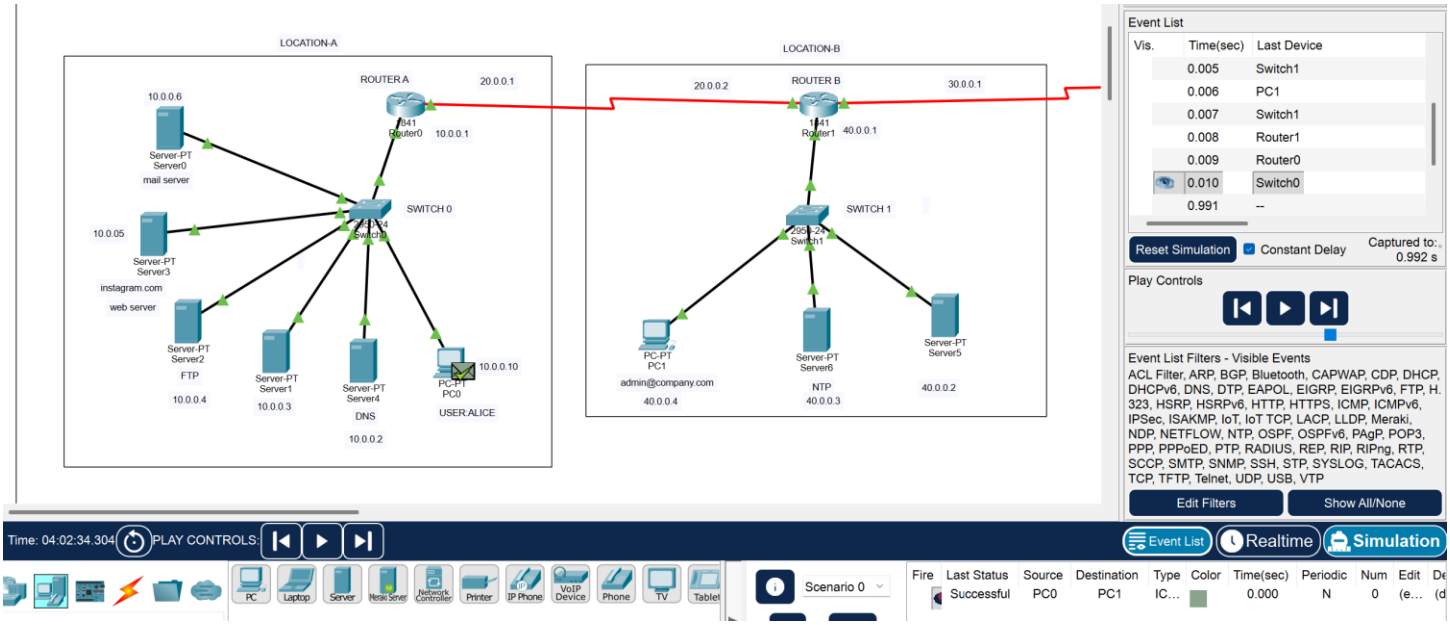

LOCATION C
30.0.0.2
ROUTER C
60.0.0.1
1841
Router2
50.0.0.1
DHCP
Switch 2
2950-24
Switch2
Sniffer
Sniffer0
switch 3
2950-24
Switch3
PC-PT
PC2
50.0.0.11
USER:BOB
PC-PT
PC3
50.0.0.12
PC-PT
PC4
50.0.0.13
PC-PT
PC5
50.0.0.14


WAN
LOCATION-A
ROUTER A
SWITCH 0
LOCATION-B
ROUTER B
SWITCH 1
LOCATION C
ROUTER C
DHCP
Switch 2
switch 3
USER:BOB
USER:ALICE

4.2 TESTS/Experiments:

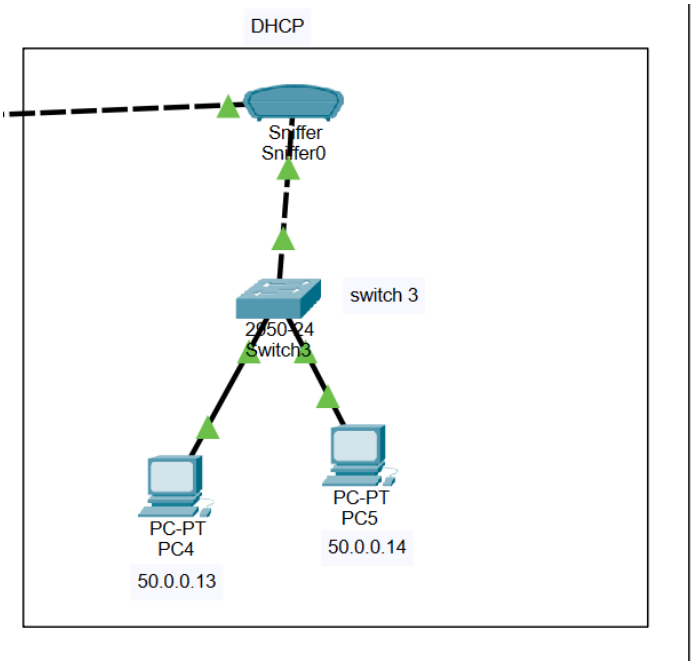
1. WAN Network Connectivity Test:



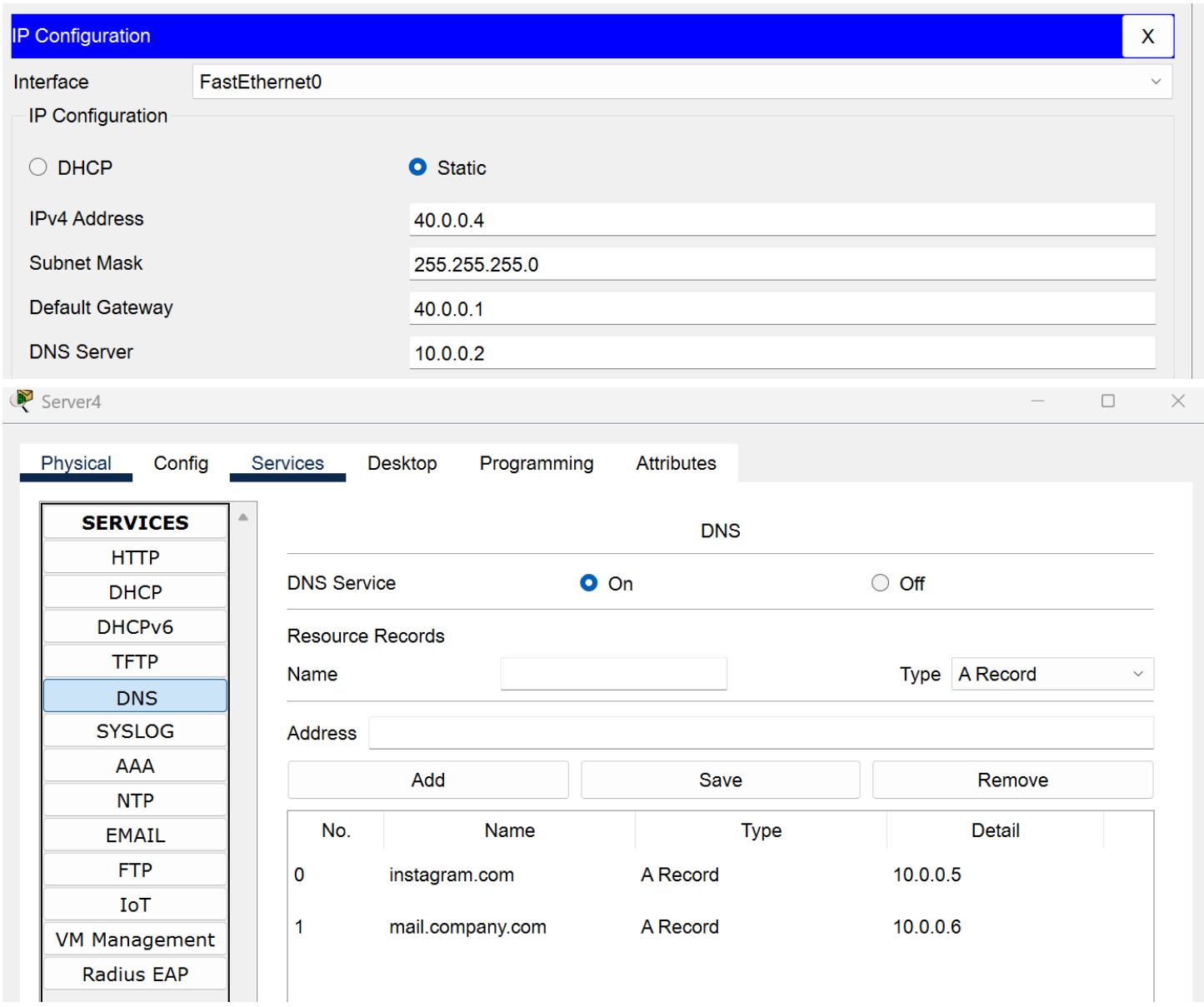


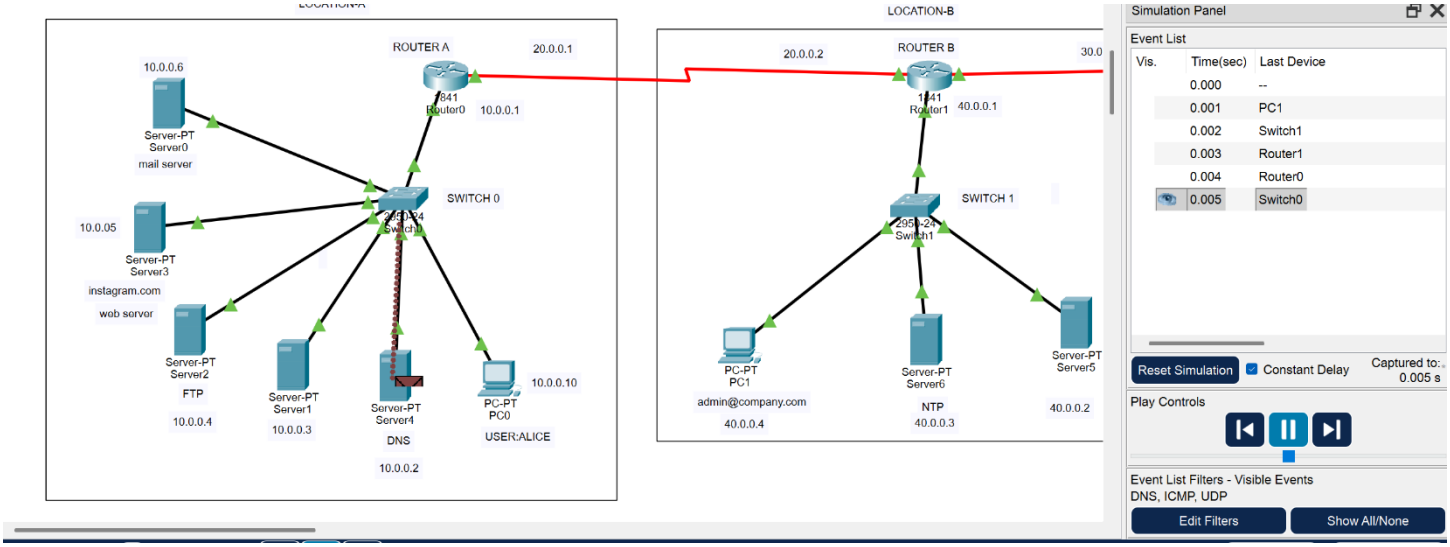
```
Pinging 50.0.0.11 with 32 bytes of data:

Request timed out.
Reply from 50.0.0.11: bytes=32 time=26ms TTL=125
Reply from 50.0.0.11: bytes=32 time=20ms TTL=125
Reply from 50.0.0.11: bytes=32 time=28ms TTL=125

Ping statistics for 50.0.0.11:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 28ms, Average = 24ms
```

2. Static IP and Dynamic IP Configuration Test:



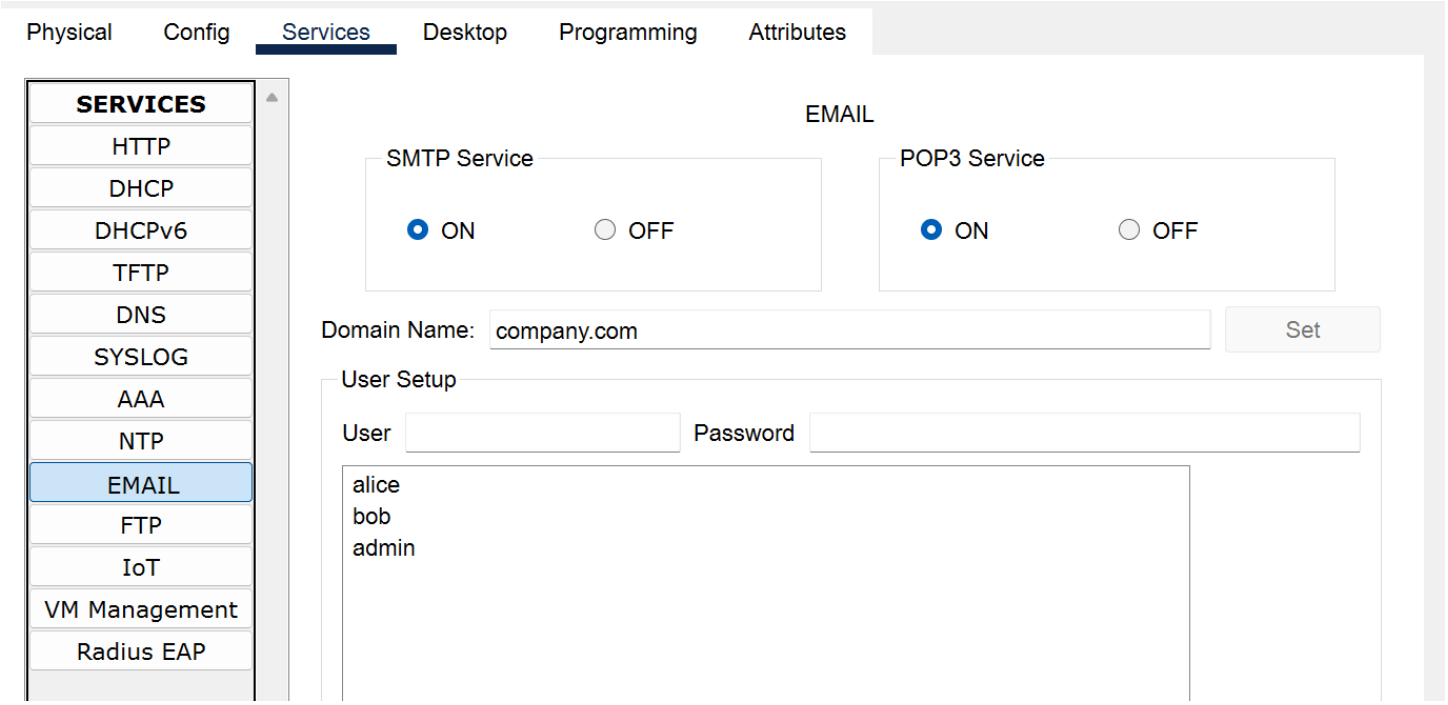
3. DNS Functionality Test:

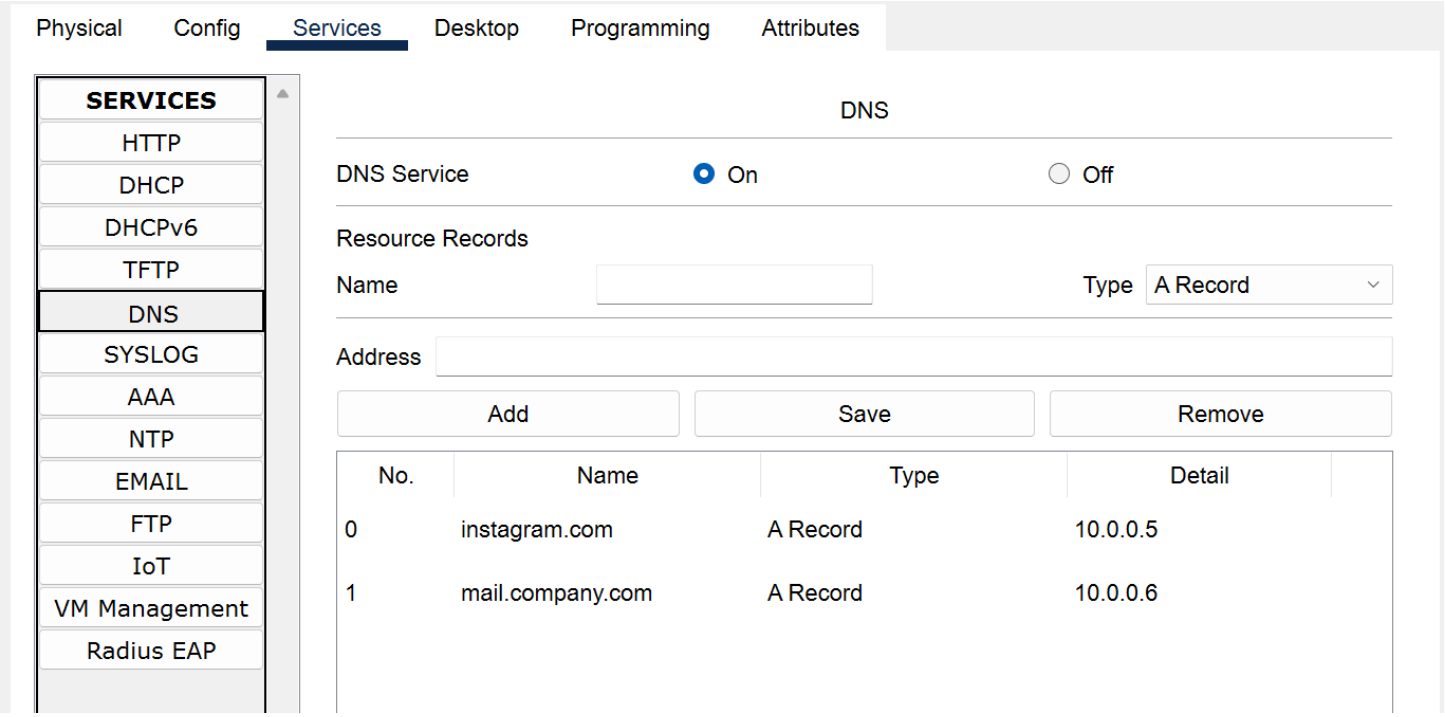


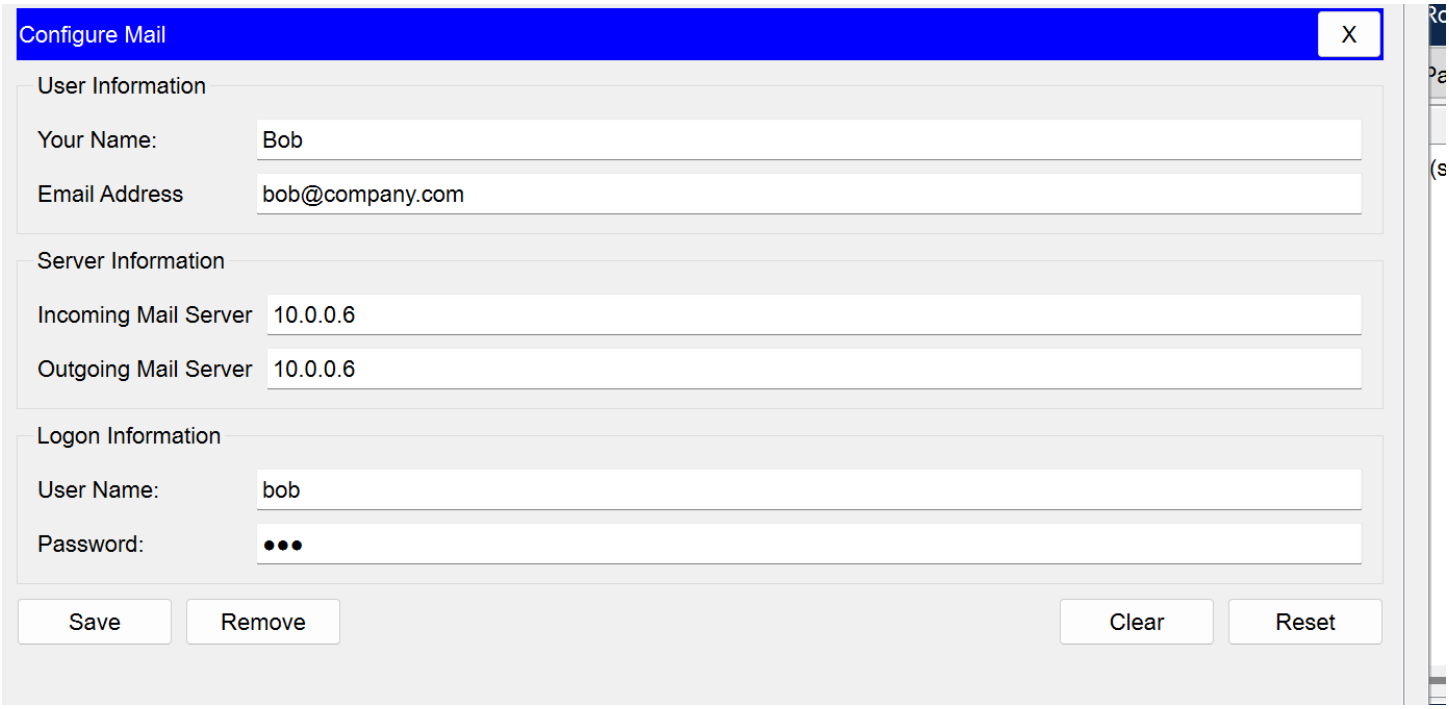


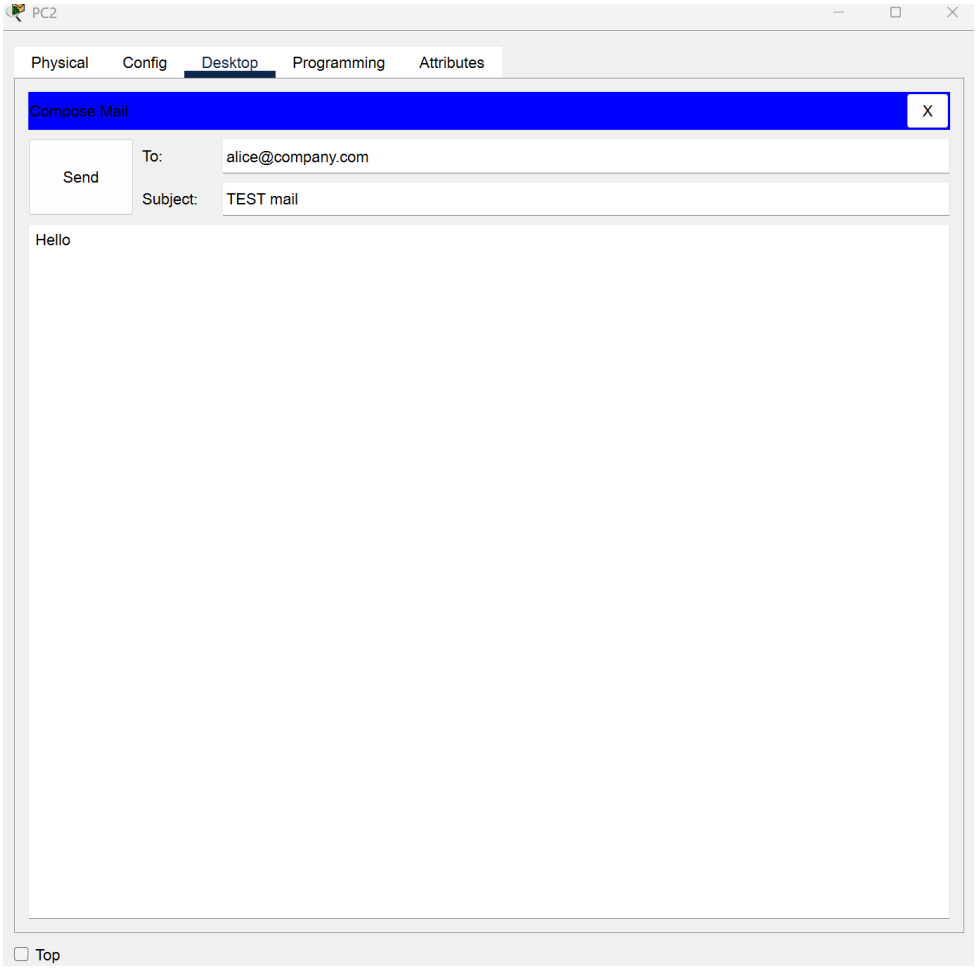

```
C:\>ping mail.company.com

Pinging 10.0.0.6 with 32 bytes of data:

Reply from 10.0.0.6: bytes=32 time=10ms TTL=126
Reply from 10.0.0.6: bytes=32 time=10ms TTL=126
Reply from 10.0.0.6: bytes=32 time=10ms TTL=126
Reply from 10.0.0.6: bytes=32 time=10ms TTL=126

Ping statistics for 10.0.0.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 10ms, Average = 10ms
```

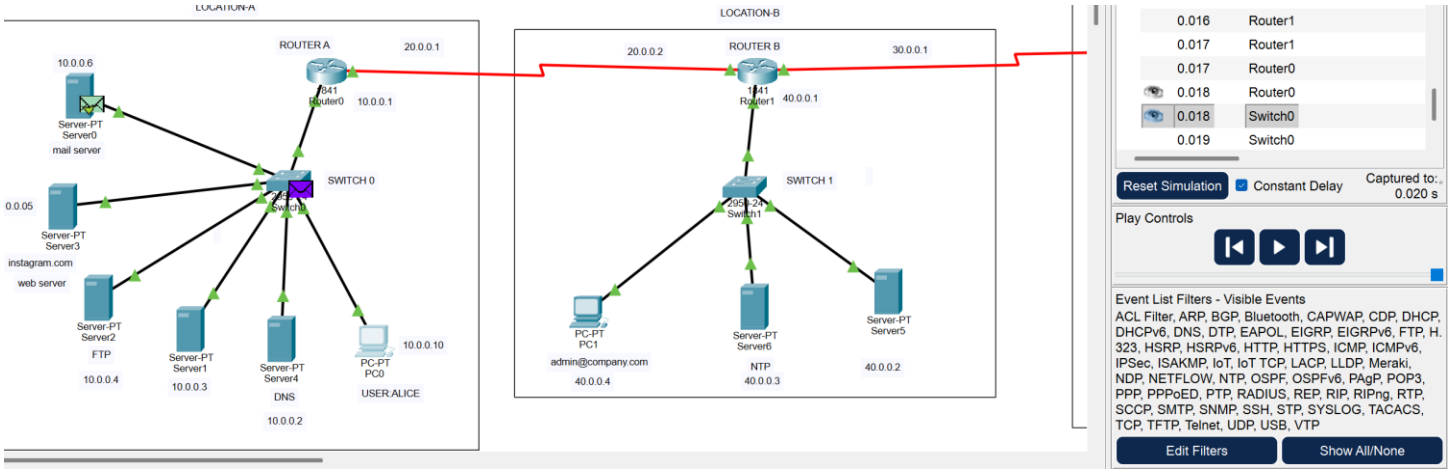
4. Email Communication Test:

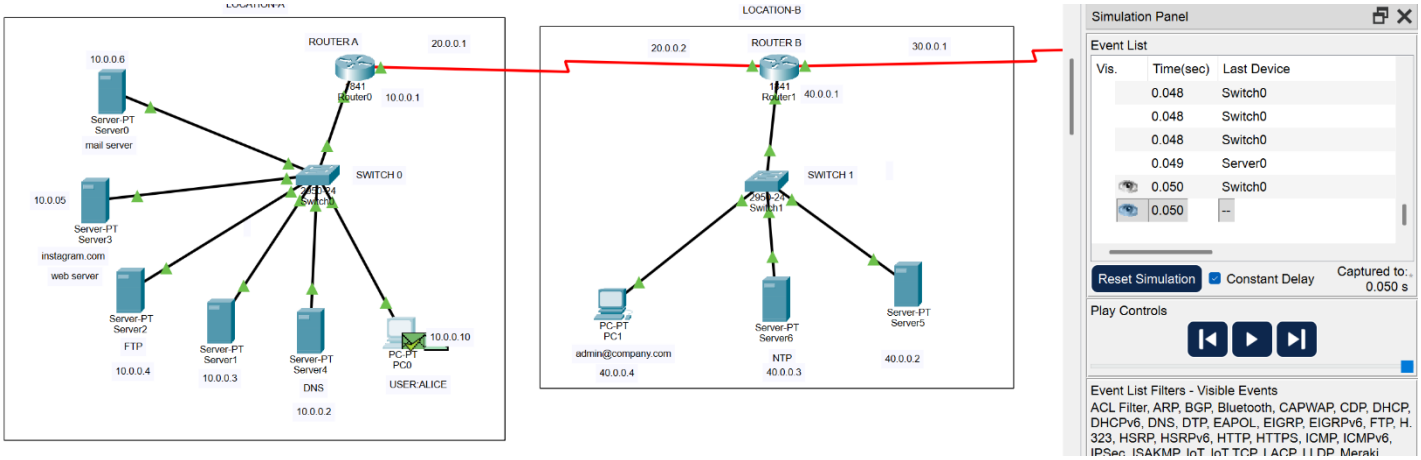



Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
DNS
DNS Service
On
Off
Resource Records
Name
Type
A Record
Address
Add
Save
Remove
No.
Name
Type
Detail
0
instagram.com
A Record
10.0.0.5
1
mail.company.com
A Record
10.0.0.6


Configure Mail
X
User Information
Your Name:
Bob
Email Address
bob@company.com
Server Information
Incoming Mail Server
10.0.0.6
Outgoing Mail Server
10.0.0.6
Logon Information
User Name:
bob
Password:
Save
Remove
Clear
Reset


PC2
Physical
Config
Desktop
Programming
Attributes
Compose Mail
X
Send
To:
alice@company.com
Subject:
TEST mail
Hello
Top


LOCATION-A
ROUTER A
20.0.0.1
10.0.0.6
Server-PT Server0
mail server
1841 Router0
10.0.0.1
SWITCH 0
0.0.05
Server-PT Server3
instagram.com
web server
Server-PT Server2
FTP
10.0.0.4
Server-PT Server1
10.0.0.3
Server-PT Server4
DNS
10.0.0.2
PC-PT PC0
10.0.0.10
USER:ALICE
LOCATION-B
20.0.0.2
ROUTER B
30.0.0.1
1841 Router1
40.0.0.1
SWITCH 1
PC-PT PC1
admin@company.com
40.0.0.4
Server-PT Server6
NTP
40.0.0.3
Server-PT Server5
40.0.0.2
0.016 Router1
0.017 Router1
0.017 Router0
0.018 Router0
0.018 Switch0
0.019 Switch0
Reset Simulation
Constant Delay
Captured to:
0.020 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, Meraki, 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



MAIL BROWSER

X

Mails

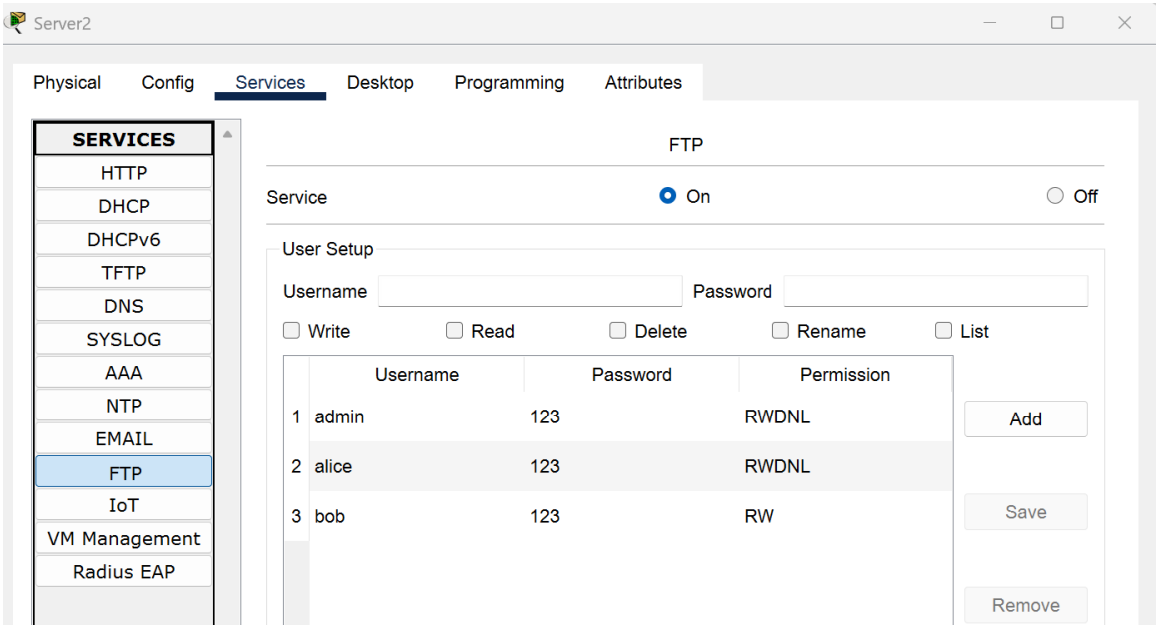
Compose | Reply | Receive | Delete | Configure Mail

	From	Subject	Received
1	bob@company.com	TEST mail	Thu Oct 23 2025 20:26:14

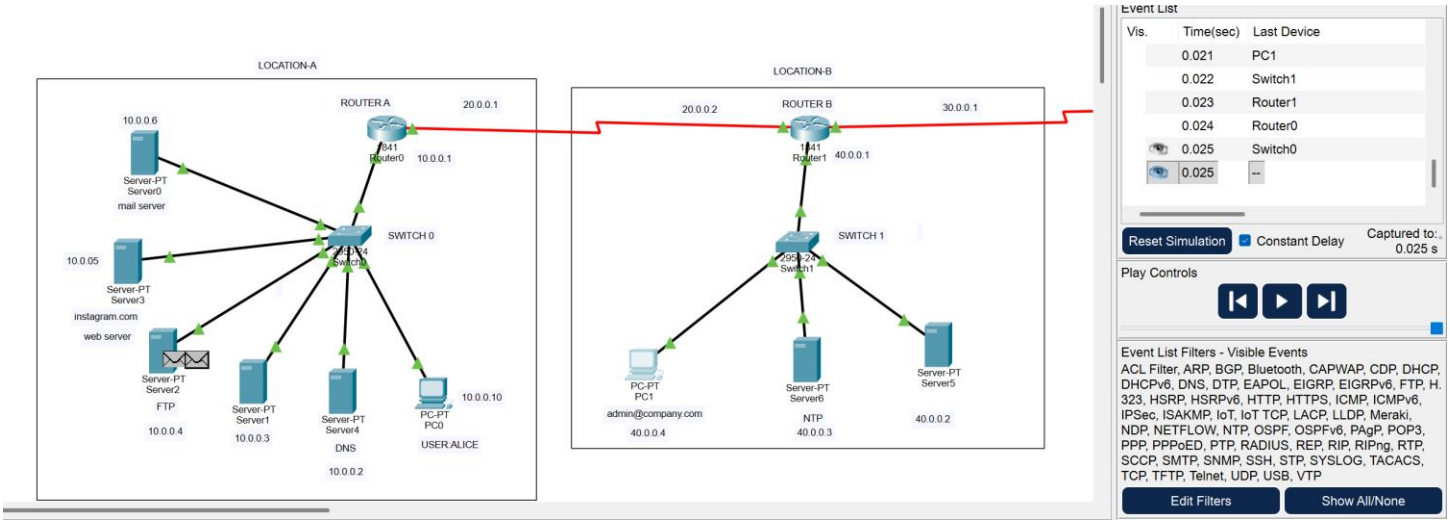
Receiving mail from POP3 Server 10.0.0.6
Receive Mail Success.

Cancel
Send/Receive

5. FTP (File Transfer Protocol) Service Test:




```
C:\>ftp 10.0.0.4
Trying to connect...10.0.0.4
Connected to 10.0.0.4
220- Welcome to PT Ftp server
Username:admin
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 10.0.0.4:
0    : asa842-k8.bin                                  5571584
1    : asa923-k8.bin                                  30468096
2    : c1841-advipservicesk9-mz.124-15.T1.bin         33591768
3    : c1841-ipbase-mz.123-14.T7.bin                  13832032
4    : c1841-ipbasek9-mz.124-12.bin                   16599160
5    : c1900-universalk9-mz.SPA.155-3.M4a.bin         33591768
6    : c2600-advipservicesk9-mz.124-15.T1.bin         33591768
7    : c2600-i-mz.122-28.bin                          5571584
8    : c2600-ipbasek9-mz.124-8.bin                    13169700
9    : c2800nm-advipservicesk9-mz.124-15.T1.bin       50938004
10   : c2800nm-advipservicesk9-mz.151-4.M4.bin        33591768
11   : c2800nm-ipbase-mz.123-14.T7.bin                5571584
12   : c2800nm-ipbasek9-mz.124-8.bin                  15522644
13   : c2900-universalk9-mz.SPA.155-3.M4a.bin         33591768
14   : c2950-i6q4l2-mz.121-22.EA4.bin                 3058048
15   : c2950-i6q4l2-mz.121-22.EA8.bin                 3117390
16   : c2960-lanbase-mz.122-25.FX.bin                 4414921
17   : c2960-lanbase-mz.122-25.SEE1.bin               4670455
18   : c2960-lanbasek9-mz.150-2.SE4.bin               4670455
19   : c3560-advipservicesk9-mz.122-37.SE1.bin        8662192
20   : c3560-advipservicesk9-mz.122-46.SE.bin         10713279
21   : c800-universalk9-mz.SPA.152-4.M4.bin           33591768
22   : c800-universalk9-mz.SPA.154-3.M6a.bin          83029236
23   : cat3k_caa-universalk9.16.03.02.SPA.bin         505532849
24   : cgr1000-universalk9-mz.SPA.154-2.CG            159487552
25   : cgr1000-universalk9-mz.SPA.156-3.CG            184530138
26   : ir800-universalk9-bundle.SPA.156-3.M.bin       160968869
27   : ir800-universalk9-mz.SPA.155-3.M               61750062
28   : ir800-universalk9-mz.SPA.156-3.M               63753767
```

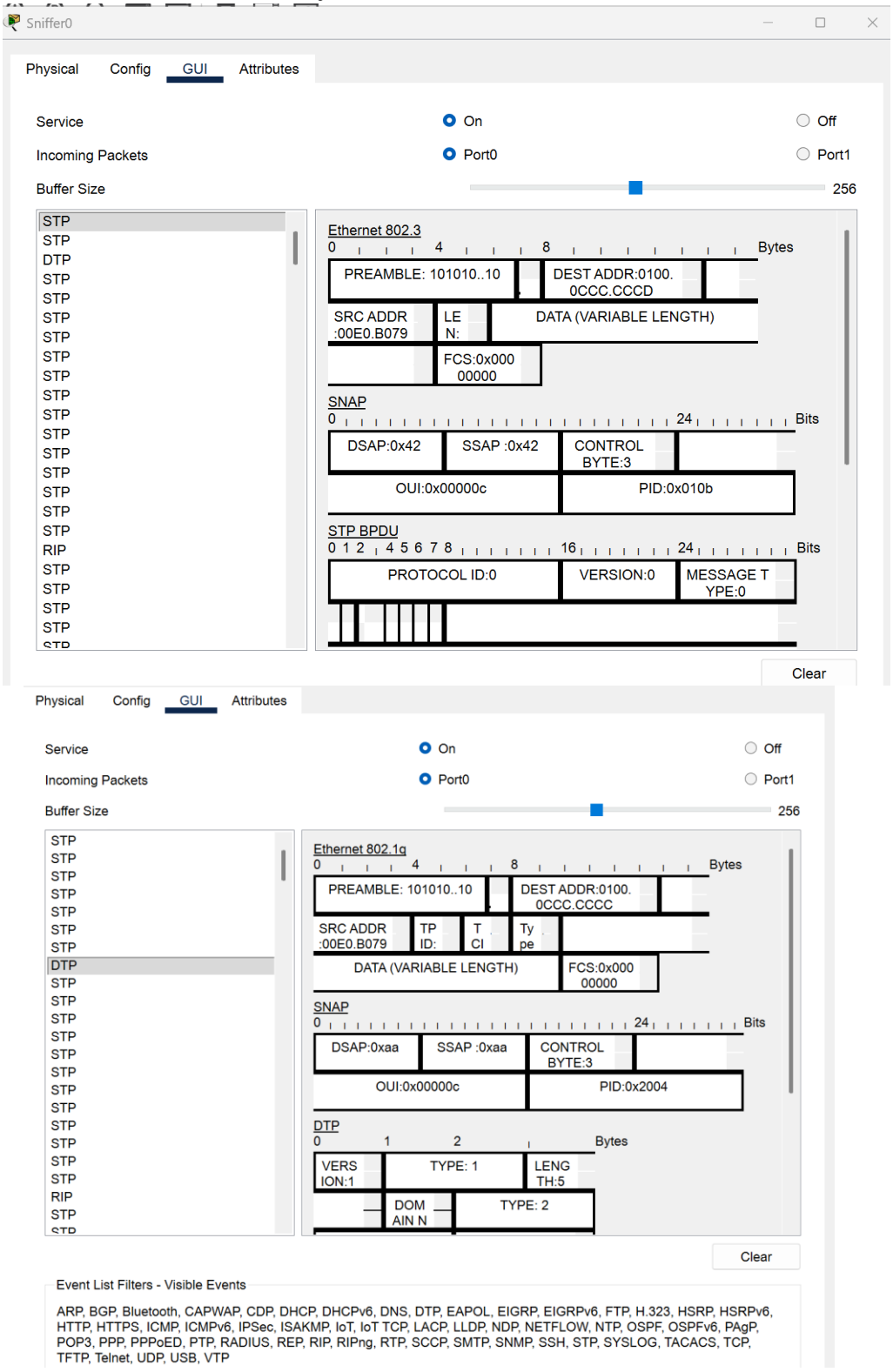


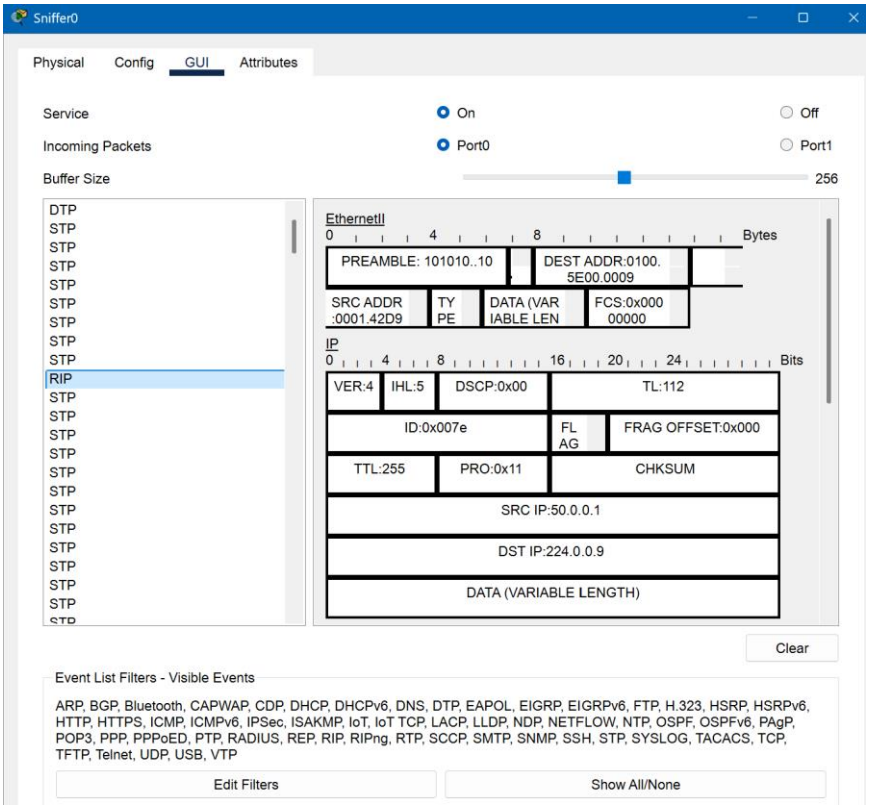
6. Packet Loss and Efficiency Test:

```
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=40ms TTL=125
Reply from 10.0.0.2: bytes=32 time=2ms TTL=125
Reply from 10.0.0.2: bytes=32 time=2ms TTL=125
Reply from 10.0.0.2: bytes=32 time=2ms TTL=125

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 40ms, Average = 11ms
```

```
C:\>ping 10.0.0.3

Pinging 10.0.0.3 with 32 bytes of data:

Request timed out.
Reply from 10.0.0.3: bytes=32 time=2ms TTL=125
Reply from 10.0.0.3: bytes=32 time=39ms TTL=125
Reply from 10.0.0.3: bytes=32 time=23ms TTL=125

Ping statistics for 10.0.0.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 39ms, Average = 21ms
```

7. Packet Sniffer Analysis:





8.Access control protocol Test:

```
Router>enable
Router#show access-lists
Extended IP access list 100
    10 deny tcp 50.0.0.0 0.0.0.255 host 10.0.0.2 eq ftp
    20 permit ip any any (180 match(es))
```

```
C:\>ftp 10.0.04
Trying to connect...10.0.04
Could not open connection to the host, on port 21: Connect failed
C:\>
```

```
C:\>ftp 10.0.0.2
Trying to connect...10.0.0.2

%Error opening ftp://10.0.0.2/ (Timed out)
.


(Disconnecting from ftp server)
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 10.0.0.4
Trying to connect...10.0.0.4
Connected to 10.0.0.4
220- Welcome to PT Ftp server
Username:alice
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 10.0.0.4:
0   : asa842-k8.bin                                 5571584
1   : asa923-k8.bin                                 30468096
2   : c1841-advipservicesk9-mz.124-15.T1.bin        33591768
3   : c1841-ipbase-mz.123-14.T7.bin                 13832032
4   : c1841-ipbasek9-mz.124-12.bin                  16599160
5   : c1900-universalk9-mz.SPA.155-3.M4a.bin        33591768
6   : c2600-advipservicesk9-mz.124-15.T1.bin        33591768
7   : c2600-i-mz.122-28.bin                         5571584
8   : c2600-ipbasek9-mz.124-8.bin                   13169700
9   : c2800nm-advipservicesk9-mz.124-15.T1.bin      50938004
10  : c2800nm-advipservicesk9-mz.151-4.M4.bin       33591768
11  : c2800nm-ipbase-mz.123-14.T7.bin               5571584
12  : c2800nm-ipbasek9-mz.124-8.bin                 15522644
13  : c2900-universalk9-mz.SPA.155-3.M4a.bin        33591768
14  : c2950-i6q412-mz.121-22.EA4.bin                3058048
15  : c2950-i6q412-mz.121-22.EA8.bin                3117390
16  : c2960-lanbase-mz.122-25.FX.bin                4414921
17  : c2960-lanbase-mz.122-25.SEE1.bin              4670455
18  : c2960-lanbasek9-mz.150-2.SE4.bin              4670455
19  : c3560-advipservicesk9-mz.122-37.SE1.bin       8662192
20  : c3560-advipservicesk9-mz.122-46.SE.bin        10713279
21  : c800-universalk9-mz.SPA.152-4.M4.bin          33591768
22  : c800-universalk9-mz.SPA.154-3.M6a.bin         83029236
23  : cat3k_caa-universalk9.16.03.02.SPA.bin        505532849
24  : cgr1000-universalk9-mz.SPA.154-2.CG           159487552
25  : cgr1000-universalk9-mz.SPA.156-3.CG           184530138
26  : ir800-universalk9-bundle.SPA.156-3.M.bin      160968869
27  : ir800-universalk9-mz.SPA.155-3.M              61750062
```

Chapter-5

Conclusion and Future Scope

5.1 Conclusion

This project successfully designed, implemented, and validated an enhanced Wide Area Network (WAN) architecture that addresses the primary limitations of foundational, static network models. The work commenced by analyzing a baseline WAN model, similar to that proposed by Bhola et al. [21], which connected multiple branch offices to a headquarters using static routing. While functional, this model was identified as lacking scalability, fault tolerance, and active security—three critical components for any modern enterprise network.

The core of this project involved the methodical enhancement of this baseline model within the Cisco Packet Tracer simulation environment. The following conclusions were drawn from the implementation and testing:

- Successful Implementation of Dynamic Routing: The static routing configuration was replaced with a dynamic routing protocol (OSPF/EIGRP). The results confirmed that this implementation was successful, as routers automatically discovered adjacent networks, populated their routing tables, and calculated the most efficient paths for data transmission. This enhancement directly addresses the scalability and administrative overhead limitations of the static model[7].
- Demonstrated Fault Tolerance: By simulating link failures between routers, the network's resilience was tested. The dynamic routing protocol successfully detected the topology change and automatically reconverged, redirecting traffic over an alternative path. This test confirmed the network's high availability and fault tolerance, a critical improvement over the fragile static-routed baseline[8].
- Effective Security Policy Enforcement: The implementation of Access Control Lists (ACLs) provided a necessary and effective layer of network security. Testing confirmed that the ACLs successfully filtered traffic as intended, blocking unauthorized access from guest networks to secure servers at the headquarters while permitting all legitimate corporate communication[3].
- In summary, this project achieved its objective by transforming a basic, static WAN design into a robust, scalable, and secure network. The resulting architecture, validated through simulation, serves as a far more practical and industry-relevant model for a modern, geographically distributed organization[13].

5.2 Future Scope

While this project represents a significant functional improvement, several avenues exist for future expansion and research. The following points outline a lucid scope for future work:

- Integration of SD-WAN: The current model could be migrated to a Software-Defined WAN (SD-WAN) architecture. This would abstract the control plane from the hardware, allowing for centralized management, dynamic path selection based on application performance, and simpler integration of cloud services, aligning with current industry trends[14].

- Advanced Security Implementation: Security could be further enhanced by moving beyond standard/extended ACLs to a Zone-Based Policy Firewall (ZBFW) configuration on the routers. Additionally, implementing IPsec VPN tunnels between the headquarters and branch offices would encrypt all data in transit, protecting sensitive corporate information from eavesdropping[16].

- Quality of Service (QoS) Implementation: The current network treats all data equally. Future work could involve implementing QoS policies to prioritize critical, delay-sensitive traffic such as Voice over IP (VoIP) and video conferencing over less-critical, bulk-data transfers. This would ensure reliable performance for real-time applications[14].

- Performance Benchmarking: A comparative study could be conducted by implementing different dynamic routing protocols (e.g., EIGRP vs. OSPF) or by comparing the performance of this traditional WAN against an SD-WAN [1] or MPTCP-based solution [10] under various load and link-failure scenarios[13].

- Expanding Branch Office Services: The branch office LANs could be expanded to include Wireless LANs (WLANs) with robust WPA2/WPA3 security and segregated guest access, reflecting a more realistic office environment[18].

References

[1] Always, K., Jha, D.N., Hernandez, E., Puthal, D., Barika, M., Varghese, B., Garg, S.K., et al.: "Iotsim-sdwan: A Simulation Framework for Interconnecting Distributed Datacenters Over Software-Defined Wide Area Network (sdwan)", Journal of Parallel and Distributed Computing, vol. 143, pp. 17-35, 2020.

[2] Ikpehai, A., Adebisi, B., Rabie, K.M., Anoh, K., Ande, R.E., Hammoudeh, M., Gacanin, H., and Mbanaso, U.M.: "Low-Power Wide Area Network Technologies for Internet-of-Things: A Comparative Review", IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2225-2240, 2018.

[3] Rady, M., Hafeez, M., and Zaidi, S.A.R.: "Computational Methods for Network-Aware and Network-Agnostic IoT Low Power Wide Area Networks (LPWANs)", IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5732-5744, 2019.

[4] Gao, S., Zhang, X., Du, C., and Ji, Q.: "A Multichannel Low-Power Wide-Area Network with High-Accuracy Synchronization Ability for Machine Vibration Monitoring", IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5040-5047, 2019.

[5] Duliński, Z., Stankiewicz, R., Rzym, G., and Wydrych, P.: "Dynamic Traffic Management for SD-WAN Inter-Cloud Communication", IEEE Journal on Selected Areas in Communications, vol. 38, no. 7, pp. 1335-1351, 2020.

[6] Jiang, X., Zhang, H., Yi, E.A.B., Raghunathan, N., Mousoulis, C., Chaterji, S., Peroulis, D., Shakouri, A., and Bagchi, S.: "Hybrid Low-Power Wide-Area Mesh Network for IoT Applications", IEEE Internet of Things Journal, vol. 8, no. 2, pp. 901-915, 2020.

[7] Cui, S., and Joe, I.: "Collision Prediction for a Low Power Wide Area Network Using Deep Learning Methods", Journal of Communications and Networks, vol. 22, no. 3, pp. 205-214, 2020.

[8] Yunus, N.A.M., Othman, M., Hanapi, Z.M., and Lun, K.Y.: "Enhancement Replicated Network: A Reliable Multistage Interconnection Network Topology", IEEE Systems Journal, vol. 13, no. 3, pp. 2653-2663, 2018.

[9] Zhao, O., Liao, W.S., Ishizu, K., and Kojima, F.: "Dynamic and Non-Centric Networking Approach Using Virtual Gateway Platforms for Low Power Wide Area Systems", IEEE Access, vol. 7, pp. 186078-186090, 2019.

[10] Zhang, Y., Tourrilhes, J., Zhang, Z.L., and Sharma, P.: "Improving sd-wan Resilience: From Vertical Handoff to Wan-Aware MPTCP", IEEE Transactions on Network and Service Management, vol. 18, no. 1, pp.

347-361, 2021.

[11] Guan, W., Zhang, H., and Leung, V.C.M.: “Analysis of Traffic Performance on Network Slicing Using Complex Network Theory”, IEEE Transactions on Vehicular Technology, vol. 69, no. 12, pp. 15188-15199, 2020.

[12] Fan, W., Xiao, F., Chen, X., Cui, L., and Yu, S.: “Efficient Virtual Network Embedding of Cloud-Based Data Center Networks Into Optical Networks”, IEEE Transactions on Parallel and Distributed Systems, vol. 32, no. 11, pp. 2793-2808, 2021.

[13] Jain, J., Jain, A., Srivastava, S.K., Verma, C., Raboaca, M.S., & Illés, Z.: “Improved Security of E-Healthcare Images Using Hybridized Robust Zero-Watermarking and Hyper-Chaotic System Along with RSA”, Mathematics, vol. 10, no. 7, pp. 1071, 2022.

[14] Jain, J., & Jain, A.: “Securing E-Healthcare Images Using an Efficient Image Encryption Model”, Scientific Programming, vol. 2022, 2022.

[15] Sharma, S.K., Jain, A., Gupta, K., Prasad, D., & Singh, V.: “An Internal Schematic View and Simulation of Major Diagonal Mesh Network-on-Chip”, Journal of Computational and Theoretical Nanoscience, vol. 16, no. 10, pp. 4412-4417, 2019.

[16] Jain, A., Dwivedi, R.K., Alshazly, H., Kumar, A., Bourouis, S., & Kaur, M.: “Design and Simulation of Ring Network-on-Chip for Different Configured Nodes”, Computers, Materials & Continua, vol. 71, no. 2, pp. 4085-4100, 2022.

[17] Jain, A., & Kumar, A.: “Desmogging of Still Smoggy Images Using a Novel Channel Prior”, Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 1, pp. 1161-1177, 2021.

[18] Kumar, A., & Jain, A.: “Image Smog Restoration Using Oblique Gradient Profile Prior and Energy Minimization”, Frontiers of Computer Science, vol. 15, no. 6, pp. 1-7, 2021.

[19] Kumar, S., Jain, A., Kumar Agarwal, A., Rani, S., & Ghimire, A.: “Object-Based Image Retrieval Using the U-Net-Based Neural Network”, Computational Intelligence and Neuroscience, vol. 2021, 2021.

[20] Kumar, S., Jain, A., Shukla, A.P., Singh, S., Raja, R., Rani, S., ... & Masud, M.: “A Comparative Analysis of Machine Learning Algorithms for Detection of Organic and Nonorganic Cotton Diseases”, Mathematical Problems in Engineering, vol. 2021, 2021.

[21] Bhola, A., Lakshmi Tulasi, M., Jain, A., Hari Chandana, D., and Lakshmi Bhavani, D.: “A Wide Area Network Design and Architecture using Cisco Packet Tracer”, 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), pp. 1646-1652, 2022