PES UNIVERSITY

Department of Computer Science & Engineering

UE22CS252B – COMPUTER NETWORKS

Mini Project Report

Financial Institution Network System

Team Number-11

Submitted to:

Dr. Geetha Dayalan

Associate Professor

Submitted By:

Name Shaswetha

SRN-PES2UG22CSC523

Name- Sharikha M

SRN-PES2UG22CS517

IV Semester

Section I

Table of Contents

Abstract

Abstract: This project aims to build a strong network infrastructure for a finance service provider, focusing on LAN, WAN, and server hosting
integration. It includes implementing dual ISPs for backup and separating departments for security. Key goals are to improve performance, redundancy, scalability, and availability. Cisco Catalyst routers and switches are chosen for their reliability. Virtual Private Networks (VPNs) and Access Control Lists (ACLs) enhance security. Overall, the project seeks to create a secure and reliable network infrastructure tailored to the finance provider's needs.

Introduction

In today's interconnected world, a reliable and secure network infrastructure is crucial for the seamless operation of organizations, especially in the finance sector. Financial Services Ltd (FSL), a prominent finance service provider recognizes the importance of maintaining a robust network infrastructure to support its operations effectively. With a commitment to delivering online finance solutions and services to its clients, FSL has embarked on a project to overhaul its network infrastructure, focusing on LAN, WAN, and server hosting integration. This project aims to address the evolving needs of FSL by designing and implementing a network infrastructure that prioritizes performance, redundancy, scalability, and availability. With an emphasis on security, the project encompasses the integration of dual Internet Service Providers (ISPs) for backup, departmental segregation for enhanced security measures, and the deployment of Virtual Private Networks (VPNs) and Access Control Lists (ACLs) to safeguard sensitive data. Through the utilization of Cisco Catalyst routers and switches renowned for their reliability, this project seeks to create a network infrastructure tailored to the specific requirements of FSL. By implementing VLANs, VoIP, and other essential networking components, the infrastructure will enable seamless communication and collaboration among departments while ensuring efficient resource utilization. This report provides a comprehensive overview of the design and implementation process, detailing the hardware and software requirements, configuration steps, and results. By undertaking this project, FSL endeavors to enhance its operational efficiency, strengthen its security posture, and ultimately deliver superior financial services to its clients

Scope

1. Network Infrastructure Design: Design and implement a comprehensive network infrastructure using Cisco Packet Tracer, focusing on routers, switches, VLANs, VoIP, and security features.
2. VLAN Configuration: Configure VLANs to segregate departments within the organization, ensuring security and network performance.
3. DNS Setup:
DNS servers to manage domain name resolution within the network.
4. VoIP Integration: Integrate VoIP services to enable internal communication within departments, ensuring seamless connectivity and call quality.
5. Security Measures: Implement robust security measures, including access control lists (ACLs), port security, and SSH configuration, to safeguard the network from unauthorized access and cyber threats.
6. Redundancy and Load Balancing: Configure dual ISP connections for redundancy and load balancing, ensuring uninterrupted internet connectivity for the organization.
7. VPN Configuration: Set up site-to-site IPsec VPNs to establish secure communication between the headquarters and external server-side location, ensuring confidentiality and integrity of data transmission.
8. Testing and Performance Analysis: Conduct thorough testing of the network infrastructure and perform performance analysis to evaluate factors such as throughput, latency, and reliability under varying network loads and conditions.

Hardware Requirements:

- No physical hardware required; simulation performed in a virtual environment using network simulation software like Cisco Packet Tracer.

Software Requirements:

1. Simulation Software: Cisco Packet Tracer is employed to configure routers, switches, VLANs, VoIP, and security features, ensuring the network infrastructure meets the financial management project's requirements.

Implementation Details

Basic Settings: Configure hostnames, passwords, and SSH for secure remote access.

VLAN Configuration: Assign VLANs for data and voice traffic, and configure access/trunk ports accordingly.

Switchport Security: Implement security measures on the server-side switch to restrict unauthorized access.

Subnetting & IP Addressing: Perform subnetting to efficiently allocate IP addresses to devices based on network requirements.

OSPF Configuration: Configure OSPF routing protocol on routers and switches to facilitate dynamic routing within the network.

Static IP Assignment: Assign static IP addresses to critical devices in the server room to ensure consistent connectivity.

Inter-VLAN Routing: Enable routing between VLANs to facilitate communication across departments.

Wireless Network Setup: Deploy wireless networks in each department to provide connectivity for user devices.

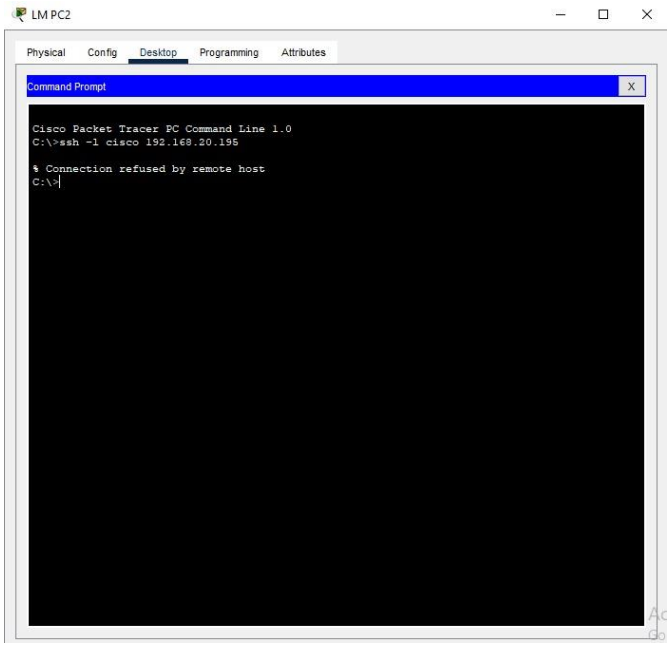
Telephony Service: Configure VoIP services for internal communication within departments, ensuring seamless connectivity.

Standard ACL for SSH: Implement a standard ACL to restrict SSH access to designated ICT department devices, enhancing network security.

PAT & ACL: Configure Port Address Translation (PAT) and Access Control Lists (ACLs) for internet access control, enhancing network security and managing network traffic.

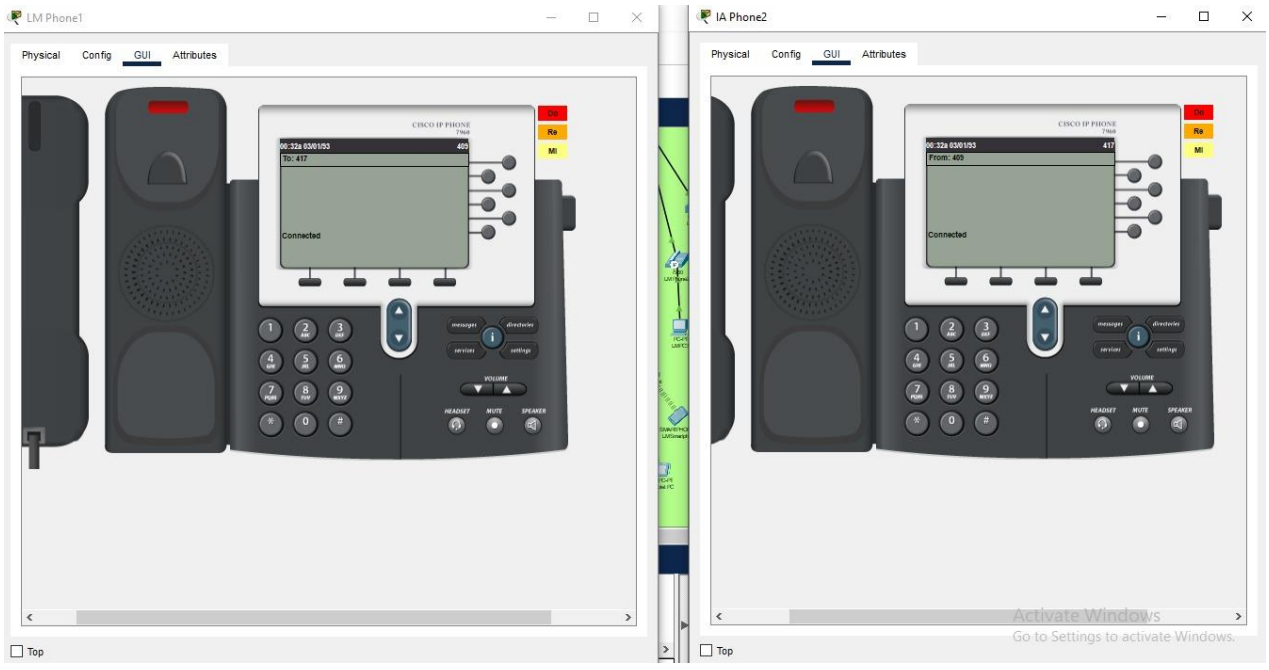
Site-to-Site VPN: Establish a site-to-site IPsec VPN between headquarters and the external server-side location to ensure secure communication.

Results & Discussion (Necessary Screenshots & Description)



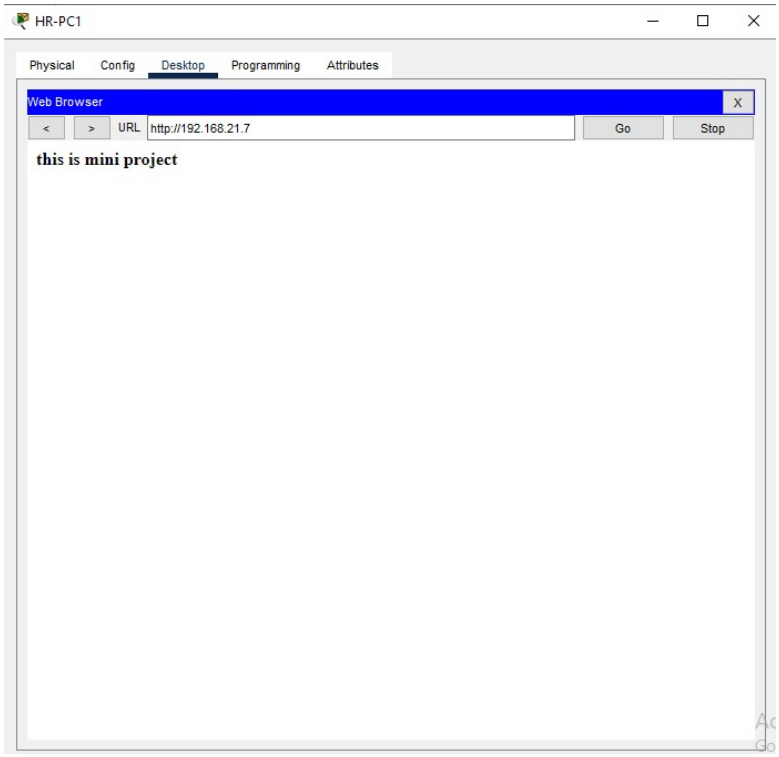
PC are data encrypted and cannot be accessed.

VoIP implementation

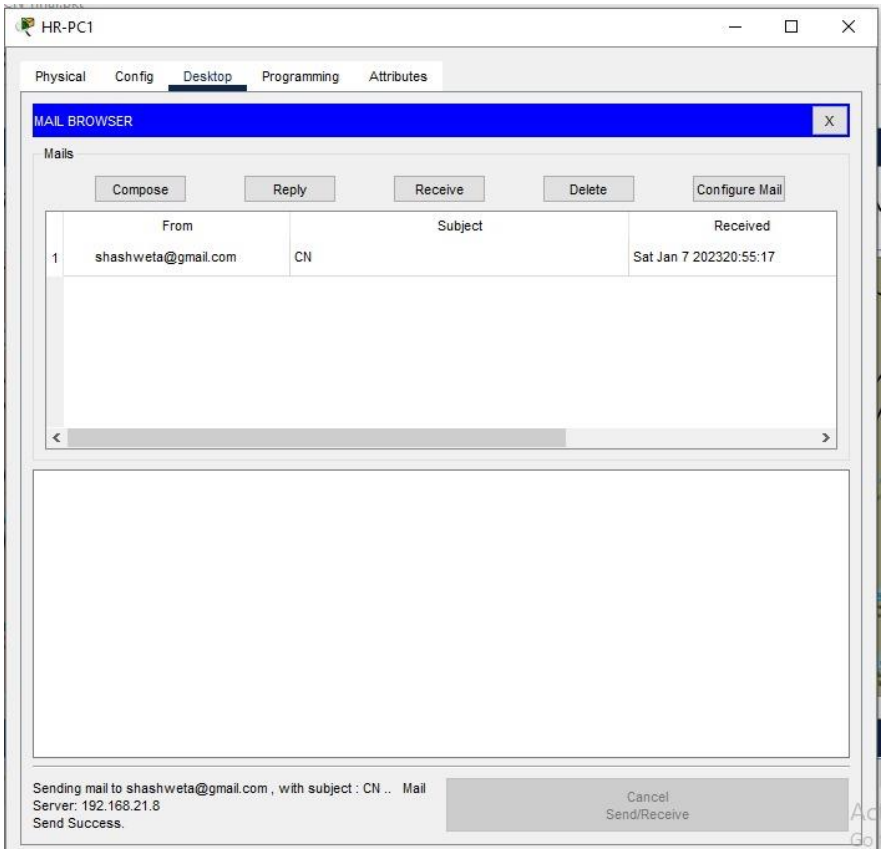


- Enabled VoIP services for intra-departmental communication.
- Configured IP phones within each department to facilitate efficient communication channels.
-

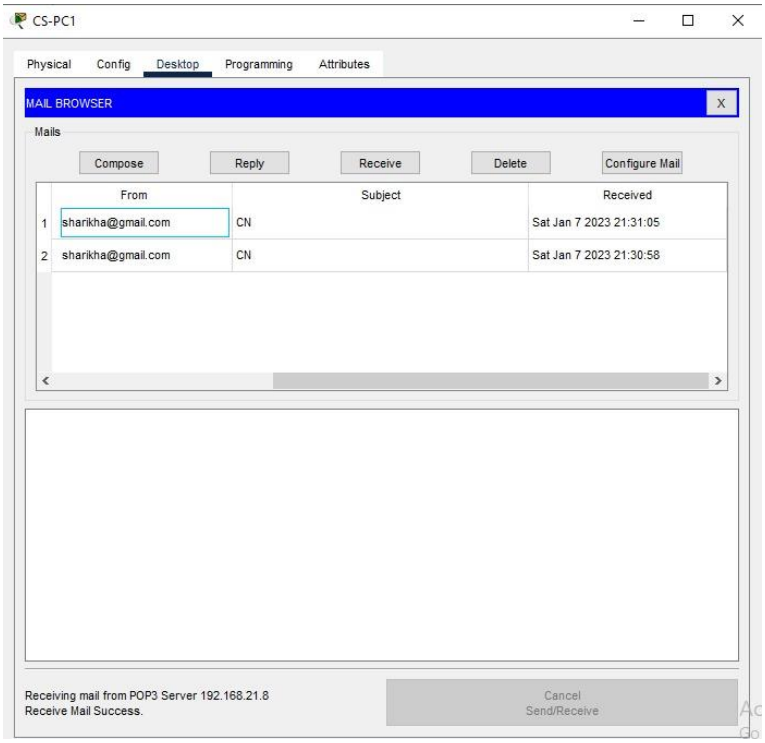
Web server



Email Server

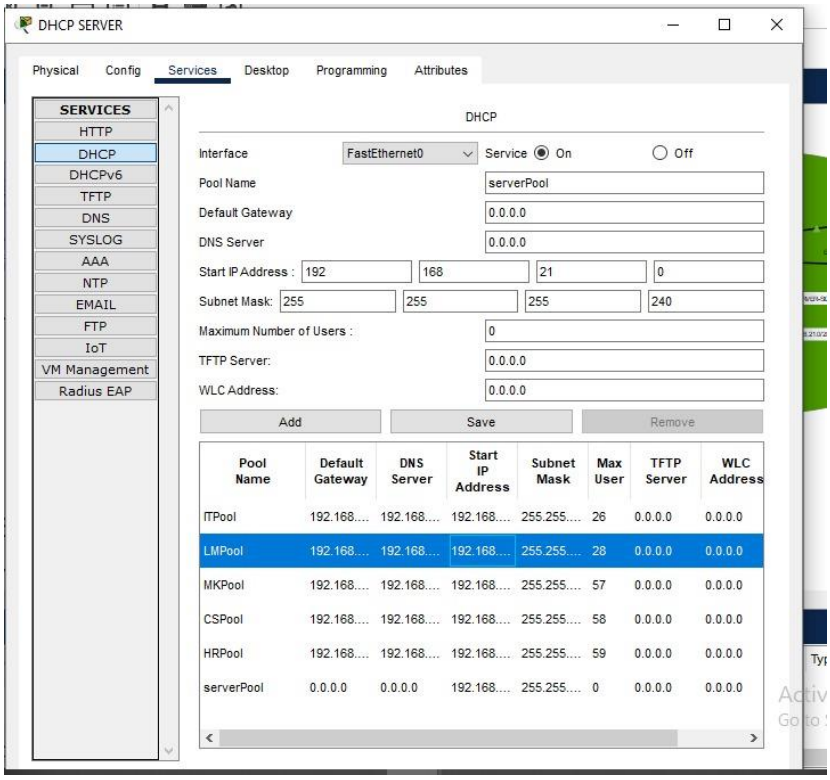


Send success



Receive success

DHCP server



Conclusion

In conclusion, the network infrastructure implemented for Financial Institution Services represents a significant step forward in bolstering operational capabilities and enhancing security measures. By prioritizing performance, redundancy, scalability, and availability, the infrastructure ensures seamless service delivery and data protection. Through the integration of dual ISPs, departmental segregation, and robust security measures, Financial Institution Services now possesses a resilient and secure network infrastructure capable of meeting the evolving needs of the organization and its clients.

This project has empowered Financial Institution Services to enhance operational efficiency, strengthen security measures, and deliver superior financial services to its clients, positioning the organization for continued success in the competitive financial services landscape.

Learning Outcome

Key learning outcomes include:

Understanding of network design principles.
Proficiency in configuring Cisco Catalyst devices.
Experience with VLANs, VoIP, and security features.
Familiarity with VPNs, ACLs, and troubleshooting.
Awareness of redundancy, scalability, and availability in network design.