رواد مصر الرقمية Digital Egypt Pioneers Initiative وزارة الاتصــــــالات وتكنولوجيا المعلومات

Title

# Enterprise Network Design and Implementation

DEPI Project

Student's names

| | |
|---|---|
| Ali Abdulqawi Ali | Mohamed Abdelaziz Eltawil |
| Abdelrahman Moustafa Elsayed | Mahmoud Ibrahim Kamal |

Supervisor

Eng. Magdy Ibrahim

Oct 2024

# Acknowledgement

Firstly, before we start the project we founded that the project will not be easy to implement but we believed that everything with and continues learn can be finished, we passed through many steps to implement each part in the project, we learned more technologies in many times through the project and to apply all of what we learned not an easy part but with the patience and trying more times we finished our project. After more hard times and more efforts from everyone in the team to finish this project and with help of Eng. Magdy Ibrahim and DEPI assistants we reached the end point now, thanks for Eng. Magdy that let us to learn more and more, to learn how to depend in ourselves and help each of us with the knowledge we gained through all time of the Internship and thanks for Eng. Magdy leaves us to apply all technologies and tools that we learned in our project. We are here to introduce this project because Eng. Magdy believed that we could make Enterprise Network Design and Implementation in this time and now we finished it successfully, so special thanks to our supervisor that helped us from the first second of this project to the end of project. many hard steps with more search and with more study and with patience we cooperated to finish what we started. So, thanks for everyone helped and believed in our team.

# Abstract

This project focuses on designing a comprehensive and resilient network for a bank with two branches, each consisting of four floors allocated for the IT unit, managers, staff, and customers. The network is segmented using VLANs, ensuring efficient traffic management and improved security across the organization. In the IT and management floors, switches connect PCs, IP telephony, and servers, while the staff floor accommodates essential devices connected via VLAN 30. The customer floor includes a wireless router that offers a separate guest network for bank visitors, as well as a dedicated network for employees.

To maintain redundancy and high availability, each branch utilizes dual multi-layer switches, ensuring that if the primary switch fails, the secondary can take over seamlessly. Similarly, two core routers are deployed in each branch for redundancy, ensuring uninterrupted connectivity with the bank's Internet Service Provider (ISP). The network incorporates a variety of key protocols, including AAA for access control, SSH for secure communication, and HSRP for high availability. Port security and rapid spanning tree protocols like BPDU Guard and PortFast are implemented to prevent loops and secure switch ports.

The core routers are configured with advanced protocols such as DHCP for dynamic IP address allocation, OSPF for dynamic routing, VPN for secure remote access, and NAT for translating internal IP addresses to external ones. The multi-layer switches support inter-VLAN routing, ACLs (Access Control Lists), and IP Helper for DHCP relay, while the wireless routers are configured to separate customer and employee networks securely. Protocols like OSPF and AAA are also implemented on the ISP routers for enhanced network efficiency and security.

Overall, this design ensures a highly reliable, secure, and scalable network that can support the bank's operations while minimizing downtime and maintaining a high level of security for both internal and external users.

## Contents

Chapter One: Introduction ........ 6

Introduction: ........ 6

Problem to Be Solved: ........ 6

Project Objectives: ........ 6

Tools Used in the Project: ........ 7

Chapter Two: System Design ........ 8

Network Architecture: ........ 8

Redundancy Design: ........ 10

Protocols Implemented: ........ 10

Chapter Three: Database and File Design ........ 12

Table Design ........ 12

VLAN Configuration Table: ........ 12

Device Assignment Table: ........ 12

Data Relationships ........ 13

VLANs and Switches: ........ 13

VLANs and Devices: ........ 13

Authentication and Users: ........ 14

File Design ........ 14

Chapter Four: System Design and Implementation ........ 15

System Overview ........ 15

System Components and Network Architecture ........ 15

Core Routers ........ 15

Multi-Layer Switches ........ 16

Floor-Based Access Switches ........ 16

Wireless Routers ........ 17

Protocols Implemented ........ 17

VLANs (Virtual LANs) ........ 17

HSRP (Hot Standby Router Protocol) ........ 17

OSPF (Open Shortest Path First) ........ 18

AAA (Authentication, Authorization, Accounting) ........ 18

VPN (Virtual Private Network) ........ 18

SSH (Secure Shell) ........ 18

Implementation Phases ........ 18

Planning and Design Phase ........ 18

Configuration and Installation Phase ........ 19

Testing and Validation Phase ........ 19

Deployment Phase ........ 19

Chapter Five: Inquiries ........ 20

Inquiry Samples: ........ 20

Chapter Six: Future Work ........ 21

Future Enhancements: ........ 21

# Chapter One: Introduction

## Introduction:

Computers have revolutionized various industries by improving efficiency and simplifying tasks. In the banking sector, having a reliable and secure network infrastructure is crucial for managing sensitive customer data, facilitating transactions, and ensuring smooth communication across branches. A well-designed network system supports banking operations, offering enhanced performance and security.

This project focuses on designing a bank's network infrastructure, covering two branches. Each branch has multiple floors dedicated to IT units, managers, staff, and customers, with specific configurations to ensure data security and seamless communication. Redundancy has also been prioritized to ensure network continuity in the event of hardware failure.

## Problem to Be Solved:

The network design addresses several key issues:

- Secure communication across branches.
- Separation of networks for different roles (IT, managers, staff, customers).
- Ensuring network redundancy to avoid downtime.
- Reliable authentication and security for network access.
- Enabling remote access through secure VPNs.
- Network scalability for future growth and technological advancement.

## Project Objectives:

The goals of this project include:

- Designing a secure, scalable network for two bank branches.
- Implementing VLANs for traffic segmentation across different floors.
- Configuring HSRP for redundancy and failover mechanisms.
- Establishing a wireless network for customers with secure access for staff.
- Ensuring secure communication using AAA and VPNs.

- Optimizing routing and network traffic with OSPF.

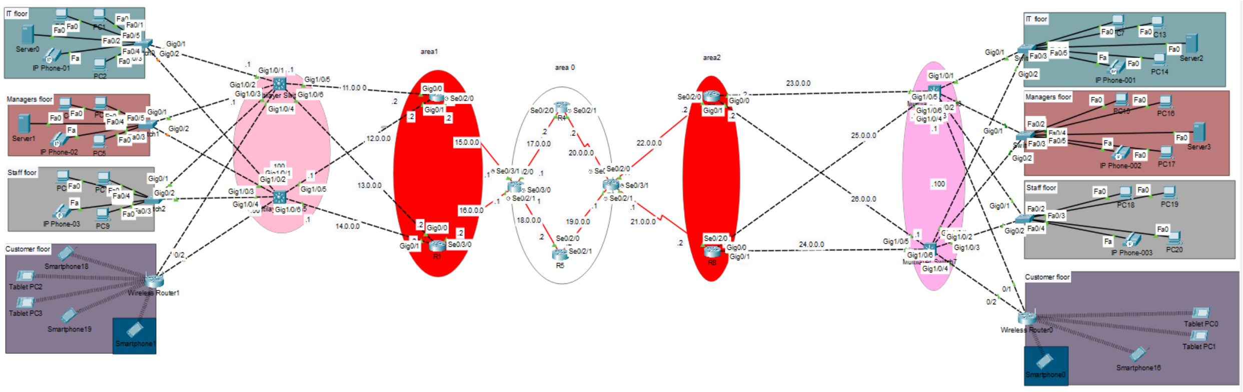
## Tools Used in the Project:

- This project was built using the following tools and technologies:
- Cisco Routers and Switches: For reliable and scalable core networking.
- VLANs: Segmentation of network traffic based on role and department.
- HSRP: Redundancy and failover configuration for routers and switches.
- AAA (Authentication, Authorization, and Accounting): Ensuring secure access control.
- OSPF (Open Shortest Path First): Dynamic routing protocol to optimize traffic.
- DHCP: Automatic IP assignment for network devices.
- VPN: Secure remote access for employees.
- SSH: Secure command-line access to network equipment.
- Wireless Routers: Configured to offer separate networks for customers and staff.

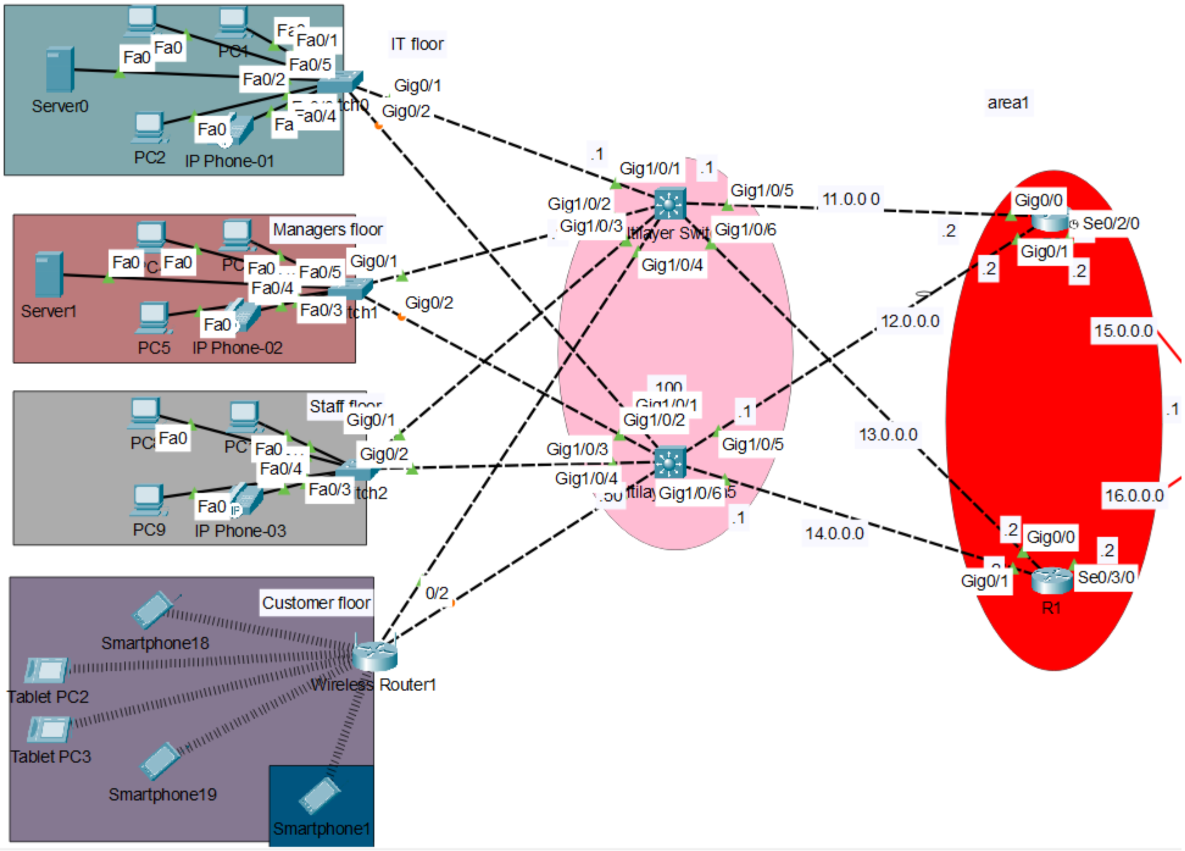
# Chapter Two: System Design

## Network Architecture:

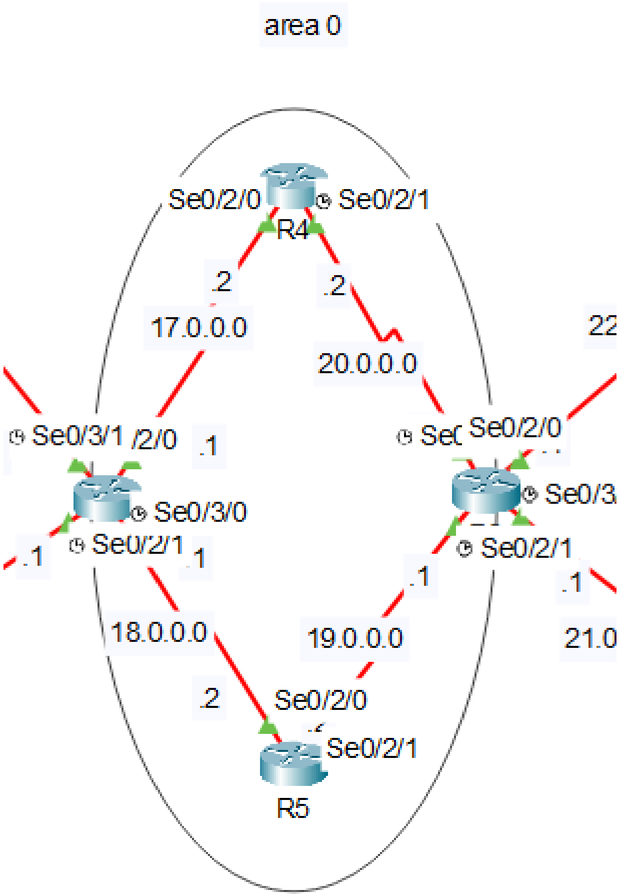
The network architecture consists of two branches, each with four floors dedicated to different operations:



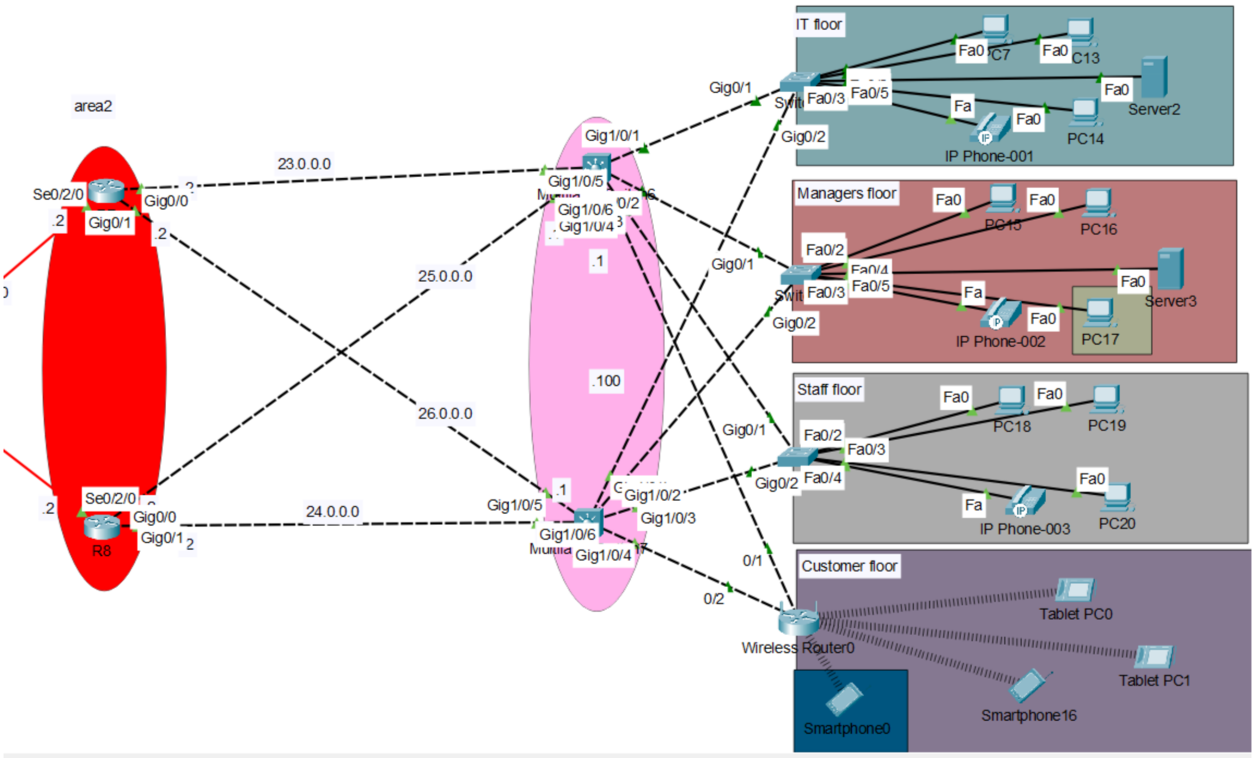
Branches with Internet Service Provider



Branche A



Internet Service Provider



Branche B

## Redundancy Design:

Two multi-layer switches are configured: one as primary, the other as backup.

Two core routers are connected to the multi-layer switches for redundancy, ensuring the network remains functional even if one router or switch fails.

Each core router is connected to the routers of the Internet Service Provider (ISP).

## Protocols Implemented:

On Switches:

- VLANs
- AAA
- SSH
- Port Security
- PortFast
- BPDU Guard.

On Multi-Layer Switches:

- VLANs
- IP Helper
- ACL
- Inter-VLAN
- HSRP
- AAA
- SSH
- PortFast
- BPDU Guard.

On Core Routers:

- DHCP
- OSPF
- VPN
- NAT
- Static Routing
- AAA
- HSRP.

On ISP Routers:

- OSPF.
- AAA.

On Wireless Routers:

- Specific configuration for customer and staff networks.

# Chapter Three: Database and File Design

In the context of network design, "database and file design" refers to how configuration files, logs, and other key data are stored, structured, and managed to ensure the smooth operation of the network.

## Table Design

While traditional database tables are not a primary component in network configurations, we can relate table design to how configuration data is organized within the network. For example, each VLAN, device, and user can be considered as an entry within a structured table to maintain clarity and ease of management. Below are sample representations of key elements.

### VLAN Configuration Table:

Each VLAN is assigned a unique ID, IP range, and purpose. The table below outlines the VLANs configured for different roles within the bank.

| VLAN ID | VLAN Name | IP Address Range | Subnet Mask | Gateway | Purpose |
|---|---|---|---|---|---|
| 10 | IT Floor | 192.168.10.0 - 255 | 255.255.255.0 | 192.168.10.100 | For IT operations |
| 20 | Managers Floor | 192.168.20.0 - 255 | 255.255.255.0 | 192.168.20.100 | For managers |
| 30 | Staff Floor | 192.168.30.0 - 255 | 255.255.255.0 | 192.168.30.100 | For staff |
| 40 | Customer Floor | 192.168.40.0 - 255 | 255.255.255.0 | 192.168.40.100 | Guest network |

This structure organizes VLAN assignments, which are critical for segregating traffic and ensuring security across the network.

### Device Assignment Table:

This table tracks network devices such as switches, routers, and servers, with their IP addresses and assigned roles.

| Device Type | Device Name | IP Address | VLAN Assignment | Location | Role |
|---|---|---|---|---|---|
| Router | Core Router 1 | 15.0.0.2 | VLAN 10, 20, 30, 40 | Branch A - Core Room | Core routing, OSPF |
| Router | Core Router 2 | 16.0.0.2 | VLAN 10, 20, 30, 40 | Branch A - Core Room | Redundant routing |
| Switch | Switch 1 | 192.168.10.100 | VLAN 10 | IT Floor - Branch A | IT operations |
| Switch | Switch 2 | 192.168.20.100 | VLAN 20 | Managers Floor - A | Managers' network |
| Wireless Router | WR 1 | 192.168.40.1 | VLAN 40 | Customer Floor - A | Guest network |

## Data Relationships

In this network design, data relationships exist between various elements such as VLANs, switches, routers, and users. Here's an explanation of the key relationships:

### VLANs and Switches:

Each switch in the network is associated with specific VLANs. For example:

- Switch 1 on the IT floor is responsible for VLAN 10, providing connectivity for IT-related devices.
- Switch 2 on the Managers' floor handles VLAN 20, ensuring that the managers' network traffic is isolated from other floors.

### VLANs and Devices:

Network devices such as routers and switches route traffic based on VLAN configurations. For instance:

- Core Routers handle traffic from all VLANs, providing the necessary routing services to direct data to the appropriate destination.
- Wireless routers are configured with VLANs (such as VLAN 40) to serve guest users without affecting staff operations.

### Authentication and Users:

Users accessing the network are authenticated via AAA, which ensures that each user only has access to their designated VLAN and services. For example:

- Network admins have access to all VLANs.
- Staff users only have access to VLAN 30, which is used by staff devices.

## File Design

Configuration files are essential to maintain network setups, and they are saved in text-based formats that can be easily backed up and restored. These files store critical data for network device configurations, including:

- Switch Config Files: Store the configurations for each switch, such as VLAN assignments, port configurations, security settings (like port security, AAA), and HSRP settings. Example file snippet for Switch 1:
- Router Config Files: Include routing protocols (like OSPF and static routes), NAT, VPN settings, and redundancy configurations (HSRP). These are vital for ensuring dynamic routing and failover. Example file snippet for Router 1:
- AAA Config Files: Define the rules for user authentication, ensuring that devices and users are properly validated before accessing the network.

# Chapter Four: System Design and Implementation

This chapter delves into the technical design and implementation process of the bank's network system, focusing on the structured steps taken to ensure high availability, security, scalability, and seamless performance across both branches. The goal of this system is to deliver a robust, efficient, and secure network that supports all bank operations, from internal communications to customer services.

## System Overview

The system design for the bank's network spans two branches, each consisting of four floors (IT unit, managers, staff, and customers), connected via a reliable and secure infrastructure. The key components include:

- Routers for ISP connectivity: Core routers connected to the internet service provider ensure reliable internet access.
- Switches and VLANs: Each floor of both branches has its own VLAN for segmented and secure network traffic, providing isolation between different departments.
- Wireless Network: A separate wireless guest network is provided for customers, ensuring limited access while maintaining security for the internal network.
- Redundancy and Failover Mechanisms: Backup multi-layer switches and core routers are implemented to ensure network resilience in case of hardware failure.

## System Components and Network Architecture

The system consists of several interconnected components, each designed to perform specific roles within the network:

### Core Routers

Core routers are at the center of the network, handling both branch-to-branch communication and external communication with the internet via the ISP. They are configured with:

- Dynamic Routing Protocol (OSPF): OSPF (Open Shortest Path First) is configured for dynamic route updates between branches and to the ISP, ensuring optimal routing of data packets.
- Static Routing: For certain critical connections where the path is predetermined, static routes are used.
- Network Address Translation (NAT): NAT allows internal devices to communicate with external networks, like the internet, using a single public IP address.

### Multi-Layer Switches

Each branch has two multi-layer switches (one primary and one backup). These switches handle traffic routing within VLANs and between different VLANs (inter-VLAN routing). The configuration includes:

- HSRP (Hot Standby Router Protocol): Provides redundancy by assigning a virtual IP to both primary and backup switches. In the event of a failure, the backup switch takes over without disrupting service.
- Inter-VLAN Routing: Traffic between VLANs (e.g., from the IT floor to the managers' floor) is routed efficiently through the multi-layer switch.
- Access Control Lists (ACLs): ACLs are configured to restrict access based on IP addresses or ports, enhancing network security.

### Floor-Based Access Switches

Each floor in both branches is equipped with dedicated switches that connect to the respective VLAN. These switches support:

- Port Security: Restricts the number of MAC addresses allowed on each port, preventing unauthorized devices from connecting to the network.
- PortFast and BPDU Guard: These features prevent delays in bringing ports online and protect against potential issues from improper device connections (e.g., loops).
- AAA (Authentication, Authorization, and Accounting): Ensures that only authenticated users can access the network. Authentication is handled through either RADIUS or TACACS+.

### Wireless Routers

Wireless routers are used on the customer floors to provide a separate guest network. The configuration includes:

- Guest VLAN: A dedicated VLAN for guest access ensures that customer devices are isolated from the rest of the bank's network.
- WPA2 Encryption: The wireless network is protected with WPA3 encryption to secure customer connections.
- SSID Segmentation: The wireless routers broadcast two separate SSIDs—one for customers (guest network) and one for employees working on the customer floor.

## Protocols Implemented

A variety of protocols have been implemented across the network to ensure secure, efficient, and reliable operations.

### VLANs (Virtual LANs)

VLANs are used to separate traffic based on the floor and role within the bank:

- VLAN 10: For IT operations, ensuring secure communications between IT staff and devices.
- VLAN 20: For managers, isolating their devices and servers for sensitive managerial operations.
- VLAN 30: For staff, allowing communication within the department while remaining isolated from other floors.
- VLAN 40 (Guest Network): For customers, ensuring that their network traffic remains segregated from the internal bank operations.

### HSRP (Hot Standby Router Protocol)

HSRP is configured on the core routers and multi-layer switches to provide redundancy. A virtual IP address is shared between the primary and secondary devices. If the primary device fails, the secondary device takes over, ensuring uninterrupted network service.

### OSPF (Open Shortest Path First)

OSPF is the primary dynamic routing protocol used to maintain routing tables and to ensure the optimal path is always chosen for data traffic. It provides faster convergence in case of topology changes and is scalable across both branches.

### AAA (Authentication, Authorization, Accounting)

AAA is implemented to control access to the network. It ensures that users are authenticated before gaining access to resources, authorized to use specific services, and their activities are logged for accountability. The two main protocols used are:

RADIUS: For user authentication and accounting.

TACACS+: For administrative access control, allowing centralized authentication for network devices.

### VPN (Virtual Private Network)

VPN is configured to securely connect remote users (such as administrators) to the bank's internal network. This ensures that sensitive operations, like remote maintenance, can be performed securely from outside the branches.

### SSH (Secure Shell)

SSH is used for secure remote management of routers and switches. This ensures that all administrative communications are encrypted, preventing unauthorized access to network configurations.

## Implementation Phases

The implementation of the network system followed a structured approach to ensure that all components were properly configured, tested, and deployed.

### Planning and Design Phase

This phase involved gathering requirements, determining network topology, and selecting appropriate hardware and software components. A detailed design document was created, outlining:

- VLAN segmentation for each department and floor.
- IP addressing schema for each VLAN and device.
- Redundancy and failover configurations for critical network components (multi-layer switches, core routers).

### Configuration and Installation Phase

During this phase, the network hardware (routers, switches, wireless routers) was installed and configured according to the design plan:

- Router Configuration: OSPF, NAT, HSRP, and VPN were set up on the core routers.
- Switch Configuration: VLANs, AAA, port security, and HSRP were configured on the switches.
- Wireless Network: The guest network and WPA2 encryption were configured on the wireless routers.

### Testing and Validation Phase

Before going live, the entire network was thoroughly tested to ensure that all components functioned as expected:

- VLAN Testing: Verified that each VLAN was properly segregated, with no communication between VLANs except where allowed.
- Redundancy Testing: Simulated device failures to ensure that the HSRP configurations provided proper failover between devices.
- Security Testing: Verified that AAA configurations blocked unauthorized access and that SSH encryption was functioning for remote device management.

### Deployment Phase

Once testing was complete, the network system was deployed in a live environment, with monitoring tools activated to ensure smooth operations. The system was transitioned into active use, with administrators monitoring logs and traffic to ensure optimal performance.

# Chapter Five: Inquiries

## Inquiry Samples:

Describe specific network queries used for troubleshooting, like checking the status of routers, monitoring VLAN traffic, and reviewing logs. This can include commands such as:

- show ip route
- show vlan brief
- show standby brief
- show ip interface brief
- show running-config
- show ip ospf neighbor
- show vlan brief
- show interfaces vlan (10/20/30/40)
- show mac address-table
- show spanning-tree vlan (10/20/30/40)
- show interfaces status
- show port-security interface GigabitEthernet0/ (0-1)
- show interfaces GigabitEthernet0/ (0-1) counters
- show ip dhcp binding
- show ip nat translations
- ping (192.168.10.1)
- traceroute 192.168.10.1

# Chapter Six: Future Work

## Future Enhancements:

Expanding the Network: The network can be expanded to accommodate more branches, integrating them into the existing structure while maintaining performance and security.

Advanced Security: Implement additional security features like multi-factor authentication (MFA) and intrusion detection systems (IDS).

Cloud Integration: Explore cloud-based solutions for data storage, backup, and network management.

Automation: Automate network monitoring and fault detection through scripts or tools like Cisco's network automation features.

IoT Integration: With the growth of IoT devices, future work may include integrating smart banking services and equipment monitoring into the network.

System Reports: Provide examples of network monitoring reports, traffic analysis reports, and system health checks. These reports help visualize network performance and spot any anomalies or issues in real-time.