رواد مصر الرقمية

Advanced Scalable and Secure Network Architecture for Bank and its Branches

prepared by:

Ahmed Ashraf Fawaz Mahmoud
Ahmed Mohamed Abd Elraheem Mohamed
Ahmed Yasser Helmy Ahmed
Mohamed Barakat Mohamed Mahmoud
Ali Magdy Ali Kamal El-deen

Supervisor:
Engineer: Hassnaa Elwan

Table of Contents

Introduction:

In today's digitally-driven world, banks and financial institutions rely heavily on robust, secure, and scalable network infrastructures to support their day-to-day operations. The **Bank Network Design** project focuses on creating a comprehensive network architecture for a banking environment, spanning multiple branches and a headquarter. The network is designed to ensure seamless communication, enhanced security, and efficient management of financial data and services across various geographic locations. The importance of an optimized bank network lies not only in its ability to provide uninterrupted service to clients but also in its critical role in safeguarding sensitive financial information against security threats. A well-architected network ensures that the bank's operations remain agile, responsive, and highly resilient to both technical failures and cyber-attacks.

Project Significance

The significance of this project stems from the crucial need for modern banks to operate securely in a highly regulated and competitive financial environment. As banking institutions increasingly move towards digitization and online services, network performance and security become paramount. This design aims to provide high availability, fault tolerance, and rapid recovery in case of failures, thereby ensuring the continuity of banking operations. The bank's clients expect round-the-clock availability of services, whether through branches, ATMs, or online platforms, making the reliability and efficiency of the network a non-negotiable requirement.

Moreover, this project addresses the fundamental challenge of maintaining strong security measures, which are vital for protecting against growing cyber threats, data breaches, and internal vulnerabilities. Banks must adhere to strict regulatory requirements, including data privacy laws and cybersecurity protocols, which further highlights the importance of building a network that can meet these demands. By integrating advanced routing, switching, and security mechanisms, this network design provides a comprehensive solution to ensure that the bank remains competitive and compliant in the ever-evolving digital landscape.

Problem Statement

The main problem being addressed by this project is the need for a highly secure, efficient, and scalable network infrastructure to support a bank with a **headquarter and multiple branches**. As the bank expands its operations, the existing network infrastructure may become strained, leading to performance issues, potential security vulnerabilities, and operational inefficiencies. This project seeks to design a **three-tier network architecture**—comprising core, distribution, and access layers—that can meet the bank's current and future needs.

The key challenges include ensuring:

- **Redundancy**: To minimize downtime and maximize availability through failover mechanisms such as **HSRP** and **EtherChannel**.
- **Security**: To protect against cyber threats using **AAA authentication**, **DHCP Snooping**, **Dynamic ARP Inspection (DAI)**, and **IP Source Guard**.

- **Efficient communication**: Between the **headquarter and branches**, ensuring fast and reliable data transfer, and supporting real-time financial operations.
- **Scalability**: To accommodate future growth in terms of new branches or increased network traffic without significant redesign or disruption.

The problem is not just technical but also revolves around managing the network in a way that complies with **financial regulations** and **data protection laws**, which mandate stringent measures for securing client information and financial transactions. By addressing these issues, the project aims to provide a solution that enhances the bank's operational efficiency and strengthens its defense against potential threats.

Objectives and Goals

The primary objective of the **Bank Network Design** project is to develop a comprehensive network architecture that supports the bank's day-to-day operations across its headquarter and branches. The design must incorporate high-performance routing and switching mechanisms, robust security measures, and scalability to handle the bank's growing data and transaction volumes. Specifically, the project aims to:

1. **Design a secure and scalable three-tier network architecture** that connects the headquarter and branches through a combination of core, distribution, and access layers.
2. **Implement advanced security protocols** such as HSRP authentication, VLAN segmentation, port security, DHCP snooping, ARP inspection, and AAA to safeguard financial transactions and sensitive data.
3. **Ensure high availability and fault tolerance** by using protocols like **RSTP**, **HSRP**, and **EtherChannel** to prevent network downtime and ensure smooth failover in case of hardware or link failures.
4. **Facilitate seamless inter-branch communication** by configuring Layer 3 routing with **OSPF** to ensure efficient and reliable data transfer between different locations.
5. **Incorporate redundancy and load balancing** within the distribution and core layers to minimize bottlenecks and ensure optimal network performance, even during peak traffic periods.
6. **Prepare for future scalability** by designing the network with modularity in mind, allowing the bank to add new branches, services, or technologies without major disruptions.

By achieving these goals, the project will provide the bank with a highly reliable and secure infrastructure that not only supports current operations but also positions the institution for future growth and digital advancements.

Methodology

The methodology for this project involves several key steps, starting from the initial network design to the detailed configuration and testing of security and routing protocols. The **Cisco Packet Tracer** simulation tool is used to design and test the network infrastructure. The design follows a **three-tier architecture** that separates the network into core, distribution, and access layers for better management and scalability.

The network design incorporates several industry-standard protocols and technologies:

1. **Routing and Switching Configuration**: The network is configured using **OSPF** (Open Shortest Path First) to ensure efficient Layer 3 routing between branches and the headquarter. **VLANs** (Virtual Local Area Networks) are used to segment the network for better traffic management and security.
2. **High Availability and Redundancy**: **HSRP** (Hot Standby Router Protocol) is implemented to ensure gateway redundancy, while **EtherChannel** provides link aggregation between distribution switches, improving bandwidth and redundancy. **RSTP** (Rapid Spanning Tree Protocol) is used for fast network convergence, preventing loops and improving fault tolerance.
3. **Security Mechanisms**: Security is a major focus, with advanced features such as **AAA** (Authentication, Authorization, and Accounting) implemented for device authentication, **DHCP Snooping** to prevent rogue DHCP servers, and **Dynamic ARP Inspection** to mitigate ARP spoofing attacks. **Port Security** and **IP Source Guard** are also configured to prevent unauthorized devices from accessing the network.
4. **VLAN Management**: **VTP (VLAN Trunking Protocol) Version 3** is employed for efficient VLAN management across the branches, allowing for centralized control and synchronization of VLAN configurations.
5. **Testing and Simulation**: The entire network is tested within the Cisco Packet Tracer environment, ensuring that the routing, switching, security, and redundancy protocols function as expected. Stress testing is conducted to simulate heavy network traffic, ensuring that the network can handle peak loads without performance degradation.

The methodology ensures that each element of the network is rigorously designed, configured, and tested before being implemented in a real-world scenario, reducing the risk of failures or security breaches once the network goes live.

Literature Review:

In recent years, the growing reliance on digital infrastructure by banking and financial institutions has led to significant research focused on the design, security, and scalability of bank networks. A well-designed network is essential for providing secure, efficient, and uninterrupted services to both internal banking operations and customer-facing applications such as online banking, mobile banking, and automated teller machines (ATMs). This section reviews existing research on network architecture, security measures, and redundancy protocols within the context of bank network design, while also identifying key gaps that the **Bank Network Design** project aims to address.

1. Network Design and Architecture in Banking Systems

The design of modern banking networks follows a structured approach, typically based on the **three-tier architecture** that includes the **core**, **distribution**, and **access** layers. According to Tanenbaum and Wetherall (2011), three-tier architectures are widely adopted in large-scale networks, such as banks, due to their ability to segregate different levels of the network for better management, scalability, and redundancy. The **core layer** is responsible for fast transport between various parts of the network, the **distribution layer** handles routing between different segments (e.g., branches), and the **access layer** is responsible for connecting end-user devices.

Studies, such as those conducted by Varghese et al. (2015), have shown that the **three-tier architecture** is particularly useful in ensuring smooth traffic flow and preventing bottlenecks in large banking environments where multiple branches need to communicate seamlessly with the headquarter. Additionally, this architecture simplifies the management of network traffic, allowing banks to segment their network into logical divisions, such as branches and departments, through the use of **VLANs**.

While significant research supports the three-tier model for large-scale financial networks, there is limited focus on how these designs can be optimized to handle the increasing demands of modern banking services. The **Bank Network Design** project aims to address this gap by proposing a network design that integrates the latest security protocols, redundancy mechanisms, and scalability considerations to future-proof the bank’s network infrastructure.

2. Security in Bank Networks

Security has always been a critical concern in banking networks, with various studies emphasizing the need for robust protection against both external and internal threats. The work of Panko (2014) highlights how financial institutions are prime targets for cyberattacks due to the sensitive nature of the data they handle. As a result, networks need to incorporate multi-layered security protocols to safeguard against unauthorized access, data breaches, and attacks such as **DDoS**, **phishing**, and **ransomware**.

Existing literature underscores the importance of implementing **AAA (Authentication, Authorization, and Accounting)** security models to control access to the network. According to Mahajan et al. (2016), **AAA protocols**, combined with **802.1x authentication**, provide a solid foundation for securing access ports and ensuring that only authenticated devices can connect to the network. However, studies also point out that there is a growing need for tighter security measures, particularly with the rise of **Internet of Things (IoT)** devices and the increased use of **mobile banking**. These technologies introduce new vulnerabilities that traditional **firewalls** and **intrusion detection systems** may not fully address.

Furthermore, the research of Awad (2017) examines the importance of **DHCP Snooping**, **Dynamic ARP Inspection (DAI)**, and **IP Source Guard (IPSG)** in preventing common network attacks such as **DHCP spoofing**, **man-in-the-middle (MitM)** attacks, and **IP address spoofing**. These mechanisms provide an additional layer of security at the network edge, particularly in the access layer where end devices connect. Despite the availability of these advanced security techniques, existing research has not fully explored how these can be efficiently integrated into a cohesive security framework for modern banking networks, particularly those with multi-branch architectures.

The **Bank Network Design** project seeks to fill this gap by combining these security protocols into a unified design that leverages the latest advancements in **AAA**, **DHCP Snooping**, **DAI**, and **IPSG**. This project will also explore how these mechanisms can be applied to a **three-tier network architecture** to maximize protection against both external and internal threats while ensuring regulatory compliance.

3. Redundancy and High Availability in Financial Networks

The concept of redundancy is a major focus in network design for critical industries like banking, where network downtime can lead to severe financial losses and reputational damage. Redundancy mechanisms such as **HSRP (Hot Standby Router Protocol)** and **EtherChannel** have been extensively studied and recommended by researchers like Odom (2018) for providing failover capabilities and preventing single points of failure.

HSRP is widely used in the distribution and core layers of financial networks to ensure that if one router or switch fails, another can seamlessly take over as the gateway, ensuring that network operations remain uninterrupted. Studies by Ali and Raza (2019) highlight how **HSRP** can be configured with **authentication** mechanisms to prevent rogue devices from attempting to become the active gateway, thus enhancing security alongside redundancy. Similarly, **EtherChannel** bundles multiple physical links between devices, providing not only increased bandwidth but also ensuring that if one link fails, the others continue to function.

While these protocols are well-established, there is limited research on how to effectively balance **load** and **traffic** between redundant devices, particularly in the context of geographically dispersed bank branches. Moreover, many studies focus on individual redundancy protocols but fail to address the integration of redundancy with other aspects of network design, such as **VLAN management** and **Layer 3 routing protocols** like **OSPF (Open Shortest Path First)**.

The **Bank Network Design** project aims to close this gap by presenting a network design that integrates **HSRP**, **RSTP**, and **EtherChannel** with **VTP** and **OSPF**. By doing so, it ensures high availability, seamless failover, and optimized traffic flow across the bank's network infrastructure.

4. Scalability and Future-Proofing of Banking Networks

Scalability is a critical consideration in bank network design, especially as financial institutions increasingly adopt digital banking services and expand their branch networks. Research by Gupta et al. (2020) emphasizes that banks need networks that can easily scale to accommodate growing numbers of users, devices, and services without requiring major redesigns.

VLAN management through **VTP (VLAN Trunking Protocol)** has been widely adopted as an effective way to scale the network by logically segmenting traffic. **VTP Version 3**, as recommended by Balaji and Parikh (2017), provides better security and functionality compared to earlier versions, ensuring that VLAN information is propagated securely across all switches. However, existing studies often neglect the complexities involved in managing VLANs in large networks that span multiple branches, particularly when integrating them with **Layer 3 routing protocols**.

The **Bank Network Design** project addresses this scalability gap by proposing a modular architecture that can accommodate future growth in branch numbers, users, and services. The use of **VTP v3** alongside **OSPF** allows for the efficient propagation of VLAN configurations and dynamic routing updates, ensuring that the bank’s network can grow without requiring extensive manual reconfiguration.

Identified Gaps in Literature

While existing research provides valuable insights into various aspects of bank network design—such as security, redundancy, and scalability—several key gaps remain:

1. **Comprehensive Integration of Security Measures**: There is a need for more research on how modern security protocols (such as AAA, DHCP Snooping, DAI, and IPSG) can be fully integrated into a multi-branch, three-tier network architecture. Existing studies often focus on individual security measures without addressing their interaction within a unified design.
2. **Redundancy and Load Balancing**: Research has highlighted the importance of redundancy, but there is limited focus on how redundancy protocols such as HSRP and EtherChannel can be optimized for load balancing and integrated with routing protocols like OSPF in a multi-branch environment.
3. **Scalability in Multi-Branch Networks**: While VTP and OSPF are established technologies for VLAN management and routing, more research is needed on how these protocols can be efficiently implemented in large-scale, multi-branch networks, particularly in the banking sector, where both security and scalability are paramount.

Project Requirements and Scope

1. Project Scope

The project scope encompasses the design and configuration of a **three-tier network architecture** that ensures secure, efficient, and scalable connectivity between the bank's headquarters and its branches. Key features such as **routing**, **switching**, **security protocols**, and **redundancy** will be implemented to address the banking institution's needs for high availability and data protection.

Key aspects of the project include:

- **Three-Tier Architecture:** Implementation of core, distribution, and access layers to segment the network for better management, scalability, and fault tolerance.
- **VLAN Configuration:** Creation and segmentation of VLANs across different locations to manage traffic flow, enhance security, and isolate departments and services.
- **Routing and Redundancy:** Use of **HSRP** (Hot Standby Router Protocol), **OSPF** (Open Shortest Path First) routing, and **EtherChannel** for link aggregation to ensure redundancy, high availability, and efficient traffic flow between the branches and headquarters.
- **Network Security:** Incorporating advanced security mechanisms like **AAA (Authentication, Authorization, and Accounting)**, **DHCP Snooping**, **Dynamic ARP Inspection (DAI)**, **IP Source Guard**, and **802.1x authentication** to protect against both internal and external threats.
- **Packet Tracer Simulation:** All network configurations, security mechanisms, and failover scenarios will be fully simulated using **Cisco Packet Tracer**, ensuring that the network operates as intended and meets all project requirements.

2. Hardware and Software Requirements

Since this project is being carried out entirely in a simulation environment, the focus is on the software required for the network setup, while physical hardware is simulated virtually through **Cisco Packet Tracer**.

Software Requirements:

- **Cisco Packet Tracer:** Version 8.0 or higher is required to simulate the entire network infrastructure. This tool will be used for creating and managing all devices in the network, including routers, switches, end devices, and security appliances.

Simulated Hardware Components:

- **Routers:** Simulated Cisco routers to handle Layer 3 routing, OSPF configuration, and inter-VLAN routing.

- **Switches:** Simulated Cisco switches for handling Layer 2 configurations, VLANs, trunking, and redundancy protocols such as EtherChannel.
- **End Devices:** Simulated PCs, servers, and other client devices to verify connectivity and demonstrate proper functioning of the network.
- **Security Appliances:** Simulated features like **AAA**, **802.1x**, and **firewalls** will be configured virtually through Packet Tracer's built-in functionalities.

3. Security Requirements

In the financial sector, ensuring the security of sensitive data and financial transactions is of utmost importance. The project incorporates multiple security layers to safeguard the bank's network from unauthorized access and cyber-attacks.

Security Protocols Implemented:

- **AAA Authentication:** To ensure only authorized users have access to network resources through centralized **RADIUS** servers.
- **802.1x Authentication:** Ensures secure access control on the edge of the network, requiring devices to authenticate before accessing the network.
- **DHCP Snooping:** Protects against rogue DHCP servers and prevents IP address spoofing.
- **Dynamic ARP Inspection (DAI):** Prevents **man-in-the-middle (MitM)** attacks by validating ARP packets on the network.
- **IP Source Guard (IPSG):** Helps prevent IP spoofing by ensuring only valid IP-MAC bindings can communicate on specific ports.
- **Port Security:** Restricts the number of MAC addresses per switch port, preventing unauthorized devices from connecting to the network.

These security protocols are designed to protect both internal and external communications, ensuring data integrity, confidentiality, and regulatory compliance within the network.

4. Design Considerations

The network design takes into account several critical factors, such as:

- **High Availability:** The use of redundancy protocols like **HSRP** and **EtherChannel** ensures that the network remains operational even during link or device failures, minimizing downtime for the bank's critical services.
- **Scalability:** The network is designed to be easily scalable, allowing for the addition of new branches, devices, and services without extensive reconfiguration. **OSPF** and **VTP v3** will facilitate dynamic routing and VLAN management across the growing infrastructure.

Project Timeline:

Week 1: Project Planning and Research

- Review project requirements and objectives, ensuring a clear understanding of the bank's network design needs, including branch connectivity, security, and scalability.
- Conduct thorough research on relevant technologies such as **HSRP**, **RSTP**, **VTP**, **OSPF**, **AAA security**, and other advanced security protocols like **DHCP Snooping**, **Dynamic ARP Inspection**, and **IP Source Guard**.
- Investigate existing network design architectures, focusing on best practices for three-tier network designs, redundancy, and high availability.
- Develop a comprehensive project plan, detailing key milestones, deliverables, and deadlines for each phase of the project.
- Identify the necessary hardware, software tools (e.g., Cisco Packet Tracer), and resources required for the project's successful execution.

Week 2: Network Design

- Begin by creating detailed **logical** and **physical network diagrams** for the headquarter and branch offices, showing how **core**, **distribution**, and **access** layers are interconnected.
- Design the **three-tier architecture**, incorporating **VLANs**, **trunking**, and **Layer 3 routing** using **OSPF** to facilitate efficient inter-branch communication.
- Plan for **redundancy** with protocols like **HSRP** for gateway failover and **EtherChannel** for link aggregation between distribution and core switches.
- Incorporate security features such as **port security**, **AAA authentication** with RADIUS, **802.1x authentication**, and **access control lists (ACLs)** to restrict unauthorized access.
- Define **VTP** settings for efficient VLAN management and ensure security by configuring VTP version 3 with password protection.

Week 3: Implementation

- Begin configuring the network devices in **Cisco Packet Tracer**, following the network design and diagrams created in the previous week.
- Implement **OSPF** routing between the branches and the headquarter, ensuring that all VLANs can communicate properly across Layer 3.
- Configure **Layer 2 features** such as **VLANs**, **VTP**, **DTP**, and **EtherChannel**, establishing connectivity between the access, distribution, and core layers.
- Set up **HSRP** for high availability at the distribution layer, providing gateway redundancy for all VLANs in both branches and the headquarter.
- Apply security configurations, including **DHCP Snooping**, **Dynamic ARP Inspection**, **IP Source Guard**, **port security**, and **BPDU Guard** on access switches.
- Test the network at each step, ensuring **end-to-end connectivity** and verifying that security settings are functioning as expected.

Week 4: Testing, Troubleshooting, and Documentation

- Perform extensive **testing** to validate the network configuration, ensuring that routing protocols, VLANs, and security features are working correctly across all branches and the headquarter.
- Conduct **stress tests** by simulating network traffic and ensuring the network can handle peak loads, while verifying **failover** scenarios for **HSRP** and **EtherChannel**.
- **Troubleshoot** any issues that arise during testing, focusing on fixing connectivity problems, security misconfigurations, or redundancy issues.
- Finalize project documentation, including:
  - Detailed **network diagrams** (both physical and logical topologies).
  - Configuration details for all network devices.
  - Test results for connectivity, security, and redundancy.
- Prepare and submit the **final project report**, summarizing the design process, implementation, and testing results. The report will also include suggestions for future network scalability.
- Deliver a **demonstration or presentation** to showcase the working network design and highlight the key features and configurations implemented.

Network Design

Network design is based on a **3-tier architecture** consisting of **core**, **distribution**, and **access** layers. Each branch has its own VLANs, and every branch can communicate with other branches through core switches using Layer 3 routing. The design includes redundancy through **RSTP**, **HSRP**, **VTP**, **DTP**, and **EtherChannel** configurations. Here is a complete and detailed breakdown of each section.

Branch 1 Network Configuration

1. VLANs and Layer 2 Trunking between Access and Distribution Switches

- **VLANs in Branch 1**: VLAN 10, 20, 30, 40.
- Trunking (Layer 2) is used between access and distribution switches to carry multiple VLANs.

VLAN Configuration:

1. **VLAN 10**: 192.168.10.0/24
2. **VLAN 20**: 192.168.20.0/24
3. **VLAN 30**: 192.168.30.0/24
4. **VLAN 40**: 192.168.40.0/24

Each VLAN is unified across all access switches in Branch 1.

2. RSTP (Rapid Spanning Tree Protocol)

RSTP is used to prevent Layer 2 loops and to ensure fast convergence.

- **Dis1** is the **primary root bridge** for VLANs 10 and 20 and the **secondary root bridge** for VLANs 30 and 40.
- **Dis2** is the **primary root bridge** for VLANs 30 and 40 and the **secondary root bridge** for VLANs 10 and 20.

RSTP Configuration :

```
# Enabling Rapid Spanning Tree on all devices in Branch 1
spanning-tree mode rapid-pvst

# On Dis1 (Root for VLAN 10 and 20)
spanning-tree vlan 10,20 root primary
spanning-tree vlan 30,40 root secondary

# On Dis2 (Root for VLAN 30 and 40)
spanning-tree vlan 30,40 root primary
```

```
spanning-tree vlan 10,20 root secondary
```

3. HSRP (Hot Standby Router Protocol)

HSRP is configured to ensure gateway redundancy for VLANs, allowing failover between distribution switches.

- **Dis1**: Active gateway for VLANs 10 and 20, backup gateway for VLANs 30 and 40.
- **Dis2**: Active gateway for VLANs 30 and 40, backup gateway for VLANs 10 and 20.

HSRP Configuration for Dis1:

```
# On Dis1 for VLAN 10
interface vlan 10
 standby 10 ip 192.168.10.254    # HSRP virtual IP for VLAN 10
 standby 10 priority 102         # Setting priority to 102
 standby 10 preempt              # Allows Dis1 to reclaim active status
 standby 10 authentication md5 key-string cisco123

# On Dis1 for VLAN 20
interface vlan 20
 standby 20 ip 192.168.20.254    # HSRP virtual IP for VLAN 20
 standby 20 priority 102
 standby 20 preempt
 standby 20 authentication md5 key-string cisco123
```

HSRP Configuration for Dis2 (Backup for VLANs 10 and 20):

```
# On Dis2 for VLAN 10 (backup)
interface vlan 10
 standby 10 ip 192.168.10.254
 standby 10 preempt
 standby 10 authentication md5 key-string cisco123

# On Dis2 for VLAN 20 (backup)
interface vlan 20
 standby 20 ip 192.168.20.254
 standby 20 preempt
 standby 20 authentication md5 key-string cisco123
```

HSRP for VLANs 30 and 40:

- Dis1 becomes the backup for VLANs 30 and 40, while Dis2 is the active gateway.

4. VTP (VLAN Trunking Protocol) Configuration

VTP is used to manage VLANs centrally across the branch. **VTP version 3** is used for better security, and **Dis1** is the **primary VTP server** for Branch 1.

VTP Configuration :

```
# On Dis1 (VTP Server)
vtp domain cisco1              # Setting VTP domain name to 'cisco1'
vtp version 3                  # Enabling VTP version 3
vtp password cisco123 hidden    # Setting the VTP password for security
vtp primary                    # Making Dis1 the primary VTP server

# On Dis2 and all access switches (VTP Clients)
vtp mode client
```

Creating VLANs on Dis1 (VTP Primary Server):

```
vlan 10
 name Sales
vlan 20
 name HR
vlan 30
 name IT
vlan 40
 name Finance
```

---

5. Trunking and EtherChannel (LACP) Configuration

Trunking: Between distribution and access switches. **EtherChannel:** LACP is used to bundle multiple physical links between Dis1 and Dis2 for redundancy and higher bandwidth.

Trunking and EtherChannel Configuration :

```
# On Dis1 (active LACP)
interface range g0/1-3, g1/0
switchport trunk encapsulation dot1q
switchport mode trunk

interface range g0/0, g1/1
channel-group 12 mode active
switchport trunk encapsulation dot1q
switchport mode trunk

# On Dis2 (passive LACP)
interface range g0/0, g1/1
```

```
channel-group 12 mode passive
switchport trunk encapsulation dot1q
switchport mode trunk
```

---

6. Dynamic Trunking Protocol (DTP)

DTP is used to negotiate trunking between access switches and distribution switches. The switches dynamically convert the interfaces to trunk mode.

DTP Configuration:

```
# On Dis1 for access switch links
interface range g0/1-3, g1/0
switchport trunk encapsulation dot1q
switchport mode dynamic desirable
```

---

7. Routing between Distribution and Core Switches (OSPF)

OSPF is used for Layer 3 routing between the distribution and core switches, enabling communication between branches and the core layer.

OSPF Configuration for Dis1:

```
# On Dis1 (connecting to core switches)
interface g1/2
 no switchport
 ip address 192.168.1.2 255.255.255.252

interface g1/3
 no switchport
 ip address 192.168.1.18 255.255.255.252

# OSPF Configuration
router ospf 1
router-id 0.0.0.1
network 192.168.0.0 0.0.255.255 area 0
```

OSPF Configuration for Core1:

```
# On Core1
interface g1/2
 no switchport
 ip address 192.168.1.1 255.255.255.252

interface g1/3
```

```
 no switchport
 ip address 192.168.1.5 255.255.255.252

router ospf 1
router-id 1.1.1.1
network 192.168.0.0 0.0.255.255 area 0
```

---

8. IP Address Configuration for VLANs

Each VLAN needs an IP address and subnet mask on both distribution switches.

IP Address Configuration on Dis1:

```
# On Dis1
interface vlan 10
 ip address 192.168.10.251 255.255.255.0

interface vlan 20
 ip address 192.168.20.251 255.255.255.0

interface vlan 30
 ip address 192.168.30.251 255.255.255.0

interface vlan 40
 ip address 192.168.40.251 255.255.255.0
```

IP Address Configuration on Dis2:

```
# On Dis2 (use different last octet for VLAN interfaces)
interface vlan 10
 ip address 192.168.10.252 255.255.255.0

interface vlan 20
 ip address 192.168.20.252 255.255.255.0

interface vlan 30
 ip address 192.168.30.252 255.255.255.0

interface vlan 40
 ip address 192.168.40.252 255.255.255.0
```

Branch 2 Network Configuration

1. VLANs and Trunking

Branch 2 VLANs: **VLAN 50, 60, 70, 80**.

2. Port Aggregation (PAGP) Configuration

PAGP (Port Aggregation Protocol) is used between Dis3 and Dis4 to bundle physical links.

PAGP Configuration :

```
# On Dis3 (PAGP mode desirable)
interface range g0/0, g1/1
channel-group 34 mode desirable
switchport trunk encapsulation dot1q
switchport mode trunk
```

```
# On Dis4 (PAGP mode auto)
interface range g0/0, g1/1
channel-group 34 mode auto
switchport trunk encapsulation dot1q
switchport mode trunk
```

3. VTP Configuration

Dis3 is configured as the **VTP primary server** for Branch 2.

VTP Configuration :

```
# On Dis3 (VTP Server)
vtp domain cisco2
vtp version 3
vtp password cisco123 hidden
vtp primary
```

```
# Creating VLANs on Dis3
vlan 50
vlan 60
vlan 70
vlan 80
```

4. HSRP Configuration for VLANs 50 and 60

HSRP Configuration for Dis3 (Active for VLANs 50 and 60):

```
interface vlan 50
 standby 50 ip 192.168.50.254
 standby 50 priority 102
 standby 50 preempt
 standby 50 authentication md5 key-string cisco123
```

Headquarter Network Configuration

1. Trunking and EtherChannel (LACP) Configuration

EtherChannel (LACP) is used between distribution switches.

Configuration :

```
# On Dis1
interface port-channel 21
 no switchport
 ip address 192.168.1.241 255.255.255.252
 no shutdown
interface range g0/0-1
 no switchport
 channel-group 21 mode active
```

2. VTP Configuration

Dis1 acts as the **VTP primary server**.

Configuration :

```
# On Dis1
vtp domain cisco3
vtp version 3
vtp password cisco123 hidden
vtp primary
```

3. HSRP Configuration

Dis1 is the active gateway for VLANs 130, 140, while **Dis2** is the backup.

HSRP Configuration :

```
# On Dis1
interface vlan 130
 standby 130 ip 192.168.130.254
 standby 130 priority 105
 standby 130 preempt
 standby 130 authentication md5 key-string cisco123
```

Campus-wide Security Configuration

Network security is crucial to protect the network infrastructure from unauthorized access, attacks, and other vulnerabilities. Your design implements multiple layers of security, including **HSRP with authentication**, **VTP with passwords**, **Port Security**, **DHCP Snooping**, **Dynamic ARP Inspection (DAI)**, **IP Source Guard**, and **AAA with 802.1x authentication**. Let’s go through each in detail:

---

1. HSRP with MD5 Authentication

HSRP is secured using MD5 authentication to ensure that HSRP messages exchanged between routers are authenticated, preventing rogue devices from taking over the gateway.

Configuration for HSRP Authentication:

```
# On Dis1 for VLAN 10
interface vlan 10
 standby 10 ip 192.168.10.254
 standby 10 authentication md5 key-string cisco123

# Repeat for all VLANs across all switches where HSRP is used.
```

---

2. VTP Version 3 with Secret Password

VTP Version 3 is used to manage VLAN information securely across branches and the headquarter. The VTP password ensures that only authorized devices can participate in the VTP domain.

Configuration :

```
# On all devices ( for Branch 1 and 2)
vtp version 3
vtp password cisco123 hidden
```

---

3. Port Security

Port security restricts the number of MAC addresses that can connect to a switch port, helping to prevent unauthorized devices from accessing the network. By setting a limit and using **sticky** MAC addresses, you ensure that only pre-authorized devices can connect.

Configuration for Port Security:

```
# On access ports connecting to end devices
interface range g0/1-24
switchport mode access
switchport port-security
switchport port-security maximum 2          # Allow a maximum of 2 devices
switchport port-security mac-address sticky # Learn MAC addresses dynamically
```

---

4. Spanning Tree PortFast and BPDU Guard

Spanning Tree PortFast is enabled on access ports to allow immediate transition to the forwarding state, skipping the listening and learning states. **BPDU Guard** is used to prevent rogue switches from being connected to access ports, which could cause Spanning Tree recalculations and possible network loops.

Configuration :

```
# Enabling PortFast and BPDU Guard on access ports
interface range g0/1-24
spanning-tree portfast
spanning-tree bpduguard enable
```

---

5. DHCP Snooping

DHCP Snooping protects the network from rogue DHCP servers by only allowing authorized servers to provide IP addresses to clients. It also helps prevent attacks such as DHCP starvation.

- **Trusted interfaces** (typically uplinks to the DHCP server or distribution switches) are marked as trusted, while client-facing ports are untrusted.

Configuration :

```
# Enabling DHCP Snooping for VLANs
ip dhcp snooping vlan 10,20,30,40
ip dhcp snooping vlan 50,60,70,80
ip dhcp snooping trust           # Trusting uplink interfaces (to DHCP
servers)

# Limiting DHCP request rate to prevent DHCP starvation
ip dhcp snooping limit rate 10
```

Additionally, the **DHCP Helper Address** is configured on distribution switches to relay DHCP requests to the centralized DHCP server, ensuring end devices receive IP addresses from trusted servers.

DHCP Relay (Helper) Configuration :

```
# On distribution switches for each VLAN
interface vlan 10
 ip helper-address 192.168.150.100  # IP address of the centralized DHCP server

# Repeat for all VLANs
```

---

6. Dynamic ARP Inspection (DAI)

Dynamic ARP Inspection (DAI) is used to prevent ARP spoofing attacks by validating ARP packets on the network. DAI works in conjunction with DHCP Snooping, ensuring that ARP packets come from legitimate devices.

Configuration :

```
# Enabling ARP Inspection for VLANs
ip arp inspection vlan 10,20,30,40
ip arp inspection vlan 50,60,70,80

# Validating ARP packets by checking MAC, IP, and destination
ip arp inspection validate src-mac
ip arp inspection validate dst-mac
ip arp inspection validate ip

# Trusting interfaces connected between distribution and access switches
interface g1/0
 ip arp inspection trust
```

---

7. IP Source Guard (IPSG)

IP Source Guard (IPSG) prevents IP address spoofing by ensuring that only legitimate IP-MAC bindings can communicate on a port. IPSG is configured on untrusted ports to block traffic if it doesn’t match the DHCP binding table or static IP-MAC bindings.

Configuration :

```
# On interfaces connected to end devices (untrusted ports)
interface g0/1
 ip verify source port-security   # Verify IP and MAC address combination
```

---

8. AAA (Authentication, Authorization, and Accounting) Security Model

AAA is implemented using **RADIUS** to authenticate users attempting to access the network. **802.1x authentication** is used to prevent unauthorized devices from connecting to the network. If a device passes authentication, it is granted network access; otherwise, it remains blocked.

Configuration :

```
# Enable AAA and configure RADIUS server
aaa new-model
radius-server host 192.168.100.250 auth-port 1812 acct-port 1813 key cisco123

# Enable 802.1x authentication using RADIUS
aaa authentication dot1x default group radius
dot1x system-auth-control

# Configure access ports for 802.1x authentication
interface range g0/1-24
authentication port-control auto
dot1x pae authenticator
```

9. Native VLAN Hopping Prevention

To prevent VLAN hopping attacks, the default **native VLAN** (VLAN 1) is changed to an unused VLAN (VLAN 77 in this case) on trunk links.

Configuration :

```
# Changing the native VLAN on all trunk links to VLAN 77
interface range g0/1-3, g1/0-1
switchport trunk native vlan 77
```

Summary of Security Features Implemented:

- **HSRP with MD5 Authentication**: Secures the gateway failover protocol.
- **VTP Version 3 with Password**: Prevents unauthorized VLAN changes.
- **Port Security**: Limits and secures the number of MAC addresses per port.
- **Spanning Tree PortFast and BPDU Guard**: Protects against bridging loops and rogue devices.
- **DHCP Snooping**: Prevents rogue DHCP servers and DHCP-based attacks.
- **Dynamic ARP Inspection (DAI)**: Prevents ARP spoofing.
- **IP Source Guard (IPSG)**: Prevents IP spoofing by binding IPs to MAC addresses.
- **AAA with 802.1x Authentication**: Provides secure network access through RADIUS.
- **Native VLAN Hopping Prevention**: Secures trunk links from VLAN hopping attacks.

Conclusion:

The **Bank Network Design Project** successfully demonstrates a comprehensive approach to creating a scalable, secure, and highly available network architecture that addresses the critical needs of a modern banking institution. By leveraging a three-tier architecture composed of core, distribution, and access layers, the design ensures efficient traffic flow, segmentation, and redundancy across the bank's headquarter and multiple branch locations. The integration of advanced technologies such as **HSRP**, **EtherChannel**, **RSTP**, and **VTP** provides the necessary failover mechanisms and VLAN management capabilities to maintain operational continuity, even in the event of network disruptions or hardware failures.

Security remains a paramount concern in the financial sector, and this project incorporates multiple layers of security measures to safeguard against external and internal threats. The use of **AAA authentication**, **DHCP Snooping**, **Dynamic ARP Inspection**, **IP Source Guard**, and **802.1x authentication** creates a robust security framework that protects sensitive financial data, prevents unauthorized access, and ensures compliance with regulatory standards. Additionally, these security protocols work in conjunction with redundancy features such as HSRP to ensure that security is maintained even during failover events.

The project also addresses the need for scalability. By using **OSPF** for inter-branch routing and **VTP v3** for VLAN management, the network is designed to accommodate future growth, allowing for the seamless addition of new branches, devices, and services without significant reconfiguration. This ensures that the bank can continue to expand its operations without facing major disruptions or requiring costly network redesigns.

In summary, the **Bank Network Design** offers a solution that not only meets the bank's current needs for security, efficiency, and redundancy but also positions the institution for future growth. The implementation of tested and proven technologies, combined with a focus on best practices in network design, ensures that the network will provide reliable service to both the bank's internal operations and its customer-facing applications for years to come. Through rigorous testing and thorough documentation, the project has demonstrated that the proposed design can meet the challenges of today's complex financial environment while remaining adaptable to future demands.