FutureNet Comprehensive Banking Network Infrastructure

Net Ninjas Team

Name
Mahmoud Al Sayed Shreef
Sherif Thabet Ahmed Yacoub
Shady Adel Tarkhan
Hussein Mohsen Abdulrahman
Aya Khaled Mohammed

Instructor:

Amr Reda

Table Of Contents

Abstract

The FutureNet Comprehensive Banking Network Infrastructure project is designed to provide Future Bank with a resilient, secure, and scalable network that connects its headquarters and branch locations seamlessly. Addressing the critical needs of a modern financial institution, this initiative focuses on creating a network that supports high-performance connectivity, data protection, and compliance with stringent banking regulations. By implementing a sophisticated design, the project ensures secure, efficient communication across all branches and departments, meeting the operational demands of today's highly regulated banking environment.

The project scope includes both physical and logical network layers, integrating advanced technologies that provide a multi-layered approach to security and network management. Core elements include VLAN segmentation, access controls, and centralized management protocols, which together fortify the network against unauthorized access and potential data breaches. The redundancy and failover configurations ensure that the network remains highly available and resilient, maintaining service continuity even in the face of hardware or connectivity disruptions.

In addition to its robust security and reliability features, the infrastructure is designed with scalability at its core. Modular network components and flexible configurations allow Future Bank to expand and adapt the infrastructure as its operations grow and technology needs evolve. Through this approach, FutureNet offers a future-proofed solution that supports long-term growth, positioning Future Bank to confidently navigate the changing technological landscape while ensuring operational efficiency and data security.

Chapter I: INTRODUCTION

1.1 Preamble:

The FutureNet Comprehensive Banking Network Infrastructure project represents a strategic initiative by Future Bank to establish a modern, secure, and interconnected network infrastructure across its headquarters and branch locations. Designed to meet the demands of a highly regulated banking environment, this project aims to support operational efficiency, compliance, and data protection while facilitating seamless connectivity and communication. By deploying this advanced network infrastructure, Future Bank is positioned to enhance its technological foundation, ensuring resilience, security, and scalability for years to come.

1.2 Background of the problem:

In today's digital age, financial institutions like Future Bank face increasing pressure to ensure data security, regulatory compliance, and reliable communication across all branches. Without an existing robust infrastructure, the bank encounters limitations in securing sensitive data, achieving efficient inter-branch communication, and adhering to compliance standards. As a response, Future Bank has chosen to implement an entirely new network infrastructure rather than upgrade an outdated system. This approach allows the bank to maintain full control over its network design, scalability, and security measures, providing a future-ready foundation that supports growth and innovation.

1.3 Statement of the Problem:

Future Bank requires a secure, scalable, and highly available network infrastructure that addresses critical challenges in security, operational efficiency, and compliance. This project aims to meet these needs by implementing a state-of-the-art network that supports high-performance connectivity between the headquarters and branch locations, secures sensitive data from internal and external threats, and aligns with industry regulations. Through this infrastructure, the bank seeks to ensure continuous, reliable service, supporting seamless operations across its locations.

1.4 Objectives:

The main objectives of the FutureNet Comprehensive Banking Network Infrastructure project are as follows:

- Enhance security to protect sensitive financial data and ensure compliance with industry regulations.
- Improve inter-branch connectivity to facilitate seamless and efficient operations.
- Develop a scalable infrastructure to accommodate Future Bank's growth and adapt to technological advancements.

.

1.5 Scope of the Problem:

This network infrastructure project is critical for Future Bank to achieve secure and compliant operations within the financial industry. The project's design prioritizes reliable connectivity, data protection, and future scalability, which together enable the bank to navigate the challenges of a regulated environment with confidence. With a strong focus on security, the infrastructure supports seamless banking operations, fosters customer trust, and establishes a foundation for sustainable growth.

1.6 Significance of the Problem:

A well-designed network, even in simulation, plays a vital role in demonstrating the critical nature of hospital operations. This project will simulate how an advanced network can improve patient care, streamline administrative tasks, and ensure compliance with healthcare regulations. The use of Packet Tracer allows for the design and testing of a scalable and secure network that can serve as a model for real-world deployment.

1.7 Conclusion:

In summary, the FutureNet Comprehensive Banking Network Infrastructure project is an essential undertaking for Future Bank. By addressing critical needs in security, connectivity, and scalability, this project aligns with the bank's mission to provide reliable, efficient, and compliant financial services. The groundwork laid in this introduction sets the stage for the detailed design, implementation, and security protocols that will follow in this documentation.

Chapter II: Project Requirements and Analysis

2.1 Functional Requirements

The FutureNet Comprehensive Banking Network Infrastructure project aims to provide a secure, scalable, and efficient network environment for Future Bank's headquarters and branch locations. The key functional requirements are as follows:

- **Data Security**: Implement robust security protocols to protect sensitive financial data from internal and external threats. This includes encryption for data in transit, access control lists (ACLs), and secure authentication methods.
- **Inter-branch Connectivity**: Establish seamless, high-performance connectivity between headquarters and branches to support efficient, real-time communication across departments. This involves implementing site-to-site VPNs and redundancy measures to prevent connectivity disruptions.
- **Regulatory Compliance**: Ensure the network meets the regulatory requirements of the banking industry, including data protection standards and secure data handling practices, to foster compliance and maintain the bank's reputation.

These functional requirements form the backbone of the network's design, ensuring that the infrastructure supports Future Bank's operational goals, protects customer data, and adheres to industry regulations.

2.2 Technical Specifications

The technical specifications outline the core hardware, software, and configurations required to achieve the project's functional requirements. Below is a list of the key network devices, including their roles and descriptions.

- **Network Devices**:
    - **Core Routers (Cisco 2911)**:
    - **Quantity**: 2
    - **Role**: These routers serve as the primary inter-branch connectivity solution, handling core routing tasks to enable secure communication between the headquarters and branch locations. Configured with OSPF and EIGRP for dynamic routing, they provide both scalability and efficient route convergence.

- **Core Switches (Cisco Catalyst 3650)**:
- **Quantity**: 4
- **Role**: The core switches are responsible for VLAN distribution and high-speed data transfer within each location. Positioned at the core of the network, these switches handle large volumes of traffic and support VLAN trunking to ensure seamless communication across departments.

- **Access Switches (Cisco Catalyst 2960)**:
- **Quantity**: 10
- **Role**: The access switches connect end-user devices to the network, enabling VLAN segmentation and providing fast data transfer. Configured with access control lists and port security, these switches ensure secure access at the edge of the network.

- **Wireless LAN Controller (WLC)**:
- **Role**: The WLC manages lightweight access points to provide wireless connectivity throughout the HQ and branch locations. It offers centralized control over SSIDs, channel assignment, and security policies, ensuring seamless and secure wireless access across the network.

- **Lightweight Access Points:**
- **Role:** Deployed across the HQ and branch locations, these access points provide wireless coverage, extending network access to mobile users. They are centrally managed by the WLC, ensuring consistent configurations and security.

- **Servers:**
    - **DHCP Server**: Responsible for dynamically assigning IP addresses to network devices, this server ensures efficient IP management across HQ and branch locations. It supports network scalability by managing IP pools for multiple VLANs.
    - **DNS Server**: The DNS server translates domain names to IP addresses, facilitating access to internal and external resources. It is essential for efficient network navigation and service discovery.
    - **NTP Server**: The NTP server synchronizes the clocks of all network devices, ensuring time consistency across HQ and branch locations. Accurate timekeeping is critical for logging, security audits, and troubleshooting.
    - **Syslog Server:** Centralized logging server that collects and stores log data from routers, switches, and other network devices. It provides critical data for network monitoring, security auditing, and issue diagnosis.
    - **Web Server:** Hosts internal websites and web applications used by bank employees, enabling access to shared resources, documentations, and company portals.
    - **Email Server:** Manages and stores emails for bank employees, ensuring secure and reliable internal and external communication. Configured to support security policies like encryption and spam filtering.
- **Configurations:**
    - **VLAN Segmentation:** Each department's traffic is segmented into its own VLAN, enhancing security and simplifying network management.
    - **Routing Protocols**: OSPF is configured for dynamic, scalable routing within HQ and branch, while EIGRP provides rapid route convergence.
    - **VPN**: A site-to-site VPN, secured with IPsec, enables encrypted communication between HQ and branch.

- **Standards**: Adhere to IEEE 802.1Q standards for VLAN tagging and use IPsec for VPN security, with expanded configurations detailed in later sections.
- **Device Specifications Table:**

DEVICE TYPE	MODEL	QUANTITY	PRIMARY ROLE	DESCRIPTION
CORE ROUTER	Cisco 2911	2	Core routing, inter-branch connection	Manages routing between HQ and branches
CORE SWITCH	Cisco Catalyst 3650	4	Core switching, VLAN distribution	Handles high-speed core traffic and VLANs
ACCESS SWITCH	Cisco Catalyst 2960	10	Access layer for end-user connections	Provides connectivity and VLAN segmentation
WIRELESS LAN CONTROLLER	(Model based on WLC)	1	Manages wireless access points	Centralized control of WiFi network
LIGHTWEIGHT ACCESS POINTS	(Model based on AP)	Multiple	Extends wireless coverage	Provides wireless access to mobile devices
DHCP SERVER	N/A	1	IP address management	Assigns IPs dynamically
DNS SERVER	N/A	1	Domain name resolution	Maps domain names to IP addresses
NTP SERVER	N/A	1	Time synchronization	Ensures consistent timestamps
SYSLOG SERVER	N/A	1	Centralized logging	Collects logs for monitoring and audits
WEB SERVER	N/A	1	Hosts internal websites	Provides access to bank resources
EMAIL SERVER	N/A	1	Email management	Manages internal and external communication

2.3 Assumptions and Constraints:

The design and implementation of the FutureNet project are based on specific assumptions and constrained by a few critical factors:

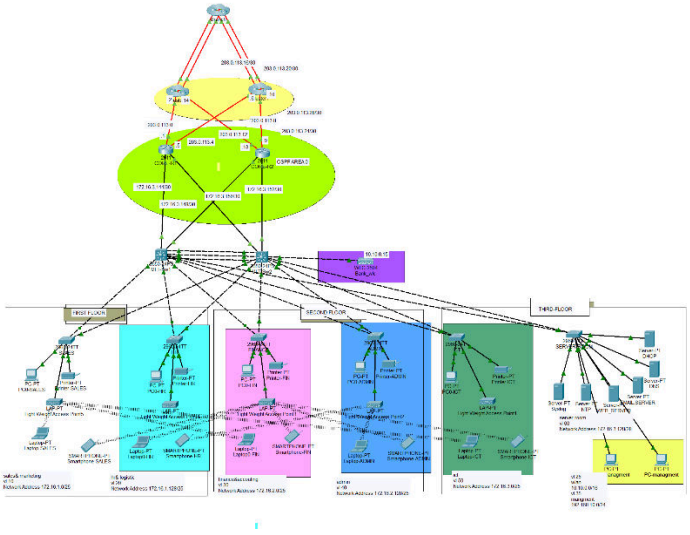
- **Assumptions**:
    - The network will support the current estimated number of users and devices across both the headquarters and branch locations.
    - All personnel accessing the network will use devices compatible with Cisco network configurations.
- **Constraints**:
    - **Budget Limitations**: The project must remain within the allocated budget, which may affect the choice of certain hardware or advanced configurations.
    - **Physical Installation Constraints**: The layout and available space at both HQ and branch locations dictate certain design choices, especially concerning hardware placement and cabling.
    - **Performance Constraints**: The network must meet minimum bandwidth and latency requirements to support banking operations and real-time data access.

These assumptions and constraints provide the boundaries within which the network must be designed, ensuring optimal performance while aligning with Future Bank's budget and physical environment.

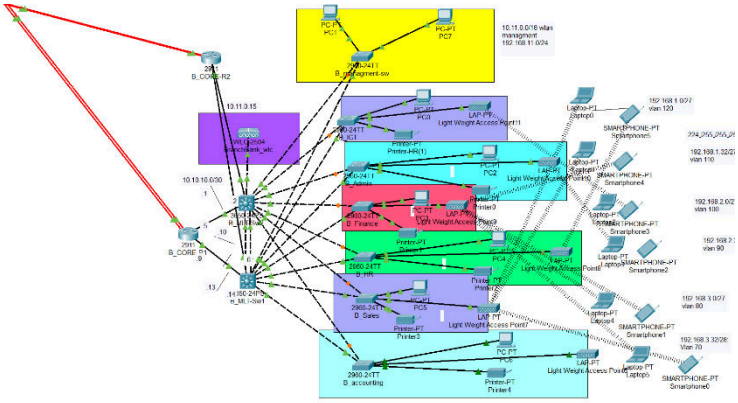
Chapter III: Network Design and Architecture

3.1 Physical Topology:

The physical topology represents the layout of network devices at both the headquarters (HQ) and branch locations, focusing on the connections between core routers, switches, servers, wireless LAN controller (WLC), and lightweight access points (APs). The diagram below provides a simplified view, emphasizing the relationship between primary devices without extensive port or cabling details.



"HQ Topology"

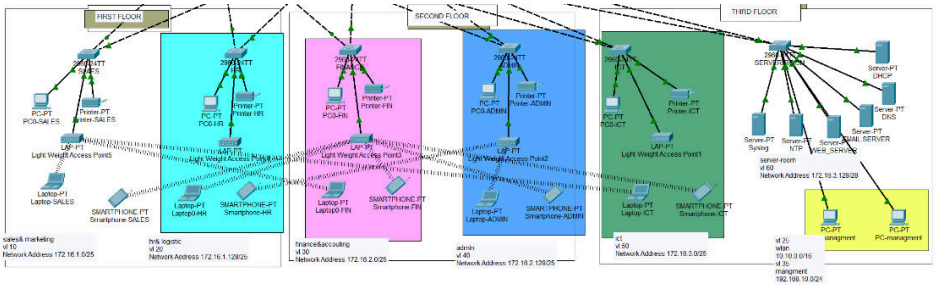


"BRANCH Topology"

A simplified diagram showing the HQ and branch setups, including connections between core routers, core and access switches, servers, WLC, and access points.

3.2 Logical Topology:

The logical topology illustrates how VLANs, IP subnets, and routing paths are organized within the network. This design leverages VLANs for network segmentation, with each department assigned a dedicated VLAN and corresponding IP subnet. Main routing paths connect HQ and branch locations, facilitating efficient data flow and inter-department communication.



3.3 Network Components:

This section provides detailed descriptions of the network components used in the FutureNet infrastructure. Devices are organized by type and location (HQ or branch) to clarify roles and placements.

Network Components Table:

Device Type	Model	Location	Role	Description
Core Router	Cisco 2911	HQ, Branch	Core routing, inter-branch connection	Manages routing between HQ and branch
Core Switch	Cisco Catalyst 3650	HQ	Core switching, VLAN distribution	Handles high-speed core traffic and VLANs
Access Switch	Cisco Catalyst 2960	HQ, Branch	Access layer for end-user connections	Provides connectivity and VLAN segmentation
Wireless LAN Controller	WLC Model	HQ	Manages wireless access points	Centralized control of WiFi network
Lightweight Access Points	AP Model	HQ, Branch	Extends wireless coverage	Provides wireless access to mobile devices

DHCP Server	N/A	HQ	IP address management	Assigns IPs dynamically
DNS Server	N/A	HQ	Domain name resolution	Maps domain names to IP addresses
NTP Server	N/A	HQ	Time synchronization	Ensures consistent timestamps
Syslog Server	N/A	HQ	Centralized logging	Collects logs for monitoring and audits
Web Server	N/A	HQ	Hosts internal websites	Provides access to bank resources
Email Server	N/A	HQ	Email management	Manages internal and external communication

Each device is essential to supporting Future Bank's operational goals, providing the necessary connectivity, data management, and network services.

3.4 Naming and IP Addressing Scheme:

A standardized naming and IP addressing scheme is used to simplify device identification and management, enhancing troubleshooting efficiency. Each department is assigned a unique VLAN, and devices within each VLAN are allocated IP addresses from specific subnet ranges.

IP Addressing Scheme Table:

VLAN	Department	Subnet	Default Gateway	Devices/Range
10	Sales	172.16.1.0/25	172.16.1.1	172.16.1.2 - 172.16.1.126
20	HR	172.16.1.128/25	172.16.1.129	172.16.1.130 - 172.16.1.254
30	Finance	172.16.2.0/25	172.16.2.1	172.16.2.2 - 172.16.2.126
40	Admin	172.16.2.128/25	172.16.2.129	172.16.2.130 - 172.16.2.254
50	ICT	172.16.3.0/25	172.16.3.1	172.16.3.2 - 172.16.3.126

60	Server Room	172.16.3.128/28	172.16.3.129	172.16.3.130 - 172.16.3.142

The IP addressing scheme assigns specific ranges to each VLAN, ensuring organized traffic segmentation and enhanced security. Device naming follows a structured convention, such as "HQ-SW-Core1" for HQ core switches and "BR-RT-Branch1" for branch routers.

3.5 Redundancy and High Availability:

To ensure high availability and minimal downtime, the network incorporates redundancy mechanisms using both HSRP (Hot Standby Router Protocol) and EtherChannel. HSRP provides router redundancy, allowing a backup router to take over in case the primary router fails. EtherChannel, configured on core switches, offers link redundancy by bundling multiple Ethernet links, which increases bandwidth and provides a failover path.

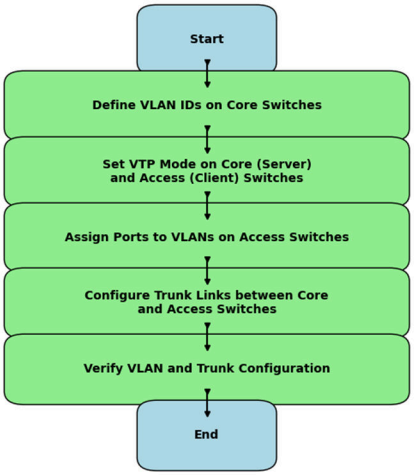
These redundancy measures ensure that Future Bank's network remains resilient and able to maintain uninterrupted service, even in the event of a device or link failure.

Chapter IV: Network Configuration and Implementation

4.1 Layer 2 Configuration:

The Layer 2 configuration for FutureNet's network establishes VLANs to ensure proper traffic segmentation and basic loop prevention to maintain a stable network environment.

- **VLAN Configuration**: VLANs are configured centrally on the core switches, with VTP (VLAN Trunking Protocol) used to propagate VLAN information to access switches. This centralized approach simplifies VLAN management and ensures consistent VLAN availability across the network.
- **Spanning Tree Protocol (STP)**: Standard STP is configured to prevent network loops. STP ensures that only the necessary paths are active at any given time, maintaining network stability and reducing potential broadcast storms.



A flowchart showing steps to configure VLANs, assign ports, and configure trunks.

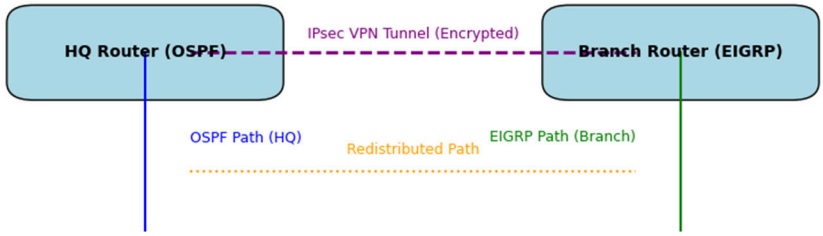
4.2 Layer 3 Configuration:

Layer 3 configuration in FutureNet's network includes dynamic routing within the HQ and branch locations, as well as secure inter-branch communication.

- **Routing Protocols**:
  - **OSPF** is implemented internally at the HQ to dynamically manage routing between subnets.
  - **EIGRP** is configured within the branch location to manage local routing.

- **Redistribution** allows OSPF and EIGRP routes to be shared between HQ and branch, enabling seamless connectivity and inter-operability.

- **VPN Configuration**: Basic IPsec VPN is set up between HQ and the branch to secure inter-branch communication. IPsec provides encryption, ensuring that data remains private and secure as it travels across the VPN tunnel.



A diagram illustrating main routing paths and VPN setup steps for inter-branch communication.

4.3 Access Control Lists (ACLs):

General network-wide ACLs are configured to control traffic flow, ensuring only authorized data passes between network segments. The table below summarizes key ACLs and their actions.

ACL Name	Action	Source	Destination	Description
ACL_Allow_Internal	Permit	Internal VLANs	Internal VLANs	Allows traffic between internal VLANs
ACL_Deny_External	Deny	External Networks	Sensitive VLANs	Blocks external access to sensitive data
ACL_Admin_Only	Permit	Admin VLAN	Management VLAN	Restricts management access to admins only

These ACLs ensure secure traffic flow and prevent unauthorized access to critical areas within the network.

4.4 Device Security

Device security in FutureNet's network relies on basic password protection, port security, and secure access protocols to restrict unauthorized access to network equipment.

- **Password Protection**: Devices are secured with strong passwords on administrative accounts. This ensures that only authorized personnel can access and manage network devices.
- **Port Security**: Port security settings are configured on access switches to limit the number of MAC addresses per port. This helps prevent unauthorized devices from connecting to the network.
- **SSH Configuration**: SSH is enabled on network devices to allow secure remote management, protecting data from potential interception during remote sessions.
- **Role-based Access Control**: Role-based restrictions are set to grant specific access levels to users, limiting administrative access to authorized personnel only.

Device Type	Location	Port Security	SSH Setup	Additional Security Settings
Core Router	HQ	N/A	SSH enabled, port 22	Strong password policy, ACLs for management access
Core Router	Branch	N/A	SSH enabled, port 22	Strong password policy, ACLs for management access
Core Switch	HQ	Enabled on user-facing ports	SSH enabled, port 22	Port security to restrict MAC addresses; ACLs for management VLAN
Access Switch	HQ, Branch	Enabled on all user-facing ports	SSH enabled, port 22	MAC address limit set per port, shutdown on violation
Wireless LAN Controller (WLC)	HQ	N/A	SSH enabled, port 22	Role-based access control, WPA2 for wireless encryption

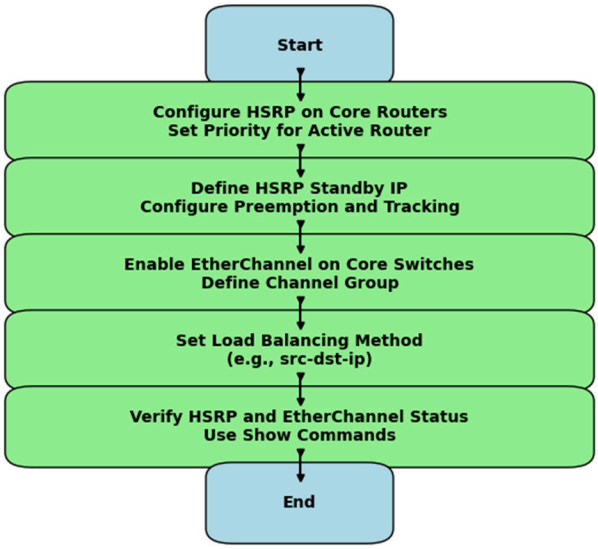
DHCP Server	HQ	N/A	Disabled (local access only)	Restricted to internal VLAN only
DNS Server	HQ	N/A	Disabled (local access only)	DNSSEC for secure queries, restricted to internal network
Web Server	HQ	N/A	Enabled for remote management	SSL/TLS for secure web access
Email Server	HQ	N/A	Enabled for remote management	SSL/TLS for email encryption
Syslog Server	HQ	N/A	Disabled (local access only)	Internal logging restricted to management VLAN

A table summarizing security configurations for each key device, including port security and SSH setup.

4.5 Redundancy and High Availability:

To maintain network uptime and support failover, FutureNet's network uses redundancy mechanisms through HSRP and EtherChannel.

- **HSRP Configuration**: A simplified HSRP setup provides router redundancy between HQ and the branch, with one active router and one standby router. This configuration ensures that if the active router fails, the standby router takes over automatically, maintaining connectivity.
- **EtherChannel**: EtherChannel is configured on core switches to bundle multiple Ethernet links, providing link redundancy. In the event of a link failure, traffic is rerouted through available links within the bundle, ensuring continuous service.



A flowchart showing HSRP and EtherChannel configuration steps to enable failover and link redundancy

Chapter V: Security Measures

To protect the FutureNet network infrastructure, a series of layered security protocols are employed, addressing both internal and external threats. This section outlines the measures taken, focusing on VLAN segmentation, access control, VPN, DMZ placement, role-based access, and monitoring.

5.1 Internal Threat Protection:

1. **VLAN Segmentation** VLANs are implemented to separate network traffic, providing enhanced security and easier management by isolating departments.

VLAN ID	Department	IP Range	Ports Assigned
10	Sales	172.16.10.0/24	Ports 1-10 on Access Switch 1
20	HR	172.16.20.0/24	Ports 11-20 on Access Switch 2
30	Finance	172.16.30.0/24	Ports 21-30 on Access Switch 3
40	Admin	172.16.40.0/24	Ports 31-40 on Access Switch 4
50	ICT	172.16.50.0/24	Ports 1-10 on Core Switch

2. **Access Control Lists (ACLs)** ACLs enforce control over traffic between departments and across the network, securing resources and restricting access where necessary.

ACL Name	Source VLAN	Destination VLAN	Action	Description
Sales_to_Finance	10	30	Deny	Restricts access from Sales to Finance
HR_to_Admin	20	40	Permit	Allows HR to access Admin resources
IT_Support	50	All	Permit	ICT can access all VLANs for support

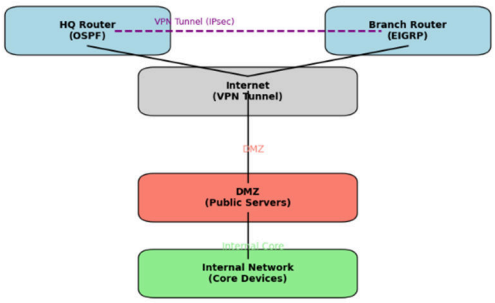
3. **Port Security** Port security measures are in place to restrict devices based on MAC address, with automatic shutdown on security violation to protect against unauthorized connections.

Switch Location	Port	Max MAC Addresses	Violation Action
Access Switch 1	Ports 1-10	2	Shutdown
Access Switch 2	Ports 11-20	1	Shutdown
Core Switch	Ports 1-10	5	Alert

5.2 External Threat Protection

1. **VPN Overview** An IPsec VPN is configured to secure communication between the HQ and branch, encrypting data and maintaining privacy across the connection. The VPN establishes an encrypted tunnel, ensuring that sensitive data remains protected even in transit.
2. **DMZ Configuration** A Demilitarized Zone (DMZ) is established to host public-facing services, allowing secure external access without exposing internal network segments.
    - **DMZ Placement**: The DMZ is placed between the internet-facing router and internal network.
    - **Hosted Services**: Public resources like the web server and email gateway are hosted in the DMZ, ensuring external requests are isolated from the core network.

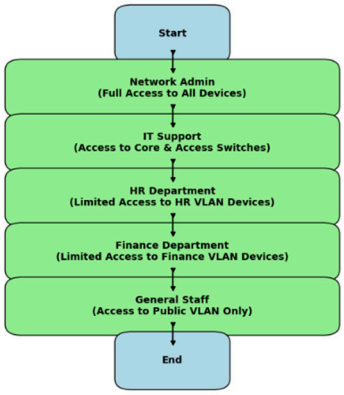
A network diagram is provided below, showing VPN connections between HQ and branch locations, and DMZ placement to indicate inbound and outbound traffic paths.



5.3 Access Control Policies:

1. **Role-Based Access Control** To maintain secure access, a role-based control policy is implemented, restricting access based on user roles and departmental needs. Only personnel in the ICT department, for example, have administrative access to core network devices.

2. **Password Policies** Strong password policies enforce a high level of security for all devices, requiring complex passwords, periodic updates, and unique combinations to prevent unauthorized access.



An access control flowchart details role-based access levels across key network devices.

5.4 Monitoring and Logging:

1. **Monitoring Overview** Monitoring and logging are essential for tracking network events and security threats. SNMP and Syslog are configured to capture and report on network activity, allowing administrators to monitor traffic patterns and receive alerts on potential security issues.

2. **Centralized Logging** A centralized logging system records logs from all critical devices, storing them in a secure location for easy retrieval and review during audits or security investigations.

This **Security Measures** section integrates multi-layered protocols to ensure both internal and external protection, supporting the secure and efficient operation of the FutureNet infrastructure.

Chapter VI: Testing and Validation

The Testing and Validation phase ensures that the network design meets FutureNet's operational requirements, providing robust connectivity, redundancy, and security. Each test is planned to validate specific aspects of the network, with results recorded to confirm successful implementation.

6.1 Testing Plan:

The testing plan includes multiple phases to validate connectivity, performance, failover mechanisms, and security controls. Each test is designed with a clear objective, expected outcomes, and target devices.

Test Type	Objective	Devices Involved	Expected Outcome
Connectivity	Verify communication across VLANs and HQ-branch link	Core routers, access switches	Endpoints in each VLAN can communicate as per ACLs
Performance	Assess network performance under typical loads	Core and access layer switches	Stable response times and no packet loss under load
Failover	Test HSRP and EtherChannel redundancy	HQ router, branch router, switches	Failover operates without downtime or packet loss
Security	Confirm access control and VPN encryption	HQ and branch routers, servers	ACLs enforce role-based access; VPN maintains encryption

6.2 Testing Procedures:

1. **Connectivity Tests**
    - **Objective**: To confirm reliable communication across VLANs and between HQ and branch locations.
    - **Steps**:
        1. **Ping Tests**: Ping devices within each VLAN to verify connectivity.
        2. **Traceroute**: Use traceroute to map the path between HQ and branch to check for routing issues.
        3. **Inter-VLAN Communication**: Test inter-VLAN communication, verifying ACLs allow/deny rules per policy.
2. **Redundancy Tests**
    - **Objective**: To ensure that redundancy mechanisms function as expected in the event of a link or device failure.

- **Steps**:
    1. **HSRP Failover**: Simulate a failure on the primary router and verify that the backup router assumes the active role seamlessly.
    2. **EtherChannel Failover**: Disconnect one of the links in the EtherChannel group and confirm that traffic is rerouted through available links without packet loss.

3. **Security Tests**
    - **Objective**: To validate access control configurations, VPN security, and port security measures.
    - **Steps**:
        1. **ACL Verification**: Test access control lists by attempting to access resources between VLANs according to specified rules.
        2. **VPN Security**: Inspect the VPN tunnel for encryption integrity using monitoring tools and verify encrypted traffic between HQ and branch.
        3. **Port Security**: Simulate unauthorized device connection to a secured port to ensure port security policies trigger a shutdown or alert.

6.3 Results:

Each test's outcome is carefully recorded to confirm the network's operational integrity. The testing results ensure the following:

- **Connectivity**: All VLANs maintain stable and controlled connectivity, with inter-VLAN communication adhering to ACL policies.
- **Performance**: Network response times and throughput meet expected benchmarks, even under simulated load conditions.
- **Failover**: HSRP and EtherChannel perform as expected, with no service interruption during failover simulations.
- **Security**: ACLs enforce role-based access, VPN maintains data confidentiality, and port security prevents unauthorized device access.

Upon successful completion, the network is validated as secure, resilient, and capable of supporting FutureNet's operational needs. Any adjustments made based on testing are documented for continuous improvement and future reference.

Chapter VII: Challenges and Solutions

During the network design and implementation, several challenges were encountered. These issues, spanning hardware limitations, configuration conflicts, and security vulnerabilities, required careful consideration and adjustments to ensure the project's success.

7.1 Challenges Encountered:

1. **Hardware Limitations**
    - **Simulation Constraints**: Cisco Packet Tracer's limitations restricted the simulation of advanced networking features, affecting the ability to fully test and validate some configurations.
    - **Device Compatibility**: Some devices experienced firmware mismatches, leading to compatibility issues that limited interoperability within the network.
2. **Configuration Conflicts**
    - **Routing Protocol Inconsistencies**: Implementing route redistribution between OSPF and EIGRP led to conflicts, resulting in occasional routing loops and connectivity issues between HQ and branch locations.
    - **ACL Rule Conflicts**: Overlapping or conflicting ACL rules inadvertently restricted intended traffic flow, leading to unintended access issues that impacted inter-departmental communication.
3. **Security Vulnerabilities**
    - **VPN Encryption Issues**: Initial VPN configurations faced encryption challenges, potentially exposing data in transit between HQ and branch locations. Addressing these issues was essential to maintain the confidentiality of inter-branch communication.

7.2 Solutions Applied:

To address these challenges, specific solutions were applied to optimize performance and maintain network security.

Challenge	Solution
Simulation Constraints	Simplified some configurations and used alternative testing environments when possible.
Device Compatibility	Standardized firmware across compatible devices to ensure interoperability and smooth communication.
Routing Protocol Inconsistencies	Adjusted redistribution settings and fine-tuned route metrics to prevent routing loops and ensure stable connectivity.
ACL Rule Conflicts	Reviewed and revised ACL rules to remove overlaps, ensuring intended traffic flow without disruptions.
VPN Encryption Issues	Applied stronger encryption protocols and verified VPN configurations to maintain secure communication.

Chapter VIII: Conclusion and Recommendations

The FutureNet Comprehensive Banking Network Infrastructure project successfully establishes a secure, scalable, and efficient network for Future Bank, connecting HQ and branch locations. This conclusion highlights the primary outcomes and suggests future enhancements to maintain the network's reliability and security as the organization evolves.

8.1 Summary of Project Outcomes:

The network infrastructure achieved the following key outcomes:

1. **Enhanced Security and Redundancy**
    - Implemented VLAN segmentation, VPN, and ACLs to safeguard sensitive data and control inter-departmental access.
    - Redundancy protocols, including HSRP and EtherChannel, ensure network availability and resilience, minimizing the risk of downtime.
2. **Scalability for Future Growth**
    - Designed with scalability in mind, the network can accommodate additional users and locations without compromising performance.
    - Logical and physical segmentation allows for seamless integration of new departments or branches as the organization expands.
3. **Network Stability and Performance**
    - Optimized routing protocols and port security enhance the network's stability and reliability.
    - Rigorous testing confirmed that the network meets performance benchmarks, supporting efficient, uninterrupted connectivity for Future Bank.

8.2 Recommendations for Future Improvements:

To maintain an optimal level of security and operational efficiency, the following recommendations are suggested for future network development:

1. **Advanced Monitoring Tools**
    - Introduce tools such as Cisco Prime or PRTG to provide in-depth, real-time network monitoring and analysis. These tools can proactively

identify performance bottlenecks or security anomalies before they impact operations.

2. **Enhanced Security Measures**
    - Implement multi-factor authentication (MFA) for remote access to further secure sensitive network devices.
    - Consider adding a firewall with DMZ segmentation to better protect public-facing services and restrict external access points.
3. **Scalability Options**
    - Expand the network architecture to support additional branches, regional offices, or remote workforce requirements. This may involve adding more VPN tunnels, extending the IP addressing scheme, and ensuring robust bandwidth management.

8.3 Visual Summary

The following table highlights the key benefits achieved through this project:

Benefit	Description
Security	Improved with VLAN segmentation, VPN encryption, and access control lists
Redundancy	HSRP and EtherChannel provide backup paths for continuous operation
Scalability	Ready for future expansion to support additional branches and departments
Performance	Stable and efficient connectivity, meeting performance benchmarks

---

This **Conclusion and Recommendations** section encapsulates the project's success in establishing a secure and resilient network for FutureNet, with a foundation for continued growth and enhancement.

Appendix

9.1 Device Configuration Files:

Below are sample configuration snippets for key network devices used in the FutureNet Comprehensive Banking Network Infrastructure. These configurations are intended as a reference for initial setup and future troubleshooting.

1. **Router Configuration (HQ and Branch)**

plaintext

Copy code

```
! Enable IP routing
ip routing


! OSPF Configuration (HQ)
router ospf 1
 network 172.16.0.0 0.0.255.255 area 0


! EIGRP Configuration (Branch)
router eigrp 100
 network 10.0.0.0 0.0.0.255
```

2. **Switch Configuration**

plaintext

Copy code

```
! VLAN Configuration
vlan 10
 name Sales
vlan 20
 name HR


! Enable Port Security
switchport port-security
```

switchport port-security maximum 2

switchport port-security violation shutdown

3. **VPN Configuration**

plaintext

Copy code

crypto isakmp policy 10

authentication pre-share

encryption aes

group 5

crypto isakmp key your_key address <remote_ip>

crypto map VPN 10 ipsec-isakmp

set peer <remote_ip>

set transform-set aes

9.2 Glossary of Terms

Term	Definition
ACL (Access Control List)	A set of rules used to filter network traffic, providing security by controlling access.
DMZ (Demilitarized Zone)	A network segment that separates public-facing services from the internal network for security.
EIGRP (Enhanced Interior Gateway Routing Protocol)	A routing protocol used for exchanging routing information.
HSRP (Hot Standby Router Protocol)	A Cisco protocol that provides network redundancy by allowing multiple routers to work together.

9.3 References:

1. Cisco Systems. *Cisco Packet Tracer Configuration Guide*. Cisco Networking Academy.
2. Cisco Systems. *Secure Network Design for Financial Institutions*. Cisco Documentation.
3. *Best Practices for VLAN and IPsec VPN Deployment*, Industry Standards Documentation.