# “Implementation of a Secure Redundant Network Infrastructure for a Financial Services Institution”

## Project Overview :-

In the modern financial landscape, institutions must operate with high levels of security, availability, and scalability to protect sensitive data and deliver uninterrupted services. This project provides an in-depth technical and operational blueprint for deploying a highly secure, redundant, and scalable network infrastructure for a mid-sized financial institution. The solution integrates on-premises HQ and branch networks with AWS cloud services while ensuring compliance with ISO/IEC 27001, PCI-DSS, and NIST CSF security frameworks.

## Case study :-

### 📍 Institution Profile:

A mid sized financial institution headquarter in Cairo, Egypt, with one regional branch and a disaster recovery/data Center in AWS Cloud ( Ireland region). The institution handles financial transaction, client database, and remote customer service-making Uptime and Security critical.

### Challenges Identified:

1) No redundancy in the WAN link, causing frequent downtime.
2) Limited VLAN segmentation leading to poor traffic isolation.
3) Insecure remote access for admins and branch users.
4) Poor scalability for future cloud integration and growth.

### ✓ Solution Objectives:

- Establish Site-to-Site VPN tunnels (GRE using IPsec) for secure connectivity.
- Implement Layer 3 Switching and VLAN segmentation.
- Enforce redundant ISP links with IP SLA( Service Level Agreement ) fail-over.
- Integration with AWS for backups and disaster recovery (DR) from an Enterprise Network, using a combination of networking, storage, and security protocols to ensure secure,efficient, and reliable connectivity.
- Apply strong AAA (Authentication, Authorization, and Accounting ), ACL( Access Control List), and firewall policies.
- Monitor performance, detect anomalies, and Log events, using a combination of network monitoring tools, protocols and logging Infrastructure ( Zabbix Network Monitor ).

## Business Requirements :-

1. Ensure secure, encrypted communications across all locations, to protect sensitive data, maintain confidentiality, and comply with industry security standards.
2. Enable redundant network infrastructure to eliminate Single point of failure ( SPOF) and ensure continuous availability, the system should be designed with high-availability, automatic fail over, and load balancing mechanism ro maintain continuity in the event of hardware, link, or configuration failures.

3. Achieve ISO/IEC (27001) : This includes establishing risk-based controls, securing communication channels, ensuring data confidentiality and integrity, enforcing access control policies, and maintaining audit-ready documentation to support continuous monitoring, incident response, and ongoing improvement.

4. The organization required centralized management of core IT Services such as :-

- Centralized DHCP : Efficiently manages IP addressing, reduces confilcts.
- Centralized DNS: Enhances name resolution speed and accuracy across sites.
- Centralized VOIP : Ensure Quality of services (QOS) and Centralized call management.
- Centralized File sharing : Simplifies access control and backup operations.

5. The network infrastructure must be designed with scalability and flexibility in mind to accommodate future integration with cloud services ( AWS OR Azure ) and ensure secure, reliable access for remote employees.

6. Ensures continuous services up time with a minimum of 99.99 % availability, minimizing downtime to support uninterrupted access to critical services and operations.

# Functional Requirements :-

1) Implement VLAN and sub-net separation for each department to ensure network segmentation enhance security, and improve traffic management across the organization.

2) Implement secure and reliable routing between the Headquarters, Branch office, and AWS cloud Environment using Site-to-Site VPN connection to ensure encrypted communication and data integrity across the locations.

3) Implement role-based access control by integrating AAA ( Authentication, authorization, and accounting ) using TACACS+ and RADIUS protocols, ensuring secure and audit- able access to network resources based on user roles and responsibilities.

4) Implement Dual WAN connectivity with automatic fail-over using IP SLA tracking, ensuring seamless internet connectivity in case of primary like failure.

5) Implement Voice Over IP ( VOIP ) communication system integrated with Quality of services mechanisms ( QOS ), to ensure clear, reliable voice transmission across the network, QOS should prioritize voice traffic to minimize latency, jitter, and packet loss, supporting high-quality, and real-time communication.

6) Deploy a Cisco ASA firewall at the network perimeter to provide traffic filtering, intrusion prevention, and secure access control between internal and external network. This ensure only authorized traffic is allowed, enhancing the overall security posture of the organization.

7) Implement a cloud VPN connection to AWS to enable secure access to disaster recovery ( DR) and backup services, utilization a combination of GRE over IPsec to ensure encrypted, resilient tunneling with support for multi-cast traffic and routing protocols.

8) Provide comprehensive wire and wireless network converges across all areas of operations, utilizing centrally managed wireless controllers to ensure seamless connectivity, efficient configuration, performance monitoring, and secure access control.

# Non-Functional Requirements

1. **Availability** : maintain 99.99 % through the implementation of network and system redundancy, high-availability protocols Such as { HSRP/ VRRP }, fail-overs mechanisms, and continuous monitoring using real-time alerting systems. This ensures business continuity and minimal service disruption.
2. **Security** : Align the network infrastructure with ISO/ IEC 27001 Standards, implementation a " Least privilege " access model across all systems. This Include : -

- ◆ Role-based Access Control ( RBAC).
- ◆ Network Segmentation via VLANs and access control lists (ACLs).
- ◆ Encrypted communications (IPsec).
- ◆ Regular vulnerability assessments and compline auditing.

3. **Scalability** : Design the network with modular and scalable architecture to support the seamless addition of new branch sites, IoT devices, and cloud-based resources (e.g., AWS, Azure). This includes scalable IP addressing schemes, expandable routing protocols (e.g., OSPF), and cloud-compatible edge appliances.
4. **Performance** : Ensure network efficiency by maintaining latency under 10 milliseconds across internal segments. This is achieved via:

- High-throughput switches and routers
- Proper Quality of Service (QoS) configuration

- Redundant and load-balanced paths
- Optimized cabling and topology layout

5. **Manageability** : Enable effective network administration through:

- **SNMP (Simple Network Management Protocol)** for real-time device and interface monitoring
- **Syslog** integration for centralized logging and event tracking
- **Unified dashboards** (e.g., SolarWinds, PRTG, Cisco DNA Center), that provide centralized visibility, configuration, and fault management.

# Department Names

1) Customer services
2) HR Department
3) Finance Department
4) Network Operations
5) Sales & Marketing
6) Legal & Compliance
7) Accounting & Administrations
8) IT Department

# Detailed Network Architecture

## High-Level Network Topology

HQ (Cairo, Egypt) – Core/Distribution/Access layers with redundant ISP links.

Branch Office – Connects via dual Site-to-Site IPsec VPNs (ISP failover).

AWS Cloud (Ireland Region) – Hybrid cloud integration using AWS Direct Connect + VPN backup.

Disaster Recovery (DR) – AWS-based backup and failover mechanisms.

## Physical & Logical Topology :

### Physical Topology :

**Core Layer :-**

Cisco catalyst 2911 ( Redundant pair )
Cisco ASA 5506_X Firewall

**Distribution Layer :-**

Cisco catalyst 3850 ( Stack For redundancy )

**Access Layer:**

Cisco Catalyst 2960 (POE and VOIP )

**WAN Edge:**

Dual ISPs (Fiber + LTE backup)
Cisco ISR 4451 routers (IP SLA-based failover)

# Technical Requirements

## High Availability:

- Dual routers/switches at core/distribution layers
- HSRP/VRRP configuration
- Dual WAN with IP SLA tracking

### Scalability:

- Modular switch stacking
- VLAN trunking with 802.1Q
- AWS VPC-ready design

### Security (ISO/IEC 27001):

- Firewall + Intrusion Detection/Prevention
- VPN encryption (AES 256-bit)
- RADIUS/TACACS+ AAA
- Port Security, Dynamic ARP Inspection, DHCP Snooping
- VLAN ACLs and role-based access control

### Monitoring & Management:

- Syslog, SNMP v3, NetFlow
- E-mail/SMS alerts on link failures or security events
- **Centralized dashboard (PRTG/SolarWinds suggested)**

# Conclusion

This architecture ensures secure, highly available, and scalable financial network operations while meeting strict compliance requirements. Future enhancements include SD-WAN, AI-based security, and multi-cloud expansion.