**Secure Network Design and Device Configuration**

**Project Scenario**

You have been hired as a **Network Security Architect by FinSecure Inc.**, a rapidly growing

**financial technology company** that handles **sensitive customer data** and supports **remote**

**workers**. The company is moving into a **new headquarters** and requires a **secure,**

**segmented, and redundant network topology design** that prioritizes the **availability**,

**confidentiality**, and **integrity** of its data.

As the **lead architect**, your task is to **design a detailed network topology** using **Cisco**

**Packet Tracer**. This project focuses on the **design and structure**, **not the full**

**implementation of services**. Your topology should incorporate foundational enterprise-grade

routing, switching, VLAN segmentation, and security measures aligned with best practices for

a fintech company.

**Project Objective**

Design a **realistic, secure, and scalable enterprise network topology** that supports different

departments, ensures secure data flow, implements VLANs, provides routing, and includes

basic network security and redundancy mechanisms.

This project emphasizes:

* Realistic enterprise network design

• Security-conscious architecture thinking

• Clear and professional documentation

**Project Requirements**

**1. Network Topology**

• At least **3 departments** (e.g., HR, IT, Finance), each in a **separate VLAN**

• A **Data Center** segment containing:

-Web Server

- DNS Server

- Mail Server

- File Server

• A **branch office** connected to HQ via a **WAN (Serial PPP) link**

• A **remote user** connecting securely via **VPN**

**2. Device Initial Configuration**

• Basic configuration of **switches and routers**, including:

-**Hostname**

- **Passwords (better with encryption)**

- **SSH access** setup for remote management

**3. VLAN and Switching**

• Minimum of:

- **3 user VLANs**

- **1 management VLAN**

- **1 native VLAN**

• Assign **ports to VLANs**

• Use **trunk links** between switches and routers

• Configure **EtherChannel** (where appropriate)

• Apply **VTP** for VLAN propagation

• Use **Spanning Tree Protocol (STP)** for loop prevention

• Enable **port-security** (e.g., sticky MAC, violation handling)

**4. Inter-VLAN Routing**

• Use either **Router-on-a-Stick** or **Multilayer Switch** configuration

• Route between VLANs.

• Ensure communication between departments as allowed.

**5. IP Addressing**

• Use **IPv4**

• Configure **DHCP**:

- Either from a router or a dedicated server

• Provide an **IP Addressing Table** with subnet, gateway, and range details

**6. Routing**

• Connect branch and HQ via **Serial WAN (PPP)**

• Use **EIGRP** for dynamic routing between all routers

• Implement a **default route** simulating internet access

**7. Security Configuration**

• Implement **Access Control Lists (ACLs)** to:

-Restrict access between departments

-Allow limited access to servers

- Block specific ports or applications

• Configure **Port Address Translation (PAT)** to simulate internet access

• Apply **SSH** for secure CLI access on routers/switches

**8. Server Design (Structural Placement Only)**

• Include the following servers in the topology (service config not required):

- Web Server (HTTP/HTTPS)

-DNS Server

- Mail Server

- File Server

- DHCP Server