**Secure Enterprise Networking Project #10**

**Design and Implementation of a Secure Company Network System for Cytonn Innovation Ltd**

**Project Overview**

Cytonn Innovation Ltd, a global leader in cloud-based solutions, is expanding into a new three-floor building to accommodate its growing workforce of **600 staff** across diverse departments. As a key member of the Networks Team, I was tasked with designing and implementing a **secure, scalable, and high-performance enterprise network** using **Cisco Packet Tracer**.

This project focuses on developing a **logical network architecture** that ensures **redundancy, availability, and robust security**, supporting both **current operational needs** and **future growth**.

**Project Objectives**

* Develop a **hierarchical, redundant network** for a multi-floor, multi-department building
* Ensure **high availability** using **dual ISPs**, HSRP, and LACP-based EtherChannel
* Secure internal resources through **segmented zones** (Inside, DMZ, and Outside) using **Cisco ASA 5500-X firewalls**
* Provide **centralized wireless access** through a **Wireless LAN Controller** and LAPs
* Integrate advanced services including **VoIP**, **DHCP**, **SSH**, **OSPF**, and **ACL-based access control**

**Key Network Design Elements**

**🔗 Infrastructure & Redundancy**

* **Two Cisco ASA Firewalls** for network security and failover
* **Two ISPs (SEACOM and Safaricom)** connected for internet redundancy
* **Core and Access Layer switching** using Catalyst 3850 and 2960 switches
* **EtherChannel (LACP)** used to bundle uplinks for fault tolerance and performance
* **HSRP** implemented for router redundancy and seamless failover

**📡 IP Addressing & VLANs**

* **Subnetting** applied to the following assigned IP ranges:
  + **192.168.10.0/24** for Management
  + **172.16.0.0/16** for LAN
  + **10.20.0.0/16** for WLAN
  + **172.30.0.0/16** for VoIP
  + **10.11.11.0/27** for DMZ
* VLANs created and mapped as:
  + VLAN 10: Management
  + VLAN 20: LAN
  + VLAN 50: WLAN
  + VLAN 70: VoIP
  + VLAN 199: Blackhole (unused ports)

**🔐 Security Measures**

* **Cisco ASA** configuration with security zones (Inside, DMZ, Outside)
* **Active Directory, DHCP, DNS, and RADIUS** servers placed in the Inside zone
* **FTP, Web, Email, App, and NAS servers** hosted in the DMZ
* **ACLs** configured to restrict SSH access only to the **Senior Network Security Engineer’s PC**
* **STP PortFast** and **BPDU Guard** implemented to prevent switching loops

**💬 Services and Features**

* **Inter-VLAN Routing** via multilayer switches (Core switches configured with IPs)
* **OSPF** as the dynamic routing protocol for optimal route advertisement
* **VoIP Gateway** configured with 4-digit dial plan
* **SSH access** securely enabled on all core network devices
* **DHCP servers** in the Server Room to dynamically assign IPs to all departments
* **Static IPs** assigned to Server Room infrastructure for stability

**Outcomes**

* A **fully secure and highly available network** infrastructure ready for production
* **Scalable** design to support future departmental expansion and cloud integration
* **Centralized wireless and voice services**, enabling mobility and modern communication
* **Segmented and controlled access**, reducing risk from internal/external threats
* Successful **connectivity, redundancy testing**, and validation of all configured services

This project demonstrates enterprise-level design and implementation skills, integrating modern networking concepts, security best practices, and real-world operational readiness.