1. Organizational Overview

Martin Luther King University supports around **30,000 users** with an expected doubling of users in each department by 2025. The institution is structured into four key faculties – Health and Sciences, Business, Engineering/Computing, and Art/Design – distributed across both campuses. The **IT Department**, based at the **main campus**, is responsible for managing and maintaining the entire network.

---

2. Network Design Principles

The network design follows the **Cisco three-layer hierarchical model** (Core, Distribution, Access) to ensure modularity, scalability, and redundancy. The implementation was carried out using **Cisco Packet Tracer**, and it integrates several critical components and best practices, including:

- **Redundant Switching and Routing** using multilayer switches and **EtherChannel (LACP)**.
- **STP enhancements** with **PortFast** and **BPDUguard** for faster convergence and loop prevention.
- **Inter-VLAN Routing** and **subnetting** to enable department-wide communication.
- **OSPF** as the dynamic routing protocol across the network infrastructure.
- **HSRP** for gateway redundancy.
- **Voice over IP (VoIP)** deployment using IP phones in all departments.
- **Wireless Access Points** managed by **Wireless LAN Controllers (WLC)**.
- **DHCP, DNS, FTP, WEB, SMTP, and Email servers** hosted in a secure **DMZ**.
- **Access Control** through VLAN segmentation (IDs 10 - Management, 20 - LAN, 50 - WLAN, 199 - Blackhole).
- **Secure static IP assignments** for server farm devices.
- **Cisco ASA 5500-X Firewalls** with defined security zones and policies for traffic control.
- **IPsec Site-to-Site VPN** for encrypted communication between the campuses.
- **ACLs** to restrict remote access to management interfaces (SSH allowed only from the Senior Engineer's PC).
- **Cloud Connectivity** to Google Cloud for scalable service delivery.

---

3. IP Addressing Scheme

- **Main Campus LAN**: 10.10.0.0/16
- **Branch Campus LAN**: 10.11.0.0/16
- **Main Campus Voice**: 172.16.0.0/16
- **Branch Campus Voice**: 172.17.0.0/16

- **WLAN Management**: 192.168.10.0/24
- **DMZ (Main Campus)**: 10.20.20.0/27
- **Public IPs**: Main: 105.100.50.0/30, Branch: 205.200.100.0/30

---

4. Security & Redundancy

The architecture employs **Cisco ASA Firewalls** at both campuses with **zone-based policies** to filter traffic. A **site-to-site IPsec VPN** ensures that data between campuses remains encrypted and protected from eavesdropping. Each firewall also connects to its respective **Airtel ISP** connection for internet access. **DHCP redundancy** is achieved via dual DHCP servers on virtual machines hosted on physical servers using a hypervisor.

---

5. Implementation & Testing

The network topology was thoroughly implemented and validated in **Cisco Packet Tracer**. Extensive testing confirmed that all services function as intended, including:

- Reliable **inter-campus communication** via VPN.
- Seamless **internet access**.
- **Dynamic IP addressing** for end-user devices.
- Secure and effective **remote management via SSH**.
- **Voice and data traffic** separation through VLANs.
- Scalable **wireless connectivity**.

---

6. Conclusion

This project demonstrates the development of a **robust, secure, and scalable enterprise network** tailored to the needs of a large academic institution. The implementation not only meets current requirements but also positions the university for future expansion and technological innovation.