COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCES

Networking Project: Development Bank of Ethiopia

Group Members:

1. Abimael Getachew ……..UGR/0275/15
2. Elias Wakgari…….. ……UGR/5344/15
3. Hamza Harun…….UGR/0688/15
4. Kidus Shimelis……UGR/0110/15
5. Nathanael Dereje…….UGR/1540/15
6. Melat Mamushet……UGR/3703/15

Supervised by: Dr. Workshet Lamenew
Submission Date: Thursday, April 10, 2025 G.C

1. Identify Needs and Requirements

Organization Overview:

Development Bank of Ethiopia (DBE) is a specialized financial institution established to support Ethiopia's national development agenda. It offers development finance and technical assistance to viable projects in priority sectors.

Vision:

To be a world-class development bank that helps achieve Ethiopia's economic transformation by 2030.

Mission:

To promote national development by financing priority sectors through mobilizing funds from domestic and foreign sources, with a focus on sustainability and capacity building.

Goals:

- Finance key sectors: agriculture, manufacturing, energy, and infrastructure.

- Enhance financial inclusion, especially for SMEs and agro-industries.
- Strengthen stakeholder partnerships.
- Improve efficiency via digital transformation.

2. User Base and Functional Needs

Departments:

- Human Resources (HR)
- Finance
- IT
- Customer Service
- Management

Also they said there are 52 departements.

User Access:

- The network primarily serves internal users only. There is no access provided to external users or the general public.
- A core banking system is in place and is accessible exclusively by higher-level management and authorized IT personnel for security and control purposes.

User Devices: Desktop computers, Laptops, IP Phones, Printers

Purpose:

- HR: Payroll, attendance management
- Finance: Financial transactions, reporting
- IT: System and network administration
- Management: Strategic planning, reporting tools

3. Existing Network

We are going to study the existing network and re-implement it. If there are any issues or areas that need improvement, we will address them accordingly to ensure a more robust and efficient infrastructure.

4. Physical Layout

The main office is located in Kasanchis. Each department is allocated to different floors. A site survey was conducted to assess cable paths, device locations, and access point placements.

5. Data Center and Access Points

The data center is located on the ground floor. It includes:

- Access control: fingerprint, facial recognition, password, card access
- Raised floor for cabling
- Dual power supplies (A & B) for redundancy
- Fire-resistant wall panels
- Cooling systems and UPS

Access points (APs) are installed throughout all floors to ensure full wireless coverage.

6. Distribution and Core Channels

The network is designed using a collapsed core architecture, which combines the core and distribution layers into a single, high-performance Layer 3 switch. Additionally, an access layer is implemented on each floor to connect end-user devices such as computers, printers, and access points.

- Collapsed Core Layer: A centralized Layer 3 switch that integrates both core and distribution functionalities, handling routing, inter-VLAN communication, and high-performance switching across the organization.
- Access Layer: Consists of edge switches on each floor, connecting to departmental devices and uplinking to the core switch.

Redundancy:

- Dual uplinks from each access layer switch to the core switch to ensure high availability and failover capabilities.

Load Balancing:

- Managed via dynamic routing protocols and link aggregation techniques to evenly distribute traffic and avoid bottlenecks.
- Managed via dynamic routing protocols to evenly distribute traffic.

7. DMZ Components

The DMZ (Demilitarized Zone) is a critical segment of the network designed to host services that must be accessible from outside the internal network while maintaining strong security boundaries.

The DMZ hosts the following services:

- Public Web Server: Provides access to the bank's official website and online services for general users and stakeholders.
- Email Server: Manages external and internal email communications while protecting internal systems from direct exposure.
- VPN Gateway: Facilitates secure remote access for authorized staff, especially for accessing sensitive systems while working off-site.

These services are isolated from the core internal network and are protected using dedicated firewall rules and intrusion detection systems to mitigate external threats.

8. External Connections

- Internet connection via EthioTelecom fiber link
- Extranet connection to branch offices using secure VPN tunnels

9. Security Components

- Next-gen firewalls
- Intrusion Detection and Prevention Systems (IDPS)
- VPN for secure remote access
- Role-based access control (RBAC)
- Physical security for the data center

10. Quality of Service (QoS)

QoS ensures prioritization of critical services:
- VoIP traffic (e.g., IP phones)
- ERP and financial system data
- Management portal traffic

Implemented using traffic shaping and priority queuing on switches.

11. Server Application and Server Farm Layout

Applications:
- ERP System
- Oracle Database
- Email and Backup Services

Networking: Primarily Cisco devices for core and edge networking, with some Huawei equipment integrated for specific functions and redundancy.

Server Farm:
- Redundant power and network connections
- Centralized under the data center with controlled access.