Rift Valley University (RVU) Network Design & Modernization Proposal

Campus: Addis Ababa (Enkulal fabrica)

Phase 1: Needs and Requirements Analysis

Understanding the Organization

· Institution: Rift Valley University (RVU)

· Type: Private, for-profit higher education institution.

· Campus in Focus: Addis Ababa, (Enkulal fabrica) .

· Mission: To provide quality, relevant, and cost-effective education that meets the demands of the national and international labor market.

· Key Drivers: Operational efficiency, student satisfaction, and cost control. The network is a critical tool for delivering educational content and managing administrative operations.

User Base and Functional Requirements

The network must support a dynamic environment focused on teaching, learning, and streamlined administration.

- Students:

· Functions: Accessing Learning Management Systems (e.g., Moodle, Canvas), online research, video lectures, and collaborative projects.

· Requirements: High-density Wi-Fi in lecture halls, libraries, and common areas. Bandwidth management is critical to prevent congestion during peak hours (between classes). A "Bring Your Own Device" (BYOD) friendly environment.

- Faculty & Instructors:

· Functions: Delivering lectures, online assessments, grade management, and communication with students.

· Requirements: Reliable and secure wired and wireless connectivity. Priority access for video conferencing and uploading course materials.

- Administration (Registrar, Finance, HR):

· Functions: Student registration, fee collection, payroll, and record keeping using centralized administrative software.

· Requirements: A highly secure and highly available network segment for sensitive financial and student data. Strict access controls and reliable uptime are non-negotiable.

- Guests & Prospective Students:

· Functions: Internet access during visits, open days, and seminars.

· Requirements: An easy-to-access captive portal that provides internet access while strongly isolating guest traffic from the internal academic and administrative network. This network also serves as a marketing tool.

Existing Network & Physical Layout

· Building Overview: The campus occupies a multi-story building.

· Current State: The network is poorly segmented network, leading to congestion and security vulnerabilities. Reliance on a single ISP may cause frequent outages during online exams or registration periods.

· Key Locations:

· Main Server Room: Houses the main router, core switch, and servers.

· Lecture Halls: High-density areas requiring multiple, powerful Access Points.

· Computer Labs: Wired connections for desktop computers used for practical exams and software training.

· Administrative Wing: Secure, wired connections for administrative staff.

Phase 2: Network Architecture

- User Devices

The network must support a wide array of devices brought by students, faculty, and staff, as well as university-owned equipment.

- ✓ Student-Owned Devices (BYOD - Bring Your Own Device):

· Laptops: Primary device for coursework, research, and assignments.

· Smartphones: For communication, quick checks of the LMS, and email.

· Tablets: For reading digital textbooks and viewing lecture materials.

- ✓ University-Owned Devices:

· Faculty/Staff Laptops: Issued to instructors and administrators for university business.

· Desktop Computers: Located in administrative offices (Finance, Registrar) and computer labs for specialized software.

· Computer Lab Thin Clients: In some labs, to access a centralized virtual desktop infrastructure (VDI).

· VoIP Phones: On every desk for internal and external communication.

· Printers/Scanners: Networked multifunction devices in libraries, labs, and administrative wings.

- Applications and Servers

The core software and services that run the university's academic and administrative operations.

- Academic Servers:

· Learning Management System (LMS) Server: Hosts the platform (e.g., Moodle) for all online courses, assignments, and grades. (Critical Priority)

· E-Library & Digital Repository Server: Provides access to online journals, e-books, and past research papers.

- Administrative Servers:

· Student Information System (SIS) Server: Manages student records, registration, and transcripts. (High Security Priority)

· Finance & Payroll Server: Runs the software for fee collection, budgets, and salary processing. (High Security Priority)

· File Server: Central storage for departmental shared folders and user home directories.

- Infrastructure Servers:

· Domain Controller & Active Directory Server: Manages user authentication, permissions, and policies across the network.

· Email Server: Hosts internal email (e.g., Microsoft Exchange).

· Web Server: Hosts the university's public-facing website.

· Backup Server: Dedicated server for nightly backups of all critical data.

- Access Devices

The networking hardware that connects users and their devices to the network resources.

· Router/Firewall: A Unified Threat Management (UTM) Firewall will serve as the gateway. It will provide:

· Routing between VLANs and to the internet.

· Firewall security policies and Access Control Lists (ACLs).

· Intrusion Prevention System (IPS).

· Web Content Filtering.

· VPN for remote faculty/administrators.

· Core Switch: A Layer 3 Switch located in the main server room. Its primary functions are:

· High-speed switching backbone for the entire campus.

· Inter-VLAN routing (to efficiently handle traffic between the different segments).

· Access Switches: Managed Layer 2 Switches with Power over Ethernet (PoE+) deployed in wiring closets on each floor. They will:

· Provide wired network connections to desktop PCs, VoIP phones, and printers.

· Supply power to Wireless Access Points and VoIP phones via Ethernet cables.

· Be configured with VLAN information and Port Security to prevent unauthorized device access.

· Wireless Access Points (APs): Enterprise-grade, Wi-Fi 6 APs mounted in ceilings across lecture halls, libraries, and offices. They will broadcast multiple SSIDs (e.g., "RVU-Staff", "RVU-Students", "RVU-Guest"), each mapped to its respective VLAN.

Logical Network Design (VLANs) & IP Addressing Scheme

A segmented network is crucial for security, performance, and management in a private college environment.

VLAN ID Department / Function Subnet Description

VLAN 10 IT Management 10.10.10.0/24 Switches, APs, Server Management

VLAN 20 Administration 10.10.20.0/24 Registrar, Finance, HR (Highly Secure)

VLAN 30 Faculty & Staff 10.10.30.0/24 Instructors and general staff

VLAN 40 Student Wi-Fi 10.10.40.0/23 Primary network for student devices

VLAN 50 Computer Labs 10.10.50.0/24 Wired labs for specific software access

VLAN 60 Guest Wi-Fi 10.10.60.0/24 Isolated internet-only access

VLAN 70 VoIP/IPT 10.10.70.0/24 Voice over IP phones for internal communication

- Device Selection

· Firewall/Router: A Unified Threat Management (UTM) firewall. This cost-effective solution combines routing, firewall, VPN, intrusion prevention, and web filtering in one device, perfect for a budget-conscious private college.

· Core Switch: A robust Layer 3 switch to handle inter-VLAN routing within the campus and provide a high-speed backbone.

· Access Switches: Managed PoE+ switches to provide power and data to Wireless Access Points and VoIP phones across the campus.

· Access Points: High-density, enterprise-grade Wi-Fi 6 Access Points to handle the concentration of users in lecture halls.

· Wireless Controller: A central software or hardware-based controller to manage all APs for seamless roaming and easy configuration.

Security & Business Policies

· Role-Based Access Control (RBAC): Users authenticate to the network, and their access level (Student, Faculty, and Admin) determines which VLAN they are placed into.

· Web Filtering & Content Control: The UTM firewall will be configured to block access to malicious and non-productive websites (e.g., social media, streaming) on the Student and Lab VLANs during class hours.

· Bandwidth Management (QoS):

  · High Priority: VoIP traffic, LMS platform.

  · Medium Priority: Faculty and Admin traffic.

  · Standard Priority: General student internet access.

· Guest Network: A captive portal will display the university's branding and require simple registration. The connection will be throttled and fully isolated from internal networks.

Implementation Plan

· Staging & ISP Upgrade: Procure and pre-configure equipment. Establish a contract with a second ISP (e.g., Ethio Telecom and Safaricom) for redundant internet links.

· Phased Installation: Install new switches and APs floor-by-floor during evenings or weekends to avoid disrupting classes.

· Migration & User Onboarding: Migrate administrative systems first, then faculty, and finally student networks. Set up a process for students and staff to register their devices for the new secure Wi-Fi.

· Testing: Conduct stress tests in lecture halls, verify administrative software functionality, and test failover to the backup ISP.