RESEARCH ON NETWORK AND SYSTEM ADMINISTRATION PRACTICES AT THE NATIONAL BANK OF RWANDA (BNR)

Course: Computer Networks

Student Name: Joseph MUTANGANA

Student ID: 29061

Lecturer: Ins. Joshua IRADUKUNDA

Date: 25/10/2025

Report title: Final Project Phase 1

COMPUTER NETWORKS

FINAL PROJECT PHASE 1

Table of Contents

Foreword

“Network and system administration are the key foundation in Information Technology. Having a strong background in them would improve knowledge and skills on modern infrastructure.”

BIZIMANA Lambert
IT Officer / System Administrator
National Bank of Rwanda

Abstract

This report presents research conducted to understand real-world practices in network and system administration. The study focused on the National Bank of Rwanda, where a system administrator provided detailed insights through a structured Google Form interview. Key areas explored include infrastructure setup, system maintenance, policy enforcement, compliance with standards, and future technological recommendations. The results bridge theoretical learning with professional IT operations, helping strengthen understanding in network and system management.

Introduction

The world today is heavily dependent on information technology, and every organization—whether a bank, university, or government institution—relies on stable and secure systems to carry out its daily operations. Behind this reliability stand **system and network administrators**, whose work ensures that technology services run smoothly, securely, and efficiently.

I titled this project *"Research on Network and System Administration Practices at the National Bank of Rwanda (BNR),"* because was conducted as part of the **CNET/SYS ADMIN Final Project Phase 1** for the **Computer Networks** course. The main purpose of this study is to bridge the gap between **academic knowledge** and **real-world professional practice** in system and network administration. Through this research, I aimed to understand how professional organizations design, configure, maintain, and secure their IT infrastructure.

The project focuses on the core responsibilities of system administrators, such as:

- Setting up and maintaining network and system infrastructures.
- Implementing policies for access control, password management, and data protection.
- Ensuring system performance, scalability, and reliability.
- Managing backups, change control, and disaster recovery.
- Maintaining compliance with national and international security standards such **as** ISO 27001 and GDPR.

The National Bank of Rwanda **(BNR)** was selected for this case study due to its reputation as one of the most technologically advanced and well-regulated financial institutions in the country. The bank's IT infrastructure requires high availability and strict data security measures, making it a perfect example for studying real-world system administration practices.

The study also seeks to understand how system administrators balance technical operations with administrative responsibilities—such as user management, policy enforcement, and incident response—and how they prepare for system scalability and future improvements.

Furthermore, the project aims to expose my self to professional communication and ethics involved in engaging with IT specialists, including how to request participation, maintain confidentiality, and analyze responses responsibly.

By the end of this study, I expect to have:

1. Gained practical insights into the management of enterprise networks and systems.
2. Compared theoretical classroom learning with field observations.
3. Understood the challenges faced by system administrators in ensuring system performance and compliance.
4. Built a foundation for future professional growth in the area of network and system administration.

In short, this introduction establishes the importance of system administration in maintaining reliable IT operations, outlines the project's purpose and scope, and emphasizes how real-world engagement with professionals enhances the student's technical and professional understanding.

Methodology

Research Approach

The research used a **qualitative method** based on an interview-style Google Form survey. The form included both multiple-choice and open-ended questions designed to gather detailed information about infrastructure setup, system policies, maintenance, and compliance.

Data Collection Process

At first, I tried to reach system administrators in several organizations through calls, text messages, and in-person visits.
After multiple attempts, the I personally visited the **National Bank of Rwanda (BNR)** and explained the project purpose at the reception.
An IT Support officer named **Ariane** assisted by forwarding the request to a System Administrator. Later, **Mr. BIZIMANA Lambert** accepted to fill out the survey form.

Ethical Considerations

The participant was informed that the study is purely academic and no confidential data would be collected.
BNR employees do not use official company emails for non-business communication, which is why the confirmation email was not sent.
However, the form response itself serves as a verified professional input.

Daily Operations

Mr. Bizimana indicated that his daily responsibilities include monitoring network health, troubleshooting connectivity issues, managing user accounts, backing up data, updating system software, and performing security audits. Each of these activities plays a vital role in keeping the organization's network stable and secure.

- Monitoring Network Health: This involves checking the condition of the network regularly using specialized tools that track performance and availability. At BNR, monitoring helps identify issues before they affect operations. System administrators typically rely on dashboards or SNMP-based tools to detect failures or unusual activity. Keeping track of this ensures that banking services remain online and reliable for customers.

- Troubleshooting Connectivity Issues: When users experience problems connecting to internal systems or the internet, the system administrator diagnoses and resolves them quickly. This may include checking cables, switches, or firewalls. Timely troubleshooting reduces downtime and maintains productivity across departments.

- Managing User Accounts: The administrator ensures that all employees have the right access based on their roles. Accounts are regularly reviewed and adjusted when staff join or leave the organization. This prevents unauthorized access and ensures accountability in system usage.

- Backing Up Data: Mr. Bizimana confirmed that backups are performed daily. This frequency is common in financial institutions because losing data could result in huge operational risks. Daily backups guarantee that the system can be restored quickly if something goes wrong.

- Updating System Software: Keeping systems up-to-date prevents security vulnerabilities and improves performance. Updates are scheduled to minimize interruptions and maintain compliance with IT policies.

- Security Auditing: Regular checks are done to ensure compliance with security standards. Audits help identify risks, verify patch levels, and maintain trust in the IT infrastructure.

Infrastructure Setup and Implementation

In the section about infrastructure setup, Lambert highlighted that security, cost, reliability, and performance are the main priorities when establishing new systems. Below is a detailed breakdown of how these elements are managed.

- Security: Security is always the top priority at BNR. Every network device, from routers to servers, must be configured with strong access controls and firewalls. The organization implements NAT for separating internal and external traffic, and VPNs for remote users. This ensures only authorized users can connect securely.

- Cost and Reliability: The system administrators balance cost with long-term reliability. Even though banking systems require high reliability, they must also remain cost-effective. Redundant links (active/standby) are used so that if one connection fails, another takes over seamlessly.

- Performance and Scalability: To keep services fast and responsive, BNR uses VLAN segmentation, switches, and firewalls optimized for large data flows. Scalability means that as the organization grows, more devices and users can be added without redesigning the whole network.

- Tools and Configuration Methods: Lambert mentioned tools such as firewalls, servers, and network switches as essential components for setup. Each configuration is tested and documented to maintain uniformity and quick recovery in case of a failure.

Policy Formulation and Enforcement

Policy implementation ensures that IT operations are consistent, secure, and compliant. Lambert provided insights into password policies, access control, and data backup strategies.

• Password Policies: The organization enforces strong password requirements including minimum length, character complexity, expiration periods, and history restrictions. Multi-factor authentication (MFA) adds an extra layer of protection for system logins. These practices prevent unauthorized access even if passwords are compromised.

• Access Control: Access is managed through Role-Based Access Control (RBAC). This means each user only has access to the resources required for their role. RBAC simplifies user management and prevents data leaks caused by excessive permissions.

• Network Segmentation: The bank uses separate VLANs and firewall rules to isolate employee networks from guest networks. This minimizes the risk of internal attacks and improves overall network security.

• Data Backup Policy: Backups are done daily using on-site storage. The policy ensures that data is regularly tested and verified for recovery. Critical financial systems must always have an up-to-date backup.

• System Administration Duties: Administrators are responsible for ensuring group policies are enforced across both on-premise Active Directory and Microsoft 365 environments. This hybrid setup allows centralized user management and consistent security enforcement.

Compliance and Regulatory Considerations

Compliance plays a major role in a financial institution like BNR. Lambert mentioned that the bank follows standards like ISO 27001, GDPR, and national IT standards.

• Remote Access: Employees connect securely through VPNs when working remotely. This ensures encrypted communication and protects the internal network from outside threats.

• Security Audits: The organization performs quarterly audits to check system security and ensure compliance. Regular reviews help identify vulnerabilities and strengthen defenses before incidents occur.

• System Security Level: Lambert rated the system security as strong, emphasizing proactive monitoring, strict access control, and timely updates as key contributors to this strength.

• Standards Compliance: ISO 27001 and GDPR guidelines shape how policies are created and enforced. Compliance helps the organization maintain integrity, protect customer data, and meet international expectations.

This combination of technical and administrative measures ensures that BNR remains compliant and secure — especially crucial in a financial institution.

Future and Recommendations

When asked about future improvements, Lambert recommended adopting more cloud technologies and AI-driven IT operations (AIOps). He believes that cloud integration could enhance flexibility and simplify management, while AIops can improve performance monitoring and automate troubleshooting.

His foreword emphasized that network and system administration form the foundation of modern IT. Having strong skills in these areas allows professionals to build and maintain reliable infrastructures that support digital transformation.

Conclusion

This project provided valuable insights into how professional organizations like the National Bank of Rwanda manage their IT environments. From daily monitoring to policy enforcement and compliance with global standards, every step demonstrates how theory connects with real practice. The interview also showed how proactive management, structured policies, and regular backups ensure

References

- ISO/IEC 27001 Information Security Standard
- NIST Cybersecurity Framework
- Microsoft 365 Hybrid AD Integration Guide