RESEARCH ON NETWORK AND SYSTEM ADMINISTRATION PRACTICES

Course: Computer Networks

Student Name: Joseph MUTANGANA

Student ID: 29061

Lecturer: Ins. Joshua IRADUKUNDA

Date: Nov 9, 2025

Report title: Final Project Phase 1

Table of Contents

Foreword

Technology is an important part of every modern organization, and strong network and system administration helps businesses run smoothly and safely. In this project, I wanted to learn how real IT professionals manage computer systems, secure networks, and support daily operations. To do that, I met with a Senior System and Network Administrator and collected information about their daily tasks, tools, and security practices. This research helped me understand how the skills we learn in class are used in real workplaces, and it also prepared me better for future work in the IT field.

Abstract

This project studies how network and system administration is done in a real organization. The research was based on a survey filled out by a Senior System and Network Administrator. The survey questions were created following the instructor's guidelines. The results show that the administrator focuses on important tasks like checking system performance, monitoring security logs, managing user accounts, and making sure backups work. The company also uses strong security practices, including role-based access control, Multi-Factor Authentication (MFA), network segmentation, and regular system updates. They follow standards such as ISO and NIST to protect data and keep systems safe. This study shows how theoretical knowledge from class connects to real-world IT work and demonstrates the importance of security, monitoring, and planning in system administration.

Introduction

Information and communication technology infrastructures have become the backbone of modern enterprises, particularly in organizations operating in mission-critical sectors. Ensuring continuous service availability, maintaining secure systems, and supporting scalable growth requires robust network and system administration practices. This research investigates real-world system and network administration operations, focusing on how professional practices align with academic and industry-standard principles.

The primary objective of this study is to explore operational activities, infrastructure design decisions, policy enforcement mechanisms, and compliance frameworks utilized by enterprise-level system and network administrators. Special emphasis is placed on hybrid Active Directory environments, monitoring systems, cybersecurity controls, automation, and adherence to regulatory standards such as ISO 27001 and NIST Cybersecurity Framework. By analyzing these elements, the study aims to bridge classroom theoretical learning with practical implementation in the field.

The scope of the project includes daily operational processes such as monitoring CPU utilization, log review, backup verification, and user support handling; infrastructure architecture considerations including scalability, high availability, NAT configuration, and hybrid identity management; policy enforcement areas such as password standards, MFA, role-based access control, and network segmentation; and governance-compliance practices like cybersecurity audits, documentation, and regulatory adherence.

To gather authentic and practical insights, I physically visited the organization and conducted a structured professional interview with a Senior System and Network Administrator. Ethical considerations were strictly respected, and confidentiality was ensured by anonymizing personal identifiers. This direct field-interaction method ensures that the findings reflect real operational environments rather than hypothetical scenarios.

Ultimately, this research does not only highlight the administrator's technical responsibilities, but also demonstrates the strategic nature of system administration work

handling security threats, ensuring uninterrupted connectivity, implementing policy frameworks, and planning for future system expansion. Through this study, the knowledge acquired from academic coursework is contextualized in a real-world setting, offering meaningful insight into enterprise-level IT administration practices and preparing I for future professional engagements in the field of network and system management.

Methodology

This research followed a qualitative approach and collected data directly from an industry professional through a structured interview-survey format. The survey questions were not created arbitrarily; instead, they were developed based on the official example and guidelines provided by the course instructor for this project. The form ensured that the questions aligned with academic expectations and covered critical areas of network and system administration such as infrastructure configuration, security policy implementation, daily operational responsibilities, and compliance standards.

To engage a suitable respondent, I physically visited a telecommunication infrastructure company located in Kigali. During the visit, I introduced the academic purpose of the study and briefly discussed the scope of the questions with a Senior System & Network Administrator. After a short conversation, the administrator agreed to participate and requested the survey to be shared digitally for convenience.

I then sent the survey form electronically, allowing the respondent to provide detailed answers without time pressure. This method ensured accuracy in responses and allowed the professional to reference real-world practices effectively. The form response served as the primary data source for this report.

Ethical considerations were fully respected. Participation was voluntary, and the respondent was informed that all information would be used strictly for academic purposes. No confidential network configurations, sensitive operational data, or personally identifying details were requested or disclosed. For privacy protection, names and direct organizational identifiers have been removed in the final report narrative.

The combination of instructor-structured questions, field engagement with an IT professional, and digital form submission provided both academic structure and real-world relevance, ensuring credible and meaningful insights for this research.

Findings

Daily Operational Practices

Monitoring Network and System Health

The interviewee explained that their role requires continuous monitoring of the organization's IT infrastructure. Monitoring network and system health ensures that systems remain stable and capable of delivering services without interruption. This includes observing bandwidth usage, tracking latency, and analyzing system response times to detect anomalies early.

Constant health checks help identify performance degradation before it impacts business services. If a server or link shows irregular behavior, the administrator can take preventive action to avoid outages.

These monitoring efforts are particularly important in their rganizational environments where uptime is critical. Large enterprise clients depend on uninterrupted service, making real-time visibility into system health essential.

By implementing proactive monitoring, the administrator reduces the likelihood of service disruptions and maintains customer trust.

Verification of Backups

The interviewee stressed the importance of backup verification to ensure data protection. Backup systems generate daily snapshots of critical operational data, but verification confirms the backup integrity and success.

Backup verification checks whether files are complete, readable, and recoverable. This is crucial for disaster recovery and business continuity.

In large organizations where massive volumes of data are processed, a failed backup could result in significant financial and operational loss.

Through routine backup verification, the administrator ensures the organization can recover swiftly in case of data loss, corruption, or cyberattacks.

Device Availability Checks

Ensuring that all critical networking and server devices are online is a core daily task. The administrator reviews device dashboards to confirm availability of switches, routers, firewalls, wireless controllers, and servers.

This facilitates early detection of device failures or power issues, reducing the risk of downtime.

Maintaining device availability through proactive tracking guarantees high service reliability and operational resilience.

Monitoring Security Logs

The interviewee noted that security logs are reviewed daily to identify potential threats and unauthorized behaviors. Logs contain information about login attempts, system alerts, firewall events, and unusual traffic patterns.

Proactive log review allows the administrator to spot brute-force login attempts, suspicious IP addresses, or malware activity.

In modern cybersecurity environments, logs play a crucial role in incident response and forensic investigation.

Timely detection and action based on logs helps protect sensitive data and infrastructure assets.

Handling Support Tickets

The administrator handles user support tickets raised by employees or system operators. These tickets often involve account issues, connectivity problems, or system access requests.

Responding efficiently enhances employee productivity and ensures smooth business operations.

Support ticket systems often integrate priority ranking, enabling the administrator to prioritize critical service issues.

This structured approach to issue handling ensures that technical problems are resolved quickly and efficiently.

Infrastructure Setup and Implementation

Security and Scalability

The interviewee highlighted that security and scalability are top priorities in infrastructure design. Secure systems protect business assets from attacks, while scalability ensures the infrastructure can grow with organizational needs.

Layered security mechanisms, including firewalls, access control, and encryption, form the foundation of infrastructure defenses.

Scalability planning includes modular equipment selection, cloud-readiness, and capacity assessments to handle future growth.

These considerations align with best practices in enterprise IT architecture.

Hybrid Integration (Azure AD Connect)

The organization integrates on-premises Active Directory with Microsoft 365 using Azure AD Connect. This creates a hybrid identity environment allowing seamless login and authentication across cloud and internal services.

Hybrid setups enhance flexibility by combining local security control with cloud scalability.

Azure AD Connect also synchronizes user accounts, reducing administrative overhead and improving consistency.

This approach enables smooth access management across modern distributed enterprise platforms.

Staging and Testing

New systems are deployed only after staging and User Acceptance Testing (UAT). This ensures no production environment disruptions.

Staging environments replicate the real network to test compatibility, performance, and security.

Security assessments check for vulnerabilities before deployment, ensuring compliance with internal and regulatory standards.

This structured testing process reduces rollout risk and improves service reliability.

Policy Formulation & Enforcement

Password & MFA Enforcement

The interviewee reported that strong password rules are enforced, including complexity, expiration, and Multi-Factor Authentication (MFA).

MFA adds a second verification method to secure accounts, significantly reducing cyberattack success rates.

Password expiration policies force periodic renewal to minimize credential theft risks.

Secure credential storage and policy enforcement ensure only authorized access to systems.

Role-Based Access Control

The organization follows Role-Based Access Control (RBAC), meaning users receive access based strictly on job responsibilities.

This prevents unauthorized access and limits internal threats by restricting access privileges.

Activity auditing tracks actions taken by users, strengthening accountability and compliance.

RBAC supports structured and efficient system management across large enterprises.

Network Segmentation & 802.1X

Network segmentation isolates user groups into separate VLANs, enhancing security by limiting attack spread.

802.1X authentication validates devices before granting network access, reducing unauthorized device risks.

Guest network isolation protects internal systems from external or unmanaged devices.

These network controls help maintain a secure and resilient infrastructure.

Compliance & Future Considerations

Compliance with Standards

The interviewee stated the organization follows ISO 27001, NIST, GDPR, and their organizational regulations. These frameworks guide security policies and data handling.

ISO 27001 ensures systematic security controls, while NIST provides cyber defense guidelines.

GDPR enforces data protection laws, particularly relevant for personal data processing.

Their organizational standards ensure regulatory compliance, protecting critical communication networks.

Discussion

The findings from the interview demonstrate significant alignment between academic theory in network/system administration and practical implementation within their organization environment. Many of the practices observed such as proactive network monitoring, hybrid Active Directory integration, VLAN segmentation, and layered security controls reflect core concepts taught in computer networks, operating systems, and cybersecurity coursework.

A key point of convergence is proactive monitoring and performance management. In theory, monitoring tools form the basis of preventive maintenance and service assurance. In practice, the interviewee utilizes industry-standard platforms such as Zabbix, PRTG, and Wireshark to identify performance trends, detect anomalies, and respond to issues before they escalate. This demonstrates the real-world importance of continuous visibility in mission-critical networks.

Infrastructure design decisions also strongly align with enterprise best practices. Concepts such as high availability, NAT configuration, hybrid cloud readiness, and modular scalability were discussed in class and observed in practical application within the organization. The use of Azure AD Connect to synchronize identities across on-prem and cloud environments reflects modern digital transformation strategies and confirms theoretical lessons on hybrid architectures and identity federation.

Policy implementation further validates academic discussions on cybersecurity and governance. The organization enforces strict password complexity, MFA, automated account management, and RBAC mirroring NIST, ISO 27001, and zero-trust security principles. Coursework emphasizes least-privilege access, network segmentation, and regular auditing, which were clearly applied in practice. While theory often treats policies

as documentation processes, real-world practice highlights their importance in operational resilience and compliance.

However, there are slight gaps where real-world environments extend beyond classroom theory. For example, structured change management workflows, disaster recovery drills, and SIEM-based security monitoring are advanced operational topics not deeply covered in introductory network studies but are crucial in enterprise environments. Similarly, predictive analytics, automation, and AI-driven network defense represent emerging industry trends that extend future learning opportunities beyond academic foundations.

In conclusion, the interview findings show strong consistency with theoretical principles while also revealing advanced enterprise practices essential in modern infrastructure environments. This reinforces the value of bridging academic knowledge with field-based experience to fully understand the complexity and responsibility required in professional system and network administration roles.

Conclusion

This research helped me understand how network and system administration is done in a real professional environment. By learning from a Senior System and Network Administrator at a telecom company, I discovered how important tasks like monitoring systems, checking backups, managing user accounts, and reviewing security logs are for keeping systems safe and running well.

The interview showed that real businesses use strong security practices like role-based access, Multi-Factor Authentication (MFA), network segmentation, and regular system updates. They also follow global standards such as ISO and NIST to keep their systems safe and meet legal requirements.

Overall, this study connected what I learned in class with real-world experience. It showed me that system administration is not only about knowing technology, but also about planning ahead, keeping security in mind, and responding quickly to problems. This research has improved my understanding of the skills needed in IT and motivated me to keep learning and practicing in this field.

Recommendations

Based on the findings from this study, the following recommendations are suggested:

1. **Continue improving automation tools**
   Automating system updates, monitoring, and reporting can save time and reduce human errors.
2. **Expand monitoring and security systems**
   Using more tools like SIEM (Security Information and Event Management) can help detect attacks faster.
3. **Increase employee cybersecurity awareness**
   Regular training for staff can help prevent issues like phishing or weak passwords.
4. **Enhance backup and disaster recovery tests**
   Practicing recovery more often ensures systems can be restored quickly during emergencies.
5. **Keep learning new technologies**
   IT environments change fast, so administrators should continue improving skills, especially in cloud computing, security, and automation.

References

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

Appendices