METHODIST UNIVERSITY GHANA

FACULTY OF SCIENCES

DEPARTMENT OF I.T AND MATHEMATICAL SCIENCES

OPTIMIZING NETWORK INFRASTRUCTURE (WITH ITS INHERENT) SECURITY: ANALYZING AND IMPLEMENTING A HIERARCHICAL NETWORK ARCHITECTURE FOR MUG (METHODIST UNIVERSITY GHANA)

BY

TETTEY MICHAEL NII AYI

OFORI DANIEL PERRY JNR

IGWEBUIKE SOLOMON JNR

ESHUN DARLINGTON EBENEZER

A PROJECT WORK SUBMITTED TO THE FACULTY OF INFORMATICS AND MATHEMATICAL SCIENCES, METHODIST UNIVERSITY GHANA. IN FULL REQUIREMENT FOR THE AWARD OF A BACHELOR OF SCIENCE DEGREE IN INFORMATION TECHNOLOGY (BSc. IT).

FEBRUARY 2025

DECLARATION

We confirm that, except where indicated through the proper use of citation and references, the content of this dissertation is our work. We confirm that, subject to final approval by the Department, a copy of this dissertation may be placed upon the shelves of the Library of Methodist University Ghana or made available electronically in the Library Dissertation repository and may be circulated as required.

31/01/2025

TETTEY MICHAEL NII AYI **DATE**

(BSSI/ED/218894)

31/01/2025

OFORI DANIEL PERRY JNR **DATE**

(BSSI/ED/210056)

31/01/2025

IQWEBUIKE SOLOMON JNR **DATE**

(BSSI/ED/221348)

31/01/2025

ESHUN DARLINGTON EBENEZER **DATE**

(BSSI/ED/218704)

Richmond O. Sarkodie

31/05/2025

DR. R.O.SARKODIE **DATE**

(SUPERVISOR)

DEDICATION

This piece of work is dedicated to God Almighty for endowing us with wisdom, knowledge and understanding and also to our beloved parents.

ACKNOWLEDGMENT

Our greatest thanksgiving goes to the Lord Almighty who has made this project a success.

Our profound gratitude goes to our project supervisor Dr. Richmond Opoku Sarkodie and also to our Head Of Department Madam Ruth Larbey (MPhil) for making this project a learning process, others in the trend are our departmental lecturers.

We also want to acknowledge our families for their great support during our academic pursuit; may the Lord Almighty who knows and sees in advance shower His abundance blessing upon them.

ABSTRACT

As organizations continue to rely on interconnected networks for their operations, the need to optimize network infrastructure and enhance security measures becomes paramount. This project focuses on analyzing and implementing a hierarchical network architecture for Methodist University Ghana (MUG) to improve network performance and strengthen security protocols. By conducting a comprehensive assessment of the current network infrastructure at MUG, this project aims to identify vulnerabilities and inefficiencies that may compromise data integrity and confidentiality. The implementation of a hierarchical network architecture will involve the segmentation of network resources into distinct layers, each with specific functions and security measures. Through this approach, MUG can better manage network traffic, enhance scalability, and mitigate potential security threats. This project will serve as a roadmap for optimizing network infrastructure and enhancing Network security in Methodist University Ghana (MUG), offering valuable insights and recommendations for similar organizations seeking to bolster their network capabilities.

The project focuses on conducting a comprehensive network assessment of MUG using a bottom-up approach based on the OSI model, identifying and documenting at least three critical vulnerabilities and shortcomings in MUG's current network architecture, and implementing effective solutions to address these weaknesses. A key part of the solution is the segmentation of the network and securing the wireless infrastructure. Additionally, the project aims to optimize IP configurations and enforce access controls on the wired network to ensure more secure and efficient traffic management. Through this approach, the project will evaluate the improvements in both network performance and security, demonstrating the effectiveness of the implemented solutions.

The final deliverable for this project will be a comprehensive set of recommendations and documented configurations aimed at optimizing Methodist University Ghana's (MUG) network infrastructure.

This study serves as a practical guide for educational institutions facing similar challenges, demonstrating how to balance performance optimization with essential security protocols under resource constraints..

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

.

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND OF THE STUDY

In today's increasingly interconnected world, a robust and reliable network infrastructure is no longer a luxury but a fundamental necessity for any organization, particularly educational institutions. Think of a university campus as a bustling city; the network infrastructure is its underlying road system, facilitating the flow of information, resources, and communication. From online learning platforms to research collaborations and administrative tasks, virtually every aspect of modern education relies on a dependable network. In an age of digital transformation, a well-designed network infrastructure is not just about enabling connectivity, it is about enabling progress and facilitating innovation. A poor network can be a major roadblock to academic efficiency and can have a devastating impact on the educational process.

Methodist University Ghana (MUG), like many other higher education institutions in Ghana and its environs, depends heavily on its network infrastructure. This digital backbone supports essential services such as accessing online learning resources, managing student records, facilitating research collaboration and providing administrative support to staff. Consequently, the reliability, efficiency, and security of MUG's network directly impact the quality of teaching, research, and day-to-day administrative operations. A seamless and reliable network is essential in any institution, however when it comes to an educational institution, the importance of an efficient network increases. It is critical to enabling learning and allowing the various stakeholders to maximize their academic potential.

To ensure optimal network performance, a structured and methodical approach is paramount when assessing and improving the network. This is where the Open Systems Interconnection (OSI) model proves invaluable. Think of a building, right? It has layers, starting from the foundation all the way up to the roof. Well, we're tackling MUG's network in a similar way, using a bottom-up approach based on the OSI Model. This model, created by the International Organization for

Standardization, is like a universal language for different communication systems, allowing them all to talk to each other. It's a kind of framework that has seven levels:

- Layer 1 (Physical Layer): The wires and wireless signals, the physical stuff.
- Layer 2 (Data Link Layer): How data moves between devices on the same network.
- Layer 3 (Network Layer): Routing data across networks, think of it as postal addresses for data.
- Layer 4 (Transport Layer): Ensuring data gets there reliably and in order.
- Layer 5 (Session Layer): Managing connections between applications.
- Layer 6 (Presentation Layer): Formatting the data so different systems understand it.
- Layer 7 (Application Layer): The programs we use – like web browsers and email.

We'll be using this layered approach for both our audit and when we roll out our solution, making sure we are tackling things in a structured and thoughtful manner.

1.2 PROBLEM STATEMENT

Despite the crucial role that the network plays at MUG, the institution's existing network infrastructure faces several critical challenges that impede its performance, reliability, and security. Through an analysis of the network, it was discovered that these shortcomings include:

Suboptimal Wireless Access Point (AP) Placement: The current layout of wireless access points exhibits a lack of strategic planning. Many AP's designed for horizontal mounting were placed vertically, causing a reduction in the wireless signal range and coverage. Furthermore, obstacles such as trees and buildings were not taken into account when designing the network topology, resulting in compromised signal strength. This poor AP layout translates to unreliable and inconsistent Wi-Fi access across the campus.

Inadequate Network Security Measures: The absence of robust security measures in the wireless network creates a highly vulnerable environment. MUG's open wireless policy allows anyone to access the network without proper authorization, leaving it exposed to a wide range of potential security risks. The absence of security protocols makes the network a playground for potential malicious activity. This presents significant dangers, from data breaches to malware infections that can potentially cripple network devices.

Flat Network Architecture and Broadcast Storms: The current network architecture operates as a single, flat broadcast domain, where all devices communicate on the same network segment. This approach leads to excessive network congestion from the large numbers of ARP (Address Resolution Protocol) broadcasts, resulting in reduced network speeds and instability. These broadcasts quickly lead to broadcast storms, which can bring the entire network to a crawl. A flat network design lacks the necessary controls and segmentation, which makes it difficult to manage and scale as the university's demands increase.

1.3 GENERAL OBJECTIVES

The primary objectives of this research are to address the identified shortcomings in MUG's existing network and establish a more reliable, efficient, and secure infrastructure. To achieve this, we have set forth the following specific objectives:

- To conduct a comprehensive network assessment of Methodist University Ghana (MUG) using a bottom-up approach based on the OSI model.
- To identify and document at least three critical vulnerabilities and shortcomings in MUG's current network architecture based on the OSI model.
- To implement network segmentation and secure the wireless network at MUG.
- To optimize IP configuration and implement access controls on the wired network at MUG.
- To demonstrate the effectiveness of the implemented solutions by evaluating network performance and security improvements and generate a report detailing the impact of the changes.

1.4 RESEARCH QUESTIONS

To guide our research and ensure a comprehensive analysis, we have formulated the following research questions:

- **What are the key vulnerabilities present in MUG's current network infrastructure?**

- **How can proper wireless AP placement and configuration improve network performance?**
- **How can segmentation and VLANs improve security and network management at MUG?**
- **How will a RADIUS server enhance user authentication and security within the network?**

1.5 SIGNIFICANCE OF THE STUDY

This research project holds considerable significance for Methodist University Ghana and the broader academic community. By addressing the identified network deficiencies, this project stands to provide a significant positive impact, which includes:

- **Enhanced Reliability and Efficiency:** Improving the network will lead to a more robust and dependable network for students, lecturers and staff. This will directly affect their daily activities, enabling seamless access to online resources and enhancing their productivity and learning outcomes.
- **Improved Network Security:** The implementation of stronger security measures and authentication protocols will protect the network from malicious attacks. The overall security enhancement will ensure the confidentiality and integrity of the institution's data and protect its users.
- **Optimized Network Management and Scalability:** The redesigned network, with proper segmentation and IP management, will be more manageable and scalable to meet future demands. By implementing a well segmented network, MUG will be able to avoid network congestion, and provide better accessibility as the university grows.
- **A Model for Other Educational Institutions:** The successful implementation of these solutions will provide MUG with a strong network infrastructure, while also serving as a potential case study for other academic institutions facing similar challenges. By sharing our approach, we can help contribute to the broader goal of creating more robust and secure networks across the educational sector.

1.6 SCOPE

This project encompasses a comprehensive analysis of the existing network infrastructure at MUG, focusing on the wired and wireless aspects of the network. It will address network segmentation using VLANs, implementation of a RADIUS server to manage users, and the overall optimization of network traffic management. The research follows a bottom-up approach based on the OSI Model, which allows us to have a structured analysis from the physical all the way up to the application layer.

1.6.1 LIMITATIONS

- This project will not include any major hardware upgrade beyond the scope of this study.
- The primary focus of the study is on the optimization of the current network infrastructure using configuration and logical implementations, it will not address any external or cloud service dependencies.
- The analysis and design will focus on best practices and standards that can be implemented within the current university's budget, considering realistic constraints.
- The scope of the study is limited to the internal university network infrastructure. It will not address external dependencies such as connections to other networks.

CHAPTER TWO

LITERATURE REVIEW

2.1 CURRENT TECHNOLOGIES AND STANDARDS

This section explores established and emerging technologies that underpin network design and operation.

2.1.1 NETWORK INFASTRCTURE STANDARDS

The Open Systems Interconnection (OSI) model serves as a foundational framework for designing and optimizing network infrastructure, enabling diverse communication systems to interoperate using standardized protocols (Kenyon, 2002). Adherence to industry standards such as IEEE 802.11 for wireless networking and RFC 2865 for RADIUS protocol implementation enhances reliability and scalability in modern networks (Wong & Yeung, 2009). These standards provide benchmarks for secure and efficient configurations, ensuring interoperability across devices and platforms. The Institute of Electrical and Electronics Engineers (IEEE) 802.11ax (WIFI 6) standard has revolutionized wireless networking capabilities in high-density environments.

IEEE 802.11 is a set of standards for wireless local area network (WLAN) communication, commonly known as Wi-Fi. It specifies the protocols for implementing wireless networking, allowing devices like laptops, smartphones, and printers to communicate without physical connections. The standard covers various frequency bands, including 2.4 GHz, 5 GHz, and 6 GHz.

RFC 2865 defines the Remote Authentication Dial-In User Service (RADIUS) protocol. RADIUS is used for carrying authentication, authorization, and configuration information between a Network Access Server and an Authentication Server. It is widely implemented for managing network access and includes details on packet formats, types, and attributes.

2.1.2 SECURITY PROTOCOLS AND TECHNOLOGIES

Security protocols play a critical role in safeguarding data within network infrastructures. Modern networks rely on robust authentication, authorization, and accounting (AAA) services, typically provided by RADIUS (Wong & Yeung, 2009). The implementation of WPA3 as a new standard for wireless security addresses vulnerabilities like KRACK (Key Reinstallation Attacks) present in WPA2, offering enhanced encryption through Simultaneous Authentication of Equals (SAE) (Vanhoef & Ronen, 2020)

Simultaneous Authentication of Equals (SAE) is a password-based authentication and key agreement protocol used in wireless networks. It is a variant of the Dragonfly Key Exchange and is designed to provide secure key exchange even when using weak passwords. Key Features include password based authentication, dragonfly handshake, enhanced security and WPA3 Integration.

Security vulnerabilities can exist at each layer of the OSI model, requiring a multi-layered approach to protection," further highlighting the importance of an expansive approach to network security protocols (Sinha et al., 2017).

2.1.3 RECENT TECHNOLOGICAL ADVANCES

Recent advances in network design showcase dynamic architectures capable of adapting to evolving demands. Frameworks for dynamic network topology optimization leverage Software-Defined Networking (SDN) principles to streamline resource allocation and improve performance (Shafigh et al., 2016). SDN can enhance campus network efficiency by decoupling control planes from data planes, enabling more granular management and reduced latency (Zancan et al., 2023).

2.2 COMMON ISSUES

2.2.1 SECURITY VULNERABILITIES

Open wireless policies without adequate security measures expose networks to significant risk. Security vulnerabilities, such as password harvesting, man in the middle attacks, and malware propagation, are direct consequences of unsecured Wi-Fi environments (Misuri et al., 2019). The

importance of multi-layered security approaches to address vulnerabilities at each layer of the OSI model is another emphasis (Sinha et al., 2017).

2.2.2 PERFORMANCE CHALLENGES

Performance bottlenecks often arise due to insufficient segmentation, inadequate bandwidth allocation, and high density environments. This can drastically affect the user experience in a campus network (Ali et al., 2013). As observed at Methodist University Ghana (MUG), excessive Address Resolution Protocol (ARP) traffic can lead to severe congestion and degradation in network performance. Environmental obstacles, such as concrete walls and metallic surfaces, can also impact wireless signal strength and coverage (Ranji et al., 2023).

2.2.3 IMPLEMENTATION DIFFICULTIES

Technical expertise requirements, budget constraints, and resistance to change are some of the challenges that come with the implementation of advanced security measures and optimized configurations. The importance of stakeholder engagement during deployment phases to minimize disruptions and maximize adoption rates has been stressed (Wong & Yeung, 2009). Implementation difficulties in resource constrained environments pose additional challenges, especially with limited budgets and a lack of specialized expertise.

2.3 EXISTING SOLUTIONS AND BEST PRACTICES

2.3.1 NETWORK SEGMENTATION

VLAN implementation has emerged as a key strategy for network segmentation. Dividing the network into distinct segments reduces broadcast domains and isolates traffic between departments, improving both security and efficiency (Chidozie, n.d).

2.3.2 ROBUST AUTHENTICATION MECHANISMS

Deploying RADIUS servers ensures secure access control, preventing unauthorized access and safeguarding sensitive information. This involves using strong passwords and authentication methods on all wireless networks.

2.3.3 SECURITY FRAMEWORKS

Industry standards and best practices have been deployed to guide network implementation. The NIST Cybersecurity Framework provides a structured approach to network security implementation, and ISO/IEC 27001 offers comprehensive guidelines for information security management.

The NIST Cybersecurity Framework (CSF) is a set of voluntary guidelines developed by the National Institute of Standards and Technology (NIST) to help organizations manage and reduce cybersecurity risks. It provides a common language and systematic methodology for managing cybersecurity risk, and is widely used across various sectors and industries.

Key Components of the NIST Cybersecurity Framework include:

Its five core functions;

- Identify: Develop an understanding of the organization's cybersecurity risks to systems, assets, data, and capabilities.
- Protect: Implement safeguards to ensure the delivery of critical infrastructure services.
- Detect: Develop and implement activities to identify the occurrence of a cybersecurity event.
- Respond: Take action regarding a detected cybersecurity incident.
- Recover: Maintain plans for resilience and restore any capabilities or services impaired due to a cybersecurity incident.

Implementation Tiers: These provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. The tiers range from Partial (Tier 1) to Adaptive (Tier 4).

Profiles: These are customized alignments of the Framework Core to the organization's requirements, risk tolerance, and resources. Profiles help organizations identify and prioritize opportunities for improving cybersecurity.

ISO/IEC 27001 is an international standard for information security management systems (ISMS). It provides a framework for establishing, implementing, maintaining, and continually improving an ISMS to help organizations manage the security of assets such as financial information, intellectual property, employee details, and information entrusted by third parties.

Key Aspects of ISO/IEC 27001 include:

- **Risk Management**: The standard emphasizes a risk management process to identify, assess, and treat information security risks.
- **Security Controls**: It includes a comprehensive set of security controls and best practices to protect information assets.
- **Continuous Improvement**: Organizations are required to continually improve their Information Security Management System (ISMS) to adapt to changing security threats and business needs.
- **Certification**: Organizations can be certified to ISO/IEC 27001 by an accredited certification body, demonstrating their commitment to information security.

Benefits include:

- **Enhanced Security**: Protects sensitive information from a wide range of threats.
- **Compliance**: Helps meet legal, regulatory, and contractual requirements.
- **Reputation**: Builds trust with customers and stakeholders by demonstrating a commitment to information security.
- **Operational Excellence**: Improves processes and reduces the likelihood of security incidents

2.3.4 REGULAR AUDITS AND MAINTENANCE

Continuous monitoring and periodic updates help identify and address emerging threats proactively. Reviewing and adjusting the IP configuration to optimize network traffic has also become a critical feature of network security.

2.4 RESEARCH GAPS AND FUTURE DIRECTIONS

Existing literature primarily focuses on solutions developed world contexts. There is a neglect of unique constraints encountered in academia, such as limited budgets and technical expertise. Few studies examine the integration of open source tools like FREERADIUS and daloRADIUS in securing wireless networks within resource constrained settings.

2.4.1 COMBINED SECURITY AND PERFORMANCE FOCUS

Most studies focus on either security or performance optimization. Limited research offers solutions that maximize both aspects simultaneously.

2.4.2 PRACTICAL IMPLEMENTATION DETAILS

A limited focus on the practical challenges of implementing complex network solutions means there needs to be more detailed implementation guidance in resource constrained environments.

This research will address the identified research gaps by providing practical and cost effective solutions that are tailored for the network in Methodist University Ghana (MUG). This project seeks to contribute to the development of novel solutions that can be applied to unique contexts by combining proven strategies to deliver optimized performance and security.

CHAPTER THREE

METHODOLOGY

This chapter details the research methods employed to analyze the network infrastructure at Methodist University Ghana (MUG), design potential security and performance enhancements, and evaluate proposed improvements based on the gathered data. Given the constraints of this project, the methodology is focused on the assessment, design, and simulated implementation rather than a full-scale deployment within the live university network. The overarching goal is to develop a theoretically sound and practically feasible network architecture enhancement, which incorporates both improved security protocols and optimized network performance.

3.1 RESEARCH DESIGN

A mixed methods approach is the most appropriate for this project, as it allows for the integration of quantitative network assessment data with qualitative insights gathered through limited engagement with key stakeholders. This approach enables a well-rounded understanding of the current state and informs the design of a hierarchical network architecture aimed at addressing identified shortcomings. The approach focused on a bottom-up perspective, using the OSI model, to thoroughly assess the network infrastructure.

The design of this research is based on the pragmatic research paradigm. This paradigm focuses on practical outcomes and real world applications. It is recognized that strict adherence to a singular methodological approach can limit the potential for meaning impact (Creswell & Plano Clark, 2017). By situating this project within a pragmatic framework, the research is grounded in real world context thus allowing for the findings to be beneficial within the constraints of the organization and time.

The research adopted a bottom up perspective using the Open Systems Interconnection (OSI) model. Instead of broadly trying to address the various issues of the network, the framework allowed for the study to have a well-structured approach that ensured nothing was missed. It also allowed for the effective identification of which actions had to be taken to rectify network problems.

Due to the constraints of time and resources, we were unable to make any direct or live interventions on the network, which also limited the scale and scope of engagement with the network IT staff, limiting to only the head of the multimedia department. There was limited collaboration with university management, which means this project only reflects insights we were able to obtain as students with limited collaboration access.

3.2 DATA COLLECTION METHODS

3.2.1 PRIMARY DATA COLLECTION

- **Site Surveys (Limited Scope):** Prior to any network adjustments, the physical components were reviewed. This was to help in getting a better understanding of the various components of the network, and to determine the layout. Tools like Ekahau, Netspot or AirMagnet also helped in determining network layout.
- **Interviews/Surveys (Qualitative):** A number of students were engaged to better understand the network concerns. This data was used to address the issues facing the institution with the aim of presenting it to the key stakeholders with the hopes of its implementation.
- **Traffic Analysis and Documentation:** The traffic captures, which were all conducted with the consent of the required individuals, were essential for figuring out the general architecture as well as the security risks of the network. The results of the traffic captures allowed for a deep study of the vulnerabilities.
- **VLAN Configuration Audits:** The proposed VLAN implementations were all documented with a test plan to review the proposed configurations and test network segmentation. These audits provided the framework for determining how traffic flows were implemented, and how these configurations were done.
- **RADIUS Assessments:** An assessment of the radius infrastructure at Methodist University Ghana (MUG) was done with a focus on user authentication, which sought to replace the current network, which has little to no authentication.

3.2.2 SECONDARY DATA COLLECTION

- **Literature review:** We analyzed existing studies on hierarchical network architectures, VLAN segmentation, RADIUS implementation, and best practices for securing educational institutions.
- **Documentation Analysis:** We reviewed MUG's current network topologies, logs, and security incident reports to establish baseline conditions.

3.3 DATA ANALYSIS TECHNIQUES

- **Packet Capture Analysis:** Analysis of packet capture using Wireshark is vital in security, troubleshooting and performance monitoring. This analysis on understanding the common protocols used, in addition to the identification of any potential security compromises to create a baseline understanding of network activity.
- **Qualitative Analysis:** An examination of student feedback from our focus groups aided in the triangulation of network performance results with real world user experience. It also allowed for the identification of trends within the user groups.
- **Configuration Testing (Simulated):** To examine the effects of the planned modifications, virtual machines (VM) and network simulation applications like Cisco Packet Tracer, GNS3 and Cisco Modeling Labs (CML) were used. This involved simulating network traffic and analyzing the behavior of the network under various situations by making various changes and measuring performance for the system.

3.4 ETHICAL CONSIDERATIONS

Ethical considerations were critical during this research. The research focused on maintaining responsible behavior and the safety of the various parties involved.

- **Data Privacy:** All data was anonymized to protect personal information. Just because we had access to IP addresses doesn't mean anyone should feel exposed.
- **Consent:** Participants were informed of the study's goal, data collecting techniques, and their right to withdraw without penalty before engaging. The participants who agreed to use their data were given the process in detail.

- **Compliance:** All procedures were reviewed and authorized by the university's relevant stakeholders to verify compliance with academic honesty.
- **Confidentiality:** Technical details and participants responses remained confidential, accessible only to those directly involved in the study. Trust is vital, whether in relationships or research.

3.5 IMPLEMENTATION STRATEGY

Given the practical constraints identified in this project, particularly the absence of direct access to Methodist University Ghana (MUG)'s operational network and the limited scope of engagement with university personnel, the implementation strategy is focused on a meticulous assessment and audit of the existing network infrastructure and the formulation of well-reasoned recommendations for potential improvements.

It is important to note that, due to these constraints, the project will conclude following the development of these recommendations, with no planned testing or validation activities on the live Methodist University Ghana (MUG) network.

The primary objective of this section is to articulate the specific steps and considerations that would be necessary for Methodist University Ghana (MUG) to implement the proposed enhancements, should they choose to pursue such a course of action. The approach emphasizes the theoretical soundness, practical feasibility, and potential benefits of the proposed solutions, based on best practices and industry standards.

3.5.2 AUDIT OF EXISTING INFRASTRUCTURE

The initial phase of the implementation strategy involved conducting a detailed, albeit limited, audit of Methodist University Ghana (MUG)'s existing network infrastructure. This assessment relied on network audits, publicly available information, existing network documentation (where accessible), and valuable insights gathered through limited engagement with key stakeholders, primarily the Head of the Multimedia Department.

Furthermore, the methodology of the assessment was non-invasive, designed not to affect the running of any existing systems.

Specifically, what this required was assessing the entire network through NMAP scanners, and Wireshark traffic captures. This allowed the team to have a high level understanding of where the security was an issue, while being non-intrusive to the existing network. The specific activities undertaken during this step included:

- **Network Mapping and Topology Discovery:** Utilizing network scanning tolls, the team mapped out the network topology, identifying active devices, operating systems, and open ports.
- **Vulnerability Scanning:** Identifying possible weaknesses with vulnerability scanning tools, and also through the manual analysis of network security configuration.
- **Network Traffic Analysis:** Gathering data and analyzing network use to pinpoint issues such as high broadcast traffic.

This audit phase was crucial for providing insights given the limitations of access to the systems.

3.5.3 PLANNING OPTIMIZATION SOLUTIONS

Following the detailed audit, the team focused on devising optimized solutions to address shortcomings in Methodist University Ghana (MUG)'s network infrastructure. We largely focused on best practices in similar institutions, existing research about IT frameworks in school environments, and what potential improvements could be made given all of the constraints.

- **VLAN Design:** Given the existing the network that Methodist University Ghana (MUG) had, it was determined that a VLAN implementation was essential to protect critical school systems. We. Designed VLAN configurations to segment the network into distinct domains: Admin, Students, Servers, Library, Wireless, and Lecturers.
- **IP Subnet Redesign:** Also given the IP issues related to the size of the subnet, it was decided that a proper subnetting scheme that reduces the hosts per subnet be implemented. We redesigned IP subnets to reduce broadcast domains and improve scalability.

- **RADIUS Authentication:** The team determined setting up user identifications, authorizations and accounting to minimize risk and adhere to compliance and security standards.

3.5.4 VALIDATION

It is extremely important to note that this project cannot and will not reflect what will happen to the school's existing network. For this reason, we are restricted to an assessment and proposed solutions in the form of documented configurations and suggestions, and do not have the permission to implement or test our design on the school's live network for a validation phase.

3.5.5 CHALLENGES IN TESTING AND VALIDATION

Testing and measuring post-implementation performance directly on MUG's live network would have been ideal but impractical due to operational constraints. Instead:

- **Simulated environments:** We utilized virtual machines and cisco packet tracer to replicate real world conditions and validate proposed changes.
- **Performance Metrics:** We compared and pre and post optimization metrics in simulations, demonstrating expected improvements in throughput, latency and security resilience,
- **Stakeholder Feedback:** We incorporated qualitative feedback from IT staff and users to refine recommendations, ensuring they align with practical needs.

3.5.6 DOCUMENTATION AND REPORTING

Finally to be able to summarize the work done and suggest the next steps, the team generated a series of documented results that could be analyzed by the relevant stakeholders at MUG.

3.6 PROJECT TIMELINE

3.6.1 AGILE MODEL

The Agile Model is a popular iterative and incremental approach to project management, particularly suited for dynamic environments where flexibility and adaptability are crucial. It

focuses on collaboration, continuous improvement, and delivering functional components in short cycles known as sprints or iterations. This model allows teams to respond quickly to changes, incorporate feedback, and refine solutions throughout the development process. In network infrastructure projects, Agile methodologies can enhance efficiency by breaking complex tasks into manageable phases, ensuring each step aligns with overall objectives while maintaining flexibility for adjustments based on results.

For this project, the Agile Model was implemented to streamline the optimization process by dividing the project into distinct phases; Audit and Planning, VLAN Configuration, IP Redesign, RADIUS Deployment, Testing and Validation.

Table 3. 1: Project Timeline Table using the Agile Model

PHASE	DURATION	ACTIVITIES
Audit and Planning	Week 1 – 3	Conduct Site Surveys, vulnerability scans and documentation reviews.
VLAN Configuration	Week 3 – 4	Define VLANs, assign ports, verify configurations, and address issues identified during audits
IP Redesign	Week 5	Implement new IP subnets, enable inter-VLAN routing, and validate settings
RADIUS Deployment	Week 6	Set up FreeRADIUS and daloRADIUS, configure authentication mechanisms, and test functionality.
Testing and Validation	Week 7 – 8	Perform security tests, gather user feedback, fine-tune configurations and prepare final reports.

3.6.2 ADVANTAGES OF THE AGILE MODEL

- **Flexibility:** The Agile Model accommodates changing requirements and unexpected challenges, making it ideal for complex projects like network optimization.
- **Collaboration:** Encourages active participation from all stakeholders, including university staff, end-users, and administrators, leading to more informed decision-making.

- **Incremental Delivery:** Functional components (e.g., VLANs, IP redesign, and RADIUS setup) are delivered incrementally, enabling early validation and reducing risks.
- **Continuous Feedback:** Incorporates regular feedback loops, ensuring solutions meet real-world needs and expectations.
- **Improved Quality:** Frequent testing and refinement improve the quality of deliverables, addressing potential issues proactively.

3.6.3 DISADVANTAGES OF THE AGILE MODEL

- **Resource Intensive:** Requires significant time commitment from team members due to frequent meetings and evaluations.
- **Scope Creep Risk:** Without strict planning, additional features or changes may delay the project timeline.
- **Documentation Overhead:** While Agile focuses on working software, proper documentation remains critical for future reference, which can add complexity.
- **Dependency on Team Expertise:** Success relies heavily on skilled team members who can effectively manage iterative processes and adapt to evolving requirements.

3.6.4 WHEN TO USE THE AGILE MODEL

The Agile Model is most effective when:

- Projects involve uncertainty or require frequent updates based on stakeholder feedback.
- Teams need to deliver functional components incrementally rather than waiting for a single, monolithic release.
- Collaboration between developers, users, and other stakeholders is essential for success.
- Flexibility and adaptability are necessary to address unforeseen challenges or take advantage of emerging opportunities.

CHAPTER FOUR

NETWORK INFRASTRUCTURE ANALYSIS

4.1 CURRENT NETWORK MAPPING

The current network infrastructure at Methodist University Ghana (MUG) operates as a flat, non-segmented architecture, where all devices reside in a single broadcast domain without logical or physical segmentation.

Below is an overview of the existing setup:

- IP Address Range: **192.168.0/19**
- Netmask: **255.255.224.0**
- Total Usable IPs: **8190**

This configuration supports a broad range of devices but lacks isolation between departments or user groups, leading to inefficiencies and vulnerabilities. For instance:

- Devices such as servers, student laptops, printers, and wireless access points are interconnected without restrictions.
- The absence of VLAN results in excessive broadcast traffic, making the network prone to congestion and potential failures.

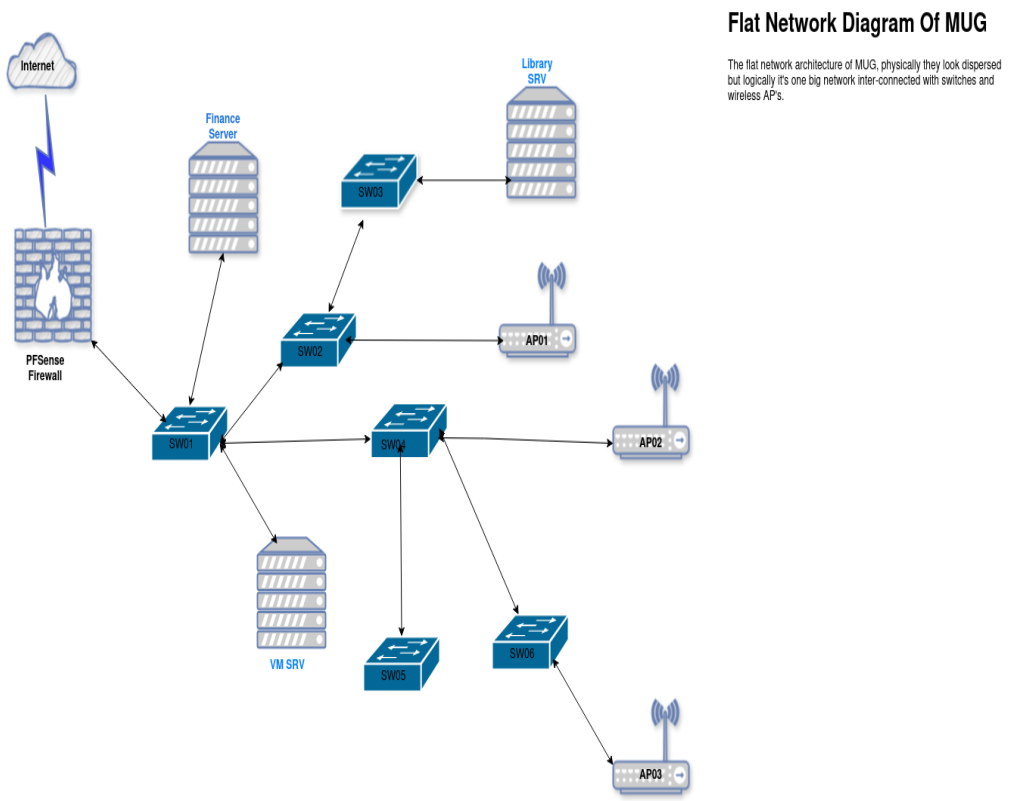

Figure 4. 1: A diagram showing the Flat network architecture of Methodist University Ghana. All devices share the same broadcast domain:192.168.0.0/19

4.2 PROBLEM ANALYSIS

The audit identified several critical issues across different OSI layers. They include:

4.2.1 LAYER 1 (PHYSICAL LAYER): WIRELESS ACCESS POINT (AP) MISPLACEMENT

We started off by conducting a site survey of Methodist University Ghana's infrastructure from the layer perspective. We first tackled the wireless infrastructure where we checked the design and layout of the wireless access points and types. Observations revealed improper placement of wireless AP's (access points), particularly ceiling-mounted units positioned vertically instead of horizontally. This affect the range of the wireless signals because aperture of the device is meant to be horizontal. Environmental factors such as concrete walls, metallic surfaces, and trees further degrade signal strength and quality.

4.2.1.1 WIRELESS ACCESS POINT (AP) LAYOUT

Wireless Signal Layout refers to the design and arrangement of the wireless network infrastructure including the placement of access points (AP's) and the coverage area of the wireless signal within a given environment. This layout is crucial for ensuring optimal wireless connectivity, network performance, and user experience. A well designed signal layout minimizes dead zones, interference, and congestion, while maximizing coverage and capacity.

Key Considerations for Wireless Signal Layout:

1. **Coverage Area:**
    - The first step in designing a wireless layout is to determine the size and shape of the area that needs to be covered. This could be a home, office, campus, or outdoor space.
    - The goal is to ensure that the entire area receives adequate wireless signal strength without over-provisioning or under-provisioning.

2. **Access Point Placement:**
    - **Access Points (AP's)** are devices that transmit and receive wireless signals, allowing devices to connect to the network.
    - Proper AP placement is essential to ensure that there is minimal overlap between the coverage areas of neighboring AP's and to avoid weak signal areas or interference.
    - In general, AP's should be placed in centralized locations to ensure even coverage, especially in larger areas, and avoid placing them in corners or near thick walls.
    - In large spaces, multiple AP's may be needed to provide sufficient coverage, and **mesh networks** may be used to extend coverage.

3. **Signal Strength and Range**
    - Wireless signal strength generally diminishes with distance and can be affected by obstacles (e.g., walls, furniture and floors) and interferences (e.g., electronic devices, microwaves).

- Signal strength is typically measured in **dBm (decibels milliwatts)**, with stronger signals being closer to 0 dBm and weaker signals being negative (e.g., -50 dBm, -70 dBm).
- Ensure that the signal strength is strong enough for the intended use case (e.g., browsing, streaming, and gaming) across the entire area.

4. **Frequency Bands**
    - Wireless networks often operate in two primary frequency bands: **2.4 GHz and 5 GHz.**
        - **2.4 GHz:** Has a longer range and better penetration through obstacles but is more susceptible to interference from devices like microwaves, Bluetooth devices, and other Wi-Fi networks.
        - **5 GHz:** Offers higher speeds and less interferences but has a shorter range and is less effective at penetrating walls and floors.
    - Some newer access points support **tri-band** (including the **6 GHz** band) and can operate simultaneously across multiple frequencies to avoid congestion and optimize performance.

5. **Channel Planning:**
    - In the **2.4 GHz** band, only three non-overlapping channels (1,6 and 11) are available in many regions, so careful channel planning is needed to avoid interference between adjacent access points.
    - The **5 GHz** band offers more non-overlapping channels, providing better flexibility and less interference in areas with multiple AP's.
    - Tools like **site survey software** can help identify which channels are being used in the environment and help in selecting the optimal channels.

6. **Environmental Factors:**
    - Different materials and obstacles can affect the strength and quality of wireless signals. Some examples include:
        - **Concrete walls:** Significant signal attenuation.

- **Metallic surfaces:** Reflection and interference.
- **Glass:** Minor signal attenuation but may affect certain frequencies.

- Wireless layout should account for these factors to determine the ideal placement of AP's to avoid dead zones (areas without coverage).

7. **Capacity and Density:**
    - For environments with a high density of devices (e.g., offices, stadiums, or large public venues), consider the **capacity** of the wireless network.
    - In high density environments, a combination of **load balancing** between AP's and **channel reuse** can help optimize performance and reduce congestion.
    - The number of devices and their usage (e.g., video conferencing, large file transfers) will determine the capacity needed at each AP.

8. **Mesh Networks and Extenders:**
    - In larger or irregularly shaped spaces, a **mesh network** might be used. Mesh networks consist of multiple AP's that communicate with each other, extending coverage without needing additional cabling.
    - Wireless **extenders** or **repeaters** can also be used to extend coverage to areas that may be too far from the main AP's.

9. **Security Considerations**
    - Ensure that the wireless network is properly secured to prevent unauthorized access. This includes setting up strong encryption methods (e.g., WPA3), using strong passwords, and configuring firewalls and access controls.
    - **Guess networks** can be set up for visitors, keeping them isolated from the internal network.

4.2.1.2 TOOLS FOR PLANNING A WIRELESS SIGNAL LAYOUT

1. **Site Survey Tools:**
    - Tools like **Ekahau, AirMagnet,** or **Netspot** can be used to conduct wireless site surveys. These tools analyze the layout of the environment, identify signal strengths, detect interference, and recommend the best AP placement and channel configurations.

2. **Heat maps:**
    - A **heat map** is a visual representation of the wireless signal strength across the layout of the building. These maps help identify areas with strong or weak signals and help determine the AP placement.

3. **RF Planning Software:**
    - Radio Frequency (RF) planning software models the environment to predict signal propagation, helping to optimize the placement of AP's.

```
16653 Captured ARP Req/Rep packets, from 212 hosts.   Total size: 957278

  IP              At MAC Address      Count      Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
172.20.0.20       18:e8:29:e0:13:95     505    21210  Ubiquiti Inc
172.20.0.19       18:e8:29:e0:14:94     830    34860  Ubiquiti Inc
172.20.0.15       18:e8:29:e0:17:cb     654    27468  Ubiquiti Inc
172.20.10.90      ea:86:df:8c:8c:b0      11      624  Unknown vendor
172.20.0.14       18:e8:29:e0:13:16     675    40500  Ubiquiti Inc
172.20.0.17       18:e8:29:e0:14:66     662    39720  Ubiquiti Inc
172.20.0.12       18:e8:29:e0:15:08     570    34200  Ubiquiti Inc
172.20.0.24       18:e8:29:e0:1d:c9     646    38760  Ubiquiti Inc
0.0.0.0           b8:c3:85:c7:c8:c3       3      180  HUAWEI TECHNOLOGIES CO.,LTD
172.20.0.18       18:e8:29:9c:c0:64     636    38160  Ubiquiti Inc
172.20.1.46       7c:76:35:8b:5b:78      22     1140  Intel Corporate
0.0.0.0           7c:76:35:8b:5b:78      26     1380  Intel Corporate
172.20.0.38       18:e8:29:9c:d4:8e     647    38820  Ubiquiti Inc
172.20.0.26       18:e8:29:e0:1b:bd     570    34200  Ubiquiti Inc
172.20.0.1        50:3e:aa:0e:b4:af     308    18480  TP-LINK TECHNOLOGIES CO.,LTD.
172.20.0.21       18:e8:29:e0:1e:3e     643    38580  Ubiquiti Inc
172.20.18.74      12:7a:14:56:93:5f       7      294  Unknown vendor
172.20.5.166      54:13:79:4b:27:ad     166     9960  Hon Hai Precision Ind. Co.,Ltd.
172.20.8.37       12:29:a9:60:13:ca      50     3104  Unknown vendor
172.20.0.27       74:83:c2:39:3c:90     170    10200  Ubiquiti Inc
172.20.20.192     42:03:2e:53:dd:77      26     1506  Unknown vendor
172.20.3.138      cc:d9:ac:57:07:33     106     6360  Intel Corporate
0.0.0.0           4a:20:95:59:33:72       2      120  Unknown vendor
172.20.30.12      4a:20:95:59:33:72       2      120  Unknown vendor
```

Figure 4. 2: A screenshot of AP and IP brands on the MUG's network

4.2.2 LAYER 2 (DATA LINK LAYER): SECURITY VULNERABILITIES AND BROADCAST STORMS

4.2.2.1 SECURITY

We observed that MUG practices an open wireless policy that has no security measures to protect both students and the network infrastructure. This is bad because any outside can enter the school's premises, connect any wireless device and perform malicious stuff like password harvesting, man in the middle attacks, spreading and infesting devices with viruses. Worse case these attackers can attack the school's network and create backdoors.

Figure 4. 3: DNS Traffic captured on an android device

As seen in figure 4.3, we captured DNS traffic from an android phone (device) where an attacker can inject viruses and backdoor on users of these devices.

4.2.2.2 BROADCAST STORMS

Out of the over 1.5 million packets captured, 99.2% of the traffic was full of ARP (Address Resolution Protocol) broadcasts.

Address Resolution Protocol (ARP) is a data link layer protocol which maps a MAC address to an IP address for end notes to communicate. Should a network be full of ARP requests, these mean certain devices or servers cannot be reached which causes broadcast storms, a condition where a network is overwhelmed with ARP packets to the point that the switch fails or a denial of service (DoS) occurs.

A **network broadcast storm** refers to a situation where there is an excessive amount of broadcast traffic on a network, leading to severe congestion and degradation of network performance. Broadcast traffic is the data sent to all devices on a network rather than to a specific device.

In Ethernet networks, this is typically done by using a broadcast **MAC (Media Access Control)** address **(FF:FF:FF:FF:FF:FF)** and in IP networks, it uses the broadcast **address (e.g., 255.255.255.255).**

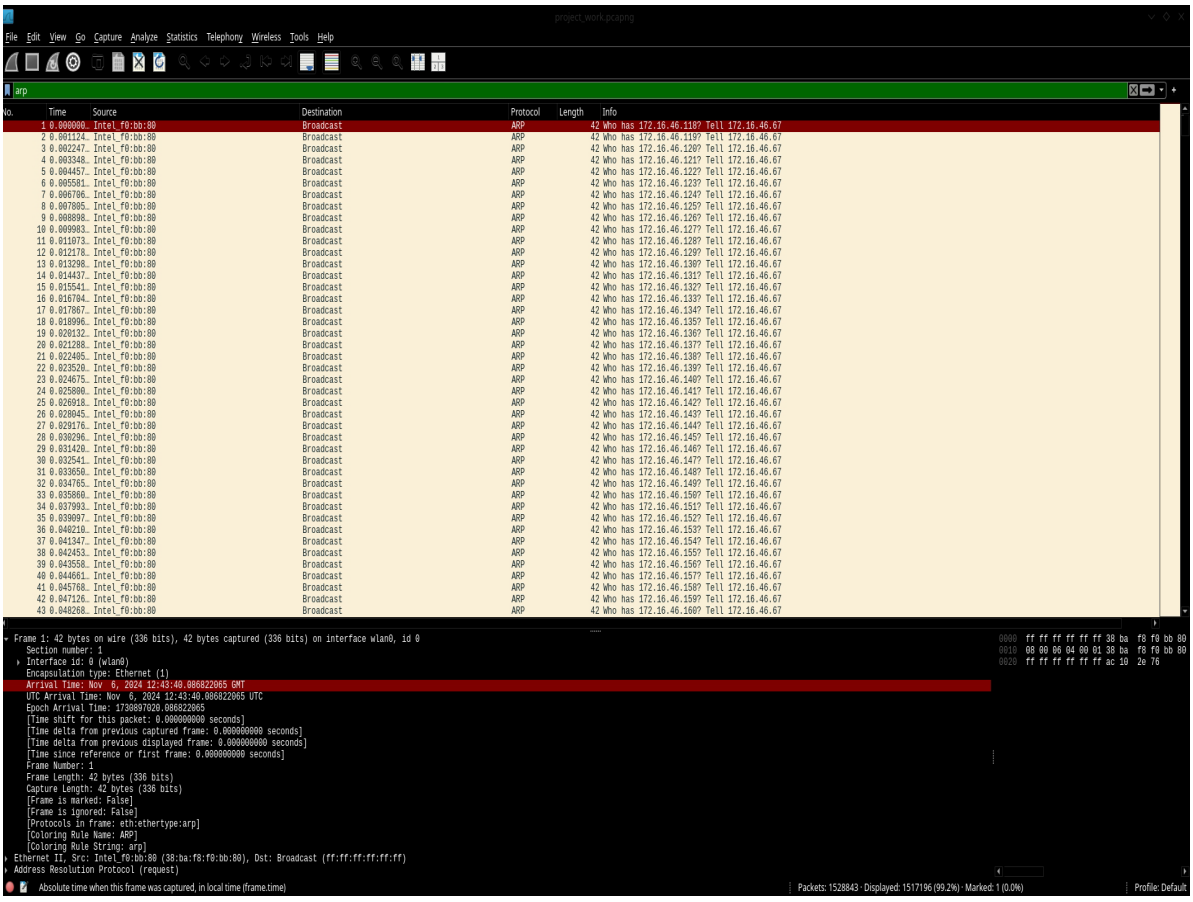

Figure 4. 4: Excessive ARP traffic captured on Wireshark. This overwhelms switches and disrupts communication

4.2.2.3 CAUSES OF BROADCAST STORMS

Broadcast storms can be caused by several factor, including:

- **Network Loops:** A common cause of broadcast storms in Ethernet networks is a loop in the network topology. When there is a loop, broadcast frames can circulate indefinitely between switches or routers, causing them to be retransmitted multiple times, creating an overwhelming amount of traffic.
- **Faulty or Misconfigured Network Devices:** Misconfigurations, such as improper VLAN setups or devices sending excessive broadcasts (e.g., ARP requests, DHCP Discover messages) can also trigger broadcast storms.
- **Defective Network Interfaces:** Malfunctioning network interfaces can send continuous broadcast traffic, which can escalate into a storm.
- **Broadcasting Protocols:** Protocols that rely on a broadcast traffic like ARP (Address Resolution Protocol) or DHCP (Dynamic Host Configuration Protocol), may generate high volumes of broadcast traffic under certain conditions, especially in large networks.

4.2.2.4 EFFECTS OF A BROADCAST STORM

- **Network Congestion:** A broadcast storm consumes significant network bandwidth, slowing down the communication of other devices.
- **Device Overload:** Devices, such as switches and routers, may become overwhelmed trying to process excessive broadcast traffic, leading to performance degradation or even crashes.
- **Connectivity Issues:** The network becomes highly unreliable, with devices struggling to communicate or being unable to send or receive data.

4.2.2.5 FLAT NON-SEGMENTED NETWORK

A **Flat Non-segmented Network** refers to a network architecture where all devices (computers, servers, printers, etc.) are placed in a single, continuous broadcast domain without being divided into smaller segments or subnets. In such a network, all devices are directly reachable from one

another, and there is no segmentation (either through physical or logical means) that isolates traffic or limits the scope of broadcast communication.

As seen in the captured log below, it is apparent that MUG's network is flat, connecting from one point you can have access to all devices on the entire network.

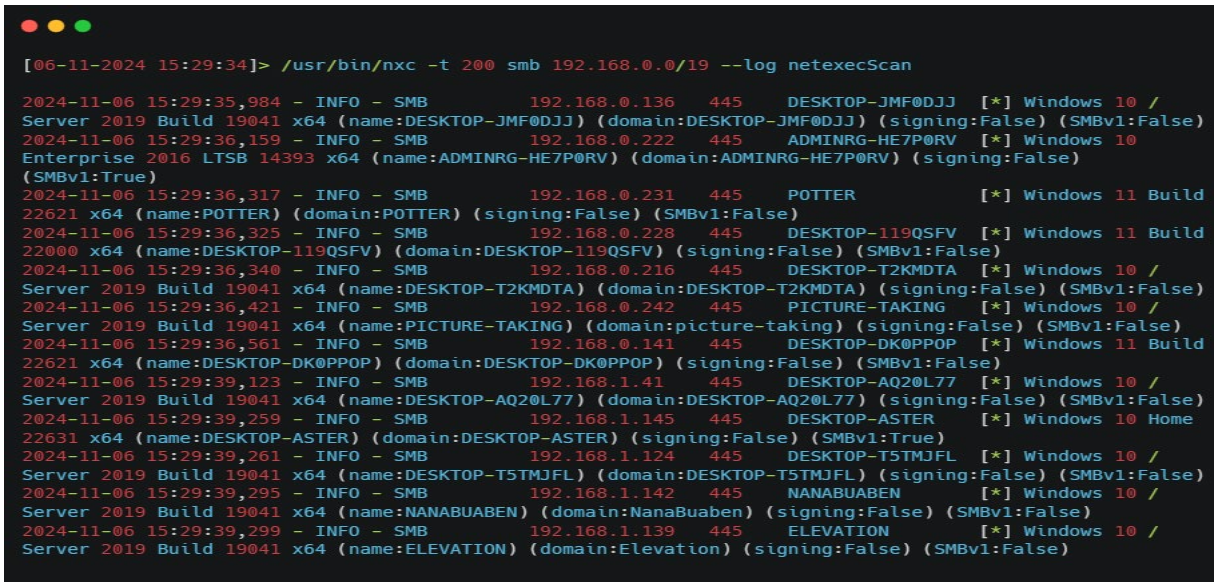

Figure 4. 5: Captured Traffic Log showing flat non-segmented network

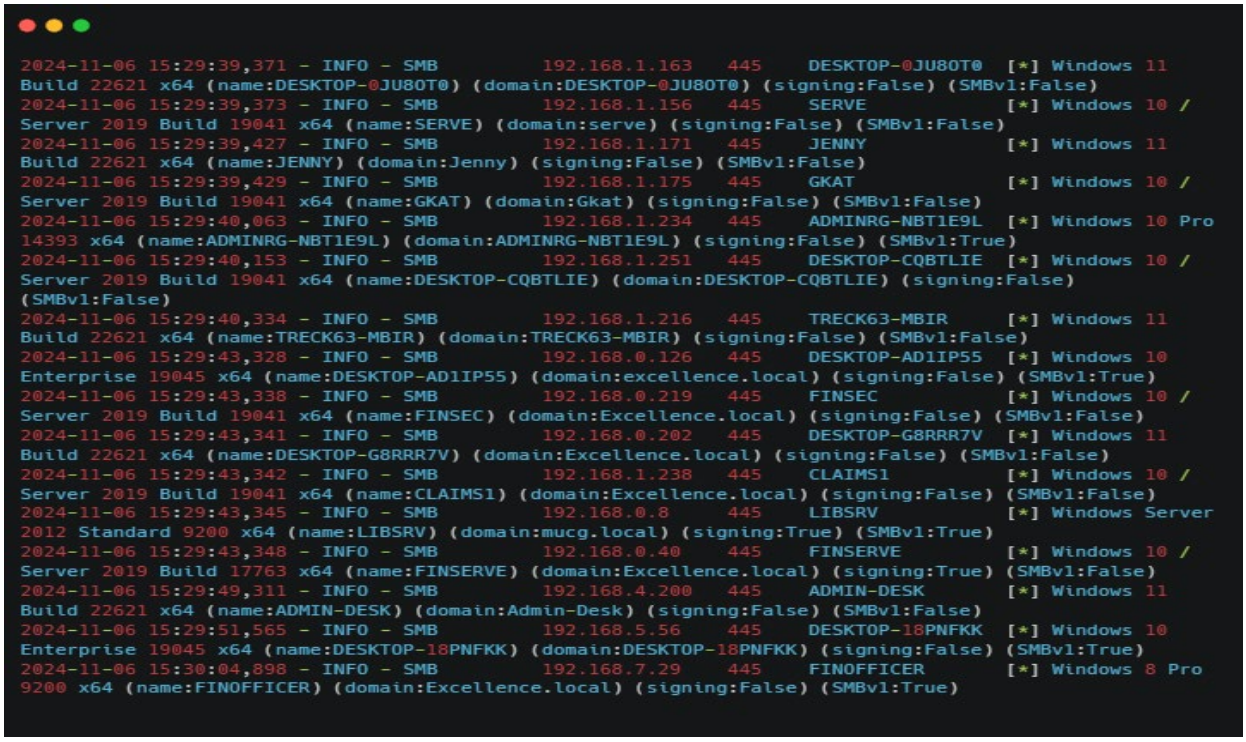

Figure 4. 6: Captured Traffic Log showing flat non-segmented network

4.2.2.6 KEY CHARACTERISTICS OF A FLAT NON-SEGMENTED NETWORK

- **Single Broadcast Domain**
    - All devices in a flat network are part of the same broadcast domain. This means that broadcast traffic (e.g., ARP request, DHCP discovery packets) sent by one device will be received by all devices in the network.
    - As a result, network traffic can quickly become congested if a large number of devices are involved, especially if a broadcast storm occurs.
- **Lack of Segmentation**
    - There are no physical or logical boundaries like VLANs (Virtual Local Area Networks) or subnets. All devices are within the same IP address range and subnet.
    - This lack of segmentation can cause issues as the network grows because the broadcasts will be sent to all devices, potentially overwhelming network resources and reducing performance.
- **Simple Configuration**
    - Flat networks are relatively simple to configure since there are fewer routing or segmentation rules to manage.
    - They are often used in all small networks with fewer devices, where complexity and overheads are not required.
- **Limited Scalability**
    - As more devices are added to the network, the number of broadcasts increases, which can lead to network performance degradation.
    - The absence of segmentation makes it difficult to scale the network effectively beyond a certain size, as broadcast traffic can saturate the entire network.
- **Single Point of Failure**
    - Since all devices are part of a single network, issues such as hardware failure or network congestion can affect the entire network.

4.2.2.7 DRAWBACKS OF A FLAT NON-SEGMENTED NETWORK

- **Broadcast Traffic Overload**
    - With no segmentation, all devices in the network receive broadcast packets. As the number of devices increases, the amount of broadcast traffic increases, which can lead to network congestion and potential broadcast storms.
- **Security Risks**
    - In a flat network, there is no isolation between devices. Any device can potentially communicate with any other device on the network. This can pose security risks, especially if devices contain sensitive information or if malware spreads through the network.
- **Performance Issues**
    - As the network grows, performance may degrade due to increased broadcast traffic, collisions (in Ethernet networks), and longer response times.
- **Scalability Limitations**
    - Flat networks are not well suited to scale beyond a certain size. Adding more devices or users increases network complexity and traffic load without adding any isolation or management capabilities.

4.2.3 LAYER 3 (NETWORK LAYER): IP SUBNET INEFFICIENCY

The current IP network and address range is as shown below.

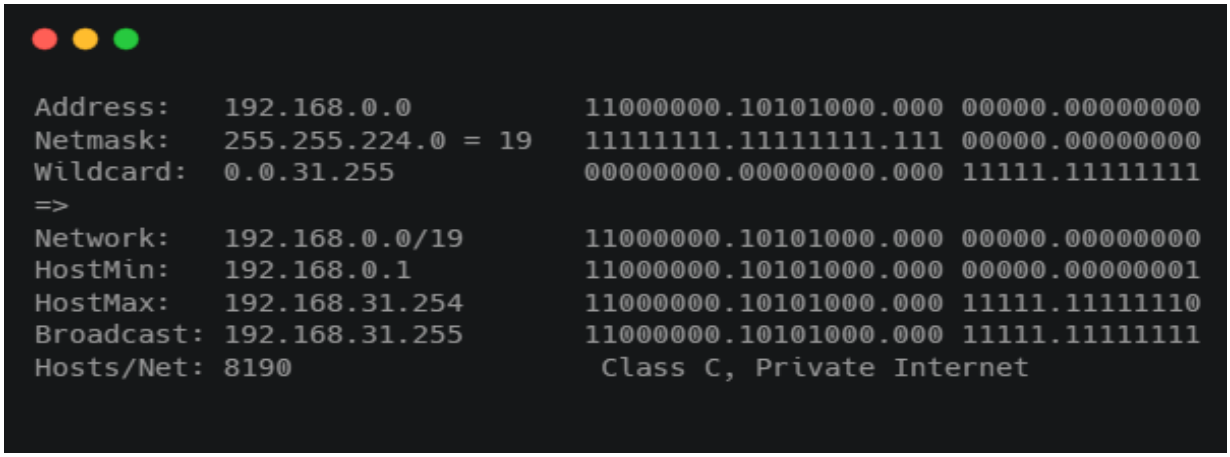

Figure 4. 7: Current IP network and address range of MUG live network

This network yields **8190** usable **IP's** which is very bad for a flat network architecture like we currently have at **Methodist University Ghana (MUG).**

4.2.4 HIGHER LAYERS (4–7): APPLICATION-LEVEL CONCERNS

At higher OSI layers, the absence of robust authentication mechanisms leaves applications vulnerable to unauthorized access.

No RADIUS server exists to enforce AAA (Authentication, Authorization, and Accounting) policies, leaving users exposed to password harvesting and man-in-the-middle attacks.

4.3 IMPACT ASSESSMENT

The identified issues significantly affect MUG's network performance, security, and reliability:

- **Performance Degradation**
    - Excessive broadcast traffic consumes bandwidth, slowing down legitimate communications.
    - High-density environments like lecture halls and libraries experience frequent disconnections due to congestion.
- **Security Risks**
    - Open wireless policies allow unauthorized devices to connect, posing risks of data breaches and malware propagation.
    - A flat network architecture enables attackers to move laterally, accessing sensitive systems and data.
- **Scalability Limitations**
    - Adding new devices increases broadcast traffic exponentially, making the network unsustainable for future growth.
    - Without VLAN segmentation, managing diverse user groups becomes cumbersome and error-prone.
- **Operational Challenges**

- IT staff face difficulties isolating faults or implementing targeted updates due to the lack of logical boundaries.
- User dissatisfaction arises from slow connections, frequent outages, and poor wireless coverage.

CHAPTER FIVE

SOLUTION DEVELOPMENT

5.1 DESIGN OF PROPOSED SOLUTIONS

The proposed solutions are structured using the OSI model to ensure comprehensive coverage of physical, data-link, network, and application(transport, session, presentation, application)-layer challenges.

5.1.1 LAYER 1 (PHYSICAL LAYER)

- **Central Placement of AP's:** Place AP's in central areas of the space to ensure even coverage, avoiding placing them in corners or near walls that can block signals.
- **Minimize Interference:** Avoid placing AP's near devices that generate significant interference (e.g., microwave ovens, cordless phones).
- **Use Multiple Bands and Channels:** For better performance, especially in high density environments, use both the 2.4GHz and 5GHz bands and ensure that neighboring AP's are set to different channels.
- **Consider Future Expansion:** Design the wireless layout with future growth in mind, allowing room for adding more devices or additional AP's without major configuration.
- **Regular Monitoring and Maintenance:** Continuously monitor the performance of the wireless network and adjust as needed (e.g., adding AP's, changing channels) to ensure optimal performance.

5.1.2 LAYER 2 (DATA LINK LAYER)

We will divide the flat network into six distinct VLANs: **Admin, Students, Servers, Library, Wireless,** and **Lecturers**. This reduces broadcast domains and isolates traffic between departments, improving both security and efficiency.

Step by step Procedure

1. **Access the switch:** Connect to the Cisco switch and enter privileged EXEC mode using **Switch# enable.**
2. **Enter Global Configuration Mode**: To start configuring the VLANs, enter global configuration mode using: **Switch# configure terminal.**
3. **Create VLANs:** Now, we define the 6 VLANs. Each VLAN will be assigned a number and a name.

```
Switch(config)# vlan 10
Switch(config-vlan)# name admin
Switch(config-vlan)# exit

Switch(config)# vlan 20
Switch(config-vlan)# name students
Switch(config-vlan)# exit

Switch(config)# vlan 30
Switch(config-vlan)# name servers
Switch(config-vlan)# exit

Switch(config)# vlan 40
Switch(config-vlan)# name library
Switch(config-vlan)# exit

Switch(config)# vlan 50
Switch(config-vlan)# name wireless
Switch(config-vlan)# exit

Switch(config)# vlan 60
Switch(config-vlan)# name lecturers
Switch(config-vlan)# exit
```

Figure 5. 1: VLAN configuration commands on Cisco switch

4. **Assign VLANs to ports:** Next, assign each VLAN to the appropriate ports. This depends on how you have the devices connected to your switch.

```
Switch(config)# interface range gigabitEthernet 0/1 - 5
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10  ! Assign to Admin VLAN
Switch(config-if-range)# exit

Switch(config)# interface range gigabitEthernet 0/6 - 10
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 20  ! Assign to Students VLAN
Switch(config-if-range)# exit

Switch(config)# interface range gigabitEthernet 0/11 - 15
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 30  ! Assign to Servers VLAN
Switch(config-if-range)# exit

Switch(config)# interface range gigabitEthernet 0/16 - 20
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 40  ! Assign to Library VLAN
Switch(config-if-range)# exit

Switch(config)# interface range gigabitEthernet 0/21 - 25
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 50  ! Assign to Wireless VLAN
Switch(config-if-range)# exit

Switch(config)# interface range gigabitEthernet 0/26 - 30
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 60  ! Assign to Lecturers VLAN
Switch(config-if-range)# exit
```

Figure 5.2: VLAN configuration commands on Cisco switch

5. **Verify VLAN Configuration:** After configuring the VLANs, use **Switch# show vlan brief** to verify the settings by checking the VLAN database and the assigned interfaces.
6. **Save the Configuration:** Finally, use Switch**# write memory to** save your configuration to make it persistent across reboots.

5.1.3 LAYER 3 (NETWORK LAYER) IP REDESIGN, ROUTING PROTOCOLS, L3 SWITCHING

With the solution of segmenting the flat network into VLAN's, it is prudent to follow it up with accompanying networks make routing and internet reachability easy. We structured the new IP networks based on observations and captured traffic on the network.

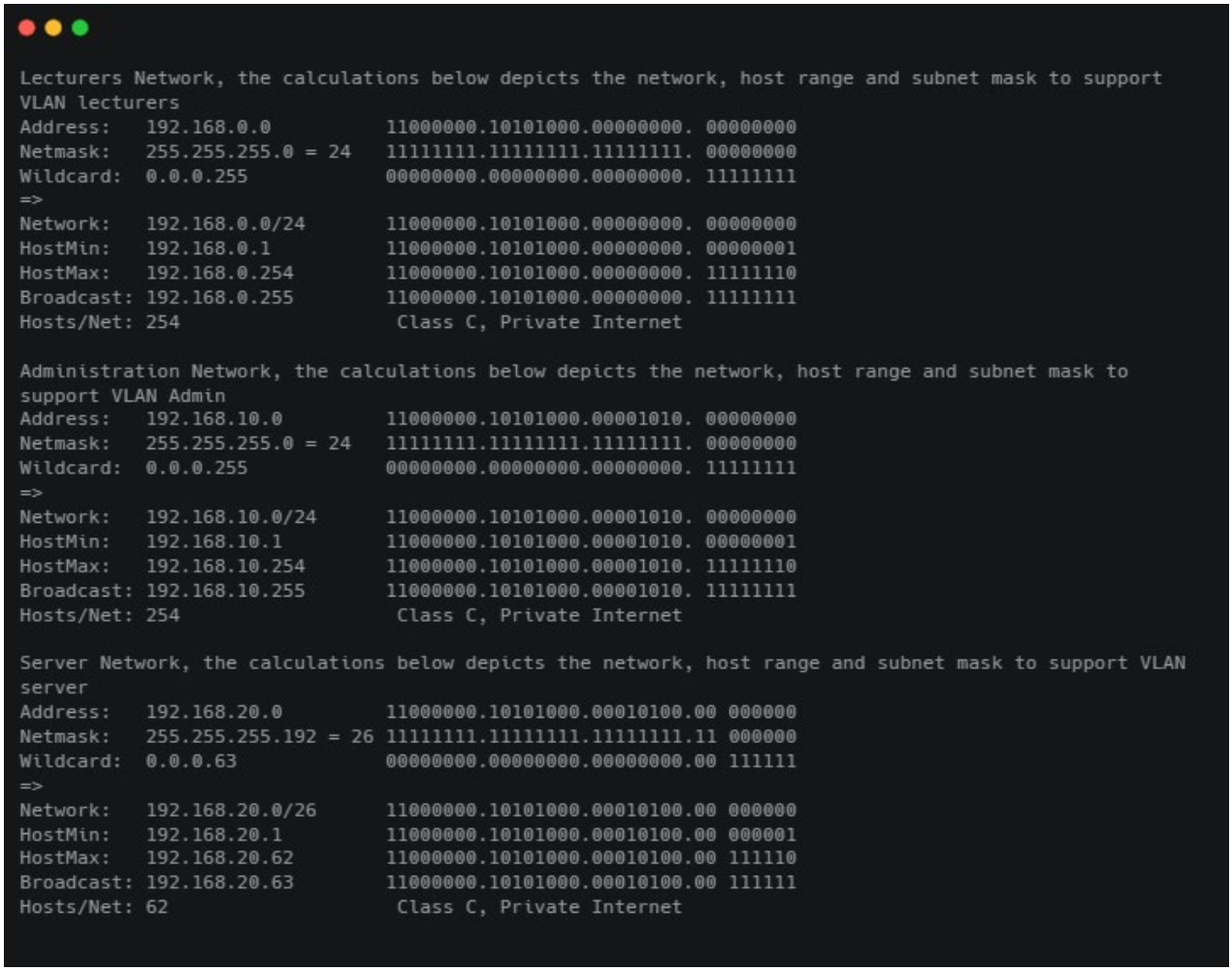

Figure 5. 3: New IP addresses created to replace the /19 subnet with VLSM-optimized ranges (e.g., /24 for Admin, /26 for Servers).

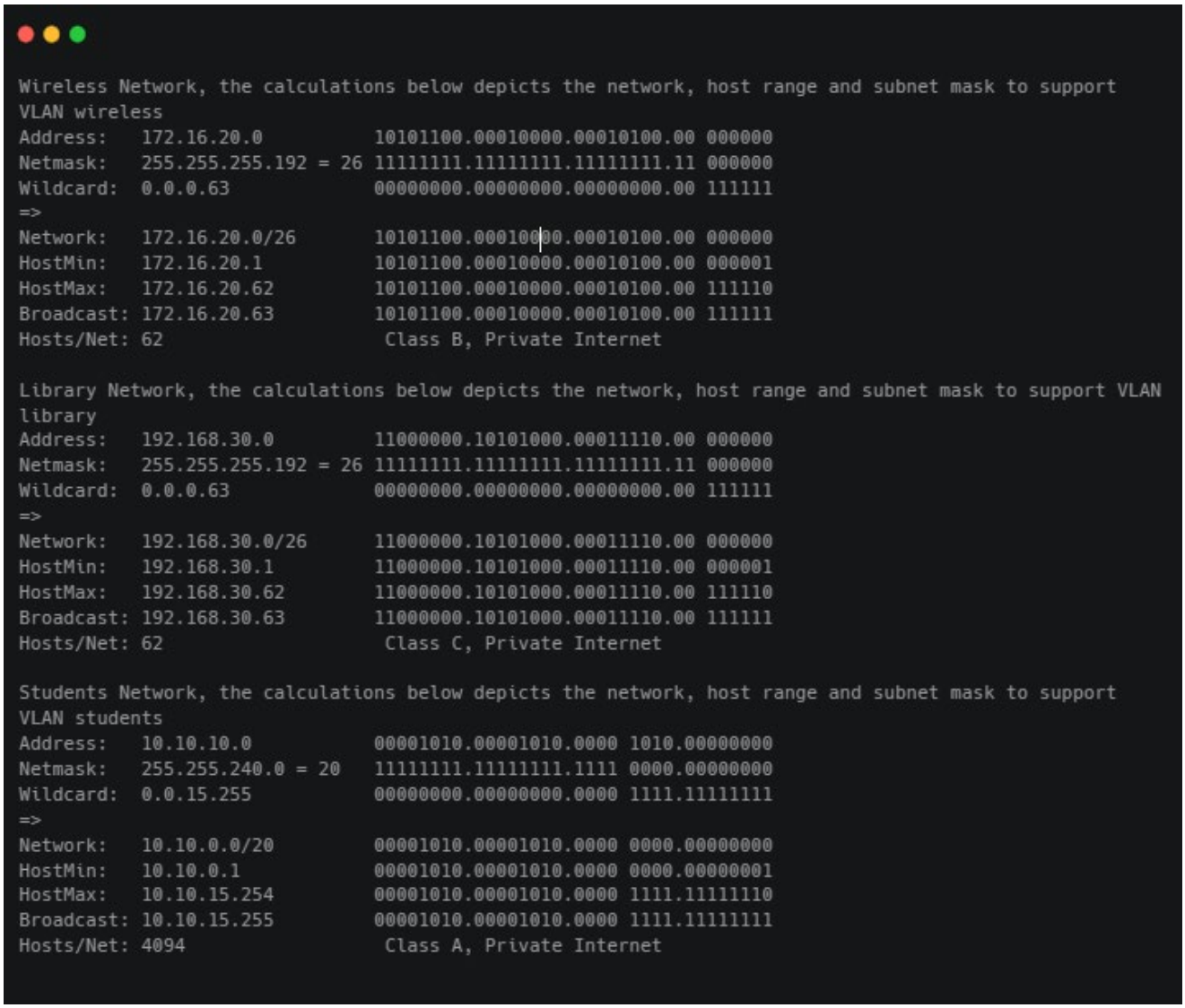

Figure 5. 19: New IP addresses created to replace the /19 subnet with VLSM-optimized ranges (e.g., /20 for Students, /26 for Wireless).

From the new IP calculations, we reduced the previous network of host 8190 to 4790 saving 3400 IPs and hence reducing excess broadcast.

5.1.3.1 IP NETWORK MAPPING TO VLANs

- Admin VLAN (VLAN 10): **192.168.10.0/24**
- Students VLAN (VLAN 20): **10.10.0.0/20**
- Servers VLAN (VLAN 30): **192.168.20.0/26**

- Library VLAN (VLAN 40): **192.168.30.0/26**
- Wireless VLAN (VLAN 50): **172.16.20.0/26**
- Lecturers VLAN (VLAN 60): **192.168.0.0/24**

We now deploy switches with OSPF for dynamic routing between VLANs.

OSPF, or Open Shortest Path First, is a routing protocol used in Internet Protocol (IP) networks. It's designed to find the best path for data packets to travel across a network. OSPF is an interior gateway protocol (IGP), which means it's used within a single autonomous system (AS).

Step by step Procedure

1. **Enable routing:** If you are using a layer 3 switch, ensure that routing is enabled on the switch using this command; **Switch(config)# ip routing**
2. **Configure VLAN Interfaces (SVIs)**
   Now configure the IP address for each VLAN interface. Each interface corresponds to a VLAN and will be used for routing between VLANs.

```
Switch(config)# interface vlan 10
Switch(config-if)# ip address 192.168.10.1 255.255.255.0  ! Admin VLAN
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface vlan 20
Switch(config-if)# ip address 10.10.0.1 255.255.240.0  ! Students VLAN
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface vlan 30
Switch(config-if)# ip address 192.168.20.1 255.255.255.192  ! Servers VLAN
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface vlan 40
Switch(config-if)# ip address 192.168.30.1 255.255.255.192 ! Library VLAN
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface vlan 50
Switch(config-if)# ip address 172.16.20.1 255.255.255.192  ! Wireless VLAN
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface vlan 60
Switch(config-if)# ip address 192.168.0.1 255.255.255.0 ! Lecturers VLAN
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Figure 5. 5: A snapshot showing IP address configuration for each VLAN interface

3. **Verify VLAN Interface Configuration**

   Once the VLAN interfaces are configured with their respective IP addresses, you can verify the configuration using this command: **Switch# show ip interface brief**

4. **Enable Routing Between VLANs (Inter-VLAN Routing)**

   Using a Layer 3 switch, the routing will be enabled as long as **ip routing** is configured. For the various VLANs to access the internet, we setup a gateway of last resort using this command: **Switch(config)# ip route 0.0.0.0 0.0.0.0 <next-hop-ip>**

5. **Save Configuration**

   To save the configuration so that it persists after a reboot, use the following command: **Switch# copy running-config startup-config**

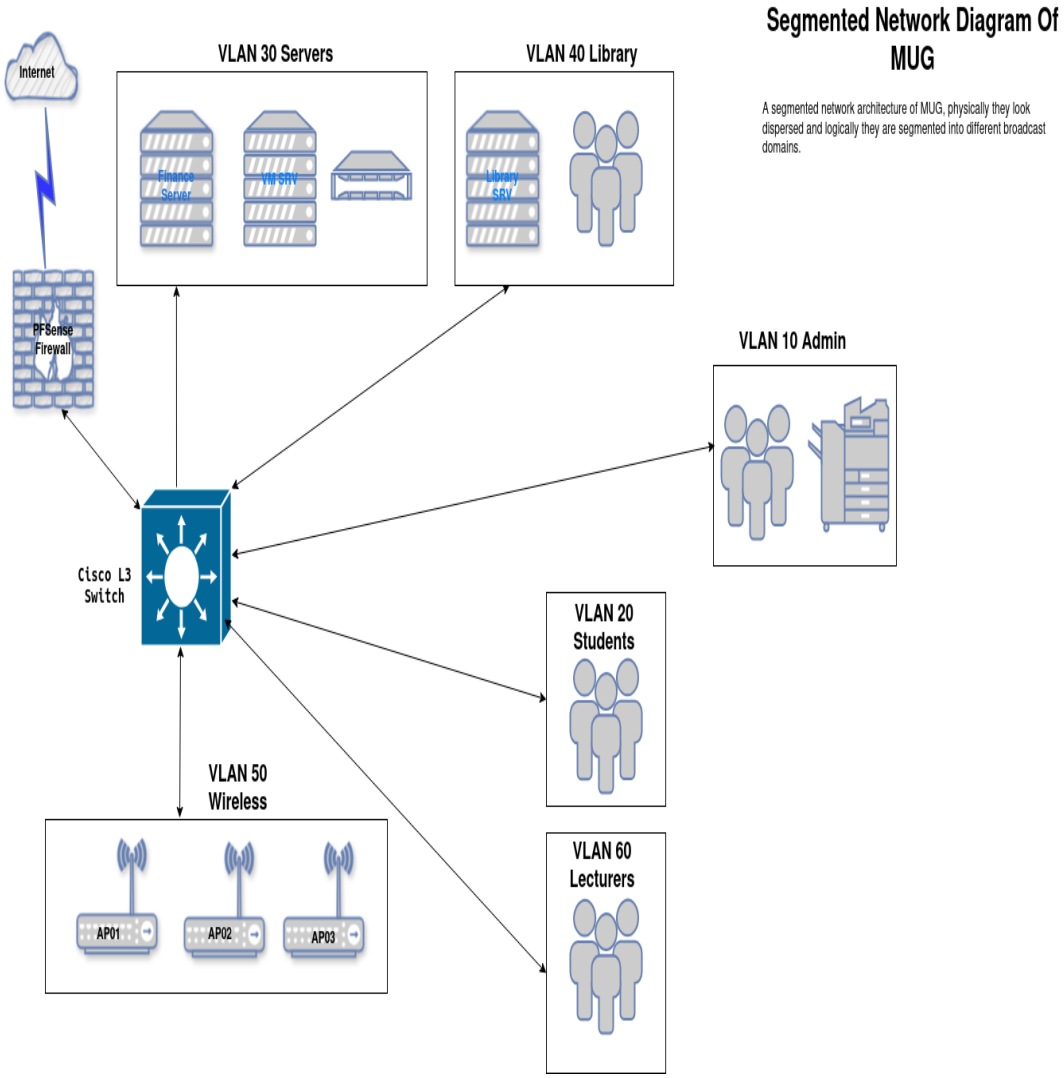

Figure 5. 6: A Hierarchical Network Architecture Post Segmentation

5.1.4 LAYER 4 – 7(TRANSPORT TO APPLICATION LAYERS)

The upper layers of the OSI model mostly deals with applications. Thus we will setup and implement a RADIUS server. The setup includes the following:

- **Ubuntu Linux Server 22.04**
- **FreeRADIUS**
- **daloRADIUS**

FreeRADIUS is an open source, high performance, modular, scalable, and feature rich RADIUS server. It ships with both server and radius clients, developments libraries, and numerous additional RADIUS related utilities.

It supports request proxying, with fail-over and load balancing, as well as the ability to access many types of backend databases.

RADIUS, which stands For: Remote **Authentication Dial-In User Service**", is a network protocol used for remote user authentication and accounting. It provide AAA services; namely **Authorization**, **Authentication**, and **Accounting.**

On the other side, **daloRADIUS** is an advanced RADIUS web management platform written in PHP and JavaScript. It is mainly aimed at managing Hotspots and general purpose ISP deployments powered by the **FreeRADIUS** server.
Some good features of **daloRADIUS** include:

- Has a database abstraction layer with support for many database systems; MySQL, SQLite, PostgreSQL, MsSQL and Oracle.
- Advanced User Management
- Powerful graphical reporting and accounting.
- Has a billing engine

Step by step Procedure

Step 1: Install Ubuntu Server

1. Begin by downloading the latest version of Ubuntu Server from the official website. Ensure you select the 64-bit version for better performance.
2. Create a bootable USB drive or use an installation disc to install Ubuntu Server on your designated machine or in this case an ISO file for installation on a virtual machine.

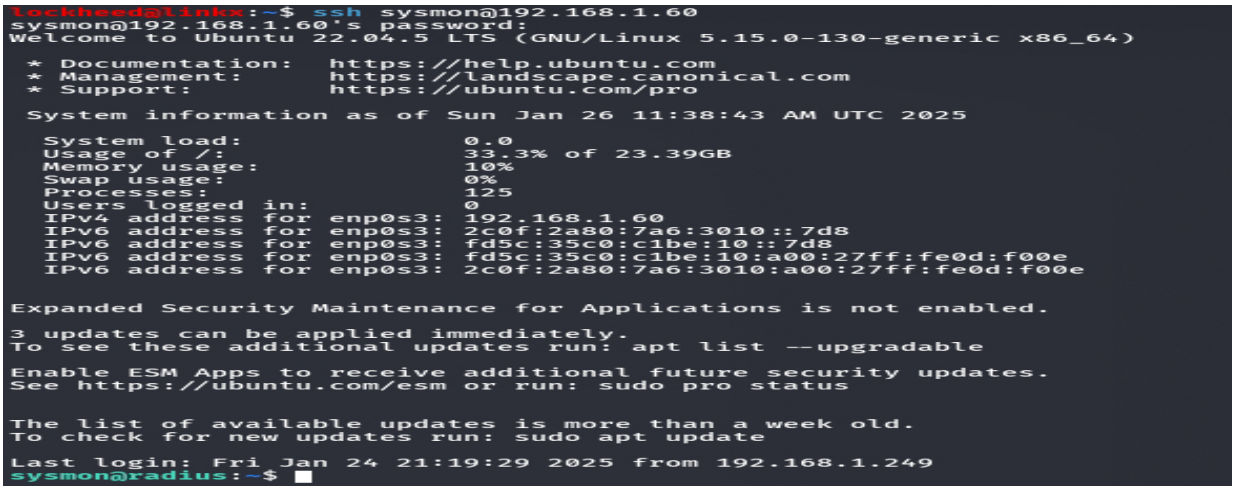

Figure 5. 7: A Snapshot showing the Ubuntu Server being startup after installation

Step 2: Update System

1. After installing Ubuntu Server, update the system to ensure al packages are current:
   sudo apt update && sudo apt -y upgrade

2. Reboot the system if required updates indicate a reboot is necessary:
   sudo [-f /var/run/reboot-required] && reboot –f

Step 3: Install Apache and PHP

1. Install the Apache web server to host the daloRADIUS interface:
   sudo apt -y install apache2

2. Install PHP and related modules required for daloRADIUS functionality:

sudo apt -y install vim php libapache2-mod-php php-{gd,common,mail,mail-mime,mysql,pear,db,mbstring,xml,curl,zip}

3. Verify the installed PHP version:
   php –v

Step 4: Install MariaDB and Create Database

1. Install MariaDB, a robust database management system:
   sudo apt update && sudo apt install mariadb-server

2. Log into the MariaDB shell as root:
   sudo mysql -u root –p

3. Create a new database named **radius** for FreeRADIUS.
   CREATE DATABASE radius;

4. Grant full privileges to the **radius** user with the password **MDSP@work2025:**
   GRANT ALL ON radius.* TO radius@localhost IDENTIFIED BY "MDSP@work2025";
   FLUSH PRIVILEGES;
   QUIT;

   Note: If using a dedicated database server, replace **localhost** with the IP address of the FreeRADIUS SERVER.

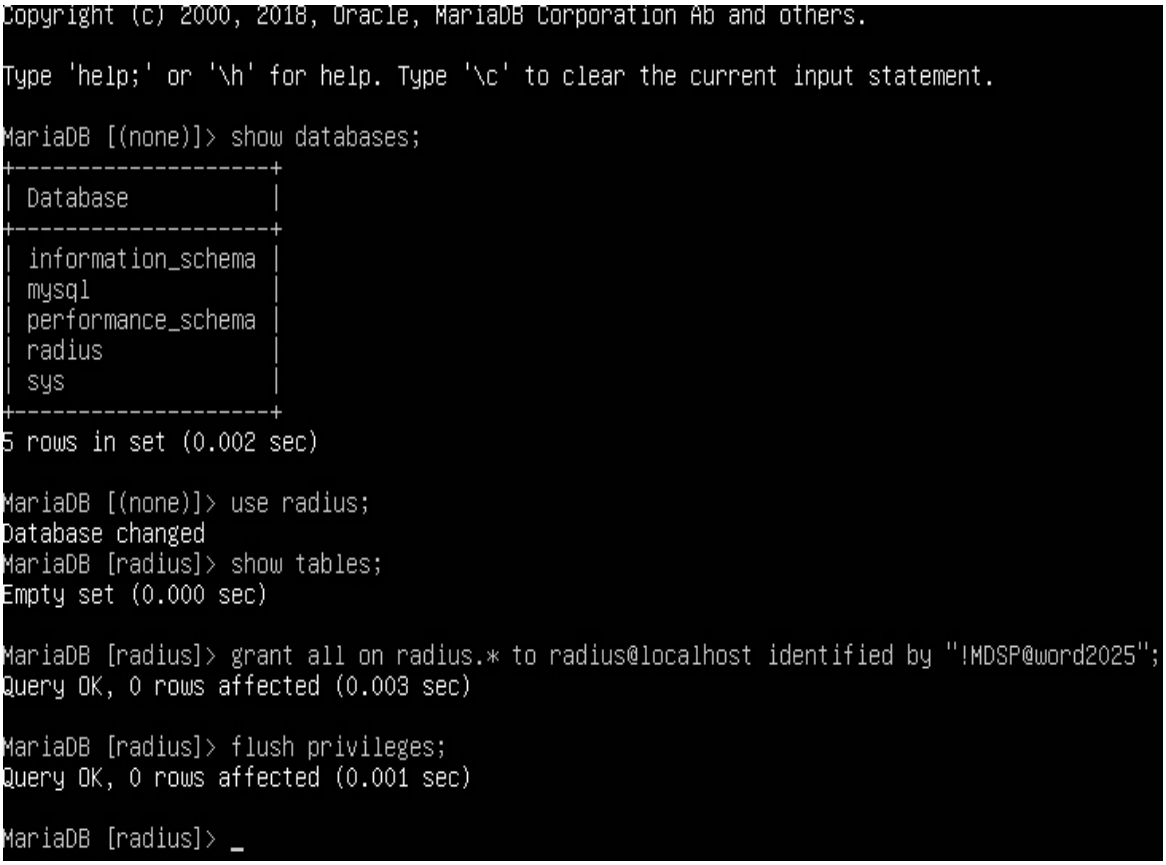

Figure 5.8: A snapshot displaying the MariaDB server

Step 5: Install and Configure FreeRADIUS

1. Install FreeRADIUS and its MySQL module:
   Install FreeRADIUS packages from official Ubuntu APT repository with commands below:
   Sudo apt –y install freeradius freeradius-mysql freeradius-utils
   Among the packages installed are **MySQL** module and **utils** package.

2. Import the FreeRADIUS MySQL database schema into the **radius** database.
   Sudo mysql –u root –p radius < /etc/freeradius/*/mods-config/sql/main/mysql/schema sql

3. Verify that the tables were created successfully:

Sudo mysql –u root –p –e”use radius;show tables;”

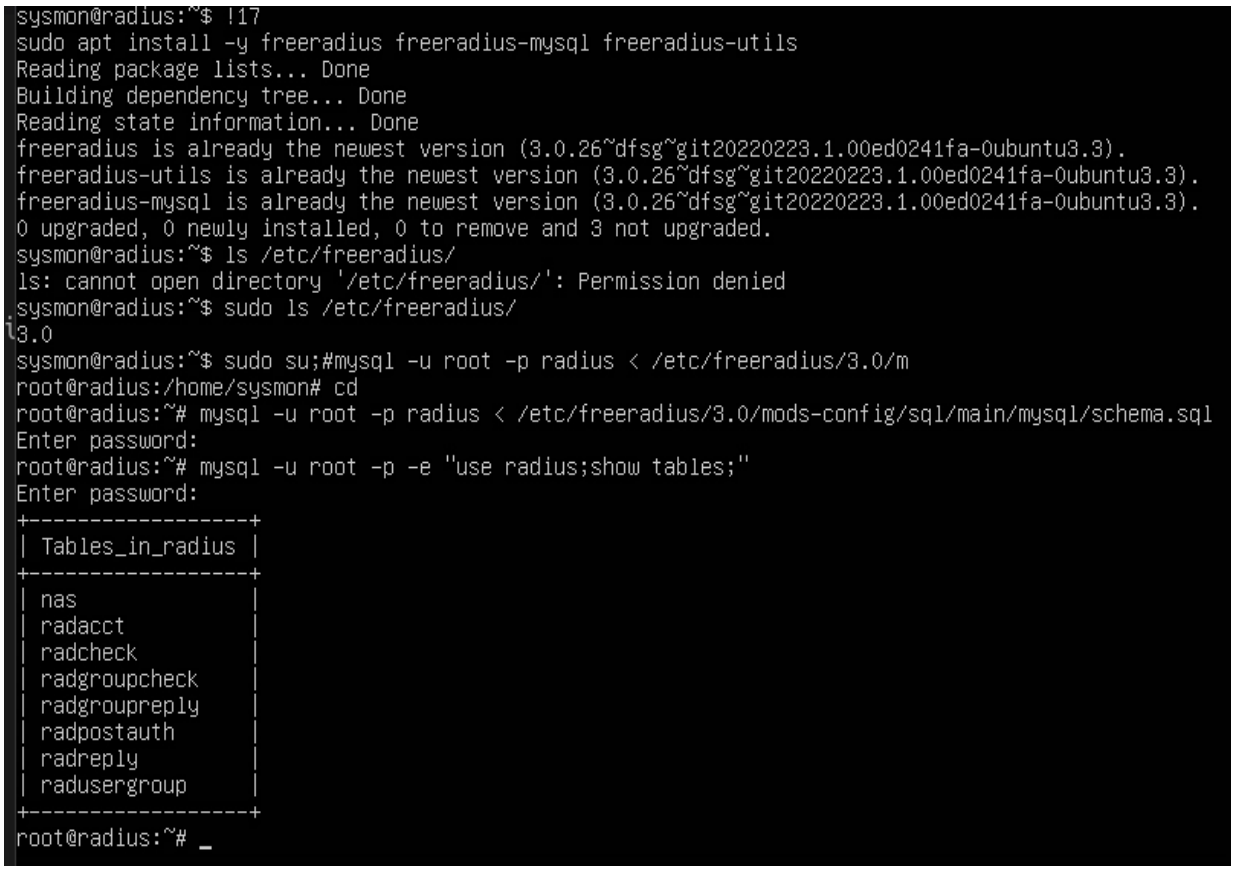

Figure 5. 9: A snapshot showing MySQL verification and FreeRADIUS installed

4. Create a syCreate a soft link for the SQL module in the **mods-enabled** directory:
   ln -s /etc/freeradius/*/mods-available/sql /etc/freeradius/*/mods-enabled/

5. Open the SQL configuration file for editing:
   nano /etc/freeradius/*/mods-enabled/sql

6. Modify the SQL section to include the following details

```
sql {
driver = "rlm_sql_mysql"
dialect = "mysql"

# Connection info:
server = "localhost"
port = 3306
login = "radius"
password = "MDSP@work2025"

# Database table configuration for everything except Oracle
radius_db = "radius"
}

# Set to 'yes' to read radius clients from the database ('nas' table)
# Clients will ONLY be read on server startup.
read_clients = yes

# Table to keep radius client info
client_table = "nas"
```

Figure 5. 10: A snapshot displaying the modified SQL section

7. Comment out the SSL sections into the MySQL configuration if not needed:

```
        mysql {
                # If any of the files below are set, TLS encryption is enabled
#               tls {
#                       ca_file = "/etc/ssl/certs/my_ca.crt"
#                       ca_path = "/etc/ssl/certs/"
#                       certificate_file = "/etc/ssl/certs/private/client.crt"
#                       private_key_file = "/etc/ssl/certs/private/client.key"
#                       cipher = "DHE-RSA-AES256-SHA:AES128-SHA"
#
#                       tls_required = yes
#                       tls_check_cert = no
#                       tls_check_cert_cn = no
#               }

                # If yes, (or auto and libmysqlclient reports warnings are
                # available), will retrieve and log additional warnings from
                # the server if an error has occured. Defaults to 'auto'
                warnings = auto
        }
```

Figure 5. 11: A snapshot displaying SQL Sections

8. Adjust group ownership and permissions for the SQL configuration files:
   chgrp -h freerad /etc/freeradius/*/mods-available/sql
   chown -R freerad:freerad /etc/freeradius/*/mods-enabled/sql

9. Restart the FreeRADIUS service to apply changes:
   systemctl restart freeradius.service

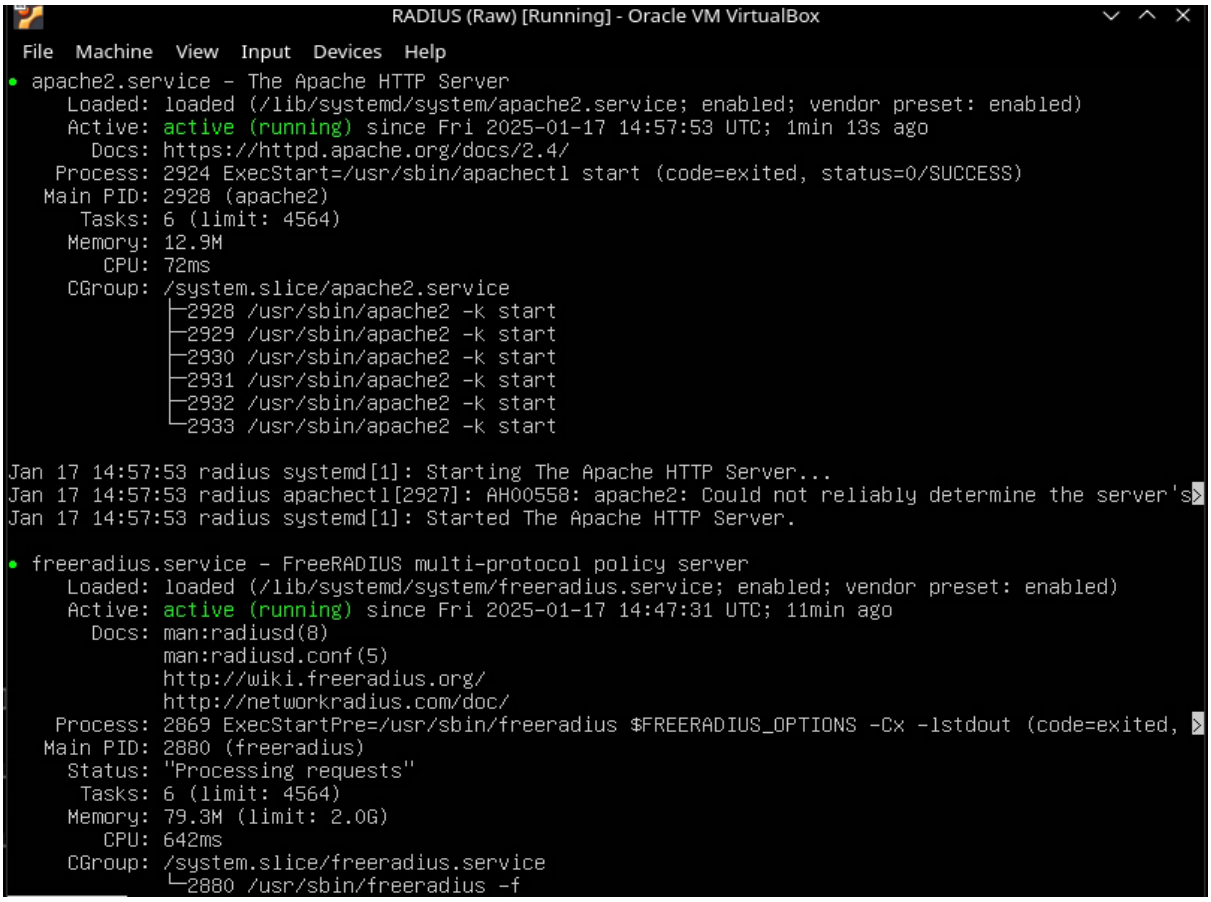

Figure 5. 12: A snapshot displaying the RADIUS server running

Step 6: Install and Configure daloRADIUS

1. Install Git to clone the daloRADIUS repository
   apt **-y install git**

2. Clone the daloRADIUS repository”

   git clone https://github.com/lirantal/daloradius.git

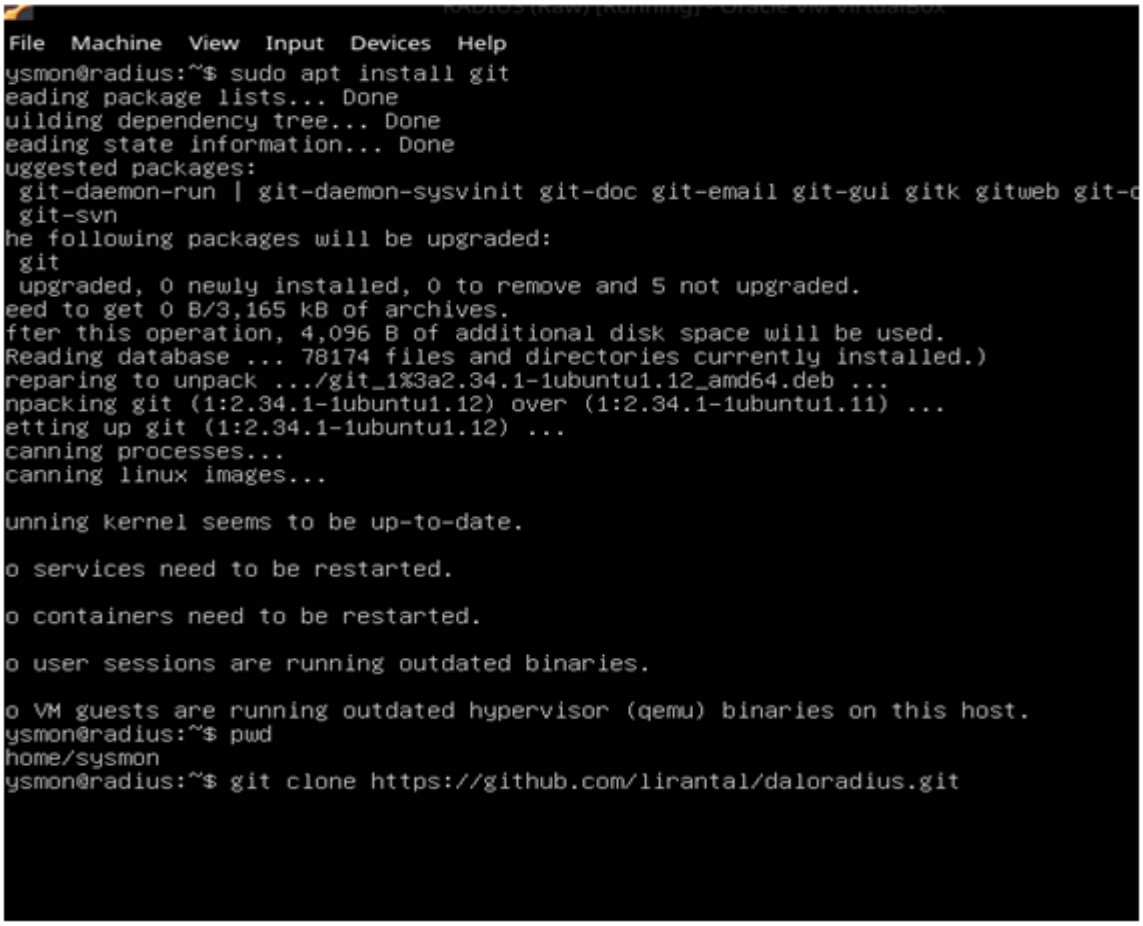

Figure 5. 13: A snapshot showing the commands above being run

3. Move the cloned folder to the **/var/www/** directory:

   mv daloradius /var/www/

4. Change the directory to the daloRADIUS configuration folder:

   cd /var/www/daloradius/app/common/includes/

5. Copy the sample configuration file and adjust its permissions:

   cp daloradius.conf.php.sample daloradius.conf.php

   chown www-data:www-data daloradius.conf.php

6. Edit the **daloradius.conf.php** file to configure database connection details:
   nano daloradius.conf.php

   Add the following details:
   $configValues['CONFIG_DB_HOST'] = "localhost";
   $configValues['CONFIG_DB_PORT'] = "3306";
   $configValues['CONFIG_DB_USER'] = "radius";
   $configValues['CONFIG_DB_PASS'] = "MDSP@work2025";
   $configValues['CONFIG_DB_NAME'] = "radius";

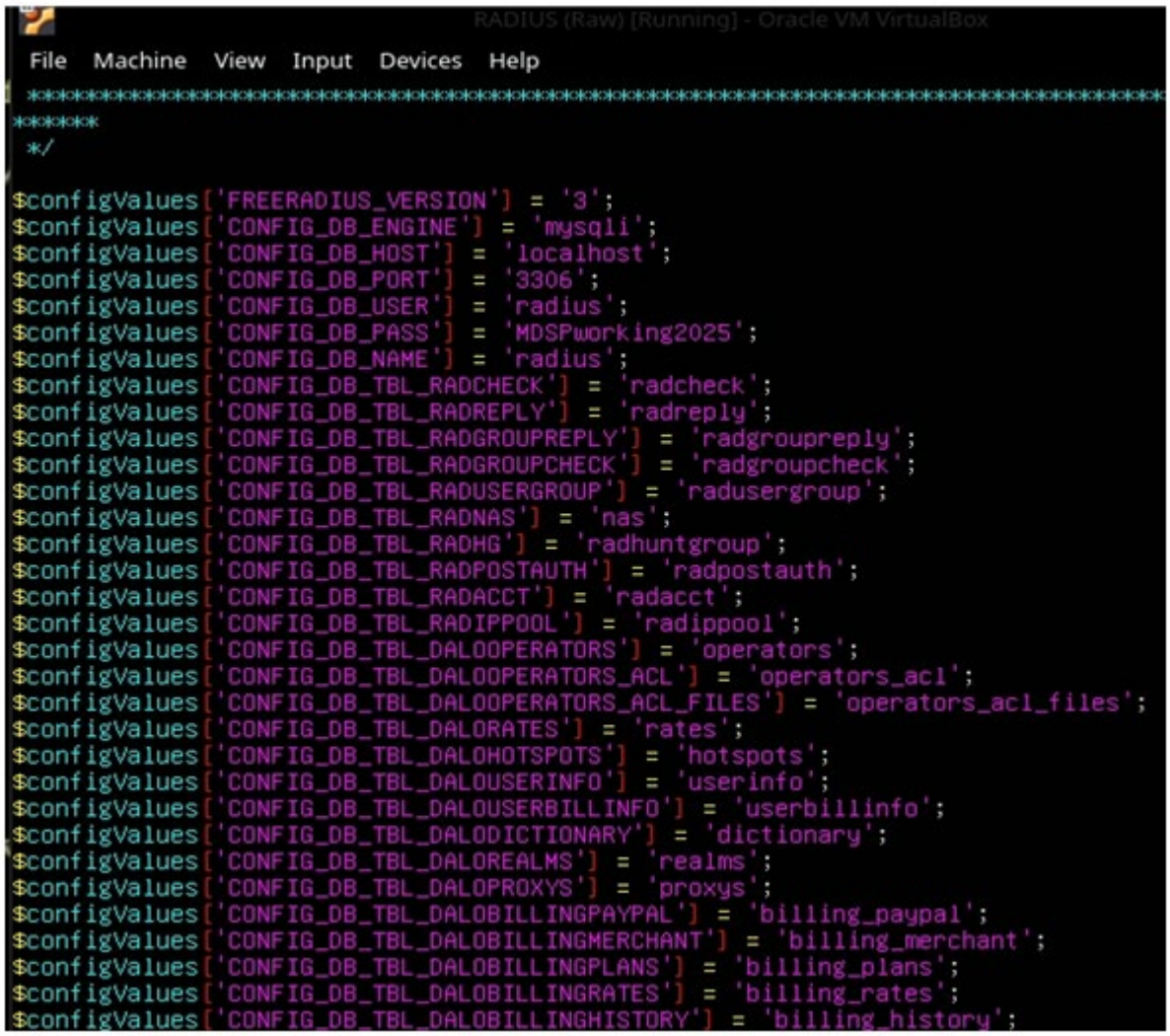

Figure 5. 14: A snapshot showing the modification of the daloradius.conf.php file to adjust the MySQL database information

Step 7: Import daloRADIUS Tables

1. Import the necessary MySQL tables for daloRADIUS:
   mysql -u root -p radius < /var/www/daloradius/contrib/db/fr3-mariadb-freeradius.sql
   mysql -u root -p radius < /var/www/daloradius/contrib/db/mariadb-daloradius.sql

Step 8: Setting up SSL Enable Management Portal

The setup of the SSL-enabled management portal for RADIUS was performed after configuring the RADIUS server itself because it ensures secure communication between users and the management interface, protecting sensitive data such as authentication credentials and configuration details.

- **RADIUS Server Configuration First** :
  - The primary goal of setting up the RADIUS server (FreeRADIUS) is to establish a robust framework for user authentication, authorization, and accounting (AAA services). This includes creating the database, importing schemas, and configuring SQL modules to manage client connections effectively.
  - Before enabling SSL, the core functionality of the RADIUS server must be operational. This ensures that all necessary components—such as the **radius** database, user tables, and authentication mechanisms—are properly configured and functional.

- **Security Layer Addition with SSL :**
  - Once the RADIUS server is operational, securing its management portal becomes critical. Without SSL, the web-based interface could expose sensitive information during transmission, making it vulnerable to interception or man-in-the-middle attacks.

- Enabling SSL/TLS encryption protects communications by encrypting data exchanged between the browser and the server. This aligns with best practices in network security, ensuring confidentiality and integrity.

- **Practical Workflow :**
  - Configuring SSL involves additional steps like generating certificates, modifying Apache settings, and updating permissions. Performing these tasks after the RADIUS server is fully functional simplifies troubleshooting. If something goes wrong during SSL setup, you can isolate the issue without affecting the core RADIUS service.
  - For example, if SSL configuration fails, the RADIUS server will still work correctly, allowing administrators to focus solely on resolving SSL-related issues.

- **User Experience and Security :**
  - After confirming the RADIUS server operates as intended, enabling SSL enhances the user experience by eliminating browser warnings about insecure connections. It also builds trust, especially when managing critical infrastructure like network access control.
- Tools like Ekahau or AirMagnet may require secure backends for optimal performance, which SSL

Thus, enabling **SSL** post-**RADIUS** setup ensures the solution is not only functional but also secure and reliable.

Step by step Procedure

Step 1: Create Subdirectories and Set Ownership

1. Navigate to the **daloradius** directory:
   cd /var/www/daloradius/

2. Create the required subdirectories (**log** and **backup**) under the **var** folder:
   mkdir –p var/{log,backup}

3. Change ownership of the **var** directory and its subdirectories to the **www-data** user and group , ensuring proper permissions for the web server:
   chown –R www-data:www-data var

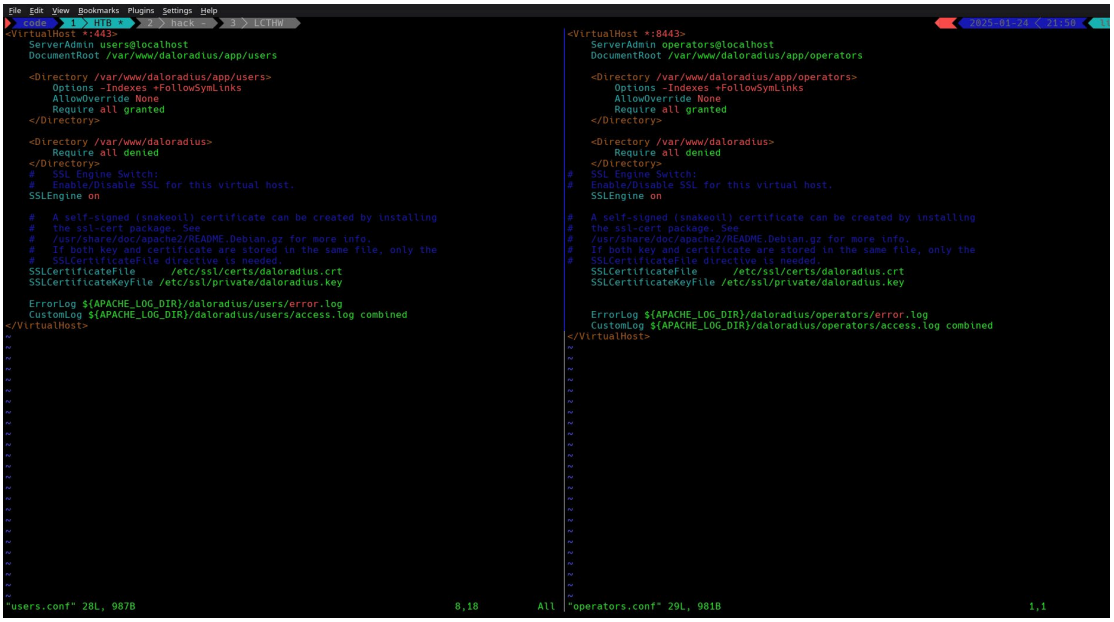

Figure 5. 15: A snapshot displaying SSL being enabled

Step 2: Configure Apache Web Server

1. Enable the virtual hosts created for the RADIUS management application:
   a2ensite users.conf operators.conf

2. Create additional directories for logging purposes:
   mkdir -p /var/log/apache2/daloradius/{operators,users}
   “These directories will store logs specific to the RADIUS application, helping with troubleshooting and monitoring.”

3. Disable the default Apache virtual host to avoid conflicts:

   a2dissite 000-default.conf

   "Disabling the default site ensures that only the configured RADIUS portals are accessible via the web server."

4. Restart both Apache and FreeRADIUS services to apply changes:

   systemctl restart apache2 freeradius

   "Restarting ensures all configurations take effect without requiring a system reboot."

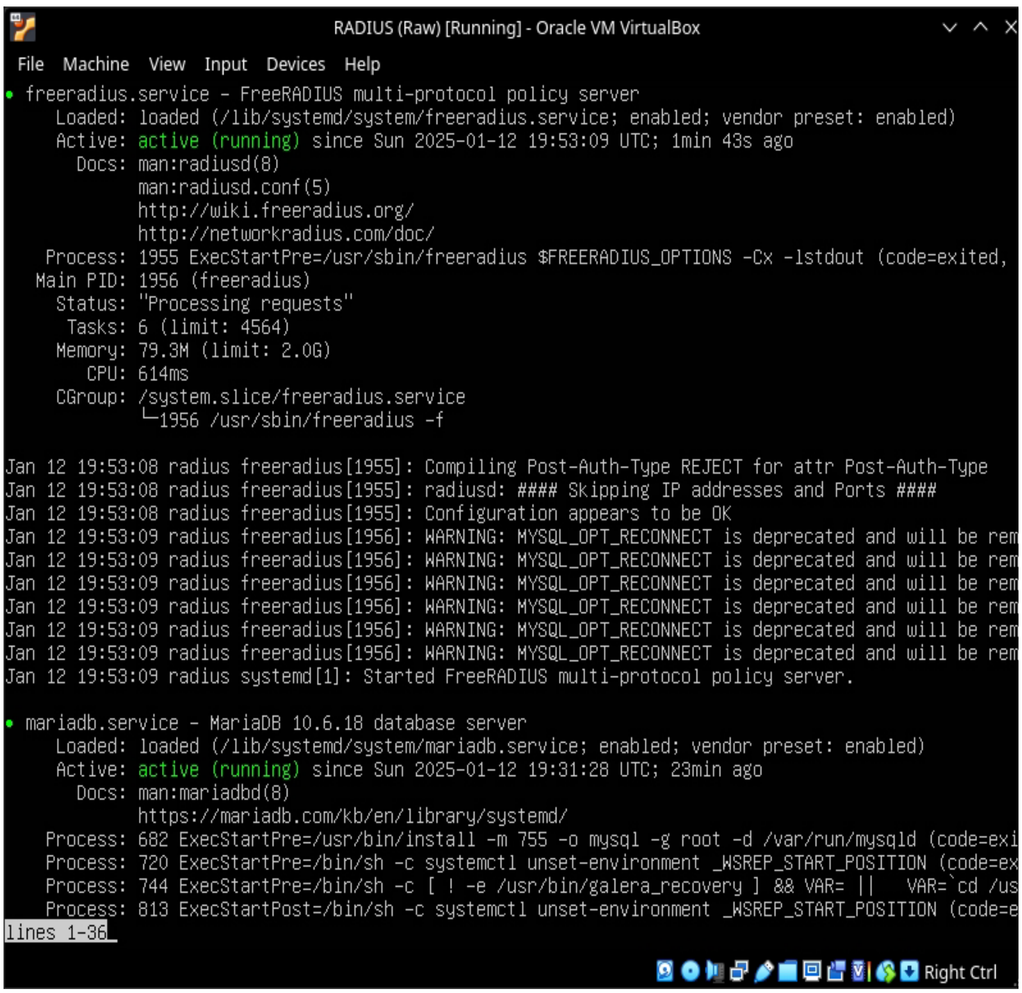

Figure 5. 16: A snapshot showing RADIUS server after configurations have taken effect

Step 3: Verify Service Accessibility

1. Access the RADIUS management application using the following URL:
   https://192.168.1.60:8443/
   "This URL provides administrative access to configure and manage the RADIUS server."

2. Access the RADIUS user portal application using the following URL:
   https://192.168.1.60
   "This URL allows end-users to authenticate and interact with the RADIUS server securely."

Step 4: Test Login Portal

1. Log in to the RADIUS management application portal using the credentials set during installation.

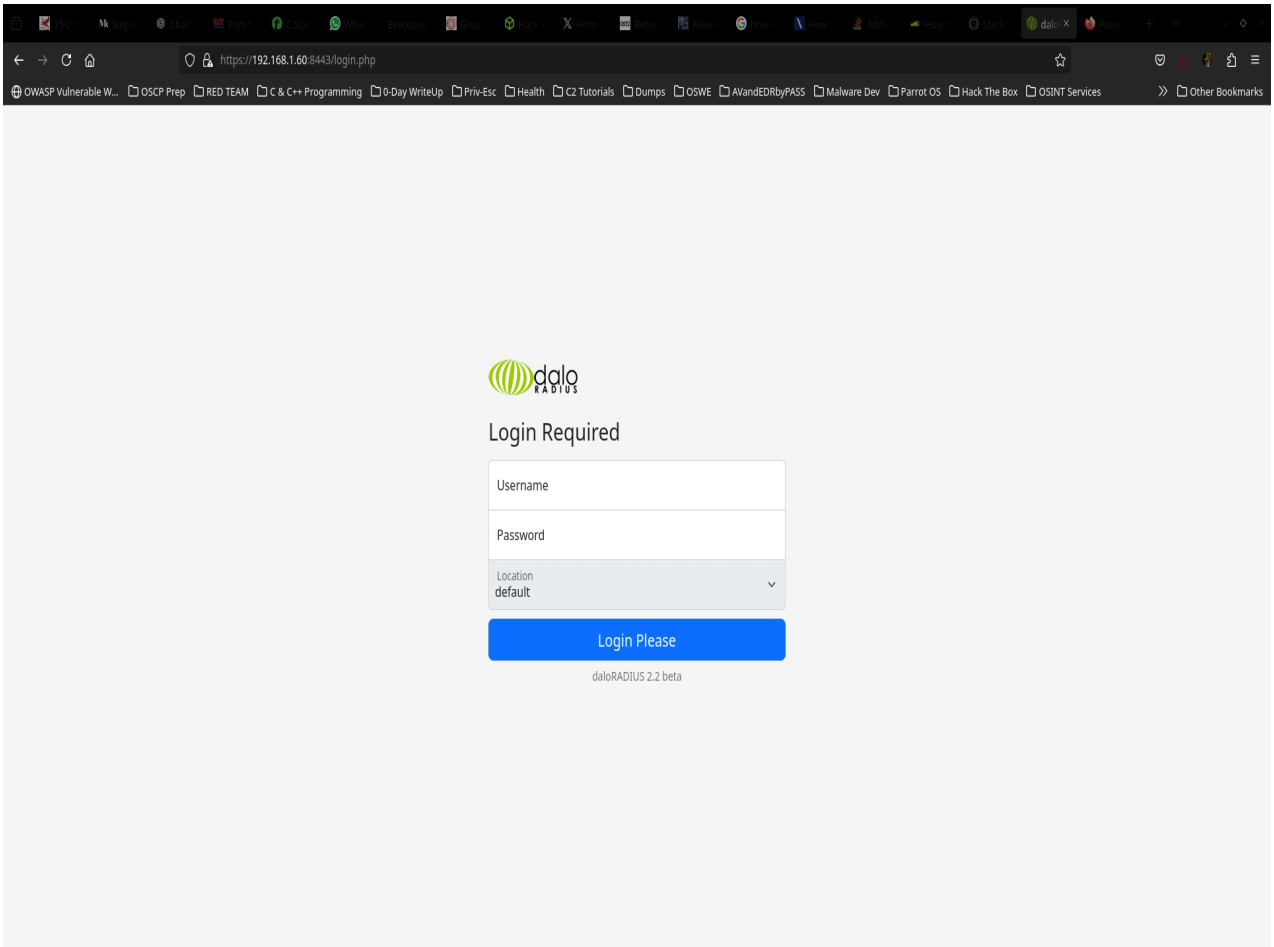

Figure 5. 17: RADIUS management application portal login page

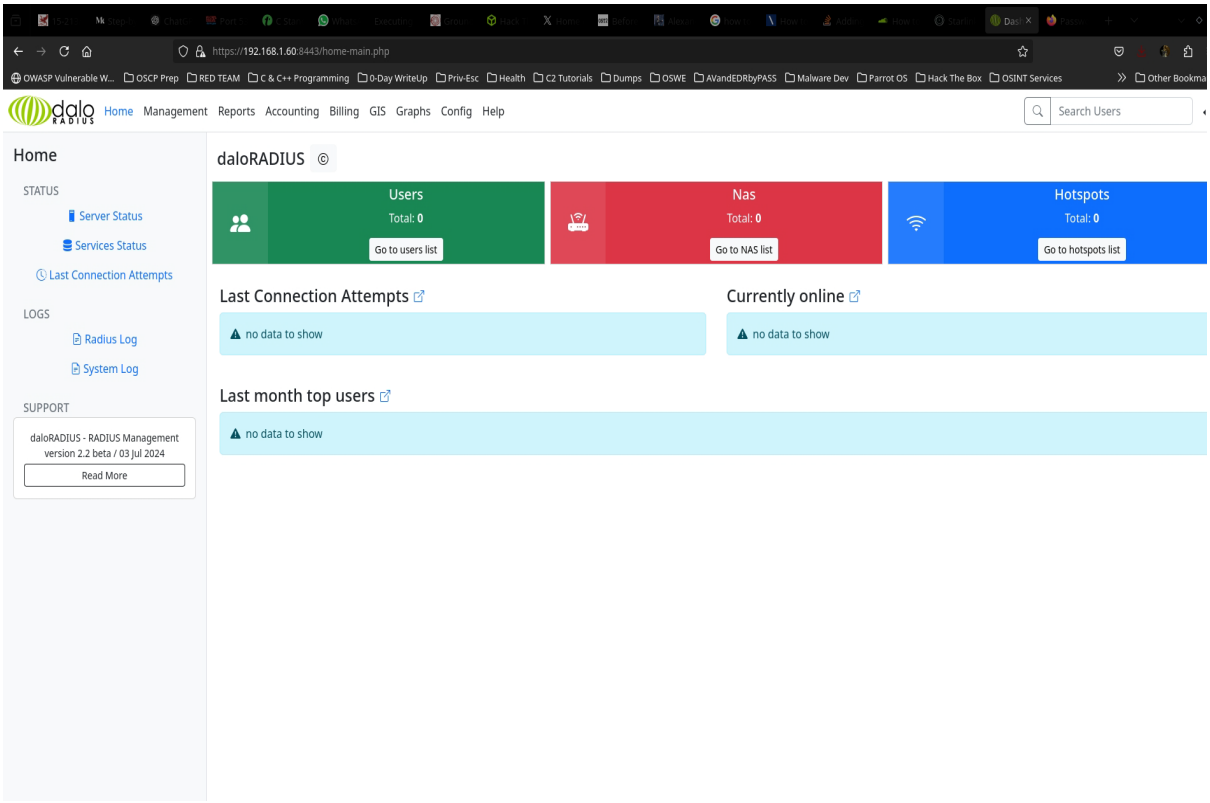

Figure 5. 18: Interface displaying options for managing users, configuring policies, and reviewing reports.

2. Verify the functionality of the CSV multiuser feature by creating sample user accounts.
    - Prepare a CSV file containing test user data (e.g., usernames, passwords, and attributes).

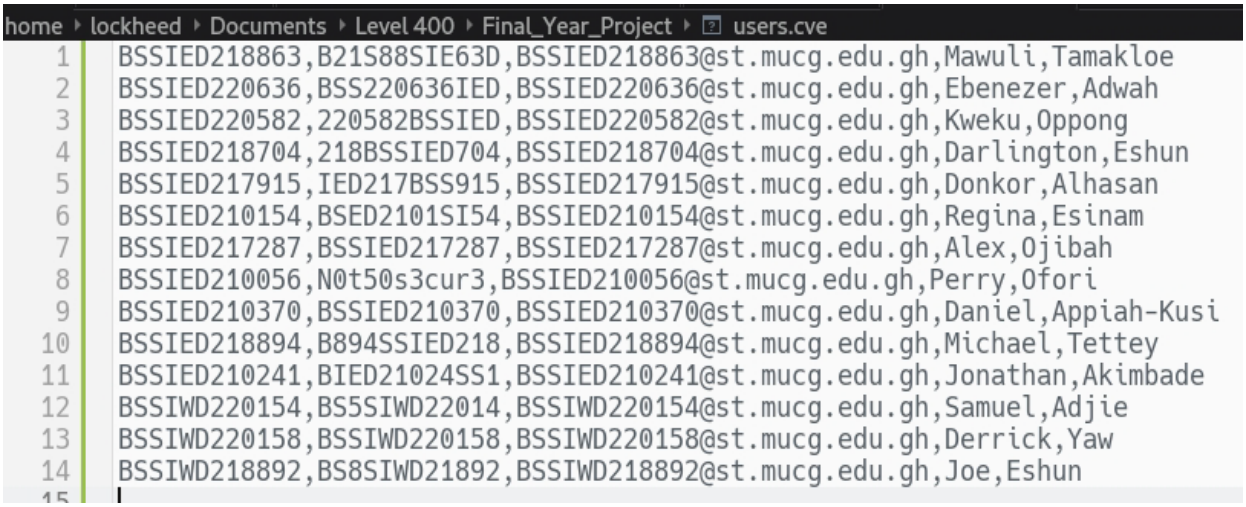

Figure 5. 19: CSV file containing Test Data

- Import the CSV file into the RADIUS server through the **daloRADIUS** web interface.

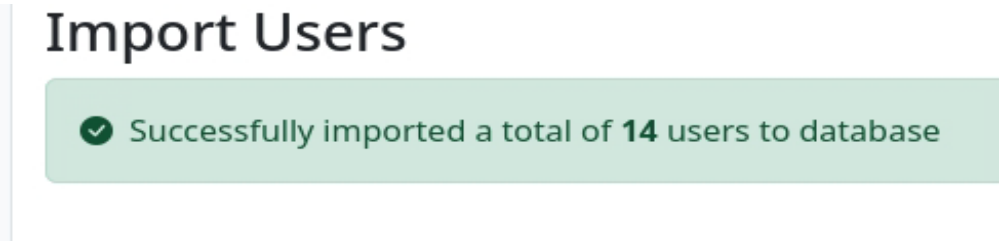

Figure 5. 20: Test Data CSV imported into RADIUS server through daloRADIUS

Step 5: Final Validation

1. Confirm that the SSL certificate is functioning correctly by checking for **HTTPs** encryption in the browser address bar when accessing either URLs.

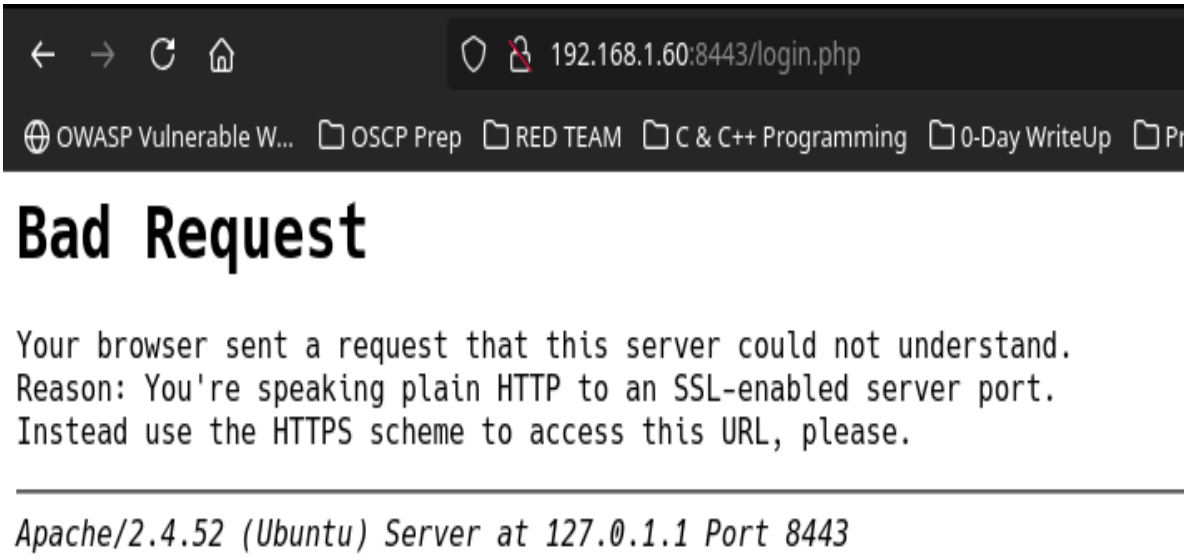

Figure 5. 21: SSL certificate working

2. Validate that both the management application and user portal are operational and responsive.

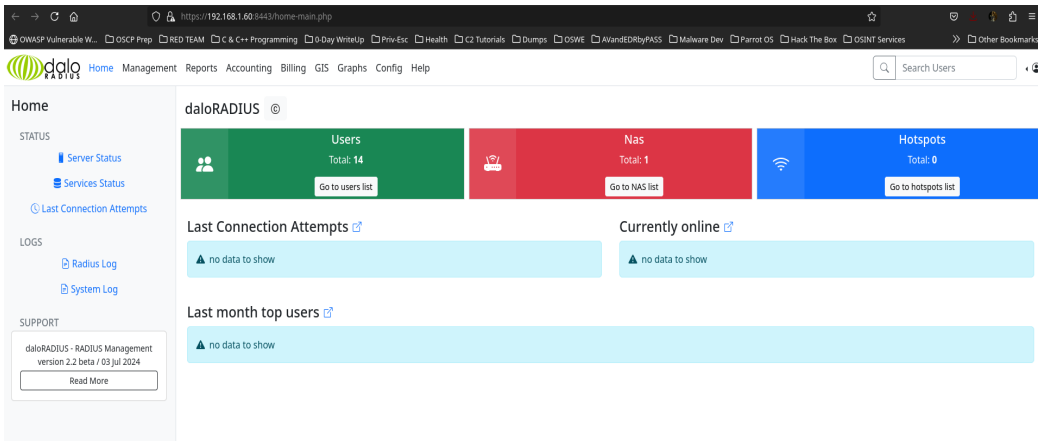

Figure 5. 22: RADIUS Management Portal

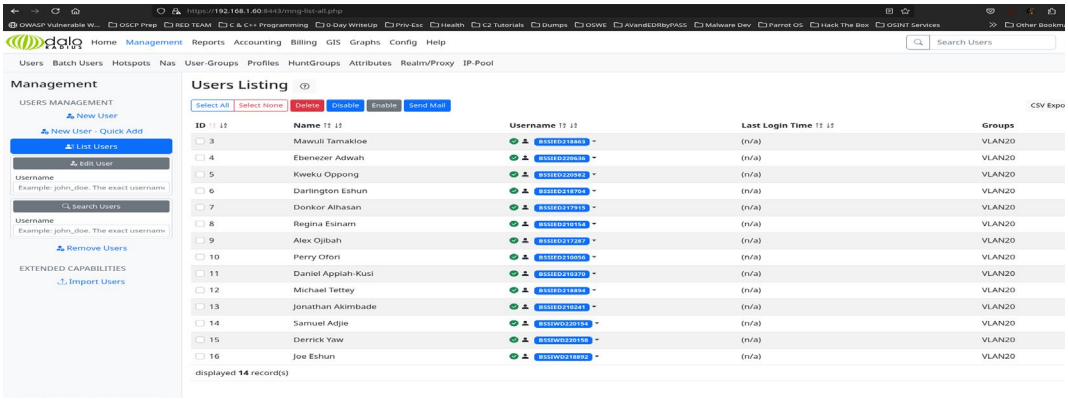

Figure 5. 23: A snapshot displaying imported users

5.2 TESTING AND VALIDATION

- **Penetration Testing:** Simulate attacks such as password harvesting and man in the middle scenarios to ensure robustness of the implemented security measures.
- **Load Testing:** Measure performance under high usage conditions to verify improvements in throughput and latency.
- **User Feedback:** Gather qualitative feedback from IT staff and end users regarding perceived changes in usability and security.

5.3 VALIDATION PROCEDURES

- **Security Validation:** Confirm that unauthorized devices cannot access the network post-RADIUS deployment. Validate against known vulnerabilities such as broadcasts storms and ARP poisoning.
- **Performance Metrics:** Compare pre-implementation and post-implementation data for metrics like bandwidth utilization, error rates and response times.
- **Configuration Verification:** Use commands like **show vlan brief** and **show ip interface brief** to ensure all configurations align with the proposed design.

5.4 SUCCESS CRITERIA

- **Reduction in Broadcast Traffic:** Achieve at least a 90% reduction in broadcast traffic, specifically ARP request, to mitigate broadcast storms.
- **Improved Security:** Eliminate unauthorized access attempts by enforcing strong encryption methods (e.g., WPA3) and centralized authentication through RADIUS.
- **Enhanced Performance:** Improve overall network reliability and reduce latency by optimizing VLAN configurations and IP address allocation

CHAPTER SIX

RESULTS

6.1 QUANTITATIVE AND QUALITATIVE DATA

The results presented in this section are based on the audit findings and feasibility analysis conducted during the project. While direct implementation on Methodist University Ghana's (MUG) live network was not feasible, the proposed solutions were tested in simulated environments using tools such as Virtual machines, Cisco Packet Tracer and Wireshark to predict their impact on performance and security.

6.1.1 QUANTITATIVE DATA

- **Broadcast Traffic Reduction:** Simulations indicate that segmenting the flat network into VLANs would reduce ARP broadcast traffic by approximately **90%**, significantly mitigating the risk of broadcast storms. The current network, with **99.2% ARP broadcasts** out of **1.5 million packets** captured, demonstrates a clear need for optimization.
- **IP Address Conservation:** Redesigning the IP subnet structure reduced the total usable IPs from **8190** to **4790, saving 3190 IPs** and minimizing unnecessary broadcast domains. This aligns with best practices for scalable network design.

6.1.2 QUALITATIVE DATA

- Feedback from IT staff and users during interviews revealed dissatisfaction with the current network setup due to slow speeds, frequent disconnections, and poor wireless coverage. These insights guided the development of practical solutions tailored to MUG's environment.
- Users expressed concerns about unauthorized access risks, emphasizing the importance of implementing robust authentication mechanisms like **RADIUS.**

6.2 USER FEEDBACK

Although the proposed solutions were not directly implemented on MUG's live network, qualitative feedback was gathered through surveys and interviews to validate their relevance and feasibility. Key highlights include:

- **University Personnel:** Agree that VLAN segmentation and inter-VLAN routing would improve manageability and reduce congestion. They noted challenges with isolating faults in the current flat architecture.
- **End Users:** Reported issues such as weak signals in lecture halls, computer laboratories, School Park, and libraries which aligns with the audit findings regarding improper **AP** placement and environment obstacles. Users also requested enhanced security measures to protect sensitive data.

DISCUSSION

7.1 INTERPRETATION OF RESULTS

The audit findings and simulation results demonstrate the potential effectiveness of the proposed solutions in addressing MUG's network infrastructure challenges:

- **Layer 1(Physical Layer):** Proper **AP** placement and channel planning would enhance wireless coverage and reduce dead zones caused by obstacles such as trees and concrete walls. Centralized AP positioning and tri-band support (2.4 GHz, 5GHz, and 6 GHz) would optimize signal strength and minimize interference.
- **Layer 2 (Data Link Layer):** Implementing VLANs would isolate traffic between departments, reducing broadcast domains and improving security, By eliminating the single broadcast domain, the risk of broadcast storms and unauthorized access would be mitigated.
- **Layer 3 (Network Layer):** Redesigning IP subnets and enabling OSPF-based dynamic routing would streamline traffic flow and improve scalability. Inter-VLAN routing ensures efficient communication while maintaining isolation between segments.
- **Upper Layers (4-7):** Deploying **FreeRADIUS** and **daloRADIUS** would enforce AAA policies, securing user authentication and accounting processes. This addresses vulnerabilities at higher OSI layers, protecting against password harvesting and man in the middle attacks.

7.2 IMPLICATIONS

The implications of these findings extend beyond immediate improvements to the university's network infrastructure:

- **Enhanced Security:** A secure authentication framework reduces the likelihood of unauthorized access and data breaches, safeguarding both institutional and personal information.
- **Improved Performance:** Optimized VLAN configurations, IP redesigns, and routing protocols ensure faster, more reliable connectivity, particularly in high density areas like lecture halls and libraries.

- **Scalability:** The hierarchical architecture supports future growth, allowing seamless addition of devices or expansion of network capacity without compromising performance or security.

7.3 LIMITATIONS

Several limitations must be acknowledged:

- **Simulation Constraints:** Testing was performed in simulated environments rather than on MUG's live network, meaning real-world results may vary slightly. However, simulations closely replicate expected outcomes under controlled conditions.
- **Resource Availability:** Budgetary and technical expertise limitations restricted the scope of hardware upgrades or extensive stakeholder engagement. Future implementations should consider additional resources if available.
- **Time Constraints:** Limited time affected the depth of testing and validation, though iterative improvements via the agile methodology ensured thorough planning.

CONCLUSIONS AND RECOMMENDATIONS

8.1 CONCLUSIONS

The project titled "Optimizing Network Infrastructure (with its inherent) Security: Analyzing and Implementing a Hierarchical Network Architecture for MUG (Methodist University Ghana)" aimed to address critical issues in the university's network infrastructure using a bottom-up approach based on the Open Systems Interconnection (OSI) model.

The findings of this study are summarized below:

- **Layer 1 (Physical Layer) :**
  Improper placement of wireless access points (AP's), particularly ceiling-mounted units positioned vertically instead of horizontally, significantly reduced signal coverage and created dead zones across campus. Environmental factors such as concrete walls, metallic surfaces, and trees further degraded signal quality. Addressing these physical layer issues is essential for improving connectivity and user experience.

- **Layer 2 (Data Link Layer) :**
  A flat, non-segmented network architecture exposed MUG to severe security risks, including unauthorized access and broadcast storms. Out of over 1.5 million packets captured, 99.2% were ARP broadcasts, indicating excessive congestion and potential performance degradation .VLAN segmentation would effectively reduce broadcast domains and enhance both security and efficiency.

- **Layer 3 (Network Layer) :**
  The current IP subnet design yielded 8190 usable IPs, far exceeding actual requirements and contributing to unnecessary broadcast traffic. Redesigning the IP structure into smaller subnets (e.g., /24, /26) would save 3400 IPs and minimize broadcast overhead, aligning with best practices outlined in existing literature.

- **Upper Layers (4–7) :**
  At higher OSI layers, the absence of robust authentication mechanisms left applications vulnerable to attacks such as password harvesting and man-in-the-middle scenarios.

Implementing a RADIUS server via FreeRADIUS and daloRADIUS would enforce AAA policies, ensuring secure access control and protecting sensitive data.

Through simulations and analysis, it was demonstrated that the proposed solutions; VLAN segmentation, IP redesign, and RADIUS deployment would significantly improve MUG's network performance, reliability, and security.

These enhancements align with industry standards such as IEEE 802.11 for wireless networking and RFC 2865 for RADIUS implementation. Furthermore, adhering to frameworks like NIST Cybersecurity Framework and ISO/IEC 27001 ensures compliance with global best practices.

This project serves as a practical example of applying hierarchical network architecture principles to optimize an educational institution's infrastructure under resource constraints. It highlights the importance of structured planning and simulation-based testing before live implementation.

8.2. RECOMMENDATIONS

Based on the audit findings and feasibility analysis, the following recommendations are made for Methodist University Ghana (MUG) and similar institutions:

8.2.1 SHORT-TERM IMPLEMENTATIONS

- **Wireless AP Optimization :**

  Conduct comprehensive site surveys to reassess AP placements, ensuring proper alignment (horizontal) for optimal signal range. Tools like Ekahau or AirMagnet can assist in identifying ideal locations and channel configurations.

  Avoid placing APs near obstacles such as thick walls or metallic surfaces, which cause significant attenuation and interference.

- **VLAN Segmentation :**

  Divide the flat network into six distinct VLANs: Admin (192.168.10.0/24), Students (10.10.0.0/20), Servers (192.168.20.0/26), Library (192.168.30.0/26), Wireless (172.16.20.0/26), and Lecturers (192.168.0.0/24). This reduces broadcast domains and isolates traffic between departments, improving both security and efficiency.

- **IP Redesign :**

  Redistribute IP subnets to conserve resources and minimize broadcast traffic. For instance, allocate smaller subnets (/24, /26) for specific departments instead of relying on a single /19 subnet. Ensure inter-VLAN routing is enabled on Layer 3 switches to facilitate seamless communication.

- **RADIUS Deployment :**

  Set up FreeRADIUS and daloRADIUS on a dedicated Ubuntu Server (22.04) to provide centralized authentication, authorization, and accounting (AAA) services. Secure the management portal with SSL/TLS encryption to protect sensitive credentials and configuration details.

8.2.2 LONG-TERM STRATEGIES

- **Dynamic Routing Protocols :**

  Deploy OSPF (Open Shortest Path First) for efficient routing between VLANs, reducing manual intervention and enhancing reachability. This aligns with modern approaches to dynamic network topology optimization.

- **Regular Audits and Maintenance :**

  Establish periodic audits and vulnerability assessments to identify emerging threats proactively. Continuous monitoring ensures rapid response to incidents and maintains long-term stability.

- **Staff Training :**

  Provide ongoing training sessions for IT personnel on advanced topics such as VLAN management, RADIUS deployment, and SDN principles. Empowering staff fosters smoother transitions during future upgrades.

- **Future Scalability :**

  Design the network with scalability in mind, allowing easy addition of devices or segments without major reconfigurations. Consider implementing Software-Defined Networking (SDN) to automate resource allocation and improve flexibility.

8.2.3 FUTURE RESEARCH DIRECTIONS

- **IoT Integration :**

  Investigate the integration of Internet of Things (IoT) devices into the network while maintaining security and performance. IoT adoption poses unique challenges due to increased device density and diverse communication needs.

- **Cloud Migration :**

  Study the feasibility of migrating certain services (e.g., email, file storage) to cloud platforms to reduce on-premises hardware dependencies and improve redundancy.

- **Advanced Security Measures :**

  Explore next-generation encryption methods (e.g., WPA3) and intrusion detection systems (IDS) to replace outdated protocols and ensure compliance with evolving cybersecurity standards.

By adopting these recommendations, MUG can transition its network infrastructure into a secure, high-performing system capable of supporting the institution's growing demands. Each suggestion is grounded in established best practices and tailored to address the unique challenges faced by the university. Additionally, this work contributes to broader discussions on optimizing network

infrastructure in African higher education institutions under budgetary and technical constraints, offering valuable insights for other organizations facing similar issues.

REFERENCES

Ali, M. N. B., Rahman, M. L., & Hossain, S. A. (2013). Network architecture and security issues in campus networks. 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), 1–9. https://doi.org/10.1109/ICCCNT.2013.6726595

Chidozie, O. K. (n.d.). Design and implementation of optimized features in a local area network for improved enterprise.

Creswell, J. W., & Plano Clark, V. L. (2017). Designing and conducting mixed methods research (3rd Ed.). SAGE Publications.

Kenyon, T. (2002). Data Networks: Routing, Security, and Performance Optimization. Elsevier.

Misuri, A., Khakzad, N., Reniers, G., & Cozzani, V. (2019). A Bayesian network methodology for optimal security management of critical infrastructures. *Reliability Engineering & System Safety*, *191*, 106112. https://doi.org/10.1016/j.ress.2018.03.028

Ranji, R., Javed, U., Boltjes, B., Bouhafs, F., & Den Hartog, F. (2023). Optimizing wireless network throughput under the condition of Physical Layer Security using Software-Defined Networking enabled collaboration. 2023 IEEE 20th Consumer Communications & Networking Conference (CCNC), 1–6. https://doi.org/10.1109/CCNC51644.2023.10060341

Rosak-Szyrocka, J. (2024). (PDF) The Era of Digitalization in Education where do Universities 4.0 Go? ResearchGate. https://doi.org/10.2478/mspe-2024-0006

Shafigh, A. S., Lorenzo, B., Glisic, S., Pérez-Romero, J., DaSilva, L. A., MacKenzie, A. B., & Röning, J. (2016). A Framework for Dynamic Network Architecture and Topology Optimization. IEEE/ACM Transactions on Networking, 24(2), 717–730. IEEE/ACM Transactions on Networking. https://doi.org/10.1109/TNET.2014.2383437

Sinha, P., Jha, V. K., Rai, A. K., & Bhushan, B. (2017). Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey. 2017 International Conference on Signal Processing and Communication (ICSPC), 288–293. https://doi.org/10.1109/CSPC.2017.8305855

Vanhoef, M., & Ronen, E. (2020). Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. IEEE Symposium on Security and Privacy https://eprint.iacr.org/2019/383.

Wong, A., & Yeung, A. (2009). Network Infrastructure Security. Springer Science & Business Media.

Zancan, C., Passador, J. L., & Passador, C. S. (2023). Optimizing network infrastructure for streamlined information technology execution in a Federal Higher Education Institution. International Journal of Scientific Management and Tourism, 9(4), 2128–2156. https://doi.org/10.55905/ijsmtv9n4-012

APPENDIX A: KEY COMMANDS

Table 9. 1: SUMMARY OF KEY COMMANDS

ACTION	COMMAND
Navigate to daloradius directory	**cd /var/www/daloradius/**
Create subdirectories	**mkdir -p var/{log,backup}**
Set ownership	**chown -R www-data:www-data var**
Enable virtual hosts	**a2ensite users.conf operators.conf**
Create log directories	**mkdir -p /var/log/apache2/daloradius/{operators,users}**
Disable default virtual host	**a2dissite 000-default.conf**
Restart services	**systemctl restart apache2 freeradius**
Update system	**sudo apt update && sudo apt -y upgrade**
Reboot system	**sudo [-f /var/run/reboot-required] && reboot -f**
Install Apache	**sudo apt -y install apache2**
Install PHP modules	**sudo apt -y install vim php libapache2-mod-php php-{gd,common,mail,...}**
Install MariaDB	**sudo apt update && sudo apt install mariadb-server**
Create Database	**CREATE DATABASE radius;**
Grant Privileges	**GRANT ALL ON radius.* TO radius@localhost IDENTIFIED BY "MDSP@work2025";**
Install FreeRADIUS	**sudo apt -y install freeradius freeradius-mysql freeradius-utils**
Import FreeRADIUS schema	**sudo mysql -u root -p radius < /etc/freeradius/*/mods-config/sql/main/mysql/schema.sql**
Check Tables created	**sudo mysql -u root -p -e "use radius; show tables;"**
Link SQL module	**ln -s /etc/freeradius/*/mods-available/sql /etc/freeradius/*/mods-enabled/**
Modify SQL Configuration File	**nano /etc/freeradius/*/mods-enabled/sql**

Change ownership of Config Files	**chown www-data:www-data daloradius.conf.php**