METHODIST UNIVERSITY GHANA

EXCELLENCE • MORALITY • SERVICE

16th June 2026

Supervisor: Dr. R.O. Sarkodie

PROJECT DEFENCE

OPTIMIZING NETWORK INFASTRUCTURE WITH ITS INHERENT SECURITY

Analyzing And Implementing A Hierarchical Network Architecture for MUG (Methodist University Ghana)

Presented By

TETTEY MICHAEL NII AYI	BSSI/ED/218894
OFORI DANIEL PERRY JNR	BSSI/ED/210056
IGWEBUIKE SOLOMON JNR	BSSI/ED/ 221348
ESHUN DARLINGTON EBENEZER	BSSI/ED/218704

Agenda

Introduction

A robust and reliable **network** is no longer a luxury but a fundamental necessity for **educational institutions**, underpining all aspects from **online learning** and **research** collaboration to daily administrative tasks.

At **Methodist University Ghana (MUG)**, the network's reliability, efficiency, and security directly influence the quality of **teaching**, the progress of **research**, and the effectiveness of day-to-day **operations.**

This project's primary aim was to analyze MUG's current network, identify key shortcomings, and implement a hierarchical network architecture to establish a significantly more reliable, efficient, and secure infrastructure.

Problem Domain

Problem Statement

Despite its crucial role, Methodist University Ghana's existing network infastructure faces significantly challenges that impede performance, compromise reliability, and expose critical security shortcomings.

Key Issues

Performance Impediments

Network congestion, slow speeds, and frequent disconnections impacting user experience.

Reliability Concerns

Inconsistent Wi-Fi access and network instability.

Security Vulnerabilities

Open wireless policies and lack of robust authentication exposing the network to significant risks.

Scalability Issues

Flat architecture struggling to meet growing university demands.

Problem Domain

Existing Network Analysis - Layer 1 & 2 Issues

Layer 1(Physical) - Suboptimal AP Placement

Finding

Improper AP mounting (vertical instead of horizontal) and environmental obstructions (trees, concrete walls).

Impact

Reduced wireless signal range, poor coverage, inconsistent Wi-Fi access.

Layer 2(Data Link) - Flat Architecture & Broadcast Storms

Finding

Operates as a single, flat broadcast domain.

Evidence

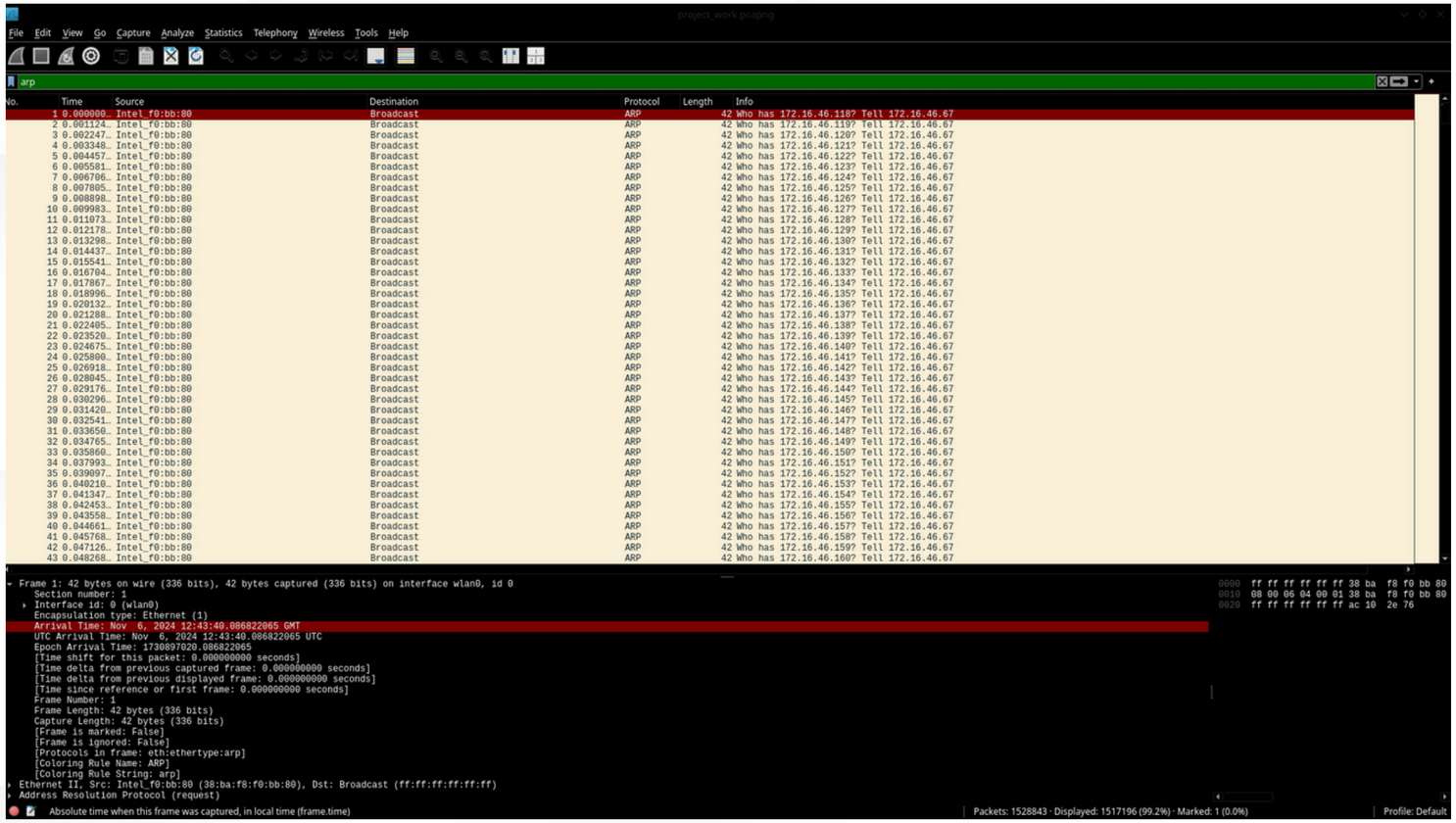
Excessive ARP broadcasts (99.2% of 1.5 million captured packets identified as ARP broadacasts

Impact

Severe network congestion, instability, reduced speeds, difficult to manage and scale

Problem Domain

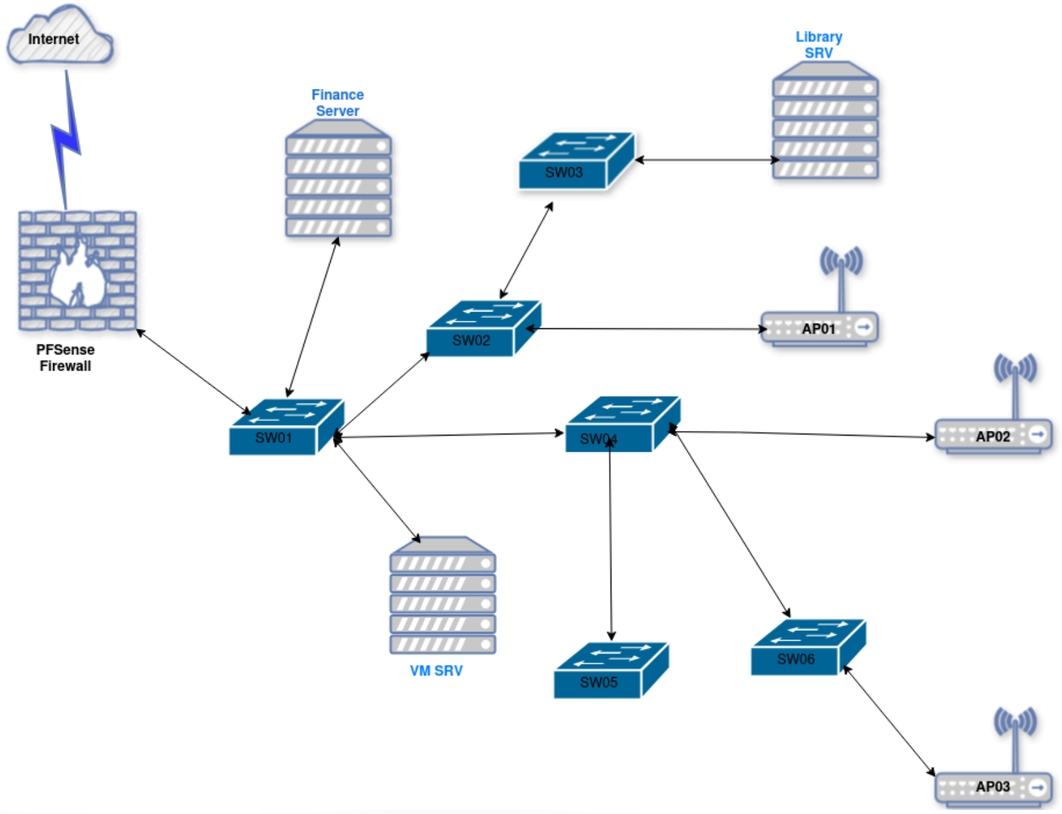
Existing Network Analysis - Layer 1 & 2 Issues



99.2% of 1.5 million captured packets identified as ARP broadcasts

Problem Domain

Existing Network Analysis - Layer 1 & 2 Issues

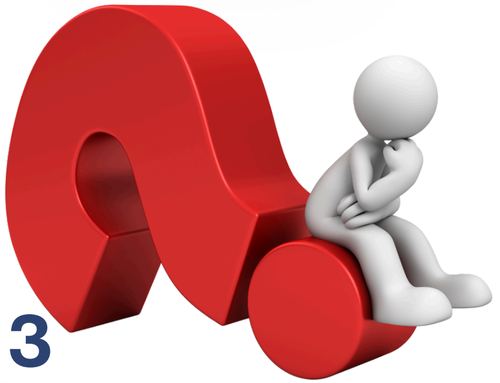


Flat Network Diagram Of MUG

The flat network architecture of MUG, physically they look dispersed but logically it's one big network inter-connected with switches and wireless AP's.

Flat network architecture of Methodist University Ghana. All devices share the same broadcast domain:192.168.0.0/19

Problem Domain



Existing Network Analysis - Layer 3 & Higher Layer Issues

Layer 3(Network) - IP Subnet Inefficiency

Finding

Current IP range 192.168.0.0/19 yielding 8190 usable IPs.

Problem

Grossly oversized for actual needs in a flat architecture, contributing to excessive broadcast traffic.

```
Address:   192.168.0.0          11000000.10101000.000 00000.00000000
Netmask:   255.255.224.0 = 19   11111111.11111111.111 00000.00000000
Wildcard:  0.0.31.255           00000000.00000000.000 11111.11111111
=>
Network:   192.168.0.0/19       11000000.10101000.000 00000.00000000
HostMin:   192.168.0.1          11000000.10101000.000 00000.00000001
HostMax:   192.168.31.254       11000000.10101000.000 11111.11111110
Broadcast: 192.168.31.255       11000000.10101000.000 11111.11111111
Hosts/Net: 8190                  Class C, Private Internet
```

Higher Layers(4-7) - Application Level & Security Concerns

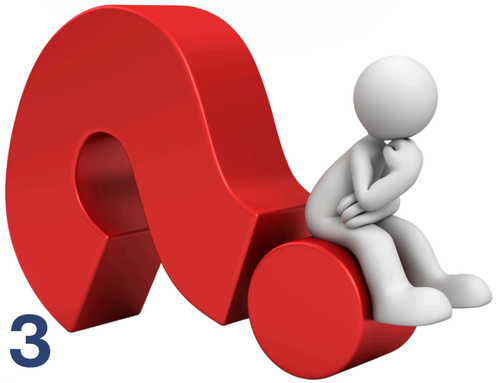
Finding

Absence of robust authentication mechanisms(No RADIUS server).

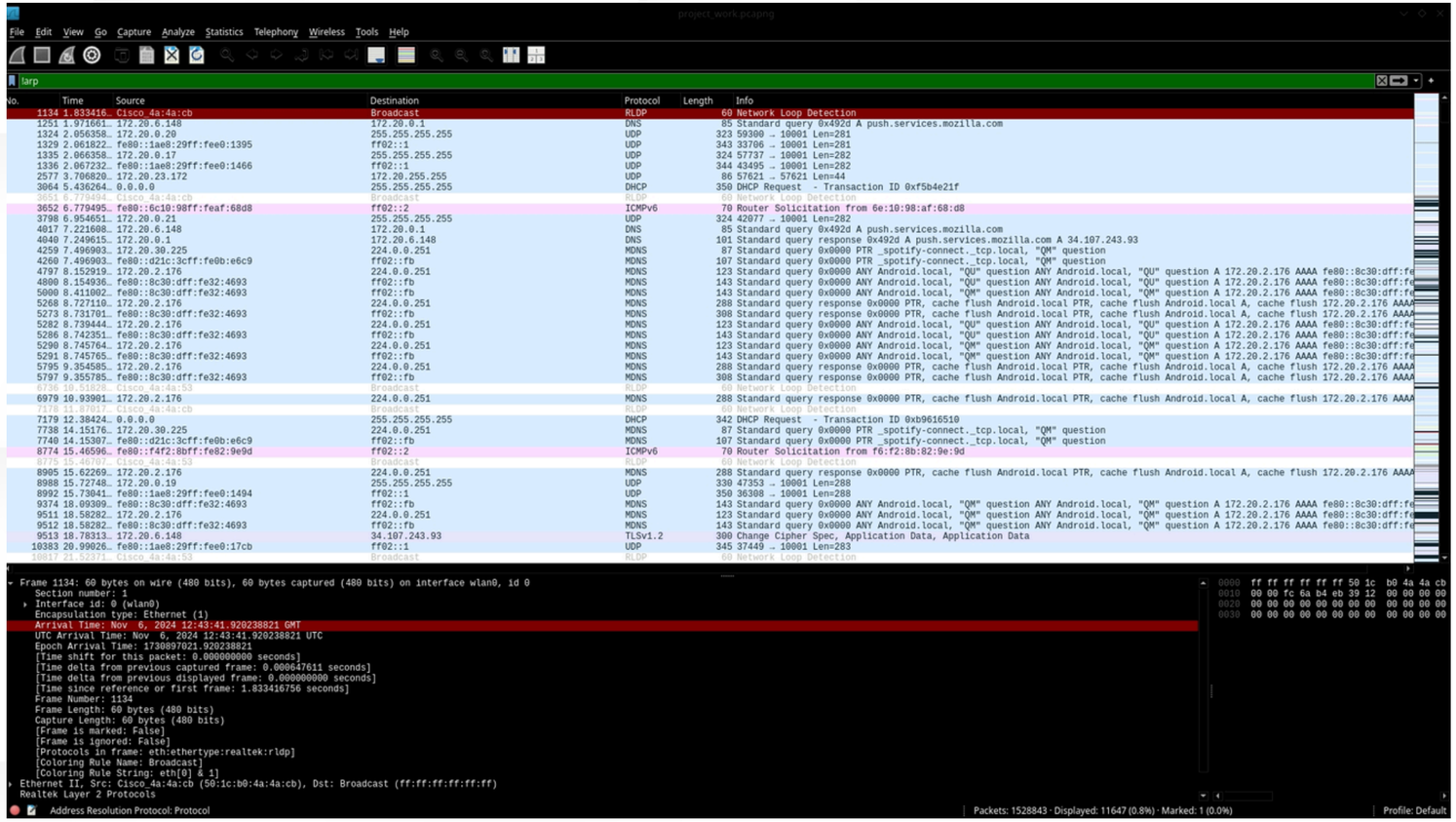
Impact

Applications vulnerable to unauthorized access; users exposed to password harvesting and ma-in-the-middle attacks.

Problem Domain

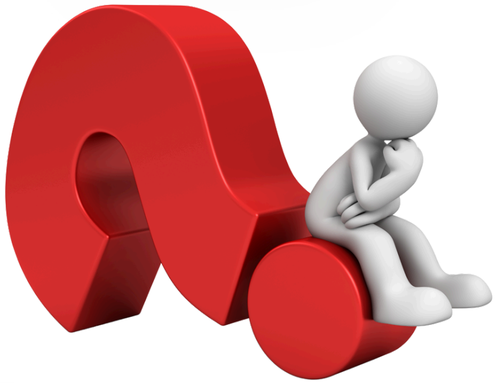


Existing Network Analysis - Layer 3 & Higher Layer Issues



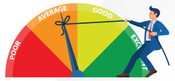
Unencyrpted sensitive DNS lookups that could be used by an attacker to inject viruses and backdoor on users of these devices.

Problem Domain



Impact Assessment Summary

These interconnected issues signficantly affect MUG's network across multiple fronts.



Performance Degradation

Excessive broadcast traffic consuming bandwidth.
Frequent disconnections in high-density areas (lecture halls, libraries, computer laboratory).

Scalability Limitations

Network unstainable for future growth due to increasing broadcast traffic.
Difficulty managing diverse user groups without segmentation.

Security Risks

Open wireless policies enabling unauthorized device connections.
Flat architecture allowing lateral movement for attackers.

Operational Challenges

Difficulties in fault isolation and targeted updates.

User dissatisfaction due to slow connections and outages.

Methodology

Objectives & Scope

General Objective

To address identified shortcomings in MUG’s existing network and establish a more reliable, efficient, and secure infrastructure through a hierarchical design.

Specific Objectives

- **To conduct a comprehensive network assessment using a bottom-up OSI model approach**
- **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.**

Methodology

Objectives & Scope

Project Scope

Focus

Internal MUG network infrastructure (wired and wireless aspects).

Implementation

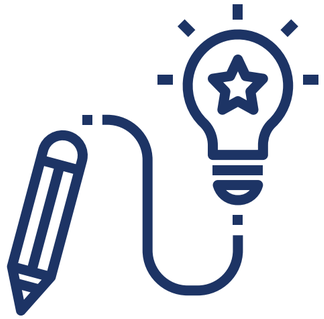
Logical configurations and optimizations (VLANs, IP redesign, RADIUS server setup).

Approach

Bottom-up analysis based on the OSI Model.

Constraints

No major hardware upgrades; primarily focused on optimizations achievable within existing (or minimal new) resources and budget; simulated testing due to live network access limitations.



Methodology

This project utilized a **Mixed Methods approach** within a **Pragmatic Research Paradigm**, focusing on practical outcomes.

A **bottom-up OSI Model assessment** provided a structured analysis of MUG's network infrastructure.

Data Collection Methods

Quantitative Approach

Primary Data

Site Surveys(Limited Scope)

Physical component reviews, layout determination.

Traffic Analysis & Documentation

Wireshark captures (with consent) for architecture and security risk identification.

Qualitative Approach

Primary Data

Stakeholder Engagement

Insights from the Head of the Multimedia Department and limited student interviews/surveys regarding network concerns.

Methodology

This project utilized a **Mixed Methods approach** within a **Pragmatic Research Paradigm**, focusing on practical outcomes.

A **bottom-up OSI Model assessment** provided a structured analysis of MUG's network infrastructure.

Data Collection Methods

Quantitative Approach

Secondary Data

Specifications of existing hardware

Hardware Specifications

Qualitative Approach

Secondary Data

Literature review

Hierarchical architectures, VLANs, RADIUS, existing MUG documentation where available

Methodology

Analysis & Validation Strategy

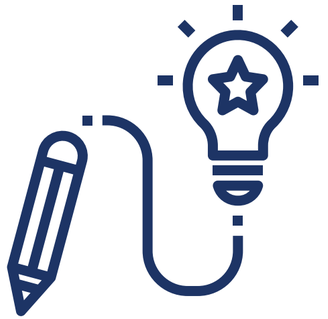
Packet Capture Analysis (Wireshark)

Understanding protocols, identifying security compromises, baseline network activity.

Configuration Testing (Simulated)

Tools: Virtual Machines (VMs).

Purpose: To model proposed changes (VLANs, IP schemes, RADIUS) and evaluate their impact on performance and security under various scenarios.



Due to live network access constraints, validation was primarily through simulation and qualitative feedback on proposed solutions, rather than live deployment testing.

Methodology

Project Management: Agile Framework

The Agile Model was implemented to streamline the optimization process, allowing for iterative development and flexibility.

PHASE	DURATION	ACTIVITIES
Audit & 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.

Methodology

Project Management: Agile Framework

Key Benefits

Flexibility

Adaptable to challenges in network optimization

Incremental Delivery

Conceptual components (VLANs, IP redesign, RADIUS) refined iteratively.

Proposed Solution

Transitioning from MUG’s existing flat network to a structured **Hierarchical Network Model.**

This industry-standard design separates the network into logical layers (Core, Distribution, Access).

Key Benefits of Hierarchical Design

Improved Performance

Efficient traffic flow, reduced congestion.

Enhanced Security

Better Isolation, controlled access.

Increased Scalability

Easier to expand and manage future growth

Simplified Management & Troubleshooting

Logical structure aids in fault isolation.

Proposed Solution

Solution Design - Layer 1 Enhancements

Addressing Suboptimal Wireless Access Point(AP) Placement

Key Benefits of Hierarchical Design

Strategic AP Placement

Centralized positioning in coverage areas, avoiding signal-blocking corners and walls.

Multi-Band & Channel Management

Utilizing both 2.4GHz & 5GHz bands(6 GHz for tri-band) with proper channel planning to reduce co-channel interference.

Interference Mitigation

Careful placement away from devices causing RF interference (microwaves, cordless phones).

Future Expansion Considerations

Designing wireless layout with future growth in mind for adding more devices/APs.

Regular Monitoring

Continuous performance checks and adjustments post-implementation.

Proposed Solution

Solution Design - Layer 2 Enhancements

Addressing Flat Network Architecture, Broadcast Storms, Lack of Segmentation

Key Action: VLAN (Virtual Local Area Network) Implementation

Dividing the flat network into **six distinct VLANs.**

Benefits

Reduces Broadcast Domains

Significantly mitigates risk of broadcast storms (addressing the 99.2% ARP issue).

Isolates Traffic

Enhances security by preventing direct communication between different user groups unless explicitly routed.

Improves Efficiency & Manageability

```
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
```

Proposed Solution

Solution Design - Layer 3 Enhancements

Addressing IP Subnet Inefficiency, Lack of Inter-Departmental Routing Control

Key Actions & Strategies

IP Subnet Redesign (VLSM)

Transitioned from inefficient /19 subnet.

Implemented Variable Length Subnet Masking (VLSM) to create appropriately sized subnets for each VLAN (e.g. /24 for Admin/Lecturers, /20 for Students, /26 for Servers/Wireless/Library)

Inter-VLAN routing & L3 Switching

Enabling on Layer 3 switches to facilitate controlled communication between VLANs.

Result

Conserved 3400 IP addresses (reduced usable IPs from 8190 to 4790), minimizing unnecessary broadcast.

Dynamic Routing Protocol: OSPF (Open Shortest Path First)

Deployed for efficient and dynamic path determination between VLANs, enhancing reachability and reducing manual configuration.

Proposed Solution

Solution Design - Layer 3 Enhancements

```
Lecturers Network, the calculations below depicts the network, host range and subnet mask to support
VLAN lecturers
Address:   192.168.0.0          11000000.10101000.00000000. 00000000
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111. 00000000
Wildcard:  0.0.0.255            00000000.00000000.00000000. 11111111
=>
Network:   192.168.0.0/24       11000000.10101000.00000000. 00000000
HostMin:   192.168.0.1          11000000.10101000.00000000. 00000001
HostMax:   192.168.0.254        11000000.10101000.00000000. 11111110
Broadcast: 192.168.0.255        11000000.10101000.00000000. 11111111
Hosts/Net: 254                   Class C, Private Internet

Administration Network, the calculations below depicts the network, host range and subnet mask to
support VLAN Admin
Address:   192.168.10.0         11000000.10101000.00001010. 00000000
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111. 00000000
Wildcard:  0.0.0.255            00000000.00000000.00000000. 11111111
=>
Network:   192.168.10.0/24      11000000.10101000.00001010. 00000000
HostMin:   192.168.10.1         11000000.10101000.00001010. 00000001
HostMax:   192.168.10.254       11000000.10101000.00001010. 11111110
Broadcast: 192.168.10.255       11000000.10101000.00001010. 11111111
Hosts/Net: 254                   Class C, Private Internet

Server Network, the calculations below depicts the network, host range and subnet mask to support VLAN
server
Address:   192.168.20.0         11000000.10101000.00010100.00 000000
Netmask:   255.255.255.192 = 26 11111111.11111111.11111111.11 000000
Wildcard:  0.0.0.63             00000000.00000000.00000000.00 111111
=>
Network:   192.168.20.0/26      11000000.10101000.00010100.00 000000
HostMin:   192.168.20.1         11000000.10101000.00010100.00 000001
HostMax:   192.168.20.62        11000000.10101000.00010100.00 111110
Broadcast: 192.168.20.63        11000000.10101000.00010100.00 111111
Hosts/Net: 62                    Class C, Private Internet
```

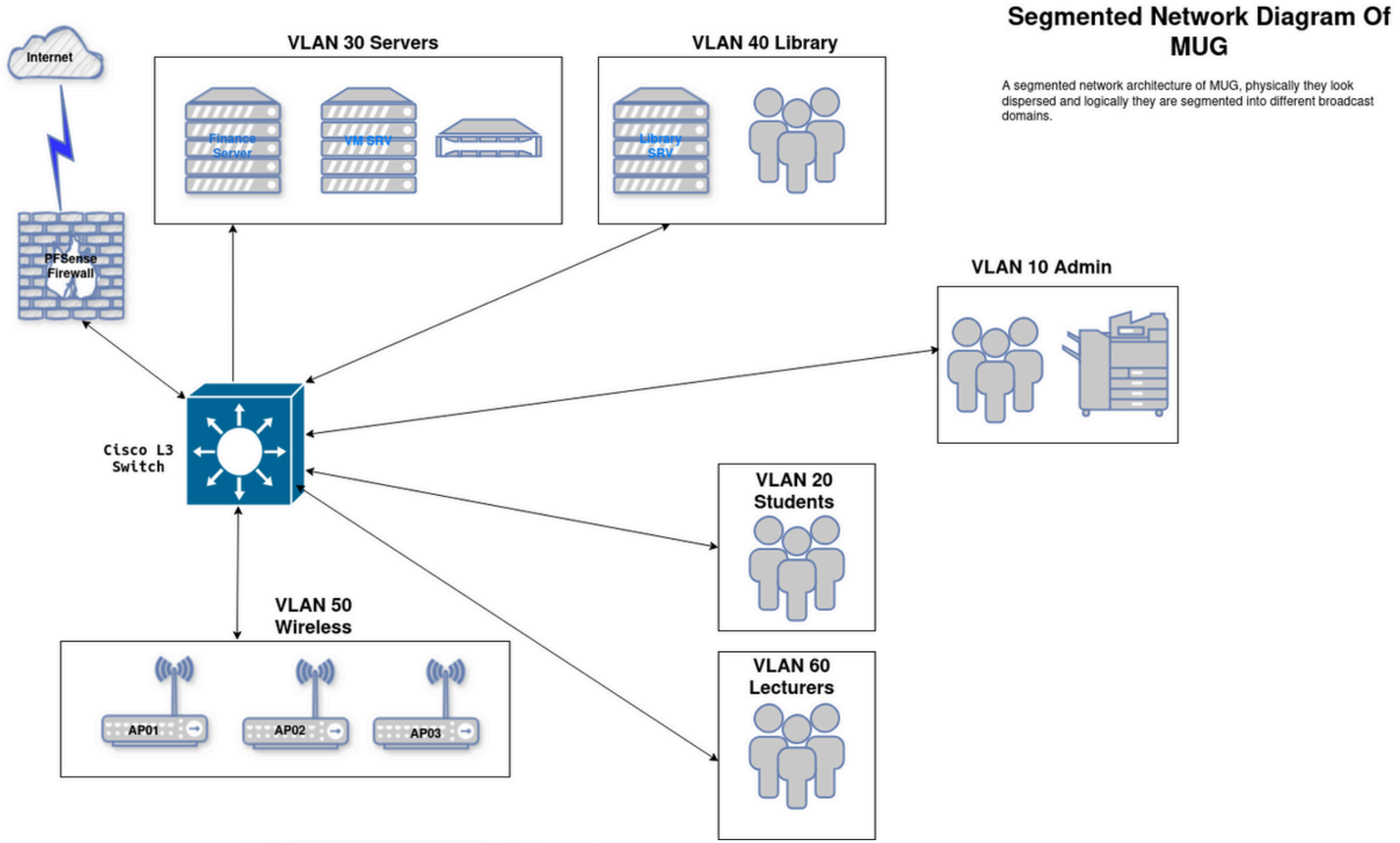
New IP addresses created to replace the /19 subnet with VLSM-optimized ranges

```
Address:   192.168.0.0          11000000.10101000.000 00000.00000000
Netmask:   255.255.224.0 = 19   11111111.11111111.111 00000.00000000
Wildcard:  0.0.31.255           00000000.00000000.000 11111.11111111
=>
Network:   192.168.0.0/19       11000000.10101000.000 00000.00000000
HostMin:   192.168.0.1          11000000.10101000.000 00000.00000001
HostMax:   192.168.31.254       11000000.10101000.000 11111.11111110
Broadcast: 192.168.31.255       11000000.10101000.000 11111.11111111
Hosts/Net: 8190                  Class C, Private Internet
```

Old IP address with the /19 subnet being replaced

Proposed Solution

Solution Design - Layer 3 Enhancements



Hierarchical Network Architecture Post Segmentation

Proposed Solution

Solution Design - Layer 4-7(Transport to Application)

Key Action: Radius Server Implementation

Technology Stack

FreeRADIUS and daloRADIUS (web management) on Ubuntu Server.

Purpose

Centralized AAA (Authentication, Authorization, and Accounting) services.

Core Benefits

Secure Access Control

Enforces strong user authentication before network access.

Protects Sensitive Data

Mitigates risks like password harvesting and man-in-the middle attacks.

Compliance & Auditing

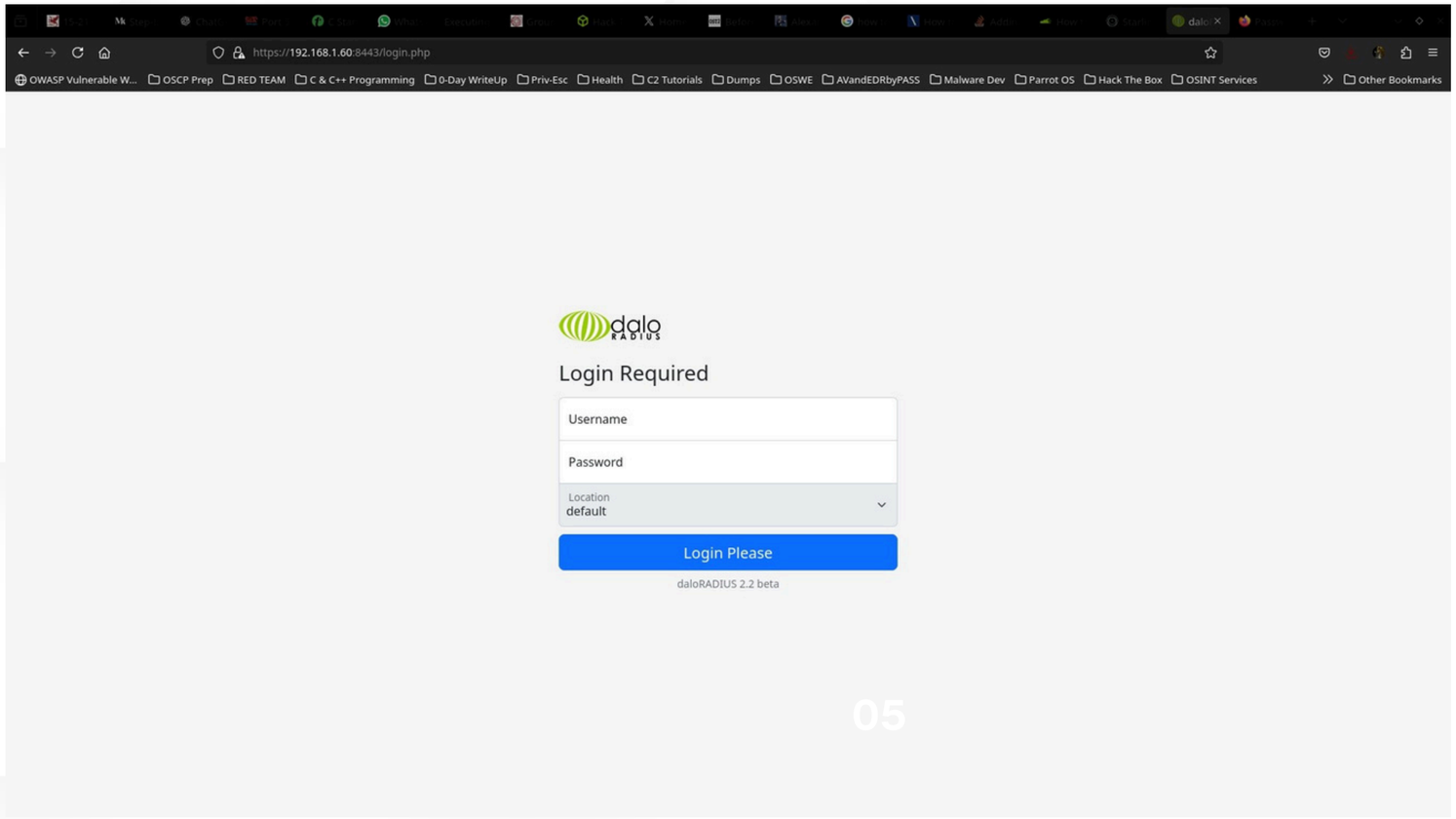
Provides accounting logs for networking usage.

Additional Security

SSL/TLS encryption for the RADIUS management portal.

Proposed Solution

Solution Design - Layer 4-7(Transport to Application)



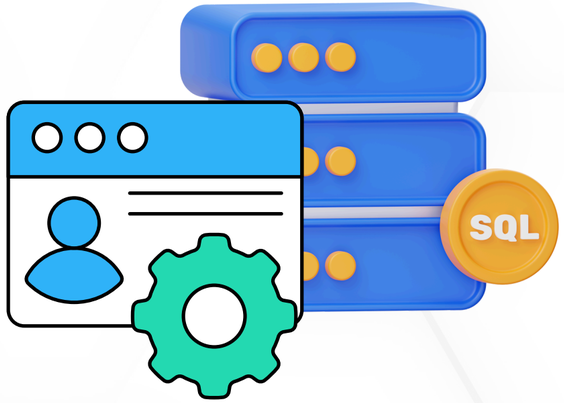
Client authentication via RADIUS before accessing network resources.

Implementation

Server Setup(Ubuntu, Apache, PHP, MariaDB)

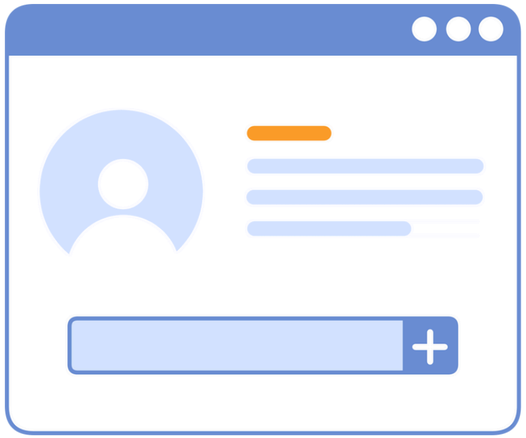
Foundation Services

FreeRADIUS & SQL Integration



Authentication Engine

Web Management (daloRADIUS & SSL)



User & Policy Interface

Our implementation involved setting up the core services, configuring the RADIUS engine, and securing the management interface, all within a simulated environmet to test our design.

Implementation

Configuration Snapshots

These snippets demonstrate the core logic for VLAN setup,connecting FreeRADIUS to its user database, and enabling secure SSL access for management.

Snapshot 1(VLAN)

```
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
```

VLAN Definition & Port Assigment (VM Simulation)

Snapshot 2(RADIUS SQL)

```
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"
```

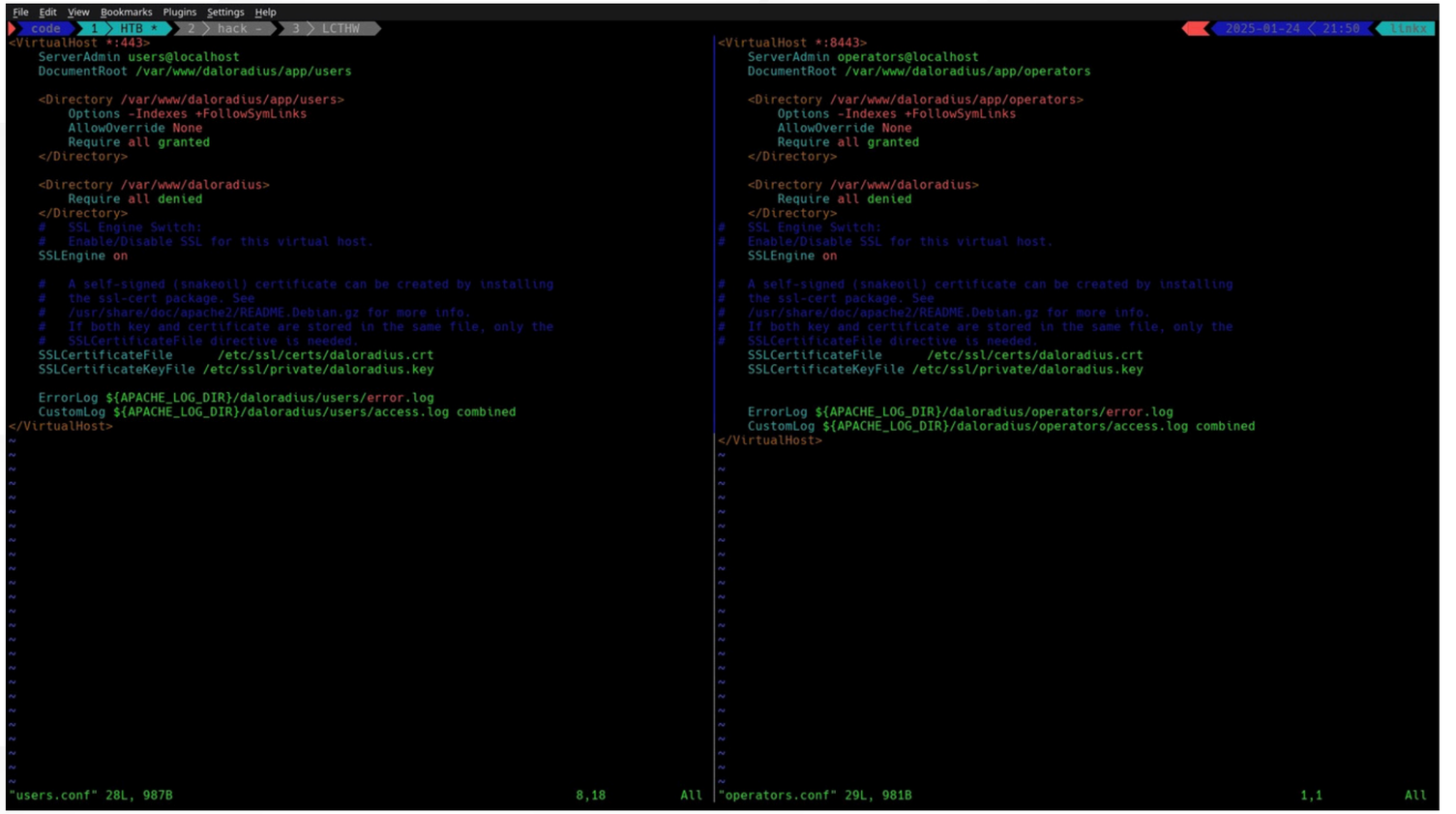
FreeRADIUS SQL Backend Connection

Implementation

Configuration Snapshots

These snippets demonstrate the core logic for VLAN setup,connecting FreeRADIUS to its user database, and enabling secure SSL access for management.

Snapshot 3(SSL)



SSL for Secure daloRADIUS Access

Implementation

Live Demonstration

Environment

Oracle VirtualBox Simulation

Showcasing

daloRADIUS: User Management & Logging

RADIUS Authentication Flow

VLAN Traffic Behavior (Conceptual)

Secure(HTTPS) Management Portal Access

To bring these concepts to life, we'll now switch to a live demonstration within our Oracle Virtualbox enviroment.

We'll focus on how users are managed via daloRADIUS, the RADIUS authentication process in action, conceptually how traffic would be handled in our segmented VLANs and the secure access to the management portal.

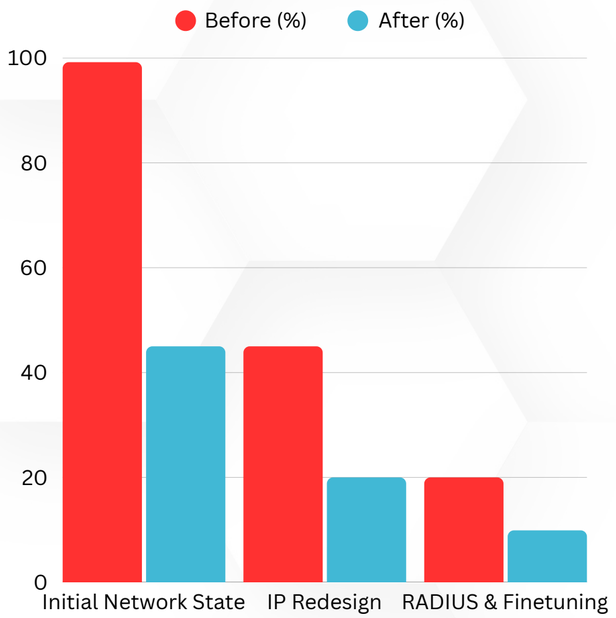
Implementation

Live Demonstration

PROCEEDING TO LIVE DEMONSTRATION

Results, Validation & Discussion

Broadcast Traffic Reduction



90% Reduction in ARP Broadcasts

From 99.2% of 1.5M packets to significantly lower

Impact: Mitigated broadcast storms risk, reduced congestion.

IP Address Conservation

3190 IPs Saved

From 8190 to 4790 usable IPs via VLSM & subnet redesign

Impact: Efficient IP utilization, enhanced scalability.

Security Validation

RADIUS Prevents Unauthorized Access

Impact: Enforced AAA policies, secure user authentication.

Results, Validation & Discussion

Validation & User Insights

Validation Against Objectives

Broadcast Reduction

Achieved target (Simulated up to 90%)

Improved Security

Unauthorized access eliminated via RADIUS

Enhanced Performance

Expected latency reduction & reliability increase.

Configuration Verification

Designs align with proposed standards (**show vlan brief, etc**)

Stakeholder & User Perspectives

User Dissatisfaction (Old System)

Slow speeds, disconnections, poor wireless coverage.

IT Personnel Agreement

VLAN & routing would improve manageability and reduce congestion.

Our OSI-Layered Solutions

Directly address these reported pain points and align with expert feedback.

Results, Validation & Discussion

Discussion: Implications of the Project

Enhanced Security

Reduced unauthorized access, data breach protection.

Enhanced Security

Faster, more stable connectivity, especially in high-density areas

Optimized Scalability & Management

Easier future growth, simplified network administration.

A Model for Educational Institutions

Enhanced Security

Conclusion & Future

Study Limitations

Simulation Constraints

Validation primarily via simulated environments; real world results may vary slightly.

Resource Availability

Project scope constrained by typical academic project limitations (budget, direct MUG IT expertise access, MUG live network).

Time Constraints

Affected depth of live testing and full-scale validation phases.

Conclusion & Future

Conclusion: Project Achievements

Optimized MUG’s network using an OSI-mode; driven,, hierarchical architecture.

Key Problems Addressed

L1/L2

Mitigated poor woreless coverage & broadcast storms (VLANs).

L3

Resolved IP inefficiency (Subnet Redeign, OSPF)

L4-L7

Secured access via robust authentication(RADIUS).

Core Outcome

Proposed solutions **demonstrably improve** (in simulation) network performance, reliability, and security.

Core Outcome

Solutions align with industry standards(IEEE, NIST, ISO).

Conclusion & Future

Recommendations & The Path Forward

Optimized MUG's network using an OSI-mode; driven, hierarchical architecture.

Recommedations

Immediate

Prioritize Wireless AP Optimization
VLAN Segmentation
IP Redesign
Full RADIUS Deployment

Ongoing

Implement OSPF
Establish Regular Audits & Maintenance
Provide Staff Training

Strategic

Design for Future Scalability(consider SDN concepts)

Future Research Directions

IOT Integration: Security & Performance Implications
Cloud Migration Feasibility
Advanced SECURITY: WPA3 adoption, IDS implementation

Closing

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.

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

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

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

Closing

THANK YOU

METHODIST UNIVERSITY GHANA

EXCELLENCE • MORALITY • SERVICE