

PROJECT DEFENCE

OPTIMIZING NETWORK INFRASTRUCTURE WITH ITS INHERENT SECURITY

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

Presented By

TETTEY MICHAEL NII AYI

OFORI DANIEL PERRY JNR

IGWEBUIKE SOLOMON JNR

ESHUN DARLINGTON EBENEZER

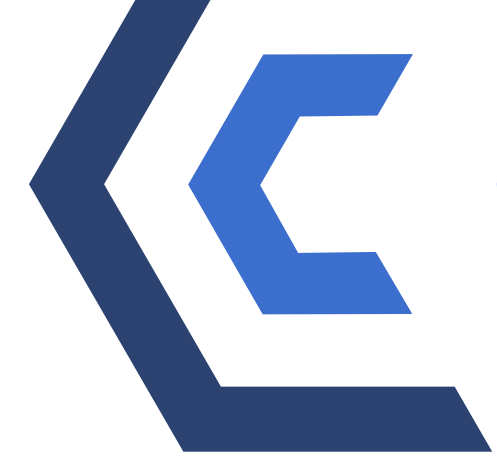
BSSI/ED/218894

BSSI/ED/210056

BSSI/ED/ 221348

BSSI/ED/218704

Agenda



Introduction 

01

Problem Domain 

02

Methodology 

03

Proposed Solution 

04

Implementation 

05

Results, Validation & Discussion 

06

Conclusion & Future 

07

Closing 

08





Introduction

A robust and reliable **network** is no longer a luxury but a fundamental necessity for **educational institutions**, underpinning 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 infrastructure 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.



Security Vulnerabilities

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



Reliability Concerns

Inconsistent Wi-Fi access and network instability.



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 broadcasts)

Impact

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

Problem Domain



Existing Network Analysis - Layer 1 & 2 Issues

The screenshot displays the Wireshark interface with a packet capture of ARP requests. The top pane shows a list of 43 packets, all of which are ARP requests from Intel_f0:bb:80 to a broadcast destination. The bottom pane provides a detailed view of the first frame, showing its structure and metadata.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.118? Tell 172.16.46.67
2	0.001124	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.119? Tell 172.16.46.67
3	0.002247	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.120? Tell 172.16.46.67
4	0.003348	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.121? Tell 172.16.46.67
5	0.004457	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.122? Tell 172.16.46.67
6	0.005581	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.123? Tell 172.16.46.67
7	0.006706	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.124? Tell 172.16.46.67
8	0.007805	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.125? Tell 172.16.46.67
9	0.008898	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.126? Tell 172.16.46.67
10	0.009983	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.127? Tell 172.16.46.67
11	0.011073	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.128? Tell 172.16.46.67
12	0.012178	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.129? Tell 172.16.46.67
13	0.013298	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.130? Tell 172.16.46.67
14	0.014437	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.131? Tell 172.16.46.67
15	0.015541	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.132? Tell 172.16.46.67
16	0.016704	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.133? Tell 172.16.46.67
17	0.017867	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.134? Tell 172.16.46.67
18	0.018996	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.135? Tell 172.16.46.67
19	0.020132	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.136? Tell 172.16.46.67
20	0.021288	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.137? Tell 172.16.46.67
21	0.022405	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.138? Tell 172.16.46.67
22	0.023520	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.139? Tell 172.16.46.67
23	0.024675	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.140? Tell 172.16.46.67
24	0.025800	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.141? Tell 172.16.46.67
25	0.026918	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.142? Tell 172.16.46.67
26	0.028045	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.143? Tell 172.16.46.67
27	0.029176	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.144? Tell 172.16.46.67
28	0.030296	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.145? Tell 172.16.46.67
29	0.031420	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.146? Tell 172.16.46.67
30	0.032541	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.147? Tell 172.16.46.67
31	0.033650	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.148? Tell 172.16.46.67
32	0.034765	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.149? Tell 172.16.46.67
33	0.035860	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.150? Tell 172.16.46.67
34	0.037993	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.151? Tell 172.16.46.67
35	0.039097	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.152? Tell 172.16.46.67
36	0.040210	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.153? Tell 172.16.46.67
37	0.041347	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.154? Tell 172.16.46.67
38	0.042453	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.155? Tell 172.16.46.67
39	0.043558	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.156? Tell 172.16.46.67
40	0.044661	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.157? Tell 172.16.46.67
41	0.045768	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.158? Tell 172.16.46.67
42	0.047126	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.159? Tell 172.16.46.67
43	0.048268	Intel_f0:bb:80	Broadcast	ARP	42	Who has 172.16.46.160? Tell 172.16.46.67

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlan0, id 0
Section number: 1
Interface id: 0 (wlan0)
Encapsulation type: Ethernet (1)
Arrival Time: Nov 6, 2024 12:43:40.086822065 GMT
UTC Arrival Time: Nov 6, 2024 12:43:40.086822065 UTC
Epoch Arrival Time: 1730897020.086822065
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
Frame Length: 42 bytes (336 bits)
Capture Length: 42 bytes (336 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:arp]
[Coloring Rule Name: ARP]
[Coloring Rule String: arp]
Ethernet II, Src: Intel_f0:bb:80 (38:ba:f0:bb:80), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

0000 ff ff ff ff ff ff 38 ba f0 f0 bb 80
0010 08 00 06 04 00 01 38 ba f0 f0 bb 80
0020 ff ff ff ff ff ff ac 10 2e 76

Packets: 1528843 · Displayed: 1517196 (99.2%) · Marked: 1 (0.0%) · Profile: Default

99.2% of 1.5 million captured packets identified as ARP broadcasts

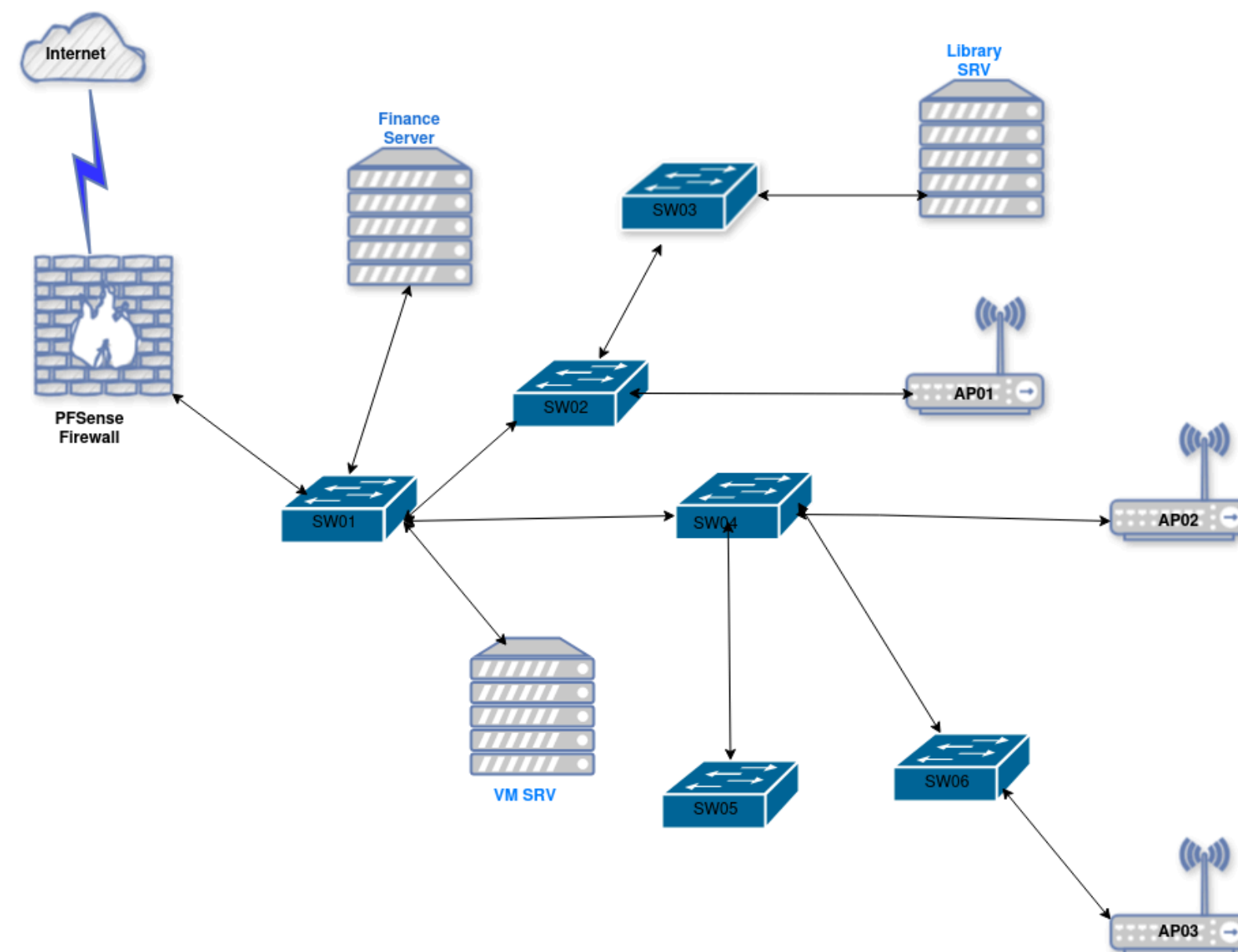
Problem Domain



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 man-in-the-middle attacks.

Problem Domain

Existing Network Analysis - Layer 3 & Higher Layer Issues



No.	Time	Source	Destination	Protocol	Length	Info
1134	1.833416	Cisco 4a:4a:cb	Broadcast	RLDP	60	Network Loop Detection
1251	1.971661	172.20.6.148	172.20.0.1	DNS	85	Standard query 0x492d A push.services.mozilla.com
1324	2.061822	172.20.0.20	255.255.255.255	UDP	323	59300 → 10001 Len=281
1329	2.061822	fe80::1ae8:29ff:fee0:1395	ff02::1	UDP	343	33706 → 10001 Len=281
1335	2.066358	172.20.0.17	255.255.255.255	UDP	324	57737 → 10001 Len=282
1336	2.067232	fe80::1ae8:29ff:fee0:1466	ff02::1	UDP	344	43495 → 10001 Len=282
2577	3.706820	172.20.23.172	172.20.255.255	UDP	96	57621 → 57621 Len=44
3964	5.436264	0.0.0.0	255.255.255.255	DHCP	350	DHCP Request - Transaction ID 0xf5b4e21f
3951	6.779494	Cisco 4a:4a:cb	Broadcast	RLDP	60	Network Loop Detection
3652	6.779495	fe80::6c10:98ff:feaf:68d8	ff02::2	ICMPv6	70	Router Solicitation from 6e:10:98:af:68:d8
3798	6.954651	172.20.0.21	255.255.255.255	UDP	324	42677 → 10001 Len=282
4017	7.221608	172.20.6.148	172.20.0.1	DNS	85	Standard query 0x492d A push.services.mozilla.com
4040	7.249615	172.20.0.1	172.20.6.148	DNS	101	Standard query response 0x492d A push.services.mozilla.com A 34.107.243.93
4259	7.496903	172.20.30.225	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
4260	7.496903	fe80::d21c:3cff:fe0b:e6c9	ff02::fb	MDNS	107	Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
4797	8.152919	172.20.2.176	224.0.0.251	MDNS	123	Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 172.20.2.176 AAAA fe80::8c30:dff:fe
4800	8.154936	fe80::8c30:dff:fe32:4693	ff02::fb	MDNS	143	Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 172.20.2.176 AAAA fe80::8c30:dff:fe
5090	8.411092	fe80::8c30:dff:fe32:4693	ff02::fb	MDNS	143	Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 172.20.2.176 AAAA fe80::8c30:dff:fe
5268	8.727110	172.20.2.176	224.0.0.251	MDNS	288	Standard query response 0x0000 PTR, cache flush Android.local PTR, cache flush Android.local A, cache flush 172.20.2.176 AAAA
5273	8.731701	fe80::8c30:dff:fe32:4693	ff02::fb	MDNS	308	Standard query response 0x0000 PTR, cache flush Android.local PTR, cache flush Android.local A, cache flush 172.20.2.176 AAAA
5282	8.739444	172.20.2.176	224.0.0.251	MDNS	123	Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 172.20.2.176 AAAA fe80::8c30:dff:fe
5286	8.742351	fe80::8c30:dff:fe32:4693	ff02::fb	MDNS	143	Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 172.20.2.176 AAAA fe80::8c30:dff:fe
5290	8.745764	172.20.2.176	224.0.0.251	MDNS	123	Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 172.20.2.176 AAAA fe80::8c30:dff:fe
5291	8.745765	fe80::8c30:dff:fe32:4693	ff02::fb	MDNS	143	Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 172.20.2.176 AAAA fe80::8c30:dff:fe
5795	9.354585	172.20.2.176	224.0.0.251	MDNS	288	Standard query response 0x0000 PTR, cache flush Android.local PTR, cache flush Android.local A, cache flush 172.20.2.176 AAAA
5797	9.355785	fe80::8c30:dff:fe32:4693	ff02::fb	MDNS	308	Standard query response 0x0000 PTR, cache flush Android.local PTR, cache flush Android.local A, cache flush 172.20.2.176 AAAA
6736	10.51828	Cisco 4a:4a:53	Broadcast	RLDP	60	Network Loop Detection
6979	10.93901	172.20.2.176	224.0.0.251	MDNS	288	Standard query response 0x0000 PTR, cache flush Android.local PTR, cache flush Android.local A, cache flush 172.20.2.176 AAAA
7178	11.87017	Cisco 4a:4a:cb	Broadcast	RLDP	60	Network Loop Detection
7179	12.38424	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xb9616510
7738	14.15176	172.20.30.225	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
7740	14.15307	fe80::d21c:3cff:fe0b:e6c9	ff02::fb	MDNS	107	Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
8774	15.46596	fe80::f4f2:8bff:fe82:9e9d	ff02::2	ICMPv6	70	Router Solicitation from f6:f2:8b:82:9e:9d
8775	15.46707	Cisco 4a:4a:53	Broadcast	RLDP	60	Network Loop Detection
8905	15.62269	172.20.2.176	224.0.0.251	MDNS	288	Standard query response 0x0000 PTR, cache flush Android.local PTR, cache flush Android.local A, cache flush 172.20.2.176 AAAA
8988	15.72748	172.20.0.19	255.255.255.255	UDP	330	47353 → 10001 Len=288
8992	15.73041	fe80::1ae8:29ff:fee0:1494	ff02::1	UDP	350	36308 → 10001 Len=288
9374	18.09309	fe80::8c30:dff:fe32:4693	ff02::fb	MDNS	143	Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 172.20.2.176 AAAA fe80::8c30:dff:fe
9511	18.58282	172.20.2.176	224.0.0.251	MDNS	123	Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 172.20.2.176 AAAA fe80::8c30:dff:fe
9512	18.58282	fe80::8c30:dff:fe32:4693	ff02::fb	MDNS	143	Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 172.20.2.176 AAAA fe80::8c30:dff:fe
9513	18.78313	172.20.6.148	34.107.243.93	TLSv1.2	300	Change Cipher Spec, Application Data, Application Data
10383	20.99026	fe80::1ae8:29ff:fee0:17cb	ff02::1	UDP	345	37449 → 10001 Len=283
10817	21.52371	Cisco 4a:4a:53	Broadcast	RLDP	60	Network Loop Detection

Frame 1134: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface wlan0, id 0

Section number: 1

Interface id: 0 (wlan0)

Encapsulation type: Ethernet (1)

Arrival Time: Nov 6, 2024 12:43:41.920238821 GMT

UTC Arrival Time: Nov 6, 2024 12:43:41.920238821 UTC

Epoch Arrival Time: 1730897021.920238821

[Time shift for this packet: 0.000000000 seconds]

[Time delta from previous captured frame: 0.000647611 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 1.833416756 seconds]

Frame Number: 1134

Frame Length: 60 bytes (480 bits)

Capture Length: 60 bytes (480 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:realtek:rl dp]

[Coloring Rule Name: Broadcast]

[Coloring Rule String: eth[0] & 1]

Ethernet II, Src: Cisco 4a:4a:cb (50:1c:b0:4a:4a:cb), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Realtek Layer 2 Protocols

Address Resolution Protocol: Protocol

Packets: 1528843 · Displayed: 11647 (0.8%) · Marked: 1 (0.0%)

Profile: Default

Unencrypted 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 significantly 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 unsustainable 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).

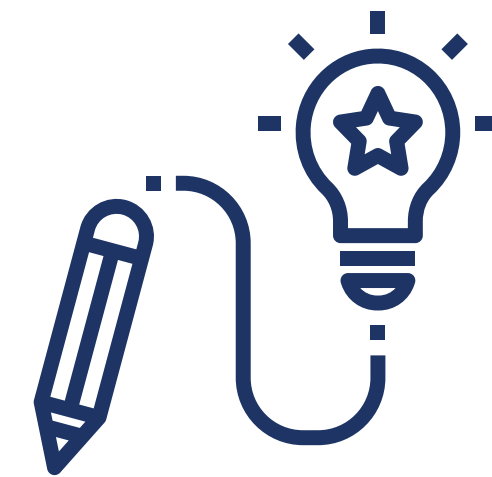
Approach

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

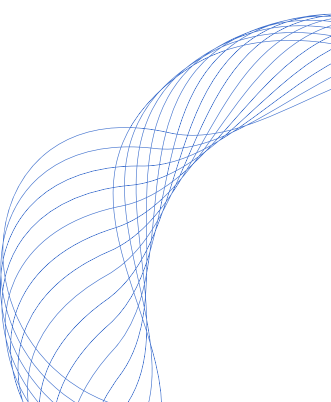
Wireshark captures (with consent) for architecture and security risk identification.

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)

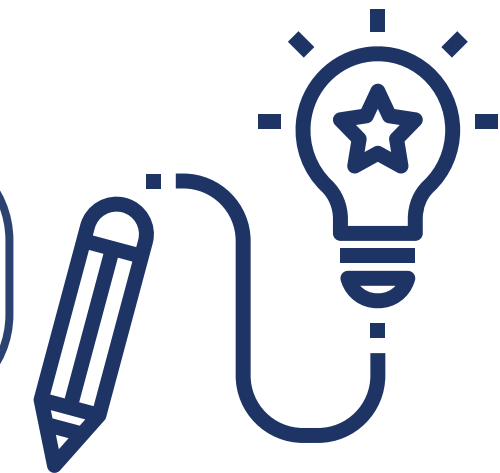
Understanding protocols, identifying security compromises, baseline network activity.

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.



Increased Scalability

Easier to expand and manage future growth



Enhanced Security

Better Isolation, controlled access.



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



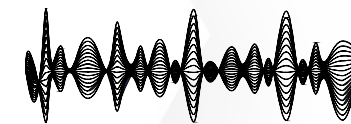
Strategic AP Placement

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



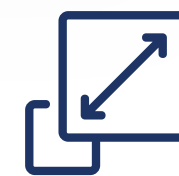
Multi-Band & Channel Management

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.



RESULTS

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

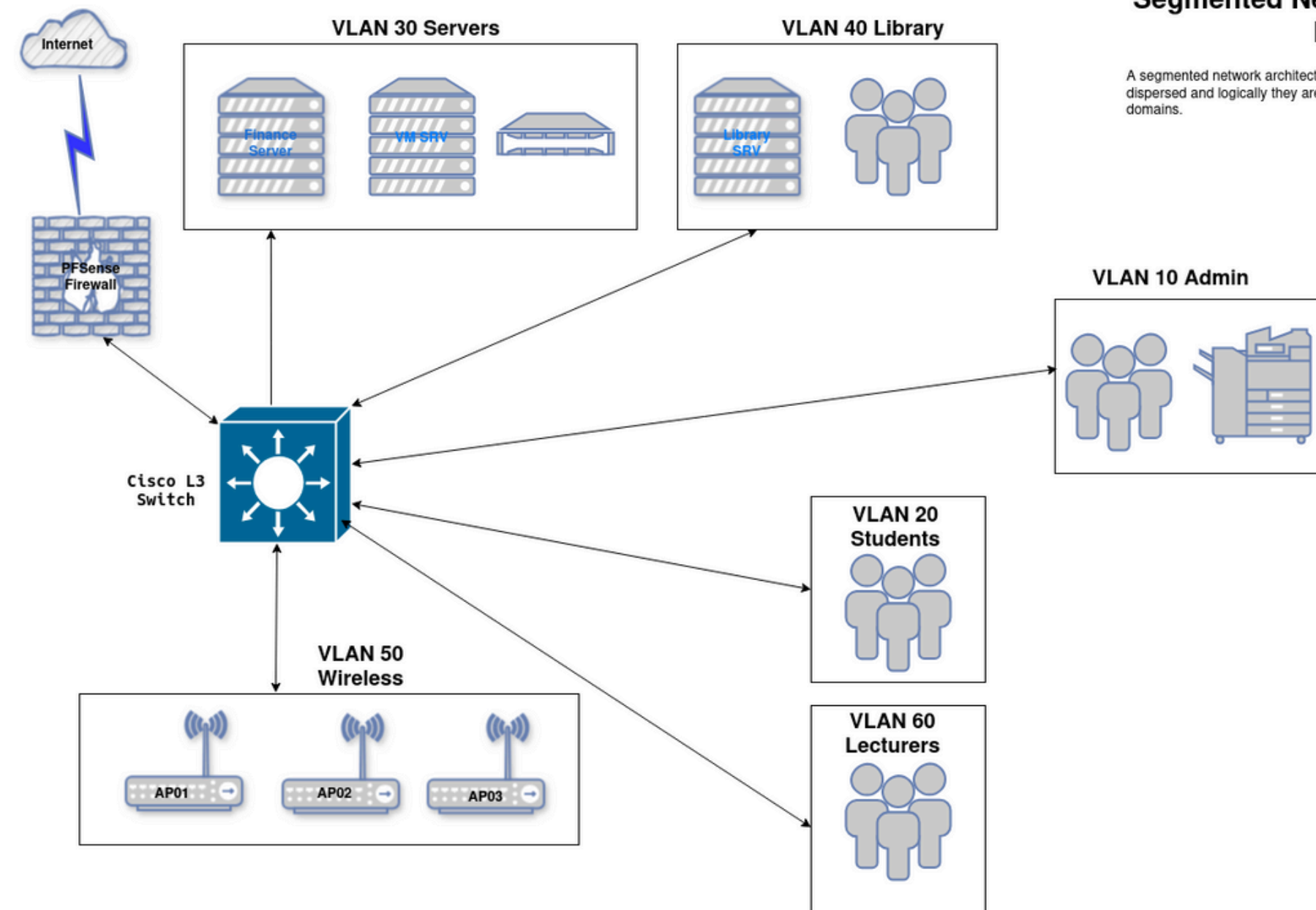
```
Address: 192.168.0.0      11000000.10101000.000 00000.00000000
Netmask: 255.255.224.0 = 19 11111111.11111111.111 00000.00000000
Wildcard: 0.0.31.255      00000000.00000000.000 11111.11111111
=>
Network: 192.168.0.0/19   11000000.10101000.000 00000.00000000
HostMin: 192.168.0.1     11000000.10101000.000 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



Segmented Network Diagram Of MUG

A segmented network architecture of MUG, physically they look dispersed and logically they are segmented into different broadcast domains.

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)

05

Client authentication via RADIUS before accessing network resources.

Implementation

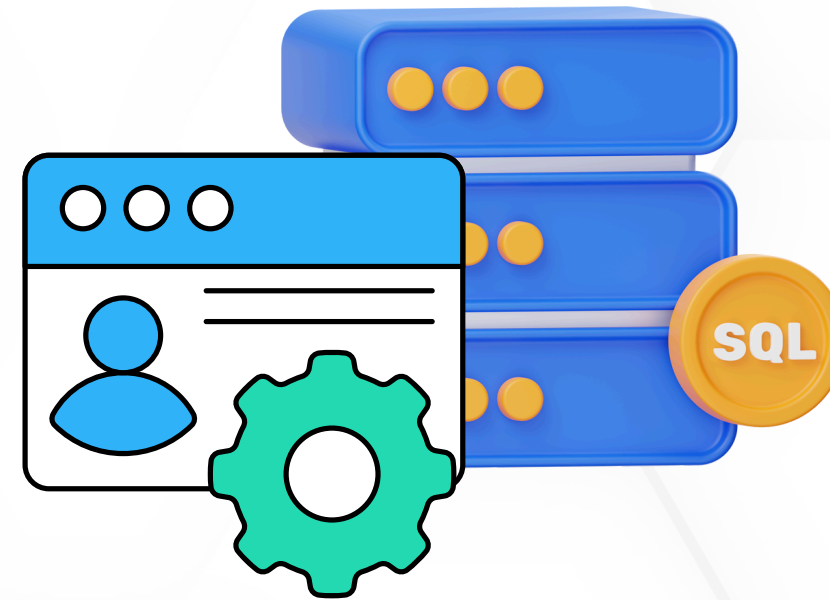


Server Setup(Ubuntu, Apache, PHP, MariaDB)



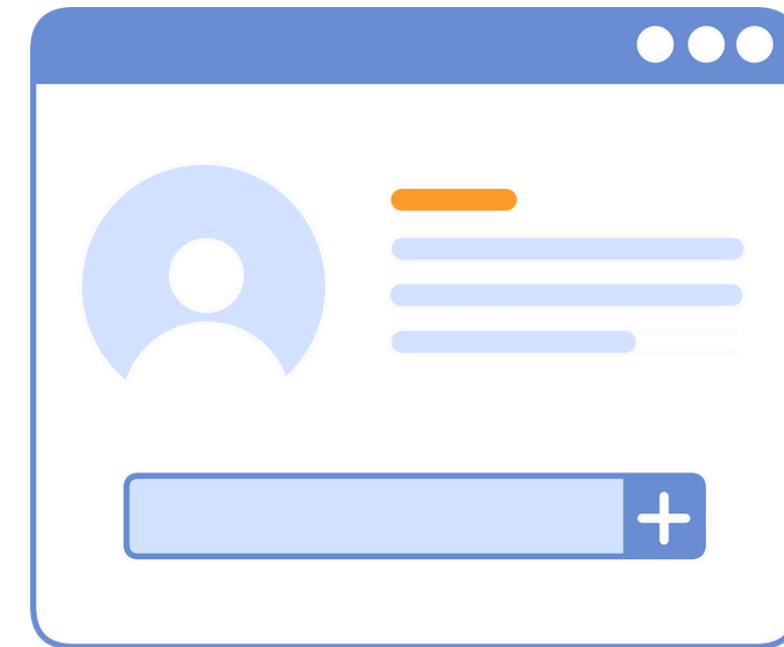
Foundation Services

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 environment 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 Assignment (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

SSL for Secure daloRADIUS Access

Implementation

Live Demonstration

Environment

Oracle VirtualBox Simulation

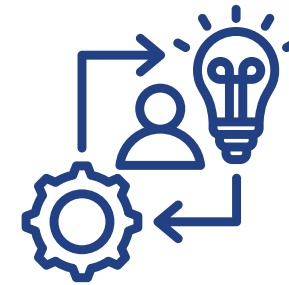
Showcasing

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 environment.

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

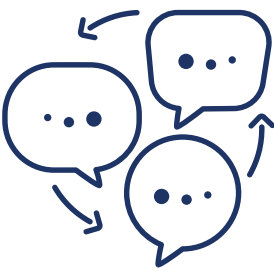
Live Demonstration



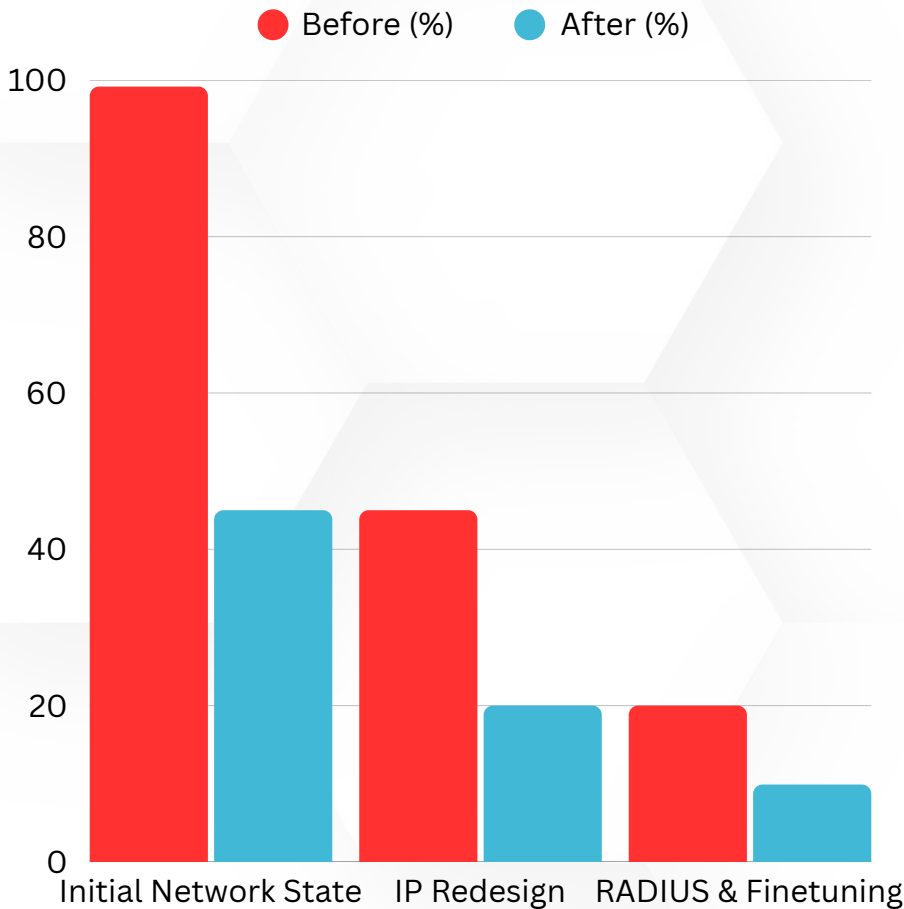
PROCEEDING TO LIVE DEMONSTRATION



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)

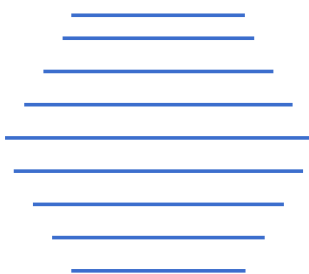
Slow speeds, disconnections, poor wireless coverage.

IT Personnel Agreement

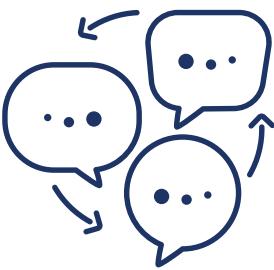
VLAN & routing would improve manageability and reduce congestion.

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

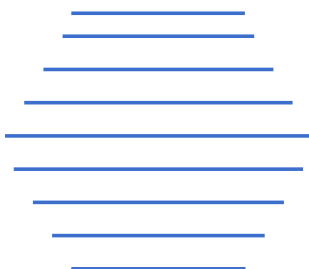


Easier future growth, simplified network administration.

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 wireless coverage & broadcast storms (VLANs).

L3

Resolved IP inefficiency (Subnet Redesign, 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.

Recommendations

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>

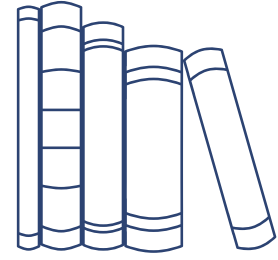
Chidozie, O. K. (n.d.). Design and implementation of optimized features in a local area network for improved enterprise.

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



