HOLY ANGEL UNIVERSITY

Optimizing Wi-Fi Coverage and Network Efficiency at City College of San Fernando, Pampanga

A Capstone Project
Presented to The Faculty of the
School of Computing
Holy Angel University

In Partial Fulfillment
of the Requirements for the Degree
Bachelor of Science in Information Technology
Major in Network Administration

Bondoc, Michael Owen G.
Jimenez, Christian Allen S.
Reyes, John Clarence G.
Tulabut, Emmanuel Greyco B.

March 2025

HOLY ANGEL UNIVERSITY

APPROVAL SHEET

This capstone entitled **"OPTIMIZING WI-FI COVERAGE AND NETWORK EFFICIENCY AT CITY COLLEGE OF SAN FERNANDO, PAMPANGA"**, prepared and submitted in partial fulfillment of the requirements for the degree Bachelor of Science in Information Technology with Area of Specialization in Network Administration, has been examined and is recommended for acceptance and oral examination.

Dr. Raymond A. Cabrera
Adviser

ORAL EXAMINATION

Approval by the committee of oral examiners on
March 7, 2025

Mr. Bernard S. De Guzman
Panel Chair

Mr. Aimer N. Dela Cruz
Panel Member

Mr. Jairenz T. Batu
Panel Member

APPROVAL

Accepted and approved in partial fulfillment of the requirements for the degree Bachelor of Science in Information Technology with Area of Specialization in Network Administration

Ms. Carisma A. Caro
Program Chairperson
Information Technology

Dr. Marlon I. Tayag
Dean, School of Computing

Acknowledgment

First and foremost, the researchers express their deepest gratitude to the Almighty God for the wisdom, strength, and will bestowed upon them to undertake this capstone project. His guidance served as the foundation throughout this journey, enabling them to overcome every challenge encountered. The researchers extend their sincere appreciation to all those who contributed to this work in any way; their help and support were invaluable.

Dr. Raymond A. Cabrera, their adviser, for providing insightful guidance and constant encouragement throughout the mentorship process. His excellent support was instrumental in the successful completion of this study.

We sincerely thank our panelists, Mr. Bernard S. De Guzman, Mr. Aimer N. Dela Cruz and Mr. Jairenz T. Batu, for their invaluable insights and guidance throughout our capstone project. Their expertise and constructive feedback have greatly contributed to refining our research. We deeply appreciate their time and support in helping us improve our work.

The faculty and administration of the City College of San Fernando (CCSFP) for their assistance and for providing the necessary materials to conduct this study. The researchers also express their gratitude to the respondents for providing considerably essential data for this study.

Their families and friends for their unwavering support, patience, and encouragement. Their belief in the researchers motivated them to persevere and complete this project.

Table of Contents

Appendices

List of Tables

List of Figures

Optimizing Wi-Fi Coverage and Network Efficiency at City College of San Fernando, Pampanga

Michael Owen G. Bondoc, Christian Allen S. Jimenez,
John Clarence G. Reyes and Emmanuel Greyco B. Tulabut

Holy Angel University

Executive Summary

Reliability is essential for wireless connectivity in modern educational institutions, fulfilling both the academic and administrative requirements. The study included interviews with the computer laboratory custodian of the school, surveys given to students and teachers through Google Forms, and the researchers also did site observations. Information gathered from these sources indicated frequent disconnections, slow internet speed, and security issues, especially due to poor authentication systems. Analysis showed that the current network did not effectively accommodate peak usage, causing disruption in online learning and administrative functions. Upgrades suggested including mesh networking, single-vendor management, and load balancing for optimal network performance. Improving security measures with WPA2-Enterprise authentication and improving roaming capability were also suggested. Scalable solutions to accommodate the increasing needs of the college were also the focus of the study. Future studies must examine predictive modeling for best placement of wireless access points, and how to integrate newer security features such as WPA3 encryption, role-based access control, and multi-factor authentication. As the campus grows, embracing cloud-managed Wi-Fi, software-defined networking (SDN), and emerging technologies like 5G and hybrid networks will further enhance connectivity and performance.

A proposed wireless upgrade entails building a reliable high-speed scalable system that is responsive to the increasing demands of the institution's students, faculty, and staff. Moreover, the upgraded network matches the strategic goals of the college, which further opens new pathways toward other upgrades and developments.

Optimizing Wi-Fi Coverage and Network Efficiency at City College of San Fernando, Pampanga.

Introduction

Wireless communication has grown to become a crucial element of the computing industry and is being increasingly used in our daily life cycle. It has emerged to perform an important function in colleges and universities, offices, and other places in which Wi-Fi connectivity is used extensively. Throughout the years, the demand to connect to Wireless Local Area Network (WLAN) has greatly increased. WLAN infrastructures are now commonly required in commercial buildings, companies, schools, and even residential homes. Muttair et al. (2021)) conducted a study on deploying a mixed wireless network with fewer Wi-Fi routers to obtain optimal coverage. Their analysis highlights the need of strategically installing Wi-Fi routers to enhance network performance and save infrastructure costs. The study used the Wireless InSite (WI) Package to simulate a real-world scenario and compare the effectiveness of two distinct types of Wi-Fi routers, TP-Link and Rocket, operating at 2.4 GHz and 5 GHz frequencies.

According to a survey that DataReportal has released in 2024, 67.5 percent of the total population of the world use the internet continuously. The total users of the internet calculated in the Philippines is at 73.6 percent, tallying people connected to the web through the use of their smartphones or other gadgets. With most communication platforms, team collaboration on assignments, and accessing digital educational resources, it becomes a basic necessity that the students should have available both wired and wireless networks. In this context, providing full Wi-Fi coverage and optimal network efficiency has emerged as one of

the main concerns for schools to fill the rising needs of students and faculty for more technological services. Dudhat et al. (2022) conducted a study on optimization of indoor wireless network coverage area. They mainly studied interference in indoor wireless networking due to multipath propagation effects, including reflection, refraction, and scattering of radio waves caused by the building structure. The study characterized the empirical and theoretical propagation models to deal with issues such as coverage, overlapping channels, and wireless performance. Adding to the knowledge about practical and theoretical planning for optimizing indoor wireless monitoring and designing network topologies with contour presentation was a significant aspect of this research.

Located in Pampanga, City College of San Fernando, Pampanga was recently established, with its new campus constructed towards the end of last year. Another campus is already under construction to cater to the expanding necessity for similar educational facilities in the area. Like any other modern institution, this college is pledged towards excellence in quality education and will, most certainly, use virtual meeting platforms as some other online portals for facilitating the learning process within a technology friendly environment. The current setup of City College of San Fernando, Pampanga currency uses a household Wi-Fi setup, the school uses 3 ISPs Converge as their main ISP (300mbps) where the faculty and admins connect. The Globe ISP (500mbps) is used to connect units on their computer laboratories. The students are using the Starlink ISP (80-350mbps). The computer laboratories accommodate 144 wired units in total, with 4 wired units for their library and 15 wireless units. They currently have a total of 20 short range access points. 4 on each floor that supports the Converge ISP and 1 on each floor for the Starlink ISP. Regarding security,

the network lackes monitoring or any web filtering tools that secures the users devices. Users rely on the laptop's built-in firewalls.

One significant inefficiency of the previous network configuration was the underutilization of the third ISP, which was intended solely for wired connections. This resulted in an imbalance in bandwidth allocation, as only the first two ISPs were utilized by the wireless network, leading to congestion and variable performance for students and faculty. To maximize resource utilization and enhance network efficiency, load balancing was achieved through FortiGate to ensure the efficient use of all available internet connections. With a total of 510 students, daily attendance typically ranges from 80% to 95%, translating to an estimated daily attendance of approximately 408 to 485 students. The school faces challenges with its internet connectivity, which is often slow, unreliable, or completely inaccessible for students, rendering the Wi-Fi practically unusable. Additionally, the school lacks a system to monitor the current state of its network, hindering its ability to track or manage the websites accessed by students. Implementing long-range access points and VLAN Segmentation are potential areas for improvement, as separating student, faculty, and administrative networks can enhance security and bandwidth management.

The school's internet connectivity experienced drops, characterized by slow configurations and weak signal strength, which hindered students' and faculty's access to online resources. This situation worsened during peak hours, leading to a significant decline in performance and connectivity. WiFiman diagnostics indicated that the 2.4 GHz band offered broader coverage but was susceptible to substantial interference, while the 5 GHz

band provided better speeds at the cost of wall penetration, particularly in adjacent classrooms and office spaces.

The study revealed the Wi-Fi coverage across different floors and identified areas with reduced signal strength. The third floor exhibited strong coverage in the 2.4 GHz band but experienced some congestion, resulting in occasional latency spikes and inconsistent performance. Conversely, the 5 GHz band delivered higher speeds with lower latency; however, its weak signal strength limited its reach to the last classrooms and halls. The fourth floor had good coverage in the 2.4 GHz band, with moderate coverage noted in other areas exhibiting signal degradation near the building's edges and in densely populated user areas. In contrast, the 5 GHz band performed well in open spaces such as common areas but poorly penetrated walls in classrooms.

Wi-Fi coverage varied with frequency and interference levels. The Ubiquiti UniFi U6-LR access points installed on campus had an estimated coverage of 185 square meters (a 13.6-meter radius in all directions in open space). Obstructions such as walls and high-density zones affected this range, with the 5 GHz band typically covering only 10-15 meters indoors before significant signal degradation occurred. The 2.4 GHz band extended further, reaching up to a 30-meter range, but experienced more interference from other devices.

Review of Related Literature

Wireless Connectivity

Wireless networking has emerged as an integral part of modern communication systems giving flexibility, cost-effectiveness, and portability, and importance that is gaining for the organizations and the users. As stated by Priya (2023), the technology may differ in contrast with the traditional wired networks as they use high-frequency radio waves to facilitate communication between the devices, thereby giving the user the freedom to connect without physical limitations. Studies note that the actual value of technology is nowadays measured in return on investment, and wireless networks have matured to the point that they deliver large benefits, justifying their wide adoption. Mobility has been such a great benefit because users can gain access and move about within the range of the network with ease, thereby improving productivity and convenience in many settings.

Connectivity can be maintained in a movement between locations making this the uniqueness of the wireless network. This has provided essential flexibility and versatility for communications. The result has been the integration of wireless and mobile communications in a wide range of applications including commercial, educational, defense, and industrial. It has revolutionized worldwide data transmissions such that it offers efficient and reliable communication in challenging environments such as overseas operations or military settings. With the widespread employment of wireless networks -both cellular and satellite-based technologies-that expand full breadth, ensuring Quality of Service (QoS) in providing voice, video, and data delivers one of the significant challenges. Chavan et al. (2022) states that one needs to have an appropriate management of bandwidth, delay, jitter, and throughput QoS

parameters to attain reliable performance while focusing considerable interest to overcome security concerns in end-to-end wireless communication.

Wireless Access Points

According to Cisco (2024), a wireless access point or (WAP) is a device, which is used in networking to allow wireless-enabled devices to join and become part of the wired network. Installing WAP to connect all devices in your network is easier rather than using cables and wires. You can expand the coverage and power of your wireless network by using WAP or “mesh extenders”. It gives you total wireless coverage and to get rid of "dead spots" that are experienced, especially in big office spaces or buildings.

As stated by Zenarmor (2024), an access point is part of WLAN but is used mostly in a workplace or large building. It connects to a wired router, switch, or hub by means of an Ethernet cable and broadcasts its WiFi signal to a particular area. For example, if you would like to have Wi-Fi in your reception area in the company but, unfortunately do not have a router close by, then you should set up an access point close to your reception area and then run an Ethernet cable through your ceiling to the server room.

A WAP is a device that connects devices wirelessly. They work on the principle of transmitting a signal through which the connected device can connect. Devices are now connecting to the internet or any other network cable-free. Such access points are being used in residential places, organizations, and public places.

A wireless router can support only around 10-20 users accessing at a time,while a wireless access point can enable over 50 or hundred users access. It can broadcast and

receive signals much more powerfully, which allows for such heavy usage. If one thinks of wireless Internet for large areas, it gives a user an added guarantee of efficiency by using a wireless access point. WAP can cover an area of up to 100-300 meters. Ideally, longer distances are suited for offices or multiple buildings. Multi-AP deployments are very common in business premises because the coverage of a single AP is too limited for an enterprise. Therefore, a multi-AP interconnection is used to extend the wireless network's coverage, allowing clients to roam within the network seamlessly (FiberPlus, 2019).

Wi-Fi in Learning Environments

It is important for colleges to understand the activity of users going through their wireless access networks in order to better manage and improve their Wi-Fi infrastructures to counter increasing connectivity and traffic demands. Thus, the analysis made of students and faculty's use of such networks enables institutions to improve knowledgeably to better class performance. With this knowledge of the behavior of mobile users, campus planning initiatives can be made even stronger by designing Wi-Fi access points for better coverage in high-traffic areas. This analysis will not only increase the performance of Wi-Fi in campus but will also serve as a part of an efficient and responsive learning environment. Therefore, campus planning initiatives can be further supported by the strategic laying out of Wi-Fi access points to ensure as much coverage as possible in high-traffic zones like libraries, lecture halls, and public areas. That ensures maximum network efficiency and allows for very little downtime operationally due to connectivity failures by the user. Apart from this, data on the activity of users can become helpful in proposing specific support services that help users in troubleshooting resources as well as usage guidelines in the way users can access the network successfully. (Oliveira et al., n.d.)

According to O'Brien et.al (2022) every student in the school has access to the internet as designed to improve learning experience. The internet use is important to education but, when overused it can be a distraction, it becomes a problem and it affects the performance and well-being of students negatively. Some Universities provide free internet through WiFi, believing that this can improve the users' learning experience. To determine whether provision of WiFi indeed improves or enriches the students, it is important to understand how it is actually used. The use of WiFi in university campuses links to higher grades and completes more courses per semester. This impact is caused by the day-time use of WiFi and more advanced students (Ferreira, n.d).

Benefits and Risks of Wi-Fi Networks

Consumer preference for network services depends on a number of major factors which define the final satisfaction and choice. Good speed has emerged as one major factor nowadays with clients desiring both cellular and Wi-Fi networks that promise to give fast performance. Other things remaining equal, usability aspects of the Wi-Fi network assume the critical role; the more the range and wider accessibility that the networks provide, the more attractiveness they give to users. Cost also has an impact on consumers' choices as lower price offers make network services more appealing. These preferences are significant while evaluating experiences of the users and its associated satisfactions. Various consumer behavior studies based on network characteristics have supported these findings. It has been indicated through the use of a mixed model along with stated preference data that the consumer's preference is maximum when the rate of cellular and Wi-Fi networks is fast, extensively usable, and available at an affordable price. It keeps to the full understanding of

the consumer's preferences regarding the importance of these factors in planning and improving network services such that user expectations are properly met (Oh et al., 2022).

College campuses Wi-Fi networks offer limitless new opportunities for connectivity and convenience but also pose significant challenges that have to be addressed. Because they multiply across the campus, from lecture halls and libraries through dining areas and student lounges, they increasingly attract cybercriminals who think them to be an easy target for illegal activities. Campus Wi-Fi is very susceptible because most of it is open and the remainder might be inadequately secured. It therefore leaves room for hacking, which can lead to interference of data being transferred and also the compromised user information. Personal details of both students and faculty members connected to such unsecured or rogue campus Wi-Fi hotspots could become easily accessible or stolen. Such emerging threats require much tighter security measures and higher user awareness to prevent data breaches as well as the protection of privacy. Even with the positive impact of the presence of Wi-Fi access on and around college campuses, there is a need for a reminder of putting in place adequate measures to secure the network, making users aware of cyber threats that free and open networks present. (Bheevgade et al, 2023).

Most college campuses today are using public access devices as hotspots or wireless access points. New wireless computing devices such as tablets and smartphones have made it easier for students and faculty members to find out information through the Internet. Again, with the increased access comes risk of security and privacy that most users are not even aware of. Most people tend to overlook such risks because they cannot practically come up

with a way of knowing their vulnerabilities. This ignorance is risky as cybercriminals can unconditionally hack campus networks and obtain private information. Moreover, if there are not viable tools and education, users become vulnerable to perils such as having data manipulated, identity stolen, or their devices tracked without consent. This requires greater awareness and systems of support to be provided to users at colleges to effectively defend their privacies from fraudsters in the online environment. (Lotfy et al., 2021).

Most campus wireless network traffic is unencrypted, and the users, in this case, are at a risk that they might not know about. Campus Wi-Fi providers appear to focus more on being easier to use, which also often sacrifices more security vulnerabilities. The cybercriminals exploit those weaknesses on the campus networks, sniffing all the sensitive data, posing a great threat to confidentiality and security of the users. Detection methods and countermeasures against cybercrime in such environments are crucial. To date, literature and studies on the field reveal that little evaluation exists with respect to the effectiveness of specific measures implemented toward specific threats, network structures, and usage types. In this context, this paper discusses new protection technologies and strategies for campus Wi-Fi networks, including the prevalent threats and vulnerabilities existing within these systems. Moreover, it should issue recommendations regarding the setting up and sustaining of all types of campus Wi-Fi networks that can support various user devices and particular security needs (Frolova et al., 2022).

Maintenance and Management of Wi-Fi Systems

One possible management mechanism of Wi-Fi connections is that a terminal, like a smartphone or laptop, retrieves a unique secret key for a given wireless network from a server. The keys are based on network names and a random seed, or start, for key generation. The key generated by the server and the router uses that random seed and the current time such that the key updates at periodic intervals. This means that there is periodic change in the key that gets used to connect the network, which makes the network connection safe. The updating of the key reduces the chances of anyone gaining unauthorized access while also enhancing the safety of the entire network. Other than that, synchronized calculations ensure that only access rights for the right key are granted to devices seeking to connect (Lixiong & Jinju, 2020).

Papadopoulos et al. (2020) identified challenges related to reliability and availability in wireless networks, particularly for mission-critical applications. Their study on Reliable and Available Wireless (RAW) explored augmenting network resilience through end-to-end Layer 3 services to mitigate lower-layer transmission problems. The research highlighted OAM capabilities that aid in detecting issues, monitoring performance, and ensuring real-time network reliability. These features include fault tolerance and resource management procedures designed to maximize a wireless network's efficiency. These findings offer insights into enhancing network performance through real-time monitoring, fault detection, and resource allocation.

User Experience and Performance in Wi-Fi Networks

Public Wi-Fi networks represent a crucial part of building user experience and measuring performance within transit systems. As more and more people rely on their smartphones and digital connectivity, the study of Wi-Fi connection data provides a panoramic view of how networks work and how satisfied passengers are. This method instantly renders insights into many aspects of public transportation-identification of train arrivals, waiting time, and changing travel time, with no need to merge data from separate sets. For example, studies like the one conducted on the Toronto subway transit system illustrate the potential for using Wi-Fi data in building service reliability and enhancement of the overall customer experience by gathering and analyzing connectivity patterns as well as travel behavior. The use of Wi-Fi data helps transit agencies improve network effectiveness and reduce service-related issues that transport organizations face effectively with increasing the reliability of transportation services and travelers' satisfaction (Grenville et al., 2023).

According to Kamienski (2020), pervasive connectivity is a critical foundation for smart cities, prompting municipalities to implement programs where Wi-Fi is a crucial component of public Municipal Wireless Networks. Despite widespread availability in cities worldwide, data on network QoS, user QoE, and general network use remain limited to a few studies. For instance, the Municipality of São Paulo provides free Wi-Fi across 120 digital squares. Over two years, the Municipality of São Paulo collected data on user connections, network performance, and service availability in these squares. Such large datasets enabled assessments of the role of current admission control methods in shaping both network QoS and QoE, as well as ensuring service availability. Additionally, it provided insights into

overall QoS/QoE issues and their causes. Furthermore, it facilitated the correlation between user activity on the network and specific events occurring in the surroundings, leading to a deeper understanding of performance in public Wi-Fi systems and its effect on user experience.

According to Kamienski (2020), pervasive connectivity is a critical foundation for smart cities and has prompted municipalities to institute programs wherein Wi-Fi constitutes a crucial component of public Municipal Wireless Networks. Despite the widespread availability in cities across the world, data on network QoS, user QoE, and general network use is limited to a few studies. For instance, the Municipality of São Paulo has free Wi-Fi across 120 digital squares. For two years in these squares, the Municipality of São Paulo has collected user connections, network performance, and service availability. Such large datasets have made it possible to make judgments on the role of current admission control methods in shaping both the network QoS as well as QoE and ensured service availability. Equally, it provided insight into overall QoS/QoE issues and why they happen. Additionally, it enabled correlation between user activity in the network and specific events taking place in its surroundings, as well as a deep understanding of performance in public Wi-Fi systems and the effect on user experience.

Conceptual Framework

Figure 1

Conceptual Framework

Conceptual Framework		
Input	**Process**	**Output**
• Connectivity Baseline • Data Acquisition Strategy • Literature Review on Wi-Fi Networks • Budget and Equipment Selection	• Design of Proposed Network Topology • Data Collection • Equipment Setup • Wi-Fi Installation & Configuration • Security Implementation & Testing	• Network Infrastructure Documentation • Assessment Report • Data Collection and Analysis Report • User Requirements Documentation • Network Infrastructure Design Documentation • Implementation Plan • Evaluation Reports

The conceptual framework of this study focuses on advancing digital inclusion among students and staff by implementing Wi-Fi connectivity and network infrastructure while ensuring secure internet access. The input phase assessed the college's current network infrastructure against established security requirements. This phase included interviews with the school’s IT staff and a literature review on Wi-Fi solutions for schools to identify user requirements and technical specifications. Budget considerations, along with the selection of appropriate hardware such as access points, switches, and cables, further defined the project's scope.

The process phase involved designing and developing a network topology, followed by site surveys to identify the most strategically advantageous locations on campus for the Wi-Fi access points. This included configuring the access points for optimal performance and integrating security measures, such as firewalls and authentication methods, to facilitate secure access. The network was then tested and evaluated for performance optimization and security.

In the output phase, the focus was on deploying access points throughout the college campus. The goals were to provide fully functional and secure Wi-Fi access across the campus to support Wi-Fi services for students and staff. This network aimed to enhance the reliability of internet connectivity, enabling access to online services and resources, and potentially offering additional value for the college's future needs.

Objectives of the Study

This study aimed to design a network infrastructure at City College of San Fernando that would provide students and staff with scalable Wi-Fi access. To enhance the network coverage of the campus, the researchers planned to position wireless access points strategically across the college campus. The main goal of the study was to offer the college reliable and efficient Wi-Fi connectivity for seamless internet access. Specifically, the study aimed to:

- Assess the campus' present network infrastructure and determine optimal access point locations.
- Design and simulate a scalable and secure wireless network for the campus.

- Analyze the network's performance, security, and expert feedback to establish reliability and efficiency.

Scope and Delimitation

The scope of this study focused on the design of a wireless network infrastructure for City College of San Fernando, with the primary objective of providing scalable Wi-Fi access to its students and staff. It addressed only the simulation of network infrastructure to create an efficient and secure network within the geographical boundaries of the campus, excluding other institutions or regions, and did not investigate non-network infrastructure

The study aimed to tackle core challenges related to Wi-Fi connectivity, specifically signal strength, bandwidth, speed, interference, and security. It emphasized both technical design and user experience to enhance the internet browsing experience for the college community. The study was grounded in practical considerations, such as access point placements and network design. The proposed network was designed to be scalable and adaptable to future needs while complying with local network standards and guidelines.

However, there were some limitations to this study. It operated within a defined timeline and did not account for long-term technological advancements or future Wi-Fi standards that might emerge after the study period. Therefore, the study was based on the current state of Wi-Fi technologies and security protocols, without addressing broader legal or environmental factors beyond what was necessary for network optimization. Additionally, while the study assessed network performance and security, the deployment of network infrastructure and access points was only simulated. Real-world implementations may present various challenges not considered in the design, requiring further adjustments.

Furthermore, the study did not include information on monitoring and maintenance following implementation, as these aspects fell outside its scope. It did not address issues related to the broader regulatory environment or data privacy concerns, which were examined only in the context of local regulations and guidelines. Finally, the precise number of access points and their locations were determined through an on-site survey, which might introduce potential challenges necessitating adjustments.

Despite these limitations, the study provided valuable insights into the practical aspects of the college's Wi-Fi network infrastructure, laying the groundwork for future network expansions. This study represented a significant step toward delivering a secure, scalable, and efficient Wi-Fi network for the college.

Methods

Requirement Analysis

The project of the study began with a comprehensive review of the college's existing network, with a focus on areas with limited to no Wi-Fi coverage. The campus's computer laboratory custodian was interviewed, and students' experiences with the campus Wi-Fi were gathered through the use of Google Forms. Gathering these data provided insights into the current connectivity challenges and user needs. A bandwidth study was performed to determine user demand and the amount of capacity needed to support applications such as online learning and streaming media. Wi-Fi Access Points were strategically positioned based on a comprehensive review of the college's physical layout, providing consistent coverage in high-traffic locations. The infrastructure was also designed to be expandable to

handle future growth and technological requirements, incorporating security controls such as encryption and access control to prevent unauthorized entry and ensure bandwidth efficiency. All hardware and software requirements were determined to ensure the network would remain cost-efficient and maintainable. Additionally, a topology diagram was used to illustrate how the network would interact with users and devices across campus, providing a clear understanding of the system's structure and functionality.

System Design and Implementation

The study focused on a reliable internet access topology for public areas across campus. This involved the planned placement of approximately 8 Wi-Fi Access Points strategically to maximize coverage while minimizing interferences such as dead zones or physical obstacles. The design also incorporated security measures against malicious attacks by applying internal firewalls and user authentication protocols. Following the completion of the design, the subsequent simulated implementation process entailed the hardware configuration and commissioning of the Wi-Fi system based on the user's requirements as indicated in the analysis. This stage included configuring internet services, setting up routers and access points, and managing the bandwidth allocation for users. Respondents were assured anonymity in the survey; therefore, the study did not collect a specific list of individual users. A dummy list of names was used for illustration and testing purposes only. In addition, diagrams such as context diagrams and data flow diagrams were developed to show how data flows through the system and the interactions between different components.

Testing and Evaluation

Usability, security, and performance tests of the network were planned to be conducted following the simulated system deployment. The wireless connection was to be evaluated at various locations across the college to ensure consistent coverage and speed. Security protocols were to be tested using FortiGate for filtering and to manage the verification of authorized users accessing the network, as well as to assess whether bandwidth limitations could be effectively enforced. Feedback was to be collected via surveys utilizing Google Forms that would be sent to students to identify any connectivity problems or issues with network performance. The tests were to target the reliability, speed, security, and overall user experience of the network. Depending on the test results and the feedback received, modifications were to be made to ensure the system efficiently achieved the set goals.

Training and Documentation

Following system deployment, tests will be conducted to evaluate its performance, security, and usability. The Wi-Fi network will be tested across various locations within the college to ensure comprehensive coverage and consistent speed. Security measures will also be evaluated to verify that only authorized users can access the network and that bandwidth restrictions are properly enforced. Surveys and feedback will be collected from students and personnel to assess satisfaction and identify any concerns regarding connectivity and network performance. The evaluation will be based on the network's reliability, speed, and security measures, as well as their impact on users. Adjustments will be made based on feedback and test results to ensure the system operates as intended.

Research Design

This study employed a quantitative approach to analyze Wi-Fi coverage and network performance at the City College of San Fernando, Pampanga. To gain an understanding of the campus network, the school's computer laboratory custodian, who has experience with the Wi-Fi system, was interviewed. Additionally, students were administered survey questionnaires to gather data on their experiences using the campus Wi-Fi.

Data

Data Collection

This study utilized both primary and secondary data to investigate Wi-Fi coverage at the City College of San Fernando, Pampanga. Data collection involved a Google Forms survey distributed to students to gather information about their experiences with the Wi-Fi, including questions on security, performance, and ease of access. Interviews were conducted with the assigned computer laboratory custodian to understand technical aspects and infrastructure issues. Furthermore, on-site observations of signal strength measurements and network performance, as well as connectivity-related problems on campus, were conducted.

Data collection methods included online surveys, recorded interviews, and Wi-Fi analysis tools. The collected data were synthesized to evaluate the college's Wi-Fi network, focusing on critical aspects for improvement in coverage, reliability, and security.

Instruments

The researchers utilized WiFiman, a free Android and iOS application developed by Ubiquiti Networks Inc., as an assessment tool for analyzing Wi-Fi networks. This tool,

initially a simple network discovery tool, has evolved into a comprehensive speed testing platform supported by a global network of servers. WiFiman offers features such as Wi-Fi scanning, network device discovery, speed testing, and latency measurement, and is freely available for download on Google Play and the Apple App Store. It also enhances the UniFi Network experience by allowing users to locate UniFi devices, test wireless performance, and establish instant remote connections via VPN.

Furthermore, the researchers used Google Forms to carry out a survey of students at City College of San Fernando. The survey gathered information regarding their experience with the campus WiFi, with an emphasis on security, performance, and accessibility.

Respondents

The researchers conducted interview sessions and answered survey questionnaires with purposive sampling in order to collect quantitative perspectives from key people directly involved or affected with the campus Wi-Fi network. Respondents included:

- The computer laboratory custodian of City College of San Fernando, who offered technical insights on the current situation of the network along with the related problems and opportunities for enhancement.
- Students who use the campus Wi-Fi for potentially showing the problems while connected, and the performance of the network across various areas on campus.

Statistical Treatment of Data

For this study, results were gathered from surveys using Google Forms. Frequency and percentage distributions were employed to present the number of respondents who preferred each option. This facilitated the interpretation of overall trends related to network performance, reliability, speed, and security. Responses from Likert-scale questions were analyzed using means and standard deviations to determine average ratings and the variability around these averages. This analysis aided in understanding common issues and measuring the overall satisfaction level of users with the wireless network. Consequently, these two methods provided a clearer basis for evaluating network problems and understanding the general level of acceptance regarding future improvements.

Research Procedures

This study utilized a structured research process for Wi-Fi optimization focusing on coverage and efficiency. Being simulation-based, the study primarily concentrated on Preparation, Planning, and Design. These three phases facilitated the evaluation of the existing network infrastructure and the development of an optimized design derived from measured performance. Furthermore, the framework involved the detailed planning and justification of organizational decisions by determining and validating technology needs. Thus, all proposed changes underwent a carefully designed process before implementation. This approach aimed to identify crucial connectivity challenges, explore potential improvements, and offer a pathway to develop a performance-optimized design.

Preparation

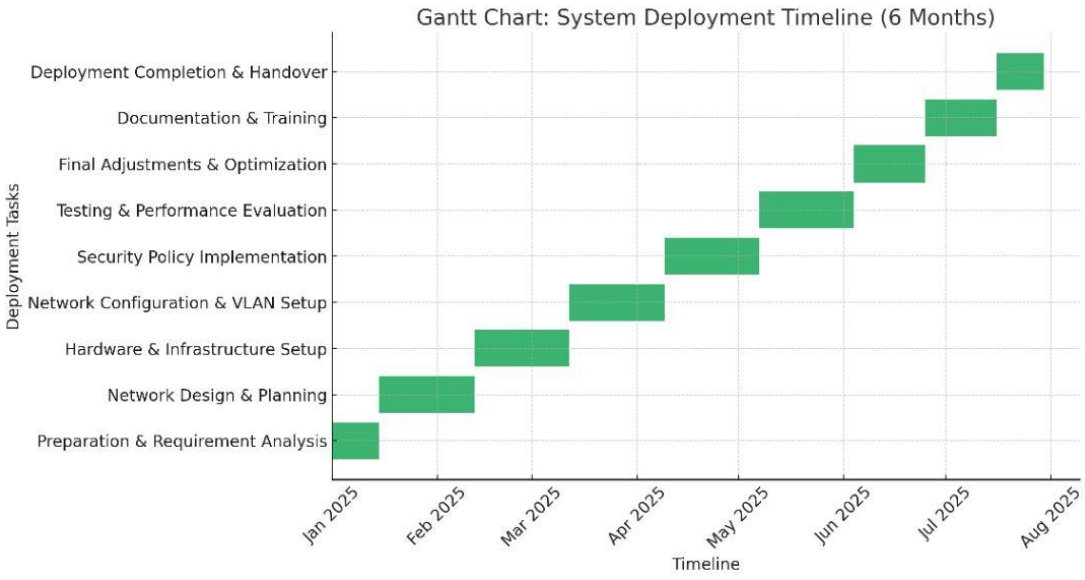
As online learning and digital resources have become increasingly essential in education, institutions must ensure their networks can accommodate the growing demand for connectivity. Regular assessments are necessary to maintain efficiency, reliability, and overall performance, as network optimization is an ongoing process. This phase involved gathering the technical and operational requirements for evaluating and enhancing the current network infrastructure. Understanding these requirements provided insight into establishing optimal technology and configurations for improvement. While the network may have been evaluated previously, evolving requirements necessitate periodic re-evaluation of the network's performance and capacity.

The current assessment of the network infrastructure is done through an interview with the computer laboratory custodian asking about the current setup, frequently connected problems or challenges and probable improvement areas. It would provide direct experience of the network's performance and user experience within campus.

Planning

Planning during this phase meant analyzing the gathered data to formulate a structured approach to optimizing the wireless network. Coverage, signal performance, and bandwidth distribution were reviewed with improvement areas in mind.

The plan included methods for access point placement, bandwidth management, firewall policies, and channel allocation to enhance connectivity. Strategic placement of WAPs was planned to ensure effective coverage throughout the building. Policies were



then created to delineate restrictions for individual ISPs. This also applied to the bandwidth management specified for the intended users.

Figure 2: System Deployment Timeline

Designing

The results from the previous phases were used to create a more efficient network design. The recommendations from the gap analysis were combined to develop a wireless network that meets both technical and operational needs while following industry standards.

Ethical Considerations

All information gathered from the organization was handled in strict compliance with Section 20 of the Data Privacy Act of 2012. All collected data were securely stored in a password-protected folder accessible only to the researchers. Recordings remained confidential, and the collected data were used solely to support and guide this study.

Results

Survey Results

This survey aimed to measure the wireless network's reliability, speed, security, and performance at City College of San Fernando. A total of 225 respondents participated in this study by sharing their experiences regarding connectivity, interruptions, and network efficiency. The findings indicated significant areas needing improvement, particularly concerning reliability and security, to enhance the network.

Table 1 shows that the survey aimed to measure the wireless network's reliability, speed, security, and performance at City College of San Fernando. A total of 225 respondents participated in this study by sharing their experiences regarding connectivity, interruptions, and network efficiency. The findings indicated significant areas needing improvement, particularly concerning reliability and security, to enhance the network. The survey collected responses from a diverse group of students across different year levels. The 225 respondents primarily consisted of 2nd-year students (30.7%), followed by 3rd-year students (26.7%), 4th-year students (22.2%), and 1st-year students (20.4%). This distribution provided the study with a relatively representative sample of students with varying levels of access to the campus Wi-Fi across different academic levels.

Table 1

Year Level Distribution of Respondents

Year Level	Frequency	Percentage
1st Year	46	20.4%
2nd Year	69	30.7%
3rd Year	60	26.7%
4th Year	50	22.2%
Total	225	100%

As shown on Table 2, the 225 respondents in the survey represented various academic departments, with the Institute of Information Technology comprising the largest proportion of respondents at 45.8%. The Institute of Business Administration accounted for 32%, and the Institute of Education represented 22.2%. This distribution suggests that a considerable number of responses came from IT students, who likely interact with the campus Wi-Fi most frequently, along with valuable input from business and education students.

Table 2

Departmental Distribution of Respondents

Department	Frequency	Percentage
Institute of Information Technology	103	45.8%
Institute of Business Administration	72	32%
Institute of Education	50	22.2%
Total	225	100%

Table 3 shows that most respondents perceive the subject as either neutral (40.9%) or somewhat unreliable (41.8%), with very few considering it reliable (4%). The converted scores indicate a tendency toward neutrality but with a slight lean toward unreliability. The majority of respondents experienced connectivity issues, highlighting the need for network improvements to stabilize and enhance performance. The weighted average score of 2.36 indicated that internet reliability was rated below neutral, suggesting that most users considered it unreliable. A score below 3 signified user dissatisfaction.

Table 3

Reliability Ratings and Converted Scores

Choices	**Percentage (%)**	**Converted Score (Percentage x Scale Value)**
Very Unreliable (Blue)	13.3%`	0.133 x 1 = 0.133
Somewhat Unreliable (Red)	41.8%	0.418 x 2 = 0.386
Neutral Orange	40.9%	0.409 x 3 = 1.227
Somewhat Reliable (Green)	4%	0.04 x 4 = 0.16
Very Reliable (Purple)	0%	0.00 x 5 = 0.00

As seen on Table 4, the weighted mean score of 2.49 implied that respondents were largely dissatisfied with the wireless network speed and bandwidth offered during off-peak hours. Given that 3 represented a neutral score, this finding indicated that a substantial number of respondents were not satisfied with the network's performance. This suggests a need to upgrade network speed and bandwidth to meet users' expectations, even during periods of light usage.

Table 4

Network Speed Perception

Satisfaction Level	Frequency	Percentage (%)	Converted Score
Very Dissatisfied	30	13.3%	30 x 1 = 30
Dissatisfied	80	35.6%	80 x 2 = 160
Neutral	94	41.8%	994 x 3 = 282
Satisfied	21	9.3%	21 x 4 = 84
Very Satisfied	0	0%	0 x 5 = 0
Total	**225**	**100%**	

Most survey respondents indicated experiencing interruptions in online services. Almost half (42.7%) reported that interruptions occurred "Rarely," while 40.9% chose "Sometimes," suggesting that disconnections were frequent enough for users to notice. Furthermore, approximately 11.1% noted interruptions occurring "Frequently," and 5.3% reported "Never" experiencing them. Notably, no respondents selected "Always." These findings suggested a need for network improvements to ensure a more reliable and stable online experience as stated in Table 5

Table 5

Frequency of Network Interruptions

Frequency of Interruptions or Disconnections	Responses	Percentage (%)
Never	12	5.3%
Rarely	96	42.7%
Sometimes	92	40.9%
Frequently	25	11.1%
Always	0	0%
Total	**225**	**100%**

The results on Table 6 showed that 37.3% of respondents connected within 4-7 seconds, 30.2% within 8-11 seconds, 20.9% within 11-15 seconds, and 11.1% took longer than 15 seconds. Interestingly, no one reported a connection time within 0-3 seconds, indicating that immediate access was uncommon. This suggested potential network responsiveness issues affecting the user experience.

Table 6

User Experience on Connectivity Stability

Time to Connect	Frequency	Percentage (%)
03 Seconds	0	0%
4-7 Seconds	84	37.3%
8-11 Seconds	68	30.2%
11-15 Seconds	47	20.9%
15 Seconds or longer	25	11.1%
Total	**225**	**100%**

According to the results, 46% of respondents expressed low confidence in the wireless network's security measures on campus: 41% reported being "Not Confident," and 5% reported being "Not Confident at All." Forty percent held a neutral stance, indicating uncertainty about the wireless network's security. Only 14% felt secure, with 10% stating they were "Confident" and 4% being "Very Confident." Table 7 shows that data security was a concern, and security measures needed enhancement to build user trust.

Table 7

Security Confidence Levels

Confidence Level	Frequency	Percentage (%)
Not Confident at All	18	8%
Not Confident	80	35.6%
Neutral	85	37.8%
Confident	37	16.4%
Very Confident	5	2%
Total	**225**	**100%**

Results on Table 8 indicated that 49% of respondents held neutral views on the overall campus wireless performance. Nevertheless, dissatisfaction was reported by 41.3% of respondents, who expressed being "Dissatisfied" (29.8%) and "Very Dissatisfied" (7.1%). In contrast, 14% of respondents indicated satisfaction, with 19.6% selecting "Satisfied" and just 2.2% choosing "Very Satisfied." The results suggested that while some experienced decent performance, there was still a need for network improvement to enhance the overall user experience and satisfaction.

Table 8

Performance Satisfaction Ratings

Satisfaction Level	Frequency	Percentage (%)
Very Dissatisfied	16	7.1%
Dissatisfied	67	29.8%
Neutral	93	41.3%
Satisfied	44	19.6%
Very Satisfied	5	2.2%
Total	**225**	**100%**

As seen on Table 9, out of all respondents, 81% supported the establishment of a new wireless network infrastructure, with 60% rating it "Likely" and 21.8% "Very Likely." Eighteen percent of respondents remained neutral, while no one chose "Unlikely" or "Very Unlikely." Therefore, these results strongly indicated support for improving network optimization and scalability, as users recognized the need for improvements in speed, accessibility, and capacity.

Table 9

Perceived Network Support Availability

Likelihood Level	Frequency	Percentage (%)
Very Unlikely	0	0%
Unlikely	0	0%
Neutral	39	17.3%
Likely	135	60%
Very Likely	49	21.8%
Total	**225**	**100%**

Most respondents (89%) believed that the proposed changes would enhance their experience on campus. Specifically, 64.9% expected some improvement, while 24.9% anticipated significant improvements. Only 10.2% believed that the changes might not have a noticeable impact. These results shown on Table 10 indicated a strong expectation that enhancing the wireless network would lead to better performance and improved connectivity.

Table 10

Perceived Impact of Network Optimization

Response Level	Frequency	Percentage (%)
Greatly Worsen	0	0%
Somewhat Worsen	0	0%
No Change	23	10.2%
Somewhat Improve	146	64.9%
Greatly Improve	56	24.9%
Total	**225**	**100%**

The majority of respondents (76%) rated the proposed simulated network as either "Very Good" (62%) or "Excellent" (14%). This demonstrated a strong belief in the simulated network's ability to enhance wireless efficiency. Meanwhile, 24% rated it "Good," indicating an overall positive assessment. Importantly, there were no "Fair" or "Poor" ratings, further supporting the idea that implementing at least some network monitoring and management tools could significantly improve CCSFP's wireless operations, as stated on Table 11.

Table 11

Efficiency of Current Network Setup

Response Level	**Frequency**	**Percentage (%)**
Poor	0	0%
Fair	0	0%
Good	41	18.2%
Very Good	129	57.3%
Excellent	54	24%
Total	**225**	**100%**

Lastly, Table 12 showed a significant majority of the respondents (88%) believed that the proposed network topology satisfied their need for reliable and fast on-campus wireless access, with 55.1% indicating it was "Well" and 34.2% rating it as "Very Well." Meanwhile, 10.7% remained neutral, and no one rated it as "Poor" or "Very Poor." Overall, these results indicated substantial agreement in favor of the proposed network improvements.

Table 12

Alignment of Network with User Need

Response Level	Frequency	Percentage (%)
Very Poorly	0	0%
Poor	0	0%
Neutral	24	10.7%
Well	124	55.1%
Very Well	77	34.2%
Total	**225**	**100%**

The survey results indicated that the campus network faced challenges related to connectivity issues, security, and performance. Many users reported frequent disconnections and slow connection speeds, leading to low confidence in the network's security. The general satisfaction rating was not high; many users expressed concerns about the network's reliability. However, there was strong demand for upgrades, and respondents anticipated that the proposed upgrades—a simulated network and an optimized topology—would improve the situation. These findings suggested an immediate need for upgrades to enhance the network's speed, stability, and security.

IT Expert's Feedback

The evaluation of Sir Jayson Paul Banal acknowledged the careful analysis conducted by the study and its recommendations aimed at improving connectivity, performance, and security. The research identified primary barriers such as network congestion, insufficient signal coverage, security threats through the use of qualitative and quantitative data collection techniques. Other relevant inputs encountered and considered were those given by

Sir Jayson concerning the project's evaluation. The systematic approach, including user input, network topology evaluations, and site surveys, further gave credence to the proposed solutions.

Mr. Banal's recommendations for this investigation were based on its practical and scalable solutions grounded in industry best practices, namely, mesh networking, load balancing, and WPA2-Enterprise authentication. He also expressed particular appreciation for the aspect of this work that ensured the network's long-term stability and growth, while emphasizing future technologies such as cloud-based Wi-Fi management, software-defined networks (SDN), and WPA3 encryption.

To further ascertain the feasibility of the proposed solutions, Mr. Banal suggested conducting real-time benchmarking tests or sample implementations to support them. A more comprehensive cost-benefit analysis could facilitate more appropriate prioritization of investments by decision-makers for such network enhancements.

Further strengthening of these proposals could be achieved through the implementation of user awareness training on network security and best practices for network usage by staff and students. In conclusion, Mr. Banal indicated that the capstone project had carefully considered technically feasible methods for optimizing network speed and Wi-Fi coverage. The recommended methods complied with current networking standards, were scalable, and practical.

The successful implementation of the solutions would broaden the scope of the institution's wireless infrastructure while improving the experience of staff members and

students. The network enhancements were recognized as well-deserved for the researchers' efforts, and the institution was encouraged to implement the suggested network changes for a more secure and dependable network environment.

Gap Analysis

Educational institutions must periodically upgrade their technologies to meet contemporary service delivery standards. The City College of San Fernando, Pampanga (CCSFP) identified several areas for improvement in its network infrastructure to provide proper and secure Wi-Fi services for students and faculty. Mr. Banal, an IT expert who assisted in this study, and Mr. Pangilinan, the IT Custodian of CCSFP, noted several core issues with the existing network, including weak Wi-Fi coverage, poor bandwidth distribution, and security risks.

Initially, the school primarily provided Wi-Fi for administrative use rather than for a large student population. However, as learning has become more digital and online resources have made internet access increasingly vital, students' need for reliable internet for schoolwork has grown. Consequently, the IT department, under Mr. Pangilinan's guidance, has taken some steps toward security improvement using VLAN segmentation and shared-key authentication. Nevertheless, the network still faced problems with slow connections due to congestion and seamless transfer issues between access points.

This gap analysis served to examine weaknesses inherent in the existing network infrastructure by comparing them to the planned improvements. Factors such as

authentication systems, access point placement, and network security were included in this analysis to identify solutions that could increase Wi-Fi coverage and optimize the network's performance at CCSFP.

The school's network had become somewhat disorganized over time due to unfulfilled upgrades. Various Wireless Access Points (WAPs) from different brands and internet providers had been implemented. These WAPs supported two types of internet connections: Starlink and Converge. In the past, TP-Link WAPs were predominantly used. While a mix of WAP brands can offer some flexibility and scalability, it also introduces challenges. One significant issue was Wi-Fi roaming. Although differently branded WAPs might be connected to the same network, they often operate on separate management systems, making a smooth roaming experience nearly impossible.

The IT expert assessment described that the existing network lacked proper authentication, utilizing an open or pre-shared key (PSK)-based system where users knowing the password could connect, leading to congestion and security vulnerabilities. A voucher-based authentication scheme with MAC address registration was proposed to enhance security and efficiency. This method would require students to log in using unique credentials assigned to VLAN groups, improving network segmentation and preventing unauthorized access. A captive portal integrated with vouchers could further streamline access control, monitoring, and optimal bandwidth allocation for all users.

Table 13.1

Gap analysis summary: Network Infrastructure

Stages	Data
Existing Setup	The school uses several ISPs with different allocations- Converge (300 Mbps) for the faculty, Globe (500 Mbps) for the computer labs, and Starlink (80-350 Mbps) for the students. The network lacks monitoring and proper traffic management.
Expectations	Establish a structured network with proper ISP allocation and VLAN segmentation, in addition to centralized network monitoring, for better bandwidth distribution and security.
Gaps	The current setup has no bandwidth management in place and no security policies leading to filtering of traffic. It also demonstrates insufficient access point coverage, leading to slow and unstable connections.
Problems	Students are found to have been complaining about their internet reliability, as this school is deprived of the power of controlling the traffic available over the network and the fact that there are loopholes for intrusion caused by the absence of monitoring tools.
Recommendations	Change Starlink with PLDT (1 Gbps) for student connectivity. Implement VLANs to have different network traffic. Install network monitoring tools for usage and possible security threats. Upgrade access points to enhance Wi-Fi coverage distribution all over the campus.

Table 13.2

Gap analysis summary: Vendor Selection

Stages	Data
Existing Setup	The deployed APs are from multiple vendors, which creates compatibility and management issues. Different brands need separate configurations, firmware updates, and management interfaces.
Expectations	Standardize all networking equipment on a single vendor, like Ubiquiti, to ensure compatibility, easy management, and one interface for centralized control.
Gaps	The lack of a unified vendor results in inconsistent network performance, increased troubleshooting complexity, and higher operational costs due to varied support requirements.
Problems	Some existing devices lack essential features like seamless roaming and VLAN support. Managing multiple vendors increases administrative workload and reduces overall network efficiency.
Recommendations	Choose a vendor that provides a balance between cost and performance. Instead of fully transitioning to premium brands, consider a hybrid approach—using cost-effective, enterprise-grade APs and switches that integrate well with existing infrastructure while offering centralized management.

Table 13.3

Gap analysis summary: Security

Stages	Data
Existing Setup	The school currently implements an open or pre-shared key (PSK) system of authentication that is difficult to manage and monitor for individual user access. There is no centralized authentication mechanism in place.
Expectations	Implement voucher-based authentication, where students can log into Wi-Fi with unique credentials. Also, register the MAC addresses and assign them to corresponding VLAN groups for better network segmentation and security.
Gaps	The current implementation does not track users or hold them accountable. Anyone with the password can connect, therefore providing more congestion and a security threat. There is no way to restrict access by students.
Problems	A solution for handling voucher distribution and MAC address registration will simplify the processes. Without policy, some users will find ways to bypass the restrictions.
Recommendations	Include a captive portal with vouchers as a login method and MAC address filtering. Having the students assigned to VLANs based on registered devices also improves network efficiency and security, stopping unauthorized access.

According to the IT expert's evaluation stated at Table 14, the proposed network infrastructure was designed for scalability. The wireless network could effectively meet increased demand, and the IP addressing scheme had been prepared for future expansion. The infrastructure could accommodate a high number of user connections and further growth given the sufficient number of switch ports. In conclusion, this meant that the network could adapt to the institution's evolving connectivity requirements.

Table 14

Scalability

Question	Response	Frequency	Percentage
Is the wireless network designed to scale efficiently as demand grows?	Yes	1	100%
	No	0	0%
Does the proposed IP addressing scheme allow for future network expansion?	Yes	1	100%
	No	0	0%
Can the proposed network infrastructure accommodate a high number of users?	Yes	1	100%
	No	0	0%
Does the network have sufficient switch ports to cater to future enlargement?	Yes	1	100%
	No	0	0%

The IT expert's assessment confirmed that a security system was well implemented within the network infrastructure. Periodic security audits and vulnerability assessments were performed to identify risks. VLAN configurations and access controls were in place to properly segment network traffic. Standard Wi-Fi authentication security was also enforced to control access. However, unauthorized access from malicious users remained a risk, necessitating continuous monitoring and security enhancements, as stated in Table 15.

Table 15

Security

Question	Response	Frequency	Percentage
Are regular security audits and vulnerability assessments conducted for detecting potential risks?	Yes No	1 0	100% 0%
Are there VLAN configurations and access controls applied to segment the network traffic?	Yes No	1 0	100% 0%
Is there any Wi-Fi security standard authentication in place on the network?	Yes No	1 0	100% 0%
Is there risk for unauthorized access by malicious users through the network?	Yes No	1 0	100% 0%

Regarding the design's manageability, the IT expert indicated that in Table 16 the design aimed for efficient management. The system managed resources and their usage, such as internet bandwidth, through centralized network configurations and updates. A network controller handled multiple access points, providing seamless connectivity. Automated monitoring tools were also in place to detect and automatically resolve network issues, ensuring a higher level of reliability with reduced downtime.

Table 16

Manageability

Question	Response	Frequency	Percentage
Will the network optimize resource usage, including internet bandwidth?	Yes	1	100%
	No	0	0%
Is there a central system that applies network configurations and updates?	Yes	1	100%
	No	0	0%
Can the network controller manage a large number of WAPs?	Yes	1	100%
	No	0	0%
Do automated monitoring tools detect and respond to the issues affecting the network?	Yes	1	100%
	No	0	0%

Furthermore, the network infrastructure was built to provide seamless connectivity across the campus, allowing users to move freely without disruption as shown in Table 17. Bandwidth was effectively allocated across dedicated Wi-Fi networks, and Wi-Fi Mesh technology provided redundancy and fault tolerance for network stability. According to the IT expert's evaluation, clear user classification was noted to have further enhanced security and optimized resource distribution.

Table 17

Availability

Question	Response	Frequency	Percentage
Can users roam across the campus with minimal disruption to their wireless connection?	Yes	1	100%
	No	0	0%
Are dedicated Wi-Fi networks assigned to different user groups?	Yes	1	100%
	No	0	0%
Does the Wi-Fi Mesh technology provide sufficient redundancy and fault tolerance?	Yes	1	100%
	No	0	0%
Is there a clear classification of the users on the network?	Yes	1	100%
	No	0	0%

The network assessment highlights its scalability, security, manageability, and availability. The infrastructure supports future growth with adequate IP addressing and switch capacity. Security measures, including audits, VLAN segmentation, and Wi-Fi authentication, are in place, though unauthorized access remains a concern. Efficient resource management, centralized configurations, and automated monitoring enhance manageability. Availability is ensured through seamless roaming, dedicated networks, and Wi-Fi Mesh for redundancy. Overall, the network is well-equipped to meet current and future demands with reliability and security.

Discussions

Standardizing the network infrastructure through devices from one vendor provides more efficiency in configuration, management, and overall network performance. With all devices running within the same environment, administrators can simplify network monitoring and troubleshooting through a single interface, eliminating complexities of managing different platforms. This method guarantees that all features and updates are compatible across devices to avoid possible integration problems that come with combining different brands.

At City College of San Fernando (CCSF), the implementation of Ubiquiti U6-LR access points is a significant factor in enhancing campus connectivity. Given the campus's single-building structure with adjacent rooms, seamless Wi-Fi coverage is essential to provide students and faculty with consistent connectivity. The U6-LR access points feature built-in seamless roaming, enabling users to move between rooms without experiencing disconnections. This is particularly beneficial in an educational setting where students and professors frequently move between classrooms, offices, and common areas. By automatically connecting devices to the nearest and strongest access point, network resources are conserved and shared more effectively, providing reliable and consistent internet access throughout the campus.

The installed access points have inherent mesh technology capabilities, which increase the network's redundancy and reliability. This means that if an AP loses its primary uplink, it can automatically connect with neighboring access points and maintain seamless

connectivity. The integration of this technology ensures enhanced coverage and fault tolerance, guaranteeing that network interruptions will not significantly impact users.

The proposed network system addresses the limitations of the previous topology, where three separate ISP networks were not unified under a single framework. The teachers' network, while previously offering stable coverage across the entire building, experienced weak signals on the 3rd and 4th floors, resulting in connectivity dead zones. The student network was even more restricted, with only one access point per floor, leading to limited coverage and unreliable connectivity. The new design consolidates these networks into a single, organized topology, ensuring optimal bandwidth allocation, increased coverage, and centralized management for both students and staff across the entire campus.

For seamless connectivity on every floor, U6-LR access points were placed strategically in every wing of the building for robust signal coverage in all the areas. These APs were ceiling-mounted for optimal signal dispersal while factoring in concrete walls that would interfere with wireless transmission. Special care was taken in high-density zones like student lounges where connectivity is necessary for academic use and online use. This deployment allows students and staff to travel freely between various parts of the campus without having to endure connection drops, dramatically enhancing the user experience.

All wireless access points are managed via the UniFi Network Controller, which offers administrators a single, centralized interface for configuration and monitoring. The Wi-Fi roaming capability, which is inherent in the equipment, guarantees that as long as a device stays on one SSID, it will be able to switch from one access point to another without dropping its connection. This is especially useful in the City College of San Fernando

(CCSF), where strategically positioned APs guarantee continuous coverage of various sections of the building.

As both roaming and mesh networking are integrated into the access points, extra configurations for these functions are negligible. After the APs are provisioned via the UniFi Network Controller, they will naturally form multiple uplinks with other accessible APs. This provides redundancy, such that if a primary link fails, the access points can continue to communicate through surrounding units, providing a stable and reliable network.

Regarding security, unauthorized access is mitigated through the implementation of both MAC address filtering and voucher-based authentication. Users are required to register their device's MAC address before joining the network, ensuring that only authorized devices can access it. Furthermore, instead of a pre-shared key, the SSID utilizes a unique voucher code provided by administrators, requiring users to enter this code for network access. This enhances network security by discouraging unauthorized system access and minimizing the risk of password leaks.

The new network architecture allocates certain ISPs to specific user groups. The first ISP is assigned to staff and teachers to provide stable and continuous connectivity for academic and administrative purposes. The second ISP is reserved for students, which enhances their experience in online learning by avoiding overloading due to many connections at the same time. The third ISP, once unused, is still allocated to wired connections but also set up as a backup connection in case one of the two main ISPs is down. Router policies on FortiGate are used to prevent each group from accessing an ISP other than its assigned one, ensuring an orderly and efficient distribution of bandwidth as well as

providing redundancy in case of a failure. To perform load balancing, policy-based routing was implemented on FortiGate to distribute traffic across the three ISPs. Router policies help prevent certain devices from accessing an ISP other than its assigned one, thus preventing users from overwhelming a single network while others remain unused. Automatic failover is provided in case of network failure, so that impacted users are redirected to a functioning ISP without any disruption in service. This strategy ensures maximum bandwidth usage while preserving network stability and efficiency.

The DHCP server is controlled via FortiGate, allocating IP addresses dynamically in line with VLAN setups. Security features have been augmented by MAC address filtering and voucher-based authentication, only allowing registered devices access to the network. Registration of the MAC addresses of students and lecturers is a necessity, whereas voucher-based authentication is applied in allowing students access to the network in a secure manner. Password-protected accounts are given to administrative staff for additional protection of sensitive institutional information.

Conclusions

The study indicated that the existing Wi-Fi network at City College of San Fernando had significant limitations regarding coverage, performance, and security. Survey responses revealed that 68% of students and faculty experienced frequent disconnections, particularly during peak hours, negatively impacting online learning and administrative tasks. Furthermore, 72% of respondents reported slow internet speeds, highlighting a need for bandwidth improvement and efficient network management.

Security was also a concern, as 61% of users expressed worry about easy unauthorized access due to weak authentication methods. Conversely, 65% indicated they would feel secure if WPA2-Enterprise authentication with individualized credentials was implemented. Wi-Fi roaming was another area of concern, with 58% of respondents experiencing interruptions while moving between locations within buildings.

Proposed network improvements to address these issues included unified management by a single vendor, mesh networking to enhance campus connectivity, and load balancing for optimization. With 70% of users supporting a network upgrade, the research supported the need for scalable and secure solutions that meet the increasing digital demands of the institution. The implementation of these recommendations would result in a more stable, high-performing network providing seamless connectivity for students, faculty, and staff.

These improvements involved adjustments to the network, load balancing for resource utilization optimization, and centralized management by a single vendor. The two-thirds user support for a network upgrade further affirmed the need for scalable and secure solutions that meet the institution's growing digital demands. Implementing these recommendations would establish a more stable and high-performing network, sustaining seamless connectivity for students, faculty, and staff.

Recommendations

This study, conducted to improve Wi-Fi coverage and network quality at City College of San Fernando, Pampanga, suggests that future research should focus on optimizing wireless access point placement using site-dependent predictive modeling and heatmaps. Given the increasing student population and the proliferation of digital platforms, ensuring continuous connectivity within classrooms, laboratories, and outdoor spaces is crucial. Additionally, leveraging modern load balancers and Quality of Service (QoS) features will enable efficient bandwidth utilization, thereby reducing network congestion during peak usage times. Security could be further enhanced by implementing WPA3 encryption, role-based access control, and multi-factor authentication.

Another recommendation is to maximize the use of fiber internet from PLDT, running at 1 Gbps, for students instead of the current Starlink ISP, to improve internet access and ensure a more stable connection. The Starlink ISP currently experiences fluctuating speeds ranging from 80 to 350 Mbps, which is insufficient for a large number of concurrent users. Transitioning to PLDT (1 Gbps) could provide the institution with a better and faster internet connection, significantly reducing congestion and optimizing the overall user experience. This change would greatly benefit students by facilitating easier access to online learning materials, research, and participation in various digital activities without frequent connectivity issues.

In conclusion, the Wi-Fi optimization study projected for City College of San Fernando, Pampanga, can serve as a foundation for future research. As the college expands, scalable services such as cloud-managed Wi-Fi and SDN should be considered. Alternatively, connectivity technologies like 5G and hybrid networks are also being upgraded

for enhanced performance. Educating users on the correct and efficient use of the network for maximum bandwidth and security is also recommended. Periodic performance evaluations will ensure that the network's performance remains optimal over time and can be adapted in response to future technological advancements.

References

Bheevgade, P., Saha, C., Nath, R., Dabhade, S., Barot, H., & Junare, S. O. (2023). The rise of public Wi-Fi and threats. In Lecture notes in electrical engineering (pp. 175–189). https://doi.org/10.1007/978-981-99-5091-1_13

Digital around the world — DataReportal – Global Digital Insights. (n.d.). DataReportal – Global Digital Insights. https://datareportal.com/global-digital-overview

Dudhat, A., Nusantoro, H., & Purba, A. E. (2022). Indoor Wireless Network Coverage Area Optimization. DOI:10.34306/ijcitsm.v2i1.86

Ferreira, P., Belo, R., Inbar, Y., & Turner, R. (n.d.). *Wifi Usage on Campus and Students Academic Performance*. Carnegie Mellon University. https://www.cmu.edu/heinz/itea/pdfs/paper-wifi-university.pdf

Frolova, N., Mykhalchuk, I., & Tyshchenko. (2022, June). *PROTECTION OF PUBLIC WI-FI SPOTS*. ResearchGate. Retrieved September 19, 2024, from https://www.researchgate.net/publication/363101518_PROTECTION_OF_PUBLIC_WI-FI_SPOTS

Grenville, A., Klumpenhouwer, W., Chui, N., & Shalaby, A. (2023). Methods for Analyzing System Performance and User Experience Using WiFi Connection Data. Methods for Analyzing System Performance and User Experience Using WiFi Connection Data. https://doi.org/10.31219/osf.io/sv6cg

Kenner Electrics. (n.d.). *The benefits of installing a wireless access point*. Kenner Electrics. Retrieved March 19, 2025, from https://www.kennerelectrics.com.au/blog/the-benefits-of-installing-a-wireless-access-point

K, S. Priya. (2023). WIRELESS NETWORKS IN DAY TODAY LIFE. *International Scientific Journal of Engineering and Management*, *02*(04). https://doi.org/10.55041/isjem00266

Kamienski, C., Ratusznei, J., Trindade, A., & Cavalcanti, D. (2020). Profiling of a large-scale municipal wireless network. Wireless Networks, 26(7), 5223–5253. https://doi.org/10.1007/s11276-020-02390-4

Lixiong, L., & Jinju, L. (2020). Wi-Fi connection management method, terminal and system. SciSpace - Paper. https://typeset.io/papers/wi-fi-connection-management-method-terminal-and-system-1ymk6v8sq6

Lotfy, A. Y., Zaki, A. M., Abd-El-Hafeez, T., & Mahmoud, T. M. (2021). Privacy issues of public Wi-Fi networks. In Advances in intelligent systems and computing (pp. 656–665). *https://doi.org/10.1007/978-3-030-76346-6_58*

Maimon, D., Howell, C. J., Jacques, S., & Perkins, R. C. (2020). Situational awareness and public Wi-Fi users' self-protective behaviors. Security Journal, 35(1), 154–174. https://doi.org/10.1057/s41284-020-00270-2

Muttair, K. S., Zahid, A. Z. G., Al-Ani, O. A. S., AL-Asadi, A. M. Q., & Mosleh, M. F. (2021). Implementation mixed wireless network with lower number of Wi-Fi routers for optimal coverage. *International Journal of Online and Biomedical Engineering (iJOE)*, *17*(13), 59-80

https://www.researchgate.net/profile/Karrar-Muttair/publication/356799301_Implementation_Mixed_Wireless_Network_with_Lower_Number_of_Wi-Fi_Routers_for_Optimal_Coverage/links/61adf88b50e22929cd500823/Implementation-Mixed-Wireless-Network-with-Lower-Number-of-Wi-Fi-Routers-for-Optimal-Coverage.pdf

O'Brien, O., Sumich, A., Kanjo, E., & Kuss, D. (2022). *WiFi at University: A Better Balance between Education Activity and Distraction Activity Needed.* ScienceDirect. https://www.sciencedirect.com/science/article/pii/S2666557321000422

Oh, M., Kim, J., & Shin, J. (2022). Does the improvement of public Wi-Fi technology undermine mobile network operators' profits? Evidence from consumer preference. Telematics and Informatics, 69, 101786. https://doi.org/10.1016/j.tele.2022.101786

Oliveira, L., Obraczka, K., & Rodriguez, A. (n.d.). *Characterizing User Activity in WiFi Networks: University Campus and Urban Area Case Studies*. Retrieved October 13, 2024, from https://par.nsf.gov/servlets/purl/10082485

Papadopoulos, G. Z., Theoleyre, F., & Thubert, P. (2020). Operations, administration and maintenance (OAM) features for reliable and available wireless (RAW) networks. *Internet Technology Letters*, *3*(4), e163.https://hal.science/hal-02613878/

Pundalik, Chavan., D., K., S., Reddy., Sharada, P, N. (2022). An analysis of wireless networks. International journal of innovative research in advanced engineering, 9(8):288-299. doi: 10.26562/ijirae.2022.v0908.25

Ribeiro, M., Teixeira, D., Barbosa, P., & Nunes, N. J. (2023). Using passive Wi-Fi for community crowd sensing during the COVID-19 pandemic. *Journal of Big Data*, *10*(1). https://doi.org/10.1186/s40537-022-00675-3

What is an Access Point? (2024, February 27). Cisco. https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/what-is-access-point.html

What is Wireless Access Point? Exploring the Benefits and Features of a Wireless Access Point - zenarmor.com. (2024, August 28). https://www.zenarmor.com/docs/network-basics/what-is-wireless-access-point

Young, W., Allen, L., & Warfield, K. (n.d.). *Developing Online/Hybrid learning Models for higher education programs.* https://eric.ed.gov/?id=EJ1120647

Appendix A
Cover Letter

HOLY ANGEL UNIVERSITY SCHOOL OF COMPUTING

January 28, 2025

ATTY. GLORIA J. VICTORIA-BAÑAS, CPA, DPA, CESO V
COLLEGE ADMINISTRATOR/PRESIDENT
CONCURRENT VICE PRESIDENT FOR ADMINISTRATION
City College of San Fernando

Thru:

MR. JUSTINE FRANCISCO
OIC, IT-PROGRAMMING
City College of San Fernando

Dear Atty. Victoria-Bañas,

As part of the requirements for the **Bachelor of Science in Information Technology with area of specialization in Network Administration**, students enrolled in the course **6NETCAP1 – Network Capstone Project (NW401)** are required to create a research paper that will contribute towards the development of their Undergraduate Capstone Project. The course includes the requirement to identify respondents and conduct data gathering through interviews and surveys relevant to our study. The objective of this course is to provide students the opportunity to create a research paper that could significantly impact the field they have chosen.

Through this letter, we respectfully seek your approval to conduct a survey aimed at evaluating the current performance and reliability of the Wi-Fi network at City College of San Fernando. The goal of this survey is to assess the current state of the network and gather feedback on areas for improvement. Specifically, we are requesting your consent to collect insights on the following aspects:

1. The reliability of the Wi-Fi connection during peak hours.
2. The typical connection times and how quickly users are able to access the internet. 3. The frequency of interruptions or disconnections while using online services. 4. The perceived importance of scalability and ease of access in the design of a new wireless network for the campus.
5. The likelihood of support for a new network infrastructure that prioritizes optimization and scalability.
6. The potential impact of network monitoring tools on the efficiency and operation of the Wi-Fi network.

In addition to the survey, we respectfully request permission to conduct interviews with relevant university staff or technical personnel to gather further insights into the Wi-Fi infrastructure's performance, challenges, and future development plans. We believe that this study will provide valuable data to improve the Wi-Fi infrastructure and enhance the overall experience for students, faculty, and staff. Thank you for considering our request. We look forward to your feedback and approval.

Sincerely,

Bondoc, Michael Owen G.

Jimenez, Christian Allen S.

Reyes, John Clarence G.

Tulabut, Emmanuel Greyco B.

Noted by:

MR. RAYMOND A. CABRERA
Capstone Adviser
6NETCAP1

DR. MARLON I. TAYAG
Dean
School of Computing

HOLY ANGEL UNIVERSITY

HOLY ANGEL UNIVERSITY SCHOOL OF COMPUTING

October 15, 2024

ATTY. GLORIA J. VICTORIA-BAÑAS, CPA, DPA, CESO V
COLLEGE ADMINISTRATOR/PRESIDENT
CONCURRENT VICE PRESIDENT FOR ADMINISTRATION
City College of San Fernando

OCT 15 2024 12:07 NN
Erica

Thru:

MR. JUSTINE FRANCISCO
OIC, IT-PROGRAMMING
City College of San Fernando

Dear Atty. Victoria-Bañas,

As part of the requirements for the **Bachelor of Science in Information Technology with area of specialization in Network Administration**, students enrolled in the course **6NETCAP1 – Network Capstone Project (NW401)** are required to create a research paper that will contribute towards the development of their Undergraduate Capstone Project. The course includes the requirement to identify respondents and conduct data gathering through interviews and surveys relevant to their study. The objective of this course is to provide students the opportunity to create a research paper that could significantly impact the field they have chosen.

The following students have expressed their intention to consider your prestigious institution, **City College of San Fernando**, as the locale for their project proposal:

Bondoc, Michael Owen G.	Jimenez, Christian Allen S.
Reyes, John Clarence G.	Tulabut, Emmanuel Greyco B.

Through this letter, we respectfully seek your approval to conduct a study on the layout of the Wi-Fi infrastructure at City College of San Fernando. Specifically, we are requesting information on the following:

- The layout and topology of the Wi-Fi infrastructure
- The bandwidth capacity of the routers in use
- The types of routers deployed across the campus
- The physical location of the routers
- The coverage areas provided by the routers
- The internet service provider currently supporting the university's network
- Information on the cable structure, including the types of cables used, their layout, specifications, and installation standards.
- Permission to conduct interviews with university staff or technical personnel to gather insights into the Wi-Fi infrastructure's performance, challenges, and development plans.

The information collected will be instrumental in helping us analyze and recommend potential improvements to enhance the university's Wi-Fi performance. Rest assured that any information provided will be used strictly for academic purposes, and we will maintain the utmost confidentiality throughout the process.

Thank you very much for your consideration. We look forward to your favorable response.

Sincerely,

Noted by:

10/15

MR. JOHN PAUL P. MIRANDA
Instructor
6NETCAP1

DR. MARLON I. TAYAG
Dean
School of Computing

#1 HOLY ANGEL AVENUE, STO. ROSARIO, ANGELES CITY, PHILIPPINES 2009
TEL. NOS.: (045) 888-8691; 888-2902; 887-5748; 887-2455; 624-5277; 625-9619 | FAX: (045) 888-1754; 888-2514
EMAIL: HAU@HAU.EDU.PH | WWW.HAU.EDU.PH

HOLY ANGEL UNIVERSITY

HOLY ANGEL UNIVERSITY SCHOOL OF COMPUTING

January 28, 2025

ATTY. GLORIA J. VICTORIA-BAÑAS, CPA, DPA, CESO V
COLLEGE ADMINISTRATOR/PRESIDENT
CONCURRENT VICE PRESIDENT FOR ADMINISTRATION
City College of San Fernando

Thru:

MR. JUSTINE FRANCISCO
OIC, IT-PROGRAMMING
City College of San Fernando

Dear Atty. Victoria-Bañas,

As part of the requirements for the **Bachelor of Science in Information Technology with area of specialization in Network Administration**, students enrolled in the course **6NETCAP1 – Network Capstone Project (NW401)** are required to create a research paper that will contribute towards the development of their Undergraduate Capstone Project. The course includes the requirement to identify respondents and conduct data gathering through interviews and surveys relevant to our study. The objective of this course is to provide students the opportunity to create a research paper that could significantly impact the field they have chosen.

We are writing to respectfully request your approval to connect to the network infrastructure using TP-Link Omada at City College of San Fernando in order to conduct a series of tests to evaluate its overall connectivity, scalability, and ease of access. Our primary goal is to assess the network's performance under typical usage conditions and to identify any potential areas for improvement.

Specifically, we seek your consent to perform the following activities:

- **Test the reliability and performance** of the network connection across various locations on campus.
- **Evaluate the scalability of the network**, particularly its ability to handle a high number of simultaneous users during peak hours.
- **Assess the ease of access** for users connecting to the network, ensuring it meets the needs of students, faculty, and staff.

We believe that these tests will provide essential insights into the current state of the network infrastructure, which will help guide future improvements and optimizations. Your approval will enable us to conduct a thorough evaluation that could enhance the overall network experience for all users on campus.

Sincerely,

Bondoc, Michael Owen G.

Jimenez, Christian Allen S.

Reyes, John Clarence G.

Tulabut, Emmanuel Greyco B.

Noted by:

MR. RAYMOND A. CABRERA
Capstone Adviser
6NETCAP1

DR. MARLON I. TAYAG
Dean
School of Computing

Appendix B
Publication Materials for CCSFP

Appendix C
Interview Guide Questions

a. Network Topology & Infrastructure

i. What is the current network topology of the campus (diagram)?

ii. Are there any redundant network components or underutilized resources?

iii. Are there any areas on campus with weak or no WI-Fi signal?

iv. How frequently is the network hardware updated or replaced?

v. Are the existing routers and access points capable of supporting modern standards? (eg., Wi-Fi 6)?

vi. Are there outdated devices in the network that could be slowing it down?

vii. What steps have been taken to optimize access point placement?

viii. Are outdoor areas, such as courtyards or sports fields, included in the Wi-Fi coverage plan?

b. Performance & Speed

i. What is the current ISP, speed, bandwidth, etc.?

ii. What is the average Wi-Fi speed experienced by users across different areas of the campus?

iii. Are there specific times of the day when network speed significantly drops?

iv. How does the network handle simultaneous connections during large events or examinations?

v. What is the average number of devices connected to the network during peak hours?

c. Usage & Connectivity

i. How many devices are connected (wired & wireless) regularly? (PCs, routers, APs, application servers, etc.)

ii. What specific network tools are used?

iii. Do they implement LMS or other cloud platforms for online access in the campus?

iv. How do students, teachers, and guests connect to the network (is there a voucher system)?

v. Are there separate networks for students, staff, and guests?

d. Security & Monitoring

i. What security measures are in place to prevent unauthorized access to the Wi-Fi network?

ii. Is the network vulnerable to common threats like unauthorized devices or malware?

e. User Experience & Common Issues

i. Are students and staff satisfied with the current Wi-Fi performance?

ii. What are the common complaints or issues raised by users regarding the network?

iii. Do users experience frequent disconnections or interruptions?

iv. Cite the difficulties encountered in their current network.

f. Scalability & Future Upgrades

i. Is the current network infrastructure scalable to accommodate future growth in student population and devices?

ii. Are there plans to implement newer technologies, such as mesh Wi-Fi or AI-based traffic optimization?

iii. What budgetary constraints impact the ability to upgrade or expand the network?

g. Optimization Strategies & Reliability

i. Have any recent surveys or heatmaps been conducted to assess Wi-Fi coverage across the campus?

ii. Are there tools or software used for dynamic bandwidth allocation and load balancing?

iii. What steps have been taken to optimize access point placement?

Appendix D
Survey Questionnaires in Google Form

Optimizing Wi-Fi Coverage and Network Efficiency at City College of San Fernando, Pampanga

Dear Participant,

We are fourth-year students from the School of Computing at Holy Angel University, currently pursuing a Bachelor of Science in Network Administration. As part of our academic requirements, we are conducting a capstone project titled "Optimizing Wi-Fi Coverage and Network Efficiency at City College of San Fernando, Pampanga."

This survey aims to gather valuable insights and feedback on the current state, performance, and overall user satisfaction with the Wi-Fi network on campus. Your responses will provide critical data that will assist us in proposing effective solutions to enhance network coverage, efficiency, and user experience.

The survey will only take a few minutes to complete, and all responses will be kept confidential and used solely for research purposes. Your participation is vital to the success of our study and will significantly contribute to achieving our project goals.

We sincerely appreciate your time and effort in completing this questionnaire. Thank you for your support!

Best regards,
Bondoc, Michael Owen G. (bondocmichaelowen@gmail.com)
Jimenez, Christian Allen S. (caasjimenez@gmail.com)
Reyes, John Clarence G. (jcreyespakzreyes@gmail.com)
Tulabut, Emmanuel Greyco B. (greycoe@gmail.com)

Name (optional):

Your answer

Year Level: *

- ◯ 1st Year
- ◯ 2nd Year
- ◯ 3rd Year
- ◯ 4th Year
- ◯ Other:

Department: *

- ◯ Institute of Information Technology
- ◯ Institute of Business Administration
- ◯ Institute of Education
- ◯ Other:

Data Privacy Assurance

We fully adhere to Republic Act No. 10173, also known as the Data Privacy Act of 2012. All information gathered through this form will be treated with the highest level of confidentiality and used solely for the purposes of our capstone research and development.

In compliance with Section 13 of the law, the processing of sensitive personal and privileged information is generally prohibited, except under the following conditions:

(a) The individual has given explicit consent for their data to be processed for a specific purpose before any processing takes place. In the case of privileged information, all involved parties must provide their consent beforehand.

(b) The processing of such data is authorized by existing laws and regulations, provided that these legal provisions ensure the protection of sensitive and privileged information. Additionally, if the law permits such processing, obtaining consent from the individuals concerned is not required. this one too

I have thoroughly reviewed all the information provided above and hereby give my informed consent to participate and share the required data as outlined *

- ◯ Yes
- ◯ No

1.) How would you rate the reliability of the internet connection in your campus during peak hours? *

- ◯ Very Unreliable
- ◯ Somewhat Unreliable
- ◯ Neutral
- ◯ Somewhat Reliable
- ◯ Very Reliable

2.) How satisfied are you with the current speed and bandwidth of the campus wireless network during off-peak hours? *

- ◯ Very Satisfied
- ◯ Satisfied
- ◯ Neutral
- ◯ Dissatisfied
- ◯ Very Dissatisfied

3.) How often do you experience interruptions or disconnections while using online services? *

- ◯ Never
- ◯ Rarely
- ◯ Sometimes
- ◯ Frequently
- ◯ Always

4.) How long does it typically take for you to connect to the internet? *

- ◯ 0-3 Seconds
- ◯ 4-7 Seconds
- ◯ 8-11 Seconds
- ◯ 11-15 Seconds
- ◯ 15 seconds or longer

5.) How confident are you in the security measures of the current wireless network on campus, especially when accessing sensitive academic or personal data? *

- ◯ Very Confident
- ◯ Confident
- ◯ Neutral
- ◯ Not Confident
- ◯ Not Confident at All

6.) How satisfied are you with the overall performance of the campus wireless network? *

- ◯ Very Satisfied
- ◯ Satisfied
- ◯ Neutral
- ◯ Dissatisfied
- ◯ Very Dissatisfied

7.) How likely are you to support a new wireless network infrastructure that prioritizes both optimization? (better speed, ease of access) and scalability (to accommodate more users and devices)? *

- ◯ Very Unlikely
- ◯ Unlikely
- ◯ Neutral
- ◯ Likely
- ◯ Very Likely

8.) How well do you think the proposed changes to the campus wireless network will improve your overall experience? *

- ◯ Greatly Worsen
- ◯ Somewhat Worsen
- ◯ No Change
- ◯ Somewhat Improve
- ◯ Greatly Improve

9.) How will you rate the proposed simulated network with the use of network monitoring and management tools in enhancing the wireless efficiency overall operation of the CCSFP? *

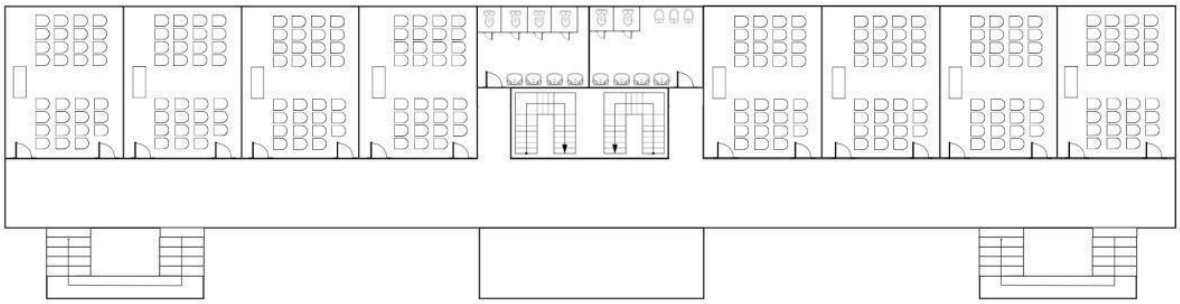
- ◯ Poor
- ◯ Fair
- ◯ Good
- ◯ Very Good
- ◯ Excellent

10.) How well does the proposed network topology align with your needs for reliable and fast wireless access on campus? *

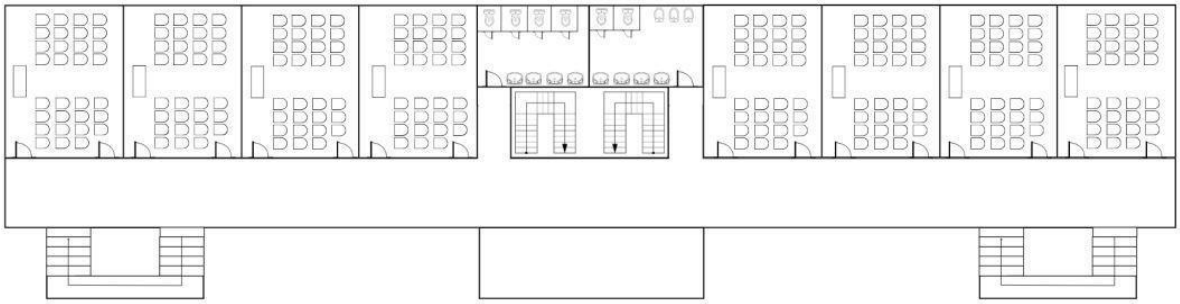
- ◯ Very Well
- ◯ Well
- ◯ Neutral
- ◯ Poorly
- ◯ Very Poorly

Appendix E
Campus Floor Plan

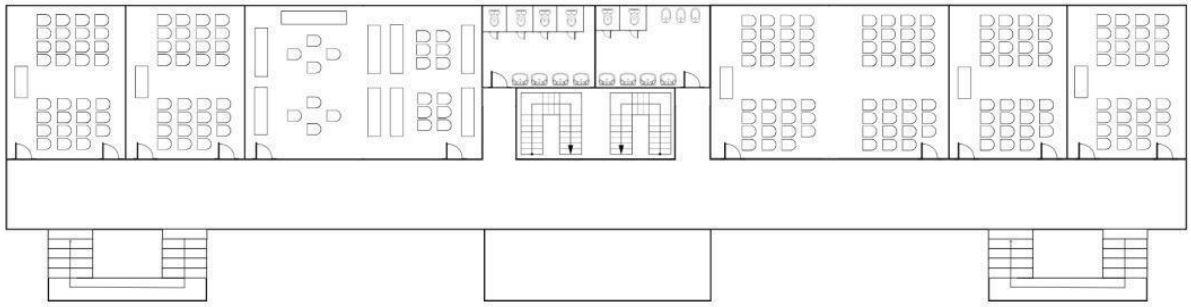
Ground Floor (Faculty, Admin Office, Registrar, and Speech Lab)



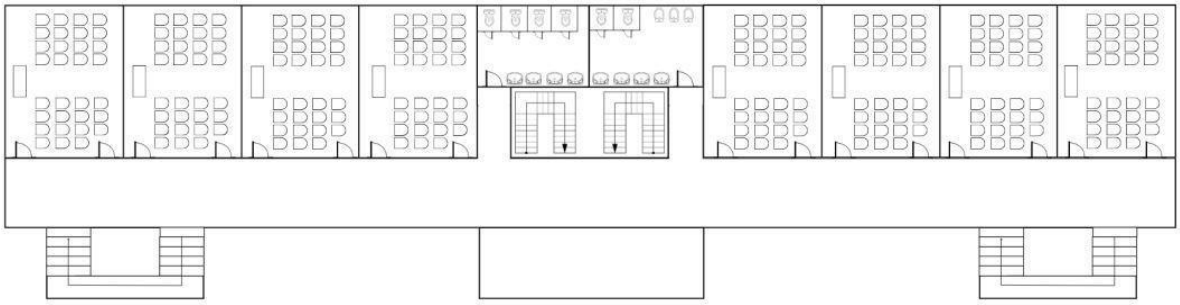
2nd Floor (Classrooms)



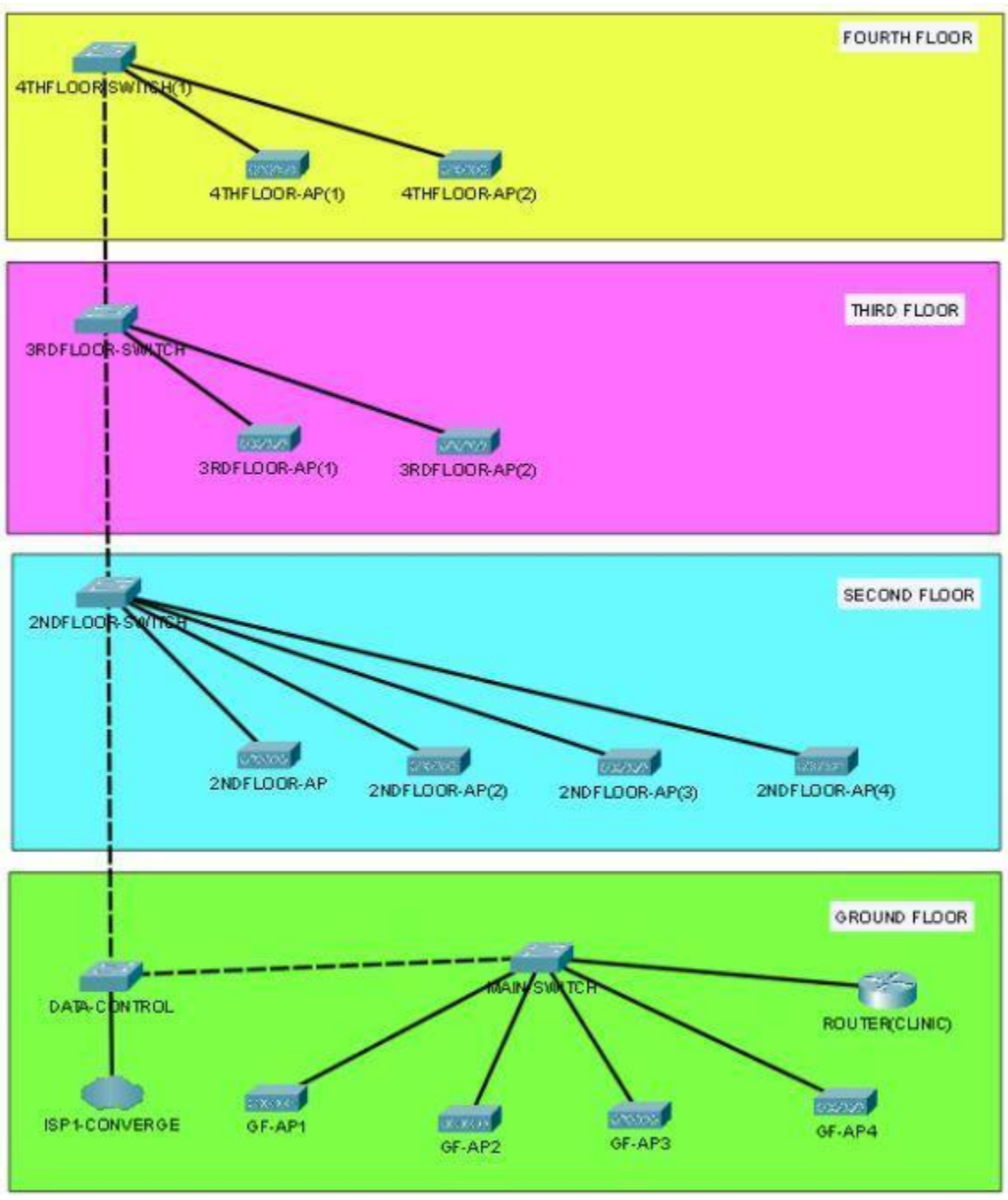
3rd Floor (Computer Laboratories, Library, and Audio Visual Room)



4th Floor (Classrooms and Chemistry Labs)

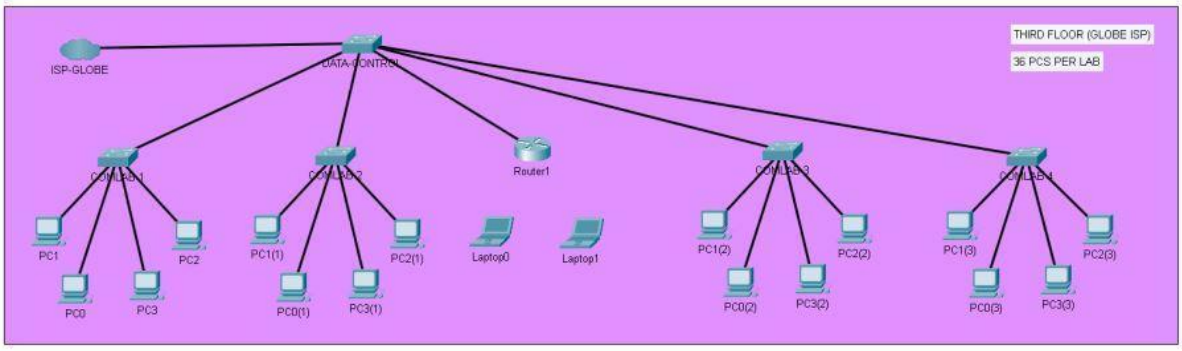


Appendix F
Current Topology Converge ISP



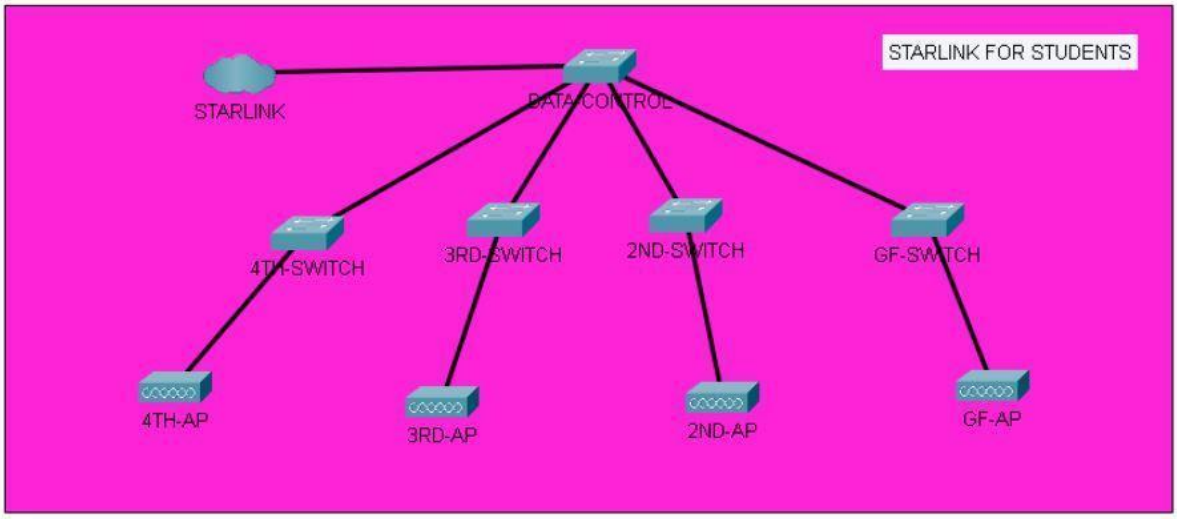
For staffs and admins

Appendix G
Globe ISP Third Floor (Computer Laboratories)



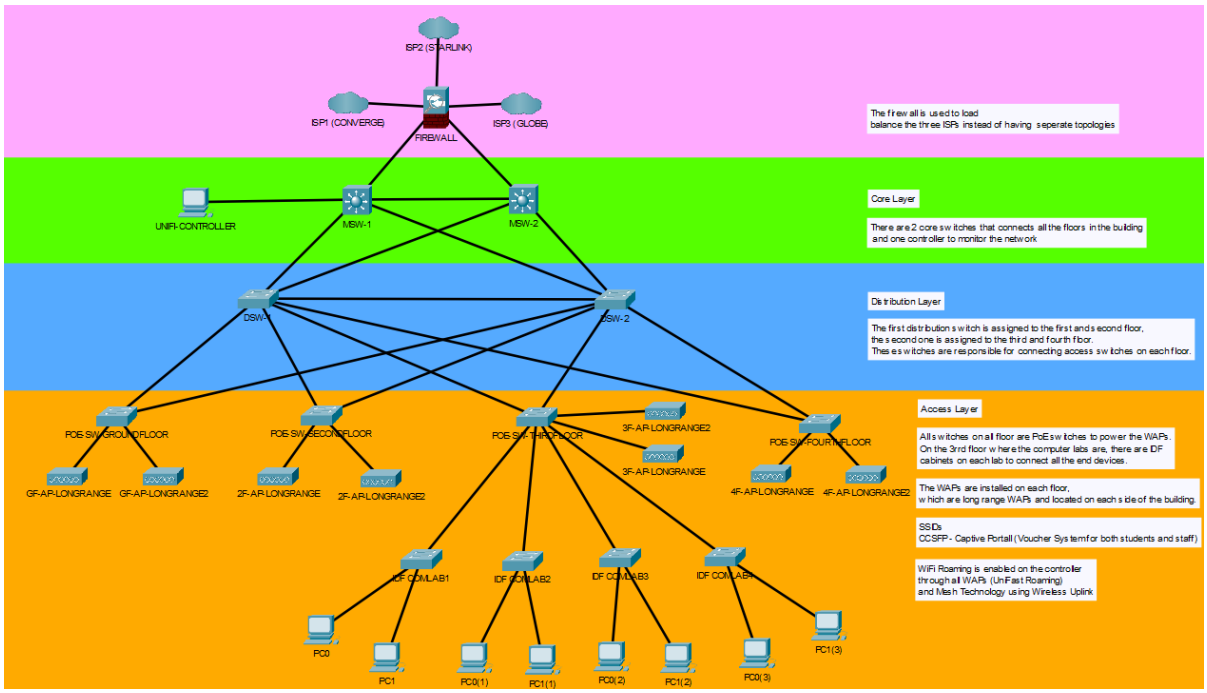
For wired computers and router for the library (Com lab 1-4)

Appendix H
Starlink ISP

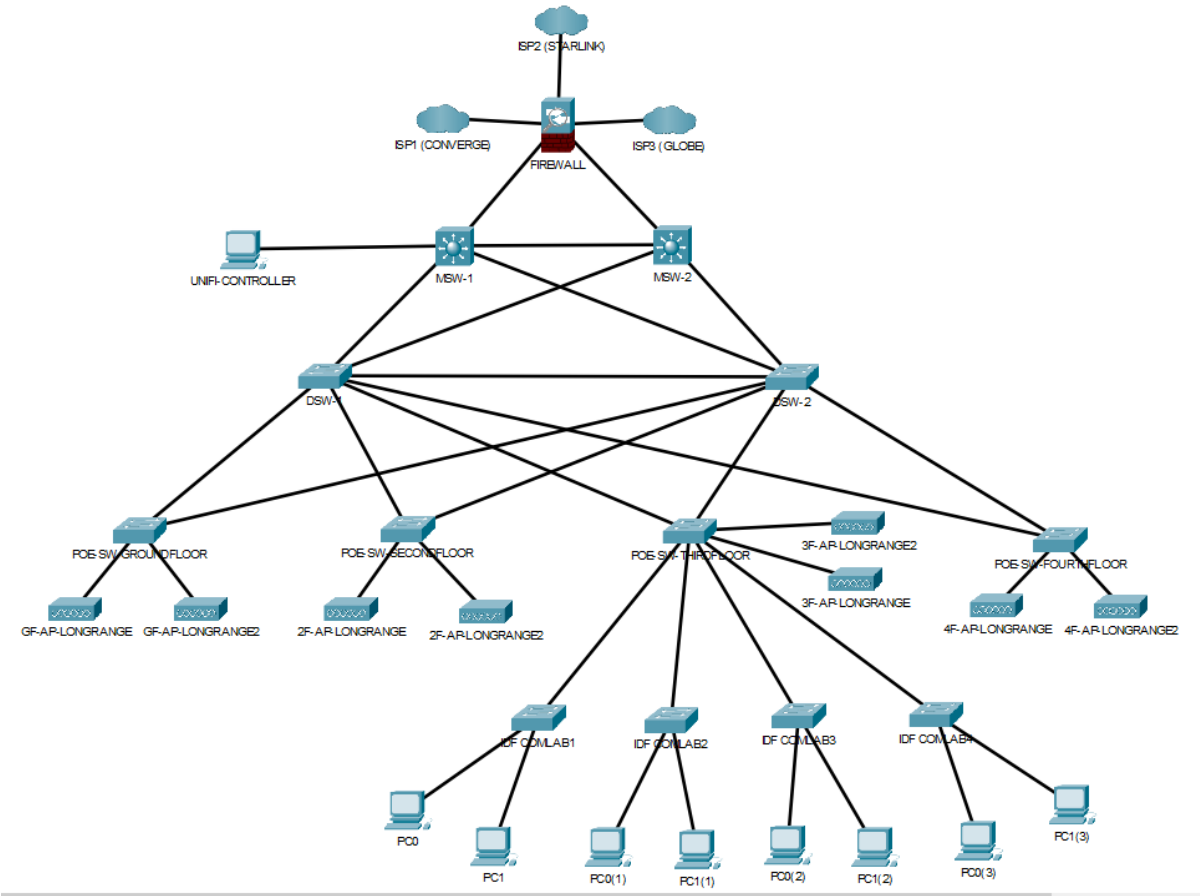


For students

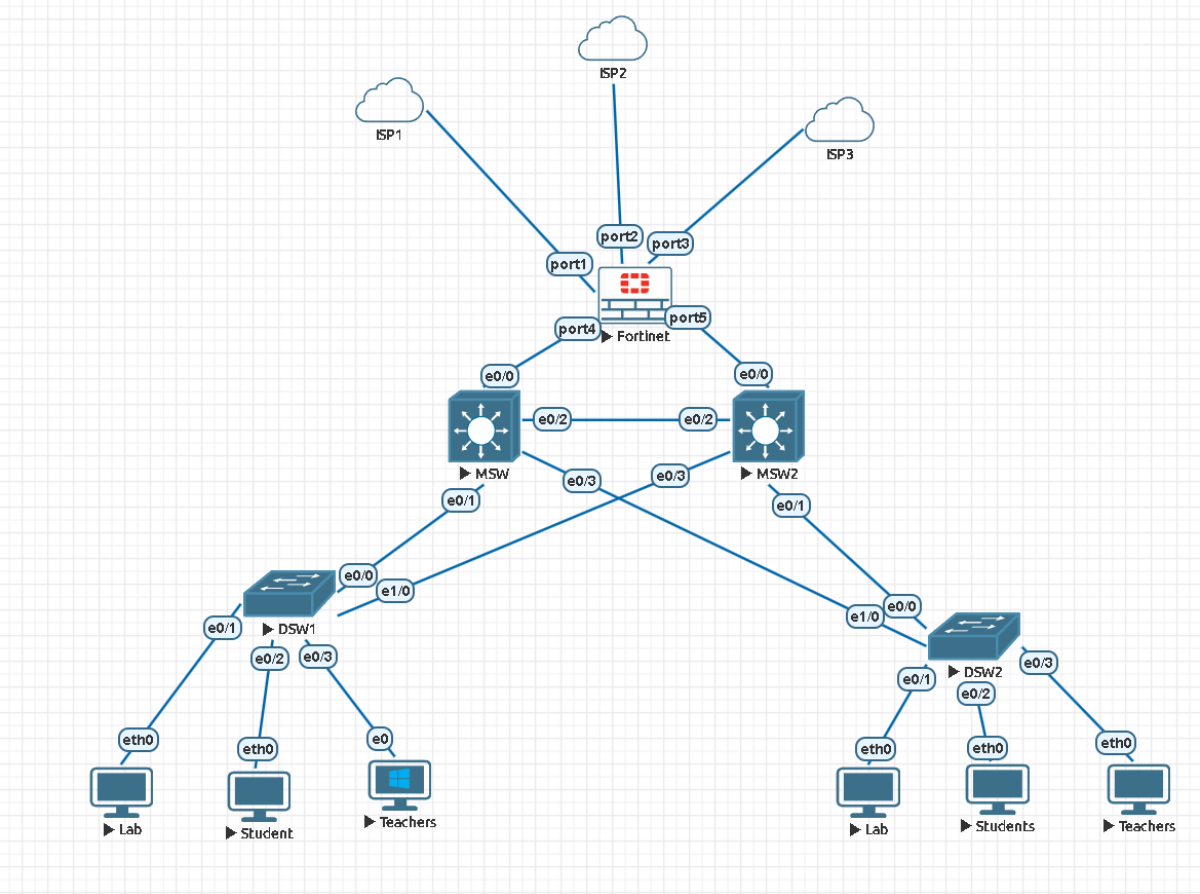
Appendix I
Logical Topology



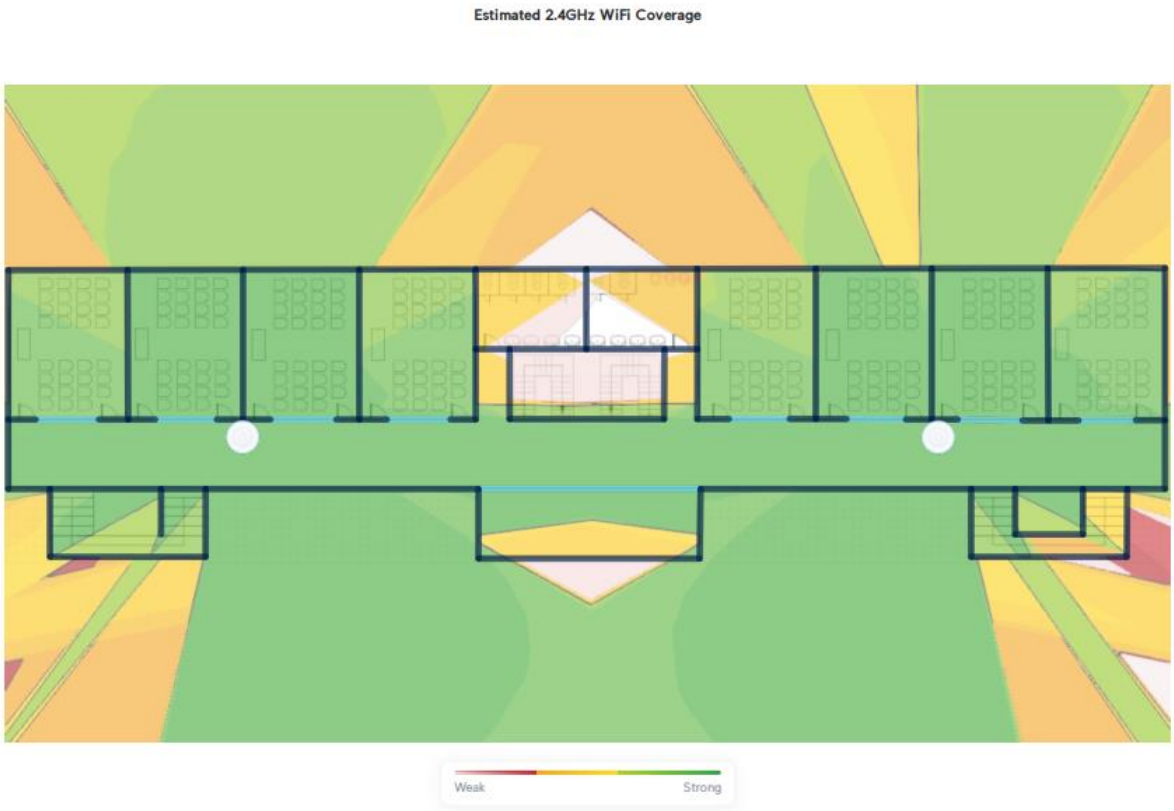
Appendix J
Proposed Topology



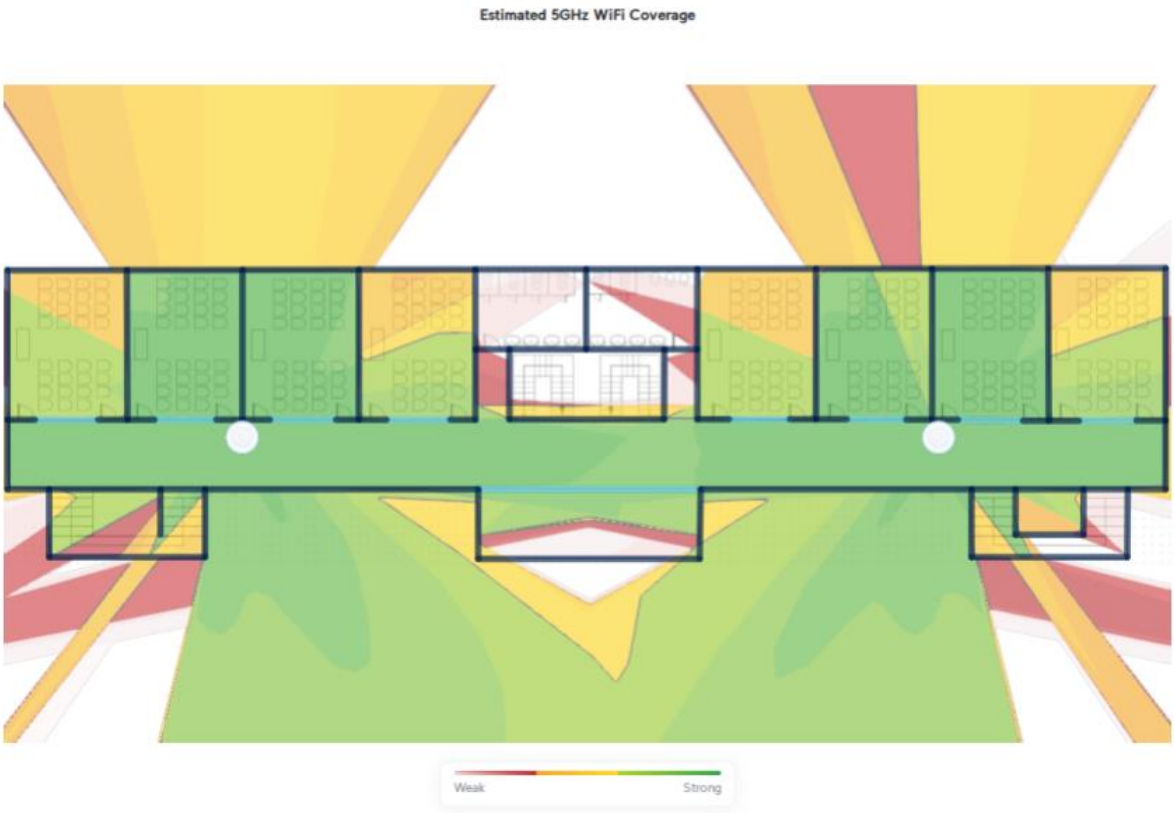
Appendix K
EVE-NG Topology



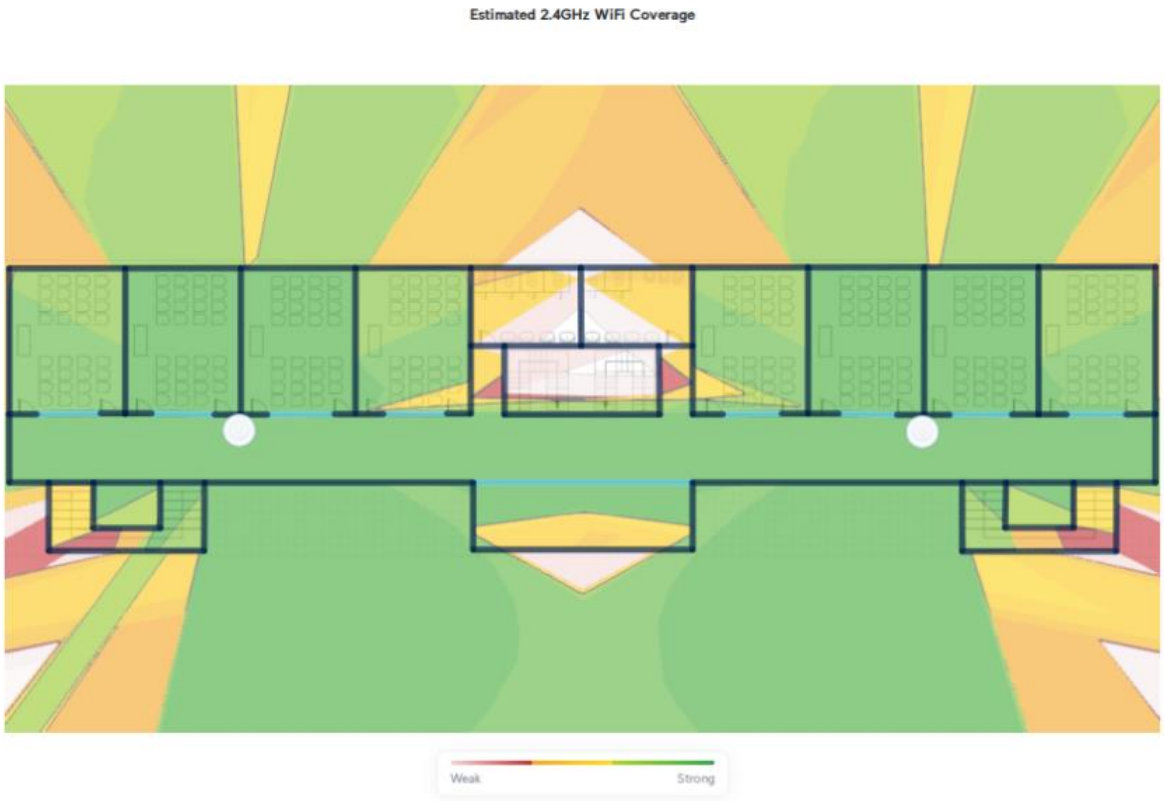
Appendix L
Sample Wi-Fi Coverage



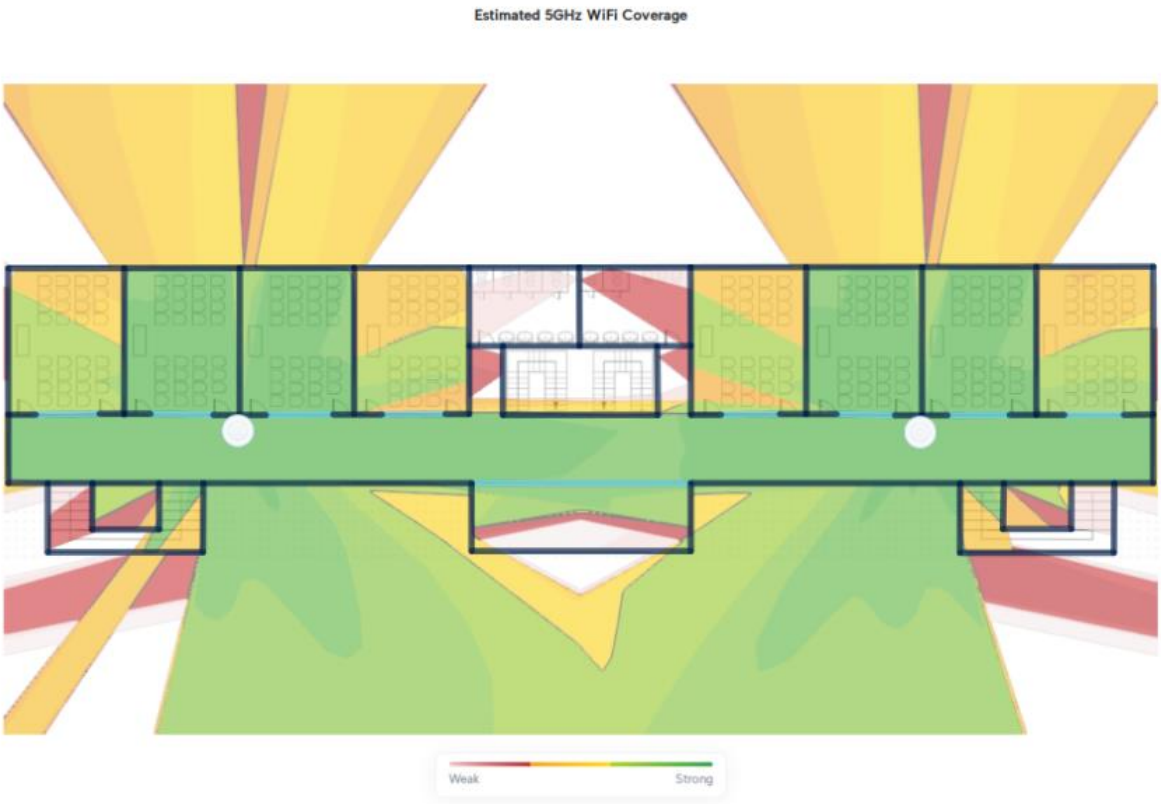
Ground Floor 2.4GHz WiFi Coverage



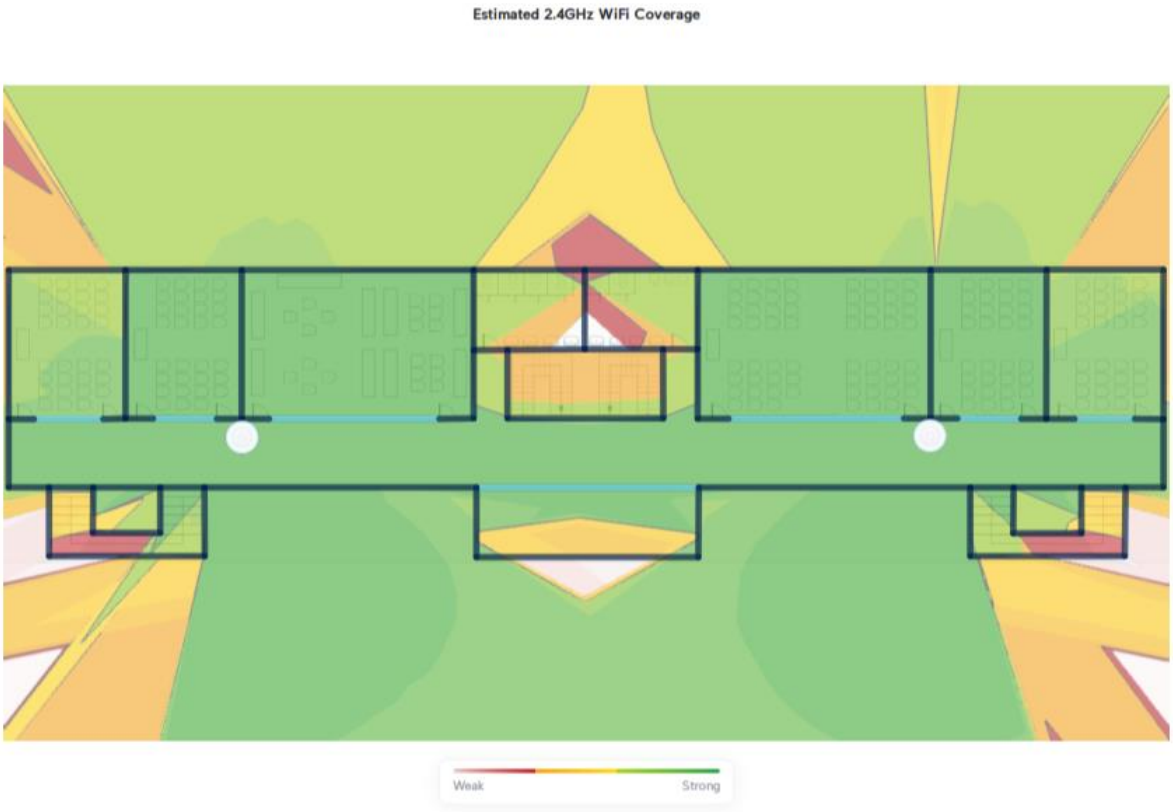
Ground Floor 5GHz WiFi Coverage



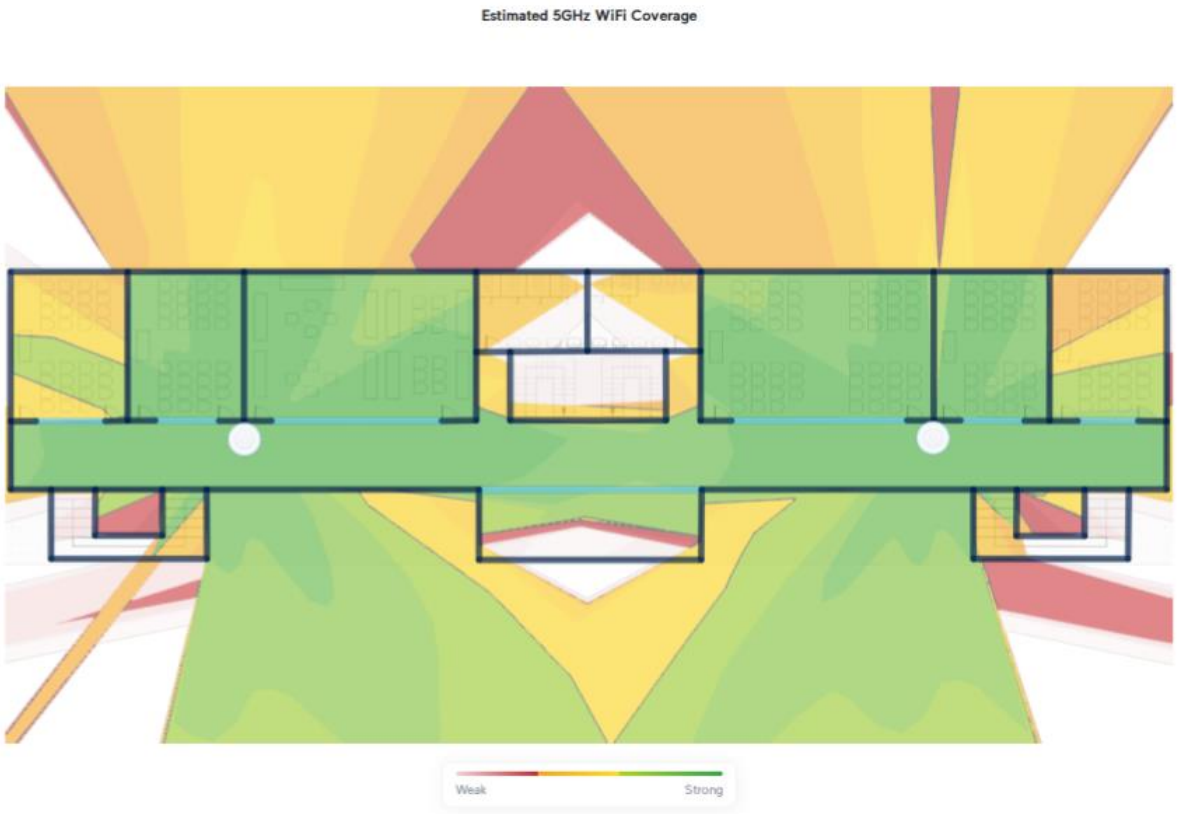
Second Floor 2.4GHz WiFi Coverage



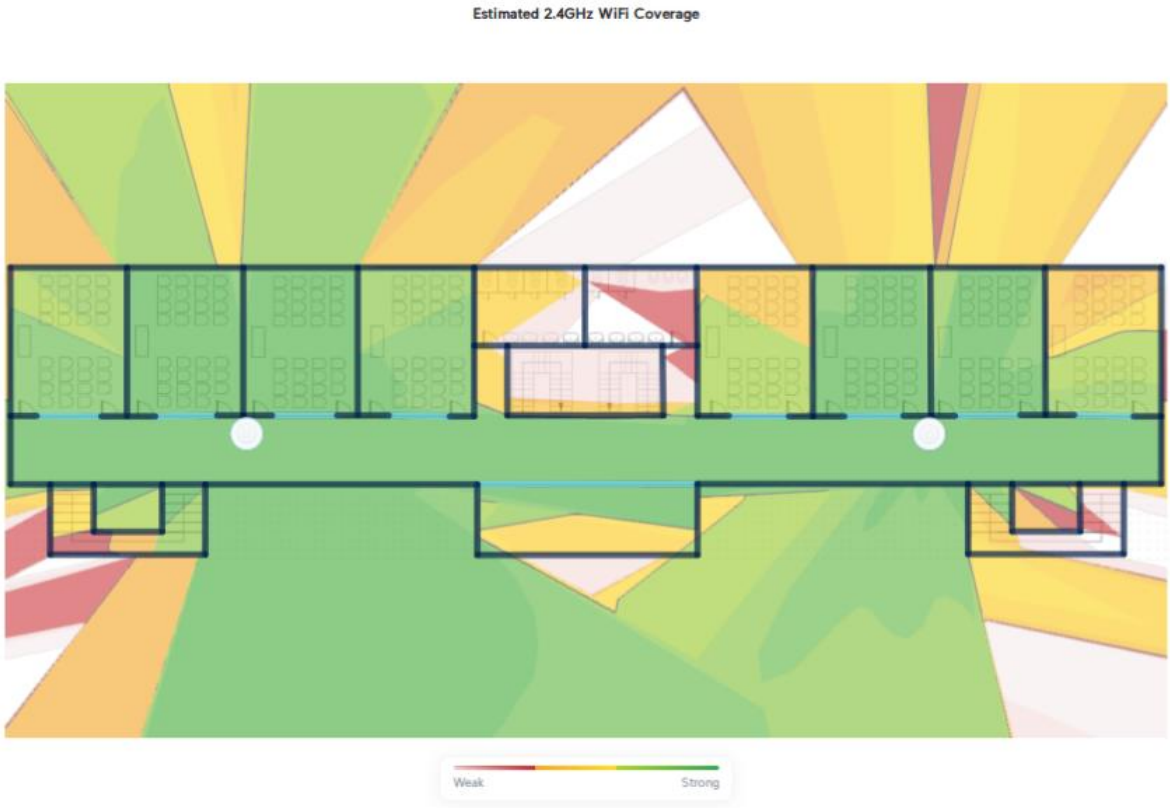
Second Floor 5GHz WiFi Coverage



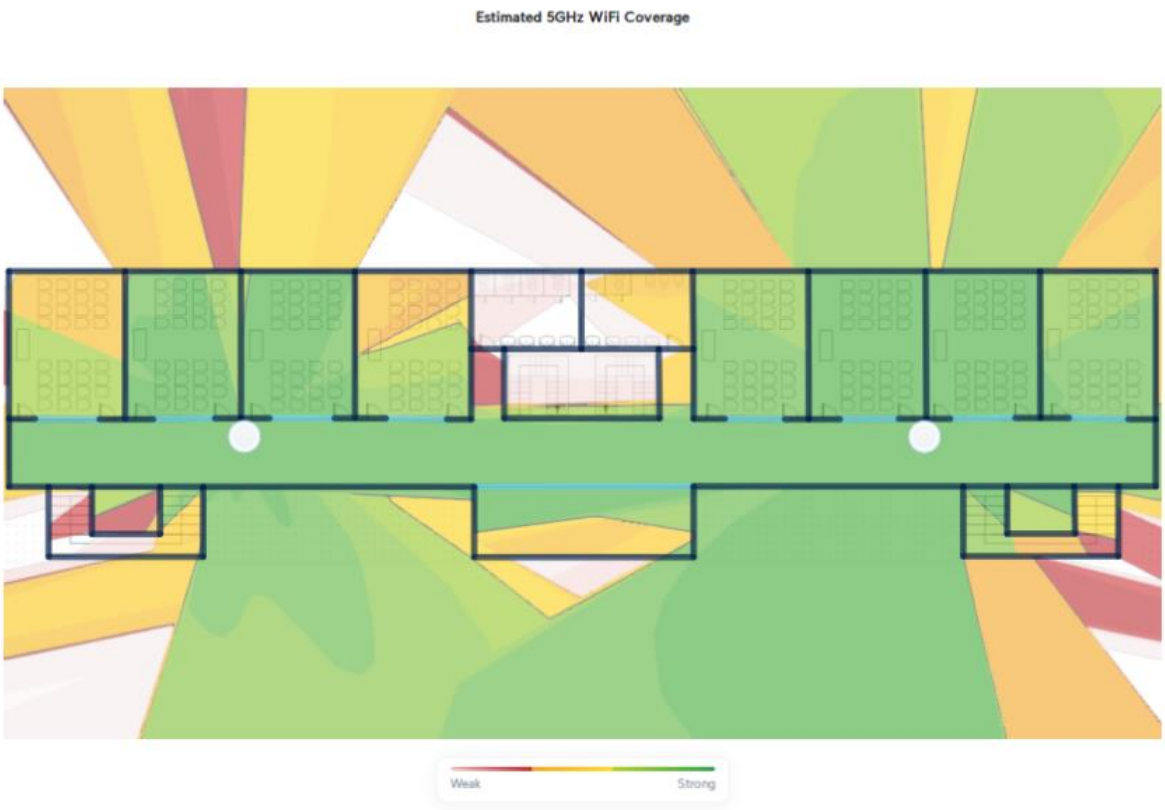
Third Floor 2.4GHz WiFi Coverage



Third Floor 5GHz WiFi Coverage

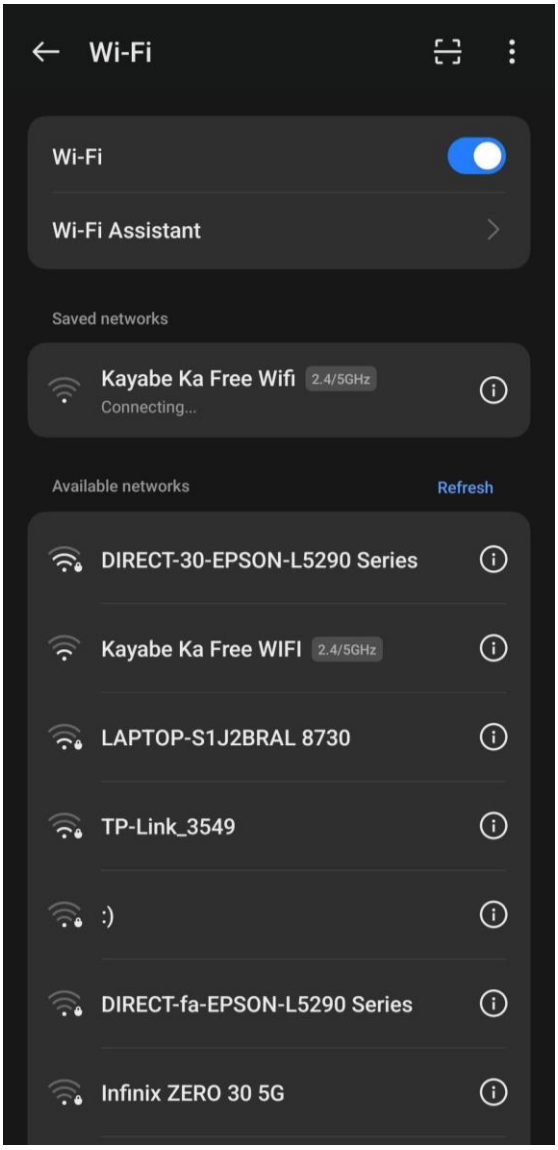


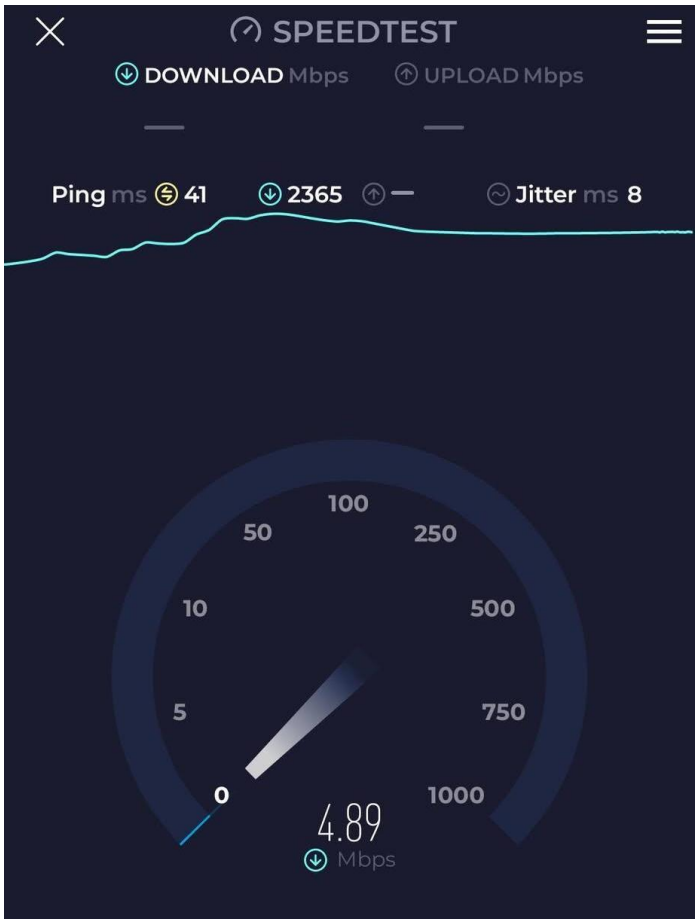
Fourth Floor 2.4GHz WiFi Coverage

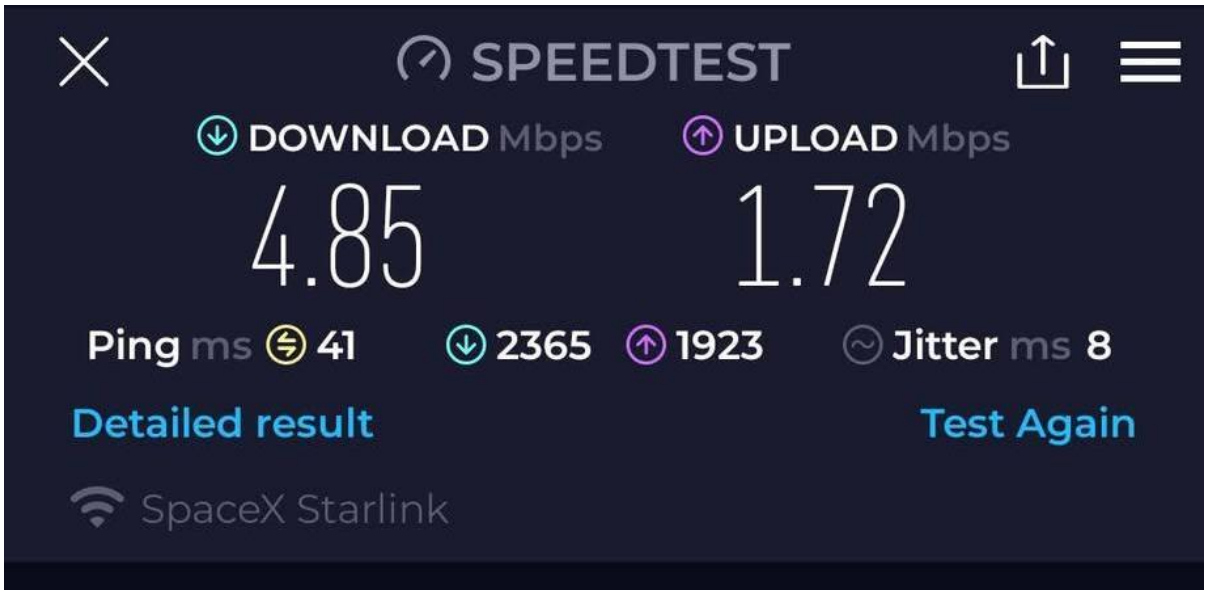


Fourth Floor 5GHz WiFi Coverage

Appendix M
Current WiFi Specifications




SPEEDTEST
DOWNLOAD Mbps
UPLOAD Mbps
Ping ms 41
2365
Jitter ms 8
100
50
250
10
500
5
750
0
1000
4.89
Mbps


SPEEDTEST
DOWNLOAD Mbps
UPLOAD Mbps
4.85
1.72
Ping ms 41
2365
1923
Jitter ms 8
Detailed result
Test Again
SpaceX Starlink

Appendix N
Security Policy

Connectivity

- Students must input or present their student number in order for them to receive a Wi-Fi Voucher.
- IT Administrators must monitor the distribution of vouchers given to the students.
- The duration of the validity of the voucher is determined by the IT Administrators.

Password

Users (Staffs)

- Passwords should not contain personal information, common words, names, or dates.
- Passwords should contain a combination of one lowercase, one uppercase, special characters, and must at least be 10 characters long.
- It is optional but passwords may be stored in a password manager like Google Password Manager as long as it is kept private.
- Passwords must be changed regularly in order to prevent data compromise.

Administrators

- Admin accounts must also follow a strong password policy requiring a mix of uppercase, lowercase letters, numbers and special characters.
- Admin should refrain from reusing previous passwords and keeping a history of the account's previous passwords.
- Admins user accounts must change their passwords every 90 days to prevent data compromise.

Physical Security

- Network devices and data centers should only be accessed by an authorized IT personnel.
- In maintaining and managing these devices, the authorized IT personnel should be present.

Appendix O
Network Requirements

Security

- Access to network cabinets and racks should be granted only to authorized IT staff in adherence to set security policies.
- Wi-Fi passwords should meet a strong password policy to avoid unauthorized access.
- User authentication should align with multi-factor authentication (MFA) standards, validating identities more than merely using a password.
- Authentication techniques need to meet industry security standards (e.g., WPA3 for Wi-Fi security, 802.1X authentication).
- Security updates should be routinely done to neutralize possible vulnerabilities.
- Administrators should be automatically notified in the event of WAP or switch failure.

Scalability

- Wireless Access Points (WAPs) need to support existing users and future users without substantial performance loss.
- Future WAP deployments need to seamlessly fit into the network without necessitating any drastic design changes.
- The network should be capable of supporting a large number of concurrent wireless connections efficiently.
- The network needs to have scalability within IP addressing and number of switch ports available to support future growth.

Availability

- Wi-Fi SSIDs must be accessible on more than one frequency band in order to ensure the greatest possible device compatibility.
- Redundant uplinks must be utilized for WAPs to enhance reliability and fault tolerance.
- Internet access must have slim to none downtime in order to provide students and faculty with constant network access.
- Newly installed WAPs must not compromise the coverage that already exists but rather enhance performance depending on feasibility and best practices.

Manageability

- The wireless network must be centrally controlled through a unified interface with minimal blocking.
- Network devices need to have a well-defined, structured naming scheme, documented along with detailed description for consistency.
- The management system needs to allow real-time monitoring and remote diagnostics to reduce downtime.

Appendix P
Implementation Plan

The devices must be acquired by a team with network proficiency. If the U6-LR WAPs are not available from the supplier that the team is acquiring it from then alternative suppliers must be secured, as the network coverage from these specific WAPs are already planned for the campus building.

For proper access point (AP) management, labeling and documentation in an inventory system of each device is recommended. A master list will help subsequent administrators track and manage network gear effectively. Since the AP installations were well thought out, such documentation can act as a reference for future modifications or expansions. Accurate documentation of deployment details will also be useful in the process of troubleshooting and optimizing the network performance later on.

During configuration, all the devices in the network must be configured prior to being deployed. FortiGate is the main component that regulates the VLAN traffic as well as policies for accessing the internet. The network has been designed with segregation of users to their assigned ISPs defined by preset VLAN routes. It ensures users like students and faculty members only gain access via the assigned ISP. A separate DHCP server is configured for each VLAN to assign proper IP addresses. The firewall also implements security protocols to block unauthorized access and impose internet usage policies.

MAC address filtering is used to ensure that registered devices of students and teachers alone can connect to the network. Unregistered devices will be blocked, blocking unauthorized usage and minimizing security threats. Web filtering is also applied to both the student and teacher VLANs, restricting access to non-educational or inappropriate content. This filtering is configured within the FortiGate firewall, ensuring compliance with the institution's internet usage policies while maintaining a safe browsing environment.

Prior to installing the APs, the APs need to be configured and adopted by the UniFi Network Controller. The APs are powered on via PoE switches, which automatically supply power according to the power needs, eliminating any chance of overloading. The APs, after being powered, are supposed to acquire an IP address from the DHCP server. For adopting the APs to the UniFi Network Controller, an SSH session has to be opened using a terminal or PuTTY. The default SSH credentials are:

Username: ubnt

Password: ubnt

Once SSH access is obtained, the following command has to be run to notify the AP of the UniFi Network Controller's IP address:

set-inform http://[UniFi Network Controller Public IP Address]:8080/inform

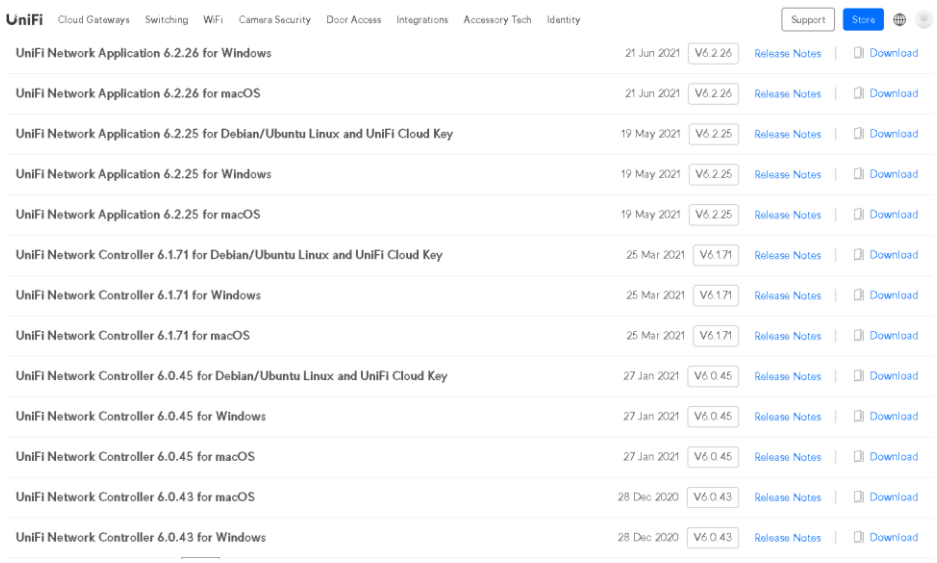
This command tells the AP to link to the network controller. The network controller web interface is accessed through a web browser via HTTPS at:

https://[UniFi Network Controller Public IP Address]:8443

The setup process begins with the configuration of the site network and adopting the APs and switches. The network settings are then applied after which all of the UniFi devices automatically inherit configurations from the controller.

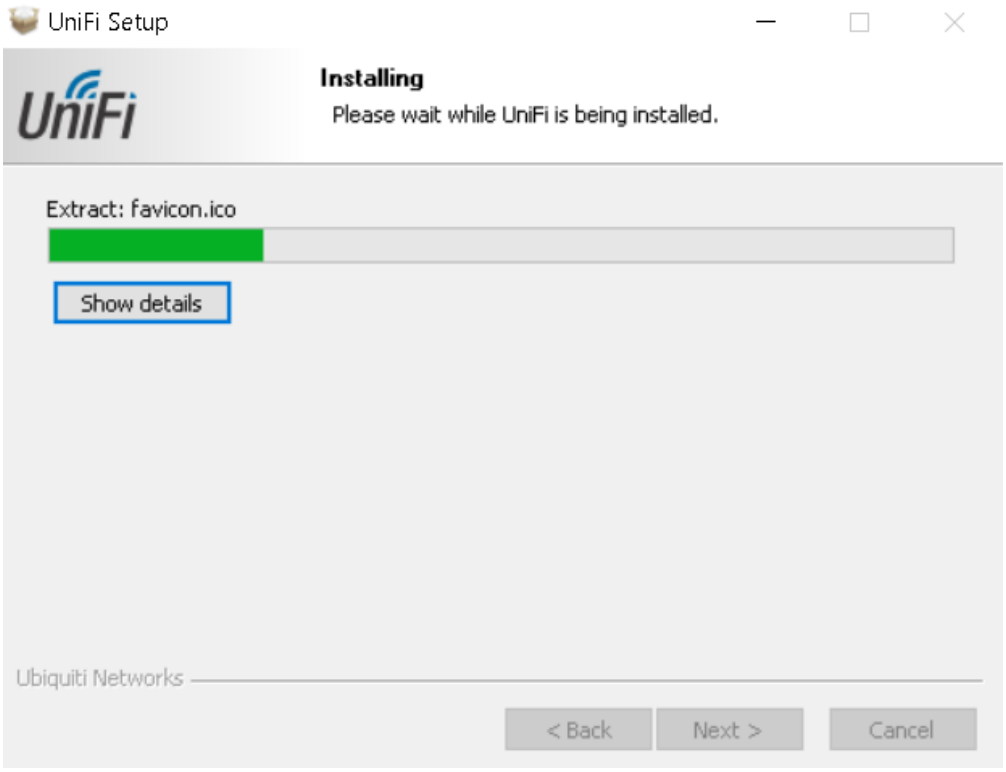
The network is configured after which the installation of the switches and APs. Each device is mounted with great care and is connected to the respective VLAN. After installation, a verification process is performed to ensure that all devices are successfully powered on, VLAN assignments are accurate, ISP routing policies work, web filtering and MAC address authentication are properly functioning, and the UniFi controller is effectively managing the APs. Network management is then handed over to the IT department, with ongoing monitoring, upkeep, and future scalability of the system.

Appendix Q
Unifi Network Controller Installation

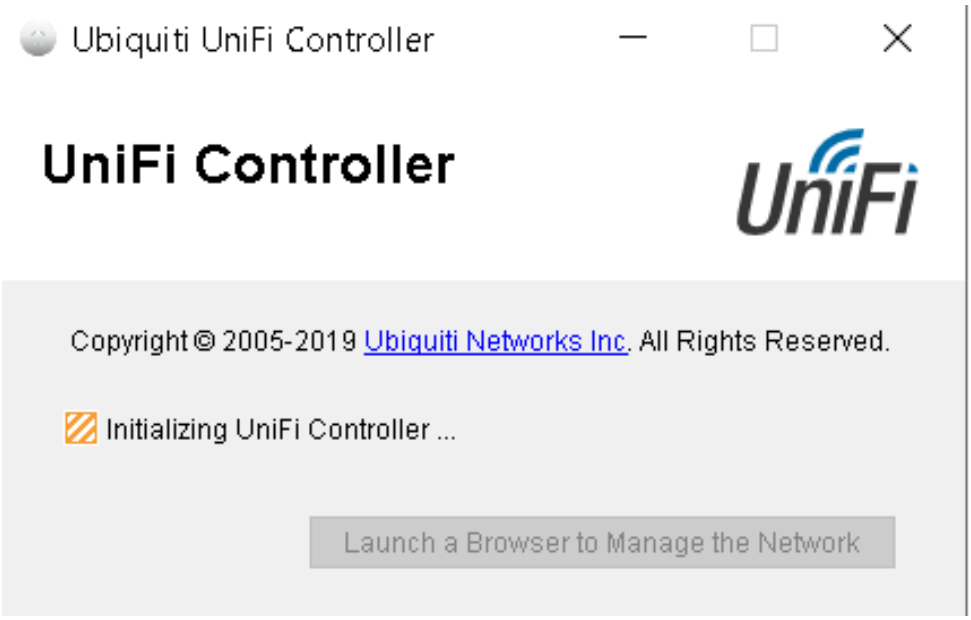


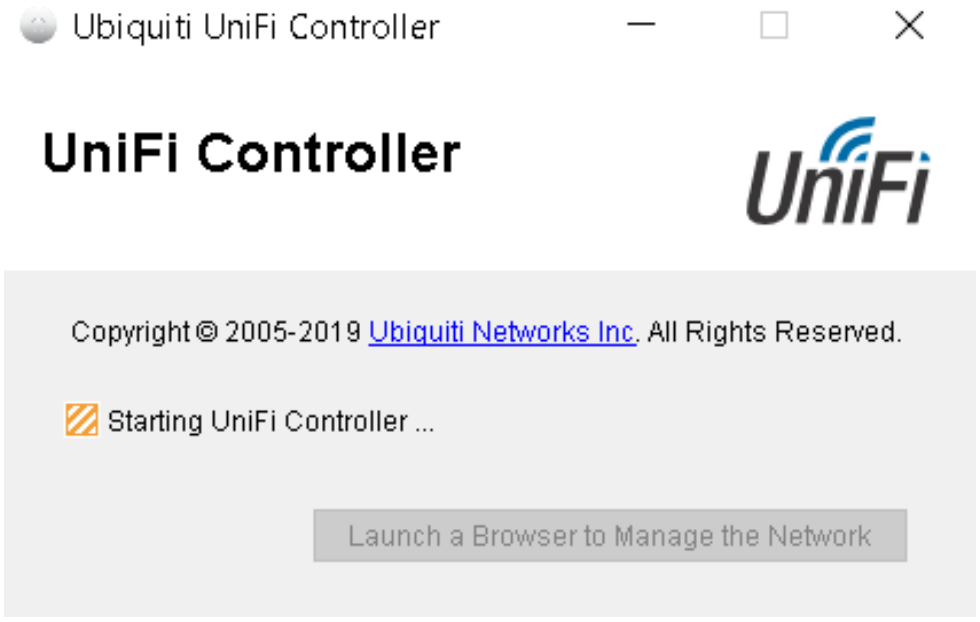
UniFi Cloud Gateways Switching WiFi Camera Security Door Access Integrations Accessory Tech Identity — Support | Store

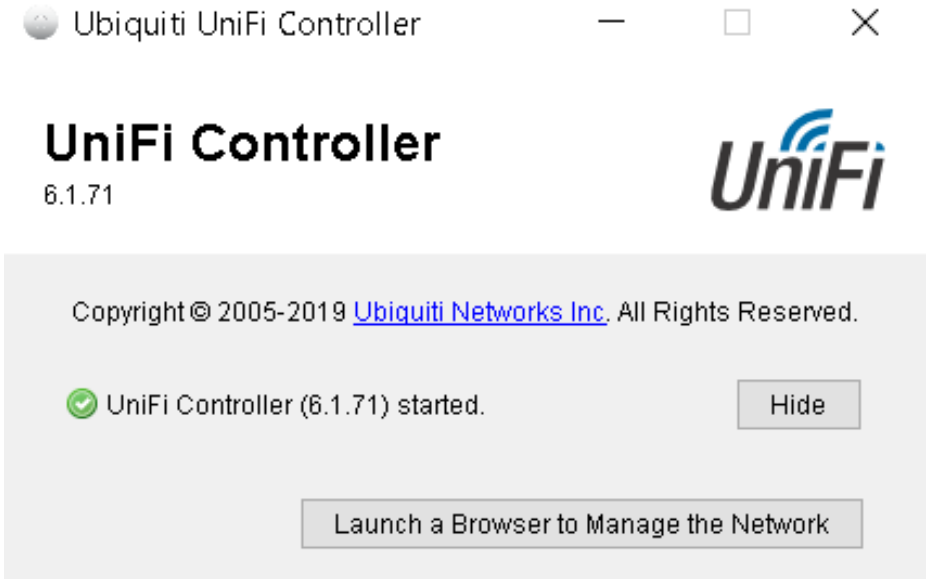
UniFi Network Application 6.2.26 for Windows	21 Jun 2021	V6.2.26	Release Notes	Download
UniFi Network Application 6.2.26 for macOS	21 Jun 2021	V6.2.26	Release Notes	Download
UniFi Network Application 6.2.25 for Debian/Ubuntu Linux and UniFi Cloud Key	19 May 2021	V6.2.25	Release Notes	Download
UniFi Network Application 6.2.25 for Windows	19 May 2021	V6.2.25	Release Notes	Download
UniFi Network Application 6.2.25 for macOS	19 May 2021	V6.2.25	Release Notes	Download
UniFi Network Controller 6.1.71 for Debian/Ubuntu Linux and UniFi Cloud Key	25 Mar 2021	V6.1.71	Release Notes	Download
UniFi Network Controller 6.1.71 for Windows	25 Mar 2021	V6.1.71	Release Notes	Download
UniFi Network Controller 6.1.71 for macOS	25 Mar 2021	V6.1.71	Release Notes	Download
UniFi Network Controller 6.0.45 for Debian/Ubuntu Linux and UniFi Cloud Key	27 Jan 2021	V6.0.45	Release Notes	Download
UniFi Network Controller 6.0.45 for Windows	27 Jan 2021	V6.0.45	Release Notes	Download
UniFi Network Controller 6.0.45 for macOS	27 Jan 2021	V6.0.45	Release Notes	Download
UniFi Network Controller 6.0.43 for macOS	28 Dec 2020	V6.0.43	Release Notes	Download
UniFi Network Controller 6.0.43 for Windows	28 Dec 2020	V6.0.43	Release Notes	Download


UniFi Setup
UniFi
Installing
Please wait while UniFi is being installed.
Extract: favicon.ico
Show details
Ubiquiti Networks
< Back
Next >
Cancel


UniFi Setup
Completing the UniFi Setup Wizard
UniFi has been installed on your computer.
Click Finish to close this wizard.
Start UniFi Controller after installation
UBIQUITI
NETWORKS
UniFi
< Back
Finish
Cancel


Ubiquiti UniFi Controller
UniFi Controller
UniFi
Copyright © 2005-2019 Ubiquiti Networks Inc. All Rights Reserved.
Initializing UniFi Controller ...
Launch a Browser to Manage the Network


Ubiquiti UniFi Controller
UniFi Controller
UniFi
Copyright © 2005-2019 Ubiquiti Networks Inc. All Rights Reserved.
Starting UniFi Controller ...
Launch a Browser to Manage the Network


Ubiquiti UniFi Controller
UniFi Controller
6.1.71
UniFi
Copyright © 2005-2019 Ubiquiti Networks Inc. All Rights Reserved.
UniFi Controller (6.1.71) started.
Hide
Launch a Browser to Manage the Network

Step 1 of 6

Name Your Controller

Use a simple name to help differentiate your controller when managing multiple networks.

Controller Name

UniFi Network

By selecting this you are agreeing to end user license agreement and the terms of service.

Or restore setup from backup

Next

Step 2 of 6

Sign in with your Ubiquiti Account

Use your Ubiquiti Account to access your Controller via the unifi.ui.com service or locally with the same credentials.

Username

caas|imenez@gmail.com

Password

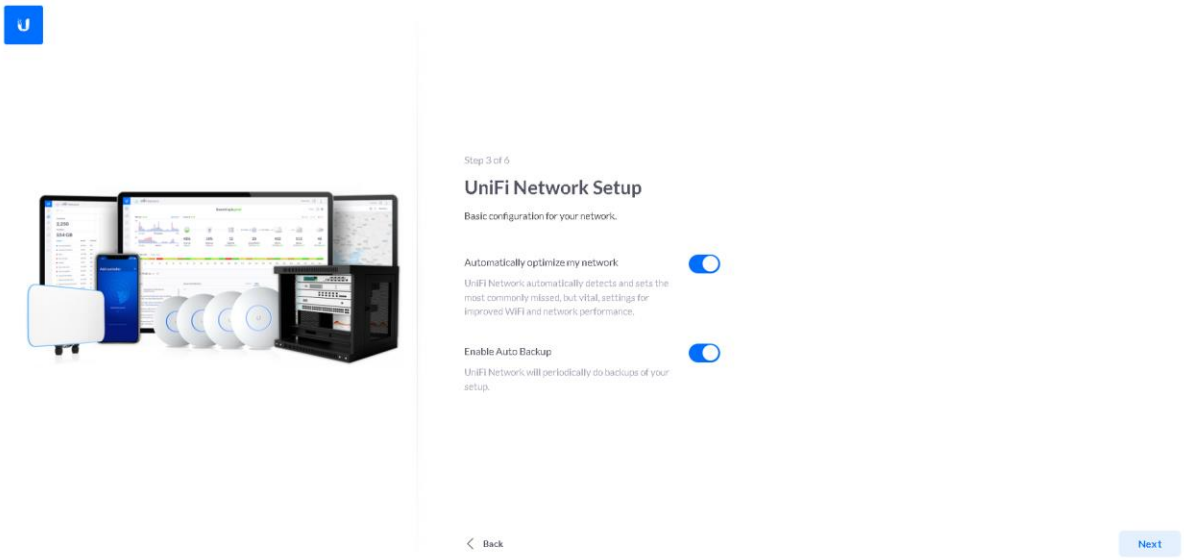
••••••••••

Invalid username or password, please try again.

Switch to Advanced Setup

Back

Next


Step 3 of 6
UniFi Network Setup
Basic configuration for your network.
Automatically optimize my network
UniFi Network automatically detects and sets the most commonly missed, but vital, settings for improved WiFi and network performance.
Enable Auto Backup
UniFi Network will periodically do backups of your setup.
Back
Next


WiFi Password
WiFi Password must be at least 8 characters.
Combine 2 GHz and 5 GHz WiFi Network Names into one

Step 4 of 6

Devices Setup

Please select the devices you would like to configure.

You have no devices

Connect devices to your network.

Back

Next

Step 5 of 6

WiFi Setup

Name your new Wi-Fi network and choose a password.

WiFi Name

CCSFP

WiFi Password

••••••••

WiFi Password must be at least 8 characters.

Combine 2 GHz and 5 GHz WiFi Network Names into one

Back

Skip

Next

Step 6 of 6

Review Configuration

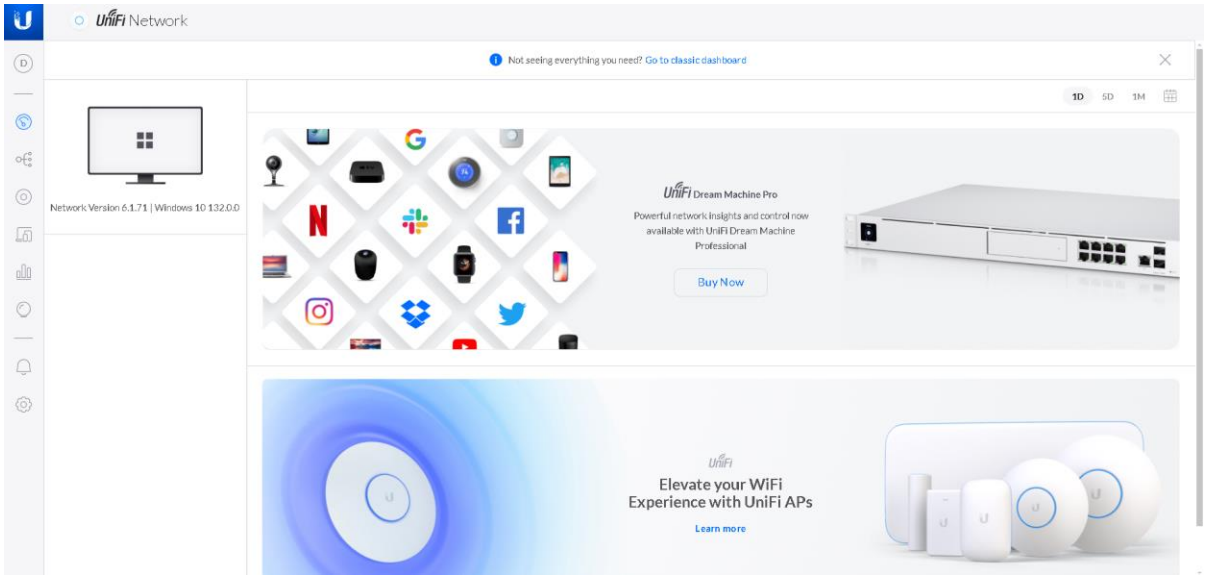
Check your configuration and setup your Controller.

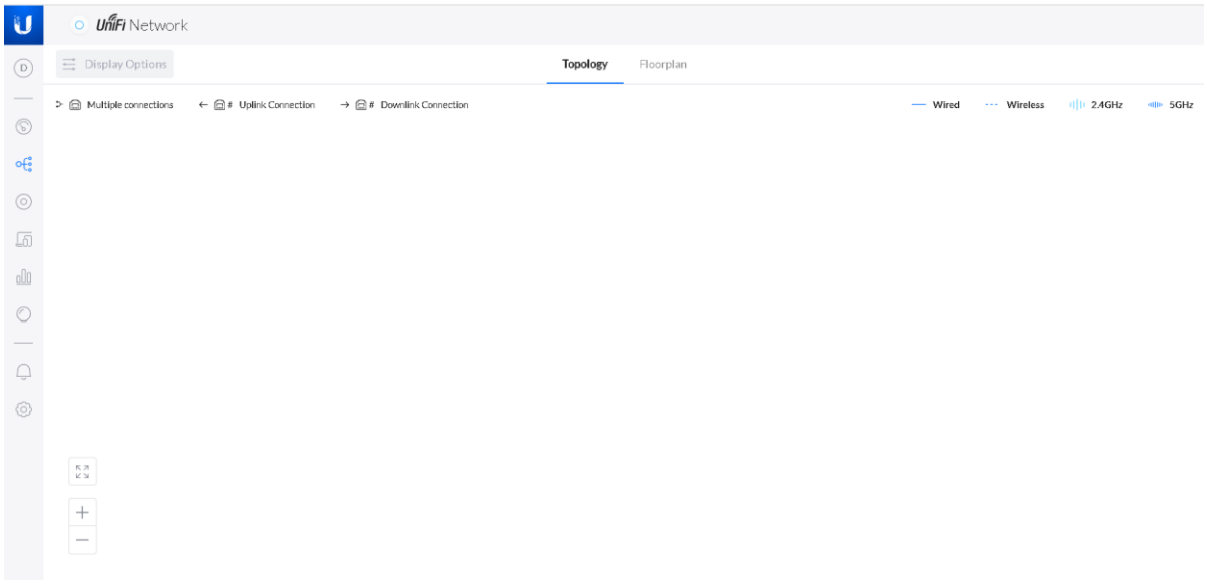
Controller Name	CCSFP
Remote Access	Enabled
Use Ubiquiti account for local access	Yes
Ubiquiti Account	caasjimenez
WiFi Name	CCSFP
Country or territory	Philippines
Timezone	(UTC+08:00) Asia/Manila

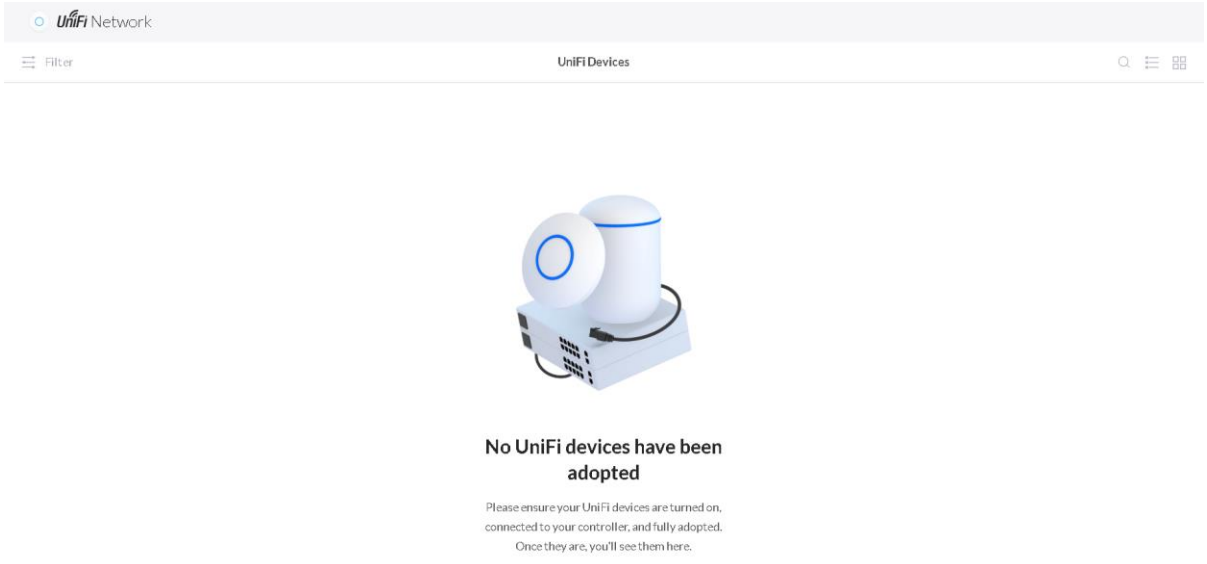
Back

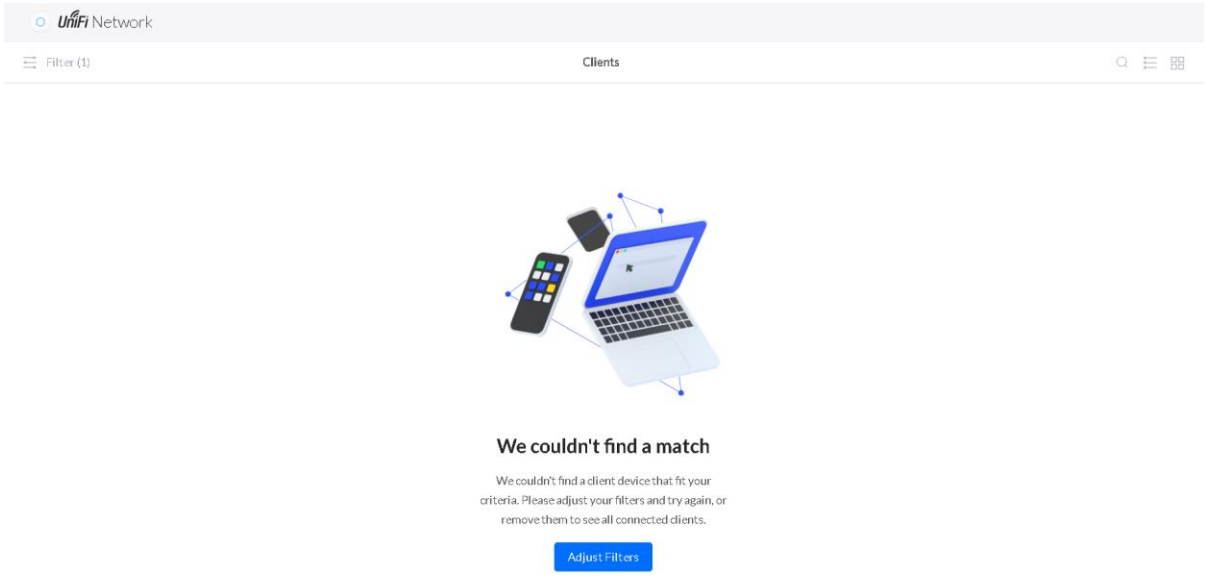
Finish

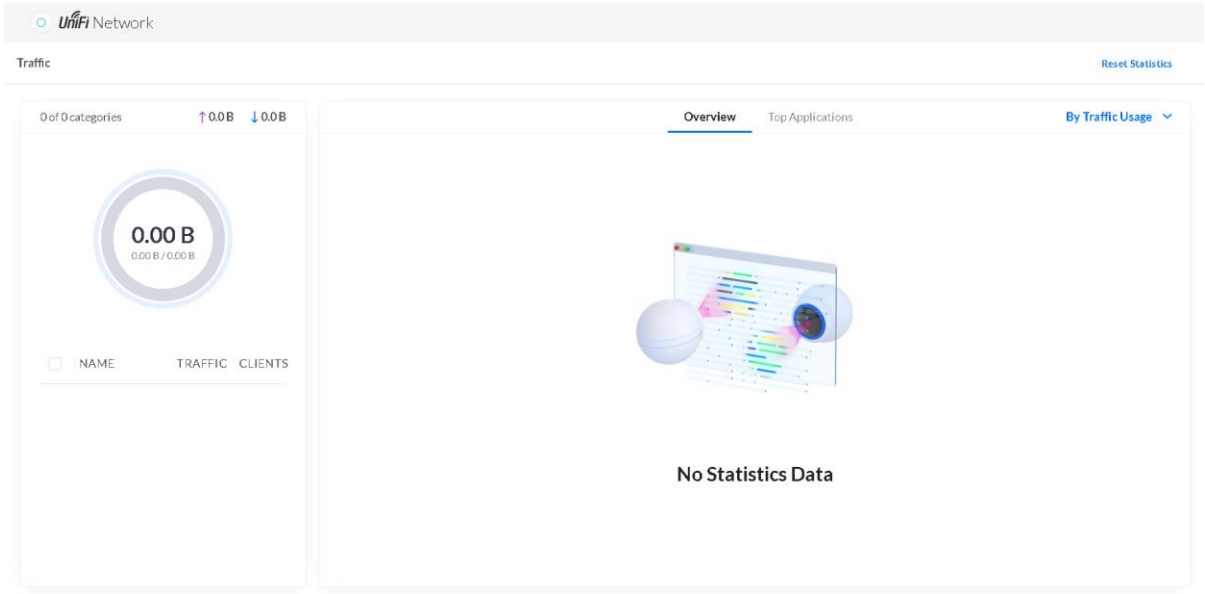
Configuring UniFi Network Controller

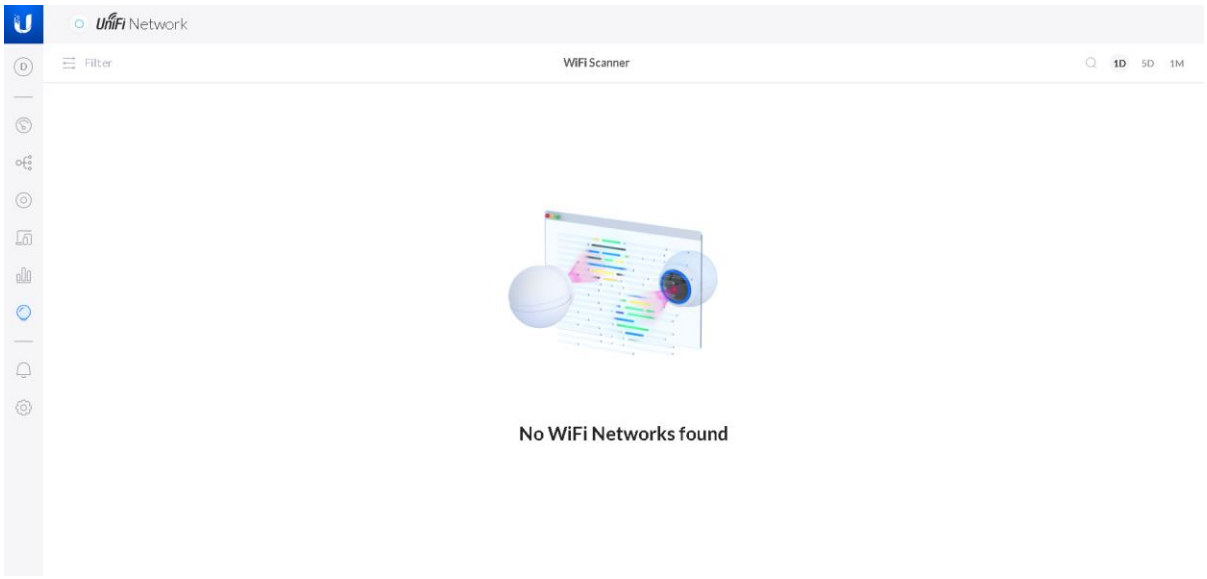

UniFi Network
Not seeing everything you need? Go to classic dashboard
1D
5D
1M
Network Version 6.1.71 | Windows 10 132.0.0
UniFi Dream Machine Pro
Powerful network insights and control now available with UniFi Dream Machine Professional
Buy Now
UniFi
Elevate your WiFi Experience with UniFi APs
Learn more


UniFi Network
Display Options
Topology
Floorplan
Multiple connections
Uplink Connection
Downlink Connection
Wired
Wireless
2.4GHz
5GHz


UniFi Network
Filter
UniFi Devices
No UniFi devices have been adopted
Please ensure your UniFi devices are turned on, connected to your controller, and fully adopted. Once they are, you'll see them here.

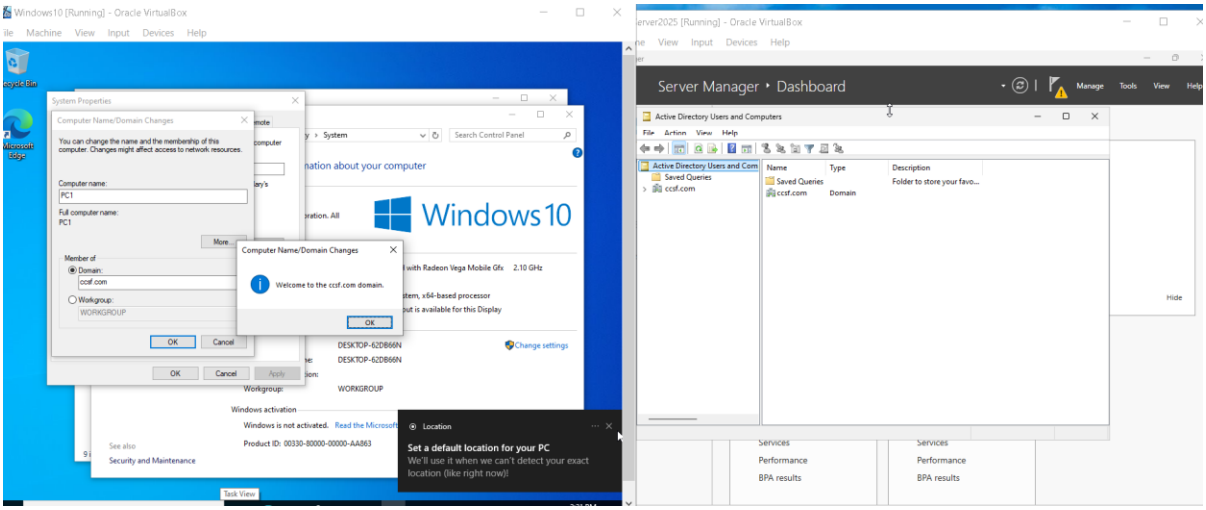

UniFi Network
Filter (1)
Clients
We couldn't find a match
We couldn't find a client device that fit your criteria. Please adjust your filters and try again, or remove them to see all connected clients.
Adjust Filters


UniFi Network
Traffic
Reset Statistics
0 of 0 categories
↑ 0.0 B ↓ 0.0 B
0.00 B
0.00 B / 0.00 B
NAME
TRAFFIC
CLIENTS
Overview
Top Applications
By Traffic Usage
No Statistics Data

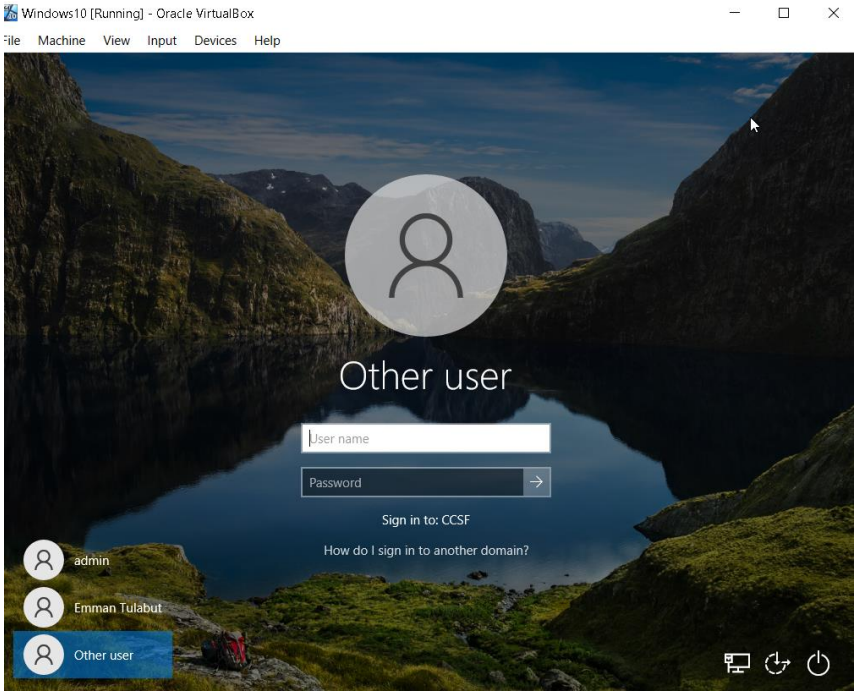

UniFi Network
Filter
WiFi Scanner
1D
5D
1M
No WiFi Networks found

Appendix R
Windows Server 2025 Domain Controller

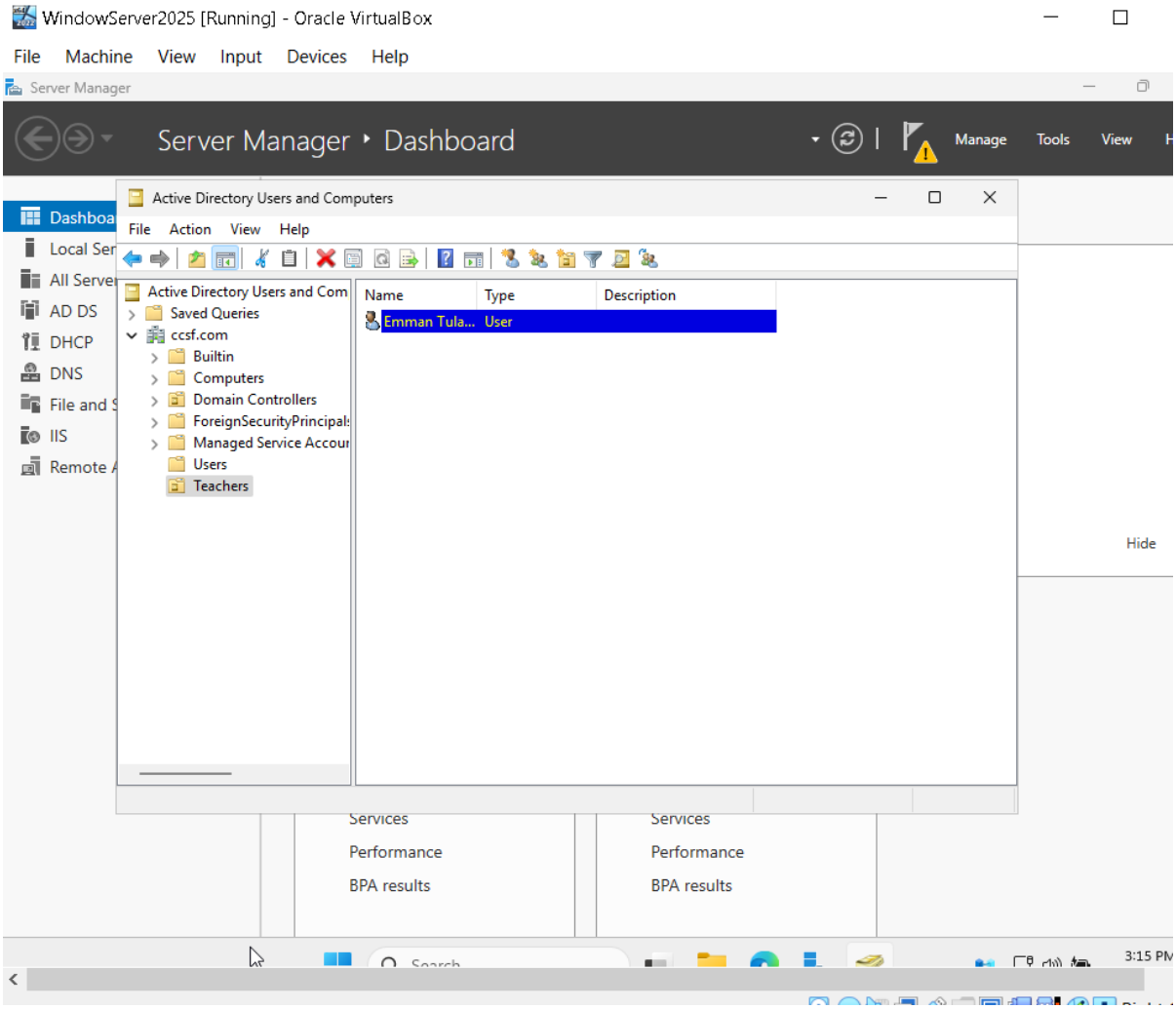
Connecting the devices to the domain



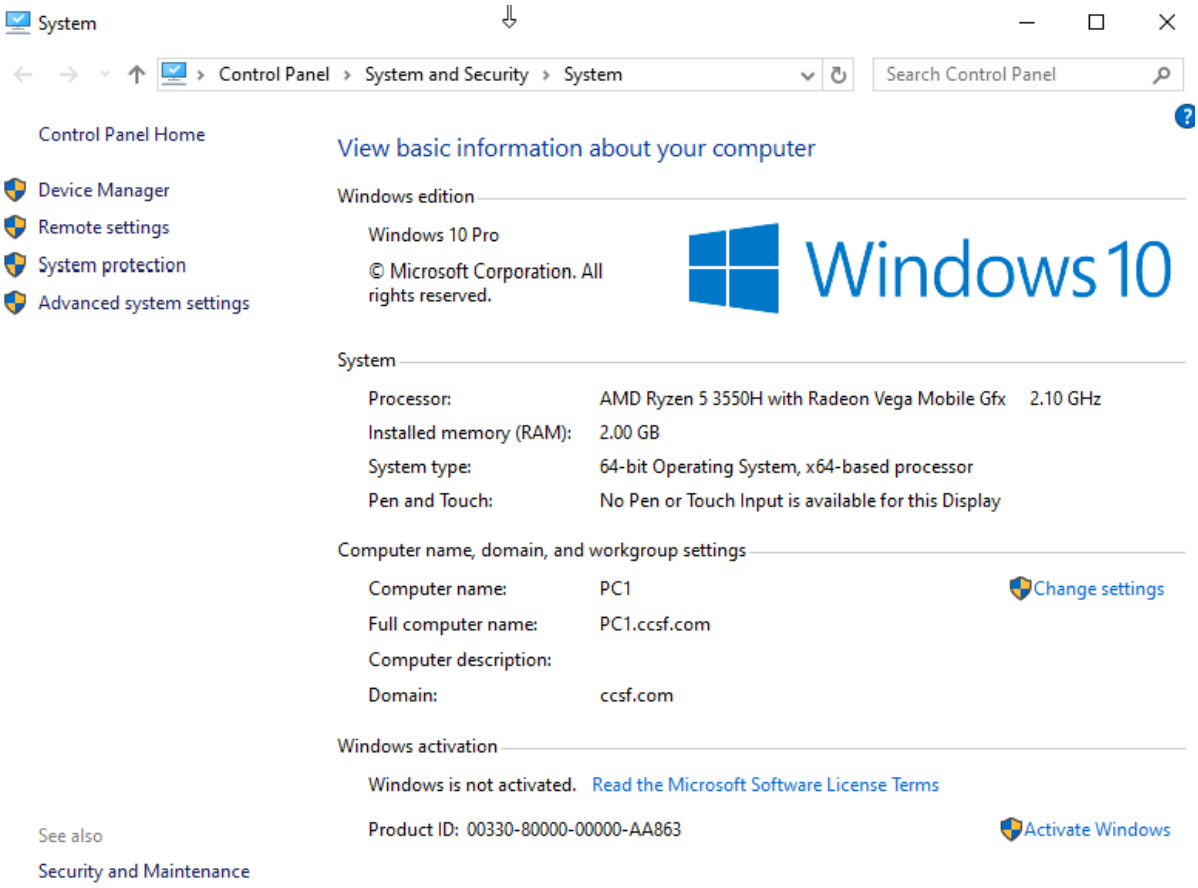
Connected the device to the domain (ccsf.com)



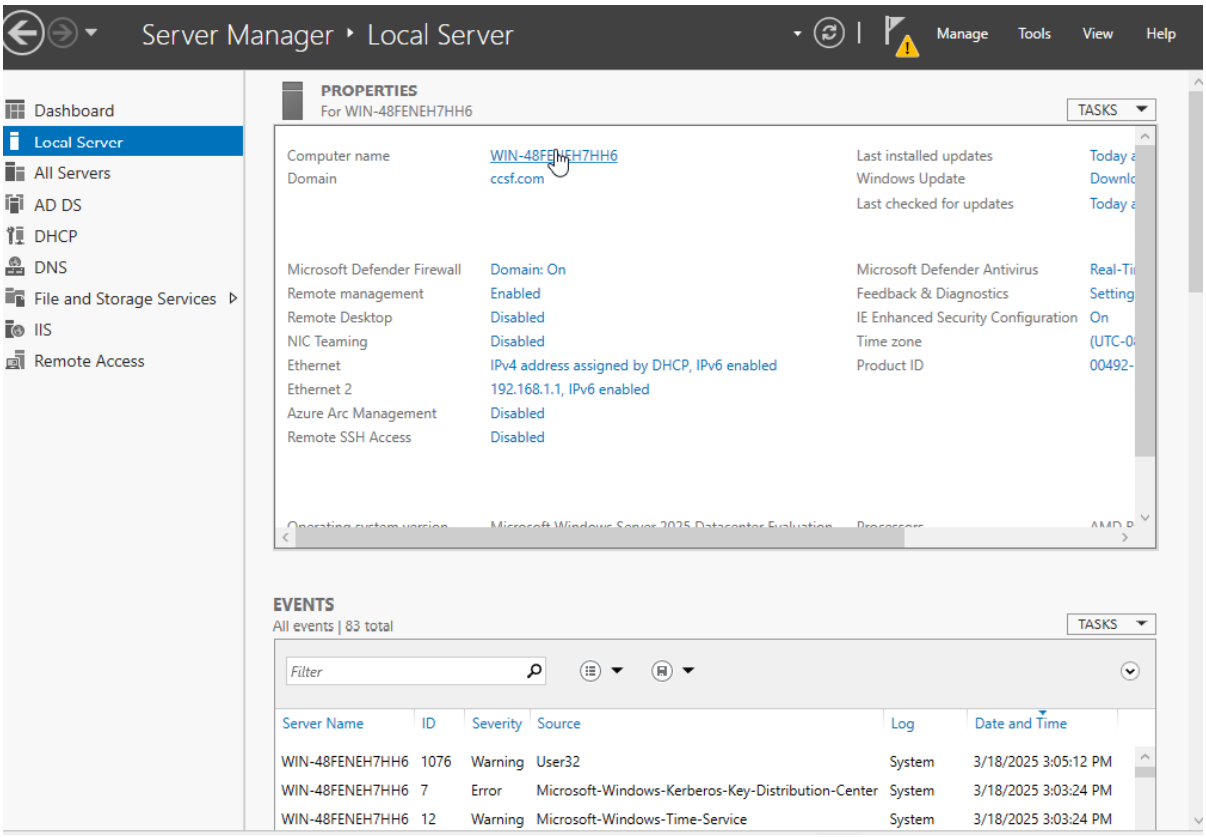
The device is connected to the domain (ccsf.com)



Added organizational units (Teachers & Students) and made users inside those organizational units

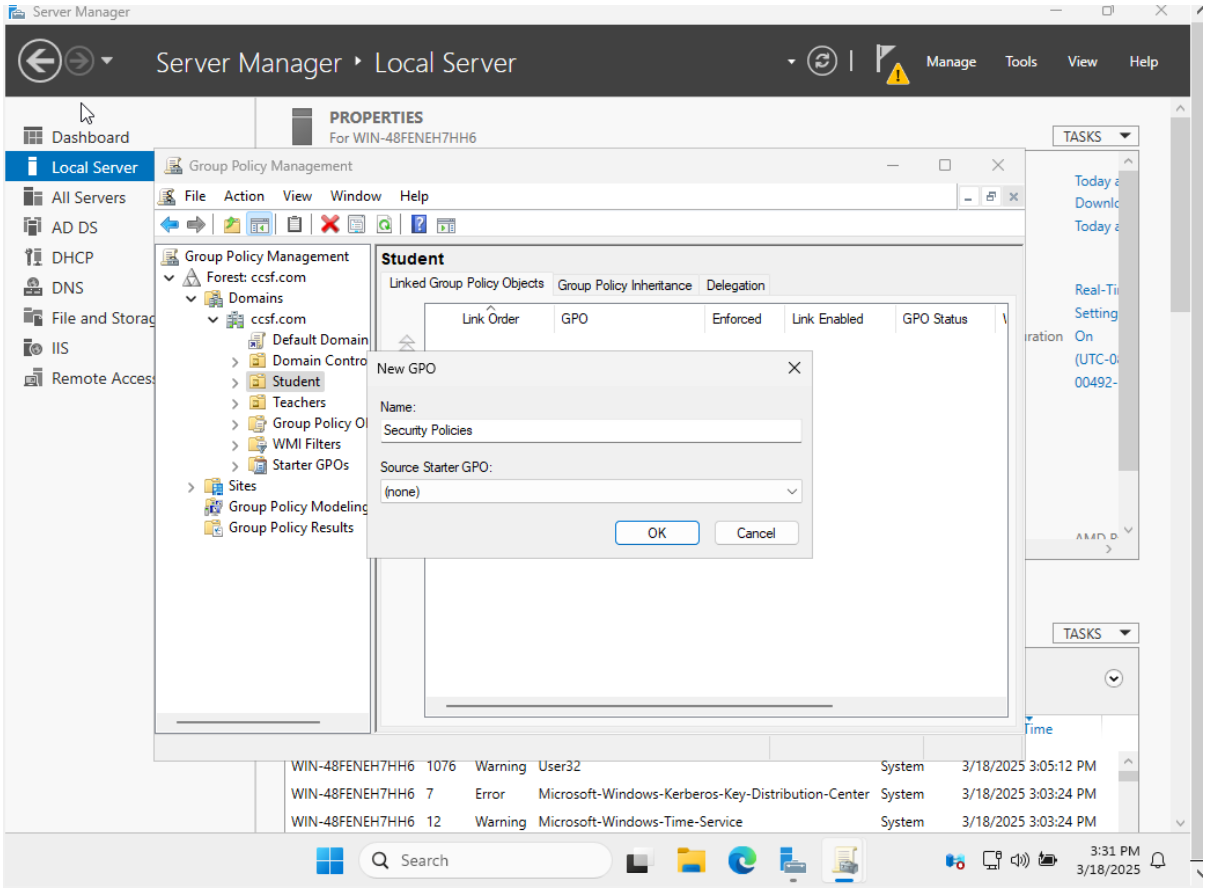


Information on the device that it is connected to the domain

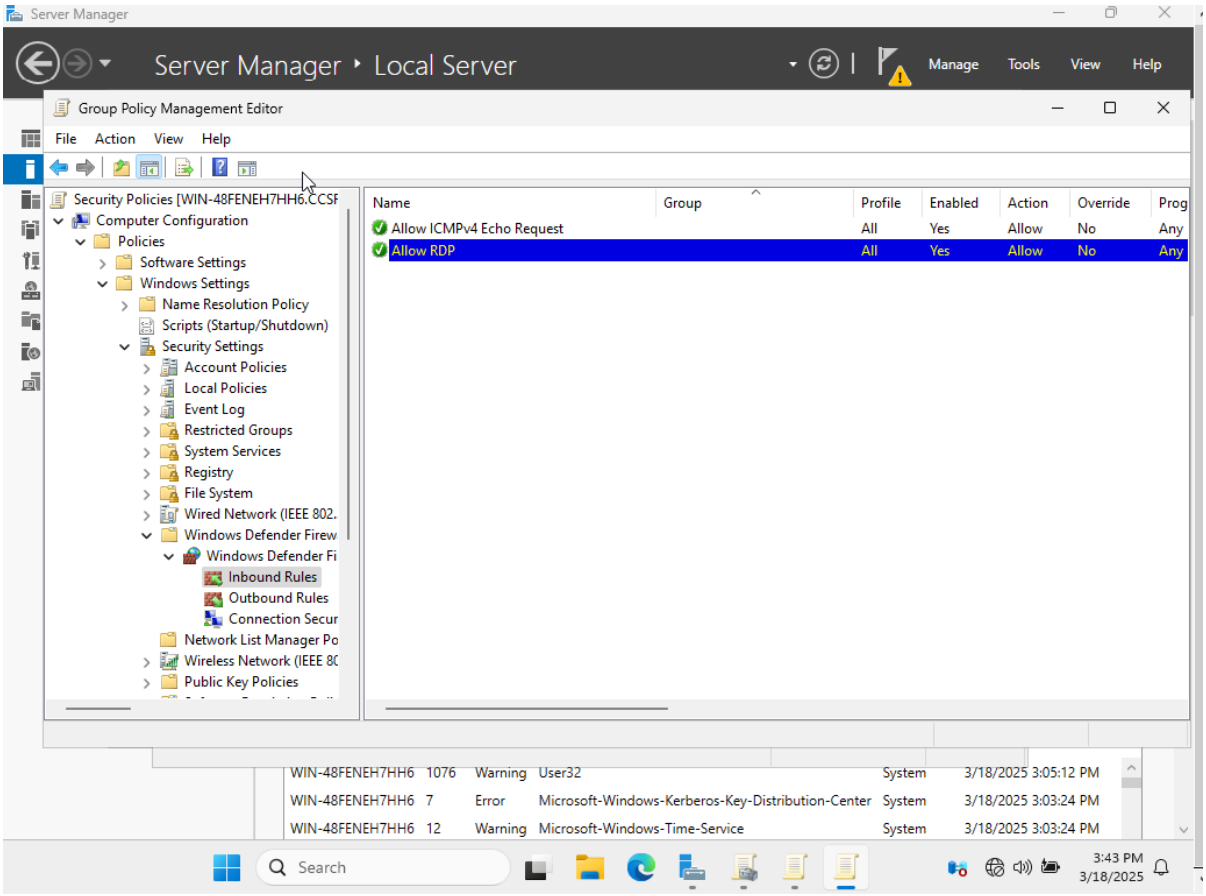


Information on the server manager about the configurations of the server

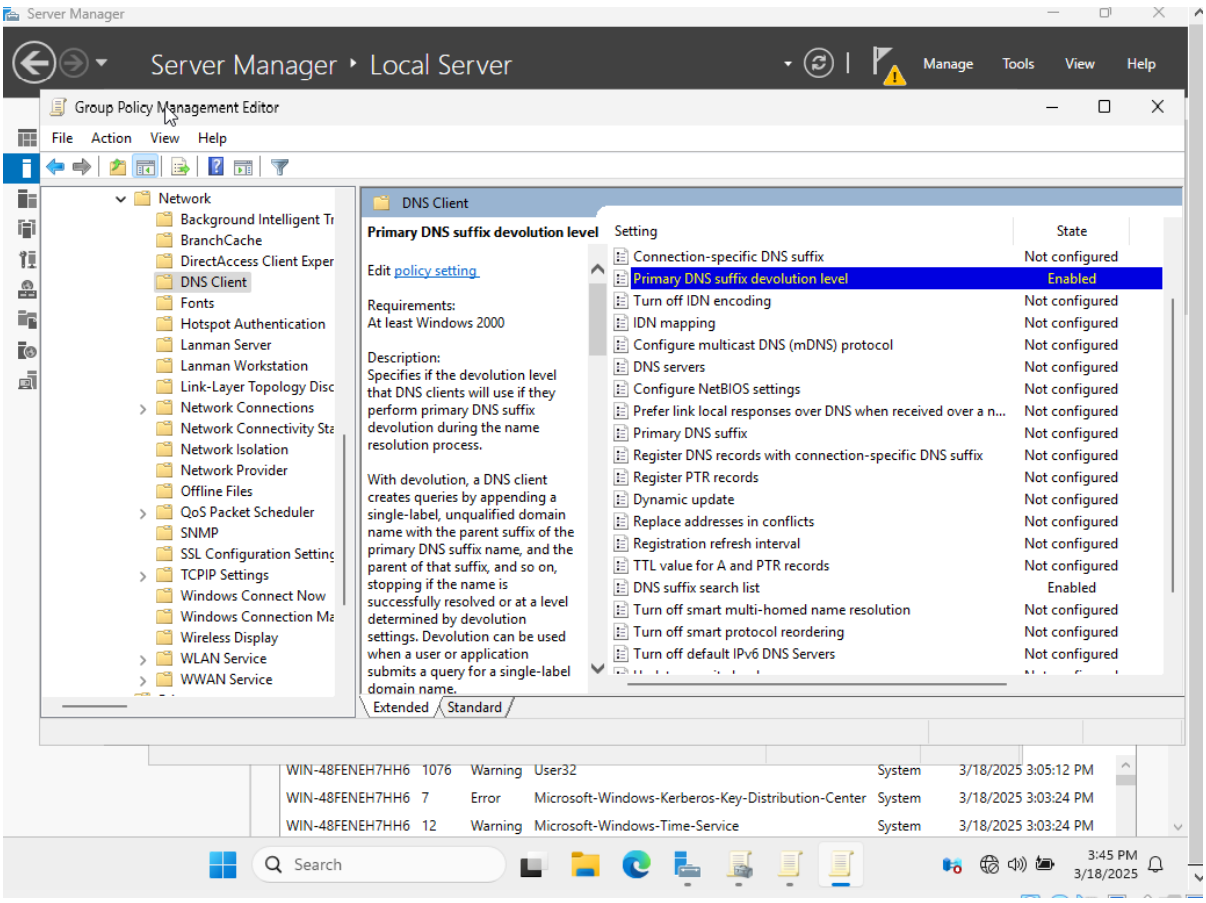
Assigning Security Policies to Organizational Units (Teacher, Students)



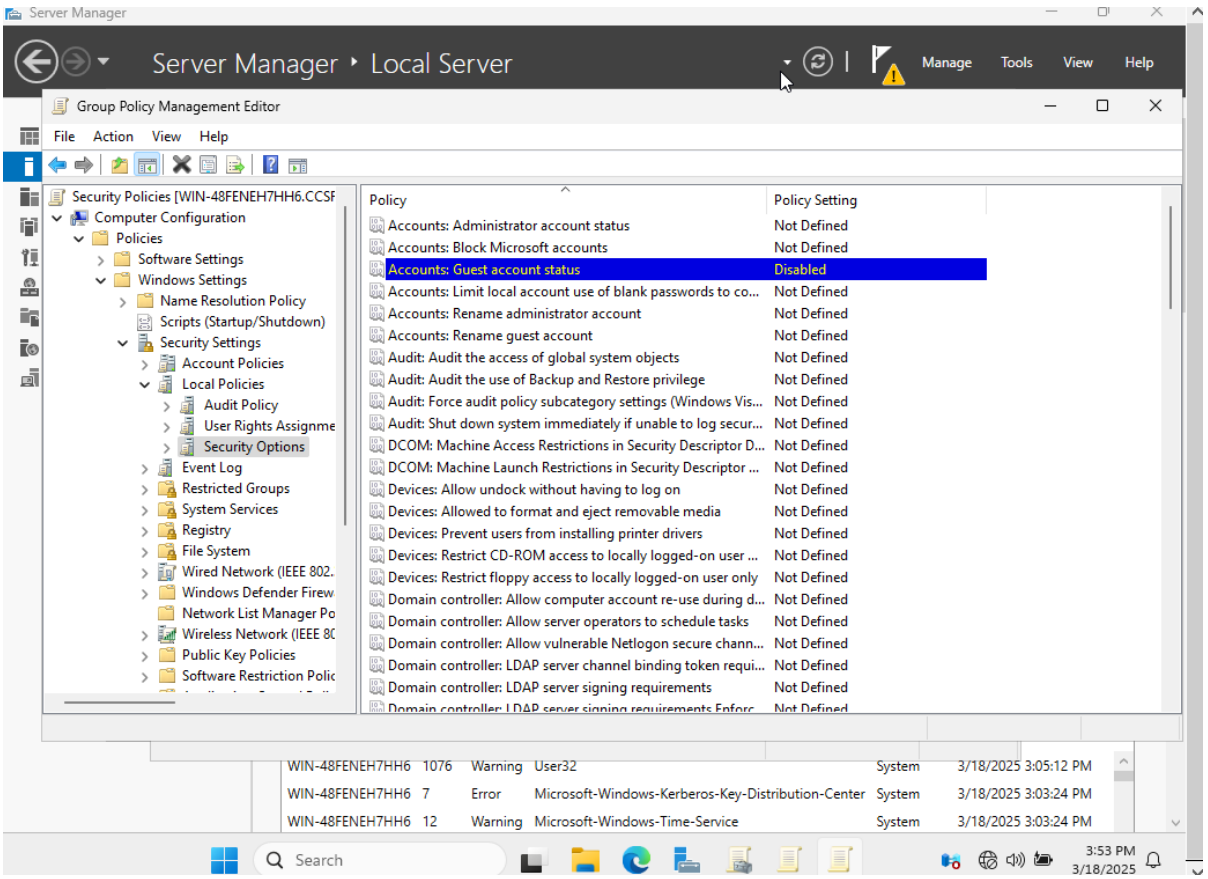
Creating the Group Policy Object (GPO) for students



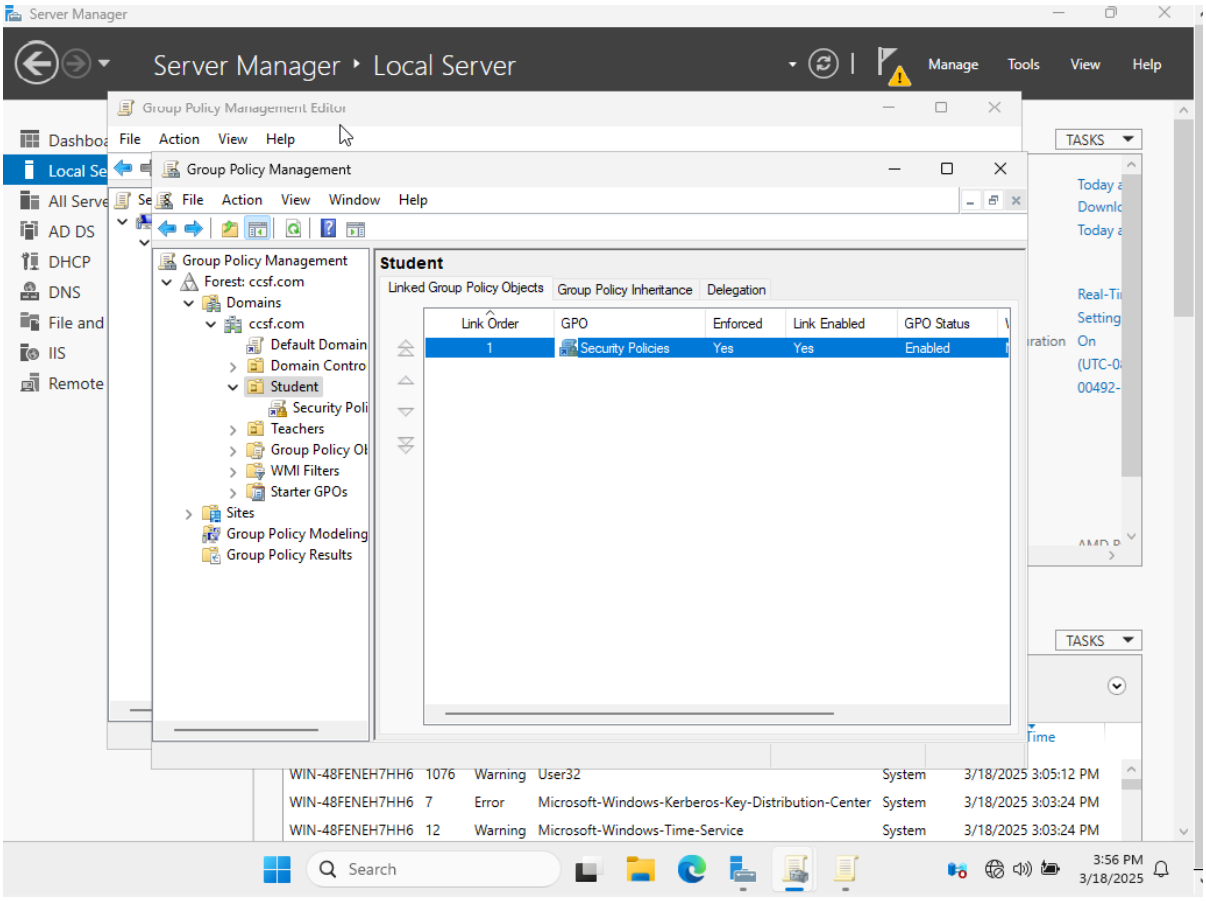
Allowing RDP and ICMP



Enforced DNS settings for Domain-Joined Clients



Disabled guest access



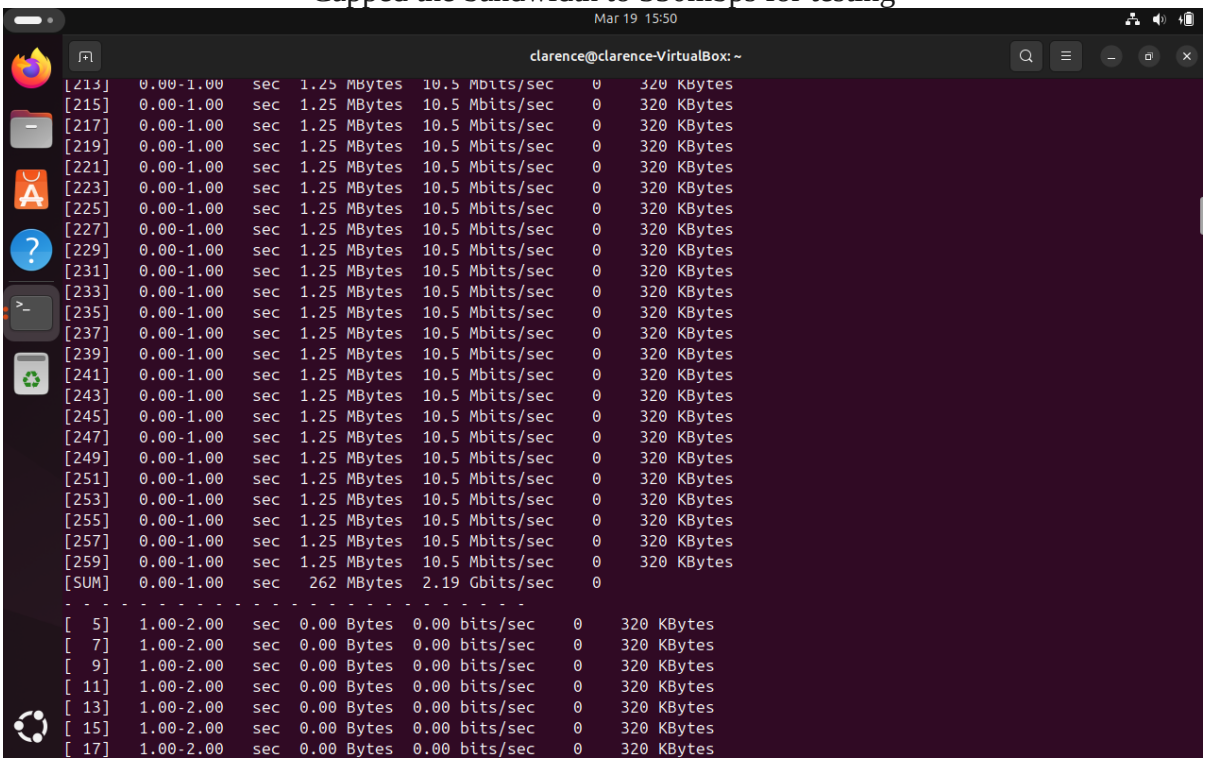
Security Policy enforced

Appendix S
Bandwidth and Throughput Test using Iperf3

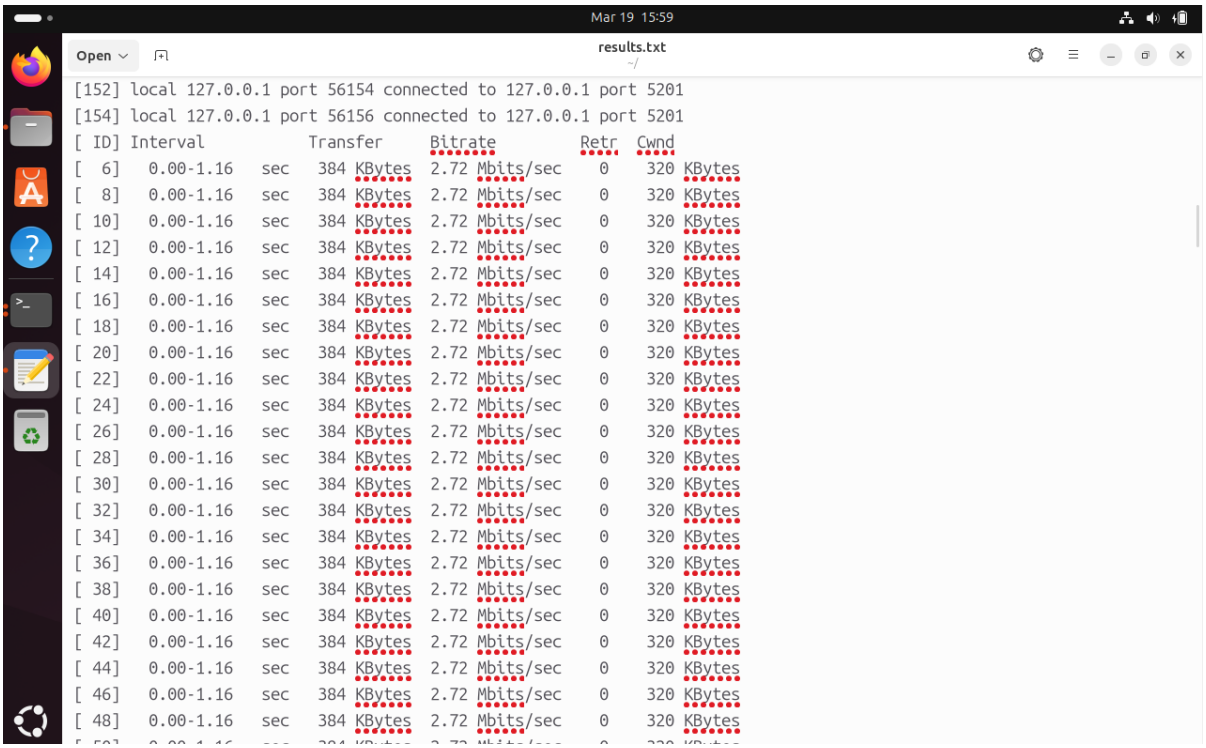
Current ISP for students (350 mbps) for the average of 430 students

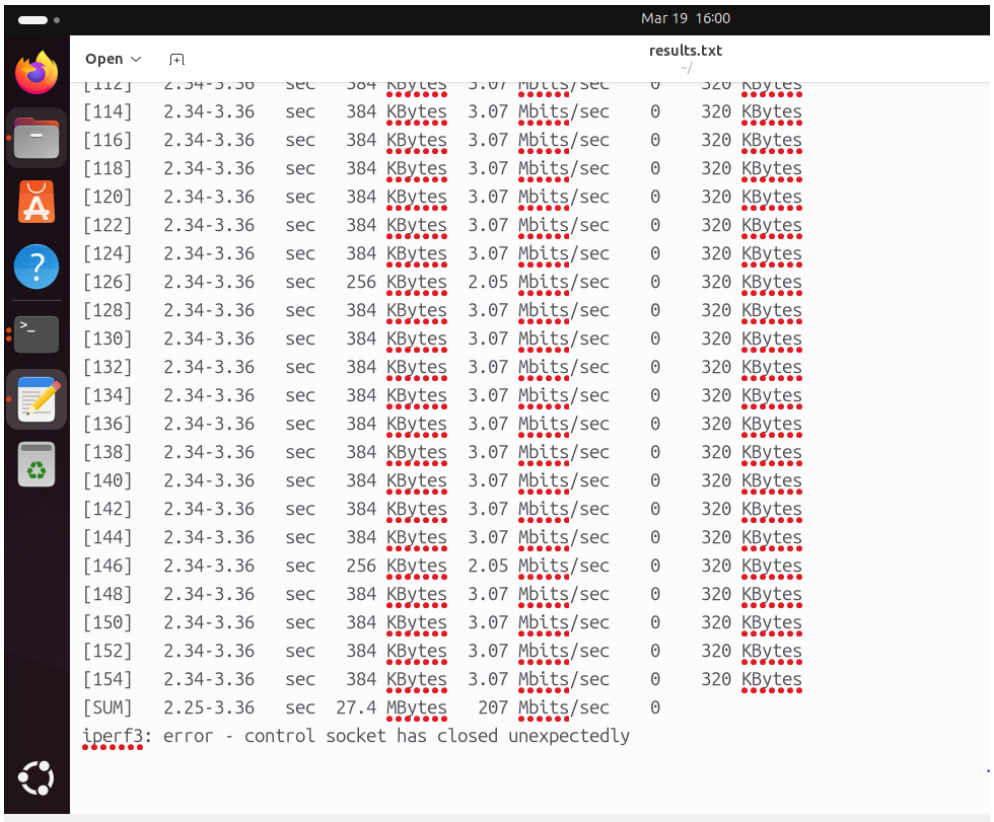
```
clarence@clarence-VirtualBox:~$ sudo tc qdisc add dev lo root tbf rate 350mbit burst 32kbit latency 400ms
[sudo] password for clarence:
clarence@clarence-VirtualBox:~$ iperf3 -c 127.0.0.2 -P 430 -t 30
```

Capped the bandwidth to 350mbps for testing



Not capped test (It exceeds the limit so it comes 0mbps after a few intervals)

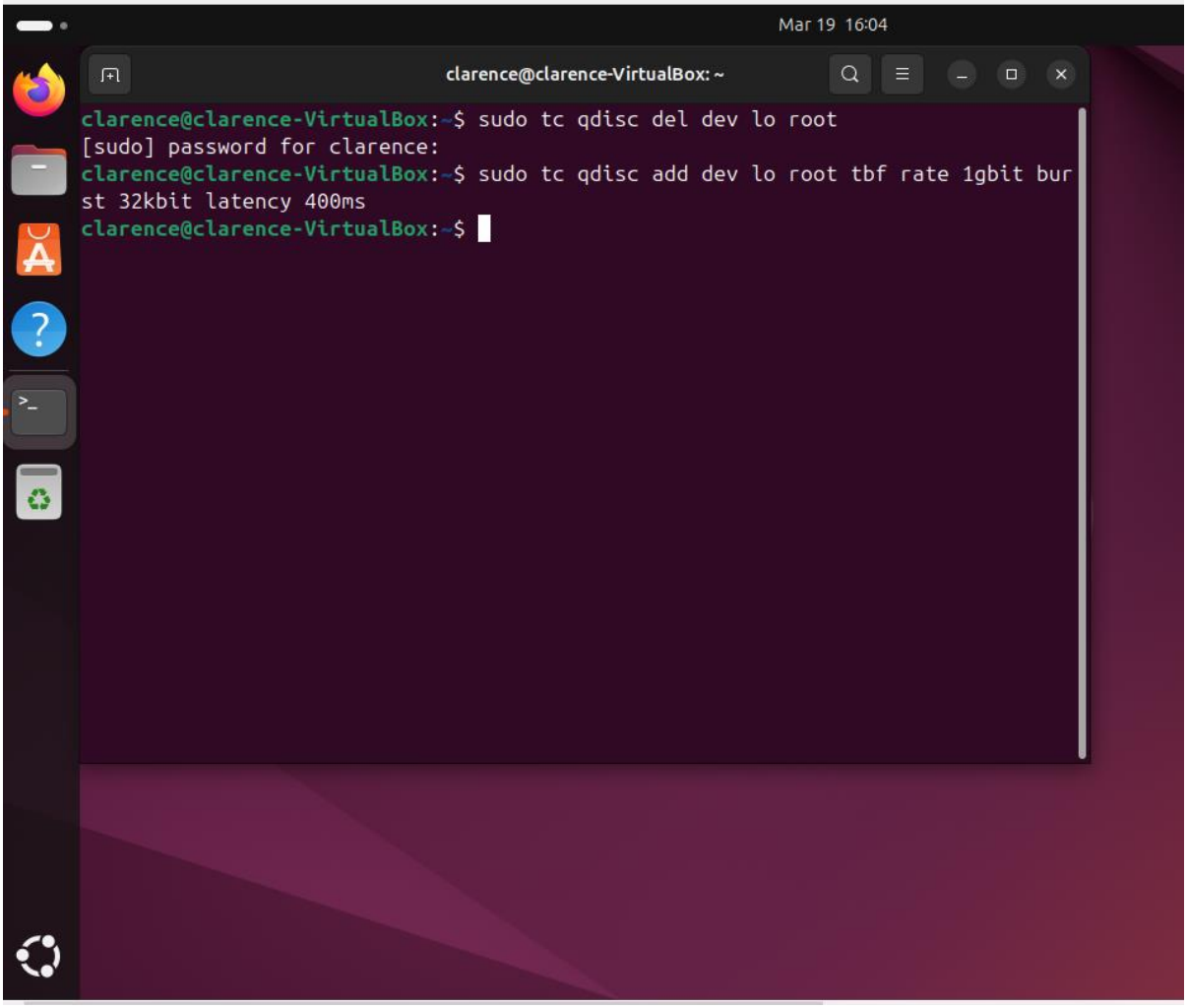

Mar 19 15:59
Open
results.txt
~/
[152] local 127.0.0.1 port 56154 connected to 127.0.0.1 port 5201
[154] local 127.0.0.1 port 56156 connected to 127.0.0.1 port 5201
[ID] Interval Transfer Bitrate Retr Cwnd
[6] 0.00-1.16 sec 384 KBytes 2.72 Mbits/sec 0 320 KBytes
[8] 0.00-1.16 sec 384 KBytes 2.72 Mbits/sec 0 320 KBytes
[10] 0.00-1.16 sec 384 KBytes 2.72 Mbits/sec 0 320 KBytes
[12] 0.00-1.16 sec 384 KBytes 2.72 Mbits/sec 0 320 KBytes
[14] 0.00-1.16 sec 384 KBytes 2.72 Mbits/sec 0 320 KBytes
[16] 0.00-1.16 sec 384 KBytes 2.72 Mbits/sec 0 320 KBytes
[18] 0.00-1.16 sec 384 KBytes 2.72 Mbits/sec 0 320 KBytes
[20] 0.00-1.16 sec 384 KBytes 2.72 Mbits/sec 0 320 KBytes
[22] 0.00-1.16 sec 384 KBytes 2.72 Mbits/sec 0 320 KBytes
[24] 0.00-1.16 sec 384 KBytes 2.72 Mbits/sec 0 320 KBytes
[26] 0.00-1.16 sec 384 KBytes 2.72 Mbits/sec 0 320 KBytes
[28] 0.00-1.16 sec 384 KBytes 2.72 Mbits/sec 0 320 KBytes
[30] 0.00-1.16 sec 384 KBytes 2.72 Mbits/sec 0 320 KBytes
[32] 0.00-1.16 sec 384 KBytes 2.72 Mbits/sec 0 320 KBytes
[34] 0.00-1.16 sec 384 KBytes 2.72 Mbits/sec 0 320 KBytes
[36] 0.00-1.16 sec 384 KBytes 2.72 Mbits/sec 0 320 KBytes
[38] 0.00-1.16 sec 384 KBytes 2.72 Mbits/sec 0 320 KBytes
[40] 0.00-1.16 sec 384 KBytes 2.72 Mbits/sec 0 320 KBytes
[42] 0.00-1.16 sec 384 KBytes 2.72 Mbits/sec 0 320 KBytes
[44] 0.00-1.16 sec 384 KBytes 2.72 Mbits/sec 0 320 KBytes
[46] 0.00-1.16 sec 384 KBytes 2.72 Mbits/sec 0 320 KBytes
[48] 0.00-1.16 sec 384 KBytes 2.72 Mbits/sec 0 320 KBytes


Mar 19 16:00
Open
results.txt
~/
[114] 2.34-3.36 sec 384 KBytes 3.07 Mbits/sec 0 320 KBytes
[116] 2.34-3.36 sec 384 KBytes 3.07 Mbits/sec 0 320 KBytes
[118] 2.34-3.36 sec 384 KBytes 3.07 Mbits/sec 0 320 KBytes
[120] 2.34-3.36 sec 384 KBytes 3.07 Mbits/sec 0 320 KBytes
[122] 2.34-3.36 sec 384 KBytes 3.07 Mbits/sec 0 320 KBytes
[124] 2.34-3.36 sec 384 KBytes 3.07 Mbits/sec 0 320 KBytes
[126] 2.34-3.36 sec 256 KBytes 2.05 Mbits/sec 0 320 KBytes
[128] 2.34-3.36 sec 384 KBytes 3.07 Mbits/sec 0 320 KBytes
[130] 2.34-3.36 sec 384 KBytes 3.07 Mbits/sec 0 320 KBytes
[132] 2.34-3.36 sec 384 KBytes 3.07 Mbits/sec 0 320 KBytes
[134] 2.34-3.36 sec 384 KBytes 3.07 Mbits/sec 0 320 KBytes
[136] 2.34-3.36 sec 384 KBytes 3.07 Mbits/sec 0 320 KBytes
[138] 2.34-3.36 sec 384 KBytes 3.07 Mbits/sec 0 320 KBytes
[140] 2.34-3.36 sec 384 KBytes 3.07 Mbits/sec 0 320 KBytes
[142] 2.34-3.36 sec 384 KBytes 3.07 Mbits/sec 0 320 KBytes
[144] 2.34-3.36 sec 384 KBytes 3.07 Mbits/sec 0 320 KBytes
[146] 2.34-3.36 sec 256 KBytes 2.05 Mbits/sec 0 320 KBytes
[148] 2.34-3.36 sec 384 KBytes 3.07 Mbits/sec 0 320 KBytes
[150] 2.34-3.36 sec 384 KBytes 3.07 Mbits/sec 0 320 KBytes
[152] 2.34-3.36 sec 384 KBytes 3.07 Mbits/sec 0 320 KBytes
[154] 2.34-3.36 sec 384 KBytes 3.07 Mbits/sec 0 320 KBytes
[SUM] 2.25-3.36 sec 27.4 MBytes 207 Mbits/sec 0
iperf3: error - control socket has closed unexpectedly

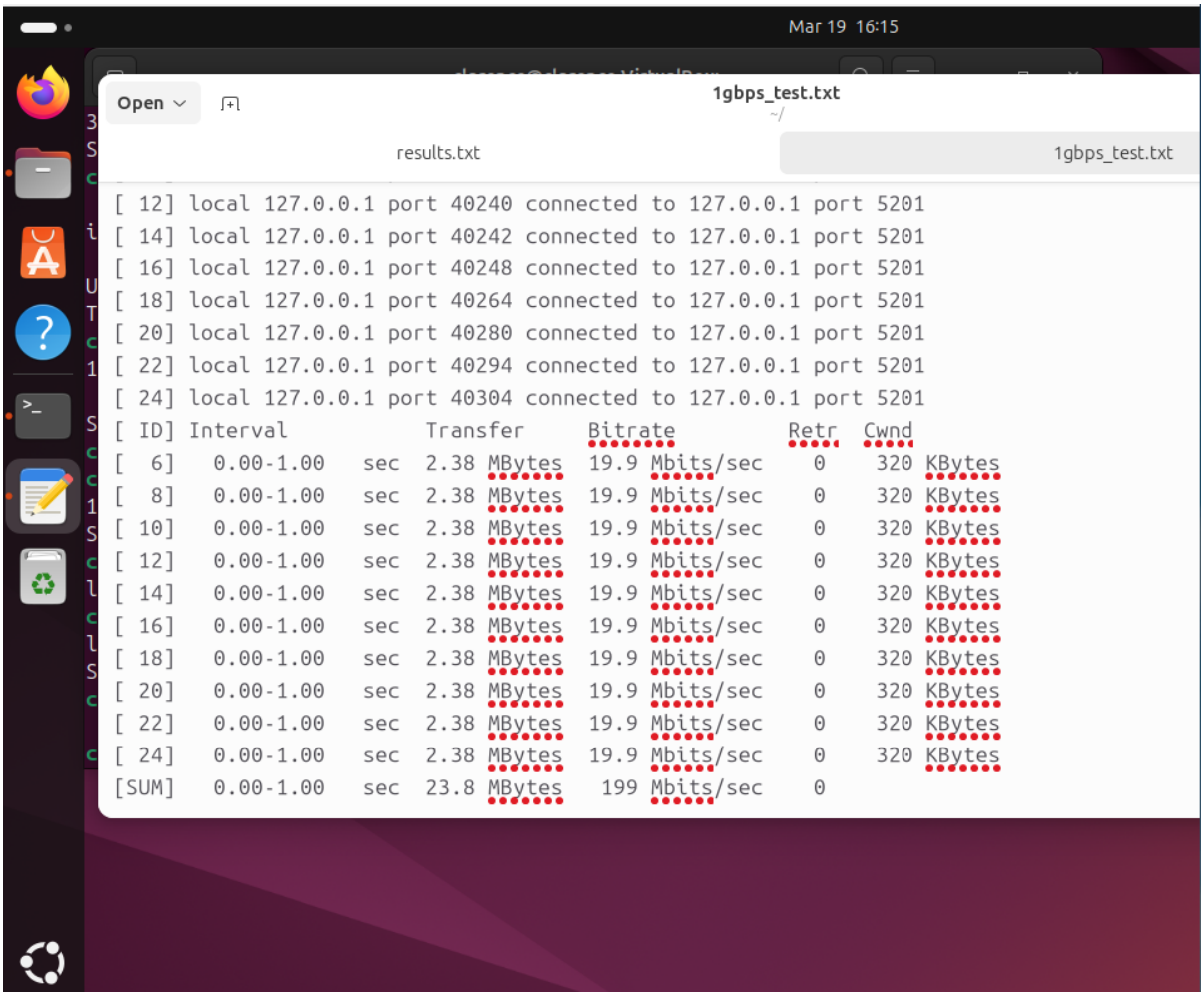
Capped bandwidth to 350mbps and tested 430 users

Also overloaded bandwidth causing packet loss and errors (It errors after a few intervals)

Proposed ISP for students (1gbps with traffic shaping) for the average of 430 students



Capped the bandwidth to 1gbps for testing

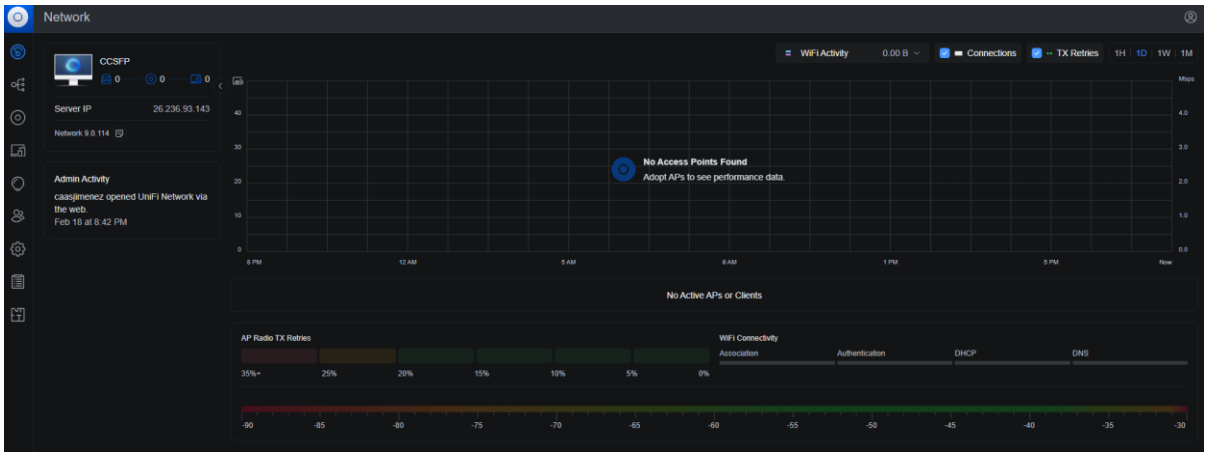


Not capped test (Stable bandwidth with the sum of 199mbits/sec per interval)

Appendix T
Metric Table

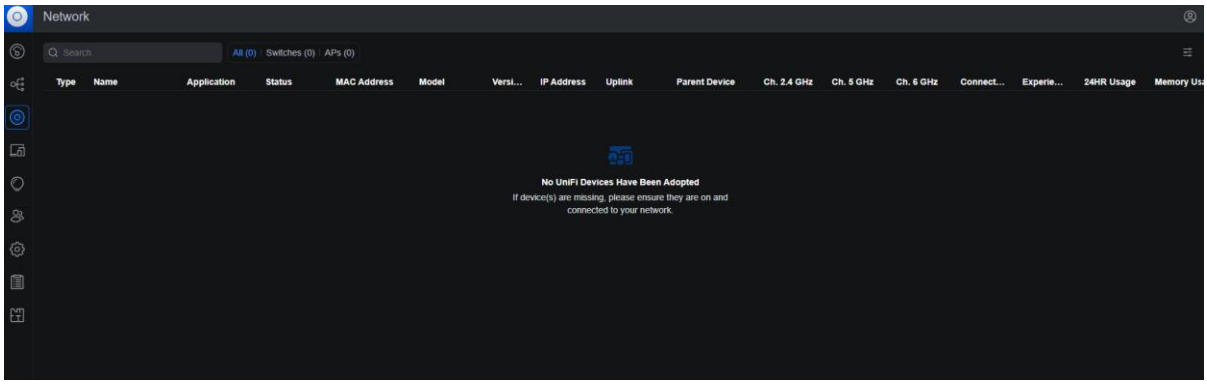
Metric	Starlink (8-350 Mbps) - Current ISP	PLDT (1 Gbps) - Proposed ISP
Bandwidth	8 - 350 Mbps	1 Gbps (1000 Mbps)
Estimated WiFi Users	430 - 460 students	430 - 460 students
Throughput per Student (Best Case)	350 Mbps / 460 = 0.76 Mbps	1000 Mbps / 460 = 2.17 Mbps
Throughput per Student (Worst Case)	8 Mbps / 460 = 0.017 Mbps	1000 Mbps / 460 = 2.17 Mbps
Max Concurrent Users (Assuming 5 Mbps per user)	70 users (at 350 Mbps max)	200 users (1 Gbps)
Max Concurrent Users (Assuming 2 Mbps per user)	175 users (at 350 Mbps max)	500 users (1 Gbps)
Per Student Base Allocation	Limited, highly variable	2 Mbps per student
Priority Apps (Zoom, Youtube, EDU, Google Classroom, etc.)	Dependent on congestion	3-5 Mbps per student
P2P/Downloads	Not Restricted but inconsistent	Restricted
Gaming, Social Media	Allowed but can be laggy	Deprioritized
Peak Hours Cap	Unpredictable speeds	2 Mbps per student
Off-Peak Flexibility	Higher speeds but inconsistent	3-5 Mbps per student

Appendix U
UniFi Controller Dashboard



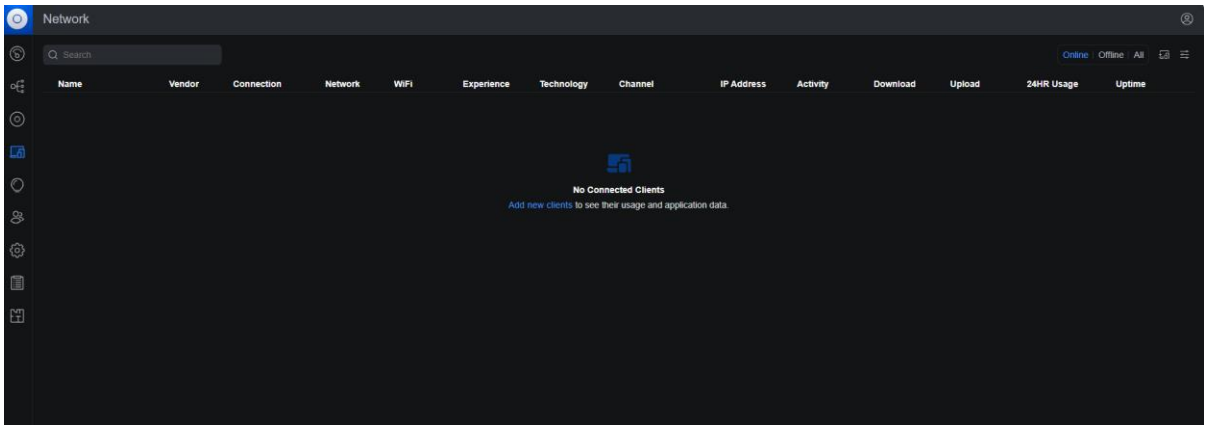
The UniFi Controller dashboard gives you a clear overview of your WiFi's network statistics.

Here you can view the connected devices, the data usage and possible errors in your system.



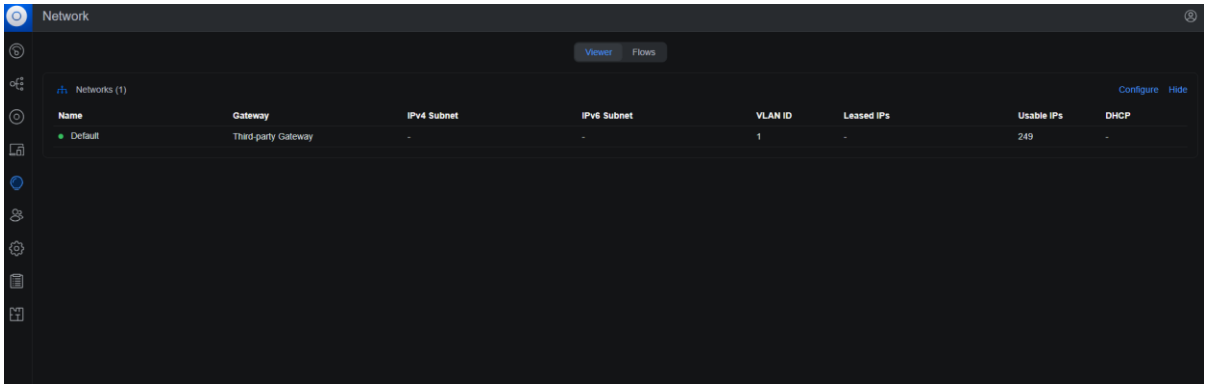
UniFi Devices Dashboard

The devices dashboard is where you can view your connected UniFi devices, in our situation because we don't have any devices connected it won't display any devices.



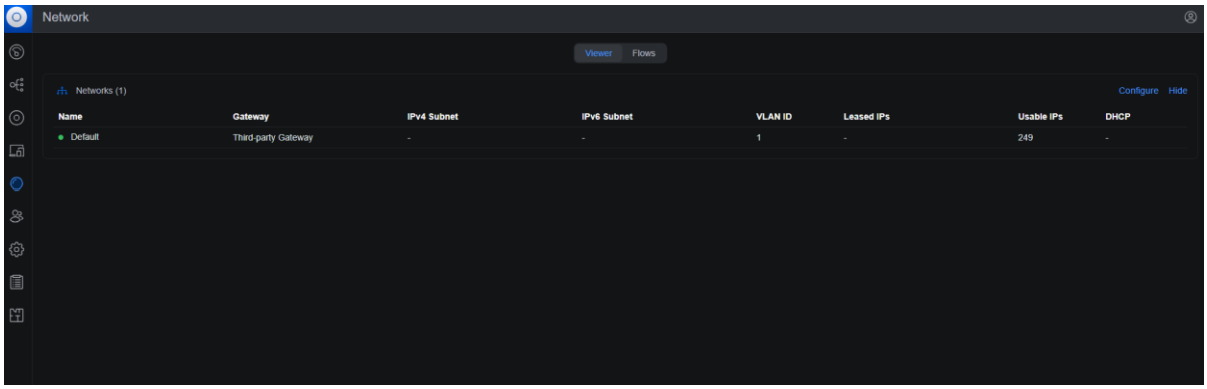
Client Devices Tab

The Client Devices tab on the UniFi Controller offers complete information on each device connected on the network, including simple details and real-time information like throughput, signal quality, and Wi-Fi band.



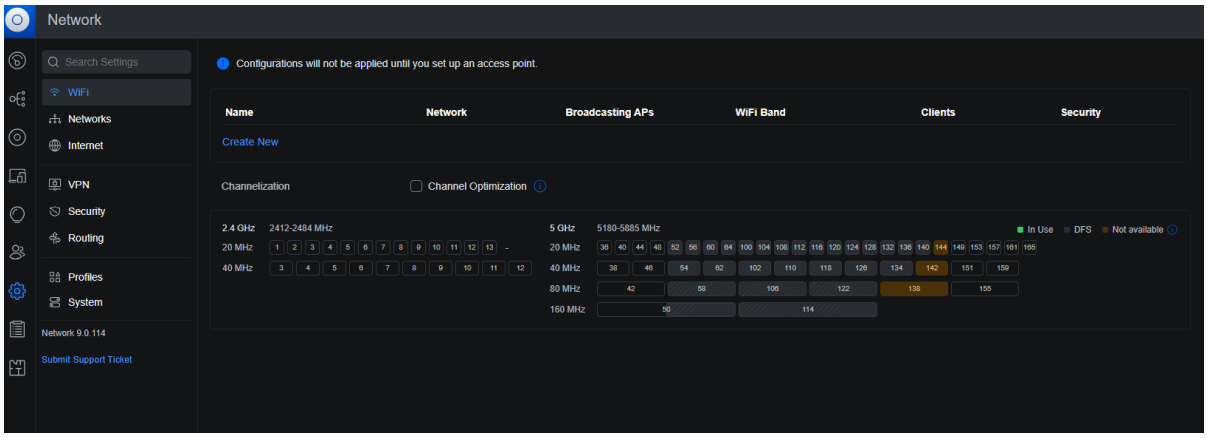
Insights Tab

The Insights tab offers in-depth performance statistics and historical trends for connected devices, enabling you to detect potential network problems and optimize device performance.



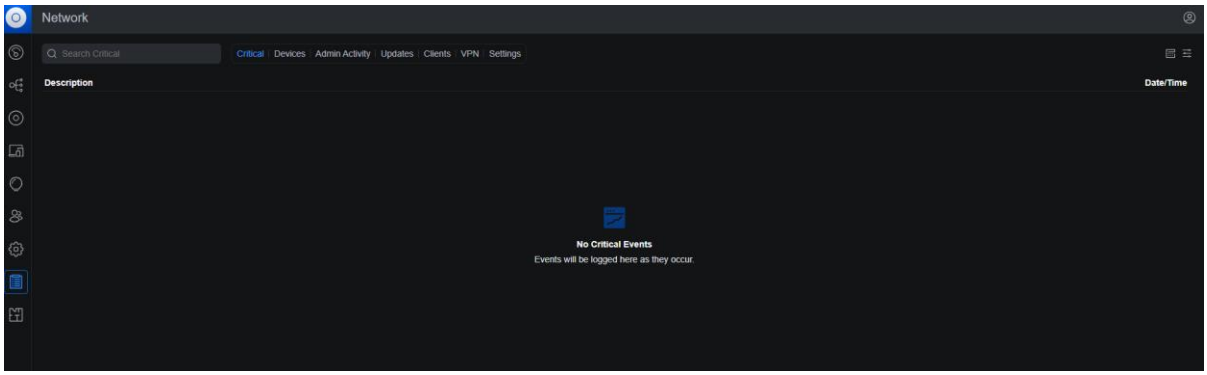
Admins Tab

The Admins tab enables you to control and set up the roles and permissions of users with access to the UniFi Controller, providing adequate access control for network management.



Settings Tab

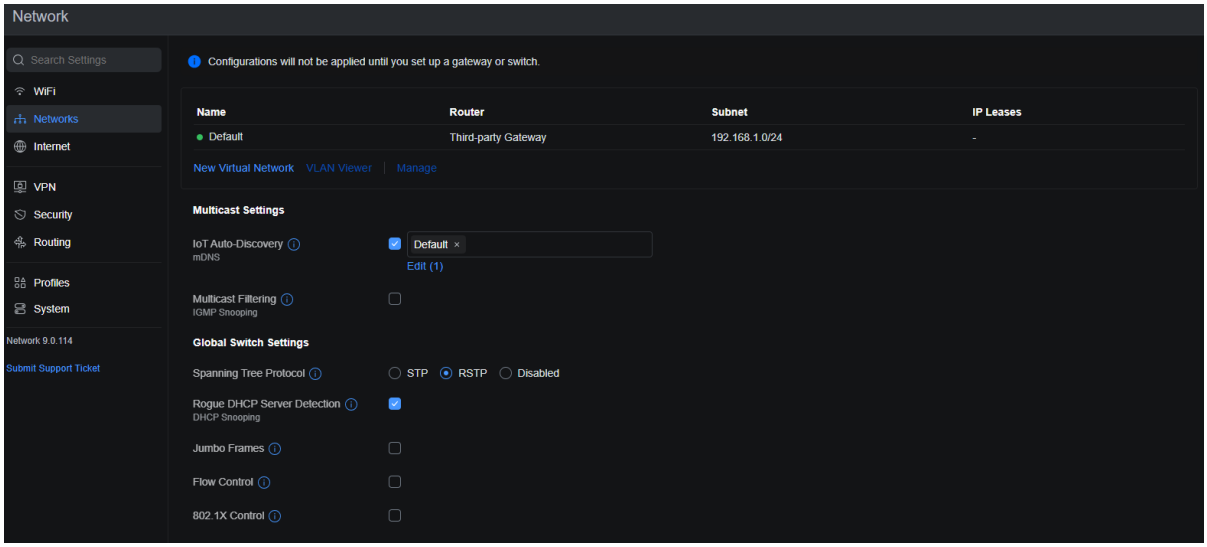
The Settings tab offers access to set up and personalize a number of network settings, such as Wi-Fi networks, security settings, system preferences, and device management to provide the best overall network performance and functionality.



System Log Tab

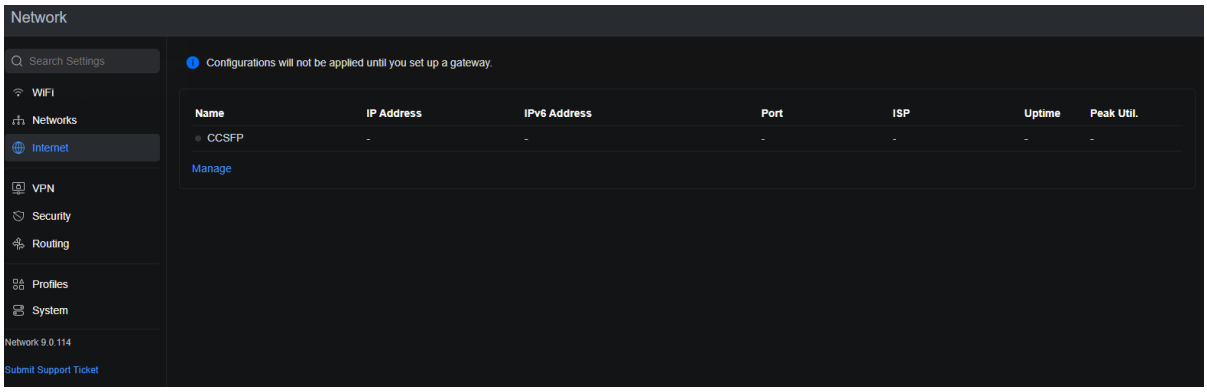
The System Log tab shows the detailed logs of system activities and events, such as errors, warnings, and informational messages, to facilitate diagnosing and troubleshooting network or system problems.

Sub tabs under settings section



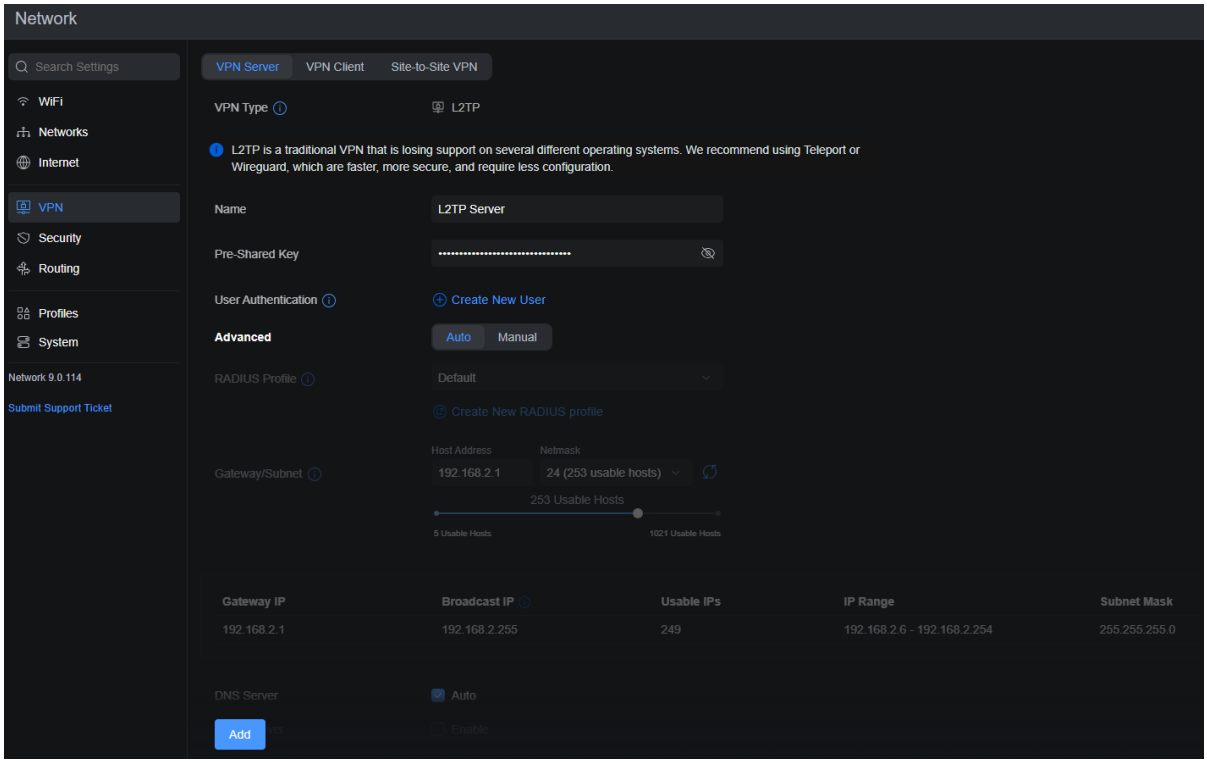
Network Tab

The Network tab provides you with the ability to set up and control the network settings, including IP addressing, VLANs, DHCP settings, and routing options, to provide proper communication and segmentation within the network.



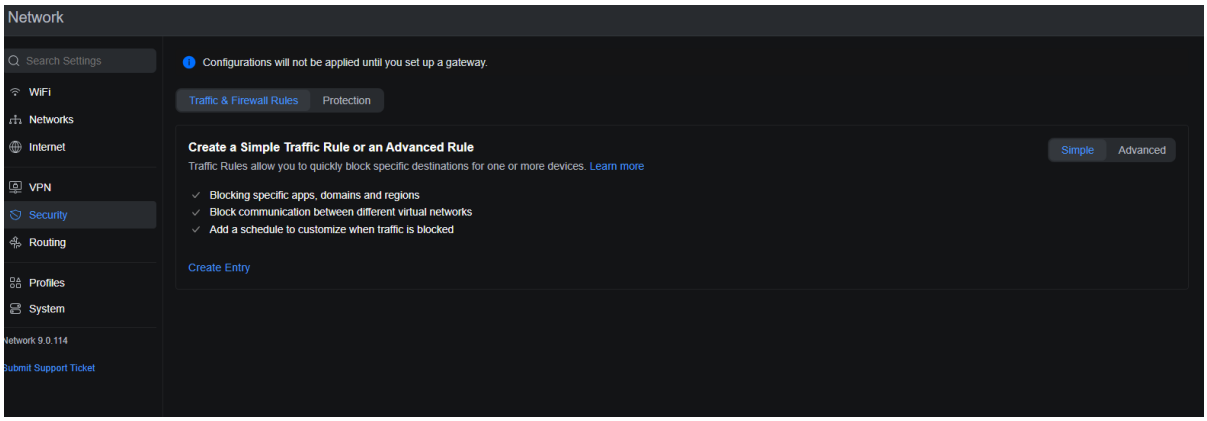
Internet Tab

The Internet tab provides you with the ability to set up the WAN settings, control the connection to your internet service provider, and configure features such as DNS, DHCP, and failover for internet access.



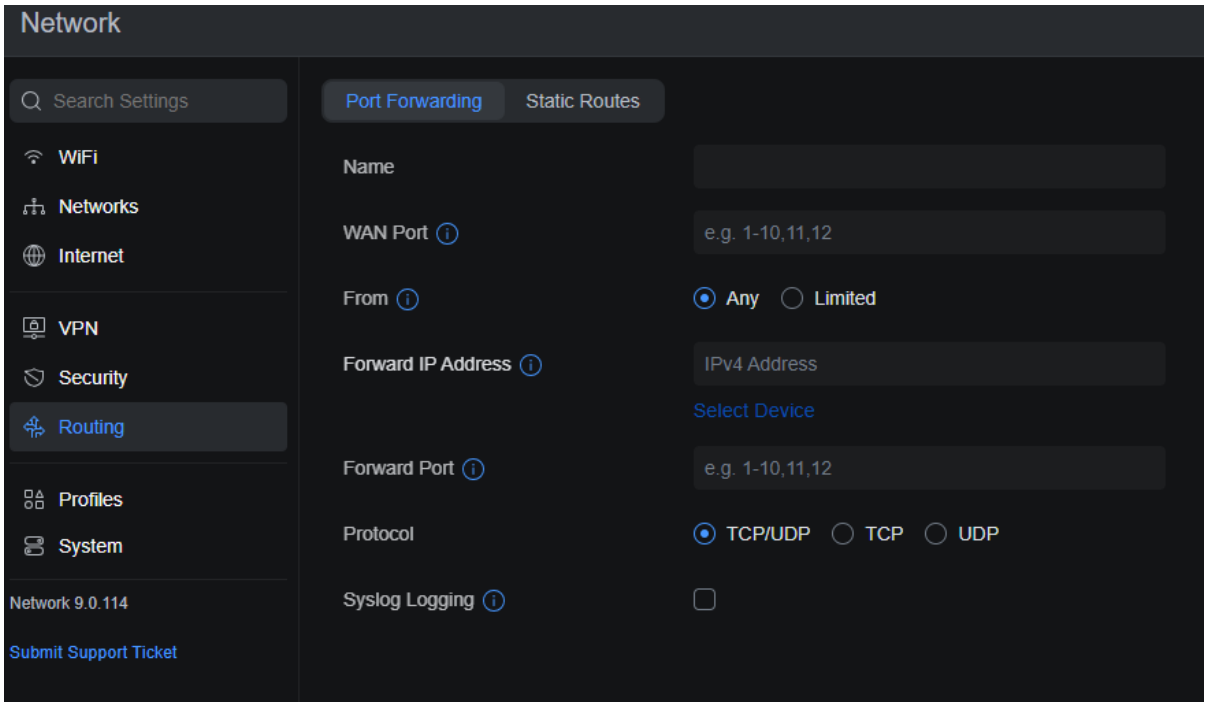
VPN Tab

The VPN tab supports the setup and management of Virtual Private Network (VPN) configurations, enabling safe remote access to the network using protocols such as L2TP, PPTP, and OpenVPN.



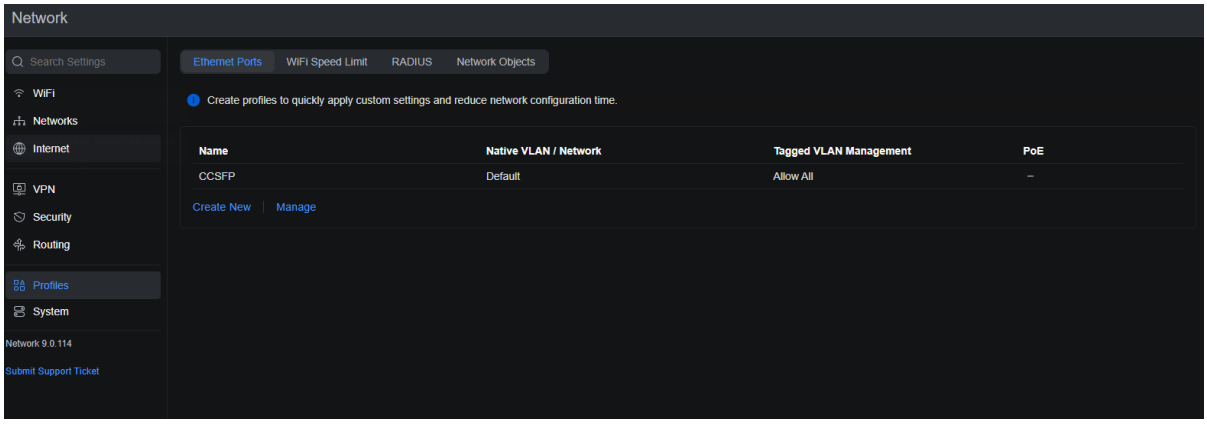
Security Tab

The Security tab permits you to set up network security options, such as firewall settings, intrusion detection, and safe guest access, to secure the network against unwanted access and malicious threats.



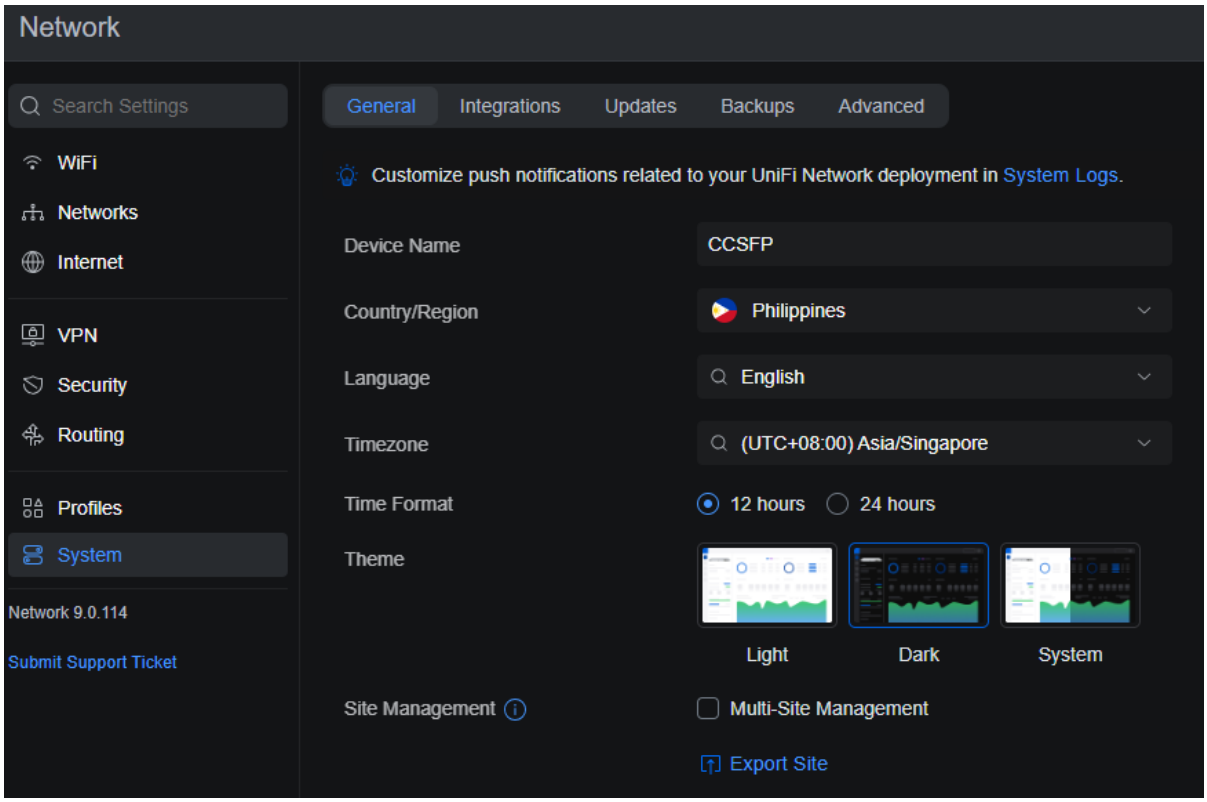
Routing Tab

The Routing tab permits you to control routing settings such as static routes, routing protocols, and routing tables in your network to organize the flow of data between a subnet or within networks.



Profile Tab

The Profile tab gives one the capacity to set device or user profiles such as data capping, controls, and modes of authenticating users on a network.



System Tab

The System tab enables one to handle system settings like firmware updates, backup, configurations, and monitoring of devices within the UniFi Controller to allow effective running and management.

Ubiquiti devices provide high-quality performance while being cost-effective, making them suitable for small to medium-sized networks. Having a centralized management through UniFi Controller makes network monitoring, configuration, and troubleshooting easier as well. Also, Ubiquiti products provide great scalability, user-friendly interface, and strong security features to ensure reliable connectivity in various network environments.

Appendix V
Network Configurations

Subnet for each VLAN

	CORE-SWITCH	Software Switch	port4 port5	192.168.1.1/255.255.255.0	PING HTTPS SSH
•	LAB (VLAN_10)	VLAN		192.168.40.1/255.255.255.0	PING HTTPS SSH
•	MANANGEMENT (VLAN_99)	VLAN		192.168.99.1/255.255.255.0	PING HTTPS SSH SNMP FMG-Access
•	STUDENT (VLAN_20)	VLAN		192.168.80.1/255.255.240.0	PING HTTPS SSH
•	TEACHER (VLAN_30)	VLAN		192.168.60.1/255.255.254.0	PING HTTPS SSH

Students: (3000 devices): 192.168.80.1 255.255.240.0
4094 usable IPs (192.168.80.1 to 192.168.95.254)

Teachers and Staff: (300 devices): 192.168.60.1 255.255.254.0
510 usable IPs (192.168.60.1 to 192.168.61.254)

LAB: 192.168.80.1 255.255.255.0
Small group, dedicated to only LAB

Management VLAN: 192.168.80.1 255.255.255.0
Dedicated for network device management

PORT1 ISP1

FortiGate-VM64-KVM # config system interface

FortiGate-VM64-KVM (interface) # edit port1

FortiGate-VM64-KVM (port1) # set vdom "root"

FortiGate-VM64-KVM (port1) # set mode dhcp

FortiGate-VM64-KVM (port1) # set allowaccess ping https ssh http fgfm

FortiGate-VM64-KVM (port1) # set role wan

FortiGate-VM64-KVM (port1) # set alias "Primary ISP"

FortiGate-VM64-KVM (port1) # next

FortiGate-VM64-KVM (interface) # end

PORT2 ISP 2

FortiGate-VM64-KVM # config system interface

FortiGate-VM64-KVM (interface) # edit port2

FortiGate-VM64-KVM (port2) # set vdom "root"

FortiGate-VM64-KVM (port2) # set ip 192.168.20.1 255.255.254.0

FortiGate-VM64-KVM (port2) # set allowaccess ping https ssh

FortiGate-VM64-KVM (port2) # set role wan

FortiGate-VM64-KVM (port2) # set alias "Secondary ISP"

FortiGate-VM64-KVM (port2) # next

FortiGate-VM64-KVM (interface) # end

PORT3 ISP3

FortiGate-VM64-KVM # config system interface

FortiGate-VM64-KVM (interface) # edit port3

FortiGate-VM64-KVM (port3) # set vdom "root"

FortiGate-VM64-KVM (port3) # set ip 192.168.30.1 255.255.254.0

FortiGate-VM64-KVM (port3) # set allowaccess ping https ssh

FortiGate-VM64-KVM (port3) # set role wan

FortiGate-VM64-KVM (port3) # set alias "Tertiary ISP"

FortiGate-VM64-KVM (port3) # next

FortiGate-VM64-KVM (interface) # end

PORT4 TO MAIN SWITCH

FortiGate-VM64-KVM # config system interface

FortiGate-VM64-KVM (interface) # edit port4

FortiGate-VM64-KVM (port4) # set vdom "root"

FortiGate-VM64-KVM (port4) # set ip 192.168.1.1 255.255.255.0

FortiGate-VM64-KVM (port4) # set allowaccess ping https ssh

FortiGate-VM64-KVM (port4) # set role lan

FortiGate-VM64-KVM (port4) # set alias "LAN"

FortiGate-VM64-KVM (port4) # next

FortiGate-VM64-KVM (interface) # end

VLAN 10 ADMIN

FortiGate-VM64-KVM (interface) # edit "VLAN_10"
new entry 'VLAN_10' added

FortiGate-VM64-KVM (VLAN_10) # set vdom "root"

FortiGate-VM64-KVM (VLAN_10) # set ip 192.168.40.1 255.255.255.0

FortiGate-VM64-KVM (VLAN_10) # set allowaccess ping https ssh

FortiGate-VM64-KVM (VLAN_10) # set type vlan

FortiGate-VM64-KVM (VLAN_10) # set interface "port4"

FortiGate-VM64-KVM (VLAN_10) # set vlanid 10

FortiGate-VM64-KVM (VLAN_10) # set alias "Admin VLAN"

FortiGate-VM64-KVM (VLAN_10) # next

VLAN 20 STUDENTS

FortiGate-VM64-KVM (interface) # edit "VLAN_20"
new entry 'VLAN_20' added

FortiGate-VM64-KVM (VLAN_20) # set vdom "root"

FortiGate-VM64-KVM (VLAN_20) # set ip 192.168.50.1 255.255.255.0

FortiGate-VM64-KVM (VLAN_20) # set allowaccess ping https ssh

FortiGate-VM64-KVM (VLAN_20) # set type vlan

FortiGate-VM64-KVM (VLAN_20) # set interface "port4"

FortiGate-VM64-KVM (VLAN_20) # set vlanid 20

FortiGate-VM64-KVM (VLAN_20) # set alias "Student VLAN"

FortiGate-VM64-KVM (VLAN_20) # next

VLAN 30 TEACHER

FortiGate-VM64-KVM (interface) # edit VLAN_30
new entry 'VLAN_30' added

FortiGate-VM64-KVM (VLAN_30) # set vdom "root"

FortiGate-VM64-KVM (VLAN_30) # set ip 192.168.60.1 255.255.255.0

FortiGate-VM64-KVM (VLAN_30) # set allowaccess ping https ssh

FortiGate-VM64-KVM (VLAN_30) # set type vlan

FortiGate-VM64-KVM (VLAN_30) # set interface "port4"

FortiGate-VM64-KVM (VLAN_30) # set vlanid 30

FortiGate-VM64-KVM (VLAN_30) # set alias "Teacher VLAN"

FortiGate-VM64-KVM (VLAN_30) # next

FortiGate-VM64-KVM (interface) # end

VLAN 99 Management

FortiGate-VM64-KVM (interface) # edit VLAN_99
new entry 'VLAN_30' added

FortiGate-VM64-KVM (VLAN_30) # set vdom "root"

FortiGate-VM64-KVM (VLAN_30) # set ip 192.168.99.1 255.255.255.0

FortiGate-VM64-KVM (VLAN_30) # set allowaccess ping https ssh snmp fgfm

FortiGate-VM64-KVM (VLAN_30) # set type vlan

FortiGate-VM64-KVM (VLAN_30) # set interface "CORE-SWITCH"

FortiGate-VM64-KVM (VLAN_30) # set vlanid 99

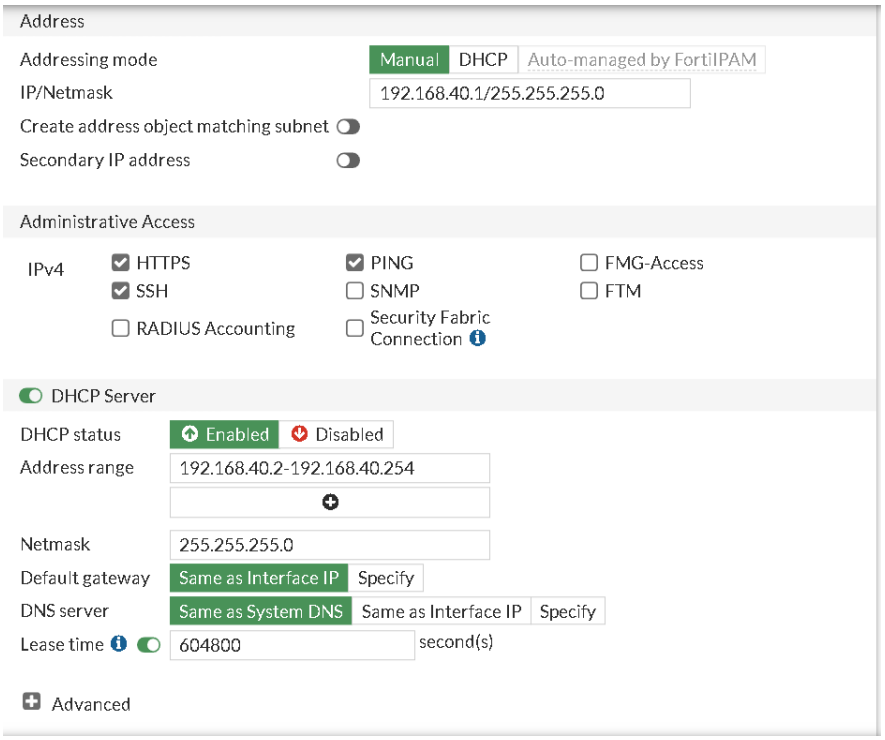
FortiGate-VM64-KVM (VLAN_30) # set alias "Management VLAN"

FortiGate-VM64-KVM (VLAN_30) # next

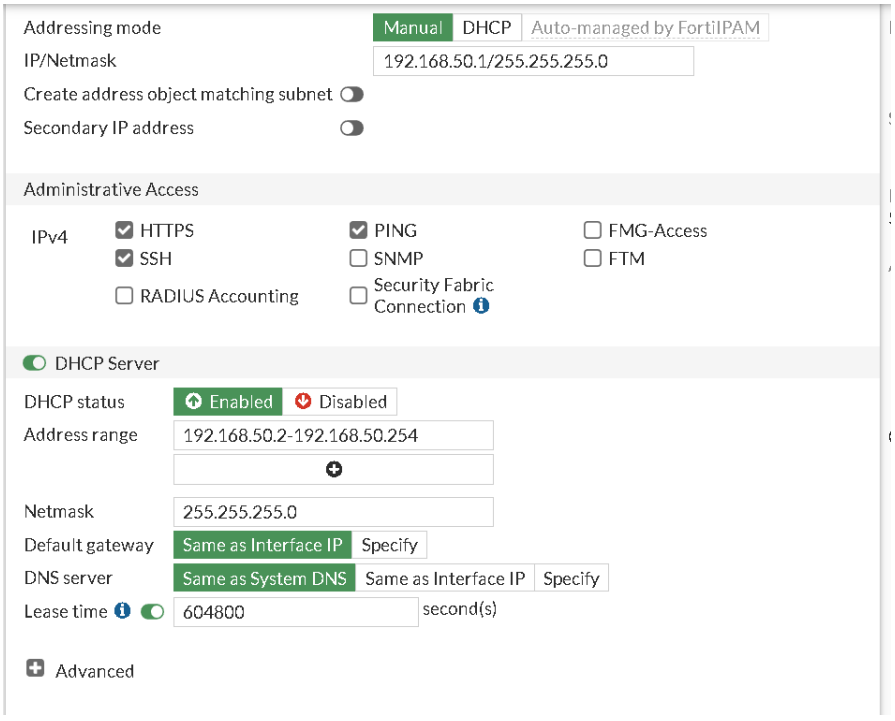
FortiGate-VM64-KVM (interface) # end

DHCP SERVER FOR VLANS (GUI)

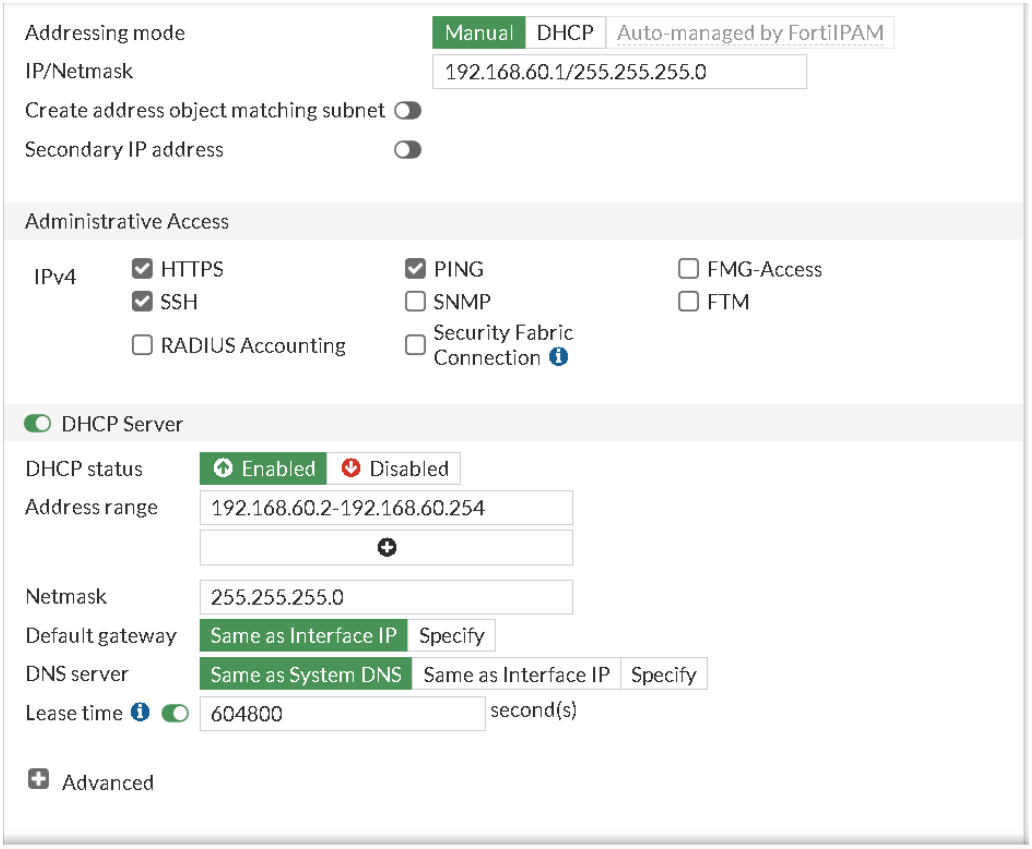
VLAN_10 IP range: 192.168.40.2 - 192.168.40.254



VLAN_20 IP range: 192.168.50.2 - 192.168.50.254



VLAN_30 IP range: 192.168.60.2 - 192.168.60.254



ROUTER POLICY (WHICH VLAN SHOULD USE)
Teacher (VLAN30) ISP 1, Student (VLAN20) ISP 2, Admin (VLAN10) ISP 3 (Wired connections)

LAB (Wired connections)

FortiGate-VM64-KVM # config router policy

FortiGate-VM64-KVM (policy) # edit 3
new entry '3' added

FortiGate-VM64-KVM (3) # set input-device "VLAN_10"

FortiGate-VM64-KVM (3) # set output-device "port3"

FortiGate-VM64-KVM (3) # set dst 0.0.0.0/0

FortiGate-VM64-KVM (3) # set gateway 192.168.30.1

FortiGate-VM64-KVM (3) # next

FortiGate-VM64-KVM (policy) # end

STUDENTS

FortiGate-VM64-KVM # config router policy

FortiGate-VM64-KVM (policy) # edit 1
new entry '1' added

FortiGate-VM64-KVM (1) # set input-device "VLAN_20"

FortiGate-VM64-KVM (1) # set output-device "port2"

FortiGate-VM64-KVM (1) # set dst 0.0.0.0/0

FortiGate-VM64-KVM (1) # set gateway 192.168.20.1

FortiGate-VM64-KVM (1) # next

FortiGate-VM64-KVM (policy) # end

TEACHERS

FortiGate-VM64-KVM # config router policy

FortiGate-VM64-KVM (policy) # edit 2
new entry '2' added

FortiGate-VM64-KVM (2) # set input-device "VLAN_30"

FortiGate-VM64-KVM (2) # set output-device "port1"

FortiGate-VM64-KVM (2) # set dst 0.0.0.0/0

FortiGate-VM64-KVM (2) # set gateway 192.168.137.129

FortiGate-VM64-KVM (2) # next

FortiGate-VM64-KVM (policy) # end

FIREWALL POLICY FOR Management (To block access)

config firewall policy

```
    edit 11
        set name "Block Other VLANs to Mgmt"
        set srcintf "VLAN_20"  # Adjust for other VLANs
        set dstintf "VLAN_99"
        set action deny
        set schedule "always"
        set service "ALL"
    next
end
```

FOR THE MSW, DSWS, AND PCS (simulating the connection of people from access points)

MSW1 and MSW2

```
enable
configure terminal

vlan 10
name Admin
vlan 20
name Students
vlan 30
name Teachers
vlan 99
name Management
exit

interface e0/0
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30
exit


interface e0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30
exit

interface e0/2
switchport trunk encapsulation dot1q
switchport mode trunk
```

```
switchport trunk allowed vlan 10,20,30
exit

interface e0/3
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30
exit

end
write memory
```

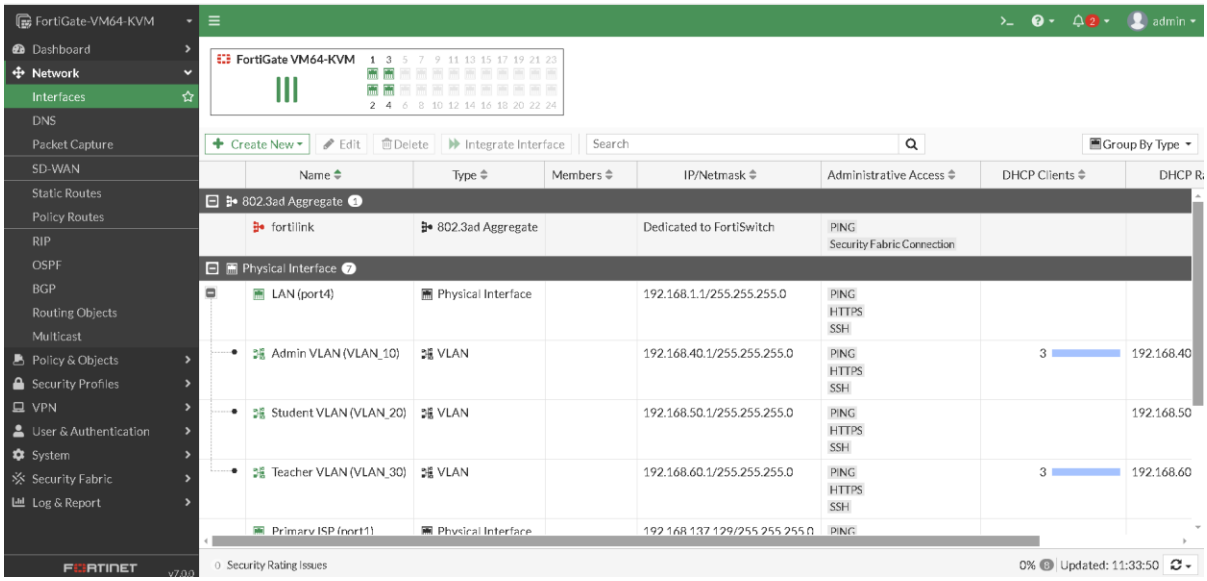
DSW1 & DSW2

```
enable
configure terminal

vlan 10
name Admin
vlan 20
name Students
vlan 30
name Teachers
vlan 99
name Management
exit

interface e0/0
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30
exit

interface e1/0
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30
exit

interface e0/1
switchport mode access
switchport access vlan 10
exit

interface e0/2
```

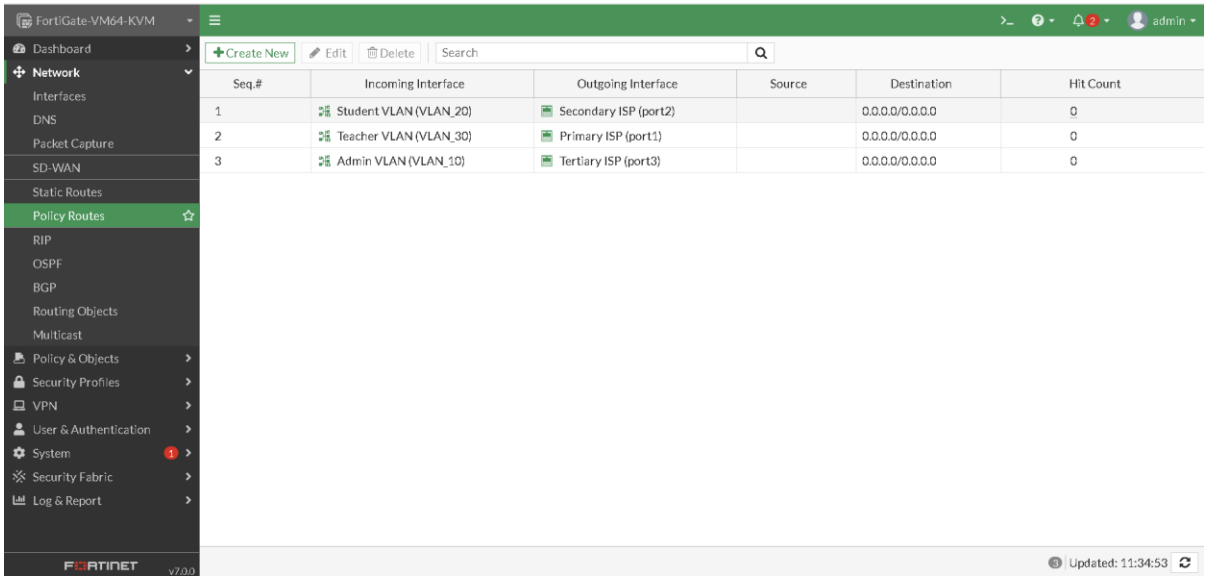
```
switchport mode access
switchport access vlan 20
exit

interface e0/3
switchport mode access
switchport access vlan 30
exit

end
write memory
```

Appendix W
Fortinet Fortigate Configuration

Interfaces

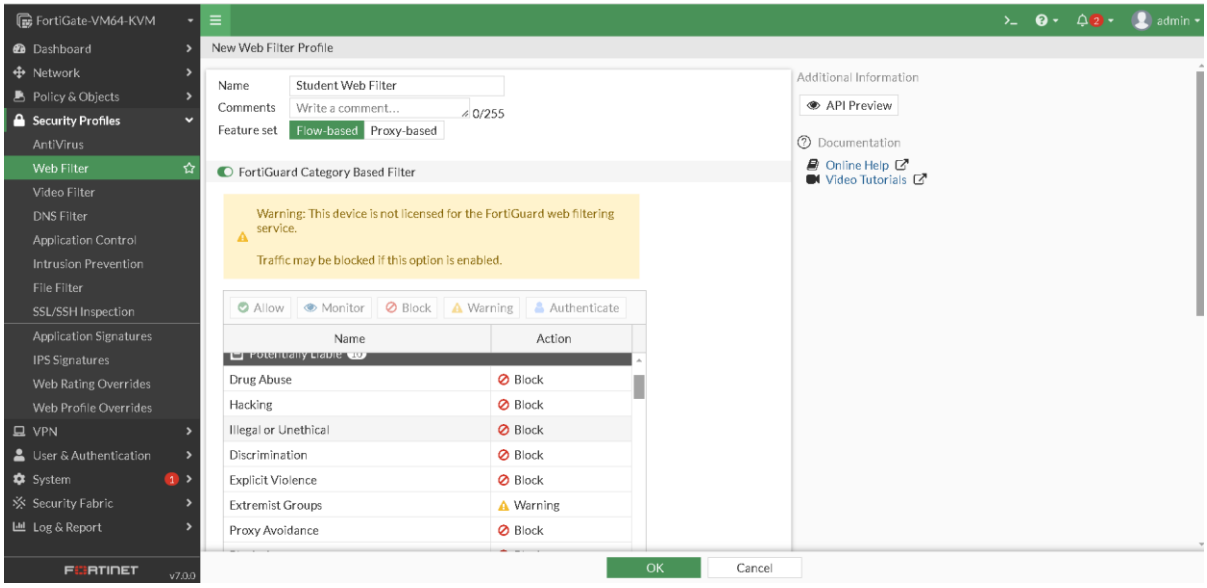


VLAN Routes

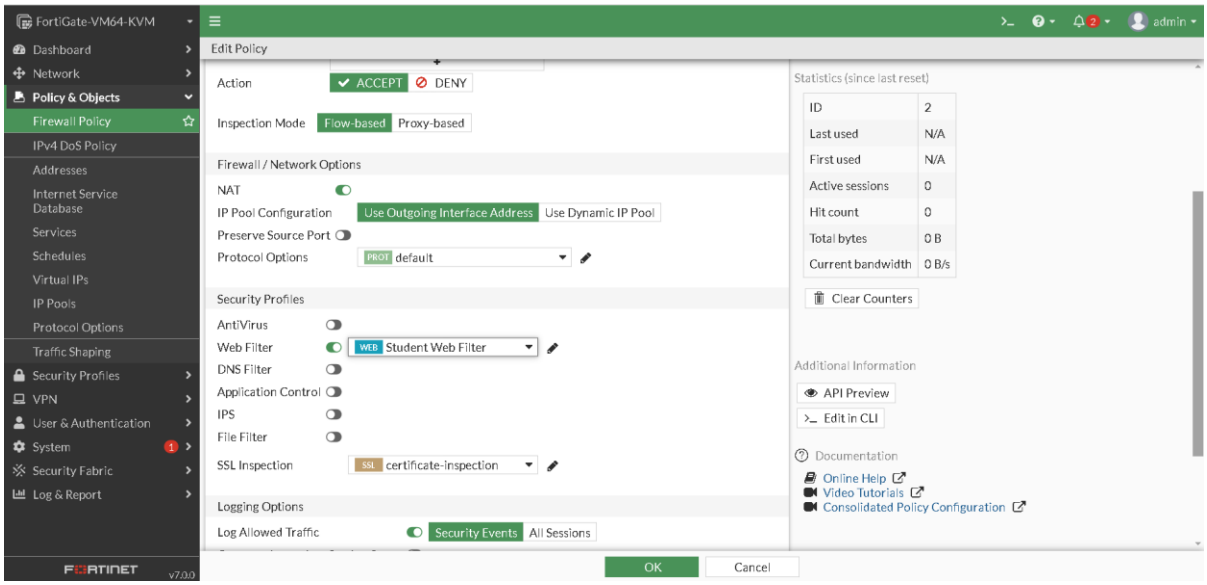


Web FIltering

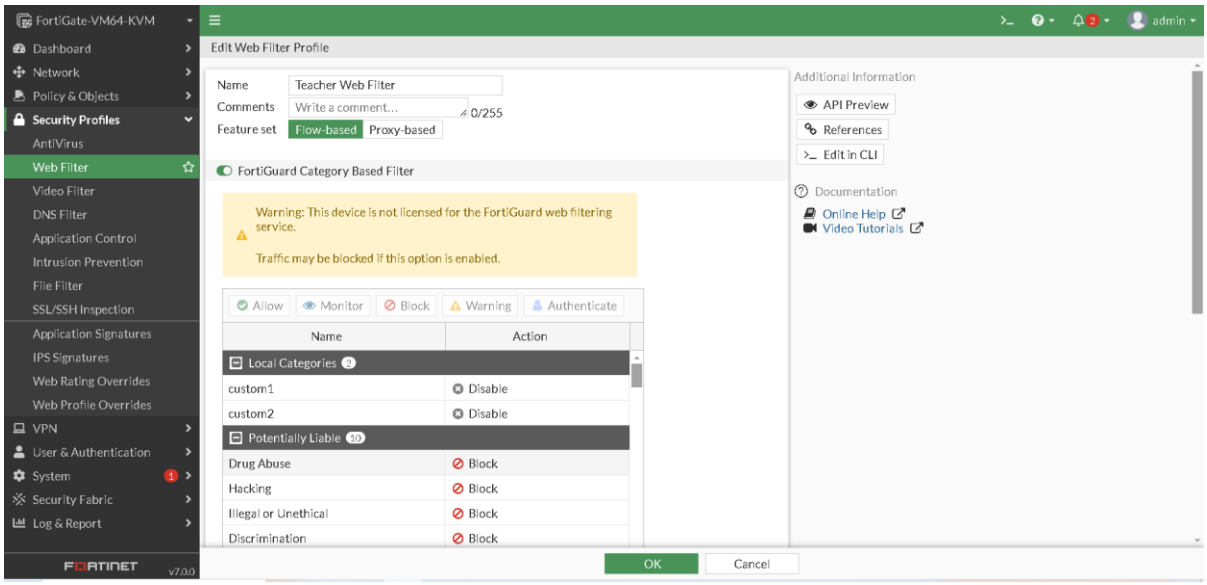
Create specific web filters for students



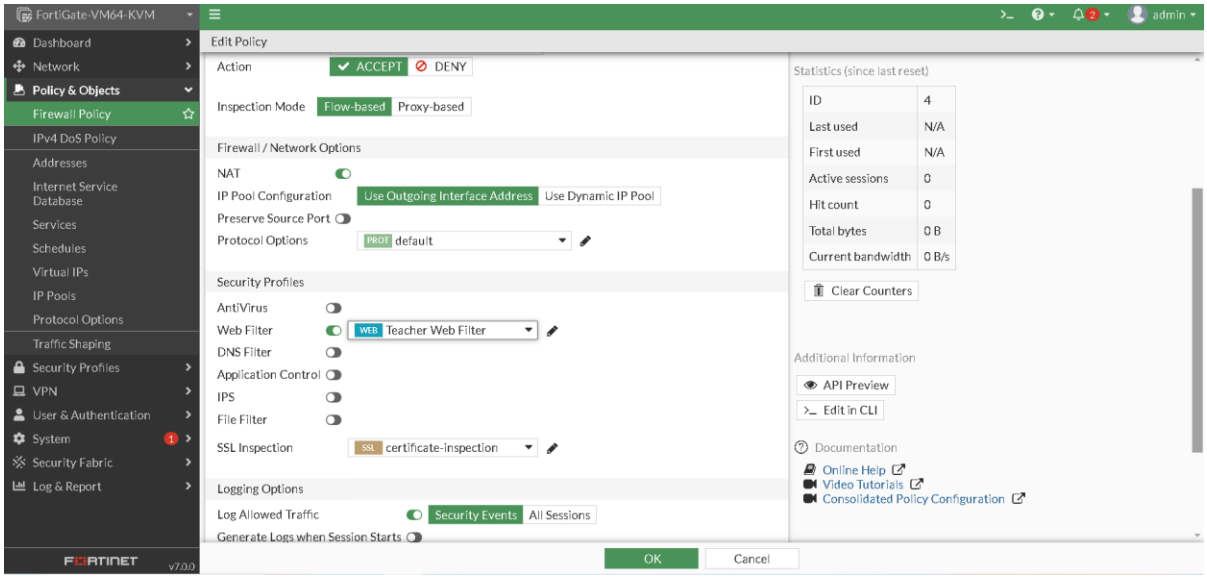
Add the Web Filter to the Firewall Policy of students



Add specific web filters for teachers

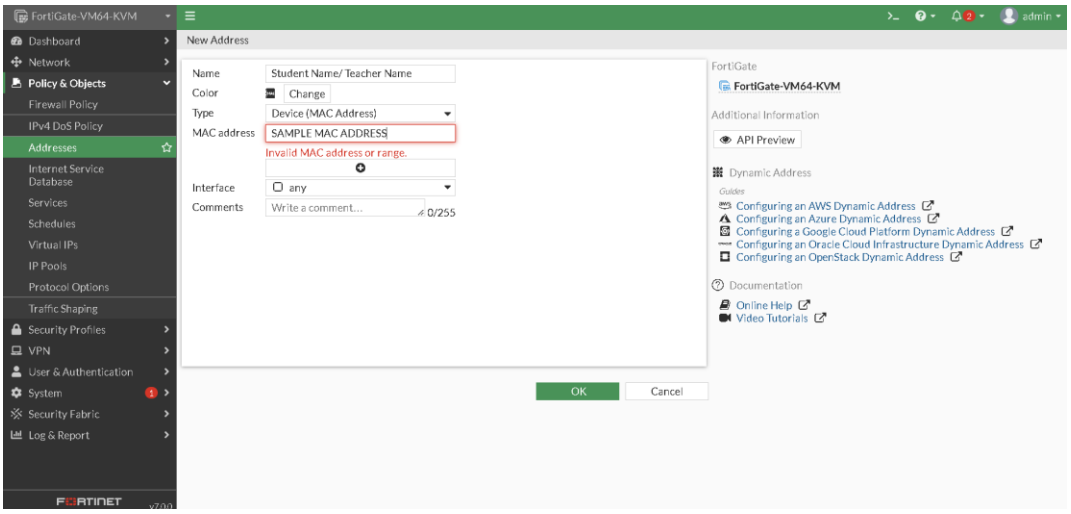


Add the Web filter to the firewall policy of teachers

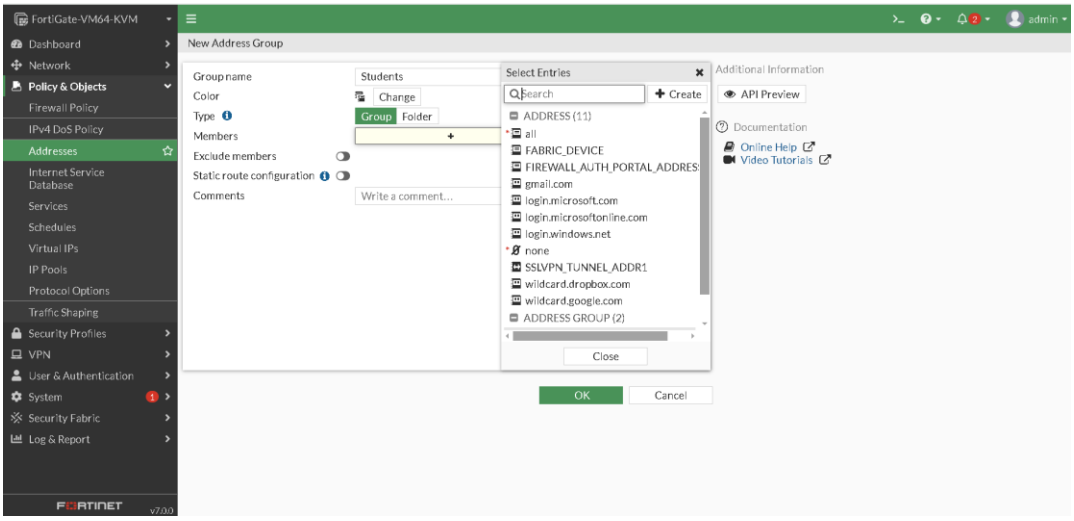


MAC Address Filtering

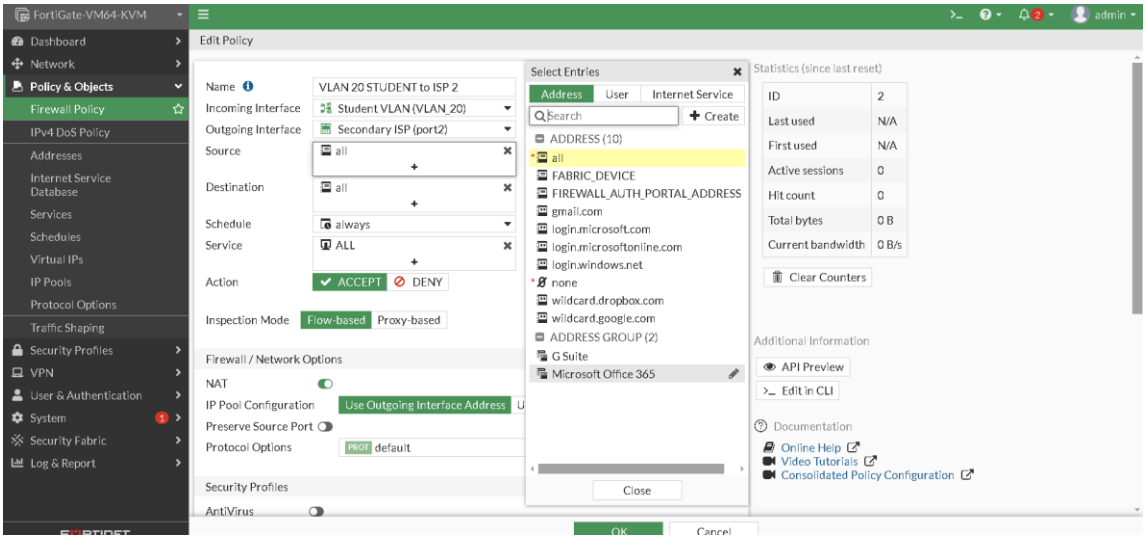
Add new address of the devices of Students/Teachers



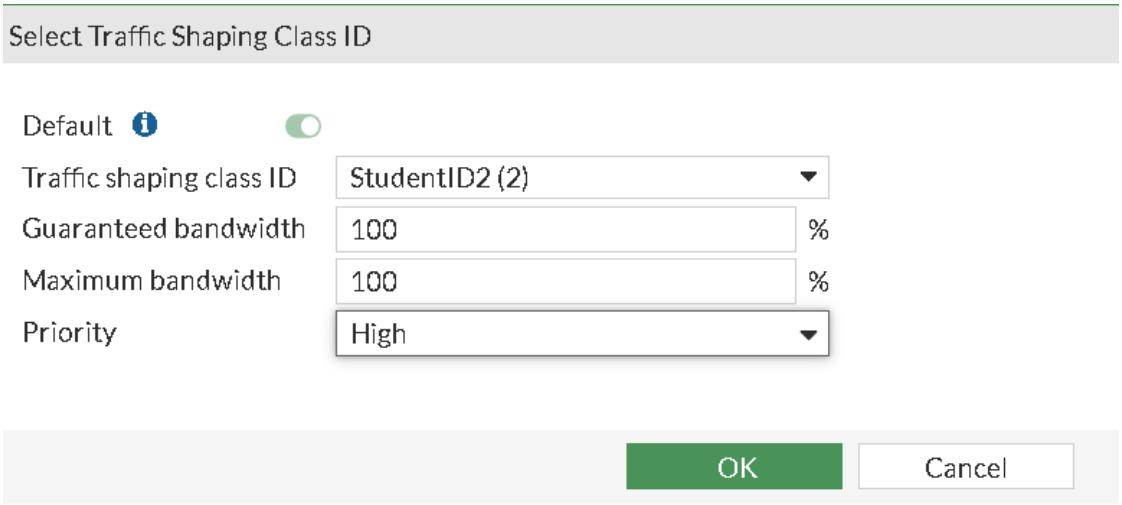
Make an address group so that all the mac address of the devices are in one group



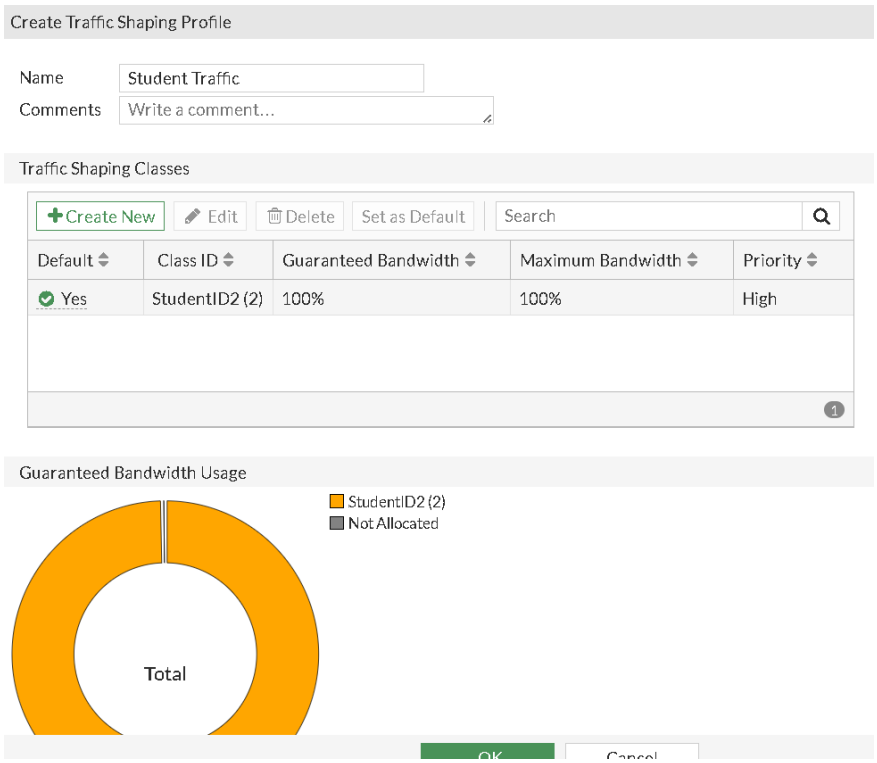
Pick the MAC address group name in the source section.



Traffic Shaping



Make a Traffic Shaping Class ID that allows Students to get 100% guaranteed of the bandwidth



Apply the Traffic Shaping Profile to a specific VLAN (Students VLAN)

This ensures bandwidth availability when it is needed. It is not always guaranteed that there are 500 students everyday in the campus or all students are using the network. With this, students who are connected can use more than their usual bandwidth allocation. There are 510 students in City College of San Fernando, and they are each guaranteed 2mbps and because there is no congestion then they can get a lot more bandwidth dynamically. It ensures fairness and no bandwidth unused while still maximizing the available capacity of the network.

Appendix X
Proof of Communications to CCSFP - Admin and Research Department

Submission of Documents and Publication Material

Submission of Documents for the Policy on Conduct of Research

Christian Allen Jimenez <caasjimenez@gmail.com>
to ccsfpresearchextensionoffice

Wed, Feb 5, 12:23 PM (12 days ago)

To whom it may concern,

I hope you're doing well.

Please find attached the documents regarding the Policy on Conduct of Research for the City College of San Fernando Pampanga.

Should you need any further clarification or additional information, feel free to reach out. I look forward to your feedback and to working together on finalizing the policy.

Additionally, here is the consent form attached to the survey we made:
https://forms.gle/WFDH4RBgP8WHFgHs9

Thank you for your attention to this matter.

Sincerely,
Christian Allen S. Jimenez
Holy Angel University

4 Attachments • Scanned by Gmail



CCSFPResearchExtensionOffice
to me

2:01 PM (4 hours ago)

Hello. Sorry for the late reply.

I have already sent to the deans your pubmat.

Good luck sa study ninyo.

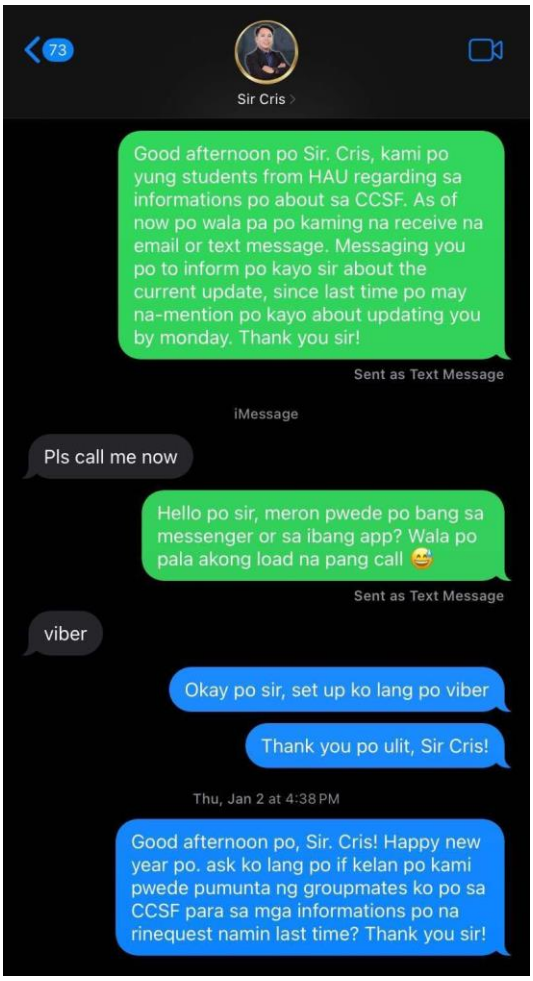
--
Director, Research and Extension Services Office
City College of San Fernando Pampanga

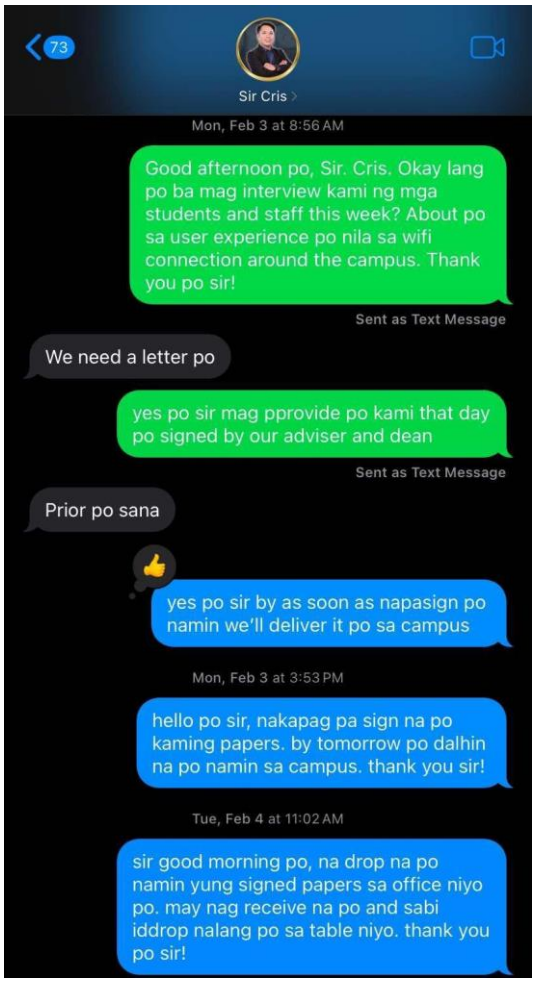
Christian Allen Jimenez <caasjimenez@gmail.com>
to CCSFPResearchExtensionOffice

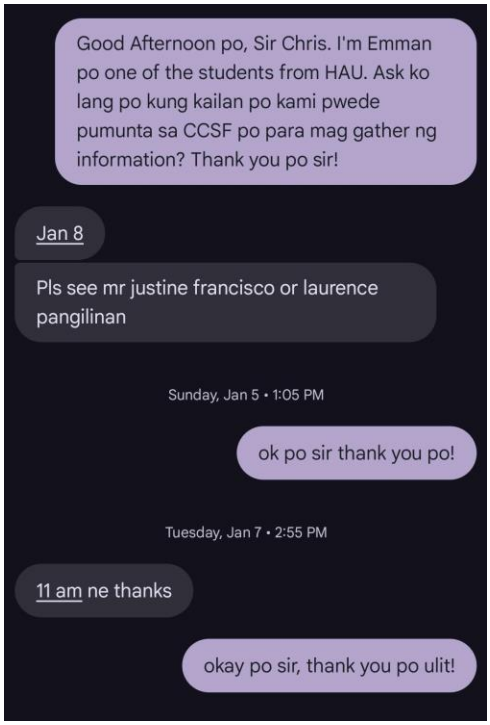
6:02 PM (56 minutes ago)

Good evening po, thank you so much po for accepting our survey request and for the goodluck!

Reply Forward

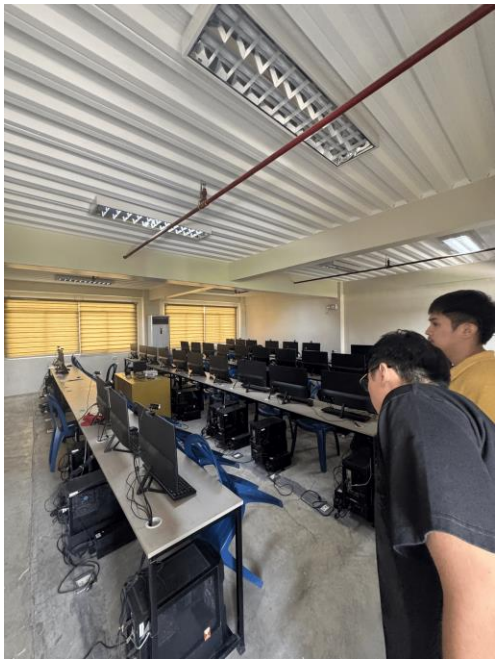

73
Sir Cris
Good afternoon po Sir. Cris, kami po yung students from HAU regarding sa informations po about sa CCSF. As of now po wala pa po kaming na receive na email or text message. Messaging you po to inform po kayo sir about the current update, since last time po may na-mention po kayo about updating you by monday. Thank you sir!
Sent as Text Message
iMessage
Pls call me now
Hello po sir, meron pwede po bang sa messenger or sa ibang app? Wala po pala akong load na pang call
Sent as Text Message
viber
Okay po sir, set up ko lang po viber
Thank you po ulit, Sir Cris!
Thu, Jan 2 at 4:38 PM
Good afternoon po, Sir. Cris! Happy new year po. ask ko lang po if kelan po kami pwede pumunta ng groupmates ko po sa CCSF para sa mga informations po na rinequest namin last time? Thank you sir!

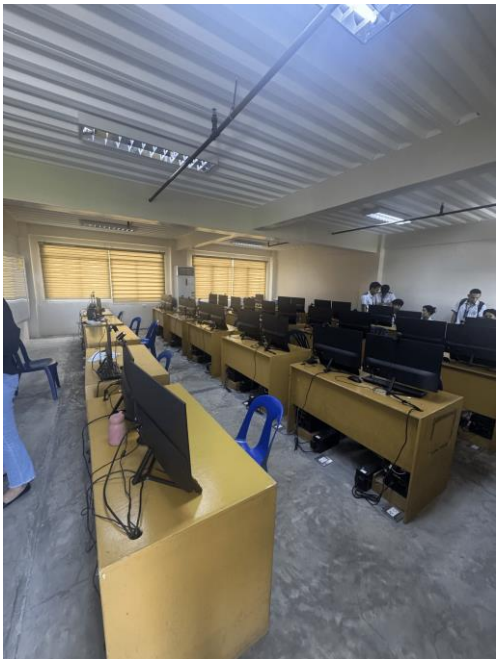

73
Sir Cris
Mon, Feb 3 at 8:56 AM
Good afternoon po, Sir. Cris. Okay lang po ba mag interview kami ng mga students and staff this week? About po sa user experience po nila sa wifi connection around the campus. Thank you po sir!
Sent as Text Message
We need a letter po
yes po sir mag pprovide po kami that day po signed by our adviser and dean
Sent as Text Message
Prior po sana
yes po sir by as soon as napasign po namin we'll deliver it po sa campus
Mon, Feb 3 at 3:53 PM
hello po sir, nakapag pa sign na po kaming papers. by tomorrow po dalhin na po namin sa campus. thank you sir!
Tue, Feb 4 at 11:02 AM
sir good morning po, na drop na po namin yung signed papers sa office niyo po. may nag receive na po and sabi iddrop nalang po sa table niyo. thank you po sir!


Good Afternoon po, Sir Chris. I'm Emman po one of the students from HAU. Ask ko lang po kung kailan po kami pwede pumunta sa CCSF po para mag gather ng information? Thank you po sir!
Jan 8
Pls see mr justine francisco or laurence pangilinan
Sunday, Jan 5 • 1:05 PM
ok po sir thank you po!
Tuesday, Jan 7 • 2:55 PM
11 am ne thanks
okay po sir, thank you po ulit!

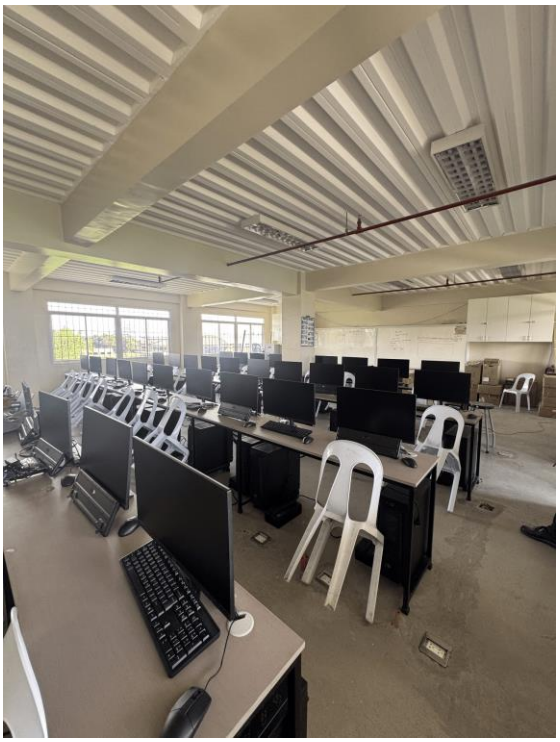
Appendix Y
Documentation for Site Observation

Interview with Sir Lawrence Pangilinan (Computer Laboratory Custodian)





HOLY ANGEL UNIVERSITY



Appendix Z
Device Cost List

Quantity	*Device Name*	*Device Picture*	*Specifications*	Unit Cost	Total Price
8	*Ubiquiti Unifi U6 Long Range*		• *WiFi 6* • *Ø220 x 48 mm (Ø8.7 x 1.9")* • *Coverage Area 185m² (2,000 ft²)* • *Max. Client Count - 350+* • *Mounting Locations - Ceiling, Wall* • *Weatherproofing - IP54* • *Power Method - PoE +* • *Wireless Meshing* • *Band Steering* • *802.11v BSS Transition Management* • *802.11r Fast Roaming* • *802.11k Radio Resource Management (RRM)* • *Captive Hotspot Portal* • *WiFi Schedules* • *Client Device Isolation* • *WiFi Speed Limiting* • *Private Pre-Shared Key (PPSK)*	₱9,864.29	₱78,914.32
2	*Ubiquiti Switch Standard 24*		• *Available connections: 24 Gigabit Ethernet Ports* • *Port Layout: 1GbE RJ45: 24 1G SFP: 2* • *Switching Capacity: 52*	₱13,198.50	₱26,397

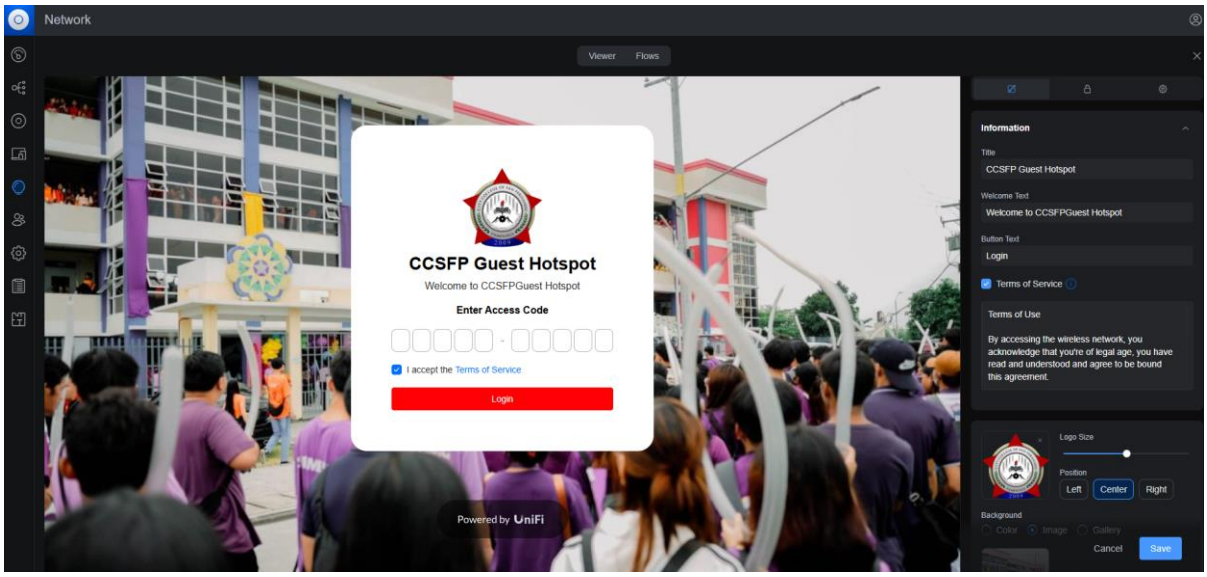
			Gbps • *Supported VLANs: 1,000* • *MAC Address Table Size: 8,000* • *Layer 2 and Layer 3 Features*		
4	*Ubiquiti Switch Lite 16 PoE*		• *Port Layout: 1GbE RJ45 16 (8 PoE+)* • *1G SFP (2 ports)* • *Total PoE Availability: 45W* • *Switching Capacity: 32 Gbps* • *Layer 2 and Layer 3 Features* • *Advanced IGMP Configuration (Querier, Fast Leave, Router Port)* • *Ambient Operating Temperature: -5 to 40° C (23 to 104° F)*	₱11,673.34	₱46,693.36
4	*Ubiquiti Switch Standard 48*		• *Port Layout: 1 GbE RJ45: 48 ports 16 (8 PoE+) 1G SFP: 4 ports* • *Total PoE Availability: 45W* • *Switching Capacity: 104 Gbps* • *Layer 2 and Layer 3 Features* • *Heat Dissipation (Excluding PoE*	₱24,343.90	₱97375.6

			Output): 136.48 BTU/hr • *Max. Power Consumption: 40W* • *Ambient Operating Temperature: -15 to 40° C (5 to 104° F)*		
1	*Ubiquiti Pro Max 48 PoE (USW-Pro-Max-48-POE)*		• *16x 2.5 Gb/s Ethernet ports with support for PoE+/++ (IEEE 802.3at and 802.3bt)* • *32x 1 Gb/s Ethernet ports (8x 802.3bt and 24x 802.3at)* • *4x 10 Gb/s SFP+* • *720W of power for PoE ports* • *LCM Display 1.3" Touchscreen* • *Etherlighting technology enabling visual verification of the port status and configuration*	₱67,138.94	₱67,138.94
1	*FortiGate-100F Firewall Appliance Plus 1 Year FortiCare Premium and FortiGuard Unified Threat Protection (UTP) (FG-100F-BDL-950-12)*		• *Includes: 1-Year FortiCare Premium & FortiGuard Unified Threat Protection (UTP)* • *Supports: 3 ISP Load Balancing, 500-1000 Users, Secure SD-*	₱255,869	₱255,869

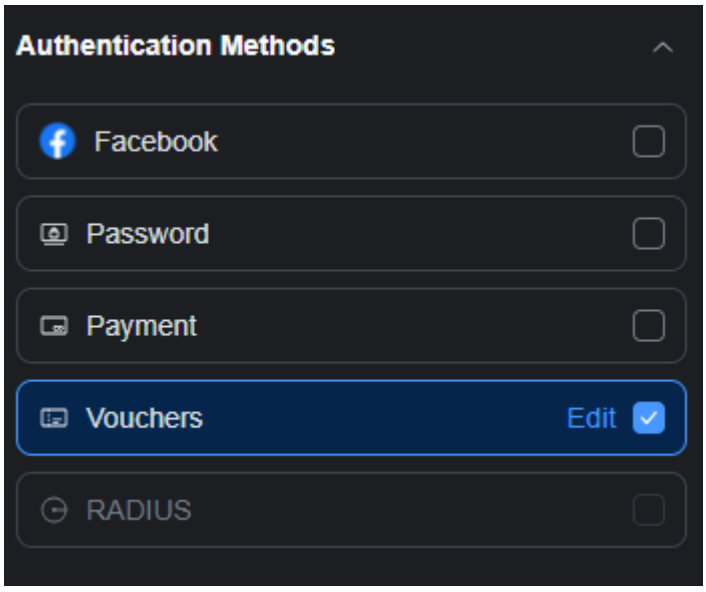
			WAN • *Security Features: IPS, Web Filtering, Antivirus, Application Control*		
1	*Cable UTP Cat6 Skylink*		• *Transmission rate: 1000mbps* • *Transmission bandwidth: 600MHZ Gold-plated RJ45*	₱10 per meter 300m	₱3,000
5	*RJ45 CAT6e*		• *RJ45 plugs for unshielded twisted pair solid or stranded cable, supports 24 to 26 AWG round or flat network cable* • *Gold-plated contacts provide reliable performance for a Gigabit Ethernet-rated network*	₱215.00	₱1,075
1	*PLDT's Fiber Plus Plan*	PLDT	• *Unlimited data with speed that reaches up to 1Gbps. It is a high- speed internet package that includes a mesh Wi-Fi System.*	₱9,499	₱113,988 (1 Year Subscription)
				Total Cost:	₱690,451

The school gets an estimated ₱275K to ₱300K from the government, but it has a flexible budget if the devices present scalability for future considerations. The total cost is ₱690,451, as selection placement prioritizes long-term performance, security, and scalability to serve a large number of users efficiently. This amount runs above normal allocation. However, it decreases future upgrade costs and ensures a stable and higher-performing network infrastructure leading to less cost in the future. Adjustments can be made if necessary, but it is advisable to raise the budget so that the institution's growing network requirements can be fully accommodated.

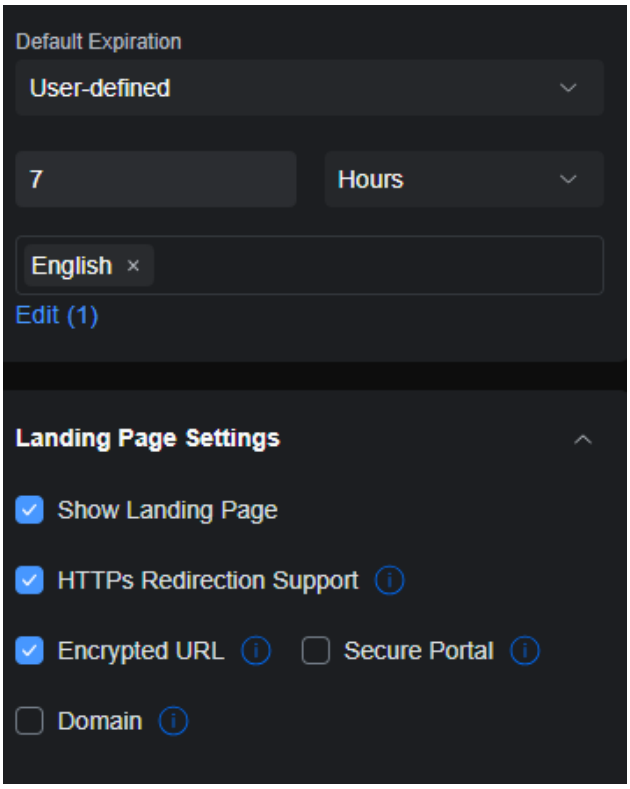
Appendix AA
Captive Portal Design and Specifications - UniFi Network



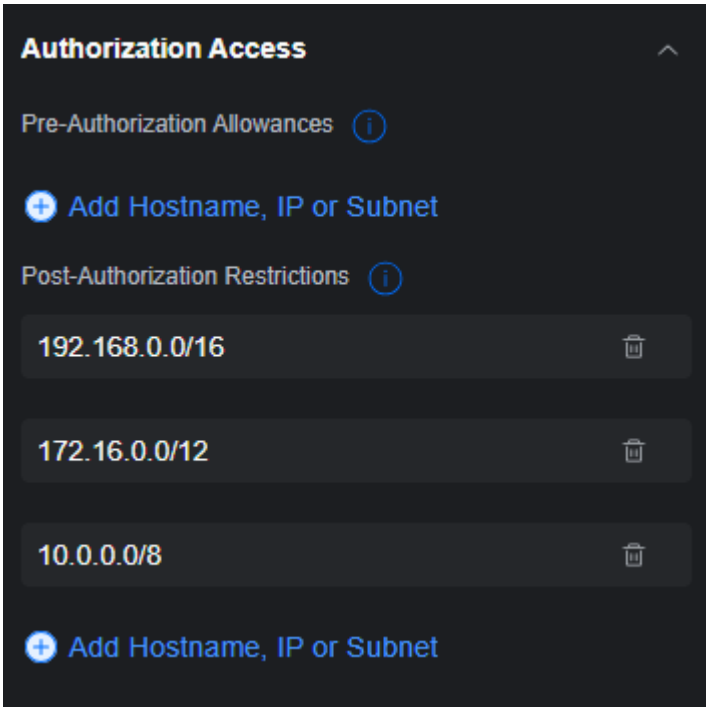
Main design of the captive portal



Authentication Methods settings



Settings of the duration of the voucher



Authorization Access settings

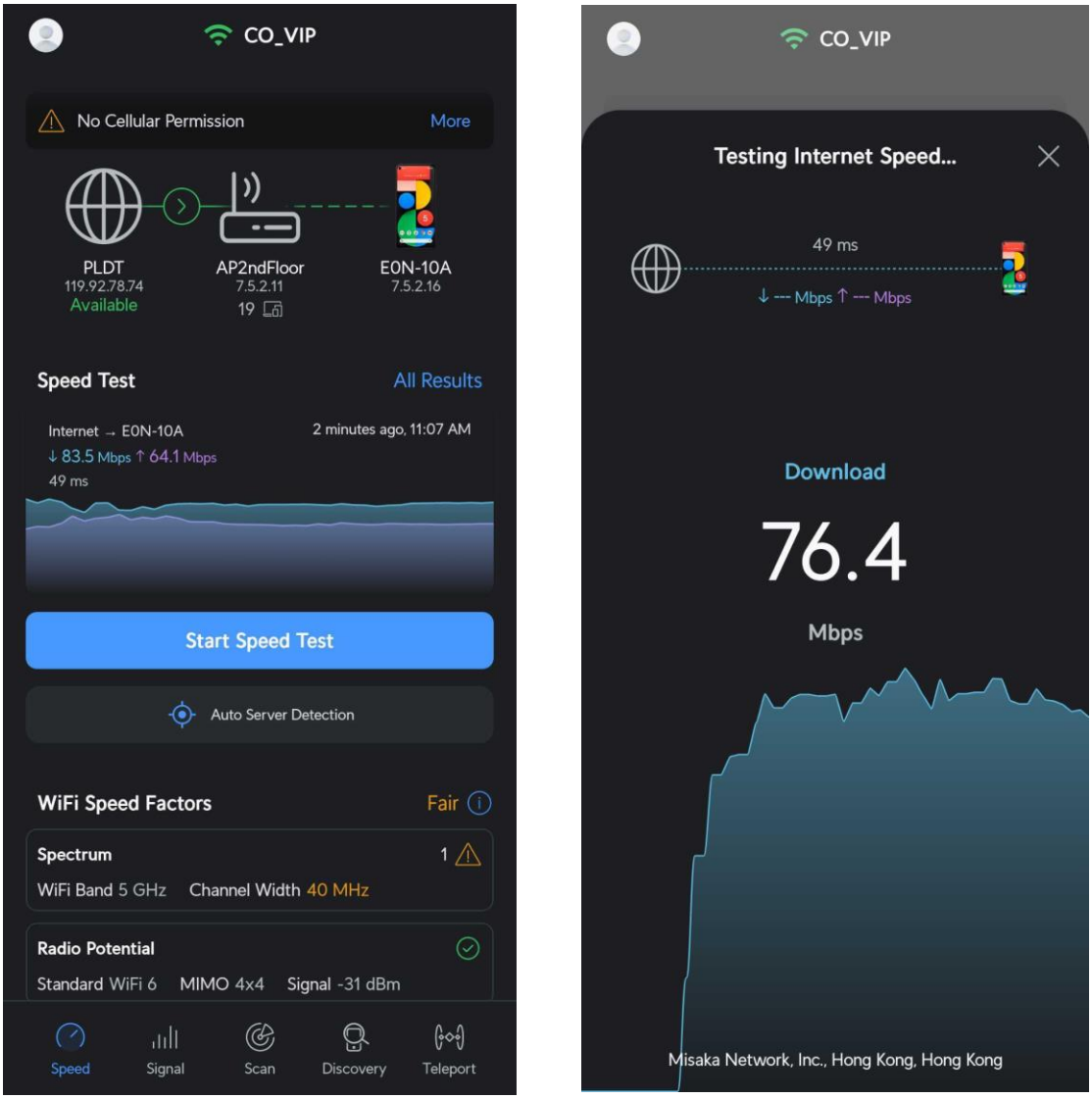
Ubiquiti was selected to implement the captive portal with its centralized management, seamless Wi-Fi integration, high scalability, and user-friendly interface. The UniFi Controller allows simple configuration and monitoring of the captive portal, thereby simplifying network access management in the institution. The other point of Ubiquiti's UniFi over Fortinet's FortiGate is centralized and simplified network management. The UniFi Network Controller provides a single interface to the administrator for configuring, monitoring, and optimizing all devices connected into that network, including access points, switches, and routers. The unified interface adds to operational efficiency because complexity-to-manage multiple-networking-components is reduced. In Fortinet's case, a manual approach is required as regards the configuration of VLANs, firewall policies, web filtering, and MAC-based authentication. All these processes tend just to build up the workload and complexity to the administrator side.

One of the major benefits of Ubiquiti's UniFi over Fortinet's FortiGate is enabling centralized and simplified network management. The UniFi Network Controller possesses a single interface that allows the administrator to configure, monitor and optimize all the connected devices between access points, switches, and routers. The last big aspect is scalability. It is easy to scale out a Ubiquiti network, which is what makes it ideal for education since needs might change over time. Fast deployment and maintenance are assured as well, which would be a flexible yet effective solution for a captive portal. Moreover, UniFi Access Points are natively compatible with the Ubiquiti system and operate excellently in terms of authentication and access control, without requiring much configuration. This allows for an uncomplicated user management scheme while maximizing network stability and performance.

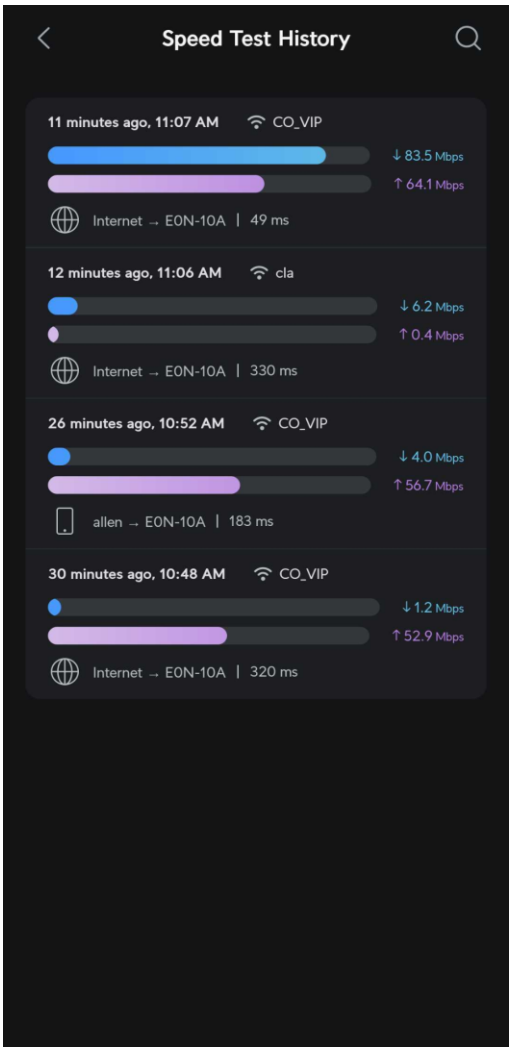
Appendix AB
Research Instrument: WiFiman

Ubiquiti developed WiFiman, a network analysis tool to diagnose the performance and connectivity of Wi-Fi. It has the availability of discovery and subnet scanning, speed tests, and channel optimization. WiFiman is useful for personal or enterprise networks and provides insights into real-time network conditions and interference source performance according to Ubiquiti Inc. These benefits make the application a major tool for network administrators to improve coverage in maximum deployments while minimizing signal degradation.

In the Speed tab, you can run speed tests for your WiFi or cellular data connection. The test results show you your upload and download speeds to allow you to evaluate your network performance. When connected to a network managed by a UniFi Cloud Gateway, the app provides you with information like signal strength and channel width that will help to optimize wireless speeds, thus improving your browser. In this section, records and lists of earlier successfully passed tests are placed, along with the mobile device's public and private IP addresses if it is connected through a wireless network. Users may choose their test server for even more personalized details. In addition, the speed test feature displays the peak download and upload speeds, the strength of the current Wi-Fi signal in dBm, PHY mode, and the PHY speed of the current Wi-Fi connection.



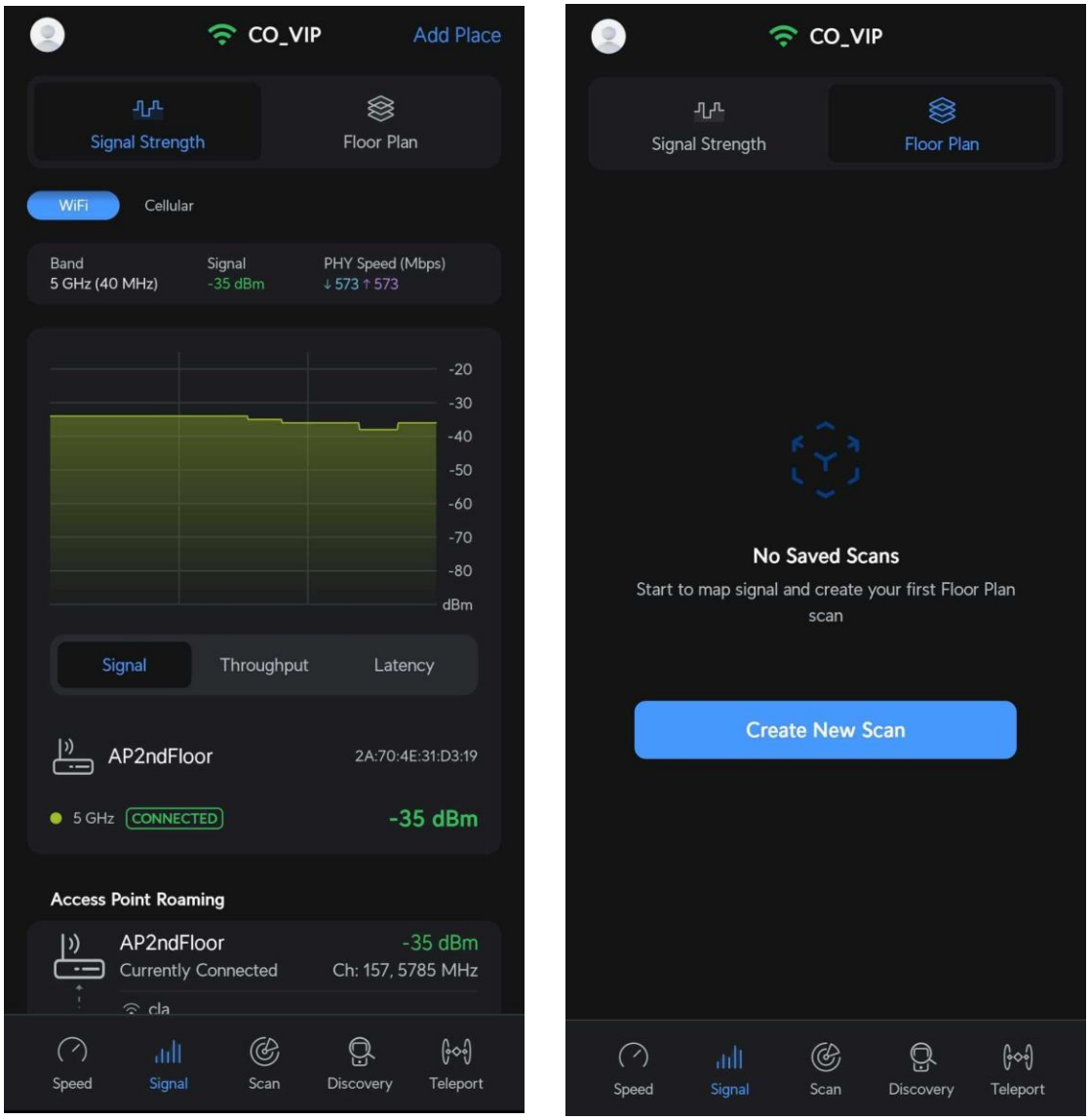
WiFiman Speed Tab



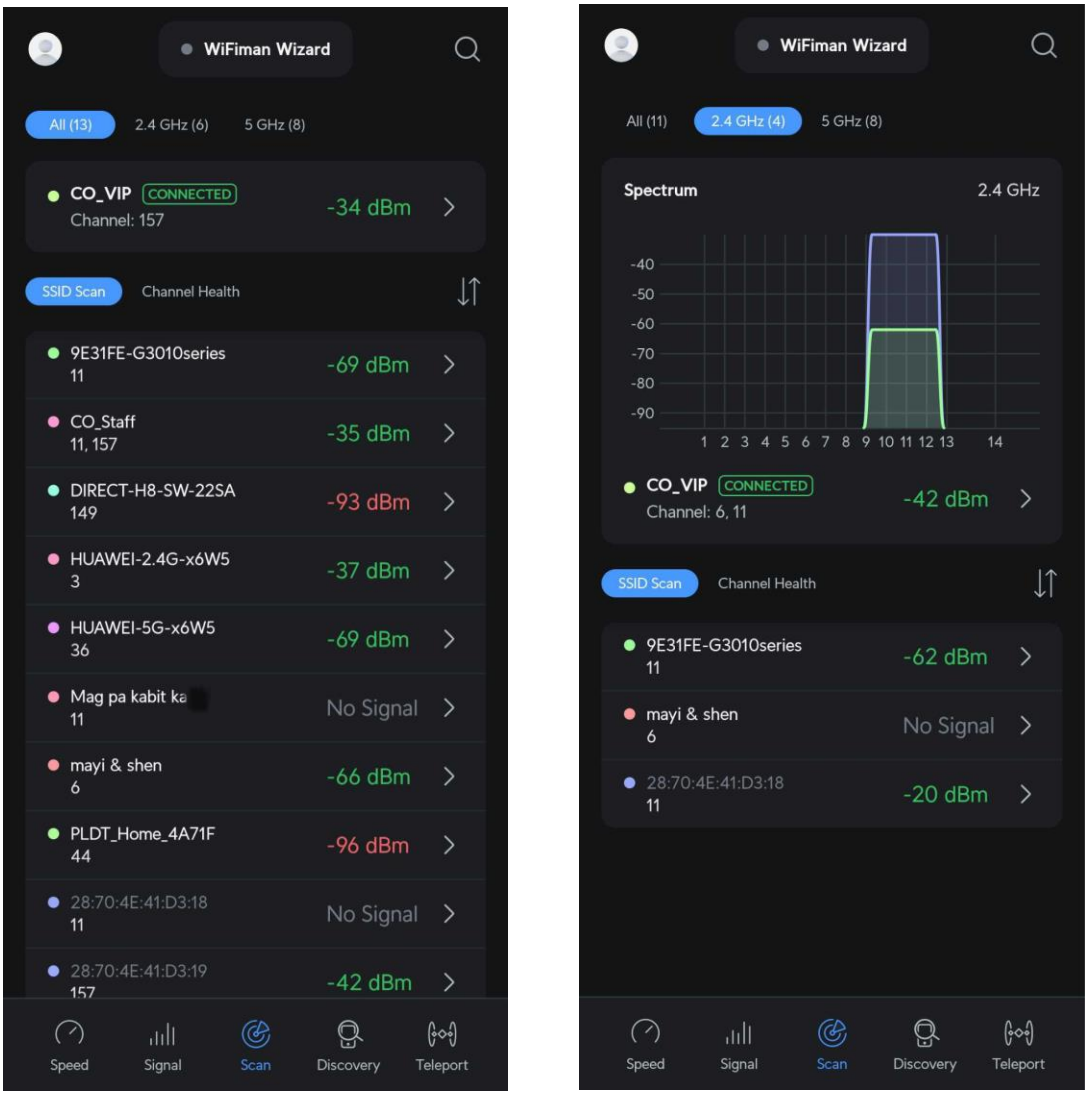
WiFiman Speed Test History Tab

The Signal tab within the WiFiman Mobile App allows you to monitor real-time essential network parameters, such as signal strength, throughput, latency, and roaming between multiple APs. By moving around your space, you can track all these metrics in order to get a reliable and consistent network connection. This section also displays basic information about the mobile device and its current association with a wireless network. Both the WiFi connection and cellular signal strengths are updated every ten (10) seconds to give

users an in-depth, real-time report of their network performance. In addition, the 'Floorplan Mapper' feature, offered by LiDAR-enabled mobile devices, provides you with a possibility to note signal strength within different areas; thus, visualizing your WiFi coverage and, accordingly, analyzing roaming patterns for your devices among access points.



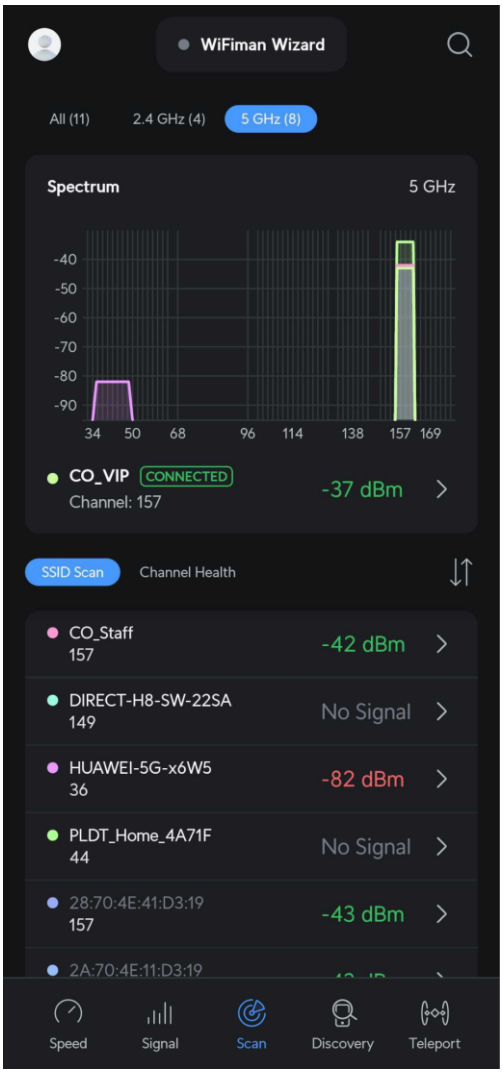
WiFiman Scan Tab

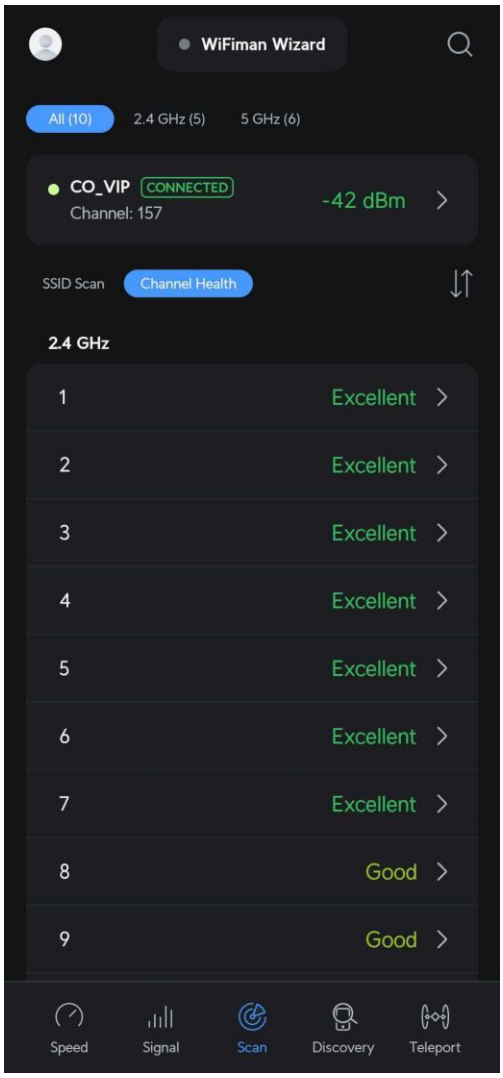


WiFiman Scan Tab

The Scan tab within the WiFiman app shows all the available Wi-Fi networks, including their SSID, signal strength (dBm), channel, and frequency band (2.4 GHz or 5 GHz). It shows the connected network and offers a Channel Health analysis to assist in deciding on congestion. The networks may be sorted or filtered by signal strength and other parameters. The tab is

helpful in resolving Wi-Fi performance, choosing the optimal channels, and optimizing network settings.

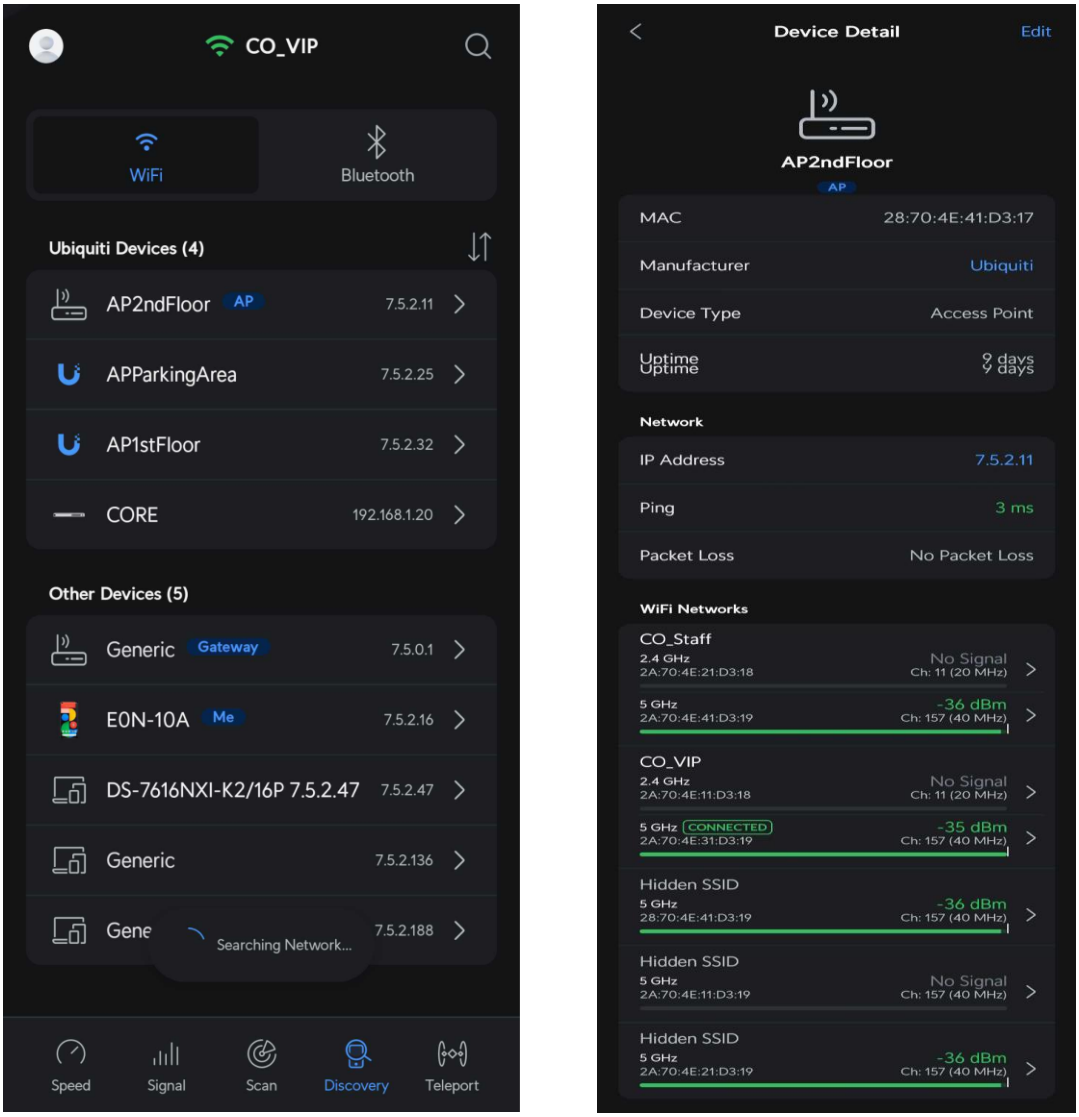




WiFiman Scan Tab

From the Discovery tab, you can diagnose network problems by viewing IP addresses and other identifying details for devices connected to your WiFi network from the app, provided that useful assistance is given to diagnose device adoption problems quickly and easily. The Discovery section lists all devices on the same network as your mobile device, which are

shown in a hostname and single IP address entry. Tapping on a device provides basic information and an option to initiate port scanning.



WiFiman Discovery Tab

HOLY ANGEL UNIVERSITY

Appendix AC
IT Expert's Curriculum Vitae

Banal, Jayson Paul L.

Address: 193 Manibaug Libutad Porac, Pampanga
Contact Number: 09613351365
Email Address:banal1618@gmail.com
Birthdate: July 18, 1998

WORK EXPERIENCE

Technical Support (January 2015 to 2021)
AVZ Enterprise
Aguas sub. Manibaug Libutad Porac Pampanga

Tool Keeper (November 2014 to 2015)
Noel Zapanta Ironworks
Aguas sub. Manibaug Libutad Porac Pampanga

Network Engineer (NOC) (December 2021 to Present) Clark Outsourcing
Building 35 Philexcel Business Park, Clark Freeport, Mabalacat, 2023 Pampanga

TECHNICAL SKILLS

- Skilled in Software Troubleshooting particularly Windows Operating system and Hardware Troubleshooting on a PC
- Basic skills in Photoshop
- Proficient in Microsoft Office programs (MS Word, Excel, PowerPoint)
- Basic Networking
- Cctv Installation
- Basic Network troubleshooting
- Basic knowledge in Fortigate firewall
- Installation Unifi Controller

PERSONAL SKILLS

- Highly Organized and efficient
- Ability to work independently or as a team
- Ability to handle stress and multitask
- Capable of learning new skills in a short span of time

EDUCATIONAL BACKGROUND

Bachelor of Science in Information Technology (2015 – 2019)
Systems Plus College Foundation
Balibago, Angeles City

REFERENCES

Catherine Rodrigueza
AR Supervisor
09097032210

Arnel David
Operation Engineer (NOC)
09273132738

Appendix AD
Editor's Note

HOLY ANGEL UNIVERSITY SCHOOL OF COMPUTING

DR. MARLON I. TAYAG
Dean

This is to certify that the document of the capstone entitled **Optimizing Wi-Fi Coverage and Network Efficiency at City College of San Fernando, Pampanga"** authored by the following proponents:

Bondoc, Michael Owen G.
Jimenez, Christian Allen S.
Reyes, John Clarence G.
Tulabut, Emmanuel Greyco B.

has been checked for grammatical and typographical errors.

Yours truly,

Maria Cristina C. Nogoy, LPT, MAEd
Faculty, Comm and Languages Department

March 26, 2025

HOLY ANGEL UNIVERSITY

Appendix AE
University Plagiarism Certificate

HOLY ANGEL UNIVERSITY **UNIVERSITY RESEARCH OFFICE**

CERTIFICATION

This certifies that the research paper entitled "**Optimizing Wi-Fi Coverage and Network Efficiency at City College of San Fernando, Pampanga"** by John Clarence G. Reyes, Michael Owen G. Bondoc, Christian Allen S. Jimenez, and Emmanuel Greyco B. Tulabut, is essentially clear of plagiarism, as subjected to Turnitin review. Scanned and reviewed by the University Research Office on March 27, 2025 with the following details:

Total number of words	11917
Final rate	8%

Certified by:

DR. RICHARD L. FIGUEROA
Director, University Research Office

#1 Holy Angel Avenue, Sto. Rosario, Angeles City, Philippines 2009
Tel. Nos.: (045) 888-8691; 888-2902; 887-5748; 887-2455; 624-5277; 625-9619 | Fax: (045) 888-1754; 888-2514
Email: hau@hau.edu.ph | www.hau.edu.ph

HOLY ANGEL UNIVERSITY

Appendix AF
Researcher's Curriculum Vitae

John Clarence Garcia Reyes

johnclarencereyes.jobs180.com

OBJECTIVE

To apply expertise in network infrastructure, cybersecurity, software engineering, and web design to develop secure, efficient, and user-friendly IT solutions.

PERSONAL INFORMATION

Birthdate: August 12, 2002
Civil Status: Single
Nationality: Filipino
Address: Pampanga, Central Luzon (Region III)
Gender: Male

CONTACT INFORMATION

Mobile: 09993370679
Email: jcreyespakzreyes@gmail.com

SKILLS

- **Cybersecurity**
- **Accounting**
- **Responsive Web Design**
- **Programming**
- **Computer Literacy**
- **Network Administration**

LANGUAGES

- **English**
- **Filipino**

ACHIEVEMENTS

Deans Lister (First Year College, First Semester, 2021-2022)

Deans Lister (First Year College, Second Semester, 2021-2022)

Deans Lister (Second Year College, First Semester, 2022-2023)

Deans Lister (Second Year College, Second Semester, 2022-2023)

Deans Lister (Third Year College, First Semester, 2023-2024)

Deans Lister (Third Year College, Second Semester, 2023-2024)

WORK EXPERIENCE

Clark Outsourcing

(2025 Jan to 2025 Apr)

Position:	ISD Intern Trainee
Specialization:	Technical and Helpdesk Support
Industry:	Computer / Information Technology (Hardware)

EDUCATION

2025 Apr — **Bachelor's/College Degree**
Holy Angel University (HAU)
Major: Network Administration
Field of Study: Computer Science/Information Technology

2021 Apr — **Senior High School Diploma**
University Of The Assumption
Major: ABM
Field of Study: Academic Track: Accountancy, Business & Management (ABM)

CERTIFICATIONS

2024 **Network Security**

2024 **Introduction To Figma**

2024 **Blockchain Conference**

2024 **DevNet Associate**

2023 **CyberOps Associate**

2023 **CCNAv7 Introduction To Networks**

2021 **Introduction To Cybersecurity**

2024 **JavaScript Essentials 1**

2024 **Responsive Web Design**

2024 **CCNA Enterprise Networking, Security, And Automation**

2024 **CCNA Switching, Routing, And Wireless Essentials**

2023 **Linux Skills Level 1**

2022 **Red Hat System Administration I (RH124)**

SEMINARS

2025 **3rd Regional Cybersecurity Conference**

2024 **1st Regional Blockchain Conference**

2025 **Cyber Resilience In The AI Era Empowering Business Leaders And Developing Next-Gen Cybersecurity Pro**

View more of my ResumèLink at http://johnclarencereyes.jobs180.com

HOLY ANGEL UNIVERSITY

Christian Allen Sicat Jimenez

caasjimenez.jobs180.com

PERSONAL INFORMATION

Birthdate: December 10, 2000
Civil Status: Single
Nationality: Filipino
Address: 16 Trinity Triangle, Villa Angela. Santo Domingo. Angeles City. Pampanga. Pampanga, Central Luzon (Region III) 2009
Gender: Male

CONTACT INFORMATION

Mobile: 09661676996
Email: caasjimenez@gmail.com

SKILLS

- **Microsoft 365 Applications**
- **Cisco Packet Tracer**
- **Customer Service**
- **Computer Software And Hardware Servicing**

LANGUAGES

- **English**
- **Filipino**

ACHIEVEMENTS

With Honors Grade 11 (STEM) 2017 - 2018
Graduated SHS With Honors (April 2018)
Dean's Lister (1st Semester 2019-2020)
Dean's Lister (1st Semester 2022-2023)
Dean's Lister (2nd Semester 2023-2024)

WORK EXPERIENCE

Clark Outsourcing

(2024 Dec to 2025 Mar)

Position: Intern
Trainee
Specialization: IT/Computer - Hardware
Industry: Computer / Information Technology (Hardware)
Nature of Work: Troubleshot hardware, software, and network issues.
Provided technical support and system configurations.
Installed and maintained software and hardware.

Pour Decisions

(2023 Apr to 2025 Feb)

Position: Staff
Fresh Grad / Entry Level
Specialization: Food/Beverage/Restaurant Service
Industry: Food and Beverage
Nature of Work: Prepared and served beverages.
Provided customer service and handled payments.
Maintained inventory and workstation cleanliness.

Uhealth Beauty Plus Incorporation

(2020 Jul to 2022 Jun)

Position: Operations Staff
Junior Associate (1-4 yrs experience)
Specialization: Manufacturing/Production Operations
Industry: Consumer Products / FMCG
Nature of Work: Handled shipping, labeling, and restocking.
Managed inventory, order processing, and supply management.
Ensured workflow efficiency and compliance.

EDUCATION

2025 Apr **Bachelor's/College Degree**
Holy Angel University (HAU)
Major: Network Administration
Field of Study: Computer Science/Information Technology

2018 Apr **Senior High School Diploma**
Chevalier School
Major: STEM
Field of Study: Academic Track: Science, Technology, Engineering and Mathematics (STEM)

CERTIFICATIONS

2024
Cisco Network Security

2024
CCNA Enterprise Networking, Security And Automation

2024
JavaScript Essentials 1

2024
Cisco DevNet Associate

2024
CCNA Switching, Routing And Wireless Essentials

2023
Cisco CyberOps Associate

2023
CCNA Introduction To Networks

SEMINARS

2025
3rd Regional Cybersecurity Conference "Cybersecurity In The Age Of AI Navigating The Double Edged-sw

2024
1st Regional Blockchain Conference

REFERENCES

Kim Joshua Dela Cruz
Manager
Manager
Pour Decisions
09064689834
kimjdc06@gmail.com

Rachael Mae Corpin
Workmate
Operations Head
Uhealth Beauty Plus Inc.
09533554229
rachael_corpin@yahoo.com

HOLY ANGEL UNIVERSITY

Emmanuel Greyco Bacani Tulabut

emmanuelgreycotulabut.jobs180.com

PERSONAL INFORMATION

Birthdate: April 20, 2003
Civil Status: Single
Nationality: Filipino
Address: #1285 Diamond Street, Ramar Village, City of San Fernando, Pampanga Pampanga, Central Luzon (Region III) 2000
Gender: Male

CONTACT INFORMATION

Mobile: 09514212704
Email: emmanuelgreycotulabut@gmail.com

SKILLS

- **Network Management**
- **Network Troubleshooting**
- **Network Configuration**
- **Network Designing**
- **Basic Programming**

LANGUAGES

- **English**
- **Tagalog**
- **Kapampangan**

ACHIEVEMENTS

Grade 9 With Honors
Grade 10 With Honors
Grade 11 STEM With Honors
Grade 12 STEM With Honors
1st Year College President's Lister 1st Semester
2nd Year College Dean's Lister 1st And 2nd Semester
3rd Year College Dean's Lister 1st And 2nd Semester

WORK EXPERIENCE

Clark Outsourcing

(2024 Dec to 2025 Mar)

Position: Tech Support Intern
Trainee
Specialization: Technical and Helpdesk Support
Industry: Computer / Information Technology (Hardware)

EDUCATION

2025 Apr **Bachelor's/College Degree**
Holy Angel University (HAU)
Major: Network Administration
Field of Study: Computer Science/Information Technology

2021 Apr **Senior High School Diploma**
Chevalier School
Major: STEM
Field of Study: Academic Track: Science, Technology, Engineering and Mathematics (STEM)

2019 Mar **High School Diploma**
Chevalier School
Field of Study:

CERTIFICATIONS

2024
CCNAv7 Switching, Routing, And Wireless Essentials

2024
DevNet Associate

2024
JavaScript Essentials 1

2024
Responsive Web Design

2024
Introduction To Figma

2023
CCNAv7 Introduction To Networks

2023
CyberOps Associate

2022
Red Hat Certified System Administration

2021
Introduction To Cybersecurity

SEMINARS

2025
3rd Regional Cybersecurity Conference

2025
Cyber Resilience In The AI Era Empowering Business Leaders And Developing Next-Gen Cybersecurity Pro

2024
1st Regional Blockchain Conference

View more of my ResumèLink at http://emmanuelgreycotulabut.jobs180.com

HOLY ANGEL UNIVERSITY

Michael Owen Guyguyan Bondoc

michaelowenbondoc.jobs180.com

OBJECTIVE

A true leader with a good attitude helps a team to be successful. Seeking an opportunity to leverage as an IT assistant, utilizing great skills to achieve the company's goal.

PERSONAL INFORMATION

Birthdate: June 28, 2002

Civil Status: Single

Nationality: Filipino

Address: Block 49 Lot 19 Nha Pandacaqui Mexico Pampanga, Central Luzon (Region III) 2021

Gender: Male

CONTACT INFORMATION

Mobile: 09350555753

Email: michaelowenbondoc@gmail.com

SKILLS

- **Positive Attitude**
- **Active Listener**
- **Adaptability**
- **Persistent**
- **Ability To Work Independently Or To Work With A Team**
- **Time Management**

LANGUAGES

- **Filipino**
- **English**
- **Kapampangan**

EDUCATION

2020 Apr — **Senior High School Diploma**
Holy Angel University
Major: STEM
Field of Study: Academic Track: Science, Technology, Engineering and Mathematics (STEM)

2018 Apr — **High School Diploma**
Holy Angel University
Field of Study:

CERTIFICATIONS

2024
RESPONSIVE WEB DESIGN

2024
DEVNET ASSOCIATE

2024
SWITCHING, ROUTING, AND WIRELESS ESSENTIALS

2024
ENTERPRISE NETWORKING, SECURITY, AND AUTOMATION

2023
CYBEROPS ASSOCIATE

2023
INTRODUCTION TO NETWORKS

View more of my ResumèLink at http://michaelowenbondoc.jobs180.com