HOLY ANGEL UNIVERSITY

Simulation of a Network Infrastructure Design for Amsic Integrated School

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

Baluyut, Kahlel Inigo I.
Bautista, Sean Matthew C.
Delos Reyes, Carl Louie G.
Delos Reyes, Joseph R.

March 2025

HOLY ANGEL UNIVERSITY

APPROVAL SHEET

This capstone entitled **"SIMULATION OF A NETWORK INFRASTRUCTURE DESIGN FOR AMSIC INTEGRATED SCHOOL"**, 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. Everly M. Chua
Adviser

ORAL EXAMINATION

Approved by the committee of oral examiners on
March 6, 2025

Mr. Wilson D. Concepcion
Panel Chair

Dr. Marlon I. Tayag
Panel Member

Ms. Ma Louella M. Salenga
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 would like to thank the Lord God Almighty for granting us the wisdom, strength, and perseverance necessary for the completion of this capstone project. His guidance has been the pillar of this project, making it easier to overcome challenges and achieve our goals.

Sincere thanks are extended to Dr. Everly M. Chua, whose expertise and professionalism as our adviser greatly contributed to the success of this research. Her valuable feedback and guidance were instrumental in enhancing the rigor and overall quality of the study.

We also express our heartfelt gratitude to Ms. Imelda Gozun, Principal of Amsic Integrated School, for granting us permission to conduct interviews and a site survey at the school. Her support was crucial in obtaining the necessary data for this research.

Gratitude is likewise extended to Holy Angel University for providing the intellectual climate and facilities that have facilitated the attainment of this study. The assistance and learnings derived from this university have been indispensable.

Finally, appreciation is given to all individuals who were involved in the research, such as faculty members, IT professionals, and other respondents who contributed priceless insights and inputs. Their assistance has been vital in identifying the findings of this study.

Laus Deo Semper!

Table of Contents

Page
Cover Page i
Approval Sheet ii
Acknowledgement iii
Table of Contents iv
List of Tables v
List of Figures v
Title Page 1
Executive Summary 2

Introduction 4
Review of Related Literature 6
Conceptual Framework 28
Objectives of the Study 29
Scope and Delimitation 30

Method 34
Requirement Analysis 35
Requirement Documentation 38
Design of Software, System, Product and/or Process 40
Development and Testing 43
Research Participants 44
Data Analysis 45
Research Instrument 46

Results 48

Discussion 68
Conclusion 72
Recommendations 74

References 76

Appendices

Appendix A Cover Letter
Appendix B Current Physical Network Layout
Appendix C Faculty Survey
Appendix D Initial Interview Guide Questions
Appendix E Amsic Integrated School's Organizational Chart

Appendix F Current Network Topology
Appendix G Proposed Logical Topology in EVE-NG
Appendix H Proposed Logical Topology in Packet Tracer
Appendix I Proposed Physical Network Layout
Appendix J Implementation Plan
Appendix K Cost Analysis for Simulation and Proposed Devices
Appendix L IP Addressing Scheme
Appendix M Firewall Configuration
Appendix N Fortigate Configuration
Appendix O Switch Configuration
Appendix P Converge and Comclark Speed Test
Appendix Q IT Expert's Curriculum Vitae
Appendix R Editor's Note
Appendix S University Plagiarism Certificate
Appendix T Researcher's Curriculum Vitae

List of Tables

Table 1 Number of faculty that bring their device(s) for work related purposes.
Table 2 Number of faculty that connect their device(s) to the school's network
Table 3 Faculty members' personal devices connected
Table 4 Faculty members' frequently used apps for school tasks
Table 5 The frequency of connectivity issues
Table 6 The level of satisfaction with the current network connection
Table 7 Matrix for Software used and its Features

List of Figures

Figure 1 Conceptual Framework
Figure 2 Iperf Stress Test
Figure 3 Run a basic throughput test
Figure 4 Ongoing test
Figure 5 Graph for VLAN 10 - VLAN 10 traffic
Figure 6 Graph of Core Switch 1 (VLAN 10 - VLAN 10)
Figure 7 Graph for VLAN 10 – VLAN 20 Traffic
Figure 8 Graph for Core Switch 1 (VLAN 10 - VLAN 20)
Figure 9 Graph for VLAN 10 – VLAN 30 Traffic
Figure 10 Graph for Core Switch 1 (VLAN 10 - VLAN 30)

Simulation of a Network Infrastructure Design for Amsic Integrated School

Kahlel Iñigo I. Baluyut, Sean Matthew C. Bautista,

Carl Louie G. Delos Reyes, and Joseph R. Delos Reyes

Holy Angel University

Executive Summary

The capstone project, “Simulation of a Network Infrastructure Design for Amsic Integrated School,” aims to develop a secure, scalable, and cost-efficient network infrastructure to support the institution’s growing technological demands. Amsic Integrated School, serving over 3,000 students, currently lacks a fully functional network, leading to connectivity challenges that affect both faculty and students. The project focuses on designing and simulating a structured network to enhance digital learning, administrative efficiency, and overall network reliability.

A site survey and consultations with key stakeholders, including Ms. Imelda Gozun (Principal), Mr. Richard Lois Pabustan (IT Officer), 55 faculty members from various departments, and network experts Mr. Florante Antonio Alfonso and Mr. Jan Henryck Dizon, provided valuable insights into the school's network challenges. The proposed network follows a collapsed core architecture, integrating both wired and wireless connectivity. A Fortinet firewall is implemented to enforce network security policies, ensuring data protection and access control.

To improve security and network performance, various network policies were introduced. The Access Control Policy employs Role-Based Access Control (RBAC) so that only VLAN 10 (administrators) can access Zabbix as well as the switches, protecting vital infrastructure. Only VLAN 10 can also ping other VLANs, and vice versa is blocked—an Isolation Policy against unwanted devices probing or accessing admin resources. A Web Content Filtering Policy denies access to YouTube and gaming sites to VLAN 30 (students), restricting access to non-educational and bandwidth-intensive sites. The Network Segmentation Policy prevents all VLANs from being configured or enforced at the firewall,

increasing traffic control and separation. Finally, Device Security Policies encompass switch passwords and password encryption, included in a Device Hardening Policy that prevents unauthorized access to Cisco switches.

The network design incorporates VLAN segmentation to optimize bandwidth usage and enhance security. The Main Distribution Frame (MDF) is placed in the secured computer laboratory, while Intermediate Distribution Frames (IDFs) are positioned in the Junior High School faculty room and the principal's office to ensure efficient network distribution. The infrastructure includes two (2) Pro Max 16 POE core switches, four (4) Lite 16 POE distributor switches, and four (4) U6+ access points, providing stable and widespread connectivity.

The network was simulated using EVE-NG, Packet Tracer, and Zabbix, allowing performance analysis, stress testing, and security validation before actual deployment. Surveys and network performance assessments confirmed the need for improved bandwidth allocation, better access point distribution, and optimized traffic management. The proposed network will address these concerns, ensuring enhanced internet accessibility, minimal downtime, and improved digital learning experiences for students and faculty.

This study provides a structured foundation for future network implementation at Amsic Integrated School. By integrating cost-efficient, high-performance networking solutions, the project ensures that the institution is equipped with a reliable, secure, and scalable infrastructure capable of supporting its long-term academic and administrative needs.

Simulation of a Network Infrastructure Design for Amsic Integrated School

Introduction

In today's digital world, a strong network infrastructure is especially vital for educational institutions as learning activities and administrative functions significantly rely on the safe and reliable availability of the Internet and other digital resources. Schools are gradually integrating ICT into their curricula to prepare their students for a high-tech workforce. Efficient school infrastructure directly influences students' performance since well-designed learning environments contribute positively to their achievements in school. Recent studies have shown that the quality of school infrastructure is closely linked to improved student learning outcomes, particularly in terms of engagement and academic performance (Shmis et al., 2021).

This capstone project aimed to simulate and design a cost-efficient network infrastructure without sacrificing reliability specifically tailored for Amsic Integrated School. The goal was to ensure secure, reliable, and efficient digital learning and operational workflows without compromising performance. The proposed network design included wired connections in the computer laboratories and wireless access for both faculty and students, prioritizing security, scalability, and accessibility. While maintaining a focus on cost efficiency, the project aimed to create a network that would meet the growing digital demands of the school and provides a reliable foundation for future developments.

Amsic Integrated School, located in Barangay Amsic of Angeles City, Pampanga, serves more than 3,000 students and is currently dealing with an inactive and poorly functioning network infrastructure. The existing network suffers from intermittent service, primarily due to its location, and relies on Converge ICT Solutions Inc. and Comclark for internet connectivity. While the internet service meets basic needs, it faces challenges related to bandwidth management and scalability to meet the school's increasing digital requirements. The school also lacks professional IT personnel and modern technologies, which means that digital resources are not available in most cases, administrative practices remain inefficient, and there are no digital learning tools. Most of the faculty members cannot connect to the school's network because the network is not yet fully operational, and the current network infrastructure is minimal and cannot support the connectivity requirements of the teaching staff. While the Department of Education (DepEd) acknowledges this and strongly promotes ICT improvement in public schools, rural and semi-urban settings like Amsic still face substantial barriers to such innovations.

This project addressed these challenges by proposing a new network design that combines cost efficiency with reliability. The network architecture focused on providing stable internet connectivity for both wired and wireless users, ensuring seamless access for students and faculty alike. Bandwidth management was integrated to ensure optimal performance across the school campus, and secure login sessions were implemented to protect student data and educational resources, adhering to the Data Privacy Act of 2012.

Cost efficiency in network infrastructure planning refers to strategic resource optimization to minimize costs without compromising the sustainability of the system. This involves deploying scalable and long-term solutions that lower operational costs, maintenance needs, and possible future upgrades without affecting critical functionalities. Reliability, in contrast, refers to the network's capability to sustain consistent and stable performance under different scenarios. A reliable network ensures minimal downtime, uninterrupted data transmission, and safe access to digital resources, all of which are important in sustaining the efficiency of institutional operations.

To achieve both cost efficiency and reliability, a network infrastructure architecture must be structured with a systematic and scalable architecture. This includes the implementation of logical segmentation to improve data flow, optimize resource utilization, and avoid congestion. Redundancy mechanisms are deployed to counter possible points of failure to enhance overall system uptime. Efficient bandwidth management techniques are used to ensure stable connections and fair distribution of network resources among users.

Review of Related Literature

According to Balcita and Palaoag (2021), integrating modern technology into school management systems improves education quality and streamlines institutional operations, while a well-structured framework enhances both technical and managerial functions. The integration of modern technology into school management systems, as highlighted by Balcita and Palaoag (2021), directly supports the need for an efficient and well-structured network management framework in educational institutions. This aligns with the objectives of this

study by emphasizing how a systematic approach to network management can enhance both technical efficiency and administrative functions.

The findings presented by Zincir-Heywood et al. (2021) on holistic network management validate the necessity of maximizing resource utilization in the proposed framework. In the context of educational institutions, Dzemydienė et al. (2023) advocate for the implementation of ITIL v4 in managing ICT infrastructure to improve administrative efficiency, while Thobiyah et al. (2024) demonstrate the benefits of using simulation tools like Cisco Packet Tracer for designing stable networks.

Additionally, Jia et al. (2024) show how expanding network infrastructure can drive digital transformation, especially in educational institutions, by improving access to digital tools and resources. Social platforms also contribute significantly to education by enhancing communication, collaboration, and knowledge sharing among students and faculty. Platforms like Google Classroom, Microsoft Teams, and educational discussion forums allow for seamless interaction, resource sharing, and peer learning beyond the traditional classroom setting. However, for these tools to be effectively utilized, a well-structured and high-performance network infrastructure is necessary. By improving the network infrastructure and bandwidth management, the school can facilitate modern digital learning methods, integrate social platforms for academic collaboration, and ensure seamless access to educational content. These improvements align with the objectives of this capstone project by promoting efficient and technology-driven education while addressing the school's existing network deficiencies.

Public School Network Design

The importance of designing scalable, secure, and adaptable network infrastructures for educational institutions has been extensively discussed in the literature. According to the SEND Smart Networks Guide, key recommendations for network infrastructure in schools include optimizing bandwidth, providing secure access for digital learning, and ensuring compliance with data protection laws such as the Data Privacy Act. These principles are particularly relevant for the simulation of a network infrastructure for Amsic Integrated School, as they address essential academic access requirements while safeguarding administrative and educational data. These recommendations underscore the need for robust network solutions to meet the dynamic demands of modern educational environments (Consortium for School Networking, 2023). These principles validate the need for a well-designed, secure, and scalable network for Amsic Integrated School, ensuring both academic accessibility and data protection.

There are several critical concerns in the design of a network infrastructure for public schools to ensure it is effective and flexible. According to the Network Encyclopedia, network designs should be scalable to adjust for future growth, secured to protect sensitive data, and reliable to ensure uninterrupted availability of educational resources. Proper hardware selection, which includes routers and switches together with efficient topologies used, such as star and hybrid configurations, enhances network performance and simplifies management. The article also emphasizes the necessity of integrating both wireless and wired connections to cater to various requirements such as lab internet access with high availability and mobility of instructors. It suggests network virtualization to gain more resource efficiency. Lastly,

there is a strong requirement for security measures like firewalls and encryption that minimize vulnerabilities and ensure compliance with data protection laws such as the Data Privacy Act of 2012 in the Philippines (Network Encyclopedia, 2023). The need for scalability, security, and reliable hardware aligns with the proposed infrastructure, ensuring it meets future growth demands while maintaining strong data protection measures.

Research insights into government programs' efficiency and effectiveness emphasize the balance between outreach and sustainability. The Philippine Institute for Development Studies (PIDS) analyzed Directed Credit Programs (DCPs) and found that while these initiatives aim to extend services to a broad audience, they often compromise operational efficiency. The study highlighted a significant issue in cost recovery, where many programs remain financially unsustainable without government subsidies. This inefficiency suggests that for these programs to be both effective and sustainable, a strategic realignment focusing on reducing operational costs or adjusting interest rates is necessary (PIDS, 2022). The findings highlight the importance of cost-effective strategies, which can be applied in evaluating the financial feasibility of network implementation for schools.

The design of an efficient network infrastructure is integral to the improvement of educational experiences via the incorporation of Information and Communication Technology (ICT). A meticulously organized network framework guarantees consistent access to digital resources and internet connectivity, which promotes collaborative learning settings and supports contemporary teaching methodologies. Scholarly investigations indicate that the integration of ICT within educational institutions markedly enhances the quality of education by providing access to worldwide resources and fostering innovative teaching strategies, thus

better equipping students for futures characterized by technological advancements (Network Encyclopedia, 2023). A well-structured network plays a vital role in enhancing digital learning, ensuring seamless connectivity, and supporting modern teaching methods.

Moreover, for institutional development, it is important that the designs are scalable, secure, and cost-effective. Suitable implementations of ICT systems enable schools to meet global standards, enhance student interaction and engagement in teaching strategy approaches, making the basic function of school infrastructure in the current learning scenario indispensable (Network Encyclopedia, 2023). The importance of scalability and cost-effectiveness reinforces the necessity of a future-proof network that aligns with global educational standards.

Network Security Practices

A higher dependency on digital infrastructures in educational organizations demands appropriate network security measures. As per Kim and Solomon (2020), employing security protocols such as a firewall, IDS, and IPS will be very useful in ensuring data confidentiality, integrity, and availability since these systems work together to prevent unauthorized access to, identify possible threats, and provide safe, continuous connectivity to networks. This process filters traffic based on specific security rules, preventing any unauthorized access. IDS and IPS detect, alert administrators to, and block malicious activity (Kim & Solomon, 2020). Both of these protocols help ensure the networks of educational institutions remain secure and functional, therefore providing a safe digital environment for users.

The National Institute of Standards and Technology encourages using its Cybersecurity Framework for any organization's network infrastructure to protect it. This consists of five major functions: Identify, Protect, Detect, Respond, and Recover. These functions form an integrated and flexible plan that can support any given cybersecurity policy.

With the increasing presence of 5G technology, the strong network security is paramount to its effective functionality. Wala and Kiran (2024) present a comprehensive analysis of the methodologies specific to 5G network security, focusing on techniques such as zero-trust architecture, vulnerability management, and the importance of periodic security assessments. The purpose of these methodologies is to address the unique security issues posed by the complex, fast-paced, and highly interconnected nature of 5G network environments. Zero-trust architecture is critical, as threats may be present both inside and outside of the network. This approach ensures that only valid users and devices can access the resources on the network (Wala & Kiran, 2024). Zero-trust architecture and security assessments are essential in safeguarding 5G networks, ensuring that only authenticated users and devices can access network resources.

The research highlights the importance of established cybersecurity frameworks, especially the NIST Cybersecurity Framework and the recommendations published by the European Union Agency for Cybersecurity (ENISA), in relation to protection of 5G implementations. Such frameworks offer organized methodologies for addressing cybersecurity threats and provide exemplary practices to guarantee that 5G networks remain secure, scalable, and dependable. In using these strategies and frameworks, the organization

can secure the 5G networks by reducing risks associated with it even as it advances in improving its security.

Wireless network

Wireless networks have become integral to educational institutions, providing reliable connectivity for students and staff. A study on the planning and design of Wi-Fi-based university wireless networks highlights critical factors for effective network infrastructure. It emphasizes the importance of scalability, coverage optimization, and adopting modern technologies like Wi-Fi 6 to support high device density and ensure seamless connectivity (Mingwen Chi; Xiaoming Zhang, 2022). The integration of advanced wireless protocols not only improves bandwidth efficiency but also enhances support for hybrid learning and IoT integration, fostering a more dynamic educational environment Additionally, the research identifies common challenges, such as interference and budget constraints, and suggests solutions like strategic access point placement and simulation tools for optimizing network design. These insights are essential for educational settings where high device density and demand for reliable connectivity are prevalent (Mingwen Chi; Xiaoming Zhang, 2024).

Fundamental to enhancing connectivity within learning institutions are models of wireless networks. According to the Office of Educational Technology, various models may be developed to suit specific institutional needs, such as scalability, cost-effectiveness, and accessibility among them (Office of Educational Technology, n.d.). An example is the use of private LTE networks in the rural areas, which has helped mitigate barriers, such as geographical limitations and resource constraints. This methodology utilizes of spectrum licenses using new technology to provide students and instructors with robust, scalable

wireless connectivity (Office of Educational Technology, n.d.). It further emphasizes the importance of considering environmental factors-such as architectural frameworks as well as regional zoning, while in the design. This means that with strategic planning combined with policies such as AUPs, connectivity can be maintained, security can be ensured, and user behavior can be effectively managed (Office of Educational Technology, n.d.) These are highly applicable findings to the development of the network infrastructure that would best meet the unique needs of education institutions like Amsic Integrated School.

Access Points

Access Points are critical components within the network infrastructure of the education sector, especially in more recent Wi-Fi deployments. In educational institutions, reliance on wireless devices to attain teaching and learning, high-speed data transfer, high coverage, and excellent performance even in a dense setting are permitted by Wi-Fi 6 access points. Properly planned access point location and deployment can prevent network congestion, ensuring stable connectivity in any location, especially when multiple users are present (Snyder, 2023).

Another critical feature in designing an efficient network is AP load management. Strong APs in dense zones, such as classrooms, auditoriums, or computer laboratories, must manage multiple connections without degrading performance. For example, 4x4 MU-MIMO Wi-Fi 6 APs can support twice the number of devices compared to earlier models, thereby enabling efficient access for both the instructor and the students. Strategically positioning APs also minimizes interference from physical barriers like walls or metallic surfaces, which may impact the signal strength. In addition, access points (APs) should be installed

according to the overall infrastructure of the institution. Educational institutions migrating to Wi-Fi 6 networks must ensure sufficient back-end bandwidth and install Multi-Gigabit Ethernet connections to avoid bottlenecks, allowing APs to operate at their full capacity. Such an infrastructure upgrade is necessary for supporting modern educational applications, such as cloud-based learning platforms and video streaming services, which require high-speed, low-latency connections (Snyder, 2023).

Campus Edge Network Design

The demand to develop a strong, efficient campus edge network, in support of seamless connectivity in educational institutions, has never been more important. Referring to the layered design framework dividing the network into access, distribution, and core layers, the Campus LAN and Wireless LAN Solution Design Guide by Cisco highlights this structure. The access layer serves as a conduit for end devices, including computers and wireless access points, while facilitating technologies such as Multigigabit Ethernet (mGig) and Power over Ethernet (PoE) to accommodate high-bandwidth applications and supply power to devices. In contrast, the distribution layer functions as a consolidation point for the access layers, implementing policies and defining routing paths. Therefore, the core layer represents the base architecture of the network, where high-speed data transfer takes place with minimal latency and maximum availability (Cisco, 2020). The layered network architecture ensures efficient traffic flow, scalability, and high-speed connectivity, which are essential for the proposed campus-wide network infrastructure at Amsic Integrated School.

There are many customized design methodologies that cater to the specific demands of campus environments. Traditional multilayer architecture is also very effective for smaller

campus environments, using Layer 2 access along with Layer 3 routing in the core and distribution layers. In large campus networks, the Layer 3 routing provided within the access layer also contributes to scalability and reduces convergence times. In addition, Cisco's SDA introduces a new paradigm using software-defined networking that simplifies management processes, increases security through segmentation, and ensures uniform policies in both wired and wireless networks (Cisco, 2020). The use of traditional and software-defined architectures provides flexible design options, enhancing network scalability, security, and management efficiency in educational institutions.

Ensuring high availability and redundancy is critical in minimizing idle time. Hardware redundancy is accommodated through methods such as Stateful Switchover (SSO), Non-Stop Forwarding (NSF), and switch stacking technologies, such as in the Cisco StackWise example. Comprehensive security protocols are also implemented at the perimeter of the network, like Dynamic Host Configuration Protocol (DHCP) snooping, Dynamic ARP Inspection, and 802.1X authentication, which prove useful against unauthorized access and attacks. The integration of wireless LAN has further strengthened the network, with Cisco Catalyst 9800 Series Wireless Controllers and Catalyst 9100 Series Access Points designed to meet the next generation's needs, such as support for IoT devices and mobile clients (Cisco, 2020). Implementing redundancy, security protocols, and wireless integration enhances network reliability and protection against unauthorized access, ensuring continuous and secure connectivity.

It is crucial in fulfilling all the technological needs of the modern academic environment to build an efficient and secure campus network. As Verizon Business states, segmented

networks are among the best practices for dealing with multi-endpoint user environments on campus. This enhances security measures and achieves a high level of operational performance by providing VLANs that categorize users by their roles, including students, faculty, as well as guests (Verizon Business, n.d.).

Moreover, a CAN allows multiple Local Area Networks within separate buildings to be interconnected; however, it remains localized in nature. In such a structure, latency is reduced, and the overall user experience is significantly improved. To improve response times, Verizon recommends deploying a distributed architecture for networks. This includes the deployment of edge computing infrastructure near end-user locations and CDNs that cache closer to the users, especially on bandwidth-intensive applications like streaming. Verizon emphasizes that on-demand bandwidth provisioning is most critical. In using resilient core fiber networks with software-defined management systems, information technology teams can dynamically adjust bandwidth distribution based on varying demands from research programs or large-scale events (Verizon Business, n.d.). Security also forms part of the base elements in campus network architecture. This should be combined with multilayered firewalls and endpoint security measures, including mobile device management to help protect sensitive data while keeping network traffic controlled (Verizon Business, n.d.).

University network infrastructure faces challenges like scalability and security. Spectra (2024) emphasizes the importance of high-speed backbones and robust wireless coverage to support growing student and faculty demands. Cloud services and software-defined networking (SDN) are also recommended to improve flexibility and reduce costs.

Additionally, a layered security approach with tools like firewalls and intrusion detection systems helps safeguard sensitive data. Proactive network monitoring is crucial to resolve performance issues quickly and maintain optimal connectivity. Scalability, security, and proactive monitoring are key factors in maintaining a reliable and future-ready university network, ensuring seamless connectivity and data protection.

Network Design Policies

Network design policies are a critical component in creating safe and effective network infrastructures, especially within school setups like Amsic Integrated School. According to EC-Council (2022), the policies establish the foundation for access management, protection of sensitive data, and monitoring of performance. For a comprehensive policy of network security to come into existence, vulnerabilities must first be identified. This assessment is vital to determine areas that require further protection, especially regarding sensitive information related to students and staff members in different institutions (EC-Council, 2022).

A comprehensive network policy generally comprises various essential components, including authentication protocols designed to confirm user access, encryption standards aimed at safeguarding data during transmission, and incident response protocols intended to effectively manage potential breaches. These are particularly relevant to school networks, which have different user groups like students, teachers, and administrators who have different access rights but must safeguard academic and other personal records. Furthermore, such policies must be regularly reviewed and updated to address emerging security threats. In this respect, firewalls and intrusion detection systems are essential for real-time monitoring and blocking of unauthorized access (EC-Council, 2022).

Simulation Tools

EVE-NG (Emulated Virtual Environment Next Generation) is a widely used network emulation software that enables professionals and instructors to design, test, and debug intricate network topologies. While exact user figures are not publicly available, its applications in education and business environments underscore its significance. One of the key advantages of EVE-NG is that it supports clientless access, which makes it the only virtual network emulator that can operate entirely through an HTML5 web interface without the need for any additional client software (CBT Nuggets, 2023). The clientless access feature reduces complexity and enhances user-friendliness. Additionally, EVE-NG supports the use of several vendor images, i.e., users are able to test multiple technologies within one environment (NetSecCloud, n.d.). It is also famous for being resource-efficient, as it is capable of simulating networks using less powerful hardware than other solutions, which makes it more user-friendly for users with lower computing power (CloudMyLab, n.d.). EVE-NG is also very scalable with the ability to simulate large network topologies suitable for enterprise-level simulations (NetSecCloud, n.d.).

When compared to other network emulators like GNS3 and Cisco Modeling Labs (CML), EVE-NG offers distinct advantages. GNS3, while powerful, often requires a more complex setup and can be less resource-efficient than EVE-NG (NetSecCloud, n.d.). On the other hand, CML is designed primarily for Cisco environments, which may limit its flexibility in multi-vendor simulations (CloudMyLab, n.d.). In contrast, EVE-NG provides a more versatile and efficient solution due to its broad compatibility, scalability, and ease of use. These features make it a preferred choice for network professionals who need an effective emulation platform for learning, testing, and enterprise-level simulations.

EVE-NG was selected as the primary network simulation tool for this study due to its ability to simulate a real, scalable, and multi-vendor networking environment. The collapsed core architecture presented for Amsic Integrated School was tested using EVE-NG before execution in the actual setup to ensure network configurations, VLAN segregation, firewall configurations, and ISP load balancing were optimized to the maximum level before implementation.

One of the best features of EVE-NG is its interactive and graphical interface, which makes it simple to configure and debug networks. Unlike the traditional physical setups, EVE-NG offers the convenience of testing various network setups without necessarily incurring expensive hardware. Through this hands-on approach, network performance and security deployments are better understood, and therefore, it is an easy tool to test various configurations (Patel, 2024).

Among the main motivations for employing EVE-NG in this research was its ability to mimic real networking environments. The network infrastructure created was subjected to rigorous stress testing, routing tests, and security scans within the platform. This rendered the design scalable and capable of supporting the expected number of users at Amsic Integrated School. Employing real vendor-specific device images provided a more realistic representation of network behavior, thus making the simulation results applicable to real-world implementation (Patil, 2024).

A number of network vendors supported by EVE-NG were instrumental during the testing phase of the present study. The platform facilitated the emulation of FortiGate firewall policies, Cisco network devices, and VLAN implementations, which were core elements of

the proposed infrastructure. Although Cisco devices were emulated, there was also experimentation with other cost-effective alternatives like Ubiquiti for actual deployment. Having such vendor flexibility allowed the study to investigate high-end and cost-effective alternatives to ensure the final network design would be cost-effective and scalable (Saharan, 2025).

EVE-NG was a critical tool in planning and testing the suggested network infrastructure. Its accurate simulation, improved learning support, and multi-vendor capability enabled thorough testing prior to deployment, and the final plan proved to be both economical and technically sound.

Monitoring Tools

A comparison of Zabbix with other network monitoring tools, such as Prometheus and Nagios, highlights the unique strengths of this tool and its applicability in specific contexts. Zabbix is recognized for offering many out-of-the-box functionalities, including integrated alerting, built-in monitoring templates, and dashboards that can be easily adjusted. It uses third-party databases such as MySQL and PostgreSQL for data storage to support complex data types and enable reporting capabilities. However, the dependency on third-party databases may affect performance in large environments with nodes exceeding 10,000. Zabbix excels at machine-based monitoring and is suited for small to mid-size networks with a friendly configuration and an intuitive interface (TechRepublic, 2022; NetAdmin Tools, 2023).

It also supports high-performance environments with large distributed deployments, including cloud-native environments, especially when used with a native, fast time-series database that can manage large datasets and queries at high velocity with ease. Although Prometheus has strengths in scalability and real-time data processing, it has limitations, such as a 14-day data retention period and native alerting functionalities that require additional tools like Alertmanager for more complex features. It is well-suited for service-oriented monitoring; however, its complexity can make it more difficult for seeking a straightforward solution (TechRepublic, 2022).

Nagios is one of the most popular tools in the market, offering extensive monitoring functionalities; however, it requires configurations through text files, which can be quite a hassle for beginners. Unlike Zabbix, Nagios does not have pre-configured monitoring templates nor a modern web-based configuration interface. These disadvantages, along with more basic visualization features, can lead to longer setup times and reduced flexibility compared to Zabbix (NetAdmin Tools, 2023; TechRepublic, 2022).

In summary, while Zabbix provides an all-inclusive monitoring solution ideal for traditional IT environments, Prometheus is suited for highly scalable cloud infrastructures, and Nagios serves as a simpler, though less feature-rich, alternative. Ultimately, the decision of which tool to use depends on an organization's specific needs, including deployment scale, usability, and types of systems monitored (TechRepublic, 2023).

Zabbix is an open-source network monitoring solution; its flexibility, scalability, and wide feature set have made it highly popular in large and complex environments. Its adoption is especially notable in smart campus networks, where it has played a significant

role in supporting digital transformation. Studies have highlighted its implementation in a large educational institution, where it was deployed with TiDB— a database especially suited for time-series data— and Grafana for rich visualization. The distributed architecture of the system allowed coherent monitoring in all access, aggregation, and core network layers. Additionally, intelligent features such as performance optimization and anomaly detection enhanced both efficiency and quality of service. More importantly, the system introduced an innovative concept called "Monitoring as a Service," which enables different stakeholders-from IT staff to end-users-access to network data effectively (Fangming Guo et al., 2024). Zabbix's scalability, performance optimization, and anomaly detection make it a powerful monitoring tool for large-scale network infrastructures. Its role in smart campus networks ensures real-time visibility, efficient network management, and proactive issue resolution, making it an essential component for maintaining high-quality service and digital transformation in educational institutions.

Another study showed how Zabbix can be integrated with Telegram to create a mobile-based monitoring solution, which is one of the adaptability features of the tool. Using Zabbix's alerting system, network administrators received real-time notifications through Telegram, enabling them to respond quickly and operate more flexibly. This allowed administrators to manage network issues remotely, thereby improving operational efficiency and reducing downtime. This integration with mobile communication tools revealed that Zabbix is an economical option, particularly for organizations seeking to monitor their networks effectively and affordably (Mardiyono et al., 2020)

Performance Evaluation Metrics & Stress Test for Network Design

The author provides a comprehensive guide on how to perform network stress tests using traffic generator tools. These tools simulate high traffic volumes, allowing network administrators to evaluate network performance under extreme conditions. The article highlights how tools like Packet Sender and Ostinato can emulate congested network environments by generating traffic with custom TCP, UDP, and SSL packets. This process helps to uncover potential network bottlenecks and vulnerabilities, ensuring the network can handle peak loads without degradation in service quality. Zelleke also emphasizes the importance of monitoring throughput, latency, and resilience during stress testing, as these metrics are crucial for optimizing network infrastructure and preventing failures (Zelleke, 2024).

Stress testing evaluates a network's ability to perform under extreme or unexpected loads, such as high traffic or system failures. It examines recovery mechanisms and ensures the system's robustness in maintaining critical data security after failures. Research by Mishra et al. (2021) demonstrates the application of stress tests on MQTT brokers, which are commonly used in IoT networks. Metrics like CPU usage, latency, and message throughput were analyzed, revealing the scalability and reliability of different broker implementations. Such tests provide insights into potential bottlenecks and enable optimizations for specific scenarios, including resource-constrained environments.

Cost-Efficient Network Design for Small Enterprise

Athab and Saheb (2022) addressed the challenges of document handling in academic institutions by designing and implementing an intranet infrastructure. Utilizing a packet

tracer simulator, they developed a virtual intranet architecture, which was then implemented using available hardware and software. The system, based on Windows Server 2012R2, managed three separate sub-networks connected through switches and a router. Operational for one semester, the intranet demonstrated success in providing fast, cost-effective, and simplified services, marking a step toward fully electronic departments in scientific establishments.

Enoch et al. (2019) focused on developing a secure, scalable, and manageable enterprise network for the Faculty of Engineering at Rivers State University. Employing the Hierarchical Network Model, they designed both physical and logical network topologies. Simulation results indicated that users attempting to connect and initiate HTTP traffic were redirected to an authentication server for credential verification before network access was granted. The design reduced device load, expedited issue identification and resolution, and enhanced network security by ensuring availability, integrity, and confidentiality.

Fortinet

Firewalls play an essential role in network security through traffic filtering to avert unauthorized access and cyber attacks. One of the widely used firewall products is Fortinet's FortiGate, which offers various security elements to provide maximum security for the network. FortiGate firewalls, according to Jon S. (2023), offer a complete security solution through the integration of intrusion prevention, antivirus, and web filtering into one platform. This integration simplifies network management while offering effective security against different types of cyber attacks. FortiGate's centralized management also enhances administrative efficiency, simplifying the management of numerous security tools. A second

significant benefit of FortiGate firewalls is high performance with scalability. As businesses grow, network traffic increases, and hence demands a firewall solution that scales with increasing demands. Fortinet's FortiGate firewalls are engineered to support high traffic levels without any trouble, making them ideal for organizations of varying sizes (Jon S., 2023). The ease of use also enables IT administrators to configure and monitor security settings easily, reducing operational costs while improving network reliability. The use of FortiGate firewalls for network security aligns with the requirement of companies and institutions to secure their data from cyber attacks. FortiGate, with its complete security features, scalability, and cost savings offers a viable solution for guaranteed secure network infrastructure.

Faizan et al. (2019) compared Cisco's Adaptive Security Appliance (ASA) and Fortinet's FortiGate, two Next-Generation Firewalls (NGFWs) widely used in network security. Their study evaluated both firewalls based on throughput, security features, configuration, and management capabilities. Cisco ASA, when integrated with Firepower services, provides modularity and performance, supporting up to 320 Gbps throughput with features like Intrusion Detection System (IDS), antivirus protection, and load balancing. Meanwhile, FortiGate is recognized for its high performance, advanced threat protection, and deep packet inspection. The study concluded that both firewalls serve different organizational needs, with Cisco ASA offering flexibility and integration, while FortiGate excels in robust security. In the context of our study, *Simulation of a Network Infrastructure Design for Amsic Integrated School*, selecting the appropriate firewall was crucial to ensuring network security and efficiency. The findings highlight the importance of

evaluating firewall performance based on institutional requirements to create a secure and scalable infrastructure.

Ubiquiti

Hanselman (2019) conducted an in-depth review of Ubiquiti's UniFi networking solution, emphasizing its advantages over consumer-grade routers. The review describes UniFi as a powerful, centralized networking solution that ensures seamless connectivity, remote management, and scalability for enterprises and large-scale networks. Among the key benefits of a UniFi network include its software-defined networking, which allows administrators to configure and automate network policies from a single platform (Hanselman, 2019). Another is the mesh network capability of devices, which UniFi offers and enhances coverage over large environments, such as offices and schools. Network dead spots are highly reduced in such places. A UniFi device, in contrast to a traditional home router, separates the networking hardware from the control plane, which improves network management and performance of network. More options for customization and better integration with third-party applications make IT administrators flexible regarding network optimization and security management as compared to TP-Link and Netgear, according to Hanselman (2019).

Jangid (2021) describes the Ubiquiti UniFi network in detail, outlining its core components and advantages in modern networking. He explains the fundamental UniFi devices, such as switches, access points, and controllers, to explain their function in improving network performance and security. This is one of the key benefits of the UniFi system: the ability to expand the network with several units, making it suitable for a growing

organization. DPI allows users to track bandwidth usage and ensure effective optimization in network traffic (Jangid, 2021). Conversely, UniFi devices are known for their user-friendly web-based interface that facilitates easy configuration and management, even for people who have little networking experience. In contrast, Mikrotik relies heavily on the CLI configurations. UniFi Controller, from Ubiquiti, provides a web-based interface for simplifying network setup and administration. On the other hand, Cisco's Meraki requires a license fee, which may be very costly in comparison. The Ubiquiti system is purchased one time and does not incur any recurring subscription, yet the performance remains at an enterprise level (Jangid, 2021)

Iperf

iPerf is an open-source network performance testing tool used to estimate the maximum available bandwidth on Internet Protocol (IP) networks. iPerf is a client-server-based tool, transmitting streams of data over TCP, UDP, and SCTP protocols to determine the throughput and analyze the performance of networks (ESnet, 2024). Another major use of iPerf is stress testing, where it generates high volumes of traffic to load networks intensely and test the stability and performance of the network under load (Chanind, 2020). iPerf is also commonly used for monitoring networks, making it easy for network administrators to identify faults and enhance performance by taking precise measurements of throughput, latency, jitter, and packet loss metrics (Vouzis, 2025). One of the major advantages of employing iPerf is that it is platform-independent, supporting a range of operating systems such as Linux, Windows, and macOS, thereby making it a flexible tool for heterogeneous networking environments (NetAlly, 2023). It also offers the functionality for the users to configure the testing

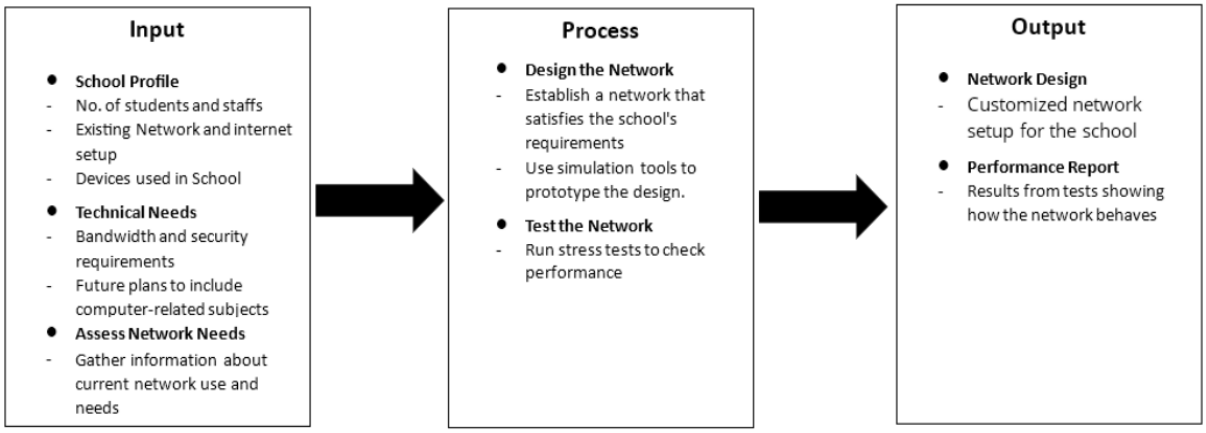
parameters, such as modifying traffic types, duration, and bandwidth limits, to accommodate specific evaluation needs (Chanind, 2020). Being an open-source software, iPerf also enables users to analyze its approaches and integrate its functionalities into other software tools, further increasing its flexibility in heterogeneous networking environments (ESnet, 2024).

Conceptual Framework

In this paper, a method is presented to qualify, design, and evaluate a network infrastructure tailored to Amsic Integrated School-. Firstly, it starts by carrying out an in-depth analysis of the current school's network infrastructure to determine its needs and requirements for scalability. Based on these outcomes, a conceptual network design was developed to specifically satisfy the needs of the school. Simulations and stress testing were conducted on the proposed framework to assess whether it could meet all the operational requirements of the school while still allowing room for future growth. The framework is designed to improve the network performance, security, and reliability, thereby preparing the institution for future growth and technological changes.

Figure 1

Conceptual Framework



Objectives of the study

The general objective of this study was to develop and simulate a network infrastructure for Amsic Integrated School that ensures efficient performance, reliability, security, scalability, and operational functionality.

1. To address the needs of Amsic Integrated School's network requirements by analyzing their infrastructure needs
2. To design and simulate a network infrastructure tailored to the specific needs of the school.
    - Wireless Network Implementation
    - Load Balancing
    - Redundancy
    - Scalability and Performance
    - Security Measures

3. To conduct stress tests and performance evaluations of the proposed network through a simulated environment using iPerf.

Scope and delimitation

This study focused on the design, simulation, and evaluation of a collapsed core network infrastructure for Amsic Integrated School. The emphasis was on the merging of two distinct Internet Service Providers (ISPs) into a single network, aimed at providing maximum bandwidth allocation, improved security, and improved network performance. FortiGate was used to merge the ISPs through SD-WAN, ensuring efficient load balancing and failover mechanisms**.** Network topology design, IP addressing schemes, VLAN segmentation, firewall security policies, and network monitoring solutions were specifically covered in the research.

The new network was simulated and tested with EVE-NG for testing and configuration, Zabbix for real-time network monitoring, and Packet Tracer for visualizing the network. These tools were used to test the scalability, efficiency, and security of the new infrastructure. Consultation with school administrators and networking experts was also conducted, and an academic staff survey was carried out to identify common connectivity problems.

In planning the network infrastructure, we decided to utilize DHCP on the Fortinet firewall instead of an independent DHCP server. This was done with the network size, efficiency, security, and manageability in mind so that the proposed solution would be

appropriate for the school environment at a low cost and could be scaled in the future if needed. Since the school network is divided into different VLANs for students, employees, and administrative staff but there is no need for the use of enterprise-class DHCP services, a separate DHCP server would be an overinvestment and would introduce unnecessary complexity. DHCP is built into the Fortinet firewall, and therefore it is an ideal choice for IP address management, lease management, and IP assignment based on VLAN.

By incorporating DHCP into the firewall, the school has a single management system, and IT administrators can control DHCP scopes, firewall policies, VLAN segmentation, and security policies from a single console. This simplifies network management and reduces the utilization of additional hardware, thus resulting in a cost-saving solution. Moreover, with the firewall serving as the DHCP server, security is enhanced, as it prevents unauthorized IP assignments and malicious DHCP servers, only assigning valid IP addresses to authorized devices. Since Fortinet firewalls are optimized to work with traffic management and security, the DHCP service does not impair network performance and offers guaranteed solution for the school. Also, the DHCP server of the firewall supports VLAN-based IP allocation, which allows each VLAN to be assigned IP addresses relevant to its subnet in order to prevent unauthorized cross-VLAN access and ensure network isolation and security. Based on the needs of the school, the most efficient and convenient way to configure DHCP is on the Fortinet firewall. It offers centralized management, increased security, easy administration, and cost savings, which are optimal for a scalable and secure school network infrastructure.

However, the study was limited to network simulation and performance testing. Physical deployment of the proposed infrastructure was not conducted. The electrical infrastructure of the school was also out of scope. Power instability issues or hardware procurement issues were not addressed. End-user device settings, for instance, faculty and student personal devices or specific software applications used in the school network, were also not addressed by the study.

The study was limited in conducting a stress test on the current network setup. Due to access restrictions and performing a live stress test on the existing infrastructure was not feasible. As a result, the stress test was only conducted on the proposed network infrastructure within the simulation environment. This limitation means that direct comparisons between the existing and proposed setups could not be made based on live performance data. Instead, the study relies on faculty surveys and expert consultations to identify the current network's challenges and validate the improvements introduced by the proposed design.

Additionally, Link Aggregation Control Protocol (LACP) was not configured as per expert consultation, since its implementation would heavily rely on Spanning Tree Protocol (STP) and be limited by firewall constraints. LACP (Link Aggregation Control Protocol) is designed to combine multiple physical links into a single logical link for greater bandwidth and redundancy. However, our network relies heavily on VLAN segmentation and SD-WAN for traffic control, and LACP would have to be configured with Spanning Tree Protocol (STP) to prevent loops. STP introduces extra convergence time, which leads to

network recovery delay upon link failure. With the network design being more efficiency- and latency-oriented, avoiding unnecessary reliance on STP was more favorable.

Another limitation this study encountered was the deployment of Fortinet firewall solutions, which require a valid license to operate at full capacity. DHCP configura Consequently, certain advanced security features could not be emulated in EVE-NG, limiting the study to basic firewall configurations and network policies.

In spite of these constraints, the research presents a general network architecture that can be used in the future and will provide a stable, secure, and scalable infrastructure for Amsic Integrated School.

Method

This study employed a descriptive research design to systematically analyze and evaluate the network infrastructure requirements of Amsic Integrated School. Descriptive research aims to characterize phenomena or systems without manipulating variables, making it effective for identifying existing conditions and challenges (Rupra, 2020). This approach allows for a comprehensive assessment of current systems, user experiences, and infrastructural limitations.

For instance, Rupra (2020) utilized a descriptive survey to gather insights into cloud security challenges faced by SMEs in Kenya, providing critical data for developing enhanced security measures. Similarly, this study's descriptive approach facilitated the assessment of the school's existing network, identified performance issues, and proposed optimizations tailored to user needs.

By employing qualitative and quantitative data collection methods, such as faculty surveys, IT officer interviews, and network simulations, this research ensured a well-rounded analysis of network performance, security vulnerabilities, and scalability concerns. The findings were essential in determining network bottlenecks, security risks, and bandwidth management issues, which were addressed through the proposed collapsed core network architecture and structured VLAN implementation.

Requirement Analysis

The current state of the network in Amsic Integrated School had to be established as a prerequisite for determining requirements for the proposed network design. This was achieved by conducting site surveys, interviews, experts' consultations, and user experience surveys.

Site Survey

Our team conducted a site survey to gauge the existing school network infrastructure relative to covering its network areas, bandwidth supply, and hardware. The school already utilizes two ISPs. The first network is provided by ComClark, a government-funded setup given to the computer lab that offers a 215 Mbps connection. However, based on Ookla Speedtest results, the actual measured speed was only 60 Mbps. A 5-port Gigabit Multi-WAN router and two access points were installed nearby. However, ComClark had disabled two of the ports on the router so the wired connections within the lab could not be extended. The second network is a private-subscription, which the school pays for 100 Mbps to the principal's office with one modem. The speedtest was observed in real time with permission from the Principal and IT officer. (See Appendix P for Speed Test Details)

A site survey was also conducted, assessing the physical and logical topology of the existing network, analyzing places where the connectivity problem occurred and where improvements were needed. (See Appendix C for full site survey details)

Interviews

Interviews were conducted with the principal, IT staff, and teachers about what could be improved in the current network. Some of the major concerns raised by the teachers and staff included the lack of internet access in faculty areas because of poor signal coverage and restricted password access. The IT staff also pointed out challenges in expanding the network due to existing infrastructure limitations.

Furthermore, plans for the school's future ICT expansions include extending its network coverage to the faculty of the Junior High School and installing connectivity into a newly constructed building that will house a computer laboratory for elementary students.

Consultation with Experts

We sought the opinion of one Mr. Florante Antonio Alfonso, who is a network engineer at Agape Enterprise Pte Ltd. He advocated for the collapsing of the two networks into one network and consolidation of the two existing networks into a unified collapsed core architecture. This implies combining core and distribution switches to increase efficiency.

The consultation with Mr. Jan Henryck Dizon and Mr. Jayson Paul Banal played a crucial role in refining the configuration and implementation of the proposed collapsed core network infrastructure for Amsic Integrated School. Mr. Jan agreed with the proposed topology outlined by Mr. Florante Antonio Alfonso and strongly recommended using EVE-NG as the primary simulation tool, as it supports Fortinet firewalls and advanced network testing, which Packet Tracer does not.

Both Mr. Jan and Mr. Jayson actively assisted in configuring VLAN segmentation, firewall policies, and network security protocols to optimize bandwidth allocation and enhance security. They provided best practices for setting up the Fortinet firewall, managing access control, and implementing structured network policies. Their hands-on guidance ensured that the proposed network design is properly configured, secure, and scalable to meet the institution's growing technological needs.

Survey and Internet Speed Analysis

To understand the perception of end-users about the network, we conducted a survey of teachers and students on their internet access and use. The results confirmed that there was no coverage or satisfactory signals in the faculty areas, and there were complaints of intermittent internet speeds. Additionally, speed tests were conducted, revealing variations in performance between the government-funded network and the privately subscribed connection. (See Appendix P for Speed Test details)

Budget Constraint

Being a public institution, Amsic Integrated School's budget was a key consideration during the design of the network. The proposed solution focused on cost-effective hardware and configurations with high scalability for maximizing performance while keeping it within feasible financial limits.

Requirement Documentation

The requirement documentation for our study outlined the proposed network topology, IP addressing scheme, and physical layout to ensure optimal performance and security. The proposed network design follows a collapsed core architecture, integrating both wired and wireless networks to accommodate the needs of the institution. The logical topology is designed to enhance scalability and network efficiency, with devices strategically placed to reduce congestion and improve accessibility. (See appendix H & I for the proposed logical topology)

The Main Distribution Frame (MDF) is located in the computer laboratory, which serves as a secured environment with metal railings to ensure physical protection against unauthorized access. The Intermediate Distribution Frames (IDFs) are strategically placed in the Junior High School faculty and the principal's office to ensure efficient network distribution while minimizing cable runs and maintaining structured cabling best practices. These placements were chosen based on network traffic flow and accessibility for maintenance. (Refer to Appendix J for the detailed physical layout.)

The IP addressing scheme follows a Class B network to support a large number of devices while maintaining subnetting flexibility. The network implements VLAN segmentation to separate different departments, ensuring enhanced security and traffic management. The VLAN assignments are as follows:

- VLAN 10 - Administration (192.168.10.1/24) → Admin
- VLAN 20 - Faculty (192.168.20.1/24) → Principal, Teachers and Academic staffs

- VLAN 30 - Students (192.168.30.1/24) → Students

VLANs also prioritize network traffic for critical operations. A combination of static IP addressing and DHCP is used, where servers and essential networking devices are assigned static IPs, while end-user devices receive dynamic addresses through a DHCP server. (Refer to Appendix M for the detailed IP addressing plan.)

Additionally, a proposed relocation of the IT office and networking equipment was considered to enhance accessibility and security. The placement of MDF and IDFs ensures a structured approach to managing network traffic and minimizing latency. The selection of networking devices, such as switches and access points, is based on a cost-benefit analysis, balancing performance with budget constraints. The network infrastructure proposal includes two separate device options: one utilizing Cisco equipment and the other using Ubiquiti equipment. (Refer to Appendix L for the cost analysis and device specifications.)

1. Cisco-Based Proposal:
    - Core Switch: Two (2) Cisco C9300X-24HX-M
    - Access Switch: Four (4) Cisco C9300X-12Y-A
    - Access Points: Four (4) Ubiquiti U6+
2. Ubiquiti-Based Proposal:
    - Core Switches: Two (2) Ubiquiti Pro Max 16 POE
    - Distributor Switches: Four (4) Ubiquiti Lite 16 POE
    - Access Points: Four (4) Ubiquiti U6+

Design of Software, System, Product and/or Process

To ensure the effectiveness of the proposed design, network simulation formed part of the process to ensure its feasibility before implementation. During the simulation process, one can detect potential performance bottlenecks, security vulnerabilities, and bandwidth distribution inefficiencies. Through the simulation process under different conditions, appropriate adjustments can be introduced to ensure greater reliability and cost-effectiveness. This pre-emptive approach reduces the risks of real-world deployment, such that the final deployment is compatible with the long-term digital needs of the institution without the expense of operational sustainability.

The network architecture structure of the Amsic Integrated School framework was created using EVE-NG, Packet Tracer, and Zabbix to assess parameters such as network performance, security, and scalability prior to actual deployment. The use of these tools allowed for end-to-end assessment of network configurations, thereby ensuring that requirements of the institution were met.

Packet Tracer was used primarily for visualization purposes, as EVE-NG does not have a configurable access point. The tool allowed the logical topology to be displayed clearly while ensuring that access points were represented accurately within the network framework. Unlike EVE-NG, which handled most of the configuration, Packet Tracer was utilized to supplement the simulation by illustrating network components that could not be directly implemented in the primary simulation environment.

EVE-NG served as the main simulation platform that supported virtualization of different network devices, such as routers, switches, firewalls, and servers. With EVE-NG,

testing of different network scenarios, such as VLAN segmentation, traffic flow management, and security policy establishment, was made possible. The platform provided real-time feedback regarding configurations, which facilitated timely and informed adjustments prior to deployment.

Zabbix was integrated in the simulated environment to monitor network performance and detect potential problems. The application provided informative feedback on bandwidth usage, device availability, and network latency, which helped in optimizing the network design before actual deployment. Simulated real-time network monitoring enabled by Zabbix verified the infrastructure's ability to handle expected levels of traffic and detected anomalies in advance.

The server configuration in simulation included necessary network services like DHCP, DNS, and firewall configurations. A separate server was allocated to Zabbix to ensure continuous network monitoring. The DHCP server handled dynamic IP address allocation for devices used by students and staff, while the firewall server enforced security policies to block unauthorized access.

The simulated design confirmed the efficacy of the suggested IP addressing scheme, VLAN segmentation, and security rules. Furthermore, it offered a test environment under control for testing various configurations, thus reducing risks prior to actual deployment. This method guarantees that the ultimate implementation meets the network requirements of the institution and is adaptable for future expansion.

Designing the network infrastructure for Amsic Integrated School required prioritizing the real needs of students, teachers, and administrators. A school network is more than just cables and routers—it is the foundation of learning, communication, and operations. To

ensure that the design supports the institution's goals, the following key criteria were identified:

1.Security – Protecting Important Data

A school network handles sensitive data, including student records, grades, and administrative files. Ensuring security means that no unauthorized person can access these records.

- Implemented FortiGate firewall for intrusion prevention and web filtering.
- Used VLAN segmentation to separate student, teacher, and admin traffic.
- Applied Access Control Lists (ACLs) to restrict unauthorized access.

2.Reliability – Ensuring a Stable Connection

A reliable network prevents interruptions in teaching and administrative work. It ensures that faculty and students can complete tasks without delays caused by poor connectivity.

- Used SD-WAN with dual ISPs for automatic failover to prevent internet loss.
- Optimized Wi-Fi access point placement to eliminate dead zones.
- Configured Quality of Service (QoS) to prioritize educational traffic.

3. Scalability – Preparing for Future Growth

As the school grows, the network must accommodate more students, devices, and digital tools without requiring major upgrades.

- Used a collapsed core architecture for easy expansion.
- Applied subnetting (/24) to allocate IP addresses efficiently.
- Ensured support for additional access points and wired connections.

4. Performance – Providing Sufficient Speed

A well-performing network allows students and teachers to work without slowdowns, buffering, or failed connections.

- Conducted bandwidth allocation for critical applications.
- Used Zabbix monitoring to detect issues before they impact users.
- Load balanced internet traffic across multiple ISPs to maximize bandwidth.

5.Cost-Effectiveness – Maximizing the Budget

A school has limited resources, so the network must provide long-term benefits while staying within budget.

- Proposed two cost analyses:

  a. Cisco-based infrastructure for enterprise reliability.

  b. Ubiquiti-based infrastructure as a more affordable alternative.

- Focused on energy-efficient devices to reduce long-term operational costs.

This network design is intended to support the real needs of Amsic Integrated School. By considering security, reliability, scalability, performance, and cost-effectiveness, the school can implement a network that is stable, efficient, and prepared for future growth.

Development and Testing

The development and testing phase of this study involved simulating the proposed network infrastructure for Amsic Integrated School using EVE-NG, Packet Tracer, and Zabbix. These tools enabled a comprehensive assessment of network configurations, security policies, and performance metrics before real-world implementation. The network design was

subjected to stress tests, latency analysis, throughput evaluation, and security validation to ensure optimal performance and reliability.

A network stress test was performed to measure latency, throughput, and packet loss in peak usage conditions. The test simulated high traffic levels, thus validating the network's ability to handle expected loads without drastic performance degradation. Several parameters such as response time, bandwidth consumption, and error rates were measured to identify possible bottlenecks.

To further evaluate network performance, an Iperf stress test was conducted. This involved running Iperf in server mode on one device to measure throughput under high-load conditions. The test was executed with the following parameters:

```
iperf -c <server-ip> -t 30 -P 5
```

- -t 30 to measure throughput over a 30-second duration
- -P 5 to simulate 5 simultaneous connections for increased load

This method allowed us to assess VLAN communication performance and analyze the behavior of the core switch when VLANs interacted with each other. The results helped identify potential bottlenecks and guided the optimization of the inter-VLAN routing configurations.

Research Participants

The study was conducted at Amsic Integrated School, focusing on the development and simulation of a network infrastructure. To gather relevant data, key stakeholders were selected based on their roles in the school's network operations and academic environment,

using the purposive sampling method. The participants included the school principal, Ms. Imelda Gozun, who provided insights into the administrative needs of the network. The IT officer, Mr. Richard Lois Pabustan, was interviewed to assess the current network infrastructure and technical requirements.

Additionally, the school has a total of 110 faculty members—61 from Elementary, 32 from Junior High School, and 17 from Senior High School. However, using a convenience sampling method, only 55 faculty members were surveyed to gather feedback on network reliability and usability.

To ensure technical accuracy, three network experts, Mr. Florante Antonio Alfonso, Mr. Jan Henryck Dizon, and Mr. Jayson Paul Banal were consulted regarding best practices for network implementation and security. The study employed a mixed-method approach, combining interviews, surveys, and expert consultations to validate the proposed network design.

Data Analysis

This study utilized qualitative analysis and frequency analysis in examining the responses given in the survey. Qualitative analysis sought to identify patterns and meanings of the open-ended responses, while frequency analysis provided the frequency of distributions of every response to the survey items.

For frequency computation, the responses were grouped and computed according to how often each response was recorded. The data from the survey were analyzed to calculate the percentage makeup of the responses, specifically on device usage, network connection,

application usage, and network infrastructure satisfaction. This approach provided a clear quantitative overview of the respondents' experience.

For network satisfaction measurement, the study employed the weighted arithmetic mean in calculating responses using a Likert scale (1 = Very Dissatisfied to 5 = Very Satisfied). The results indicated issues of the faculty on network accessibility, speed, reliability, and its effect on their productivity. The obtained responses were aggregated into summary tables, which provided significant findings from the experience of the faculty. This practice enabled more meaningful interpretation of levels of user satisfaction on network speed, file uploading, and downloading.

For the qualitative aspect, open-ended responses and trends in the data were reviewed to provide contextual insights. Observations were drawn based on user feedback, highlighting key concerns such as connectivity issues, network reliability, and the usability of the school's network infrastructure. This analysis helped in understanding the underlying challenges and user preferences, guiding recommendations for network improvements.

Research Instrument

A well-structured questionnaire was completed by faculty members to gather observations about network usage, device attachment, and satisfaction with the existing network setup. This survey contained multiple-choice and rating-scale questions, covering a wide range of areas such as device usage, network access, usage of applications, connectivity issues, and general satisfaction with the network performance. Important questions included: "How often do you have connectivity problems?", "What applications do you use most for teaching?", and "How would you rate the network speed during peak hour?" The results indicated that a high percentage of faculty members faced frequent connectivity problems, especially for online lectures and data-intensive computing. These findings indicated the

need for increased bandwidth allocation and optimized access point planning to enhance overall network stability. The questionnaire was a self-created instrument and was validated by our Capstone adviser, Dr. Everly M. Chua, ensuring its relevance and accuracy for the study. (See Appendix D for complete survey questions.)

Apart from survey results, a semi-structured interview was conducted with the IT manager of the institution. This interview addressed key areas of the network infrastructure, policies, and issues, stressing the number of computing devices, internet service providers, bandwidth configurations, network security policies, and maintenance policies. The specific questions included: "What are the most common issues in managing the institution's network?", "How often is network maintenance performed?", and "Are security policies implemented to protect student and faculty information?" The answers indicated that bandwidth limitations and old equipment were pressing concerns, along with the need for a more formal network management system. These findings provided detailed insights into the operation of the institution's network helped identify areas requiring immediate improvement. (See Appendix E for complete interview guide questions.)

A site survey was conducted to assess the current status of the network infrastructure. This included observation on the placement of current network devices being used, as well as the distribution of wired and wireless connections throughout the school. Internet speed tests were conducted in various locations to identify areas with weak signals or bandwidth limitations. Security measures, such as locked network equipment rooms and protections against power fluctuations, were also evaluated to ensure network stability and longevity.

Results

Site Survey Result

The site survey was conducted to assess the current network infrastructure of the school and serve as the foundation for designing a structured network. The school currently has minimal to no existing network infrastructure, making it necessary to plan an efficient system that will provide stable and reliable connectivity for students, faculty, and administrative staff. The survey involved mapping out the physical layout of the school, identifying key locations for network equipment, and evaluating potential challenges in implementing a network solution.

The school layout consists of multiple elementary buildings, junior high school (JHS) and senior high school (SHS) buildings, a faculty office, a computer lab, administrative offices, and other facilities such as restrooms (CR) and a guardhouse. Some areas are currently undergoing renovation, which may impact future network installation.

During the survey, a few existing network devices were identified. A Wi-Fi router from Converge is installed in the Principal's Office near the SHS Building, providing basic connectivity for administrative offices but lacking campus-wide coverage. A Multi-WAN router from ComClark is located in the Computer Lab within the SHS Building, likely serving as the main internet source for the lab. Additionally, two wireless access points were found: one inside the Computer Lab to provide localized wireless coverage and another placed in a different section of the SHS Building to extend Wi-Fi connectivity.

Since the current setup is insufficient to support the school's needs, the next phase will focus on designing a network infrastructure that ensures comprehensive coverage, secure access, and reliable performance for both academic and administrative operations.

The observations confirmed that certain areas had weak Wi-Fi coverage, particularly in classrooms far from access points. Additionally, some network devices were placed in open areas without adequate security, increasing the risk of unauthorized access and potential damage. These findings reinforced the need for improved network design, with better placement of network components and enhanced security protocols. (See Appendix C for full site observation details.)

The current network infrastructure of Amsic Integrated School is poorly connected and lacks network segmentation, which affects overall performance and scalability. The computer laboratory serves as the hub of internet access, where a router is installed to share the network. ComClark is the school's Internet Service Provider (ISP), and connectivity is augmented by two (2) access points to offer wireless coverage in the lab. The coverage, however, is insufficient for the increasing number of users and devices reliant on the network. In the Principal's Office, there is a regular Wi-Fi router provided by Converge, which operates independently from the network of the computer laboratory. This isolated setup limits centralized network management and does not support seamless communication between different departments. (See Appendix G for the current logical topology)

The Junior High School (JHS) faculty office is not yet internet-enabled, as the network infrastructure is not yet ready for utilization. The network is expected to be made available during the fourth quarter of the school year. This delay in connectivity affects faculty operations, limiting their access to online teaching resources, communication tools, and administrative systems.

The school also features an elementary computer lab that is under construction, which requires cabling, access points, and efficient bandwidth allocation when operational. The expansion indicates a requirement for an extensible network design that will ensure future growth and integrate all school departments into a single system.

Faculty Survey Result

To assess the opinion of the faculty on network connectivity and infrastructure, a systematic survey was conducted among the faculty members using a questionnaire designed by the researchers for this specific purpose. The survey aimed to gather information related to the experience of the faculty with the network of the institution, the impact of connectivity on their professional work, and their satisfaction in general. The purposive sampling method was used to ensure that the respondents were faculty members who actively used the school network for teaching, research, and administrative tasks. To enhance the sampling process, a convenience sampling approach was also incorporated by distributing surveys among readily available faculty members who were accessible during the data collection period. The respondents provided their opinions using a structured questionnaire with Yes/No, frequency-based questions, and Likert scale rating (1 = Very Dissatisfied, 5 = Very Satisfied).

Table 1 shows that the majority of the faculty members bring their devices to the school premises. This indicates that the network design should be scalable so that it can cater to those faculty members who use their laptop for work related purposes.

Table 1

Number of faculty that bring their device(s) for work related purposes.

Response	Count	Percentage (%)
Yes	53	96.36%
No	2	3.64%

Table 2 demonstrates that the majority of the faculty staff do not connect their devices to the school network. This implies that the network may experience fewer traffic jams from the use of personal devices, thereby leaving more bandwidth for school use. However, the faculty staff who do connect personal devices highlight the need for network security features to keep out unauthorized users or potential vulnerabilities.

Table 2

Number of faculty that connect their device(s) to the school's network

Response	Count	Percentage (%)
Yes	16	29.09%
No	39	70.91%

Table 3 shows that most of the faculty members are only connecting one device, while only a few are not connecting any. That implies the network traffic load is relatively low since fewer users are connecting two or more devices. Fewer users connecting two or more devices implies that the network can be designed with more emphasis on speed and stability rather than accommodating a high volume of simultaneous connections.

Table 3

Faculty members' personal devices connected at the same time to the school's network.

Number of Devices	Count	Percentage (%)
0	21	38.18%
1	29	52.73%
2	4	7.27%
3 or more	1	1.82%

Table 4 indicates that Google Workspace and Microsoft Office are the most used applications by instructors. This means that the network infrastructure must have a priority for stable and consistent access to productivity suites since they are used daily. The heavy use of communication tools and email means uptime consistency and low latency are required to support effective communication and collaboration.

Table 4

Faculty members' frequently used apps for school tasks.

Application	Count	Percentage (%)
Microsoft Office (e.g., Word, Excel, PowerPoint)	55	100%
Google Workspace (e.g., Google Docs, Sheets, Drive)	50	90.91%
Zoom	15	27.27%
Microsoft Teams	15	27.27%
Learning Management Systems (LMS) (e.g., Moodle, Canvas)	16	29.09%
Email	45	81.82%
Communication Tools (e.g., messaging apps)	30	54.55%
Social Media	18	32.73%
Video Editing Tools	14	25.45%
Other	Not specified	

Table 5 shows that the majority of faculty members experience frequent connectivity problems, and there are fewer members with such problems happening ocassionally and rarely. It indicates that the network is unstable and unreliable, and this can slow down school operations as well as reduce productivity. The large percentage of frequent problems indicates the need for improved infrastructure and performance optimization to offer a stable and efficient network environment.

Table 5

The frequency of connectivity issues experienced by users was assessed, revealing varying levels of network reliability

Response	Count	Percentage (%)
Rarely (1)	10	18.18%
Occasionally (2)	13	23.64%
Frequently (3)	32	58.18%

The result of the computation is 1.85, which falls within the Very Dissatisfied to Dissatisfied category, as shown in Table 6. This indicates significant user dissatisfaction with the current network performance, highlighting the need for immediate improvements to enhance internet connectivity and reliability.

Table 6

The level of satisfaction with the current network connection was evaluated based on specific criteria, with responses rated on a scale of (1 = Very Dissatisfied, 2 = Dissatisfied, 3 = Neutral, 4 = Satisfied, 5 = Very Satisfied)

Category	N	Weighted Mean
Speed in accessing applications	55	1.78
Uploading files	55	1.91
Downloading files	55	1.87
Average		1.85

Note. Following the gathering of data from participants, the researchers calculated the weighted mean using the following formula: $\Sigma\ (Response\ x\ Weight)\ /\ \Sigma\ Weight$

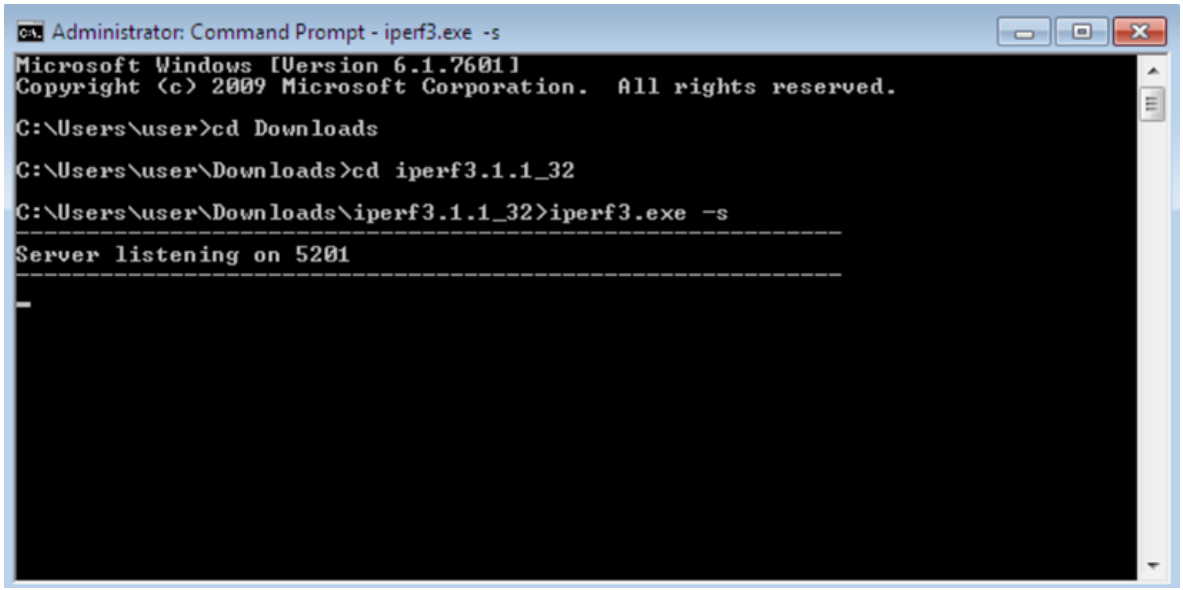
Overall Total:
= 1.78 + 1.91 + 1.87 / 3
= 5.56 / 3
= 1.85

Stress Test Results

Figures 2 to 4 illustrate the preparation steps prior to performing the stress test.

Figure 2

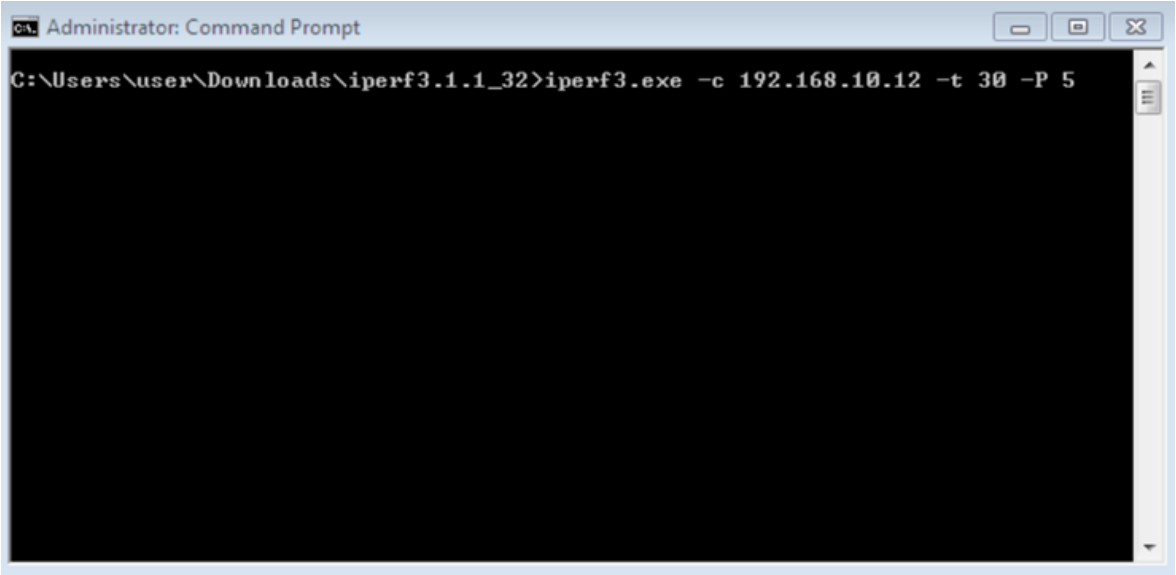
Iperf Stress Test



Note: Start iperf in server mode for 1 device

Figure 3

Run a basic throughput test

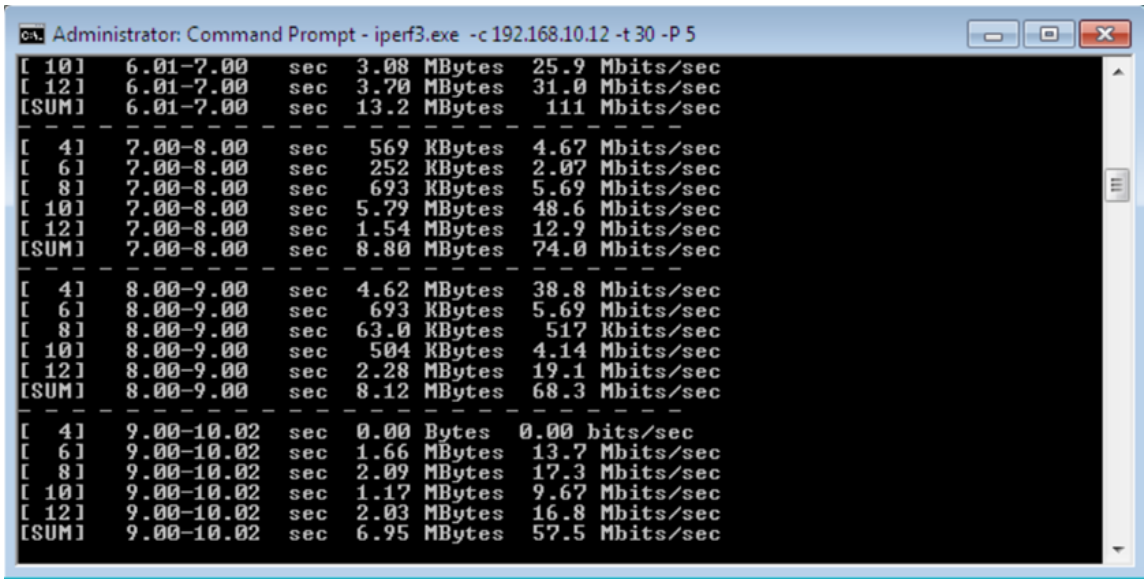


-t 30 is to test for 30 seconds

-P 5 is to test with higher load (5 simultaneous connections)

Figure 4

Ongoing test

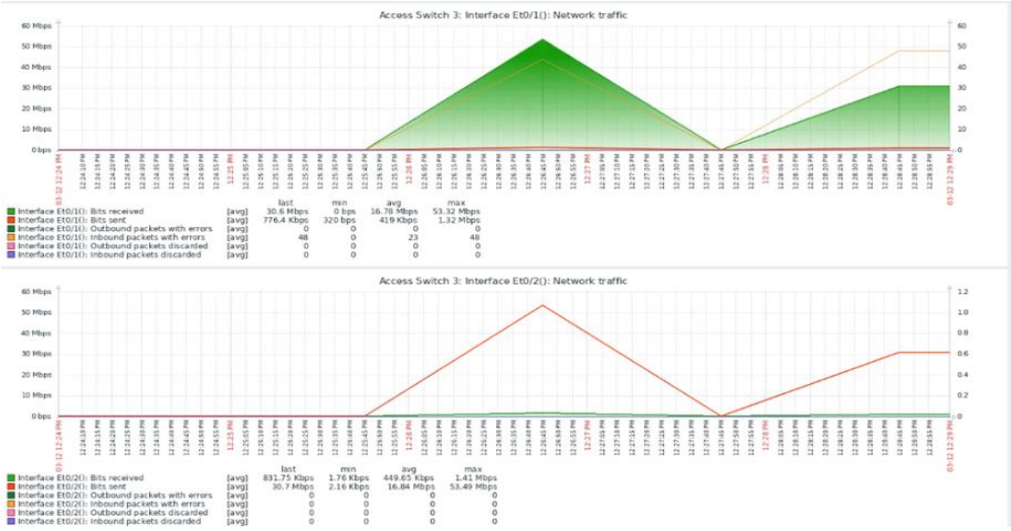


As seen in figure 5, access Switch 3 traffic analysis exhibits different patterns on its interfaces. Inbound traffic on Interface E0/1 hit a high of 53.32 Mbps, an average of 16.78 Mbps, which signifies much incoming data. Outbound traffic, however, was considerably less, hitting a high of merely 1.32 Mbps, an average of 419 Kbps. This signifies most of the data movement on this interface as incoming. The 48 received packet errors also signify some degree of network instability or congestion.

For Interface E0/2, the incoming traffic was relatively low, reaching a high of 1.41 Mbps and averaging 469.65 Kbps. Outgoing traffic, on the other hand, reached a high of 53.49 Mbps, averaging 16.84 Mbps, highlighting that this interface was primarily utilized for sending data rather than receiving data. No errors or packets dropped were detected on this interface, showing constant data transmission. The traffic pattern detected shows that Interface E0/1 is more interested in receiving data, while Interface E0/2 is actively sending, possibly as part of inter-VLAN communication or traffic forwarding within the network.

Figure 5

Graph for VLAN 10 - VLAN 10 traffic



The VLAN 10 to VLAN 10 traffic on Core Switch 1 (CS1) as seen in figure 6 shows that the switch is successfully processing intra-VLAN traffic. On the Et1/0 interface, the average received traffic is 9.07 Mbps, with a high of 45.32 Mbps, showing a high rate of data being received. Traffic out on this interface is low, with an average of 248.19 Kbps, high of 1.23 Mbps. This shows that the majority of the traffic is either being forwarded internally within the VLAN or being transferred through other network channels.

On interface Et1/1, traffic is partially reversed with an elevated rate of data exiting. Average traffic out is 9.39 Mbps with a high of 45.68 Mbps, and low incoming traffic of 265.79 Kbps with a high of 1.25 Mbps. These findings indicate that CS1 successfully forwards VLAN 10 traffic between access switches, maintaining network stability. The minimal packet errors and discards recorded confirm that the network is functioning efficiently without severe congestion or data loss.

Figure 6

Graph of Core Switch 1 (VLAN 10 - VLAN 10)

The Access Switch 4 (ASW4) traffic shows heavy communication between VLAN 10 and VLAN 20 as seen in figure 7. The first graph for interface E0/2 indicates an average incoming traffic of 423.46 Kbps and outgoing traffic of 35.25 Kbps, peaking at 2.41 Mbps outgoing. The second graph for interface E0/3 indicates an average incoming traffic of 47.46 Mbps and an outgoing rate of 24.46 Kbps, peaking at 39.99 Mbps. These figures demonstrate that ASW4 is forwarding a great deal of data between endpoints, with VLAN 20 traffic being the most prevalent. Because the firewall performs inter-VLAN routing, ASW4 is behaving as a pure Layer 2 switch, tagging and forwarding VLAN traffic efficiently.

Figure 7

Graph for VLAN 10 – VLAN 20 Traffic

The Core Switch 1 (CS1) graph in figure 8 illustrates the aggregation of VLAN traffic before it is delivered to the firewall. Interface E0/2, likely connected to the firewall, shows an average inbound rate of 18.09 Kbps and an outbound rate of 1.17 Mbps, with a peak outbound traffic of 4.31 Mbps. Interface E1/1/0, likely connected to ASW4, shows an average inbound traffic of 24.1 Kbps and an outbound rate of 12.66 Kbps, with a peak outbound traffic of 43.25 Mbps. These figures confirm that CS1 is utilized to forward much VLAN 10-to-VLAN 20 traffic to the firewall, where inter-VLAN routing occurs. The peak traffic at certain times shows instances of heavy communications between devices in both VLANs, further confirming the aggregation and forwarding of inter-VLAN data flows by CS1.

Figure 8

Graph for Core Switch 1 (VLAN 10 - VLAN 20)

Figure 9 shows that on Interface E0/3, incoming traffic is trends downward from a peak of 40 Mbps, then consistently decreases to 0 Mbps. The average incoming traffic is approximately 7.89 Mbps, with the all-time high being 29.5 Mbps. Outbound traffic remains generally low, with an average of 218.95 Kbps, with the occasional spikes of up to 1.01 Mbps. The presence of outbound packet errors, averaging 21.33, suggests minor transmission issues.

On Interface E0/2, outgoing traffic begins at approximately 40 Mbps and immediately drops to 0 Mbps. The average outgoing traffic is 10.38 Mbps with a maximum of 39.97 Mbps. No packet errors were recorded, indicating good transmission quality.

Figure 9

Graph for VLAN 10 – VLAN 30 Traffic

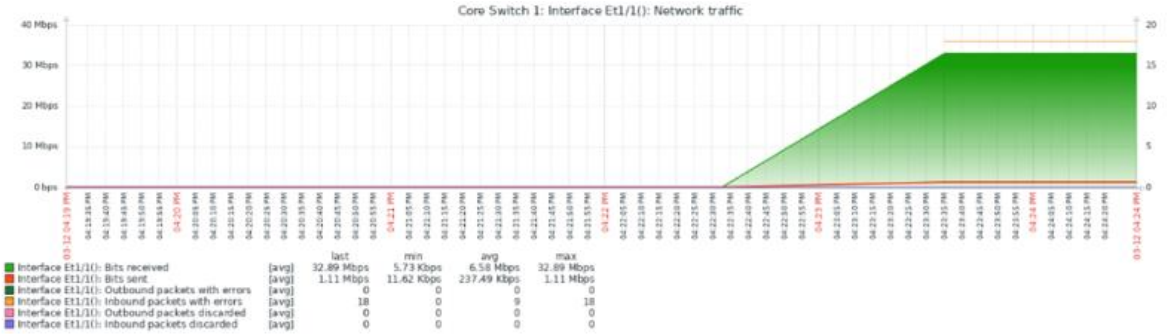
As seen in figure 10, Interface E1/1, inbound traffic steadily increases, peaking at 32.89 Mbps, with an average of 6.58 Mbps. Outbound traffic remains low, with an average of 237.49 Kbps, suggesting that most of the data flow is inbound. A few outbound packet errors (18 recorded) indicate minor issues in data transmission.

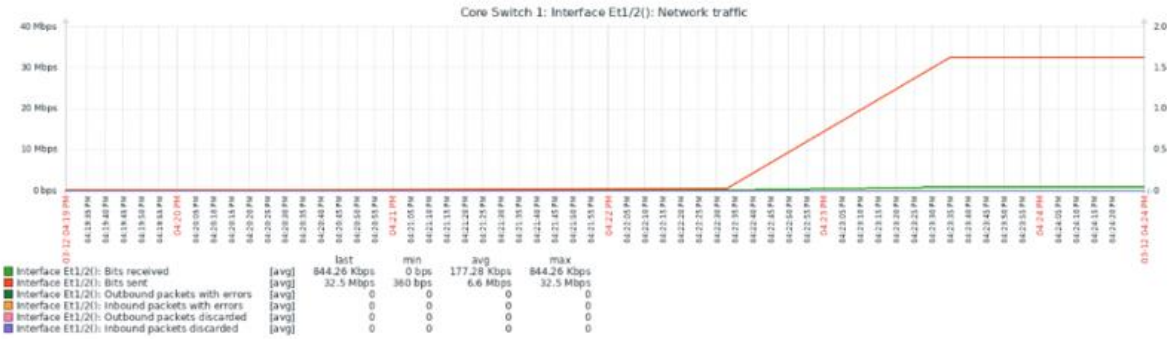
On Interface E0/2, the outbound traffic follows a gradual increase, peaking at 1.7 Mbps before stabilizing. The inbound traffic is minimal, averaging 844.2 Kbps, with minor fluctuations. No errors or packet drops are recorded, indicating stable data handling.

Overall, the data indicates that traffic flow from VLAN 10 to VLAN 30 is primarily processed through ASW4, with CS1 managing the transit. The decreasing trend on ASW4 suggests a burst transfer that diminished over time.

Figure 10

Graph for Core Switch 1 (VLAN 10 - VLAN 30)





ICT Coordinator Interview Results

According to Mr. Richard Pabustan, the ICT coordinator of Amsic Integrated School, the school currently has 9 PCs, which are not yet operational as they are still in the setup process. The main devices in use are 96 laptops, which are connected to the internet via Wi-Fi, as they do not have LAN ports. The network infrastructure consists of 5 router switches connected to 2 Access Points (APs), with the remaining 2 APs currently disabled. The computer lab is equipped with a 215 Mbps internet connection provided by ComClark. Online games are prohibited on the network, but social media platforms such as Facebook, TikTok, and YouTube are permitted for use through the Wi-Fi connection. The school utilizes two ISPs: Converge for the Principal's office and ComClark for the computer laboratory, with the Converge connection being a standard service. There is an ongoing project to construct an ICT lab for elementary students. The computer lab is shared among senior, junior, and elementary students. It is primarily used for seminars, but beginning next quarter, it will be used daily for the KHAN Academy program, where students will engage in streaming content (such as YouTube) then after the streaming they will be taking exams related to the videos they just watched. The computer lab accommodates up to 40 students per session, with each session lasting 40 minutes, allowing for a maximum of 800 students using the computer laboratory. Network monitoring is handled by ComClark, and the Junior High School faculty is identified as the priority area for network improvements.

Interview Results

The current network at AMSIC is supported by two separate ISPs: one provided by ComClark, which is government-supported, and another paid for by the school. The proposed network design, as outlined by Mr. Florante Antonio Alfonso, aimed to consolidate these two networks into a unified system using a collapsed core architecture, where the core and distribution switches are combined into a single unit for efficiency. Ubiquiti network equipment was selected, with a FortiGate firewall to ensure strong security, and an Ubuntu Server to manage the network's operations.

The core network infrastructure consisted of two multilayer core switches with stacking functionality and Power over Ethernet (PoE) capabilities. These switches offer advanced routing features, Quality of Service (QoS) for efficient bandwidth management, and redundancy. At least two Layer 2, PoE-capable access switches were deployed to support the Access Points (APs), with VLANs for network segmentation and secure traffic management. The Wi-Fi 6, PoE-capable APs provide higher throughput and improved performance, especially in environments with multiple connected devices, using technologies like Orthogonal Frequency Division Multiple Access (OFDMA) and Multi-User, Multiple Input, Multiple Output (MU-MIMO) for enhanced efficiency.

For subnetting, a /24 configuration was adopted, supporting up to 200 hosts per subnet, allowing room for future expansion. Older devices may hinder performance, so more advanced devices were recommended for optimal speeds. The network layout includes a Main Distribution Frame (MDF) in the computer lab and Intermediate Distribution Frames (IDFs) in the Junior High School faculty room and principal's office. To ensure redundancy,

the two core switches were stacked, with access switches connected to them. Additionally, two APs were installed in each IDF room, and Link Aggregation Control Protocol (LACP) was used to connect core switches, the server, and access switches for better performance and fault tolerance.

The design of the network is highly scalable to allow growth with additional access switches and APs when the school expands. The /24 subnetting gives ample IP space and supports up to 200 devices on a single subnet. The use of Wi-Fi 6 technology ensures that the wireless network will easily deal with more devices and higher speeds in the future. Security is ensured through the FortiGate firewall, which provides intrusion prevention, application control, web filtering, and VPN support for secure remote access. Access control will be realized through VLANs, which will segregate the network into secure zones, protecting administrative systems from student devices. WPA3 encryption will be used on the Wi-Fi 6 APs to ensure secure wireless communication, protecting against eavesdropping and cyberattacks. This design aims to deliver a secure, scalable, and efficient network infrastructure, supporting AMSIC's current and future technological needs while maintaining high performance and strong security. Upon consultation with the network design expert, the following were recommended in the proposed network design.

- Core Infrastructure: Two multilayer core switches with stacking and PoE features for scalability and redundancy.
- Access Layer: A minimum of two Layer 2 PoE-enabled access switches that support the Wi-Fi 6 access points.

- Security and Management: A FortiGate firewall for security, an Ubuntu Server for network management, and VLAN segmentation for traffic isolation.
- Wireless Network: Deployment of Wi-Fi 6 PoE-capable APs using OFDMA and MU-MIMO to support high-density device connections.
- Network Design: MDF in the computer lab and two IDFs, one in the Junior High School faculty room and the other in the principal's office. There will be two APs in each IDF room.
- Performance Improvement: Link Aggregation Control Protocol (LACP) to aggregate bandwidth efficiency and fault tolerance.
- Subnetting: A /24 subnet supports a maximum of 200 hosts in a subnet. Therefore, there would be a subnetting allowing room for the future.

Additionally, Mr. Jan Henryck Dizon agreed with the proposed topology by Mr. Florante Antonio Alfonso and recommended using EVE-NG as the primary network simulation tool due to its advanced features and vendor compatibility. He also highlighted that EVE-NG allows for Fortinet firewall integration, which was a limitation in Packet Tracer. Mr. Jayson Paul Banal provided further insights into the network configuration process, offering recommendations on VLAN segmentation, firewall policy implementation, and optimization strategies to enhance security and performance. The proposed design, therefore, allows for a robust, scalable and high-performance network infrastructure for the Amsic Integrated School for its current as well as for future ICTs.

Discussion

The implementation of a collapsed core architecture successfully consolidated the two separate Internet Service Providers (ISPs) into a unified system, improving network efficiency, management, and security. This architecture reduced network complexity by merging the core and distribution layers, leading to simplified administration and cost savings (Cisco Systems, n.d.). The streamlined design allowed for better traffic management, ensuring optimized bandwidth allocation and improved connectivity throughout Amsic Integrated School.

Ubiquiti and Cisco were both considered for network hardware, each offering distinct advantages. Cisco devices were used in the simulation due to their enterprise-grade security, reliability, and compatibility with EVE-NG. However, Ubiquiti presents a more cost-effective alternative while still delivering reliable performance for a growing institution. The final selection between these two brands will depend on budget constraints and the school's long-term network scalability needs. Regardless of the chosen brand, FortiGate will be used for firewall security, providing intrusion prevention and web filtering to protect critical network resources (Fortinet Community, n.d.). Traffic separation through VLANs also prevented unwanted bottlenecks and secured administrative information by segregating network areas (Paguigan et al., 2022).

To further ensure the stability and performance of the new network infrastructure, Zabbix was used for real-time monitoring to track system health, detect faults, and prevent potential downtime. The implementation of EVE-NG enabled comprehensive network simulations, ensuring proper configuration before actual deployment. Packet Tracer was

utilized for visualization, particularly for demonstrating access point placements and logical topology designs (Juniper Networks, 2023). These tools facilitated the assessment of network performance, confirming that the proposed design met the institution's needs.

The /24 subnetting scheme effectively allocated IP addresses for up to 200 hosts per subnet, enabling systematic network segmentation and future growth (Cisco Systems, n.d.). Careful placement of the Main Distribution Frame (MDF) and Intermediate Distribution Frames (IDFs) positioned the network for the greatest coverage of the most critical areas in the school. The scheme optimized data transmission, with minimal latency and seamless connectivity for faculty, students, and administrative functions.

The results demonstrated that the collapsed core design, VLAN segmentation, firewall security policies, and structured monitoring significantly improved network security, traffic management, and scalability. The findings confirmed that the implemented infrastructure met the school's operational requirements, ensuring a secure, stable, and high-performing network capable of supporting future technological advancements.

To support the financial feasibility of the project, two cost analyses are proposed:

- Cost Analysis for simulation devices utilizes Cisco network devices, which were used in the simulation. Cisco hardware is known for its enterprise-grade security, performance, and reliability, making it suitable for long-term scalability. However, this option comes with a higher cost. (Refer to Appendix L for full details)
- Cost Analysis for proposed devices proposes the use of Ubiquiti network devices as a more affordable alternative. While Ubiquiti may lack some advanced enterprise

features, it provides excellent network performance at a significantly lower cost, making it a viable option for institutions with budget constraints. (Refer to Appendix L for full details)

- By evaluating both options, the school can decide whether to prioritize cost savings or enterprise-level performance, ensuring that the final implementation aligns with both financial and operational goals.

To enhance digital access provision, a stable and well-structured infrastructure is necessary to support web-based learning. Through an efficient allocation of resources, the network optimizes performance while maintaining cost-effectiveness, ensuring that the institution can sustain long-term operations without excessive expenditures.

Additionally, the design improved administrative efficiency by streamlining record-keeping and document submission processes to DepEd. With a focus on reliability, the network integrates measures to reduce downtime and maintain seamless connectivity, allowing teachers to access digital resources and facilitate learning with greater flexibility. By implementing a cost-efficient and dependable network, this infrastructure addressed the school's operational and educational challenges while promoting equitable digital access for students and faculty.

Table 7 presents the description of the software that were used in the study.

Table 7
Matrix for Software used and its Features

Software	Features
EVE-NG	● Supports full network virtualization for testing and simulation. ● Allows integration of multiple vendors (Cisco, Fortinet, Zabbix, etc.). ● Provides a real-world testing environment before actual deployment.
Packet Tracer	● Cisco's visual simulation tool for designing and testing network topologies. ● Provides a simplified way to configure routers, switches, and wireless networks. ● Supports logical and physical network visualization.
Zabbix	● Real-time network monitoring with alerts for performance issues. ● Tracks bandwidth usage, device health, and uptime. ● Provides data visualization through graphs and reports.
Fortigate	● Enterprise-grade firewall with intrusion prevention, web filtering, and traffic control. ● Supports SD-WAN for merging multiple ISPs and optimizing bandwidth usage. ● Provides VPN, deep packet inspection, and access control for enhanced security.

Conclusion

The study's objectives focused on designing and simulating a secure, scalable, and high-performance network infrastructure to improve connectivity, security, and network management within Amsic Integrated School. Through expert consultations, site surveys, and quantitative analysis, the study assessed the current network limitations and developed an optimized solution that enhances traffic management, access control, and overall network efficiency. The integration of VLAN segmentation and Fortinet firewall policies ensures structured network security, prevents unauthorized access, and improves bandwidth allocation.

During the simulation, the researchers successfully demonstrated the feasibility of the collapsed core network architecture in optimizing network stability and performance. The use of EVE-NG as a simulation tool enabled realistic testing of network configurations, while Zabbix was utilized for real-time monitoring to track latency, packet loss, and bandwidth allocation. Packet Tracer was used for visualization, particularly for access points. The implementation of security measures and network policies validated the effectiveness of the proposed design, ensuring that the network can handle current and future demands while maintaining reliable connectivity for faculty, students, and administrators.

The evaluation of the proposed network was based on expert recommendations, stress testing results, and faculty feedback. The findings confirmed that the objectives of the study were met, with significant improvements observed in network security, performance, and

scalability. The recommendations provided by the respondents were considered in refining the network design, further supporting the feasibility of its implementation.

The results of the network simulation and stress test confirm that the proposed VLAN segmentation and traffic management methods enhance network performance and security. The VLAN 10 to VLAN 10 communication test demonstrated stable intra-VLAN traffic, high-data rate transfer, and low errors for efficient communication between the same VLAN.

For VLAN 10 to VLAN 20, there was significant inter-VLAN communication, with more traffic flow occurring VLAN 20. Inter-VLAN routing was well handled by the firewall, with traffic bursts indicating periods of active data exchange times between devices in various VLANs. This demonstrates that the network configuration supports good inter-VLAN communication while still maintaining isolation where necessary.

The pattern of data transmission between VLAN 10 and VLAN 30 was bursty, with data rising before falling, suggesting periodic rather than constant interaction between the VLANs. While there were some packet errors from time to time, transmission was mostly stable, again suggesting the stability of the inter-VLAN routing mechanism.

In general, the results confirm the efficacy of VLAN segmentation, inter-VLAN routing, and core switch traffic aggregation in a secure, stable, and high-performance network. The organized design allows devices in VLANs to communicate freely while permitting controlled and efficient inter-VLAN traffic. These results confirm that the

proposed network architecture fulfills the operational and security needs of Amsic Integrated School with optimized performance, less congestion, and improved network reliability.

Recommendations

Based on the findings of this study, the following recommendations are provided for the successful deployment, stability, and sustainability of the new Amsic Integrated School network infrastructure:

- **Address Electrical Voltage Issues**
  - Conduct a comprehensive evaluation of the school's electrical system.
  - Install voltage regulation equipment to provide a stable power source for network devices.
  - Deploy Uninterruptible Power Supply (UPS) devices and voltage regulators to mitigate power fluctuations.
  - Provide dedicated electrical circuits for networking equipment (MDF, IDFs, and access points) to prevent interference and reduce power failure risks.
- **Enhance Network Maintenance and Administration**
  - Conduct training workshops for staff and faculty on:
    - Basic troubleshooting
    - Network monitoring using Zabbix
    - Security best practices
  - Consider hiring a dedicated IT staff to manage network maintenance, security patches, and system performance monitoring.

- **Ensure a Systematic Deployment Plan for the Practical Implementation of this Project in the Real World**
    - Implement structured planning before procurement to ensure the school is technically and electrically prepared for network deployment.
    - Follow a staged rollout approach, which includes:
        - Upgrading the electrical infrastructure
        - Cabling and network installation
        - System testing and tuning to support a stable and high-performing network

References

Anderson, P. (2023). *Zabbix vs Nagios Comparison for Network and Bandwidth Monitoring*. https://www.netadmintools.com/zabbix-vs-nagios-comparison/

Athab, O. A., & Saheb, A. M. (2022). Design and Implementation of Electronic Infrastructure for Academic Establishment. arXiv preprint arXiv:2202.03801.

Balcita, R. E., & Palaoag, T. D. (2020). Building a framework for the integration of school management systems (BFISMS). *International Journal of Information and Education Technology*, *10*(6), 455–459. https://doi.org/10.18178/ijiet.2020.10.6.1406

Barrett, P., Treves, A., Shmis, T., Ambasz, D., & Ustinova, M. (2019). The Impact of School Infrastructure on Learning. In *International Development in Focus*.

Chanind. (2020, May 15). Network bandwidth stress testing with iPerf. https://chanind.github.io/2020/05/15/network-bandwidth-stress-testing-iperf.html

CBT Nuggets. (2023, May 15). 5 best network simulators for Cisco exams: CCNA, CCNP, and CCIE. Retrieved from https://www.cbtnuggets.com/blog/career/career-progression/5-best-network-simulators-for-cisco-exams-ccna-ccnp-and-ccie

Chi, M., & Zhang, X. (2022). Planning and design of wifi-based university wireless networks. *2022 IEEE Conference on Telecommunications, Optics and Computer Science (TOCS)*, 1271–1275. https://doi.org/10.1109/TOCS56154.2022.10016078

Cisco. (2020). *Campus LAN and Wireless LAN Solution Design Guide*. https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html

CloudMyLab. (n.d.). EVE-NG vs CML: Battle of network emulators. Retrieved from https://blog.cloudmylab.com/eve-ng-vs-cml-battle-of-network-emulators

Comparitech. (2023). Fortinet FortiGate firewall review. https://www.comparitech.com/net-admin/fortinet-firewall-review

Dzemydienė, D., Turskienė, S., & Šileikienė, I. (2023). Development of ICT Infrastructure Management Services for Optimization of Administration of Educational Institution Activities by Using ITIL-v4. *Baltic Journal of Modern Computing*, *11*(4), 558–579. https://doi.org/10.22364/bjmc.2023.11.4.03

EC-Council. (2022). *Understand, design, and implement network security policies*. https://www.eccouncil.org/cybersecurity-exchange/network-security/understand-design-implement-network-security-policies/

Editorial Team of Network Encyclopedia. (2023). *Network Infrastructure Design – Planning a Campus Network*. https://networkencyclopedia.com/network-infrastructure-design/#google_vignette.

Enoch, J. D., Orike, S., & Ahiakwo, C. O. (2019). Design and Simulation of a Secured Enterprise Network for Faculty of Engineering, Rivers State University. Journal of Information Engineering and Applications, 10(5), 35-

45.https://www.researchgate.net/publication/335967480_Design_and_Simulation_of_a_Secured_Enterprise_Network_for_Faculty_of_Engineering_Rivers_State_University

ESnet. (2024). iperf3: A TCP, UDP, and SCTP network bandwidth measurement tool. https://github.com/esnet/iperf

Faizan, M., Hegde, S. S., & Yaligar, N. V. (2019). Comparison between Cisco ASA and Fortinet FortiGate. IOSR Journal of Computer Engineering, 21(3), 34-36.

Hanselman, S. (2019, August 21). Review: UniFi from Ubiquiti Networking is the ultimate prosumer home networking solution. Retrieved from https://www.hanselman.com/blog/review-unifi-from-ubiquiti-networking-is-the-ultimate-prosumer-home-networking-solution.

Inouye, J. (2022). *Prometheus vs Zabbix: Network monitoring tools comparison*. https://www.techrepublic.com/article/prometheus-vs-zabix/

Jangid, R. (2021). An Introduction to Ubiquiti UniFi Network Solutions. https://www.loginradius.com/blog/engineering/introduction-to-unifi-ubiquiti-network/

Jon S. (2023, January 15). Overview of Fortinet FortiGate Firewalls. Nexigen. Retrieved February 10, 2025, from https://www.nexigen.com/cyber-security/fortinet-fortigate-firewalls-everything-you-need-to-know/

Li, K., Chen, C., & Guo, F. (2024). *Research on Zabbix Monitoring System for Large - scale Smart Campus Network from a Distributed Perspective*. 631–648. https://journal.esrgroups.org/jes/article/view/5153/3736

Mardiyono, A., Sholihah, W., & Hakim, F. (2020). *Mobile-based Network Monitoring System Using Zabbix and Telegram*. https://doi.org/10.1109/IC2IE50715.2020.9274582

Mellia, M., Zincir-Heywood, A., & Diao, Y. (2021). *Overview of Network and Service Management* (pp. 1–18). https://doi.org/10.1002/9781119675525.ch1

Mishra, B., Mishra, B., & Kertesz, A. (2021). Stress-Testing MQTT Brokers: A Comparative Analysis of Performance Measurements. In *Energies* (Vol. 14, Issue 18). https://doi.org/10.3390/en14185817

Navarro, A. M. (2022). School Infrastructure in the Philippines: Where Are We Now and Where Should We Be Heading? *Philippine Institute for Development Studies (PIDS)*. https://www.pids.gov.ph

NetAlly. (2023). Test accessory - iPerf test tool for network performance testing. https://www.netally.com/products/testaccessory/

NetSecCloud. (n.d.). EVE-NG vs GNS3: A detailed comparison of network emulators. Retrieved from https://netseccloud.com/eve-ng-vs-gns3

Oikonomou, N. V, & Oikonomou, D. V. (2024). Educational Applications and Comparative Analysis of Network Simulators: Protocols, Types, and Performance Evaluation. *Journal of Engineering Research and Sciences*, *3*(6), 18–32. https://doi.org/10.55708/js0306003

Patel, A. (2024). Top features of EVE-NG: Enhancing your network simulation experience. NetSecCloud. Retrieved from https://netseccloud.com/top-features-of-eve-ng-enhancing-your-network-simulation-experience

Patil, A. (2024). Understanding EVE-NG: A comprehensive guide for beginners. Orhan Ergun. Retrieved from https://orhanergun.net/understanding-eve-ng-a-comprehensive-guide-for-beginners

Saharan, A. (2025). EVE-NG vs CML: Battle of network emulators. CloudMyLab Blog. Retrieved from https://blog.cloudmylab.com/eve-ng-vs-cml-battle-of-network-emulators

Snyder, J. (2023). *How to Design Your K-12 School's Wi-Fi 6 Upgrade for Network Nirvana*. https://edtechmagazine.com/k12/article/2023/08/how-design-your-k-12-schools-wi-fi-6-upgrade-network-nirvana-perfcon

Spectra. (2024). *Challenges and best practices for university network infrastructure*. https://www.spectra.co/resources/blog/challenges-and-best-practices-for-university-network-infrastructure

T, T., Franciscus, A., Fakrurrozi, Wichaksono, I., Baqi, I., Daeli, R., & Tarigan, R. (2024). Design and Simulation of a LAN Network for Optimizing IT Infrastructure at SMKS XYZ Depok Using Cisco Packet Tracer. *International Journal Software Engineering and Computer Science (IJSECS)*, *4*, 731–744. https://doi.org/10.35870/ijsecs.v4i2.2673

Techblonhub. (2024). Fortinet Firewalls: Key Features, Benefits, and Protection Tips. Retrieved from https://techblonhub.com/fortinet-firewalls/

Technology, O. of E. (n.d.). *School District Wireless Network Models*. https://tech.ed.gov/wireless-brief/network-models/

Verizon. (n.d.). *Campus network design best practices*. https://www.verizon.com/business/resources/articles/s/campus-network-design-best-practices/

Vouzis, P. (2025, January 10). iPerf and network performance testing. NetBeez. https://netbeez.net/blog/how-to-use-iperf/

Wala, F. B., & Kiran, M. (2024). *5G Network Security Practices: An Overview and Survey*. http://arxiv.org/abs/2401.14350

Xiaofang Jia, B. X., & Wang, X. (2024). The impact of network infrastructure on enterprise digital transformation ——A quasi-natural experiment from the “broadband China” Strategy. *Applied Economics*, *56*(12), 1363–1380. https://doi.org/10.1080/00036846.2023.2176450

Zelleke, L. (2024). *Network stress test – How to stress test your network with a network traffic generator*. https://www.comparitech.com/net-admin/network-stress-testing/

Appendix A
Cover Letter

HOLY ANGEL UNIVERSITY SCHOOL OF COMPUTING

December 16, 2024

DEPARTMENT OF EDUCATION
SCHOOLS DIVISION OF ANGELES CITY
RECEIVED
BY: JAN 02 2025

Engr. Edgard C. Domingo, PhD, CESO V
School Division Superintendent
Division of Angeles City

Dear Engr. Domingo,

Greetings of peace!

This letter is to respectfully request approval to conduct a survey at **Amsic Integrated School** as part of the requirements for the Undergraduate Capstone Project of the students enrolled in **6NETCAP2 - Network Capstone Project (NW401)** under the **Bachelor of Science in Information Technology** program, specializing in Network Administration.

The project aims to design an efficient network infrastructure that addresses the current needs of **Amsic Integrated School** while ensuring scalability for future expansion. To achieve this, they need to gather information regarding the school's current network setup and understand its technological practices. Specifically, they would like to conduct:

1. **A site survey** to evaluate the existing network layout and infrastructure.
2. **A survey for employees** to determine whether they bring their own devices (BYOD) to work and how these devices are integrated into the network and what software do they use.

We assure you that all information collected during this study will be treated with the utmost confidentiality and used solely for academic purposes.

Below are the names of the students who will conduct the survey:

Baluyut, Kahlel Inigo I.
Bautista, Sean Matthew C.
Delos Reyes, Carl Louie G.
Delos Reyes, Joseph R.

We are hopeful for your kind consideration and approval of our request. Should you have any questions or require further clarification, please do not hesitate to contact us at carllouiedelosreyes1225@gmail.com or through 0999-359-2735.

Thank you for your time and support. We look forward to your favorable response.

Respectfully yours,

Dr. Everly M. Chua
Capstone Adviser

Noted by:

Dr. Marlon I. Tayag
Dean
School of Computing

Received
BY: DEVERLY LEMIQUE
DATE: 1/2/25

#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 SCHOOL OF COMPUTING

Site survey execution plan:

1. Persons in Charge

Kahlel Inigo I. Baluyut

Task: Network Layout Mapping

Responsibility: Document the physical layout and assess the network topology.

Sean Matthew C. Bautista

Task: Equipment and Device Audit

Responsibility: Identify existing networking equipment, BYOD practices, and software used.

Carl Louie G. Delos Reyes

Task: Connectivity and Signal Testing

Responsibility: Evaluate network performance, including signal strength and bandwidth usage.

Joseph R. Delos Reyes

Task: Data Compilation and Documentation

Responsibility: Collect and organize all findings into a cohesive report.

2. What to Measure

- **Network Infrastructure**

Number and types of networking devices (e.g., routers, switches, access points).

Cable types and physical layout.

- **Device Inventory**

List of staff devices (BYOD), connectivity types (wired/wireless), and software utilized.

- **Signal Strength**

Wi-Fi signal strength in key areas to identify dead zones or weak coverage.

- **Bandwidth and Speed**

Internet speed tests and bandwidth usage at different times of the day.

- **Usage Patterns**

#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 SCHOOL OF COMPUTING

Employee feedback on network reliability, challenges, and common use cases.

3. Materials Needed

- **Measuring Tape**

To measure distances between devices and coverage zones.

- **Pen and Notebook**

For manual note-taking during the survey.

- **Speed Test Tool**

To evaluate internet speed and bandwidth.

- **Survey Questionnaires**

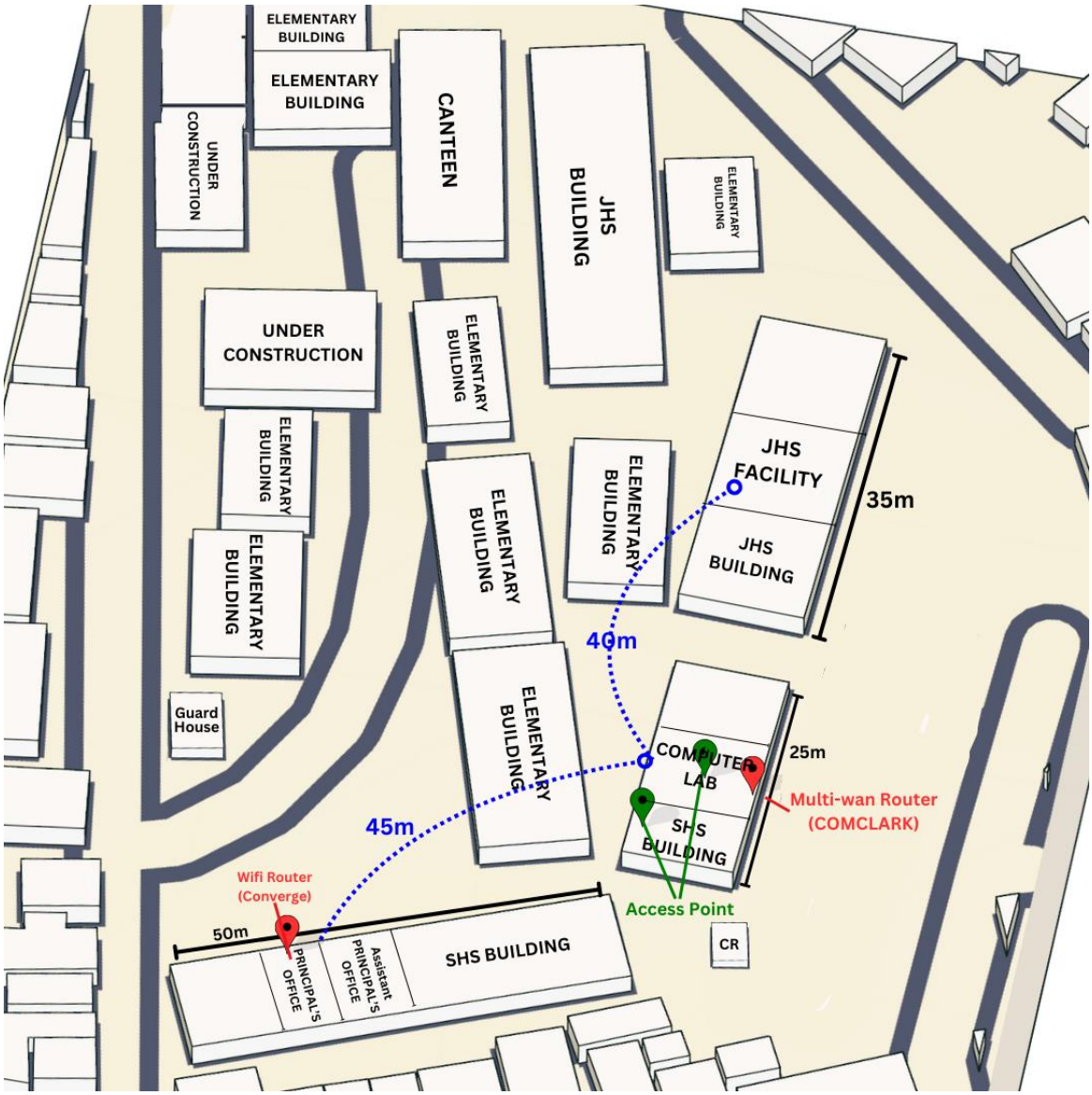
To gather qualitative feedback from employees.

- **Camera or Smartphone**

To capture images of network devices and infrastructure for documentation.

#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

Appendix B
Current Physical Network Layout



Appendix C
Faculty Survey

Faculty BYOD Survey

We are Group 1 of NW-401 from Holy Angel University, conducting a survey for our capstone project, **"Simulation of a Network Infrastructure Design for Amsic Integrated School."** Your input is essential to help us design a better network for the school.

1. Do you bring your own device (BYOD) to school for work-related purposes?
☐ Yes
☐ No

2. Are you allowed to connect your device(s) to the school's network?
☐ Yes
☐ No

3. How many personal devices do you connect to the school's network at the same time?
☐ 1
☐ 2
☐ 3 or more

4. What apps do you frequently use for school tasks? *(Check all that apply)*
☐ Microsoft Office (e.g., Word, Excel, PowerPoint)
☐ Google Workspace (e.g., Google Docs, Sheets, Drive)
☐ Zoom
☐ Microsoft Teams
☐ Learning Management Systems (e.g., Moodle, Canvas)
☐ Email (e.g., Gmail, Outlook)
☐ Communication Tools (e.g., WhatsApp, Messenger, Viber)
☐ Social Media (e.g., Facebook, Instagram, Twitter)
☐ Video Editing Tools (e.g., Canva, Adobe Premiere)
☐ Other: _____

6. How often do you experience connectivity issues?

☐ Rarely (less than once a week)

☐ Occasionally (1-3 times a week)

☐ Frequently (daily)

6. Rate your satisfaction with the current network connection in terms of: *(1 = Very Dissatisfied, 2 = Dissatisfied, 3 = Neutral, 4 = Satisfied, 5 = Very Satisfied)*

a. **Speed in accessing applications that require network connection**
1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

b. **Uploading files**
1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

c. **Downloading files**
1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

Thank you for your time and responses. This will greatly help us improve the network for Amsic Integrated School.

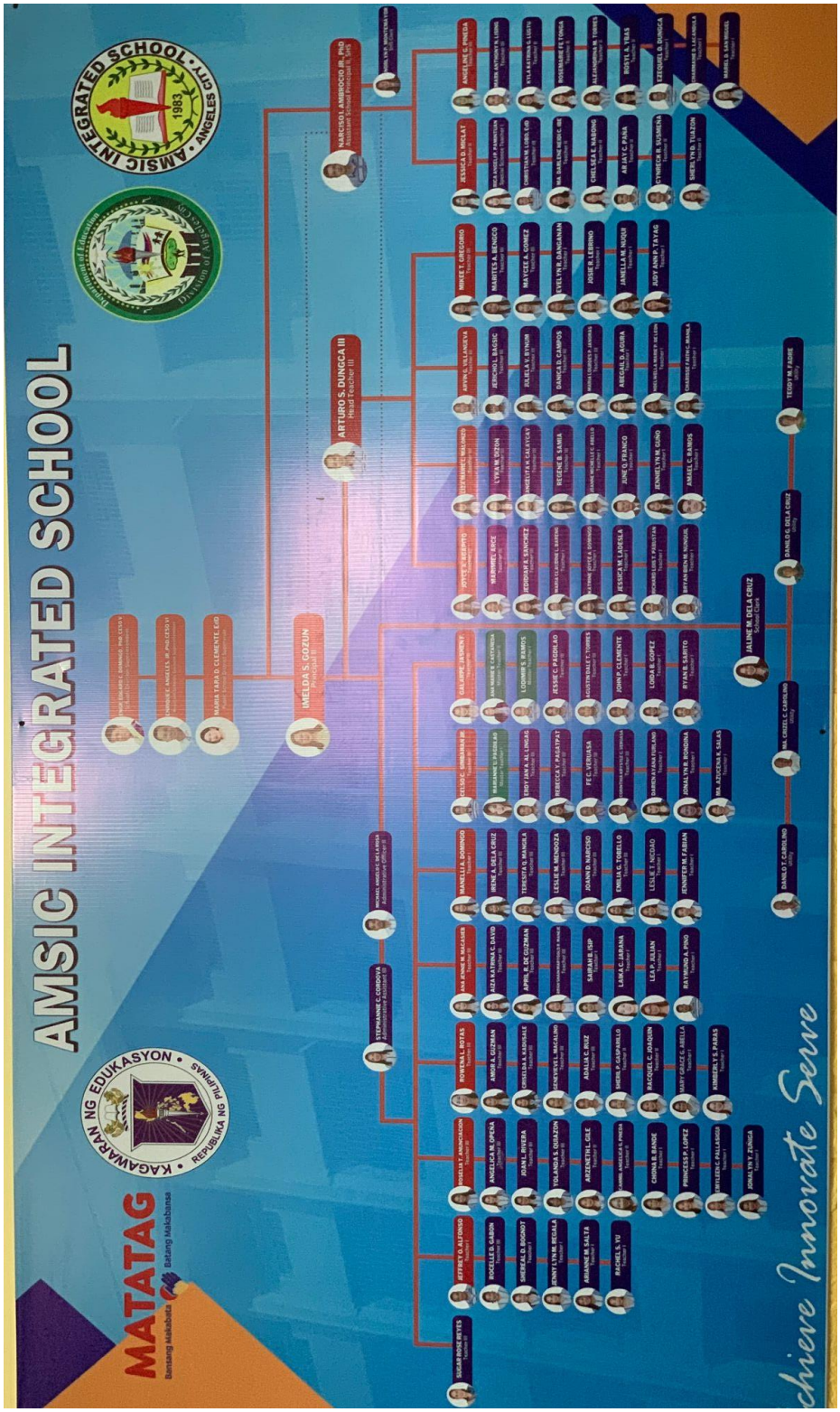
NW-401 | Group 1
Holy Angel University

Faculty BYOD Survey

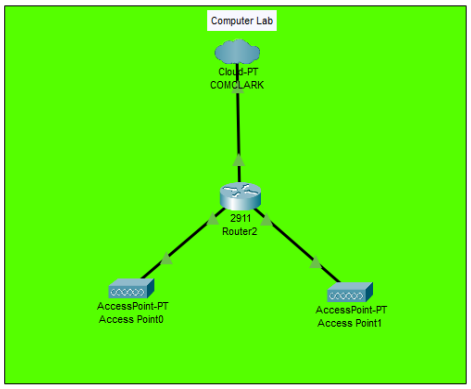
Appendix D
Initial Interview Guide Questions

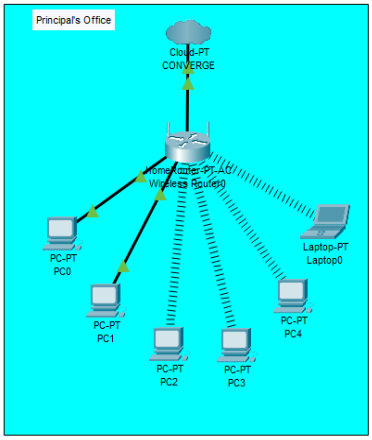
- How many devices are currently in use, if any?
- Where is the internet router or modem located?
- What is the total number of computers available?
- Are there established policies for internet usage?
- How many Internet Service Providers (ISPs) are in use?
- What are the primary issues encountered with the current network setup?
- Is the ISP an enterprise-grade service or not?
- How many computer laboratories are available?
- How is the computer laboratory utilized?
- What software or applications are used in the computer laboratory?
- How frequently is the computer laboratory utilized?
- How many students make use of the computer laboratory?
- Is there a designated location for the installation of network equipment?
- Is there an individual or team responsible for managing and maintaining the network?
- What are the priority areas for internet access within the institution?

Appendix E
Amsic Integrated School's Organizational Chart

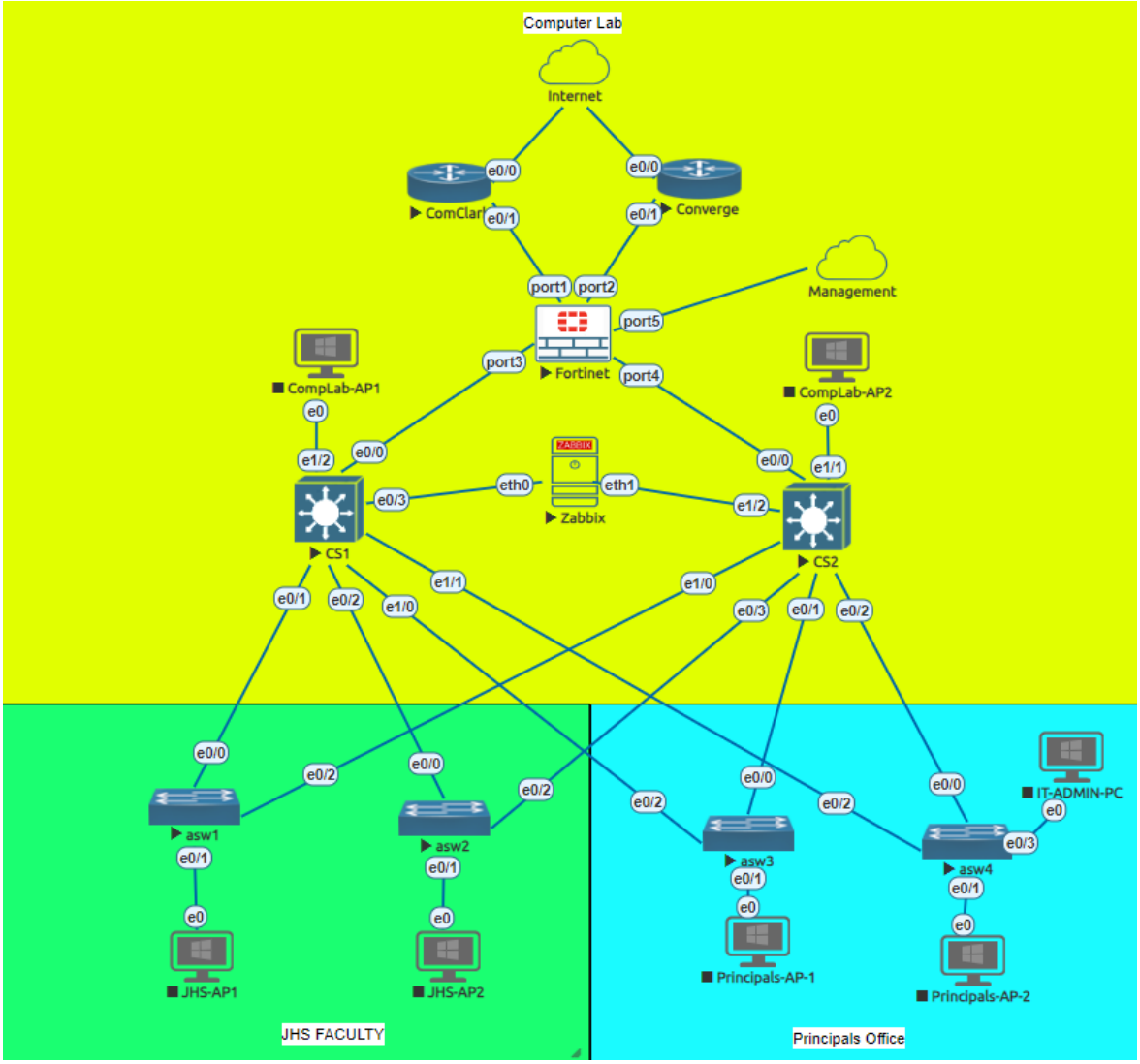


Appendix F
Current Network Topology

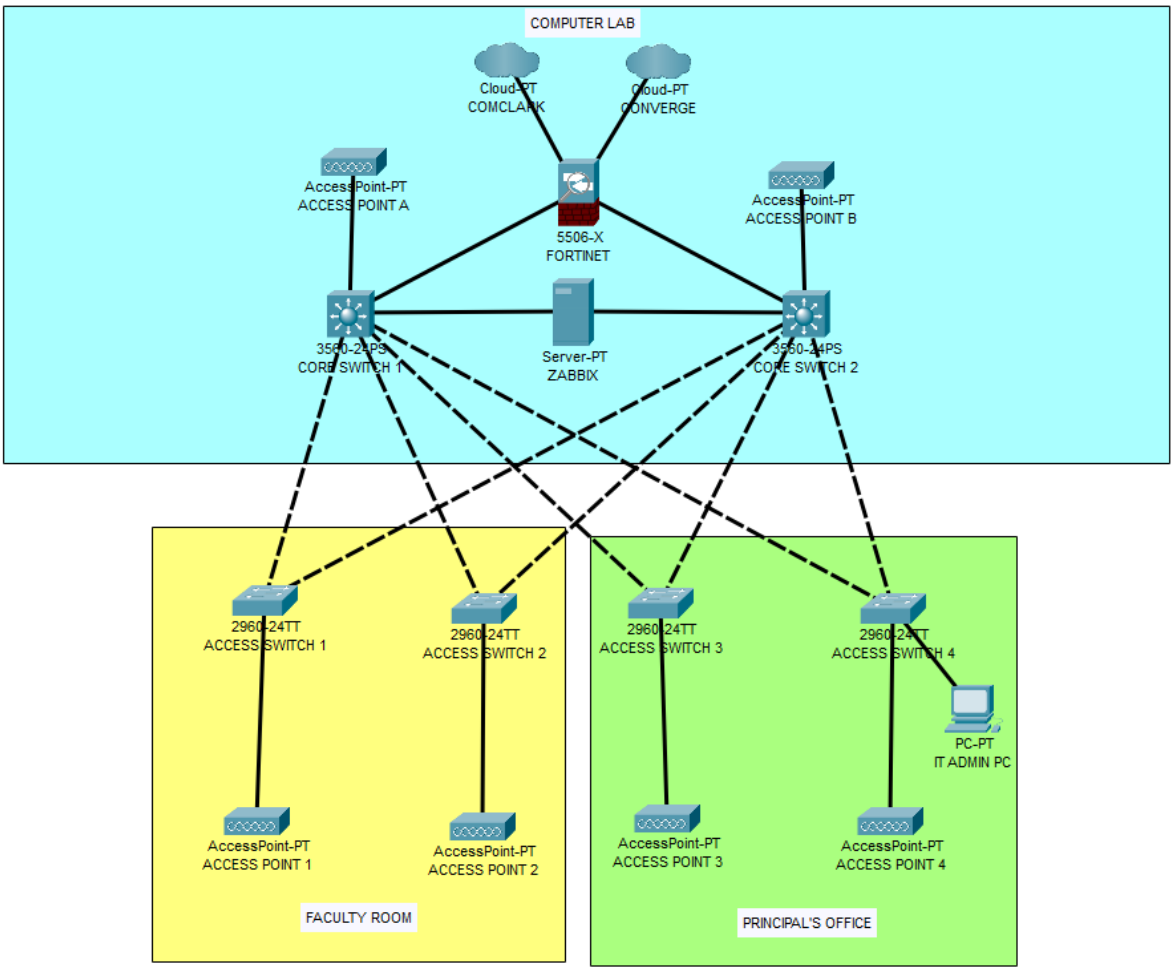




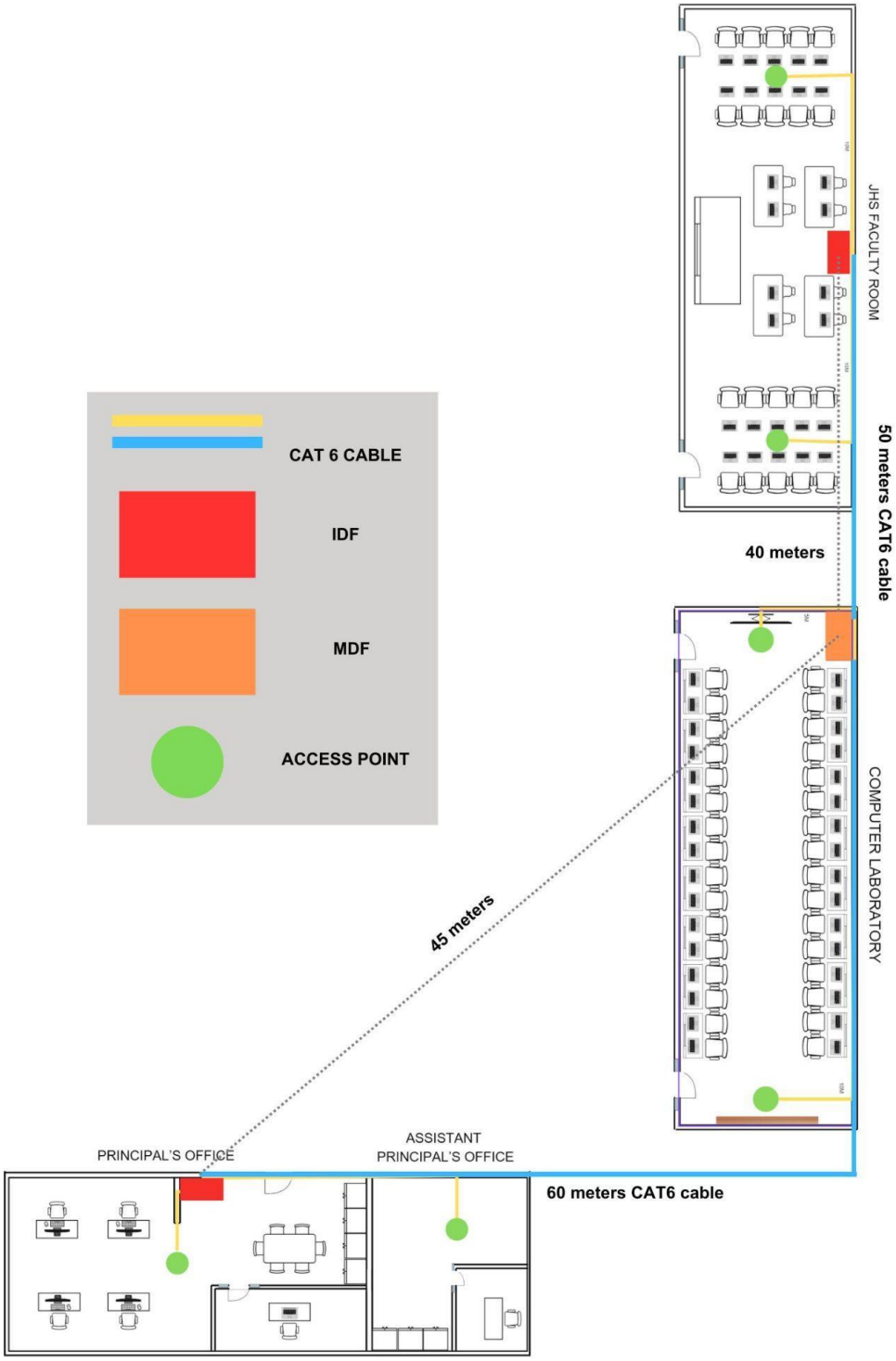
Appendix G
Proposed Logical Topology in EVE-NG

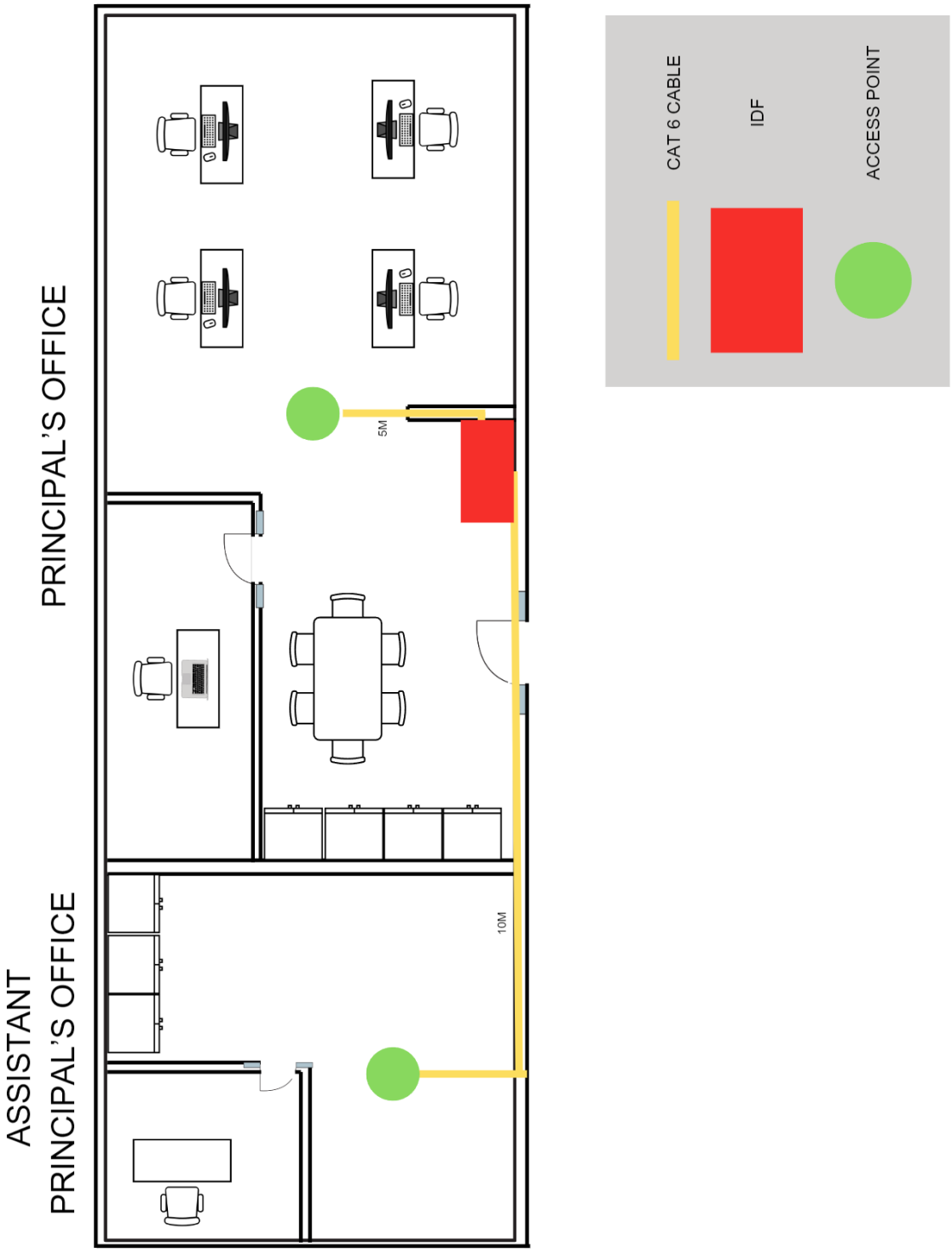


Appendix H
Proposed Logical Topology in Packet Tracer

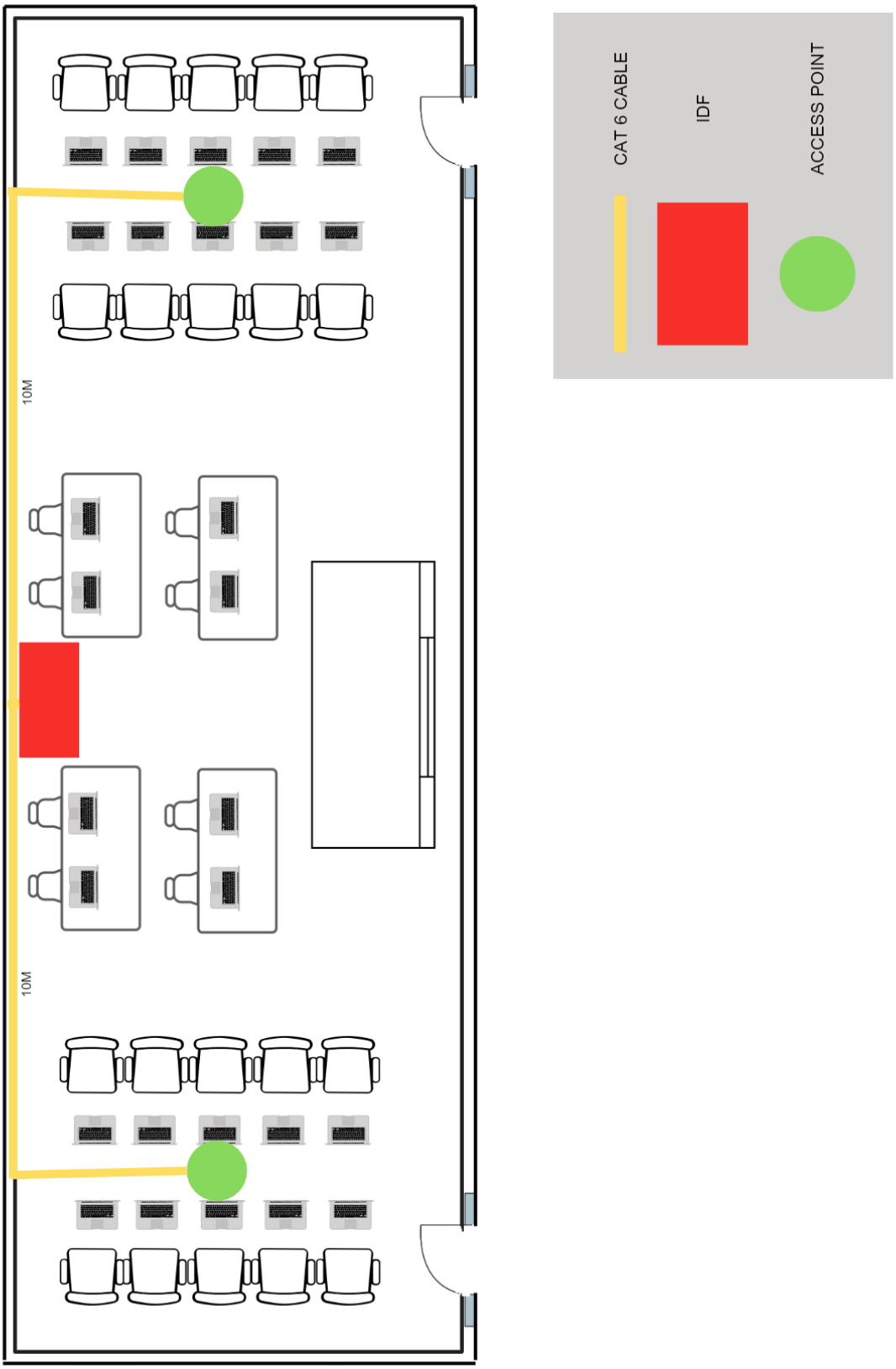


Appendix I
Proposed Physical Network Layout

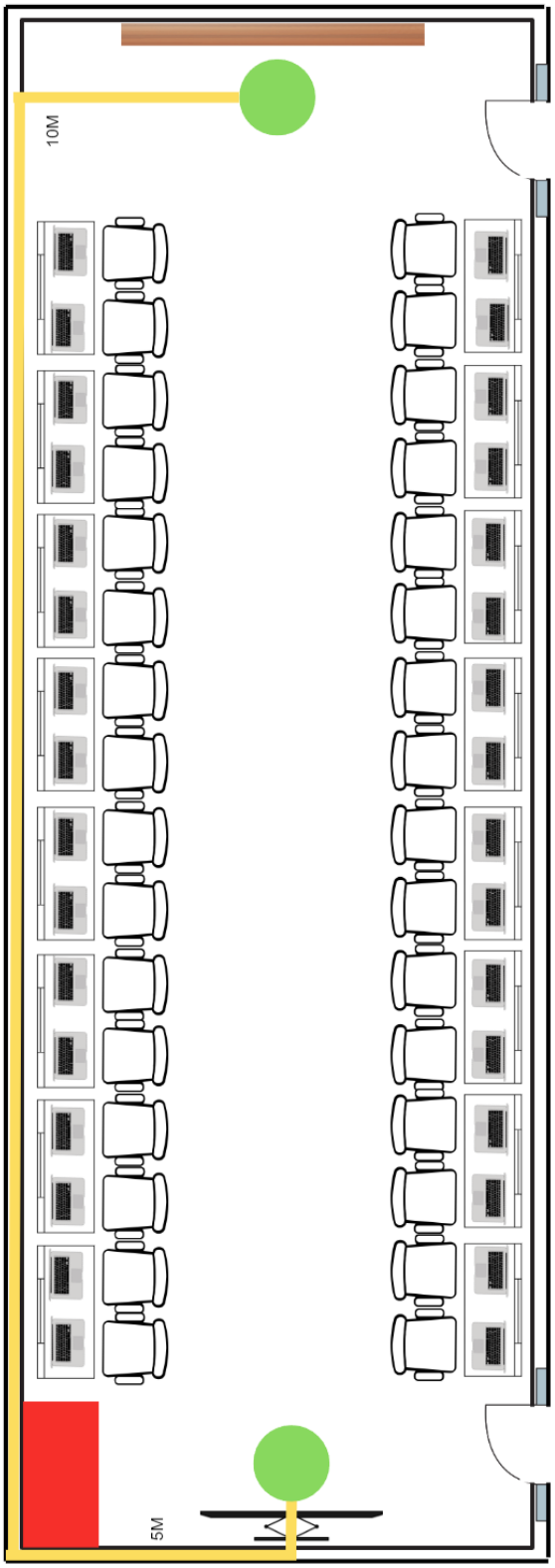


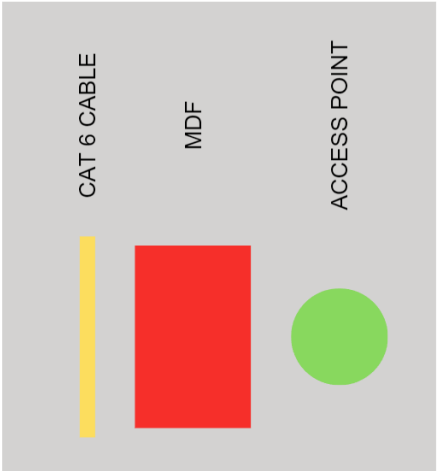

ASSISTANT
PRINCIPAL'S OFFICE
PRINCIPAL'S OFFICE
10M
5M
CAT 6 CABLE
IDF
ACCESS POINT

JHS FACULTY ROOM



COMPUTER LABORATORY





Appendix J
Implementation Plan

The procurement of network hardware is to be done before the commencement of physical installation, hence ensuring that all the equipment required is in place for deployment. The purchase entails two (2) Pro Max 16 POE core switches, four (4) Lite 16 POE distributor switches, four (4) U6+ access points, and one FortiGate firewall. The procurement process is to be done in the first phase of implementation to avoid any installation delays.

Order of Installation

1. Cabling and Network Infrastructure Planning – Installation of network cabling will be the initial step in physical implementation, as it is the core support of the entire network. This entails the planning of Ethernet cables, the installation of fiber optic connection, and planning of the structured cabling route to link the Main Distribution Frame (MDF) in the computer lab to the Intermediate Distribution Frames (IDFs) in the Junior High School faculty room and the principal's office. Cable management and cable labeling will be properly done at this point to facilitate maintenance and troubleshooting.

2. Electrical Work and Power Allocation – After cabling has been completed, electrical installation will be done to ensure Power over Ethernet (PoE) support for switches and access points. This will entail the review of power needs, provision of power redundancy for critical networking equipment, and the installation of required outlets or uninterruptible power supply (UPS) systems.

3. Deployment of Networking Equipment – After cabling and electrical infrastructure have been done, the installation and configuration of network equipment, including switches, routers, access points, and the firewall, will be done. VLAN segmentation, security features, and bandwidth management features will be done to ensure maximum performance and security.

4. Testing and Optimization – After the installation process is finished, a full range of stress and connectivity tests will be conducted using Zabbix monitoring tools in conjunction with EVE-NG simulations to ensure that all the equipment is working. Tuning will be performed based on the results of such tests to improve network stability and security.

Appendix K
Cost Analysis for Simulation and Proposed Devices

Cost Analysis for Simulation Devices

PHOTO	DEVICE	FEATURES	QUANTITY	PRICE
	C9300X-24HX-M	• Layer-3 • 40G/100G or 10G/25G modular uplink options on all models • mGig support • 1T/480G Dual Dedicated Hardware Stacking Ports 90W UPoE+ Support (802.3bt) StackPower in a ring topology supporting upto 4 switches	2	₱403,920.28
	C9300X-12Y-A	The C9300X-12Y-A is a Catalyst 9300 switch model by Cisco. This model comes with 12 ports of 25G/10G/1G SFP28 and modular uplinks. It is part of the Cisco Catalyst 9300 Series, which provides flexible deployment options, including small to medium-sized businesses, enterprise branches, and campuses.	4	₱262,873.29
	UBIQUITI U6 PLUS WiFi	WiFi 6 4 spatial streams 140 m² (1,500 ft²) coverage	6	₱8,200.00

	Access Point	300+ connected devices Powered using PoE GbE uplink		
	ALLAN Outdoor Cat6 300M Full Meter Outdoor UTP Cable CCA Cat6e Lan Cable	-Standard: Cat6 Ethernet cable -Support bandwidth up to 600Mhz -Support speed up to 1Gbps connector optimizes signal quality The Cat6 network Ethernet cable is made of 4 twisted-pair copper wires Universal compatibility	2	₱1,850
	Box of 100pcs RJ45 Connector Pass through cat6	cheap cost, solderless wiring and connector assembly, rapid custom cable production, easy insertion and removal, field assembly with basic tools, and on-site cable customization.	1	₱200
	FortiGate-60F Hardware plus 1 Year FortiCare Premium and FortiGuard Enterprise Protection	● All-in-one security: Firewall, antivirus, IPS, web filtering. ● High performance: Fast threat protection, SD-WAN capabilities.	1	₱54,824.71

		● Compact design: Desktop form factor. ● FortiGuard powered: Up-to-date threat intelligence. ● Strong connectivity: Multiple Gigabit Ethernet ports.		
			TOTAL	₱1,967,258.43

Cost Analysis for Proposed Devices

PHOTO	DEVICE	FEATURES	QUANTITY	PRICE
	UBIQUITI USW-PRO-Max-16-PoE Switch	A 16-port, Layer 3 Etherlighting™ switch with 2.5 GbE, PoE++ output, and versatile mounting options. Etherlighting™ ports that illuminate to indicate port location, speed/link, and native VLAN/network ● (4) 2.5 GbE PoE++ ports ● (12) GbE PoE+ ports ● (2) 10G SFP+ ports ● 180W total PoE availability ● Versatile desktop, wall, and rack** mounting Silent, fanless cooling system	2	₱32,150
	UBIQUITI USW-Lite-16-PoE Switch	A wall-mountable, 16-port, Layer 2 PoE switch with a fanless cooling system. zz ● (8) GbE PoE+, (8) GbE ports ● 45W total PoE availability Wall mountable	4	₱16,650
	UBIQUITI U6 PLUS WiFi Access Point	WiFi 6 4 spatial streams 140 m² (1,500 ft²) coverage 300+ connected	6	₱8,200.00

		devices Powered using PoE GbE uplink		
	ALLAN Outdoor Cat6 300M Full Meter Outdoor UTP Cable CCA Cat6e Lan Cable	-Standard: Cat6 Ethernet cable -Support bandwidth up to 600Mhz -Support speed up to 1Gbps connector optimizes signal quality The Cat6 network Ethernet cable is made of 4 twisted-pair copper wires Universal compatibility	2	₱1,850
	Box of 100pcs RJ45 Connector Pass through cat6	cheap cost, solderless wiring and connector assembly, rapid custom cable production, easy insertion and removal, field assembly with basic tools, and on-site cable customization.	1	₱200
	FortiGate-60F Hardware plus 1 Year FortiCare Premium and FortiGuard Enterprise Protection	● All-in-one security: Firewall, antivirus, IPS, web filtering. ● High performance: Fast threat protection, SD-WAN capabilities.	1	₱54,824.71

		● Compact design: Desktop form factor. ● FortiGuard powered: Up-to-date threat intelligence. ● Strong connectivity: Multiple Gigabit Ethernet ports.		
			TOTAL	₱238,825

Appendix L
IP Addressing Scheme

INTERFACE	SUBNET ADDRESS	HOST RANGE	SUBNET MASK
VLAN 10	192.168.10.1	192.168.10.2-192.168.10.254	255.255.255.0
VLAN 20	192.168.20.1	192.168.20.2-192.168.20.254	255.255.255.0
VLAN 30	192.168.30.1	192.168.30.2-192.168.30.254	255.255.255.0

VLANs	USER's
10	Admin
20	Teachers, Principal, Academic Staff
30	Students

Appendix M
Firewall Configuration

```
FortiGate-VM64-KVM # show system int

config system interface

  edit "port1"

  set vdom "root"

  set mode dhcp

  set allowaccess ping snmp

  set type physical

  set alias "WAN1"

  set lldp-reception enable

  set role wan

  set snmp-index 1

  next

  edit "port2"

  set vdom "root"

  set mode dhcp

  set allowaccess ping snmp

  set type physical

  set alias "WAN2"

  set lldp-reception enable

  set role wan

  set snmp-index 2

  next

  edit "port3"
```

```
set vdom "root"
set type physical
set snmp-index 3
next
edit "port4"
set vdom "root"
set type physical
set snmp-index 4
next
edit "port5"
set vdom "root"
set mode dhcp
set allowaccess ping https ssh http telnet fgfm
set type physical
set alias "MANAGEMENT"
set snmp-index 5
next
edit "port6"
set vdom "root"
set type physical
set snmp-index 6
next
edit "ssl.root"
set vdom "root"
set type tunnel
```

```
set alias "SSL VPN interface"
set snmp-index 7
next
edit "OUT"
set vdom "root"
set allowaccess ping https ssh snmp
set type switch
set device-identification enable
set lldp-transmission enable
set role lan
set snmp-index 9
next
edit "fortilink"
set vdom "root"
set fortilink enable
set ip 10.255.1.1 255.255.255.0
set allowaccess ping fabric
set type aggregate
set lldp-reception enable
set lldp-transmission enable
set snmp-index 8
next
edit "VLAN10"
set vdom "root"
set ip 192.168.10.1 255.255.255.0
```

```
set allowaccess ping https ssh snmp
set device-identification enable
set role lan
set snmp-index 10
set interface "OUT"
set vlanid 10
next
edit "VLAN20"
set vdom "root"
set ip 192.168.20.1 255.255.255.0
set allowaccess ping snmp
set device-identification enable
set role lan
set snmp-index 11
set interface "OUT"
set vlanid 20
next
edit "VLAN30"
set vdom "root"
set ip 192.168.30.1 255.255.255.0
set allowaccess ping snmp
set device-identification enable
set role lan
set snmp-index 12
set interface "OUT"
```

```
  set vlanid 30
  next
end
```

Appendix N
FortiGate Configuration

FortiGate-VM64-KVM
Dashboard
Network
Interfaces
DNS
Packet Capture
SD-WAN
Static Routes
Policy Routes
RIP
OSPF
BGP
Routing Objects
Multicast
Policy & Objects
Security Profiles
VPN
User & Authentication
System
Security Fabric
Log & Report
FORTINET
v7.0.0
SD-WAN Zones
SD-WAN Rules
Performance SLAs
Bandwidth
Volume
Sessions
port1
port2
Total
Create New
Edit
Delete
Interfaces
Gateway
Cost
Download
Upload
virtual-wan-link
SDWAN
WAN1 (port1)
1.1.1.1
0
1.19 kbps
1.24 kbps
WAN2 (port2)
2.2.2.2
0
902 bps
890 bps
Updated: 10:44:39
admin

Appendix O
Switch Configuration

Core Switch 1

```
Current configuration : 4705 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
!
hostname cs1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 daKYKG/09tp/TYVbvxlDi8/85nzz5u/yaMu4xzSWSiA
!
no aaa new-model
no ipv6 cef
ipv6 multicast rpf use-bgp
!
ip cef
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
!
!
!
!
!
!
!
```

```
!
!
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
 duplex auto
!
interface Ethernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
duplex auto
!
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
 duplex auto
!
interface Ethernet0/3
 switchport access vlan 10
 switchport mode access
 duplex auto
!
interface Ethernet1/0
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
 duplex auto
!
interface Ethernet1/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
 duplex auto
!
interface Ethernet1/2
 switchport access vlan 30
 switchport mode access
 duplex auto
!
interface Ethernet1/3
 duplex auto
!
```

```
interface Ethernet2/0
 duplex auto
!
interface Ethernet2/1
 duplex auto
!
interface Ethernet2/2
 duplex auto
!
interface Ethernet2/3
 duplex auto
!
interface Ethernet3/0
 duplex auto
!
interface Ethernet3/1
duplex auto
!
interface Ethernet3/2
 duplex auto
!
interface Ethernet3/3
 duplex auto
!
interface Ethernet4/0
 duplex auto
!
interface Ethernet4/1
 duplex auto
!
interface Ethernet4/2
 duplex auto
!
interface Ethernet4/3
 duplex auto
!
interface Ethernet5/0
 duplex auto
!
interface Ethernet5/1
 duplex auto
!
interface Ethernet5/2
 duplex auto
!
```

```
interface Ethernet5/3
 duplex auto
!
interface Vlan1
 no ip address
!
interface Vlan10
 ip address 192.168.10.2 255.255.255.0
!
!
no ip http server
!
!
!
!
snmp-server community public RO
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flowmon
snmp-server enable traps tty
snmp-server enable traps casa
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
snmp-server enable traps bgp
snmp-server enable traps dlsw
snmp-server enable traps isis
snmp-server enable traps msdp
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps slb real virtual csrp
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps vtp
```

```
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps isakmp policy add
snmp-server enable traps isakmp policy delete
snmp-server enable traps isakmp tunnel start
snmp-server enable traps isakmp tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps bfd
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps mvpn
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps syslog
snmp-server enable traps ethernet cfm alarm
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
!
control-plane
!
!
line con 0
 password 7 03550958
 logging synchronous
 login
line aux 0
line vty 0 4
 password 7 03550958
 login
!
end
```

Core Switch 2

```
Current configuration : 4666 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
```

```
service compress-config
!
hostname cs2
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 daKYKG/09tp/TYVbvxlDi8/85nzz5u/yaMu4xzSWSiA
!
no aaa new-model
no ipv6 cef
ipv6 multicast rpf use-bgp
!
ip cef
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
 duplex auto
!
interface Ethernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30
```

```
 switchport mode trunk
 duplex auto
!
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20
 switchport mode trunk
 duplex auto
!
interface Ethernet0/3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
 duplex auto
!
interface Ethernet1/0
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20
 switchport mode trunk
 duplex auto
!
interface Ethernet1/1
 switchport access vlan 30
 switchport mode access
 duplex auto
!
interface Ethernet1/2
 switchport access vlan 10
 switchport mode access
 duplex auto
!
interface Ethernet1/3
 duplex auto
!
interface Ethernet2/0
 duplex auto
!
interface Ethernet2/1
 duplex auto
!
interface Ethernet2/2
 duplex auto
!
interface Ethernet2/3
 duplex auto
```

```
!
interface Ethernet3/0
duplex auto
!
interface Ethernet3/1
 duplex auto
!
interface Ethernet3/2
 duplex auto
!
interface Ethernet3/3
 duplex auto
!
interface Ethernet4/0
 duplex auto
!
interface Ethernet4/1
 duplex auto
!
interface Ethernet4/2
 duplex auto
!
interface Ethernet4/3
 duplex auto
!
interface Ethernet5/0
 duplex auto
!
interface Ethernet5/1
 duplex auto
!
interface Ethernet5/2
 duplex auto
!
interface Ethernet5/3
 duplex auto
!
interface Vlan10
 ip address 192.168.10.3 255.255.255.0
!
!
no ip http server
!
!
!
```

```
!
snmp-server community public RO
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flowmon
snmp-server enable traps tty
snmp-server enable traps casa
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
snmp-server enable traps bgp
snmp-server enable traps dlsw
snmp-server enable traps isis
snmp-server enable traps msdp
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps slb real virtual csrp
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps isakmp policy add
snmp-server enable traps isakmp policy delete
snmp-server enable traps isakmp tunnel start
snmp-server enable traps isakmp tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps bfd
```

```
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps mvpn
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps syslog
snmp-server enable traps ethernet cfm alarm
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
!
control-plane
!
!
line con 0
 password 7 01425457
 logging synchronous
 login
line aux 0
line vty 0 4
 password 7 101F5B4A
 login
!
end
```

Access Switch 1

```
Current configuration : 4022 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
!
hostname as1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 daKYKG/09tp/TYVbvxlDi8/85nzz5u/yaMu4xzSWSiA
!
no aaa new-model
no ipv6 cef
ipv6 multicast rpf use-bgp
!
```

```
ip cef
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
 duplex auto
!
interface Ethernet0/1
 switchport access vlan 20
 switchport mode access
 duplex auto
!
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
 duplex auto
!
interface Ethernet0/3
 duplex auto
!
interface Ethernet1/0
 duplex auto
!
```

```
interface Ethernet1/1
 duplex auto
!
interface Ethernet1/2
 duplex auto
!
interface Ethernet1/3
 duplex auto
!
interface Ethernet2/0
 duplex auto
!
interface Ethernet2/1
 duplex auto
!
interface Ethernet2/2
 duplex auto
!
interface Ethernet2/3
 duplex auto
!
interface Ethernet3/0
 duplex auto
!
interface Ethernet3/1
 duplex auto
!
interface Ethernet3/2
 duplex auto
!
interface Ethernet3/3
duplex auto
!
interface Vlan10
 ip address 192.168.10.4 255.255.255.0
!
!
no ip http server
!
!
!
!
snmp-server community public RO
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flowmon
```

```
snmp-server enable traps tty
snmp-server enable traps casa
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
snmp-server enable traps bgp
snmp-server enable traps dlsw
snmp-server enable traps isis
snmp-server enable traps msdp
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps slb real virtual csrp
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps isakmp policy add
snmp-server enable traps isakmp policy delete
snmp-server enable traps isakmp tunnel start
snmp-server enable traps isakmp tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps bfd
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
```

```
snmp-server enable traps mvpn
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps syslog
snmp-server enable traps ethernet cfm alarm
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
!
control-plane
!
!
line con 0
 password 7 01425457
 logging synchronous
 login
line aux 0
line vty 0 4
 password 7 12485744
 login
!
end
```

Access Switch 2

```
Current configuration : 3579 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
!
hostname asw2
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 daKYKG/09tp/TYVbvxlDi8/85nzz5u/yaMu4xzSWSiA
!
no aaa new-model
no ipv6 cef
ipv6 multicast rpf use-bgp
!
ip cef
!
!
!
```

```
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30
switchport mode trunk
 duplex auto
!
interface Ethernet0/1
 switchport access vlan 20
 switchport mode access
 duplex auto
!
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
 duplex auto
!
interface Ethernet0/3
 duplex auto
!
interface Vlan10
 ip address 192.168.10.5 255.255.255.0
!
!
no ip http server
!
!
```

```
!
!
snmp-server community public RO
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flowmon
snmp-server enable traps tty
snmp-server enable traps casa
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
snmp-server enable traps bgp
snmp-server enable traps dlsw
snmp-server enable traps isis
snmp-server enable traps msdp
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps slb real virtual csrp
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps isakmp policy add
snmp-server enable traps isakmp policy delete
snmp-server enable traps isakmp tunnel start
snmp-server enable traps isakmp tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
```

```
snmp-server enable traps bfd
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps mvpn
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps syslog
snmp-server enable traps ethernet cfm alarm
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
!
control-plane
!
!
line con 0
 password 7 01425457
 logging synchronous
 login
line aux 0
line vty 0 4
 password 7 075E731F
 login
!
end
```

Access Switch 3

```
Current configuration : 4022 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
!
hostname as3
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 daKYKG/09tp/TYVbvxlDi8/85nzz5u/yaMu4xzSWSiA
!
no aaa new-model
no ipv6 cef
```

```
ipv6 multicast rpf use-bgp
!
ip cef
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
 duplex auto
!
interface Ethernet0/1
 switchport access vlan 10
 switchport mode access
 duplex auto
!
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
 duplex auto
!
interface Ethernet0/3
 duplex auto
!
interface Ethernet1/0
```

```
 duplex auto
!
interface Ethernet1/1
 duplex auto
!
interface Ethernet1/2
 duplex auto
!
interface Ethernet1/3
 duplex auto
!
interface Ethernet2/0
 duplex auto
!
interface Ethernet2/1
 duplex auto
!
interface Ethernet2/2
 duplex auto
!
interface Ethernet2/3
 duplex auto
!
interface Ethernet3/0
 duplex auto
!
interface Ethernet3/1
 duplex auto
!
interface Ethernet3/2
duplex auto
!
interface Ethernet3/3
 duplex auto
!
interface Vlan10
 ip address 192.168.10.6 255.255.255.0
!
!
no ip http server
!
!
!
!
snmp-server community public RO
```

```
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flowmon
snmp-server enable traps tty
snmp-server enable traps casa
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
snmp-server enable traps bgp
snmp-server enable traps dlsw
snmp-server enable traps isis
snmp-server enable traps msdp
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps slb real virtual csrp
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps isakmp policy add
snmp-server enable traps isakmp policy delete
snmp-server enable traps isakmp tunnel start
snmp-server enable traps isakmp tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps bfd
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
```

```
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps mvpn
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps syslog
snmp-server enable traps ethernet cfm alarm
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
!
control-plane
!
!
line con 0
 password 7 055A545C
 logging synchronous
 login
line aux 0
line vty 0 4
 password 7 01425457
 login
!
end
```

Access Switch 4

```
Current configuration : 3630 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
!
hostname asw4
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 daKYKG/09tp/TYVbvxlDi8/85nzz5u/yaMu4xzSWSiA
!
no aaa new-model
no ipv6 cef
ipv6 multicast rpf use-bgp
!
ip cef
!
```

```
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
 duplex auto
!
interface Ethernet0/1
 switchport access vlan 10
 switchport mode access
 duplex auto
!
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
 duplex auto
!
interface Ethernet0/3
 switchport access vlan 10
 switchport mode access
 duplex auto
!
interface Vlan10
 ip address 192.168.10.7 255.255.255.0
!
```

```
!
no ip http server
!
!
!
!
snmp-server community public RO
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flowmon
snmp-server enable traps tty
snmp-server enable traps casa
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
snmp-server enable traps bgp
snmp-server enable traps dlsw
snmp-server enable traps isis
snmp-server enable traps msdp
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps slb real virtual csrp
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps isakmp policy add
snmp-server enable traps isakmp policy delete
snmp-server enable traps isakmp tunnel start
snmp-server enable traps isakmp tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
```

```
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps bfd
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps mvpn
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps syslog
snmp-server enable traps ethernet cfm alarm
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
!
control-plane
!
!
line con 0
 password 7 101F5B4A
 logging synchronous
 login
line aux 0
line vty 0 4
 password 7 01425457
 login
!
end
```

Appendix P
Converge and Comclark Speed Test

Converge Speed Test

ComClark Speed Test

Appendix Q
IT Expert's Curriculum Vitae

Florante Antonio S. Alfonso
50, Lorong 40 Geylang,
Lobby 16, #03-49, The Sunny Spring,
Singapore, 398074
97540743/+63927-3774484
FIN #: G5213698P
duoazrael21@gmail.com

Professional Experience

Network Engineer, *Agape Enterprise PTE LTD,* *#03-01 NEON Building, 25 Tai Seng Avenue, Singapore, October 3, 2016 - Present*

- Level 2 Network Engineer that handles preparing, planning, designing, implementing, and maintaining network infrastructure offered to new and existing clients locally and overseas.
- Possesses a high level of expertise in Layer 2 network features including VLANs, spanning-tree, link-aggregation, and port security, as well as Layer 3 features like inter-VLANs, gateway redundancy (HSRP, VRRP, GLBP), routing protocols (OSPF, EIGRP, BGP), Quality of service (QoS), and Network Address Translation (NAT).
- Knowledgeable about Layer 4 features such as access-list (ACL), and VPN (client-server, site-to-site, DMVPN).

Network Systems Engineer, *Communication Services PTE LTD,* *#09-08, 55 North Serangoon Avenue 4, Singapore, October 20, 2011 - September 30, 2016*

- Troubleshooting, designing the network, data, and/or voice implementation for our existing clients, and creating or making proposals to meet the requirements of our new and/or potential new clients.
- Handles mostly Small-Medium Enterprise (SME) projects and sometimes extends work capabilities beyond my job title, when necessary, like project management and/or project planning to satisfy client needs whether locally or outside the country of Singapore.

Network Engineer, *Fujitsu WeServ Systems International,* *Bonifacio Global City, Taguig City, October 4, 2010 – October 5, 2011*

- Monitored and managed all the network and servers of our clients 24 hours a day, seven days a week using tools like Solarwinds.
- When a problem occurs, depending on the priority, we call the engineers directly and email the ticket using our ticketing tool Triole. For other priorities, tickets can be accomplished by email alone.

Contract: Network Systems Engineer, *Alsons/AWS Information Systems Incorporated*, *Ayala Avenue, Makati City, July 1, 2010 – September 30, 2010*

- Supported and fixed problems of clients concerning structured cabling, network (routers, switches, and wireless), and PABX.
- Provided technical advice to clients who need new implementation and/or upgrades in their organization.

Field Network Engineer, *Trends and Technologies Holding Incorporated*, *H.V. dela Costa Street, Makati City, June 2, 2008 – September 7, 2009*

- Troubleshooting /diagnosing and fixing network problems on clients, 24 hours a day, seven days a week as well as site-to-site troubleshooting using Cisco or Nortel equipment.
- Managed a large-scale LAN/WAN with a solid background in Cisco routers, switches, and layer 3 switches.
- Knowledge of VPNs, firewalls, VoIP, and associated protocols.

Technical Experience and Proficiency

Hands-on Network hardware/equipments

- Cisco equipment
- Alcatel-Lucent equipment
- HP Network equipment
- Stellar Wireless
- Mitel - Aastra 470 and Mitel Mobile Client

Hands-on Network Exposure/Configuration

- Routing and Switching
- Security
- Design
- Network Technologies (DMVPN, IPv6, EZVPN, etc)
- Wireless
- Structured Cabling

Resource Speaker and Facilitator

Facilitator: Cisco VoIP Technology
Holy Angel University
Angeles City, Pampanga
January 28, 2013

Speaker: Implementing Cisco IP Switch Network
Holy Angel University
Angeles City, Pampanga
August 23, 2012

Seminars/Trainings Attended

Alcatel-lucent Switch and Wireless Training
Alcatel-lucent Enterprise
#05-01/02, Technopark@Chaichee
750E, Chai Chee Road, Singapore

Building Scalable Cisco Internetworks (BSCI)
Trends.Net
H.V. Dela Costa st., Makati City
June 22 – 26, 2009

Ruckus Wireless Training
Comclark
99 Reliance Center, Brgy. Ugong
C-5 Road, Pasig City
September 23, 2010

Fluke Networks:
Certified Cabling Test Technician Associate
Holy Angel University
Angeles City, Pampanga
January 13, 2007 and January 22, 2007

Educational Attainment

Tertiary:
Bachelor in Computer Science
Holy Angel University
2004 - 2008

Character References

References Available Upon Request

I certify that the above information is true and correct to the best of my knowledge.

Florante Antonio S. Alfonso
Signature

_____
Date

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

BUSINESS DOCUMENT This document is intended for business use and should be distributed to intended recipients only.

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

BUSINESS DOCUMENT This document is intended for business use and should be distributed to intended recipients only.

JAN HENRYCK C. DIZON

#384 Burgos St., Cubcub, Capas, Tarlac City.

0949- 441 - 8791

Janhenryckdizon28@gmail.com

Personal Information

- ✓ Civil Status: Single
- ✓ Date of Birth: May 28, 1997
- ✓ Height: 5'9"
- ✓ Religion: Iglesia ni Cristo
- ✓ Language & Dialects: English, Tagalog

Character Reference

- Rhoda Vicente | Software Engineer at TIPCO | 09178633305
- Keannu Paul Brillante | Software Engineer at Accenture | 09261848617
- Randell Perez | Full-stack Web Developer at Shore360 | 09506562490
- Miguel Patrick Sugui | Technical Support Rep. at TaskUS | 09213822225

Objectives

To further enhanced my educational and professional skills in the field of IT and continue to help and contribute for the welfare of others and to maximize one's potential for self-fulfillment.

Educational Background

- **TERTIARY:**
  - **Tarlac State University**
  - Bachelor of Science in Information Technology
  - Romulo Blvd., Tarlac City
  - S.Y. 2013 – 2017
- **SECONDARY:**
  - **Dominican College of Tarlac**
  - Capas, Tarlac
  - S.Y. 2008 - 2013

Skills and Abilities

- Knowledgeable in using various programming languages such as Java, C#, C++, JavaScript, MySQL, HTML, CSS and PHP.
- Advance knowledge upon using Windows OS platform.
- Basic knowledge upon using MacOS X and Linux OS.
- Advance knowledge upon using various graphics and animation editing software such as Sony Vegas, Google SketchUp and Photoshop.
- Knowledgeable in configuring Cisco switches, routers and access points.
- Advance PC Hardware/Software troubleshooting knowledge.
- Basic knowledge in Virtualization software such as Hyper-V, vSphere and Virtual box.

Working Experience

- **JR. SYSTEMS ENGINEER/DEVELOPER & SYSTEMS SUPPORT:**
  - **YOKOHAMA TIRES PHILS. INC.**
  - January 10, 2018 – March 23, 2021
  - IE5 Clark Freeport Zone, Pampanga 2023, Philippines
- **DATABASE ADMINISTRATOR/SYSTEM ANALYST(RELIEVER):**
  - **NAMBAWAN SEAFOODS PNG LTD.**
  - December 10, 2017 – December 28, 2017
  - Portion 677, Busu Road, Malahang, Lae, Morobe Province, Papua New Guinea.
- **SOFTWARE DEVELOPER (OJT):**
  - **FILAM SOFTWARE AND TECHNOLOGY INC.**
  - 2017
  - Building 2519 D, Samat Street, Clark Freeport Zone, Angeles, Pampanga.

Trainings and Seminars

- **SAP PM TRAINING** (March-April 2019)
  - SAP maintenance/scheduling training
  - Yokohama Tires Phils. Inc.
- **AVANT SYSTEM TRAINING** (May 13, 2017 – December 02, 2017)
  - Avant System database and program training
  - TIPCO Compound.

I hereby certify that the above information is true and correct to the best of my knowledge and belief.

JAN HENRYCK C. DIZON
Applicant

Appendix R
Editor's Note

ENGLISH EDITING CERTIFICATION FORM

This is to certify that the undersigned has edited the final revised manuscript of this Research Output

SIMULATION OF A NETWORK INFRASTRUCTURE DESIGN FOR AMSIC INTEGRATED SCHOOL

prepared by

KAHLEL INIGO I. BALUYUT
SEAN MATTHEW C. BAUTISTA
CARL LOUIE G. DELOS REYES
JOSEPH R. DELOS REYES

and has found it complete and satisfactory with respect to grammar and organization as prescribed by the University Research Office of Holy Angel University

KIMBERLY P. LINTAG, MAELLT
Grammar Editor

March 25, 2025

Appendix S
University Plagiarism Certificate

HOLY ANGEL UNIVERSITY **UNIVERSITY RESEARCH OFFICE**

C E R T I F I C A T I O N

This certifies that the research paper entitled "**Simulation of a Network Infrastructure Design for Amsic Integrated School**" by Sean Matthew C. Bautista, Kahlel Iñigo Baluyut, Carl Louie Delos Reyes, and Joseph Delos Reyes, 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	15888
Final rate	7%

Certified by:

DR. RICHARD L. FIGUEROA
Director, University Research Office

Appendix T
Researchers' Curriculum Vitae

Kahlel Iñigo Baluyut
kahlelbaluyut.jobs180.com

PERSONAL INFORMATION

Birthdate: August 30, 2003
Civil Status: Single
Nationality: Filipino
Address: 443 Jesus Street, Poblacion Floridablanca Pampanga Pampanga, Central Luzon (Region III) 2006
Gender: Male

CONTACT INFORMATION

Mobile: 09297946812
Email: kahlel.baluyut@gmail.com

SKILLS

- Microsoft Office
- Computer Literate
- Adaptability
- Canva
- Java
- HTML

LANGUAGES

- Filipino
- English

EDUCATION

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

CERTIFICATIONS

2024
DevNet Associate

2024
CCNA Switching, Routing, And Wireless Essentials

2024
JavaScript Essentials 1

2023
CyberOps Associate

2023
CCNAv7 Introduction To Networks

2024
Simplilearn Introduction To Figma Course

2024
FreeCodeCamp Responsive Web Design

2024
CCNAv7 Enterprise Networking, Security, And Automation

2023
Linux Skills Level 1

2019
Introduction To IoT

SEMINARS

2024
1st Regional Blockchain Conference

2024
CYBER RESILIENCE IN THE AI ERA - EMPOWERING BUSINESS LEADERS AND DEVELOPING NEXT-GEN CYBERSECURITY P

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

Sean Matthew Cuizon Bautista

seanbautista2002.jobs180.com

OBJECTIVE

To join an organization that will give me an opportunity to enhance and share my knowledge, skills, and capabilities and earn a job that provides personal and professional growth that will lead to a successful long-term career relationship.

PERSONAL INFORMATION

Birthdate: August 27, 2002

Civil Status: Single

Nationality: Filipino

Address: B11 L2 Salem St. Villa Leoncia Subd. Angeles City, Central Luzon (Region III) 2009

Gender: Male

CONTACT INFORMATION

Mobile: 09612704364

Email: seanbautista2002@gmail.com

SKILLS

- **Computer Literate**
- **Interpersonal Skills**
- **Fast Typing**
- **Photo Editing**
- **Video Editing**

LANGUAGES

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

ACHIEVEMENTS

With Honors Grade 11 ABM 1st Semester

With Honors Grade 11 ABM 2nd Semester

With High Honors Grade 12 ABM 1st Semester

Dean's Lister 1st Semester 2021-2022

Dean's Lister 1st Semester 2023-2024

Dean's Lister 2nd Semester 2023-2024

EDUCATION

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

2021 May — **Senior High School Diploma**
Holy Angel University
Major: Business Management
Field of Study: Academic Track: Accountancy, Business & Management (ABM)

2019 Apr — **High School Diploma**
Holy Angel University
Field of Study:

CERTIFICATIONS

2024
JavaScript Essentials 1

2024
CCNAv7 Enterprise Networking, Security, And Automation

2024
DevNet Associate

2024
CCNAv7 Switching, Routing, And Wireless Essentials

2024
Responsive Web Design

2023
CyberOps Associate

2023
CCNAv7 Introduction To Networks

SEMINARS

2024
1st Regional Blockchain Conference

2024
CYBER RESLIENCE IN THE AI ERA - EMPOWERING BUSINESS LEADERS AND DEVELOPING NEXT-GEN CYBERSECURITY PR

2024
The 10th International Conference On Next Generation Computing 2024

2021
Professional Development Workshop

View more of my ResumèLink at http://seanbautista2002.jobs180.com

Carl Louie Goriding Delos Reyes

CLdelosreyes.jobs180.com

OBJECTIVE

To obtain a Network administrator-related position where I can apply my expertise in troubleshooting, network configuration, and network security to ensure the efficiency of Information Technology infrastructure. I aim to contribute to the organization's technology growth while continuously expand knowledge in network technologies.

PERSONAL INFORMATION

Birthdate: March 12, 2003

Civil Status: Single

Nationality: Filipino

Address: Lot 8 Block 23 1st Street Plaridel II Barangay Amsic Angeles City Pampanga Angeles City, Central Luzon (Region III) 2009

Gender: Male

CONTACT INFORMATION

Mobile: 09993592735

Email: carllouiedelosreyes1225@gmail.com

SKILLS

- **Computer Proficiency**
- **Teamwork**
- **Communication**
- **Adaptability**
- **Time Management**

LANGUAGES

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

EDUCATION

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

2021 May
Senior High School Diploma
Holy Angel University
Major: GAS
Field of Study: Academic Track: General Academic Strand (GAS)

2019 Apr
High School Diploma
Holy Angel University
Field of Study:

CERTIFICATIONS

2024
CCNAv7 - Switching, Routing, And Wireless Essentials

2024
CCNAv7 - Enterprise Networking, Security, And Automation

2024
DevNet Associate

2023
CCNAv7 - Introduction To Networks

2023
CyberOps Associate

2021
Introduction To IoT

SEMINARS

2025
3rd Regional Cybersecurity Conference

2024
Blockchain Campus Conference

2023
PHP SQL - The Backbone Of Thousands Of Databases And The Dynamics Of Websites

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

Joseph Rosquita Delos Reyes

OBJECTIVE

Dedicated and adaptable, I am seeking a role where I can leverage my knowledge in Information Technology, with a focus on innovative hospitality skills. My recent completion of NetAcad has equipped me with relevant skills and expertise, and I am excited to contribute to your organization's success while growing professionally and personally.

PERSONAL INFORMATION

ResuméLink:	Seph12k.jobs180.com
Address:	Angeles City, Central Luzon (Region III)
Birthdate:	March 12, 2003
Civil Status:	Single
Gender:	Male
Nationality:	Filipino
Email:	josephdelosreyes12345@gmail.com
Mobile:	09199830369

EDUCATION

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

2021 May — **Senior High School Diploma**
Holy Angel University
Major: GAS
Field of Study: Academic Track: General Academic Strand (GAS)

2019 Apr — **High School Diploma**
Holy Angel University

SKILLS

- **Microsoft Office Proficiency**
- **Basic Troubleshooting**
- **Technical Support**
- **Cisco Networking**
- **Routing And Switching**

CERTIFICATIONS

2024 — **CCNAv7 - Switching, Routing, And Wireless Essentials**

2024 — **CCNAv7 - Enterprise Networking, Security, And Automation**

2024 — **DevNet Associate**

SEMINARS

2025 — **3rd Regional Cybersecurity Conference**

2023 — **PHP SQL - The Backbone Of Thousands Of Databases And The Dynamics Of Websites**

2024 — **Blockchain Campus Conference**

View more of my ResumèLink at http://Seph12k.jobs180.com