Proceedings of the 4th South American Conference on Industrial Engineering and Operations Management, Lima, Peru, May 9 - 11, 2023

A Proposed Wireless Campus Network Planning and Design of Salapungan Elementary School

Nicholai Ethan Enriquez Bolus, Danica Villate Calma, and Jinky Anne Espino
College of Computer Science, Angeles University Foundation
Angeles City, Philippines

Professor Benedict M. Guarin
Faculty of College of Computer Science, Angeles University Foundation
Angeles City, Philippines

Abstract

The existing network topology of Salapungan Elementary School poses issues in their networking activities with inconsistencies within their network. The aim of the study was to propose a wireless network topology that will provide solutions and consistencies without first applying it to the campus. This study focuses on the use of proper and necessary routing protocols to improve the overall performance of the network topology of Salapungan Elementary School. The testing of the network was done in Cisco Packet Tracer, where it involved the analyzation and management of the devices and connection of the proposed network topology. In addition to the implementation in Cisco Packet Tracer, the researchers utilized the Top-Down Design in aiding them with the needs for their study. The findings indicate in the proposal that with standardized routing protocols such as Static Routing, DHCP, OSPF, VLAN and HSRP, the wireless network drastically improved. Further, the use of WPA2 amongst the Access Points serves as an extra layer of security in the network. It becomes evident that it expanded the network's availability, provided a network failover solution and easier manageability.

Keywords

Networking Configuration, Access Points, WPA2 network security, Cisco Packet Tracer, Network Topology

1. Introduction

The impact of how technology is utilized by the hour and day highlights the progress of our society. Global access to the internet made the achievement of continuous innovation possible. Macabale et al. (2020) stated that the internet has played a vital role in teaching and collecting information and communication in academic institutions. This reinforces the substantial role of campus networks in the educational setting.

The emergence of campus networks in academic institutions plays a pivotal role in this period of Information Technology. This new age has made campus networks just as important as our everyday essentials. Many educators, students, and researchers adapted to modernizing how to pass information and acquire study materials to complete their tasks (Ahmed et al. 2021). Both educators and students can use campus networks for various purposes, including teaching, learning, e-learning, supervising, publishing results, and connecting with external users (Somasundaram and Chandran 2018). Thus, networks contribute not only in one area of life but almost everywhere, notably in educational organizations. The researchers have observed that one of the predominant issues in the Salapungan Elementary School faces lies in the lack of wireless network security, which is crucial for a wireless campus network. In addition, the existing network does not have a failover solution plan and network documentation, which affects the availability and manageability of the network. This study focuses on giving practical solutions to the problems mentioned earlier. Through this study, a suitable wireless campus network design will be developed along with the necessary wireless network security and protocols based on the school's needs. The network designed in this study is an improved network of the school's existing network, which will be mainly simulated using Cisco Packet Tracer version 8.2.

1.1 Objectives

The general goal of this study is to re-design the current network structure of Salapungan Elementary School, while prioritizing the wireless security and performance. The designed wireless campus network proves to tackle most problems experienced by the school's faculty. It is then specified into specific objectives in order to provide solutions for the problems Salapungan elementary School is experiencing. The first specified objective is to re-design the network structure of the school. Secondly, is to develop a logical and physical network design for the client. Thirdly, is to apply a wireless network security protocol for encryption of the data and enhancement of security for the network. Lastly, is to implement an internet redundancy for the network high-availability. The researchers assessed the existing network and proposed the best viable option for the client and its networking devices they currently have in inventory.

2. Literature review

This chapter primarily introduces different scholarly works from both foreign and local research. Those that are included in this chapter helps in broadening the researcher's knowledge that are important and similar to this study.

According to Musril et. al. (2020), Campus Area Network consists of multiple Local Area Networks (LAN) that forms a connected network inside a campus. This type of network requires a connection of buildings, labs, and area that make learning and studying more convenient among students and faculties. These networks may be connected by either routers and switches and produce a network. The biggest thing to note is that Campus Area Network may both be wired and wireless. The purpose of utilizing a Campus Area Network may vary but primarily tackles most modern educational requirements (Kagai 2020). Institutions are putting in more investments into an enhanced network to strive for excellence in learning for their students. This opens up the potential to provide effective high- quality services to campuses without compromising network connectivity and performance.

The expected services have set a bar in most facilities in campus networks (Borah and Sharma 2020). This puts a heavy emphasis and reliability on having strong connection in Campus Area Networks. The network design must be readily be available at all times over the campus in order to keep the users satisfied at all times. Furthermore, to promote clarity among all users in a campus network, it must be safe, reliable and available.

In recent years, WLAN has been one of the most increasingly popular network technologies for connecting to the local resources and the internet (Saeed and Kolberg 2018). Nowadays, most of our gadgets and devices (i.e., phones, laptops, and tablets) contain Wireless Network Interface Controller (WNIC) that can connect and access wirelessly through all Access Points. According to Michel et. al. (2020), WLANs have become wide stream due to their low implementation cost, reliable communication, easy implementation technology, and high flexibility. In addition, WLANs' benefits greatly assist teachers and students in e-learning as accessing content in the internet, learning at a comfortable setting and travelling in buildings are all done with ease. WLAN's introduces new content into classrooms and prove to aid the challenges that traditional teaching methods faces. Michel et. al. (2020) also specified that the sharing of academic resources that are catered to students who are exposed to outdated materials and mundane lessons are now more able to enjoy learning because of the direct channel a WLAN provides from teacher-to-student. Furthermore, faculties are now provided with a gateway in which they can access real time resources anywhere. And with the emergence of COVID-19, the need for WLAN has become a priority and e-learning has transcended into becoming the new norm.

Heightened network security within an academic infrastructure is a must since most of the data contained within an institution are the personal data of students and faculties. Educational institutions are trusted to protect its users, yet an inadequate network security infrastructure might compromise their safety (Osowski 2018). Especially now with the increasing number of devices utilizing a school's network because of digitalized on-site curriculums, it poses an increasing threat to educational institutions

Educational Institutions are a common target for hackers because nowadays, faculty and staff alike data are no longer contained within tangible reach. These entities can now be stored within an institution's system. This can open up the risk of data exploiters utilizing third-party software to perform Data Theft since the specified data contained within these academic institutions include sensitive and personal details such as addresses and names. Cybercriminals may utilize this kind of information for a number of purposes, such as selling it to third parties or using it as leverage in negotiations (Osowski 2018). It is only rational that improvements to security are not only desired, but prioritized as managing the safety of campus networks becomes increasingly crucial due to their importance (Wang 2020).

Many users are unaware of the wireless network's security state, or how susceptible it is to hacking attempts from outside cyber criminals (Rahman and Ali 2018). A wireless security protocol sets the foundation on how a network should be secured. Various protocols such as Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and Wi-Fi Protected Access 2 (WPA2) are intended to achieve wireless security. These protocols all achieve encryption and authentication in a wireless network system, but are broken down on which is the best suitable protocol for the network requirements (Rana et al. 2021).

Strong security standards in both personal and business contexts are enhanced with WPA2 (Stoilov 2020). Stoilov states that all require 802.11i standard tasks, are carried out via WPA2. With the comparison between WEP and WPA, WPA2 substantially offers more security than the other two. The study done by Stoilov (2020), where the experiment tested on which securities could protect, authenticate, and encrypt the passphrases, WPA2 exhibits its improvement on user experience and dependency against security threats in Wi-Fi. In addition, WPA2 also provided data security for private and data-sensitive Wi-Fi network settings.

WPA2 paired with Dynamic Host Configuration Protocol (DHCP), leverages the potency of the security for a network. This applies an almost impenetrable network security by cybercriminals. According to Moris (2022), DHCP is by far the popular choice for dispersing IP Addresses for users due to its cheaper and effortless deployment. It is given that DHCP does not need manual configuration as it automatically sets an IP Address to the devices that join a network. The security aspect of using DHCP is questionable as it is possible for a hacker to invade the network through an unauthorized DHCP server. Thus, having WPA2 with DHCP becomes the most potent duo in providing a safe and secure network for its users. The counterpart of DHCP, which is static IP, does not change until the administrator does so, and can become costly. Moris states that Static IP holds additional charges since ISPs are forced to give away an IP Address. Additionally, Static IP Addressing proves more complex to configure and can become a daunting task for an administrator. Moreover, Static IP addressing is hard to configure when there are vast number of devices connected to a network. Thus, DHCP proves to be the best viable option for networks that need access to the internet. The effortless transition of plugging in a device to the network has is one of the primary satisfactory uses amongst users globally.

Lepaja et. al. (2018), has concluded that WPA2 (Wi-Fi Protected Access 2) has become some of the best security measures to add in a network system. Their study demonstrates a set of controlled throughputs to be tested with a handful of other security measures (WEP, WAP, WAP2). Lepaja et. al. (2018), described that WPA2 have disabled security scheme and provides tougher security level. The results justify that WPA2 delivers average throughputs in a more consistent matter without getting in the way of delivering data to the client and servers. Moreover, WPA2 provides the best security without significantly degrading the throughput performance.

According to Shanmugam and Malarkodi (2019), a network connection is a necessity as faculty gather information for the students' materials. This leaves no room for failure for IT Coordinator to keep a constant network connection in their institutions. Therefore, the network must be accessible at all times for faculty in order to meet the requirements for the students. In addition, Shanmugam and Malarkodi emphasized that if a network lacks availability, the campus will face challenges that will result in problems hindering the ability for teachers to provide e-learning tools for students and reduce their productivity.

According to Alam et. al. (2018), to overcome network unavailability and connection failures, an organization's network should employ Hot Standby Routing Protocol (HSRP). The Hot Standby Router Protocol offers a technique that is intended to facilitate non-conservative IP traffic failover in circumstances where a network or device may fail. While planning a network, it is very important to make sure that data transfer is secured, cost of operation and maintenance is low, and that the link between users and facilities are continuously open. Alam et. al. (2018) also stated that by using HSRP protocol, connection loss will not occur while all networking devices are communicating and are connected within each other. With the provisions of prioritizing network availability, the campus network opens the gateway for future development in instructing, research, collaboration with other institutions, and in general solidifying the strength of the school (Macabale et al. 2020).

According to Wu et. al. (2018), a network's task is to provide the basic operating platform, variety of services from internet applications so that information may be delivered in a timely and accurate manner. Each school network's infrastructure design and execution need to be thoroughly scrutinized and investigated, in order to improve management level and teaching methods. The characteristics of the build of a network infrastructure must be technical, advanced and simple to achieve vital aspect of education, as well as higher education for skilled employees and labor pools (Ran 2020).

A conventional wireless network is planned and developed based on the maximum capacity of its resources, without disrupting the users' traffic and network load (Liu et. al., 2020). Ensuing that the network's performance cannot be altered to accommodate the service adjustments. Liu et. al. (2020) also stated that a network must be compatible with its design protocols so that its new functions would prevent having an influence on older network components and terminals. Moreover, a network must be capable of adapting to any changes unless really necessary to do so. Its capabilities should either horizontally or vertically adapt to what the services are needed for an organization. The plan of designing a complete network must meet the goal of meeting various and unique service requirements of an institution (Kafle et. al. 2018).

In order to develop networking and Internet of Things (IoT) simulations, students can use Cisco Packet Tracer; a proprietary multi-platform program from Cisco, without the requirement for hardware or a network that already exists (Finardi 2018). Cisco Packet Tracer was built to give networking students or professionals the hands-on experience without the need for a network infrastructure and long arduous hardware setups. The application allows users the ability to incorporate realistic debugging tools and teaches how to diagnose network-related issues. In addition, Cisco Packet Tracer provides an extension of hardware and cabling options to enable students to construct networks ranging from very simple to complex. The use of Cisco Packet Tracer is nearly identical to implementing a network in real life (Al-hamarneh 2021). Cisco Packet Tracer users interact with the devices in the software similarly to how a person would in real time. The dynamic functions in Cisco Packet Tracer allows all of these activities on a network for a network administrator. Moreover, the configurations on connecting a device are the same as how a person would do it on their network devices in real time.
According to Enoch et al. (2019), utilization of Cisco Packet Tracer is a must for the deployment of a secure network on institutions globally. Their study allowed them to implement routing protocols such as Dynamic Host Configuration Protocol (DHCP), Network Address Translation (NAT), inter-VLAN Routing, Wi-Fi Protected Access 2 (WPA2), and Hot Standby Router Protocol (HSRP). Cisco Packet Tracer provided them the tools that allowed them to create, configure and simulate their proposed design and showcase their idea for their institution. It also allowed them to test network connectivity and verified the correct configurations on their chosen protocols. Cisco Packet Tracer not only stresses the significance of using its software but also captured the needed analyzation and designing of a secured network topology. In addition, the built-in mechanisms for developing a secured network in Cisco Packet tracer were seamless and aided in exhibiting the optimized performance of the researchers' proposed network design (Enoch et al. 2019).

3. Methods

This chapter explains the procedure and the analysis that were gathered during the study. It covers the project design, data instrumentation, and data analysis plan.

3.1 Project Design

The researchers used a framework called Top-Down Network Design. The methodology assisted the researchers in assessing and reviewing the existing network topology into proposing a network plan to maximize the client's needs. The Top-Down Network Design is complex yet simp method in which network administrators deploy and configure the network for security, redundancy, and performance. In this study, the Top-Down Network design explained the process of proposing a network topology for Salapungan Elementary School.

Below will explain the processes the researchers forego for this proposal:

1. **Analyze Requirements** - The researchers interviewed the IT Coordinator of Salapungan Elementary School and analyzed the situation and problems of the network. The information gathered was used to base the needs, requirements and solutions for the wireless network design.

2. **Develop Logical Design** - A logical topology is developed as well as the selection of proper configurations and security planning.

3. **Develop Physical Design** - The selection of specific technologies and devices, such as routers, cables, switches, and access points for the campus network was done in this phase**.**

4. **Testing, Optimizing and Documenting Network Design** - This final phase includes the testing of the configurations and simulation of the proposed wireless network. Issues encountered with the performance during the testing were optimized and updated in the documentation.

4. Data Collection

The researchers gathered data through these methods:

- **Interview** - This method consists of face-to-face interview with the IT Coordinator, wherein a set of questions were asked by the researchers regarding the problems, needs, recommendations, and improvements for the study. Consequently, the researchers were able to gain an insight in order to support their study and understand what needs to be worked on. To specify the date of the interview, it was conducted on the date of September 16th, 2022.

- **Existing Data** - The existing campus network of the Salapungan Elementary School was collected and was provided by the IT Coordinator. Thus, it was used as a basis and a blueprint in distinguishing the improvements and issues of the network system.

- **Internet Research** - The researchers utilized the Internet to understand and gather information in regards to their study. Moreover, the vast resources of the Internet hold the major details to further support the study and provide a new path in improving and designing a wireless network system.
- **Survey** - A survey was conducted for the IT Coordinator, and other networking professionals to identify their satisfaction and recommendations from the proposed wireless network.

4.1 Data Analysis

Based on the interview, one of the problems that Salapungan Elementary School experiences is the inconsistency and slow connection to their existing campus network. Mr. Josell A. Hernandez, IT Coordinator of Salapungan Elementary School, describes the network system to be inefficient, lacking in security and poor manageability. The faculty experiences the inability to have internet connection in the times they need to finish their tasks or access and download learning materials. The IT Coordinator further detailed that he was only able to set up extra ranges for their network without assigning proper configurations and security protocols. The IT Coordinator stated that the best place to start for the improvements, is to begin with the network design, set up basic security, and expand availability. Moreover, the IT Coordinator specified that there are 8 buildings on campus, 5 routers, 1 switch, 2 ISP (65 MBPS and 15 MBPS), 4 Access Points, and 23 teachers that are using their personal laptops across the network. Thus, the researchers proposed to design a wireless campus network to improve the overall performance, enhance security and availability. The simulation was done in Cisco Packet Tracer to determine how the proposed campus network design will perform. The researchers applied the Likert Scale System to the responses from the respondents. Table 1 presents the details of the Likert Scale

WHERE: **WM** = Weighted Mean
w = Number of each category, **f** = Number of respondents in each category, **N** = Total number of responses

Table 1. Likert Scale Weighted Mean

Rate	Verbal Interpretation	Score Range
5	Strongly Agree	4.50 - 5
4	Agree	3.50 - 4.49
3	Neutral	2.50 - 3.49
2	Disagree	1.50 - 2.49
1	Strongly Disagree	1.0 - 1.49

FORMULA: $WM = \frac{\Sigma wf}{N}$

5. Results & Discussion

This chapter presents the result of the study. This includes the discussion of the proposed network topology and interpretations of the topology.

5.1 Discussion

To check the connectivity within the wireless devices connected to the Access Points across the wireless campus network, the IT Coordinator can use the command “ping -t 8.8.8.8” as it will show the connection from the ISP. This command can be done across all wireless network devices via Command Prompt as shown on Figure 1.

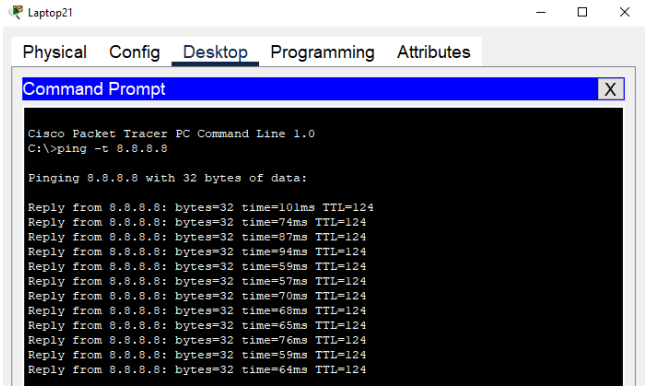

Figure 1. Device Successful Pin

And to verify that a network redundancy is set up and is working across all wireless devices in the wireless campus network. The IT Coordinator can use the command “tracert 8.8.8.8”. This command traces the route the internet travels within the topology of the network. If the command displays closely similar to what the example below displays. Then its trace route is complete and should display the IP Address of the Modem. (The IP Address of the Modem below is the 4th trace with the IP 209.200.201.2). Figure 2 shows the tracing route from the command prompt.

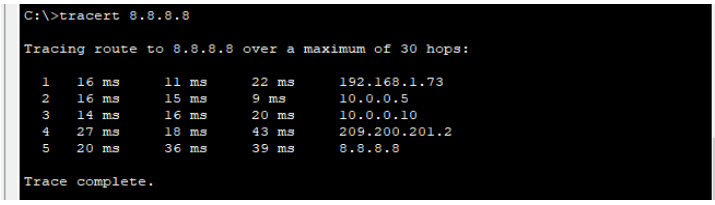

Figure 2. Command Prompt Trace

5.2 Graphical Results

The researchers' proposed wireless campus network design aims to supply the solutions to what the users are currently experiencing and the necessary changes based from the existing network**.** The following are the proposed topology diagrams and the necessary devices that would help in visualizing the proposed wireless network infrastructure. Figure 3 presents the whole topology of the network.

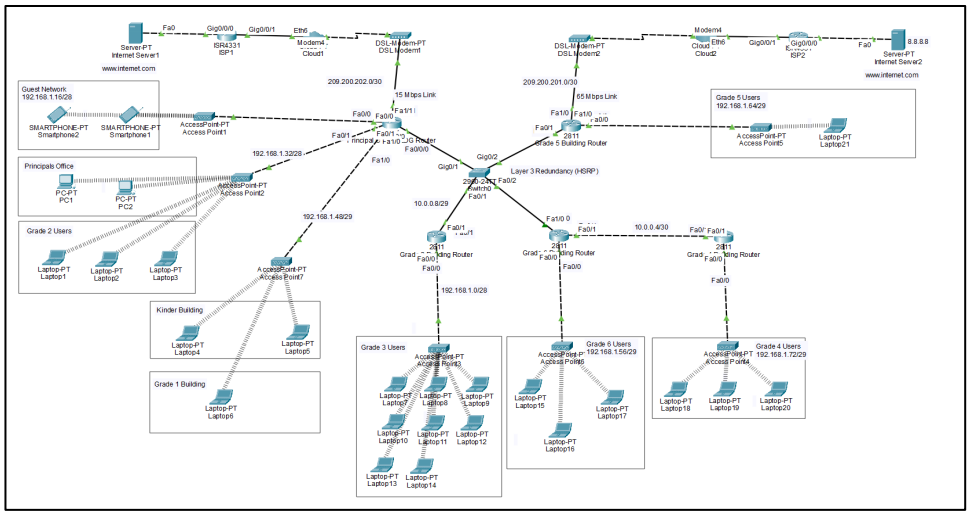

Figure 3. Logical Topology Diagram: Proposed Wireless Campus Network of Salapungan Elementary School

Figure 4 presents Layer 1 of the topology. The internet and cloud servers as well the ISP are present in this layer.

Figure 4. Logical Topology Diagram (Layer 1): Proposed Wireless Campus Network of Salapungan Elementary School

Figure 5 presents Access points 1,2 and 7 and also the devices that are connected within this layer of the topology. Under this area of the topology are the following: The principles office, Kinder building, Grade 1 building, Users from Grade 2 and a guess network.

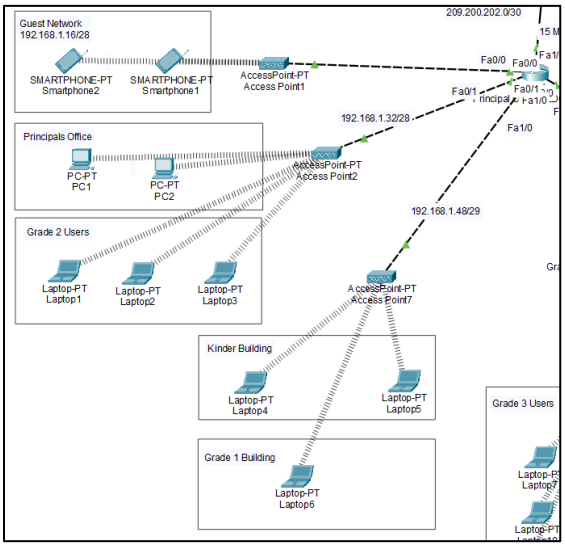

Figure 5. Logical Topology Diagram (Access Points 1,2,7): Proposed Wireless Campus Network of Salapungan Elementary School

Figure 6 presents Access points 3, 4 and 6 as well as the devices that are connected within this layer of the topology. The devices connected on this layer are for users from Grades 3, 6 and 4.

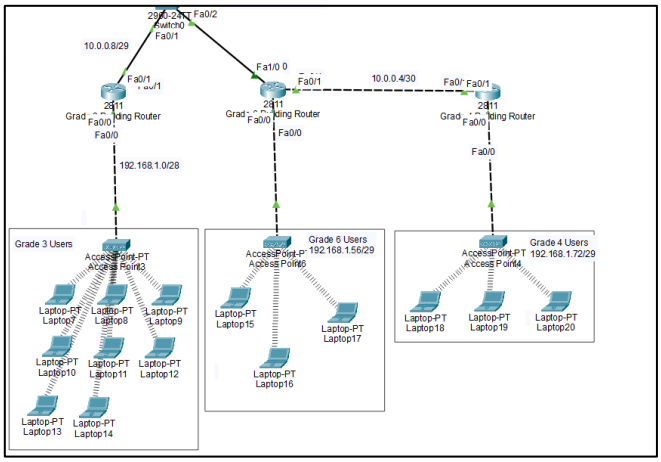

Figure 6. Logical Topology Diagram (Access Points 3, 4, 6): Proposed Wireless Campus Network of Salapungan Elementary School

Figure 7 presents Access Point 5. In this layer of the topology, the access point is for Grade 5 users.

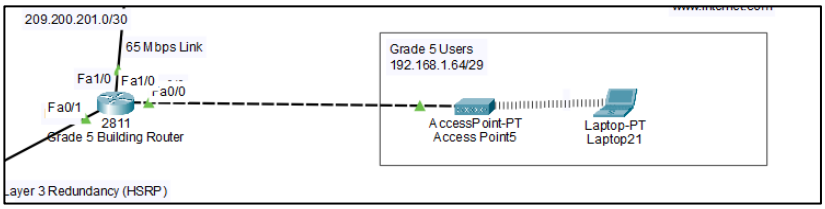

Figure 7. Logical Topology Diagram (Access Point 5): Proposed Wireless Campus Network of Salapungan Elementary School

5.3 Proposed Improvements

This research is intended for those who will conduct future researches on wireless campus networks. The researchers believe that there is more that can be improved in the upcoming future. The comments and recommendations taken from the survey done by the networking professionals have suggested:

- To add a security policy to ensure safe data and file transferring.
- Set a captive portal for faculties in order for them to not manually ask the IT Coordinator to provide them the Wi-Fi passwords.
- Implement Network and Host-based firewalls to mitigate viruses and possible cyberattacks.
- Integrate inventory and network monitoring system.

5.4 Validation

The aim of the study is to propose a wireless campus network structure of Salapungan Elementary School while providing improved network availability, enhanced security and manageability. The proposed design provided real-life applicable solutions to combat the inability to have consistent connection, assigned proper configurations to maximize capabilities of their existing network, and the expansion of their network across the buildings. Throughout the development of the proposal, the researchers met with the IT Coordinator multiple times in order to obtain the necessary information. Then the information obtained was utilized and assessed to transpire best suited solutions for Salapungan Elementary School's network specifications. The researchers utilized and implemented the proposed wireless campus network through Cisco Packet Tracer.

The researchers have conducted a series of tests and simulations in Cisco Packet Tracer and primarily focused on providing the solution to the observed network analysis of Salapungan Elementary School. In addition, a survey was carried out to obtain a degree of opinions from networking professionals about the proposed wireless campus network. From the survey, the respondents generally agreed that the proposed wireless campus network provided the practical solutions and improved the network's high-availability, security, and manageability.

6. Conclusion

This study presents a wireless campus network designed based on the needs and requirements of Salapungan Elementary School. By implementing standardized routing protocols such as Static Routing, DHCP, OSPF, VLAN and HSRP, the wireless network drastically improved. These expanded the network's availability, provided a network failover solution and easier manageability. The IT Coordinator approved and is open to implement the proposed wireless campus network of Salapungan Elementary School, given that the financial restriction and time is no longer an issue. The proposal demonstrated that the right configurations and protocols were implemented properly in order to meet the requirements and demands of Salapungan Elementary School's wireless network. As a result, the networking professionals survey forms came out positive and the findings gathered, weighted to the mean of 4.67 to 5.00, shows that the respondents Strongly Agree and satisfied with the improvements offered by the proposed wireless campus network.

References

Ahmed, A. H., Al-Hamadani, A., & Mokhaled, N. Designing a secure campus network and simulating it using Cisco packet tracer, 2021. Available: https://doi.org/10.11591/IJEECS.V23.I1.PP479-489, 2021.

Alam, T., & Hamid, K.Implementation of Dynamic Multipoint VPN over IPsec for Secure Enterprise Network (Doctoral dissertation, IIUC Central Library). and Computer Science, vol. 23, no. 1, pp. 479–489, 2018. Available: https://doi.org/10.11591/ijeecs.v23.i1.pp479-, 2018.

Alhamarneh, Raed. Improve Security in Smart Cities Based on IoT, Solve Cyber Electronic Attacks with Technology by using Packet Tracer. *International Journal of Network Security & Its Applications*, vol. 13, 2021. 10.5121/ijnsa.2021.13605, 2021.

Borah, A., & Sharma, B. (A Survey on Remote Diagnostic of Campus Network using IoT devices.

DHCP vs Static IP: What's the Difference? | FS Community, 2022. Knowledge. Available: https://community.fs.com/blog/dhcp-vs-static-ip-differences.html, 2020.

Enoch, J., Orike, S., & Ahiakwo, C. Design and Simulation of a Secured Enterprise Network for Faculty of Engineering, Rivers State University. *Computer Engineering and Intelligent Systems, 2019*. https://doi.org/10.7176/CEIS/10-5-04, 2019.

Finardi, A. *IoT Simulations with Cisco Packet Tracer*, 2018.

Kafle, V. P., Fukushima, Y., Martinez-Julia, P., Miyazawa, T., & Harai, H. Adaptive Virtual Network Slices for Diverse IoT Services. *IEEE Communications Standards Magazine*, vol. 2, no. 4, pp. 33–41, 2018. Available: https://doi.org/10.1109/MCOMSTD.2018.1800018, 2018.

Kagai, F. K. ICT Infrastructure for Campus Big Data: Network, Storage and Security Design and Implementation, 2019. https://doi.org/10.13140/RG.2.2.13175.88481, (2019)

Lepaja, S., Maraj, A., Efendiu, I., & Berzati, S. The impact of the security mechanisms in the throughput of the WLAN networks. 2018 7th Mediterranean Conference on Embedded Computing (MECO), 2018. Available: https://doi:10.1109/meco.2018.8406067, 2018.

Liu, L., Shafin, R., Chandrasekhar, V., Chen, H., Reed, J., & Zhang, J. C. Artificial Intelligence-Enabled Cellular Networks: A Critical Path to Beyond-5G and 6G. IEEE Wireless Communications, pp. 1–6, 2020. doi:10.1109/mwc.001.1900323, 2020.

Macabale, N. A., Naagas, M. A., & Palaoag, T. D. IPv6 campus transition: A central Luzon State University case study. *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 3, pp. 1167–1175, 2020. Available: https://doi.org/10.11591/EEI.V9I3.2173, 2020.

Michel, E., Journals, I., Djomadji, D., Petmegni, M., Steve, D., & Ekonde, S. M. *WLAN simulations using Huawei eNSP for e-laboratory in engineering schools*. Vol. 15, no. 2, pp. 47–70, 2020. Available: https://doi.org/10.9790/2834-1502014770, 2020.

Musril, Antoni H., Sri, Artika F., Derta, S., Darmawati, G., & Okra, R. Quality of Service EIGRP Routing Protocol on Campus Area Network. *Journal of Physics: Conference Series*, vol. 1779, no. 1, 2021. https://doi.org/10.1088/1742-6596/1779/1/012005, 2021.

Naagas, M. A., Mique, E. L., Palaoag, T. D., & dela Cruz, J. S. Defense-through-deception network security model: Securing university campus network from DOS/DDOS attack. *Bulletin of Electrical Engineering and Informatics*, vol. 7, no. 4, pp. 593–600, 2018. https://doi.org/10.11591/EEI.V7I4.1349, 2018.

Osowski, K. *The Importance of Network Security & Planning in Educational Institutions | Kentik Blog,* 2018. Available:https://www.kentik.com/blog/the-importance-of-network-security-planning-in-educational-institutions/, 2018.

Rahman, A., & Ali, M. Analysis and Evaluation of Wireless Networks by Implementation of Test Security Keys. Emerging Technologies in Computing, pp. 107–126, 2018. Available: https://doi:10.1007/978-3-319-95450-9_9, 2018.

Ran, D. Design and Planning of University Campus Network. Journal of Physics: Conference Series, vol. 1533, pp. 022109, 2020. Available: https://doi:10.1088/1742-6596/1533/2/022109, 2020.

Rana, M. E., Abdulla, M., & Arun, K. C. Common Security Protocols for Wireless Networks: A Comparative Analysis. *Proceedings of the 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021)*, vol. 4, pp. 632–638, 2021. Available: https://doi.org/10.2991/AHIS.K.210913.080, 2021.

Saeed, A., & Kolberg, M. Towards optimizing WLANs power saving: novel context-aware network traffic classification based on a machine learning approach. *IEEE Access*, vol. 7, pp. 3122–3135, 2019. Available: https://doi.org/10.1109/ACCESS.2018.2888813, 2019.

Shanmugam, T., & Malarkodi, B. Analysis of campus network management challenges and solutions. *Proceedings of the 2019 TEQIP - III Sponsored International Conference on Microwave Integrated Circuits, Photonics and Wireless Networks, IMICPW 2019*, pp. 312–316, 2019. Available: https://doi.org/10.1109/IMICPW.2019.8933236, 2019.

Shanmugam, T., & Malarkodi, B. Analysis of Campus Network Management Challenges and S/olutions. 2019 TEQIP III Sponsored International Conference on Microwave Integrated Circuits, Photonics and Wireless Networks (IMICPW), 2019. Available: https://doi:10.1109/imicpw.2019.8933236, 2019.

Somasundaram, S., & Chandran, M. A Simulation based study on Network Architecture Using Inter-VLAN Routing and Secure Campus Area Network (CAN). *Article in International Journal of Computer Sciences and Engineering,* 2018. Available: https://d/oi.org/10.26438/ijcse/v6i3.111121, 2018.

Stoilov, E. P. An overview of the recent standards and security technologies for wireless local area networks 22. *Proceedings of University of Ruse*, 2020.

Wang, B. *Journal Pre-proof Safety intelligence as an essential perspective for safety management in the era of Safety 4.0: From a theoretical to a practical framework,* 2020. Available: https://doi.org/10.1016/j.psep.2020.10.008, 2020.

Wu, Q., Zeng, Y., & Zhang, R. Joint Trajectory and Communication Design for Multi-UAV Enabled Wireless Networks. IEEE Transactions on Wireless Communications, vol. 17, no. 3, pp. 2109–2121, 2018. Available: https://doi:10.1109/twc.2017.2789293, 2018.

Biographies

Nicholai Ethan Enriquez Bolus is an undergraduate student from Angeles University Foundation, currently undertaking B.S. in Information Technology program. His interest's best lines up with Networking and overlooking network systems.

Danica Villate Calma is an undergraduate student from Angeles University Foundation under B.S. in Information Technology program. Her interest's best describes QA and Networking.

Jinky Anne Espino is an undergraduate student from Angeles University Foundation under B.S. in Information Technology program. Her interest's best describes Businesses Administration and Networking.