





# Crafting a Network Plan for a Microfinancing Establishment and Its Branch Network through Virtual Private Network (VPN) Implementation

Erielle DC. Bitbit, Mark Anthony B. Gampoy, Therese S. Ricafort, Rojelyn D. Tinio,

Racquel L. Pula\* , Rodibelle F. Leona, Cris Norman P. Olipas 

*College of Information and Communications Technology, Nueva Ecija University of Science and Technology, Philippines*

## Article Information

### Suggested Citation:

Bitbit, E.D.C., Gampoy, M.A.B., Ricafort, T.S., Tinio, R.D., Pula, R.L., Leona, R.F. & Olipas, C.N.P. (2023). Crafting a Network Plan for a Microfinancing Establishment and Its Branch Network through Virtual Private Network (VPN) Implementation. *European Journal of Theoretical and Applied Sciences*, 1(3), 441-448.  
DOI: [10.59324/ejtas.2023.1\(3\).43](https://doi.org/10.59324/ejtas.2023.1(3).43)

### \* Corresponding author:

Racquel L. Pula  
e-mail: [racquelpula@gmail.com](mailto:racquelpula@gmail.com)

## Abstract:

This study successfully designed a network plan incorporating a Virtual Private Network (VPN) for Kasipag Microfinancing Incorporated (KMI). Employing a developmental research design approach and following the network development life cycle stages of planning, analysis, design, and simulation, the researchers evaluated the feasibility of the network design for implementation in KMI. The findings strongly recommend KMI to proceed with the implementation of the designed network plan that includes a VPN, as it offers significant benefits and advantages. Implementing a VPN in KMI's network infrastructure will greatly enhance network security and enable secure remote access to valuable resources, which is particularly crucial in today's digital landscape emphasizing remote work and data privacy. The thorough simulation of the network plan confirms its feasibility and ensures KMI will have a reliable and efficient network infrastructure. Additionally, the implementation of the network plan will provide KMI with a

competitive edge by enabling seamless communication and streamlined data transfer between branches. This will enhance collaboration, improve operational efficiency, and increase overall organizational effectiveness. The cost analysis conducted by the researchers guarantees that the project remains within budget, offering KMI a clear breakdown of expenses for informed decision-making. In conclusion, the recommended implementation of the network plan incorporating a VPN will empower KMI with improved network security, secure remote access, and a competitive advantage in the microfinancing industry. By embracing these advancements, KMI can foster growth, productivity, and success in the ever-evolving digital landscape.

**Keywords:** *Developmental Research, NDLC, Network Plan, VPN.*

## Introduction

Kasipag Microfinancing Incorporated (KMI), known for its mission to provide financial assistance with lower interest rates and longer payment periods, has grown significantly since its establishment as a family business in 2015.

KMI recognized the barriers faced by small businesses due to a lack of capital. Traditional loans proved to be inaccessible and expensive. In response, KMI introduced a revolutionary idea—loan sharing among client groups to guarantee repayment and enable access to much-



needed funds for small business investment. With this concept, KMI quickly gained prominence in both urban and rural areas, paving the way for the dawn of KASIPAG Microfinancing, Inc.

With 54 branches spread across North and Central Luzon, including provinces like Nueva Ecija, Bulacan, Pampanga, and Batangas, KMI aims to continue providing assistance, creating new programs for progress, and enhancing the quality of life for individuals in need. KMI's vision is to become synonymous with Microfinancing Services, not only in Central Luzon but also throughout the Philippines, by consistently offering financial assistance while promoting integrity, hard work, and sound financial management.

To further streamline operations and promote efficient communication, it is imperative to connect the three branches of KMI—San Antonio, San Jose, and Guimba—using a Virtual Private Network (VPN). This study aims to leverage VPN technology to establish secure connections, safeguard data, and reduce the time required for submitting reports to the main branch.

By implementing a VPN, KMI will create a protected network connection between the computers used in each branch. VPNs are highly effective in ensuring privacy and security online, as they encrypt internet traffic and prevent unauthorized access. This added layer of protection will make it significantly more challenging for hackers, governments, or internet service providers to monitor or manipulate data.

Moreover, utilizing VPN technology with IPsec (Internet Protocol Security) encryption enables KMI to safeguard sensitive information, including financial transactions, medical records, and corporate communications. This level of security is crucial for both KMI employees and clients, ensuring the safe transfer of data and faster, more efficient transactions.

In summary, by designing a network plan that incorporates a Virtual Private Network (VPN), KMI will not only enhance connectivity between

its branches but also fortify the security of their data and streamline their reporting processes. This network infrastructure will empower KMI to continue its mission of providing financial assistance while maintaining the highest standards of integrity, hard work, and sound financial management for the betterment of individuals' lives.

### Importance of VPN Technology in Enhancing Network Security

In Alam et al.'s (2018) study, the focus was on enhancing the availability and remote access of secure enterprise network infrastructure. They utilized dual hub dual DMVPN, implementing the DMVPN technique and employing the hot standby routing protocol (HSRP) to overcome network failures. Through simulations and packet captures, they demonstrated the efficacy of DMVPN technology with HSRP protocols in meeting the demand for availability, providing faster and more efficient operation, and ensuring a safer and reliable network infrastructure.

Muc et al. (2020) emphasized the need for modern network technologies that enable secure remote access to company IT resources, considering the rise in remote work. They highlighted the cost and data security concerns associated with cloud services and VPS. Encrypted VPN tunneling emerged as a cost-effective and secure alternative, allowing devices at remote locations to securely connect to a company's local network and access its resources as if physically connected.

Santoso et al. (2021) discussed the implementation of VPN site-to-site using L2TP and IPsec protocols. Their aim was to improve data communication in organizations while addressing the vulnerability of intranet networks to wiretapping. Through performance analysis and security testing, they demonstrated the successful design and configuration of L2TP and IPsec VPNs, establishing secure connections and providing enhanced network security.

Ezra et al. (2021) conducted a review focusing on the design of an IP security VPN. They explored the use of VPNs as a means to bypass censorship and access geographically restricted

services. Their work presented an IP security VPN layout that utilized virtual connections to securely transmit packets over a public network. The study aimed to ensure secure enterprise access and overcome access restrictions imposed by encrypted communication.

Thiara (2021) explained the significance of VPNs in establishing virtual networks over the Internet, connecting internal networks of different company branches. The author emphasized the importance of VPNs in ensuring the secure transmission of sensitive company data, highlighting the confidentiality, authentication, and integrity provided by VPNs. The study discussed various VPN protocols, such as IPsec, TLS, and SSTP, and highlighted overlay and peer-to-peer models for VPN implementation. Specific tunneling protocols, such as IPsec and DMVPN, were also mentioned.

Damanik (2021) proposed a Data Network Security Configuration for Business Growth, focusing on the use of private networks to optimize network services and applications. The study provided solutions for businesses with limited bandwidth and rapid deployment requirements, utilizing VPN architecture and mobile network connectivity. VPN tunneling protocols such as EOIP and SSTP were explored, and VLAN Bridging was employed for virtualization schemes on WAN connectivity.

In an explorative study by Veroniek (2021), the mental models of corporate VPNs among experts and non-experts were examined. The study found partial alignment in high-level technical understanding while observing diverging views on VPN usage parameters. The need for accurate mental models, even among experts, was highlighted to ensure secure VPN usage. The findings led to recommendations for practitioners, including training interventions, improved communication, and the development of standardized guidelines for VPN implementation and usage.

These articles collectively demonstrate the importance of VPN technologies in enhancing network security, enabling remote access, and ensuring the confidentiality and integrity of data

transmission. The studies highlight various VPN protocols, techniques, and configurations that contribute to the development of secure and reliable network infrastructures for enterprises.

### The Need to Conduct the Study

One potential research gap in relation to crafting a network plan for Kasipag Microfinancing Incorporated (KMI) and its branch network through VPN implementation could be the lack of specific guidelines or best practices for implementing VPNs in the context of microfinance institutions. While VPNs are widely used for secure network communication, their implementation and configuration can vary depending on the specific needs and requirements of an organization. Microfinance institutions, such as KMI, have unique operational and security considerations that may differ from other industries.

Therefore, conducting research to identify and develop specific guidelines or best practices for implementing VPNs in the context of microfinance institutions could fill this research gap. This research could involve studying the specific challenges and requirements of microfinance institutions, such as data confidentiality, transaction security, and network scalability, and then formulating recommendations for VPN implementation that address these specific needs.

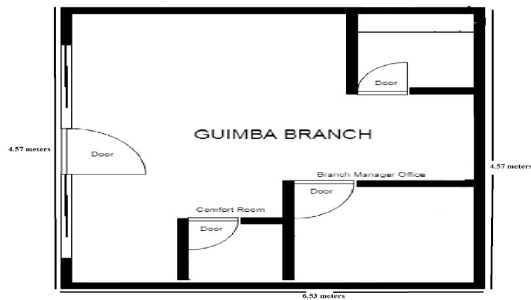
By providing tailored guidelines for VPN implementation in microfinance institutions like KMI, this research could assist in crafting an effective network plan that optimizes security, efficiency, and scalability. It would contribute to the development of standardized practices that can be applied across similar organizations, ensuring the successful deployment and operation of VPNs within the microfinance sector.

### Materials and Methods

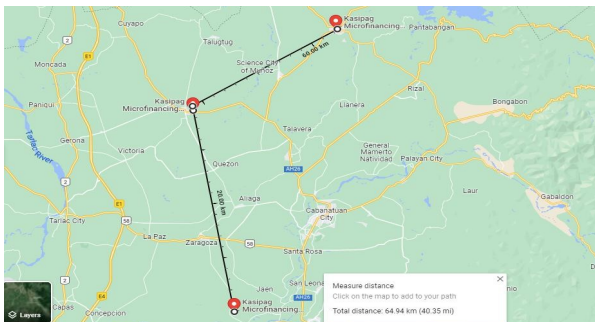
This study employed a developmental research design in which the researchers designed and crafted a network plan for KMI. In the past, several studies utilized this research design and







**Figure 4. Floor Dimension of KMI Guimba Branch**



**Figure 5. Distance between Branches**

Furthermore, the researchers specifically focused on analyzing the implementation of VPN. They assessed how VPN would function within the network infrastructure and its compatibility with the organization's requirements. This analysis aimed to ensure that the VPN implementation would meet the desired objectives and provide secure and reliable connectivity between the main branch and the selected branches. Figures below depict the floor dimensions of the area and the distances, which proved beneficial for conducting this study.

In addition to analyzing floor dimensions and distance, the researchers also examined the cost associated with the project implementation. Table 1 presented the proposed budget breakdown for establishing the network.

### Design Stage of NDLC

In this stage, the researchers designed the logical layout and the physical layout. The logical and physical layout are crucial in designing network plans as they ensure efficient network operation,

effective management, enhanced security, optimal resource allocation, and scalability.

**Table 1. Proposed Cost of Devices**

QTY	DEVICE	COST	UNIT COST
3	Router	₱529.00	₱1,587.00
3	Switch	₱3,500.00	₱10,500
15	Computer	₱8,000.00	₱120,000.00
150	Rj45	₱ 5.00	₱750.00
150m	Cable wire	₱1,820.00	₱1,820.00
4	Printer	₱8,300.00	₱33,200.00
1	File Server	₱9,959.00	₱9,959.00
<b>Total:</b>			<b>₱177,816.00</b>

The logical layout defines the network's architecture and communication paths, allowing for optimal data flow and improved network performance. It also enables effective network management and troubleshooting, reducing downtime and disruptions. Moreover, logical layouts facilitate the implementation of security measures such as network segmentation and virtual private networks (VPNs). Figure 6 shows the logical layout designed by the researchers.

### Simulation Stage of NDLC

In the simulation stage of the NDLC, the researchers actively tested the designed network and observed its performance using simulation software. They utilized a simulation software to assess how the network operated and identify any potential issues. Additionally, they developed a configuration and set-up procedure to ensure a systematic implementation process for the network. This procedure was carefully crafted to guarantee that the network implementation followed a structured and organized approach.

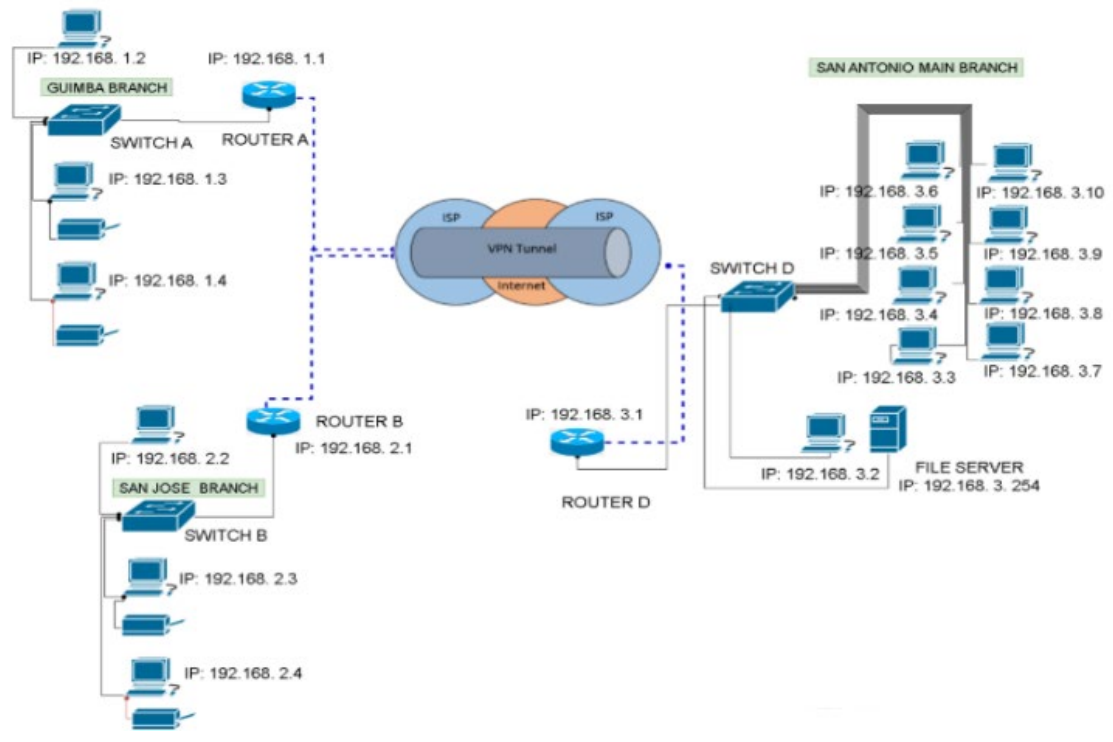


Figure 6. Logical Layout



Figure 7. Physical layout

## Conclusion and Recommendations

In conclusion, the researchers successfully designed a network plan that implemented a VPN for KMI. The researchers utilized a developmental research design approach to systematically develop the project, following the stages of the network development life cycle. They planned, analyzed, designed, and simulated the network design and determined its feasibility for implementation in KMI, providing them with significant benefits and advantages.

Based on the conclusion of the study, it is recommended that KMI proceed with the implementation of the designed network plan incorporating a VPN. The systematic approach followed in the network development life cycle ensures a well-planned and analyzed network infrastructure that can effectively meet the organization's needs.

By implementing a VPN, KMI can enhance its network security and enable secure remote access to its resources. This will be particularly beneficial in today's digital landscape, where remote work and data privacy are paramount. The designed network plan has been thoroughly simulated and found to be feasible, providing KMI with a reliable and efficient network infrastructure.

Furthermore, the implementation of the network plan will offer KMI a competitive advantage, enabling seamless communication and data transfer between branches. It will promote collaboration, streamline operations, and improve overall efficiency within the organization. The cost analysis conducted by the researchers ensures that the project remains within budget and provides a clear breakdown of expenses.

## Acknowledgement

The researchers would like to express their gratitude to the individuals who have become instrumental for the conduct of this study.

## Conflict of interests

No conflict of interest.

## References

- Alam, T., Refat, C. M. M., Imran, A. Z. M., Rashid, S. Z., Kabir, H., Tarek, R. H., & Gafur, A. (2018). Proceedings from 2018 International Conference on Innovations in Science, Engineering and Technology (ICISSET): *Design and Implementation of a Secured Enterprise Network using Dynamic Multipoint VPN with HSRP Protocol*. Chittagong, Bangladesh. <https://doi.org/10.1109/iciset.2018.8745601>
- Amboya, J.M., Francisco, R.M., Hernandez, R.J., Opena, J.S., Samson, I.V., & Olipas, C.N.P. (2022). HighTeach: A web-based teacher evaluation system for a higher learning institution in the Philippines. *African Journal of Advanced Pure and Applied Sciences*, 1(4), 8-15. <https://doi.org/10.5281/zenodo.7816941>
- Binkhorst, V. (2022). Security at the End of the Tunnel: The Anatomy of {VPN} Mental Models Among Experts and {Non-Experts} in a Corporate Context. Retrieved from <https://www.usenix.org/conference/usenixsecurity22/presentation/binkhorst>
- Damanik, H.A. (2021). Securing data network for growing business VPN architectures. *Acta Informatica Malaysia (AIM)*, Zibeline International Publishing, 6(1), 01-06. <https://doi.org/10.26480/aim.01.2022.01.06>
- Dela Fuente, M.A.M, Facunla, J.A., De Guzman, H.N.F, Jacinto, E.F., Hilario, J.B, Olipas, C.N.P. & Cunanan, A.I. (2023). Project Clinic: A Cross-Platform Scheduling and Appointment Reservation System. *Formosa Journal of Computer and Information Science*, 2(1), 13-24. <https://doi.org/10.55927/fjis.v2i1.4077>
- Ezra, P. J., Misra, S., Agrawal, A., Oluranti, J., Maskeliunas, R., & Damaševičius, R. (2021). Secured Communication Using Virtual Private Network (VPN). In *Lecture notes on data engineering and communications technologies*. Springer International Publishing.

[https://doi.org/10.1007/978-981-16-3961-6\\_27](https://doi.org/10.1007/978-981-16-3961-6_27)

Muc, A., Muchowski, T., Murawski, L., Szelenzinski A. (2020). Providing the ability of working remotely on local company server via VPN. *Multidisciplinary Aspects of Production Engineering*, 3, 195-205. <https://doi.org/10.2478/mape-2020-0017>

Olipas, C.N.P. (2020). The developmental and assessment of an online student affairs system with short message service. *International Journal of Scientific and Technology Research*, 8(12), 1674-1681. <https://www.doi.org/10.5281/zenodo.7817465>

Olipas, C.N.P., Sawit, R.C.M., & Esperon, R.M. (2021). The design and assessment of a church records and information management system. *International Journal of Research and Innovation in Applied Science*, 6(1), 48-52. <https://doi.org/10.5281/zenodo.8024706>

Olipas, C.N.P., Villoria, J.P., Mateo, S.M., Sta Maria, S.A.P., Bisnar, E.P., & Vallecera, M.L.M. (2022). MediCord: A web-based healthcare management system. *Journal Healthcare Treatment Development*, 2(5), 35-35. <https://doi.org/10.55529/jhtd25.35.45>

Reguyal, J.M.T., Agno, A.M.S., Martinez, M.C., Castro, J.T., Cariazo, B.V.C., Olipas, C.N.P. & Alegado, R.T. (2023). Ob-Gyn Clinic Online Scheduling System. *Formosa Journal of Computer and Information Science*, 2(1), 25-36. <https://doi.org/10.55927/fjcis.v2i1.4076>

Santoso, B., Sani, A., Husain, T., & Hendri, N. (2021). VPN site to site implementation using protocol L2TP and IPSEC. *Teknokom*, 4(1), 30-36. <https://doi.org/10.31943/teknokom.v4i1.59>

Thiara, V.B.S. (2021). Enterprise Based VPN. *Education and Research Archive*. <https://doi.org/10.7939/r3-ax5r-h012>