ISSN 2278-3091
Volume 14, No.4, July - August 2025
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse041442025.pdf
https://doi.org/10.30534/ijatcse/2025/041442025

Development of a Network Subnetting System for Enhanced Connectivity and Data Management in Barobo LGU

Jan Kylle A. Abunda[1], John Lester L. Albero[2], Eugenio A. Sajulga[3], Queenie B. Matin-ao[4], Cresaldo Jr. S. Lozada[5], Emmer P. Ruaya[6]

[1]North Eastern Mindanao State University-Tagbina Campus, Philippines, jankyllebnda16@gmail.com
[2]North Eastern Mindanao State University-Tagbina Campus, Philippines, alberojohnlester@gmail.com
[3]North Eastern Mindanao State University-Tagbina Campus, Philippines, eugeniosajulga41@gmail.com
[4]North Eastern Mindanao State University-Tagbina Campus, Philippines, matinaoqueenie.00@gmail.com
[5]North Eastern Mindanao State University-Tagbina Campus, Philippines, lozadacresaldo2@gmail.com
[6]North Eastern Mindanao State University-Tagbina Campus, Philippines, emmerruaya@gmail.com

Received Date: June 27, 2025 Accepted Date: July 30, 2025 Published Date: August 06, 2025

ABSTRACT

In today's digital era, local government units (LGUs) depend on reliable networks to manage data and deliver public services efficiently. The Municipality of Barobo in Surigao del Sur faces communication delays, data management inefficiencies, and slow network performance due to a lack of structured network design. This study proposes the development and implementation of a subnetted network system tailored to the LGU's needs. Subnetting divides the network into smaller, more manageable segments, improving performance, security, and fault isolation. The proposed design utilizes a Cisco 2911 router and two switches, connecting five offices and 25 computers across two floors. Each floor is assigned a /27 subnet, allowing efficient IP address allocation and future scalability. The system enhances data flow, simplifies administration, and reduces network congestion without requiring complex configurations like VLANs. With projected uptime of 99.9%, the solution supports essential operations and ensures reliable communication across departments. The study emphasizes practical implementation, cost-effectiveness, and ease of maintenance, making it ideal for public sector environments. By adopting this subnetting strategy, the Barobo LGU can achieve streamlined operations, better service delivery, and readiness for future digital expansion.

Key words: Subnetting, Network Design, Local Government Unit, Barobo LGU, IP Address Management, Connectivity, Data Management, Network Security, Fault Isolation, Network Scalability

1. INTRODUCTION

In today's increasingly digital world, local government units (LGUs) depend on reliable and secure network systems to manage data and deliver services efficiently. As their operations become more complex and interconnected, the need for seamless communication between offices and effective data management becomes even more critical. In the Municipality of Barobo, Surigao del Sur, the current network setup across various LGU offices has begun to show limitations—such as slow internet speeds, communication delays, and difficulties in data sharing and management. These issues not only hinder daily operations but also negatively impact the quality of public service delivery.

To address these challenges, this study focuses on implementing a structured network subnetting strategy for the Barobo LGU. Subnetting involves dividing a large network into smaller, more manageable segments. As stated in [1], subnetting provides several key benefits: it reduces unnecessary network traffic, enhances performance, simplifies management, and strengthens network security. Rather than relying on one large, complex network, subnetting breaks it into smaller segments, making it easier to manage while improving efficiency by isolating traffic and limiting exposure to critical data. This approach is especially beneficial for LGUs with multiple offices, such as Barobo. Through subnetting, the LGU can expect improved communication, reduced network congestion, and a scalable infrastructure that supports future technological upgrades.

Similar subnetting strategies have been explored in related studies. For instance, [2] implemented a complete network solution for Barangay Pinagsama in Taguig City, utilizing subnetting to effectively manage IP address allocation, resulting in improved network performance and management. Likewise, [3] proposed a wide area network (WAN) design for government agencies, emphasizing the importance of subnetting in organizing and securing network segments to achieve better connectivity and control. These

studies highlight the relevance and feasibility of applying subnetting in local government operations.

This study is significant because it aims to enhance the internal operations of the Barobo LGU. It will simplify network management for IT personnel and improve communication and collaboration among employees. Ultimately, a more efficient network will lead to better public service delivery. It is important to note that this study focuses specifically on the design and implementation of subnetting within the LGU's existing network infrastructure and does not include upgrades to internet services or physical hardware.

1.1 Objective

To develop a structured network subnetting strategy for the Local Government Unit (LGU) of Barobo, Surigao del Sur, aimed at enhancing inter-office connectivity, improving network performance, and ensuring efficient data management across multiple offices.

2. METHODOLOGY

Projected Benefits

The implementation of subnetting is expected to enhance the overall efficiency of the LGU's internal network. This includes faster communication, better data handling, and easier scalability for future expansions.

Simplified Network Administration

Subnetting divides the network into manageable segments, making it easier for IT personnel to monitor, maintain, and troubleshoot.

Improved Security

By isolating traffic within smaller subnetworks, sensitive data is less exposed to potential threats, thus strengthening internal security.

Easier Fault Management

If a problem arises within one subnet, it can be isolated and resolved without affecting the entire network, reducing downtime and impact.

Improved Quality of Service (QoS)

Network performance is optimized through reduced traffic congestion, leading to faster and more reliable communication between offices.

Network Management

Network management involves the tools and processes used to monitor, control, and maintain a network. It ensures that the network runs smoothly, securely, and efficiently. According to Tawalbeh (2020), a network management system is a set of control and monitoring tools designed to carry out network management tasks. For the Barobo LGU, this means better control over network performance, easier troubleshooting, and improved service delivery.

Administration

Administration serves as the foundation of network management. It involves managing and documenting all networking assets such as servers, routers, switches, and access points. This process ensures that network components are accounted for and easily traceable when updates or replacements are needed. Good administrative practices include keeping an updated inventory, tracking network configurations, and ensuring licensing compliance for network software. It also aids in resource planning, bandwidth allocation, and maintaining operational efficiency across departments. By maintaining accurate records, administrators can make informed decisions that improve network performance and reduce unnecessary expenses.

Operation Control

Operation control involves monitoring and managing the network's real-time performance once it is up and running. It ensures that data flows efficiently and that each device functions as expected. Through network monitoring tools, administrators can observe packet transmission paths, signal strength, latency, and data loss. This step also includes load balancing, device activation or deactivation, and identifying performance bottlenecks. Operation control provides visibility into the network's overall health, enabling administrators to proactively adjust configurations to handle varying levels of demand. This is particularly important in multi-office environments like LGUs, where service delays can disrupt public service delivery.

Maintenance and Troubleshooting

This component focuses on preserving network integrity by identifying and resolving issues before they lead to significant problems. Maintenance includes tasks such as hardware checks, software updates, patch installations, and performance optimization. Troubleshooting, on the other hand, involves diagnosing connectivity issues, isolating faults, and implementing corrective measures to restore normal operations. In some cases, devices may need to be calibrated or physically replaced. A proactive maintenance and troubleshooting process minimizes downtime, improves user experience, and helps the organization avoid costly disruptions.

Security

Security is critical in safeguarding the network from internal misuse and external threats. It includes implementing firewalls, antivirus software, intrusion detection systems, and user authentication mechanisms. Additionally, it involves securing physical devices—especially those installed in outdoor or exposed environments—by using protective casings and ensuring proper grounding. By segmenting the network through subnetting, administrators can limit access to sensitive areas and reduce the risk of widespread breaches. For LGUs that manage public data and confidential information, robust security measures are essential to maintain trust, ensure data privacy, and comply with legal regulations.

[4] Highlights the susceptibility of Filipinos to cyberattacks, particularly phishing and malware, due to limited implementation of internet security practices despite awareness. This underscores the need for comprehensive cybersecurity strategies within LGUs. Furthermore, [5,6] emphasizes the importance of proactive security measures, including the enhancement of incident response capabilities and the establishment of standardized audit frameworks for government entities, to bolster the country's cyber resilience.

Project Gantt Chart

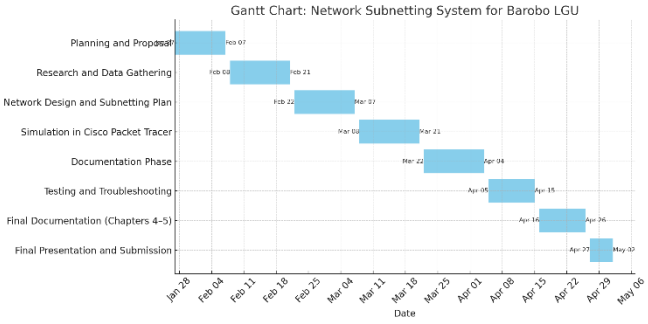

Figure 1: Gantt Chart

Figure 1 shows the project timeline for developing the subnetting system. It covers eight major phases, beginning with Planning and Proposal in late January and ending with Final Presentation and Submission in early May. Each task, such as Research and Data Gathering, Network Design and Subnetting Plan, and Simulation in Cisco Packet Tracer, is scheduled sequentially to ensure smooth progress. Overlapping tasks, like documentation and testing, indicate concurrent activities to optimize time. This visual representation helps track deadlines and ensure project milestones are achieved on schedule.

Capital and Operating Requirement

Table 1: Capital Expenditure

Operating Expense	**Description**	**Estimated Cost**
Subscription	Internet/Data center/VPN services	₱180,000/year
Personnel Wages	IT Admin / Tech support	₱480,000/year
Training	For staff handling the system	₱20,000 one-time
Maintenance Cost	Hardware servicing, replacements	₱100,000/year
Total Operating Expenditures		₱780,000
Total Capital and Operating Expenditures for the first year of Implementation		₱884,000

CAPITAL EXPENDITURES		
Particulars	**Quantity**	**Estimated Cost**
Routers	1	₱15,000
Switches	2	₱18,000
Ethernet cables	~500m	₱10,000
Access Points	4	₱16,000
Patch panel	2	₱5,000
Network Rack Cabinet	1	₱10,000
Installation		**₱30,000**
Total Expenditures		**₱104,000**

Table 1 presents the estimated costs for implementing the subnetting system at Barobo LGU, which include both operating and capital expenditures. The annual operating expenses amount to ₱780,000 and cover several components: internet, data center, and VPN subscription services costing ₱180,000 per year; personnel wages for IT administrators and technical support amounting to ₱480,000 per year; a one-time training expense of ₱20,000 for staff handling the system; and maintenance costs of ₱100,000 per year for hardware servicing and replacements. For capital expenditures, the estimated cost is ₱104,000, which includes one router priced at ₱15,000, two switches costing ₱18,000, approximately 500 meters of Ethernet cables at ₱10,000, four access points for ₱16,000, two patch panels for ₱5,000, a network rack cabinet for ₱10,000, and an installation cost of ₱30,000. Combining both operating and capital costs, the total projected expenditure for the first year of implementation is ₱884,000.

2.1 Proposed Network Design

Network Analysis

Data Types

The network will support various types of data essential for daily LGU operations. These include internal memos, public announcements, financial records, employee records, legal documents, and e-governance forms. Most data will be in text format (e.g., Word documents, spreadsheets, PDFs), though occasional multimedia content such as images, scanned documents, and video conferencing files (e.g., meeting recordings) will also be handled by the system. Support for web-based platforms and applications is also considered for future expansion.

Data Sources

Data will originate from computers and digital devices across different LGU departments, including the Mayor's Office, Treasurer's Office, Engineering Department, and other administrative units. Common software sources include Microsoft Office (Word, Excel, PowerPoint), database systems like MS Access, and communication platforms like Zoom, Google Meet, and Microsoft Teams. Additional tools such as Notepad, Paint, and PDF editors will also contribute to the overall data workload.

Number of Users and Priority Levels

The estimated number of active users on the network is around 35 to 50, representing staff across 7 office departments. These users will be assigned different priority levels based on their roles and network usage:

High Priority – Network administrators and department heads

Medium Priority – Regular staff involved in document processing and communication

Low Priority – Background processes such as scheduled backups and file synchronization

Priority-based traffic handling will help ensure that critical operations receive bandwidth preference during peak hours.

Transmission Speed Requirements

The network is designed to deliver seamless performance across all departments. Users should experience minimal delay when accessing shared files, conducting video calls, or retrieving data from central storage. Internal applications, database queries, and even remote access (if applicable) should appear as responsive as local programs, thereby promoting productivity.

Load Variation Estimates

Peak traffic is expected during business hours from 8:00 a.m. to 5:00 p.m., Monday to Friday, with the highest usage likely to occur during document submissions, reports processing, and scheduled meetings. Lighter traffic is expected on weekends and during lunch hours. Backup operations and system updates will be scheduled for off-peak times (evenings or weekends) to avoid service interruptions.

Storage Requirements

Each LGU workstation will be allocated a minimum of 100 GB of storage for daily operations. Each department will have access to a shared drive hosted on a local file server, with 500 GB to 1 TB total storage capacity depending on departmental needs. The central data server, located in the main administrative office, will have at least 2 TB of storage to accommodate backups, shared files, and system logs.

Reliability Requirements

The network is expected to maintain at least 99.9% uptime, consistent with public sector standards. Fault tolerance measures such as redundancy for key switches and auto-recovery protocols for critical services will be included. Routine diagnostics and network monitoring will help ensure continuous service delivery.

Security Requirements

To ensure secure access and data integrity, a firewall system will be deployed alongside user authentication protocols (username and password logins). Role-based access control (RBAC) will distinguish between general users and network administrators. Sensitive departments will have limited access zones within the network to protect confidential data. Antivirus software and system logs will be regularly updated to detect and respond to potential threats.

Physical Design

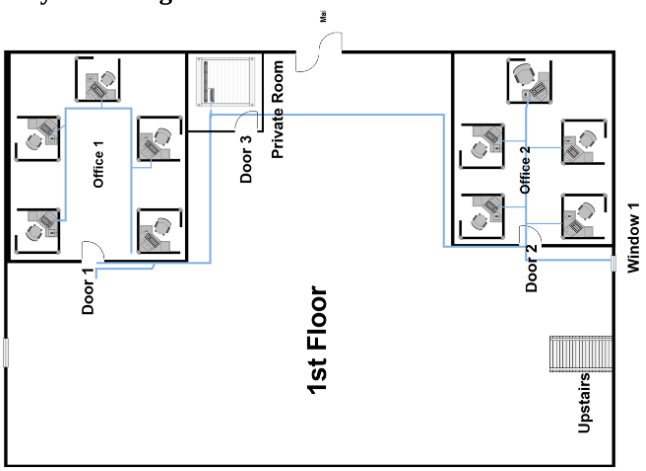

Figure 2: Physical Design 1st Floor

Figure 2 shows the physical layout of the structured cabling plan for the first floor of the LGU building. It includes two main offices (Office 1 and Office 2), a Private Room, and access points such as doors and a window. Network cables are routed to connect multiple workstations, ensuring organized and efficient connectivity. The cabling runs through designated pathways to minimize clutter and maintain safety. This structured design supports easy maintenance and ensures that devices in all rooms on the first floor have reliable network access.

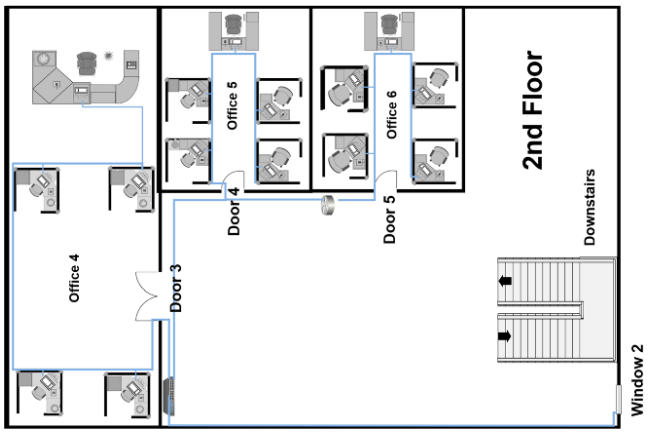

Figure 3: Physical Design Second Floor

Figure 3 shows the physical layout of the structured cabling plan for the second floor of the building. It includes multiple offices (Office 4, Office 5, and Office 6) and key access points such as doors and a window. Network cables are routed efficiently to connect workstations in each office, ensuring organized and reliable connectivity. The cabling follows designated pathways to minimize clutter and ensure safety, supporting easy maintenance and consistent network access across all offices. This layout is designed to facilitate a productive working environment while maintaining operational efficiency and connectivity throughout the floor.

Logical Design

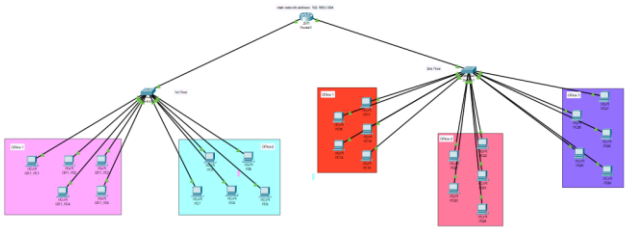

Figure 4: Network Logical Design

Figure 4 shows the proposed network design for the Barobo Local Government Unit (LGU) it is built to improve the connectivity and management of office data across two floors of the municipal building. The setup is kept simple but efficient, using a Cisco 2911 router and two switches to connect all devices.

Instead of using VLANs, the network is divided into two subnets, one for each floor. This structure still allows us to organize and manage the flow of data more efficiently across departments and devices.

- On the 1st Floor, we have two offices with a total of 10 computers. These are all connected to Switch 1, which then connects to the router. This floor uses the subnet 192.168.0.0/27, which provides 30 usable IP addresses—enough for all devices and a few more in case we add printers, IP phones, or other networked equipment in the future.
    - The router's gateway for this subnet is 192.168.0.1.
- The 2nd Floor has three offices and 15 computers; all connected to Switch 2. This floor uses a separate subnet, 192.168.0.32/27, which also provides 30 usable IPs.
    - The router's gateway for this subnet is 192.168.0.33.

The two switches are connected to the router through its Gigabit Ethernet interfaces. The router not only allows the devices on both floors to communicate with each other, but also handles connections outside the local network (such as internet access or remote data services, if needed).

By using IP subnetting, the network becomes easier to manage, and it's more secure and organized even without using VLANs. This design is also scalable, meaning the LGU can add more devices or expand offices later on without needing to overhaul the system.

In short, this logical design balances simplicity, cost-efficiency, and future readiness—all aligned with the goal of enhancing connectivity and data management within the Barobo LGU. Table 2 below shows the Network Cost of ownership.

Network Cost of Ownership'

Table 2: Network Cost of ownership

TCO Components	Cost
One Time Installation Costs hardware and labor for deployment	104,000
Operating Expenses per year	780,000
Total Capital and Operating Expenditures for the first year of Implementation	**₱884,000**

3. RESULT AND DISCUSSION

Implementation

The goal of this study was to develop a simple and cost-effective network subnetting system designed specifically for the Barobo Local Government Unit (LGU). The network setup was tailored to fit the current structure of the LGU office, which consists of 5 offices and 25 computers distributed across two floors.

To organize the network efficiently, two subnets were created—one for the first floor (with 10 PCs) and one for the second floor (with 15 PCs). A /27 subnet mask was used for each subnet, providing enough usable IP addresses while keeping the setup clear and manageable. This avoids the complexity of VLANs, making it easier for staff to maintain and understand the system.

A Cisco 2911 router connects both subnets, while two switches—one per floor—handle the local network traffic. IP addresses were carefully assigned to avoid any conflicts, and structured cabling ensures stable connections between all devices.

This network design supports better communication, faster data sharing, and smoother day-to-day operations. It also considers realistic expenses, such as hardware costs, internet subscriptions, installation labor, and IT support. By following this plan, the LGU can build a strong digital foundation that can grow over time.

4.CONCLUSION

To conclude, implementing a subnetted network system at the Barobo LGU is a smart, manageable solution for improving connectivity between its offices. Even without complex network technologies like VLANs, the system still delivers organized and secure communication among all devices.

This design helps simplify network management, reduces the risk of issues, and provides room for future expansion. With proper setup and support, this network can improve the LGU's productivity and services for years to come.

REFERENCES

[1] Sisat, S. N. (2013, March). *IP subnetting*. *International Journal of Knowledge Engineering and Soft Data Paradigms*, 2(5), 5–10. Newtek Electrical.

[2] Amito, R. (2018). *A complete network solution for Barangay Pinagsama*. Academia.edu. https://www.academia.edu/36290472/A_Complete_Network_Solution_for_Barangay_Pinagsama

[3] Lunar, M. J. E. (2018). *Proposed wide area network design*. Academia.edu. https://www.academia.edu/35859632/PROPOSED_WIDE_AREA_NETWORK_DESIGN_docx

[4] Omorog, C. D., & Medina, R. P. (2020). *Internet security awareness of Filipinos: A survey paper*. arXiv. https://arxiv.org/abs/2012.03669

[5] Department of Information and Communications Technology. (2023). *National Cybersecurity Plan 2023–2028*. https://cms-cdn.e.gov.ph/DICT/pdf/NCSP-2023-2028-FINAL-DICT.pdf

[6] Ruaya, E. P., & Buladaco, M. V. M. (2022). Virtual local area network (vlan) network design for nemsu-administration building. *International Journal*, *11*(6).