International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(Research Article)

Designing scalable network architectures for state universities and colleges (SUCS): A longitudinal case study of Sorsogon State College Bulan campus (2018–2025)

Ramon B. Gimena *, Christian Paul Sabayle and Dazzle G. Gillego

College of Information and Communications Technology, Sorsogon State University (formerly Sorsogon State College), Bulan Campus, Bulan, Sorsogon, Philippines.

International Journal of Science and Research Archive, 2026, 20(01), 013-022

Publication history: Received on 03 April 2026; revised on 29 June 2026; accepted on 02 July 2026

Article DOI: https://doi.org/10.30574/ijsra.2026.20.1.0991

Abstract

Introduction: The modernization of infrastructure within State Universities and Colleges (SUCs) in the Philippines is a critical mandate for national development, yet it is frequently hampered by budgetary constraints and the rapid rate of technological obsolescence. As noted by Abaidulla (2022), the post-pandemic landscape has forced SUCs to pivot toward digital-first priorities, though rural campuses still struggle with a widening "digital divide". In the Bicol region, this divide is exacerbated by geographical and socio-economic hurdles that limit broadband penetration (Bongalos-Perez, 2021). The Sorsogon State University (formerly SSC) Bulan Campus represents a critical ICT education hub, yet its physical expansion historically outpaced its technological backbone. This study treats the 2018 proposal as a baseline to determine how architecture can remain relevant despite hardware obsolescence, aligning with the CHED (2024) Strategic Framework for Smart Campus Development.

Objective: This study presents a longitudinal analysis of the network infrastructure planning process for the Sorsogon State College (SSC) Bulan Campus. It utilizes a baseline network design proposal developed in 2018 as a historical case study, re-validating its architectural principles against the evolved "Smart Campus" standards of 2025.

Methods: The research employed a descriptive-developmental approach. Phase one involved a rigorous 2018 baseline assessment via ocular inspections and stakeholder interviews, which revealed a fragmented, "island-based" topology with no centralized connectivity. Phase two involved the design of a Three-Layer Hierarchical Network Model (Core, Distribution, Access) to unify the campus. Phase three, conducted in the present day, applied a comparative gap analysis to assess the design's longevity.

Results: The 2018 proposed architecture successfully consolidated independent workstations into a unified Campus Area Network (CAN), utilizing VLAN segmentation to secure administrative data and centralized server architecture to eliminate peer-to-peer inefficiencies. However, the retrospective analysis indicates that while the hierarchical *topology* remains valid, the specific hardware specifications (Cisco 4500x/3560x) and reliance on wired connectivity are insufficient for the high-bandwidth, mobile-first demands of 2025.

Limitations: The study delineates the boundaries between logical simulation and physical throughput, acknowledging the constraints of the Packet Tracer environment used for the topological validation.

Conclusion: The study concludes that sustainable IT planning in SUCs must shift from purely hardware-centric procurement to modular, framework-based designs. While hardware reaches end-of-life status within 5-7 years, a robust hierarchical framework provides the necessary agility to integrate emerging technologies such as Wi-Fi 6 and Zero Trust security without requiring complete infrastructural overhaul.

* Corresponding author: Ramon B. Gimena

Keywords: Network Infrastructure; Hierarchical Network Design; Campus Area Network (CAN); Sorsogon State College; IT Modernization; SUC Technology Planning; Educational Technology

1. Introduction

In the rapidly evolving landscape of global education, the network infrastructure of a higher education institution functions as its central nervous system. It is no longer merely a utility for sending emails or printing documents; it is the foundational backbone that supports Learning Management Systems (LMS), real-time collaborative research, administrative governance, and the security of sensitive institutional data. For State Universities and Colleges (SUCs) in the Philippines, maintaining this infrastructure presents a unique paradox: institutions are expected to produce globally competitive graduates proficient in the latest technologies, yet they must often do so using infrastructure funded by constrained public budgets and procured through rigid, lengthy government processes (Republic of the Philippines, 1993).

The challenge is magnified in satellite campuses located outside major metropolitan centers. The Sorsogon State College (SSC) Bulan Campus, now part of the Sorsogon State University system, stands as a primary provider of Information and Communication Technology (ICT) education in the municipality of Bulan. However, historically, the physical growth of the campus, the construction of new buildings and the increase in student population—outpaced the development of its technological underpinnings.

In 2018, an initial comprehensive assessment of the campus revealed a startling disconnect. Despite offering specialized courses in technology, the campus operated without a unified network. Computer laboratories functioned as isolated silos; administrative offices transferred data via flash drives (a practice known as "sneaker-net"); and security was virtually non-existent beyond simple desktop passwords. This environment not only hampered operational efficiency but also exposed the institution to significant data integrity risks.

This paper revisits the comprehensive network infrastructure plan proposed for SSC-Bulan Campus in 2018. However, rather than presenting it solely as a historical artifact, this study treats the 2018 proposal as a baseline dataset for a longitudinal analysis. By contrasting the technical solutions designed for the constraints of 2018 against the hyper-connected realities of 2025, this study seeks to answer a critical question for academic IT planners: How can SUCs design network architectures that remain scalable and relevant despite the rapid obsolescence of the hardware they are built upon?

The study aims to validate the resilience of the Hierarchical Network Design model—a standard in enterprise networking—when applied to the resource-constrained environment of a Philippine SUC. It analyzes whether the structural decisions made seven years ago would still serve as a valid foundation for a modern "Smart Campus" upgrade today.

2. Review of Related Literature

To contextualize the design decisions made in this study, it is necessary to understand the theoretical frameworks governing campus networking and the specific challenges faced by educational institutions in the Philippines.

2.1. The Campus Area Network (CAN) Evolution

A Campus Area Network (CAN) is defined as a proprietary Local Area Network (LAN) or a set of interconnected LANs serving a university, government agency, or similar organization (Ali et al., 2015). Unlike a corporate office contained in a single tower, a CAN must connect multiple buildings across a geographical area, requiring robust backbone cabling—often fiber optics—to bridge distances that standard copper cabling cannot reach.

Historically, CANs were designed primarily for "wired" traffic—desktop computers sitting in laboratories or faculty offices. However, the literature indicates a massive paradigm shift occurring between 2015 and 2025. The modern campus network has transitioned from a "connectivity-focused" model to a "service-focused" model (Cisco Systems, 2024). Today's networks must prioritize mobility (Wi-Fi), low latency for video conferencing, and seamless access to cloud-based resources (Google Workspace, Microsoft 365), drastically changing the bandwidth requirements at the network core.

2.2. The Hierarchical Network Design Model

The industry standard organizes devices into Core, Distribution, and Access layers. While Tanenbaum & Wetherall (2021) emphasize this for reliability, Stallings (2022) highlights that hierarchical designs are the necessary foundation for future Software-Defined Networking (SDN) and Network Function Virtualization (NFV). This modularity is crucial for SUCs, as Zhang (2023) confirms that a well-structured multi-tiered design significantly outlives the hardware components it hosts.

Standard approach to managing the complexity of a CAN is the Cisco Hierarchical Network Model. This framework avoids the chaos of a "flat" network by organizing devices into three distinct layers, each with a specific function:

- **The Core Layer:** This is the high-speed backbone of the network. Its only purpose is to switch traffic as fast as possible. It should not perform complex processing or filtering. Reliability here is non-negotiable.
- **The Distribution Layer:** This acts as the boundary between the Core and the Access layers. This is the "smart" layer where routing, packet filtering, policy implementation, and inter-VLAN routing occur.
- **The Access Layer:** This is the edge of the network where end-user devices (PCs, printers, Access Points) connect. This is where port security and Power over Ethernet (PoE) are delivered.

Chetty and Feamster (2012) argue that adopting this modular approach allows for easier troubleshooting and scalability. If a new building is constructed, new Access switches are simply added and uplinked to the Distribution layer without disrupting the Core. This modularity is crucial for SUCs, which often expand their facilities in phases based on funding availability.

2.3. Network Security in Educational Environments

Security in academic environments is notoriously difficult to manage. Unlike corporations that can lock down devices strictly, universities must support a "Bring Your Own Device" (BYOD) culture. While 2018 focused on perimeter firewalls, the current gold standard is **NIST SP 800-207**, which defines **Zero Trust Architecture (ZTA)—**where no device is trusted by default. Rose (2023) notes that implementing identity-based security is the only way to mitigate risks in open academic environments where "sneaker-nets" have been replaced by sophisticated ransomware threats (Security Magazine, 2024). By 2025, the standard has shifted to "Zero Trust" architectures, where no device is trusted by default, even if it is inside the campus network (Department of Information and Communications Technology [DICT], 2023). This requires networks to have sophisticated segmentation capabilities, such as Virtual Local Area Networks (VLANs), to ensure that a student's infected laptop cannot spread malware to the finance department's server.

3. Methodology

This study employs a **descriptive and developmental research design**, structured into three distinct phases: the baseline assessment (historical), the design development (technical), and the longitudinal validation (analytical).

3.1. Phase 1: The 2018 Baseline Assessment

The primary data gathering techniques used were ocular inspection and unstructured interviews with the SSC-Bulan Campus ICT faculty and administrative personnel. The researchers conducted a physical walkthrough of four key zones: The Administration Building (two floors), the ICT Department (including three laboratories), the library, and faculty offices.

During the inspection, a Network Inventory Checklist was utilized to document:

- **Active Equipment:** The make, model, and port density of existing switches and routers.
- **Passive Infrastructure:** The type and condition of cabling (Cat5e/Cat6), the presence of patch panels, and cable management practices.
- **Logical Configuration:** The IP addressing schemes used and how devices were named and organized.

Figure 1 Site Map of Sorsogon State College Bulan Campus (2018 Baseline)

3.2. Phase 2: Developing the Solution

Based on the gathered data, a proposed network infrastructure plan was developed using **Microsoft Visio** for topological mapping and **Cisco Packet Tracer** for simulation. The design strictly adhered to the Three-Layer Hierarchical Model.

The design process involved:

- **Capacity Planning:** Estimating the number of required ports based on the number of students and staff in 2018.
- **Simulation Testing:** The topology was built virtually in Packet Tracer to test connectivity between VLANs (e.g., pinging from the Admin VLAN to the Server Farm) and to verify that Access Control Lists (ACLs) correctly blocked unauthorized traffic.

3.3. Phase 3: The 2025 Longitudinal Re-validation

This phase represents the analytical core of the current study. The researchers engaged in a "Gap Analysis," comparing the specifications proposed in 2018 against the industry standards of 2025.

The metrics for this comparison included:

- **Throughput Capacity:** 1 Gigabit vs. 10/40 Gigabit requirements.
- **Wireless Standards:** 802.11n (Wi-Fi 4) vs. 802.11ax (Wi-Fi 6/6E).
- **Security Posture:** Local authentication vs. 802.1X/Identity Management.

3.4. Limitations of the Study

While this study utilizes the Cisco Hierarchical Network Model to validate architectural resilience, it acknowledges the inherent limitations of the simulation environment. The network topology was modeled using Cisco Packet Tracer, a logical simulation tool. Unlike hardware emulators (e.g., GNS3 or EVE-NG) that run actual device kernels, Packet Tracer simulates the behavior of network protocols. Therefore, this study limits its scope to the validation of logical connectivity, VLAN segmentation efficacy, and Access Control List (ACL) logic. It does not purport to measure physical phenomenon such as precise hardware throughput, CPU stress loads under high-volume packet switching, or electrical power consumption. The results should be interpreted as an architectural proof-of-concept for SUC planning rather than a hardware performance benchmark.

4. Results: The 2018 Baseline and Proposal

To understand the necessity of the proposed design, one must first appreciate the severity of the infrastructure deficit identified during the baseline assessment.

4.1. The "Before" Scenario: Anatomy of a Fragmented Network

The ocular inspection painted a picture of a facility struggling to cope with modern demands. The network was not merely "slow"; it was structurally incoherent.

- **The "Island" Problem:** There was no campus-wide backbone. The Administration Building had a small local network for the Registrar, but the Accounting and Cashier offices—which rely on shared financial data—were operating on standalone PCs. Data transfer required staff to physically walk flash drives between desks, introducing delays and potential for data corruption or theft.
- **The "Spaghetti" Infrastructure:** In the ICT Laboratories, cabling was haphazard. Unmanaged switches were daisy-chained together (a practice that creates bottlenecks), and cables were often laid across floors without conduits, posing physical safety hazards.
- **The Resource Wastage:** Without a network, resources could not be shared. The inspection found multiple personal printers attached to individual desktops in the same room. A networked environment would have allowed a single, high-volume printer to serve the entire office, significantly reducing hardware and toner costs.
- **The Security Vacuum:** Perhaps most critically, there was no centralized user management (such as Active Directory). Students and staff logged into PCs using local accounts. If a user changed their password, it only applied to that specific machine. There was no way for an administrator to push security policies or updates to all computers at once.

Figure 2 Existing Standalone Network Layout of Administration Building (2018). Note the lack of interconnection between offices (first floor and second floor)

4.2. The Solution: A Hierarchical Campus Area Network

The proposed solution (Figure 3) was designed to bring order to this chaos through centralization and segmentation.

4.2.1. Infrastructure Architecture

The design called for a star topology radiating from a central **Main Distribution Facility (MDF)** located in the ICT Building. This location was chosen due to its proximity to the technical staff who would manage the system.

The Core Backbone: The design specified **Dual Cisco 4500x Series Switches.** In 2018, these were powerhouse devices capable of routing gigabit traffic with high reliability. The "Dual" specification was crucial—it provided redundancy. If one switch failed (e.g., power supply burnout), the secondary switch would instantly take over, preventing a campus-wide blackout.

The Distribution/Access Layer: For the individual buildings, the design proposed **Cisco 3560x Series Switches**. These were chosen for their PoE (Power over Ethernet) capability, allowing them to power wireless access points and IP phones directly through the network cable, eliminating the need for extra power outlets.

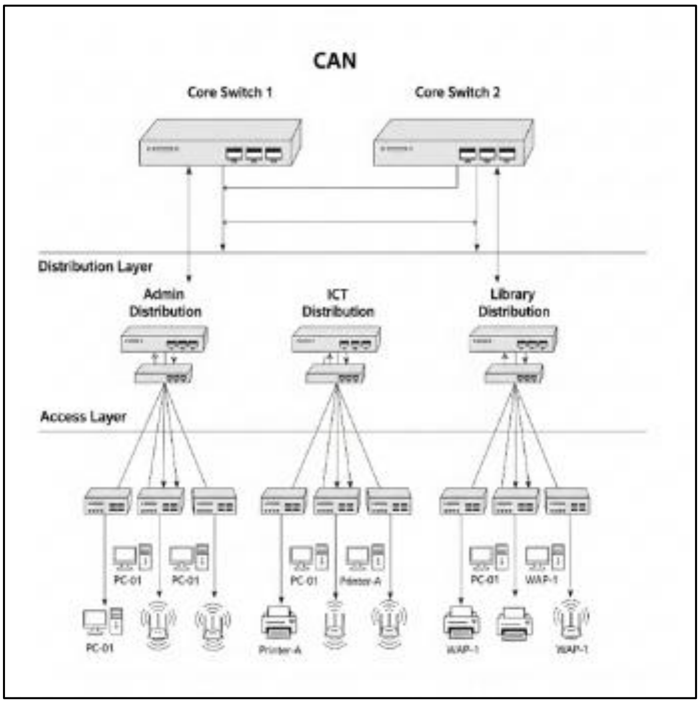

Figure 3 Proposed Campus Area Network (CAN) Hierarchical Topology. Source: Simulation Results

4.2.2. Logical Segmentation (VLANs)

A key innovation of the proposal was the implementation of **Virtual Local Area Networks (VLANs)**. In the old "flat" network design, if a computer in the student lab was infected with a virus that broadcasted traffic, it could flood the entire network, slowing down Dean's computer.

The proposal segmented the campus into logical groups:

- **VLAN 10 (Admin):** Strictly for Registrar, Accounting, and Cashier data.
- **VLAN 20 (Faculty):** For instructor use.
- **VLAN 30 (Student Labs):** For general instruction.
- **VLAN 99 (Management):** A hidden network for IT staff to manage the switches.

This segmentation acted as a digital quarantine system—problems in one department would not affect the others.

4.2.3. Centralized Services

Finally, the plan introduced a **Dedicated Server** running Windows Server 2008 (the standard at the time). This server would handle **DHCP** (automatically assigning IP addresses so staff didn't have to type them in manually) and **DNS** (resolving web addresses). This marked the shift from a peer-to-peer network to client-server architecture.

5. Retrospective Analysis: The 2018 Design in a 2025 World

Seven years is an eternity in information technology. While the 2018 proposal was robust for its time, evaluating it against 2025 standards reveals significant gaps. This analysis illustrates the challenge SUCs face: the "moving target" of technological currency.

5.1. The Bandwidth Gap: From Gigabit to Multi-Gigabit

The 2018 proposed 1Gbps backbone is now a severe bottleneck. Lim (2024) posits that 10Gbps or 40Gbps fiber uplinks are now mandatory to handle concurrent high-definition video streams.

In 2025: The consumption profile has changed drastically. Modern education involves high-definition video streaming, Zoom/Teams video conferencing, and heavy cloud-based Learning Management Systems (Canvas/Moodle). A 1Gbps backbone today would be a severe bottleneck.

Gap Analysis: Modern SUC networks require a minimum of **10Gbps (10G)** or **40Gbps** fiber uplinks between buildings to handle multiple concurrent video streams without lag. The Cisco 4500x, while a capable device, is now considered End-of-Life (EoL) and lacks the throughput for a modern, video-heavy campus.

5.2. The Wireless Gap: From "Nice-to-Have" to "Mission Critical"

The 2018 plan was heavily focused on wired connections—running cables to desktop PCs in labs. Wireless Access Points (APs) were treated as supplementary conveniences. Today, the landscape is mobile-first. As detailed in Khorov et al. (2021), Wi-Fi 6 (802.11ax) is required to handle high-density environments where hundreds of devices connect simultaneously. Furthermore, Gast (2022) notes that the wattage requirements for these modern radios often exceed the PoE standards available in legacy 2018-era switches.

In 2025: The device landscape is mobile-first. Students and faculty carry laptops, tablets, and smartphones. The expectation is "connectivity everywhere," not just in the lab.

Gap Analysis: The 2018 design lacks density for modern wireless needs. A modern design would require **Wi-Fi 6 (802.11ax)** or **Wi-Fi 7** access points. These new standards are designed to handle hundreds of devices per room (high density), whereas the older APs would crash under such a load. Furthermore, the switch infrastructure proposed in 2018 (PoE) might not provide enough wattage (PoE+) to power modern, high-performance Wi-Fi 6 radios.

5.3. The Security Gap: The Death of the Perimeter

The 2018 security strategy relied on "Perimeter Security" essentially a firewall at the edge of the network and passwords on PCs. The assumption was that threats came from *outside*. Modern SUCs must move toward Zero Trust Network Access (ZTNA), utilizing 802.1X authentication as described by Ward (2021). Additionally, the reliance on Windows Server 2008 now constitutes a major risk, as Microsoft (2024) has officially ended support, leaving these systems vulnerable to unpatched exploits.

In 2025: The threat landscape includes sophisticated Ransomware that can enter via a student's USB drive or a phishing email.

Gap Analysis: The reliance on local PC passwords or even simple Active Directory authentication is no longer enough. Modern SUCs are moving toward **Zero Trust Network Access (ZTNA)**. This requires **802.1X authentication**, where the network switch itself challenges every device that plugs in. If a device doesn't have the latest antivirus update, the network refuses to let it connect. The 2018 hardware supports basic forms of this, but lacks the advanced telemetry needed for modern threat hunting.

5.4. The Operating System Gap

The proposal specified **Windows 7** and **Windows Server 2008**. Both are now obsolete and unsupported by Microsoft. Continuing to run these operating systems in 2025 would constitute a severe security violation, as they no longer receive security patches, making them easy targets for hackers.

---

6. Discussion: Implications for SUC Infrastructure Planning

The findings of this longitudinal case study offer crucial lessons for Sorsogon State University and other SUCs in the Philippines.

6.1. The Resilience of Architecture Over Hardware

The most significant finding is that while the *hardware* (the switches, the servers) proposed in 2018 is now obsolete, the *architectural logic* (the Hierarchical Design Model) remains perfectly valid. The decision to separate the Core, Distribution, and Access layers was sound.

Because the network was designed with modularity, upgrading it for 2025 does not require ripping out the entire system. The campus can simply swap out the Access switches for newer models that support Wi-Fi 6, or upgrade the Core switches to 10Gbps models, without having to redesign the fiber optic pathways or the logical IP addressing scheme. This vindicates the importance of using standard enterprise frameworks rather than ad-hoc, flat network designs. Good architecture outlives the hardware it runs on.

6.2. Navigating Procurement Constraints

The Total Cost of Ownership (TCO) Approach The longitudinal analysis highlights a critical financial friction point in SUC administration: the disconnect between the 5-7 year lifecycle of IT hardware and the rigid nature of government procurement. While Marrone (2020) suggests ITIL 4 frameworks to improve service management, SUCs must operate under RA 9184 and DBM (2023) guidelines. The proposed "Hybrid Lifecycle" model allows SUCs to pre-pay for 5-year support bundles, effectively securing the network's future through strategic Capital Expenditure (CAPEX). Traditionally, SUCs rely on CAPEX models, where large budget releases are utilized for one-time hardware acquisitions.

However, the rapid obsolescence observed in this case study suggests that SUCs must explore alternative procurement strategies within the bounds of Republic Act 9184. While a full shift to Operational Expenditure (OPEX) such as Managed Network Services (MNS) or equipment leasing—offers agility, it faces bureaucratic hurdles regarding Multi-Year Contracting Authority (MYCA).

Therefore, this study recommends that SUC IT planners advocate for a "Hybrid Lifecycle" budget model. This entails:

Strategic CAPEX for passive infrastructure (fiber optics, cabling) which has a lifespan of 15+ years.

Service-Bundled Procurement for active components (switches/access points), where the initial bid includes a 5-year support and licensing maintenance agreement. This effectively "pre-pays" OPEX using CAPEX funds, ensuring the network remains secure and updated without requiring annual budget realignments.

6.3. Bridging the Digital Divide in Rural Campuses

For campuses like SSC-Bulan, robust infrastructure is an equalizer. A high-speed, reliable network allows students in rural Sorsogon to access the same global knowledge bases, cloud laboratories, and collaborative tools as students in Manila or abroad. The delay in implementing such designs due to bureaucratic hurdles widens the digital divide. The implementation of the proposed CAN is not just a technical upgrade; it is an academic imperative required for maintaining accreditation (e.g., AACCUP) and ensuring instructional quality. By adopting Gartner's (2024) "Cloud-First" trends and the ISACA (2023) COBIT 2019 framework, the university can ensure that its technological roadmap aligns with both accreditation standards (AACCUP) and global instructional quality.

---

7. Conclusion and Recommendations

The network infrastructure plan developed for Sorsogon State College Bulan Campus in 2018 was a necessary and competent response to the needs of that time. It identified the critical flaws of fragmentation and proposed a robust, standardized solution using the Hierarchical Network Model.

However, the longitudinal validation reveals that "implementation" is not a finish line. To make this design scalable for 2025 and beyond, the following updated recommendations are made:

- **Upgrade the Backbone:** The fiber optic backbone must be certified for **10 Gigabit** speeds to support modern video and cloud traffic.
- **Prioritize Wireless First:** Future investments should focus heavily on **Wi-Fi 6/6E high-density deployment** rather than just wired ports, acknowledging the mobile-centric nature of modern students.
- **Implement Identity-Based Security:** Move beyond simple passwords to **Role-Based Access Control (RBAC)** using 802.1X, ensuring that a student's personal laptop is isolated from the finance department's server automatically.
- **Adopt Cloud-Hybrid Services:** Instead of relying solely on on-premises servers (like the 2018 plan), the network should be optimized to connect to cloud services (Google Workspace/Microsoft 365) which offer better resilience and lower maintenance overhead for the IT staff.

By retaining the structural integrity of the 2018 topological design but refreshing the technological components, Sorsogon State University-Bulan Campus can build a network that is not only robust today but adaptable for the future.

Compliance with ethical standards

Disclosure of conflict of interest

The authors declare no conflict of interest. The hardware recommendations provided in this study (Cisco Systems) are based on industry standards and do not represent a commercial endorsement.

Statement of ethical approval

The study was conducted in accordance with the research ethics standards of Sorsogon State College (now Sorsogon State University). Institutional permissions were secured for the ocular inspection and analysis of campus infrastructure.

References

[1] Abaidulla, M. (2022). Digital Transformation in Philippine Higher Education: Challenges and Opportunities for SUCs. Philippine Journal of Higher Education.

[2] Ali, M. N., Hossain, M. E., & Parvez, M. M. (2015). Design and implementation of a secure campus network. International Journal of Scientific & Engineering Research, 5(7), 1580–1585.

[3] Bongalos-Perez, R. (2021). Broadband Penetration and the Digital Divide in Rural Bicol: A Policy Review. Bicol University Research Journal.

[4] CHED (Commission on Higher Education). (2024). Strategic Framework for Smart Campus Development in the Philippines. CHED Memorandum Order.

[5] Chetty, M., & Feamster, N. (2012). Refactoring network infrastructure to improve manageability: A case study of home networking. ACM SIGCOMM Computer Communication Review, 42(3), 76–82.

[6] Cisco Systems. (2024). Cisco 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.

[7] Department of Budget and Management (DBM). (2023). Guidelines on the Procurement of ICT Equipment under RA 9184. Government Procurement Policy Board (GPPB).

[8] Department of Information and Communications Technology (DICT). (2023). National ICT ecosystem framework (NICTEF). https://dict.gov.ph/nict-ecosystem-framework/.

[9] Gartner. (2024). Top Strategic Technology Trends in Higher Education. Gartner Research.

[10] Gast, M. S. (2022). 802.11ax: A Survival Guide. O'Reilly Media.

[11] IEEE Standard 802.11be. (2024). Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wi-Fi 7. IEEE Standard Association.

[12] ISACA. (2023). COBIT 2019 for SUCs: A Governance Framework for Digital Transformation. ISACA Manila Chapter.

[13] Khorov, E., Kiryanov, A., Lyakhov, A., & Akyildiz, I. F. (2021). A Tutorial on IEEE 802.11ax (Wi-Fi 6): High Efficiency WLANs. IEEE Communications Surveys & Tutorials.

[14] Kumari, L., Debbarma, S., & Shyam, R. (2016). Security problems in campus network and its solutions. International Journal of Advanced Research in Computer Science, 7(3).

[15] Laguda, R. (2020). Resilience in Philippine Education: Technology Integration in Resource-Constrained Environments. De La Salle University Press.

[16] Lim, H. S. (2024). Campus Area Networks: Managing the Core-to-Edge Bottleneck in the 10Gbps Era. Journal of Network Systems Management.

[17] Marrone, M. (2020). ITIL 4 in Academia: Improving IT Service Management in Universities. Springer Nature.

[18] Microsoft. (2024). The End of Life of Windows Server 2008 and 2012: Security Implications. Microsoft Security Response Center.

[19] NIST (National Institute of Standards and Technology). (2020). Special Publication 800-207: Zero Trust Architecture. U.S. Department of Commerce.

[20] Rose, S. (2023). Implementing Zero Trust in Higher Education: A Practical Framework. Journal of Cybersecurity Education.

[21] Security Magazine. (2024). Ransomware Trends in Southeast Asian Educational Institutions. Security Media Group.

[22] Sorsogon State University. (2024). Annual ICT Modernization Roadmap (2024-2029). Internal Institutional Document.

[23] Stallings, W. (2022). Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. Pearson Education.

[24] Tanenbaum, A. S., & Wetherall, D. J. (2021). Computer Networks (6th ed.). Pearson.

[25] Verma, A. (2023). Managing the BYOD Storm in Academic Networks: Capacity and Security. TechScience Press.

[26] Ward, J. (2021). 802.1X Authentication and Access Control: The Campus Perspective. Cisco Press.

[27] Zhang, L. (2023). The Transition from Flat to Multi-Tiered Hierarchical Designs in Emerging University Networks. Journal of Educational Technology Systems.