International Journal of Science and Engineering Science Research
Volume 2 | Issue 2 | April-June 2026 | ISSN 3049-2793
Peer Reviewed (Referred Journal)
DOI: https://doi.org/10.63671/ijsesr.v2i2.114

A Star-Bus Hybrid Network Infrastructure Design and Management Framework for St. Nicolas College of Business and Technology

Marla Dimple P. Bagares[1], Glennjo T. Quinto[2], Joselito D. Faylogna[3],

Caren M. Sumaganday[4], Jesus Lorenz Mago[5]

[1] St. Nicolas College of Business and Technology, Mel-Vi Compound, Jose Abad Santos Avenue, City of San Fernando, 2000 Pampanga, Philippines

Email: marladimplebagares24@gmail.com

Abstract

The need for higher speed internet connectivity as well as the protection of student's sensitive information has created the need for advanced networking systems. A complete network system will be implemented at St. Nicolas College of Business & Technology (SNC). The initial number of users will be approximately 300 but there is room for growth. The system will utilize a star-bus hybrid topology which supports the segregation of faults and central administration. VLSM within the SNC $10.10.0.0/16$ address block will allow optimal utilization of bandwidth while creating security by segregating departments. Technical testing included integration of firewall with IDS/IPS as well as development of an automated maintenance process. The findings show that this proposed infrastructure can provide a solid scalable and reliable platform for the institutions transition into a digital campus.

Keywords

Hybrid Star-Bus Topology; Variable Length Subnet Masking (VLSM); Network Security Integration; Scalable Infrastructure; Automated Network Maintenance

1. Introduction

Higher education is experiencing an entirely new era of the delivery of educational content. Institutions are moving away from traditional in-classroom instructional models toward increasingly digitalized learning environments that have high-speed internet access as a fundamental utility. For institutions such as St. Nicolas College of Business and Technology (SNC) —the network architecture provides the foundational operational platform for both academics and administration. As user populations expand and data-driven applications with increased bandwidth requirements such as cloud-based computing and multimedia streaming continue to be widely adopted by all levels of education —many community-based institutions will begin to experience "network stagnation" as their legacy networks fail to provide adequate bandwidth and/or meet the needed level of security required for this modern model of teaching and learning.

A reliable campus network is much more than just being able to connect the users in a particular area. A good structured CAN will have to be both accessible and have a “defense-in-depth” security model (Adke & Bhawar, 2020), if it does not have an scalable structure then this could lead to constant service disruption for students and faculty while also exposing sensitive student/faculty data to potential cyber threats.

International Journal of Science and Engineering Science Research
Volume 2 | Issue 2 | April-June 2026 | ISSN 3049-2793
Peer Reviewed (Referred Journal)
DOI: https://doi.org/10.63671/ijsesr.v2i2.114

Currently, St. Nicolas College has a diverse group of users using the system, from administrative office users through the Registrar, and other specialized technical facility users such as the Cisco Lab. The major problem is the possibility of creating "Single Point of Failure (SPoF)" vulnerability conditions. In isolated configurations that use either a traditional star topology or a bus topology, if there were to be an occurrence of a hardware failure at a central juncture, it could shut down all operations on the entire campus. Additionally, the absence of an overall IP addressing strategy for all devices on campus results in many instances of broadcast storms and unmanaged traffic congestion; both are major contributors to poor performance for the approximately 300 users in college constituents.

To addressed these challenges there is a need to develop and deploy a star bus hybrid network. This approach combines the centralized management of a star network with the backbone robustness of a bus system. By integrating vlsm into this network structure, the institution can logically segment its departments so that high traffic areas like computer labs will not disrupt the mission critical operations of the administrative.

2. Methodology

The current research used a developmental research design to develop the framework and evaluate the functionality of a local network system. A developmental research design is based upon the process described by Fajardo et al. (2026) for developing an Institutional System. In this case, the college-based project followed a structured SDLC process which consisted of three major phases; Analysis, Design and Simulation. These phases were designed to allow for a systematic review of the Star-Bus Hybrid topology's ability to meet the college's administrative needs as well as its academic needs.

The proposed infrastructure will be based on St. Nicolas College of Business and Technology. The college has a number of different operational requirements in terms of its educational and administrative needs. It requires a network that is capable of supporting a growing community of users and can scale with the institution's growth. For example, there are currently three hundred or so stakeholders at St. Nicolas College of Business and Technology including administrative personnel (Registrar and HR) and faculty staff. There are also specialized IT departments such as the Cisco Lab.

3. Results and Discussion

The results of the network design simulation are presented in this section and discuss the implications of implementing both a hybrid topology and the logical addressing model.

Network Topological Resilience and Fault Isolation

One major outcome of the Design Phase is that the Star Bus Hybrid Topology Architecture was successfully mapped. Unlike traditional star bus models where all communication flows linearly; with the central Firewall/switch (core) as the single point of entry into the star, it provides an immediate hierarchical flow through each layer of the architecture.

The simulated results confirm that the Hybrid model provides effective Fault Isolation. More specifically, when an Access Switch in a High Density Area (such as the Cisco Lab) has a Hardware Failure/Broadcast Storm it will be limited to only that one Node. All other areas of the campus, including Mission-Critical Administrative Offices (i.e., Registrar & HR), can continue to provide service via the Bus Backbone. Thus, this Resiliency Architecture meets the Institutional requirement for Continuous Service Delivery to all 300+ Users.

Variable Length Subnet Masking (VLSM) and Addressing Efficiency

International Journal of Science and Engineering Science Research
Volume 2 | Issue 2 | April-June 2026 | ISSN 3049-2793
Peer Reviewed (Referred Journal)
DOI: https://doi.org/10.63671/ijsesr.v2i2.114

Phase 2 (the Logical Configuration phase) created an extremely efficient address matrix using the $10.10.0.0/16$ Private IP Space by employing Variable Length Subnet Masking (VLSM). In addition, Phase 2 segmented the /16 Primary Block in to smaller /24 Subnets that were specifically designed for each Department based upon the departments number of Hosts.

Table 1. Proposed Subnet Allocation and Capacity

Department	Subnet Mask	CIDR	Host Capacity	Traffic Priority
Core Services (DHCP/File)	255.255.255.0	/24	254	High
Cisco Laboratory	255.255.255.0	/24	254	Medium
Administrative Office	255.255.255.0	/24	254	High
Registrar / HR	255.255.255.0	/24	254	High

The outcomes show that this approach to addressing the campus has given the college an estimated total number of possible networked host systems of well over sixty-five thousand; which would be sufficient for many years into the future as SNC continues to grow from the increasing use of portable device technology and IoT's. Additionally, since the VLSM method allows for segmentation of the network, it also gives the college additional ability to create firewalls to protect the student accessible lab networks from unauthorized access into sensitive administration networks.

Maintenance and Escalation Protocol Outcomes

A key finding of the Management Framework was the automation of "time to resolution" metrics by use of an automated escalation matrix. The research also developed a prioritized ticketing system for IT tickets with each type of issue assigned one of four categories: critical, high, medium, or low.

An “automatic” transfer of responsibility occurs when there is an unresolved High-priority problem, (e.g., departmental access switch failure) from the Tier 1 Help Desk to a Network Engineer in less than one hour. Further discussion on this model illustrates how the use of proactive monitoring with tools similar to Nagios/Zabbix has transformed the MIS Department into a Predictive Maintenance Model, rather than just being a Reactive “Break-Fix” Model; which is critical for achieving the 99.9% uptime standards of today's education.

Discussion of Security Integration

A layered protection approach - both at the perimeter (Core Firewall) and endpoints - has greatly improved the previous architecture used by the institution. A centralized point of management for all

DOI: https://doi.org/10.63671/ijsesr.v2i2.114

campus security (access control and IDS) is provided in the Core Switch/Firewall; therefore, with this design the MIS team is able to enforce role based access control as well as centrally managed detection systems for intrusion. With centralization of security policy enforcement it will be easier to prevent misconfigurations, and ensure consistent application of campus-wide security policy across all departments.

4. Conclusion

The researchers conclude that the proposed network is both robust and scalable to meet the digital needs of St. Nicolas College of Business and Technology. A hybrid star-bus design has effectively mitigated the "point of failure" issues associated with less complex systems. Long term technical viability will be ensured through the application of variable length subnet mask (VLSM). The move toward a proactive to reactive maintenance approach utilizing real time monitoring and an automated escalation matrix is required to support all critical business and educational functions at the college. The described framework provides the reliability needed for the college to take advantage of emerging technologies such as cloud based education initiatives and expanding Bring Your Own Device (BYOD) policies.

References

1. H. Abdul-Razzaq and A. Osamah, "Design and implementation of a VLSM simulator," Journal of Engineering, vol. 18, no. 9, pp. 1045-1055, 2012.
2. S. Adke and R. Bhawar, "A review on: Network design for college campus," International Journal of Recent Academic Research, vol. 7, no. 1, pp. 112-118, 2020.
3. M. N. B. Ali, "Design and implementation of a secure campus network," Journal of Surface Engineered Materials and Advanced Technology, vol. 5, no. 7, pp. 44-52, 2015.
4. N. Allen, Network Maintenance and Troubleshooting Guide: Field Tested Solutions. Pearson Education, 2010.
5. ElProCus, "Hybrid topology: Features, working, types & its applications," 2021. [Online]. Available: https://www.elprocus.com/hybrid-topology-working-types-applications/
6. A simulation-based study on network architecture using inter-VLAN routing and secure campus area network," International Journal of Computer Sciences and Engineering, vol. 6, no. 3, pp. 220-225, 2018.
7. SentinelOne, "Cybersecurity in higher education: Risks, best practices & frameworks," 2026. [Online]. Available: https://www.sentinelone.com/blog/cybersecurity-higher-education/
8. St. Nicolas College of Business and Technology, "Institutional network infrastructure proposal and technical plan," Internal MIS Documentation, 2026.