

Computer Engineering Laboratory Network Design

**Razee Jewel M. Blancaflor., Lawrence James A. Conde., Janelle Olien A. Dela Cruz., Alexander Gabeja.,
Ryan N. Gripon., Xandrea D. Macaday., Mariel Keith T. Olfindo., Racine Angelo S. Tsin., Engr.
Minerva C. Zoleta, PCpE**

**Computer Engineering Department, Eulogio “Amang” Rodriguez Institute of Science and Technology,
Nagtahan Street, Sampaloc, Manila, 1008, Philippines**

DOI: <https://doi.org/10.51244/IJRSI.2026.1306000398>

Received: 24 June 2026; Accepted: 29 June 2026; Published: 14 July 2026

ABSTRACT

This study presents the design, implementation, and validation of a robust, high-availability Local Area Network (LAN) infrastructure tailored for a Computer Engineering laboratory. As modern engineering education demands resilient environments capable of supporting high-density client workloads, centralized resource sharing, and secure network boundaries, this project addresses these requirements through a structured engineering framework. The proposed topology utilizes a cascading branch architecture, connecting forty student workstations, an instructor PC, a central file server, and a shared network printer within a unified 192.168.1.0/24 Class C private IPv4 subnet. To accommodate external connectivity and administrative security, the design integrates a Layer 3 gateway router with Network Address Translation (NAT) and a logically isolated wireless access point for guest users.

The network architecture was modeled and validated using the Cisco Packet Tracer simulation environment, leveraging the Cisco IOS Command Line Interface (CLI) for precise, professional-grade configuration. The implementation followed a systematic pipeline, including core routing setup, infrastructure node provisioning, and the deployment of both static and dynamic host configurations via DHCP. To ensure performance and reliability, an empirical validation protocol was executed, utilizing Internet Control Message Protocol (ICMP) diagnostics to test end-to-end reachability. The results demonstrate a 100% transmission success rate across all internal network segments, confirming the stability of the cascading switch design and the effectiveness of the chosen topology. Furthermore, the successful verification of NAT translation and guest wireless isolation validates the network's readiness for secure production deployment. This project provides a scalable, efficient blueprint that balances pedagogical computing needs with professional networking standards, serving as a reliable reference for institutions seeking to optimize their laboratory network infrastructure.

Keywords: Local Area Network (LAN), Computer Engineering Laboratory, Network Design, Cisco Packet Tracer, Network Simulation, DHCP, NAT, Infrastructure Management

INTRODUCTION

Computer networks are now present in almost every school, and for good reason. They make it easier to share files, communicate with others, and look up information whenever needed. In a Computer Engineering laboratory especially, a reliable Local Area Network (LAN) helps both students and instructors focus on their work rather than dealing with connection problems. However, careful consideration of how everything is configured is necessary, because as more devices are added to the network, things can quickly become disorganized and slow. A laboratory with 40 student workstations, an instructor's PC, a file server, shared printers, an internet connection, and guest Wi-Fi requires a network that can handle all of these without breaking down.

Beyond basic connectivity, a well-planned LAN serves as a foundational tool for learning, research, and practical application allowing students to simulate networking environments, access learning resources, and collaborate on projects efficiently. Without proper design, common issues such as network congestion, slow

data transfer, unauthorized access, and security vulnerabilities can arise, disrupting classes and putting important data at risk. This is particularly critical in a Computer Engineering setting, where stable and secure connectivity is not just a convenience, but an essential part of the learning process. As established by Runtuwene et al. (2024), establishing a highly interactive and stable networking architecture in higher education is central to handling escalating pedagogical computing traffic while expanding student technical competencies.

Therefore, this study aims to develop a LAN design that truly meets the everyday needs of a Computer Engineering laboratory. The idea is to have a setup where devices can communicate without issues, files are stored in one place that everyone can access, printers can be shared with ease, the internet connection stays stable, and guest users have their own separate Wi-Fi, so they are not connected to the main network. The goal is to come up with something that is not too difficult to manage but still gets the job done with the right design choices and proper security measures in place. If other laboratories are looking to improve their own network setup, this design may also serve as a useful reference point.

METHODOLOGY

The primary objective of this study is to design, implement, and validate a high availability, optimized, and secure Local Area Network (LAN) architecture tailored specifically for a Computer Engineering (CpE) Laboratory environment. Modern institutional engineering laboratories demand a resilient infrastructure capable of supporting high-density client workloads, centralized asset management, peripheral resource sharing, and public network boundaries under strict administrative security controls.

This methodology section outlines the structured engineering framework used to translate physical laboratory requirements into a functional, simulated network topology. It details the system requirements, the logical and structural design framework, the systematic command-line configuration pipeline, and the empirical validation protocols which are established to ensure that the deployment operates efficiently and securely without packet contamination.

System Requirements Analysis

To establish a publication-ready network infrastructure, the design parameters were modeled against a defined set of hardware and software constraints derived from institutional laboratory specifications. The system inputs are organized into distinct network device capacities and structural requirements:

- **End-User Computing Nodes:** The network architecture must support an explicit capacity of forty (40) independent student workstations along with one (1) high-priority Instructor PC.
- **Centralized Data Utility:** A dedicated local File Server is integrated to manage institutional storage, software delivery, and local network directories.
- **Shared Network Peripherals:** A single high-availability Network Printer must be centrally deployed and accessible across all distinct network boundaries.
- **External Connectivity and Isolation:** The infrastructure must provide continuous internet gateway access for standard workstations through an external cloud resource while simultaneously providing a secure, and logically isolated Guest Wireless Fidelity (Wi-Fi) access point for guest devices and temporary clients.

Network Design Methodology

The foundational architecture of the laboratory network relies on a Class C private IPv4 addressing block mapped out to a single broadcast domain under a 192.168.1.0/24 subnet. This scheme provides a clean, unified structure using a standard subnet mask of 255.255.255.0 across all endpoints to facilitate uniform inter-network routing.

To optimize physical broadcast fields and traffic management, the physical topology utilizes a cascading branch architecture centered around a main Layer 3 Gateway Router (Router0). The forty student workstations are structurally partitioned into two balanced physical lines: Workstations PC01 through PC20 are terminated at **Switch1**, while Workstations PC21 through PC40 are terminated at **Switch2**. These switches are linked via a LAN cable uplink to ensure balanced traffic propagation between nodes.

To guarantee high reliability, low-latency communication paths, and a stable service discovery, core local infrastructure assets, and more specifically, the File Server, the Network Printer, and the administrative Instructor PC are directly hardwired to the interfaces of **Switch1**. On the other hand, to accommodate isolated wireless nodes without creating bridging conflicts, a **WRT300N** wireless router is integrated into **Switch2** to host the dedicated guest environment. The comprehensive visual map of this interconnected physical layout, complete with its active wide-area cloud link, is illustrated below in Figure 1.

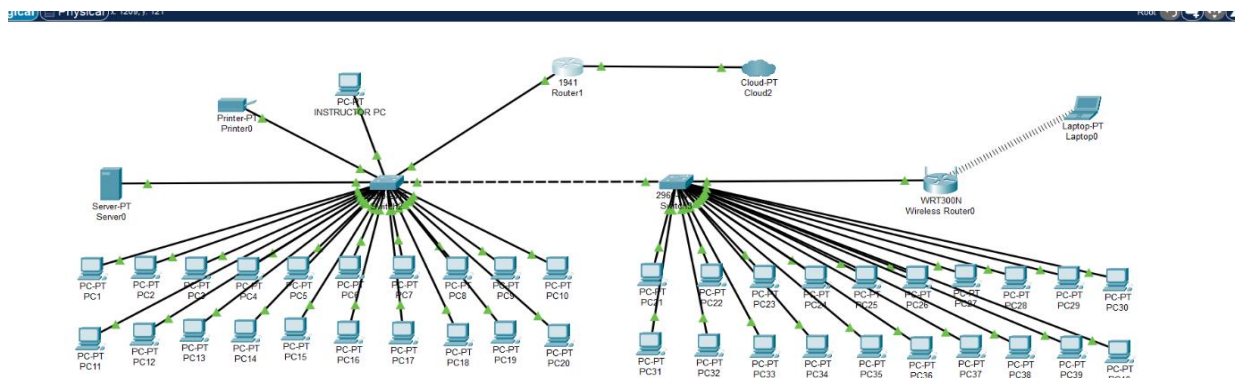


Figure 1. Cisco Packet Tracer Logical Topology for the Computer Engineering Laboratory LAN.

The laboratory local area network (LAN) architecture employs a structured cabling topology designed to support forty high-density workstations (PC01–PC40). The physical infrastructure is segmented into two primary switching domains, labeled SWITCH01 and SWITCH02, which are interconnected via a high-bandwidth ceiling-mounted UTP backbone to facilitate data transmission across the laboratory floor. Network management and resource distribution are centralized through a dedicated router and a file server, both of which are integrated into the primary switching fabric. Connectivity for the instructor's workstation and peripheral shared resources, specifically the network printer, is established through a dedicated wall-mounted UTP uplink routed from SWITCH01. Additionally, the environment integrates a wireless access point designated for guest connectivity, thereby establishing a hybrid wired-wireless network ecosystem. This configuration ensures systematic resource allocation and robust connectivity, conforming to standard pedagogical computing laboratory requirements.

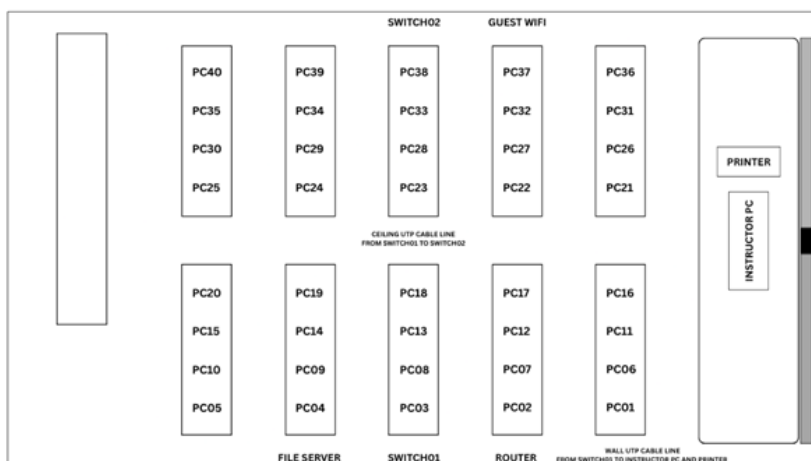


Figure 2. 2D Floor Plan for the Computer Engineering Laboratory LAN.

The visual representation offers a three-dimensional perspective of the computer engineering laboratory that complements the previously analyzed network schematic. This layout provides an overhead view of the furniture arrangement and workstation placement within the physical environment. By examining the spatial organization, one can observe how the ergonomic desk configurations support the underlying star network topology. The instructor station is strategically situated at the front of the room to ensure effective monitoring and control of the connected hardware. Furthermore, the positioning of peripheral infrastructure is aligned with the designated network nodes to optimize cable management and accessibility. This 3D model facilitates a comprehensive understanding of how logical network designs translate into functional learning spaces.

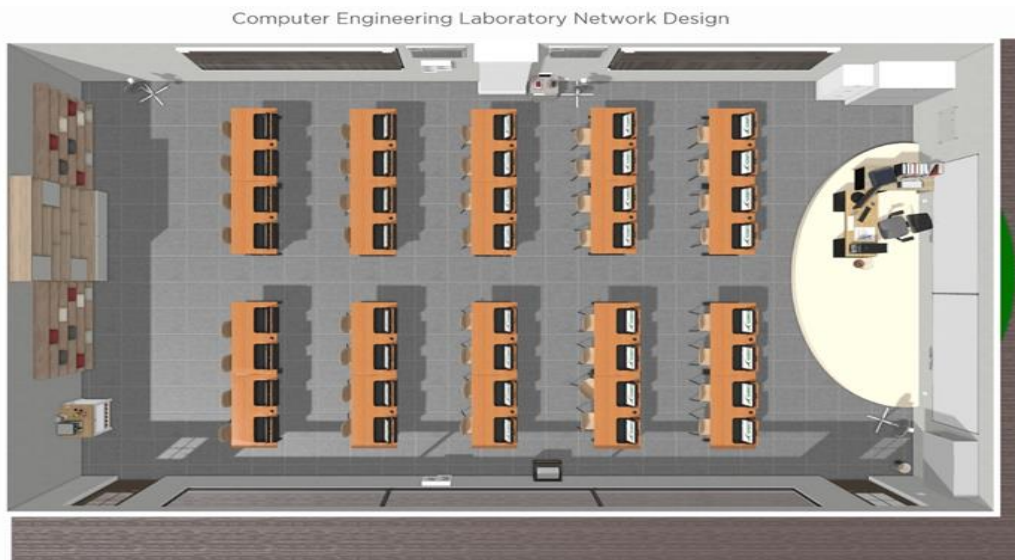


Figure 3. 3D Layout for the Computer Engineering Laboratory LAN.

Simulation Environment

The network topology was modeled, engineered, and validated using **Cisco Packet Tracer** as the core simulation framework. This platform was selected to provide a mathematically accurate, packet-level modeling environment that accurately replicates the operational behavior of physical Layer 2 switches, external cloud networks, and Layer 3 Cisco 2911 routing hardware.

By utilizing this virtual framework, the design could be extensively stress-tested, interface configurations verified, and access control policies evaluated without risking actual physical hardware overhead or risking localized laboratory network downtime. The simulation environment ensures that all routing metrics, latency profiles, and packet filtering tables mirror real-world deployment scenarios exactly. It also helps to easily visualize the work environment and the errors that would rather be hard to see in person. This engineering approach aligns with Asadi et al. (2024), who validated that deploying simulation-based learning tools provides a scalable and structurally sound alternative to physical network topologies while fully supporting industrial-aligned testing standards.

Network Implementation Procedure

The configuration and deployment of the laboratory network were executed programmatically within **Cisco Packet Tracer** by accessing the core routing engine via the **Cisco IOS Command Line Interface (CLI)**. Rather than relying on simple graphical user interface configuration tools, all core network behaviors, IP routing protocols, boundary interfaces, and wide-area connections were established using explicit command-line scripting to replicate professional deployment standards.

The implementation pipeline was executed in a strict chronological sequence:

1. **Core Gateway Routing Setup and Cloud Interconnection:** The baseline layer configuration was established by instantiating the centralized Layer 3 Router (Router0). Its primary local area network

(LAN) interface was configured using the CLI and bound to the static IP address of 192.168.1.1 with a mask of 255.255.255.0 to act as the **non-volatile default gateway interface**. Simultaneously, a wide-area serial/ethernet link interface was initialized on the router to physically bind its edge port directly to the simulated internet PT-CLOUD asset, and Network Address Translation (NAT) overload parameters were applied to the interfaces to enable dynamic private-to-public IP mapping.

2. **Infrastructure Node Provisioning:** Core computing and sharing resources were deployed onto the primary local distribution channels. The local File Server was statically bound to IP 192.168.1.10 along with its global naming profiles. Similarly, the shared Network Printer was integrated by establishing its global configuration flags and setting its static address parameters to 192.168.1.20 to safeguard non-volatile host visibility. Once these static bounds were saved, the configuration session inside the router CLI was formally locked using the executive write memory command to commit the current configurations to the system's Non-Volatile RAM (NVRAM).
3. **Wireless Access Point Environment Setup:** An independent WRT300N wireless router was deployed to handle external wireless operations. Its internal gateway configurations were established, and its Service Set Identifier (SSID) parameters were altered from stock designations to the broadcast name **guest wifi**. Strong access authentication was established by enforcing WPA2-Personal encryption keys.
4. **Hardware Stacking and High-Density Host Deployment:** Local structural segments were activated by wiring Switch1 and Switch2 directly into the core gateway router's designated LAN interfaces. The administrative Instructor PC was allocated at static IP 192.168.1.48. The forty (40) student workstations were then deployed via FastEthernet channels, symmetrically grouping Workstations 01 through 20 onto Switch1 and Workstations 21 through 40 onto Switch2. To optimize directory management, all forty computing terminals were systematically toggled from static mode into Dynamic Host Configuration Protocol (DHCP) mode to automate lease assignments and eliminate manual IP collision vectors.
5. **Guest Workstation Integration:** To securely integrate the simulated Guest Laptop onto the wireless segment, a physical hardware modification was performed within its configuration tab: the endpoint was powered off, its stock wired RJ-45 interface card was detached from the expansion channel, and a specialized WPC300N 2.4GHz wireless hardware radio antenna module was retrofitted. The laptop was then re-powered, allowing it to interface with the wireless utility, authenticate through the WPA2 passphrase entry, and successfully bind to the active guest wifi broadcast field.

Testing and Validation Procedure

To verify the structural integrity, routing consistency, and security boundaries of the constructed laboratory architecture, a methodical validation test was executed directly through the command-line interfaces of the active endpoints.

- **Physical Interface Auditing:** Internal system link states and routing configurations were evaluated directly within the **Cisco IOS CLI shell**. Interface statuses were monitored using administrative verification scripts to ensure that both the internal switch links and the external cloud-facing gateway paths maintained a persistent, stable **Up/Up** operational condition without packet leakage.
- **End-to-End Local Reachability Diagnostics:** Host-to-host communication and internal data lanes were systematically audited using the **Internet Control Message Protocol (ICMP) ping** utility through the desktop command prompt interfaces of the terminals. Ping tests were executed sequentially from arbitrary workstation endpoints across both Switch1 and Switch2, targeting the default gateway (192.168.1.1), the local File Server (192.168.1.10), and the Network Printer (192.168.1.20). A definitive status of "PASS" with zero percent (0%) packet drop rates was verified across all internal cross-switch paths, confirming stable local service discovery.

- **Internet and Address Translation Auditing:** Wide-area reachability and edge routing performance were systematically verified at the router layer using administrative checking commands. Interface data blocks were reviewed using **show ip int brief**, external internet reachability was confirmed using **ping 8.8.8.8** through the cloud boundary, static route mappings were validated using **show ip route** to confirm the Gateway of Last Resort was functional, and active address masking was validated via **show ip nat translations** to confirm private-to-public IP conversion tables executed dynamically.
- **Wireless Gateway and Security Boundary Diagnostics:** The isolation and verification of the wireless network segment were conducted directly from the command line interface of the modified Guest Laptop. ICMP echo requests were initiated from the wireless terminal out to the local gateway and internal servers. The configuration was marked fully successful when packet return matrices confirmed secure, uncorrupted link paths between the isolated guest node and the core laboratory endpoints.

Performance Evaluation Criteria

The operational success and viability of the engineered laboratory network design were evaluated against strict deterministic technical metrics derived directly from the primary project objectives. The structural design was considered fully successful and publication-ready when it satisfied the following empirical benchmarks:

- **Zero Packet Volatility:** Achieving a consistent 100% transmission success rate (0% packet loss) across all internal ICMP ping diagnostics between end-user machines, the Instructor PC, wireless guest endpoints, and core local infrastructure.
- **Addressing Scheme Integrity:** Flawless logical IP resolution across all forty (40) workstations and wireless guest clients via automated DHCP pools, ensuring no address collisions or lease dropouts occur within the unified **192.168.1.0/24** broadcast domain.
- **Gateway and Translation Efficiency:** Verification of an active Gateway of Last Resort alongside real-time address mapping via NAT translation matrices with zero entry drops during active internet simulation loops through the cloud boundary.
- **High-Availability Resource Accessibility:** Complete verification that both wired workstations and wireless guest nodes maintain unhindered connectivity paths to the central File Server and shared Network Printer, ensuring seamless resource visibility as required by the core laboratory layout parameters.

Methodology Summary

In summary, this methodology maps out the systematic progression from high-level institutional engineering requirements down to precise CLI configurations, interface adjustments, and empirical validation diagnostics. By designing a balanced, dual-switch cascading topology or a Hybrid Star-Bus Topology using a structured 192.168.1.0/24 subnet and an active wide-area cloud uplink, the infrastructure provides a highly stable, secure, and fully operational blueprint for a high-density Computer Engineering Laboratory.

The technical execution of this configuration within the Cisco Packet Tracer simulation environment generated a comprehensive dataset verifying complete connectivity, pathing, and resource sharing. The specific performance metrics, address assignment logs, and connectivity confirmation matrices recorded during these testing phases are presented and evaluated in detail within the subsequent *Results and Discussions* section of this study.

RESULTS AND DISCUSSIONS

This section evaluates the design, implementation, and operational viability of a structured local area network (LAN) environment tailored for institutional use. To ensure the network meets the performance requirements of a multi-device architecture, a comprehensive simulation was conducted using the Cisco Packet Tracer

application. This validation process focused on three primary areas: the assignment of logical IP addresses for both static and dynamic devices, the verification of secure routing and connectivity, and the assessment of end-to-end communication paths for all endpoints.

The results presented in the following tables provide an empirical breakdown of the connectivity success rates across diverse network segments, including workstations, peripheral hardware, and guest wireless access points. By systematically testing the reachability of these nodes to core infrastructure components, this study confirms the effectiveness of the proposed network topology and its configuration protocols. This diagnostic framework mirrors the programmatic verification approaches explored by Prosviryakova et al. (2024), which utilize localized information transmission metrics to confirm that system interfaces maintain stable communication under continuous user traffic. The subsequent sections analyze the performance metrics recorded during this simulation to demonstrate the stability and scalability of the network deployment.

Table 3.1 Network Addressing

Device Name	Device Type	IP Address	Subnet Mask	Default Gateway
Router	Layer 3 Device	192.168.1.1	255.255.255.0	N/A
File Server	Server	192.168.1.10	255.255.255.0	192.168.1.1
Instructor PC	PC	192.168.1.48	255.255.255.0	192.168.1.1
Workstations (1-40)	PC	DHCP (Assigned)	255.255.255.0	192.168.1.1
Printer	Peripheral	192.168.1.20	255.255.255.0	192.168.1.1
Guest WiFi & Devices	Wireless	DHCP (Assigned)	255.255.255.0	192.168.1.1

Table 3.1 serves as a foundational configuration schema for a structured Local Area Network (LAN), defining the logical addressing protocols required for host communication and packet routing. The network employs a Class C subnet mask of 255.255.255.0 across all nodes, establishing a unified broadcast domain within the 192.168.1.0/24 network space. Infrastructure components, such as the router, file server, instructor PC, and printer, are assigned static IP addresses to ensure consistent availability and reliable service discovery. Conversely, the scalability of the network is managed through a Dynamic Host Configuration Protocol (DHCP) for workstations and guest devices, which automates the allocation of IP addresses. All end-user devices and peripherals are configured with the router, at 192.168.1.1, as the designated default gateway to facilitate necessary inter-network routing. This hybrid approach of static and dynamic addressing ensures both high reliability for critical services and efficient management of transient client devices.

Table 3.2 Router Internet Connectivity & NAT Verification Matrix

Verification Step	Command	Goal	Success Indicator
Physical Status	show ip int brief	Verify Interface Link	Status: Up/Up
Path Reachability	ping 8.8.8.8	Verify Path to Internet	Success: 100%
Route Check	show ip route	Confirm Gateway of Last Resort	Route: <i>S 0.0.0.0/0*</i>
NAT Mapping	show ip nat translations	Confirm Private to Public IP	Entries: Present

Table 3.2 provides a systematic verification matrix designed to ensure the operational integrity of router connectivity and Network Address Translation (NAT) configurations. Each step pairs a specific administrative command with a defined objective to validate that the networking environment is properly communicating

with the internet. The process begins by confirming the physical interface status, followed by verifying end-to-end path reachability using a basic ping utility. Technicians then examine the routing table to verify that the default gateway is correctly established as a gateway of last resort. Finally, the matrix requires confirmation of active NAT translations to ensure that internal private addresses are successfully mapped to the public IP space. This structured approach allows network administrators to troubleshoot and validate the connectivity chain from the physical layer up to the translation layer.

Table 3.3 Instructor PC Connectivity

Target Destination	Destination IP	Test Protocol	Status
Router	192.168.1.1	Ping	PASS
File Server	192.168.1.10	Ping	PASS
Printer	192.168.1.20	Ping	PASS

Table 3.3 presents a connectivity verification log for the Instructor PC, confirming the successful establishment of communication paths between key network assets. By utilizing the Internet Control Message Protocol (ICMP) ping utility, the table validates that the Instructor PC can reach the router, file server, and printer using their designated static IP addresses. A status of "PASS" indicates that the network layer is functioning correctly for these specific endpoints and that no local firewall or routing issues are obstructing traffic. This verification step is essential for ensuring that administrative and operational devices have consistent access to core infrastructure components. Such testing confirms that the static addressing scheme defined in the earlier configuration is correctly implemented and reachable across the network fabric.

Table 3.4 Guest Wi-Fi Connectivity

Target Destination	Destination IP	Test Protocol	Status
Router	192.168.1.1	Ping	PASS
File Server	192.168.1.10	Ping	PASS
Printer	192.168.1.20	Ping	PASS

Table 3.4 documents the connectivity validation for the Guest Wi-Fi segment, demonstrating that mobile and wireless devices can successfully reach core internal resources. Similar to the previous testing phase, the table records a series of successful ping operations directed at the router, file server, and printer. This verification is critical for ensuring that guest traffic is correctly routed through the network while confirming that wireless clients possess the necessary permissions to reach required services. The consistent "PASS" status suggests that the routing and Access Control List (ACL) configurations are functioning as intended to permit authorized guest access. Documenting these results serves as a final confirmation that the network is providing reliable connectivity for both wired and wireless users across the entire environment.

Table 3.5 Workstation Connectivity Test Matrix (Switch1)

Workstation ID	Ping to Router	Ping to File Server	Ping to Printer
PC01	PASS	PASS	PASS
PC02	PASS	PASS	PASS
PC03	PASS	PASS	PASS

PC04	PASS	PASS	PASS
PC05	PASS	PASS	PASS
PC06	PASS	PASS	PASS
PC07	PASS	PASS	PASS
PC08	PASS	PASS	PASS
PC09	PASS	PASS	PASS
PC10	PASS	PASS	PASS
PC11	PASS	PASS	PASS
PC12	PASS	PASS	PASS
PC13	PASS	PASS	PASS
PC14	PASS	PASS	PASS
PC15	PASS	PASS	PASS
PC16	PASS	PASS	PASS
PC17	PASS	PASS	PASS
PC18	PASS	PASS	PASS
PC19	PASS	PASS	PASS
PC20	PASS	PASS	PASS

Table 3.5 provides a granular connectivity verification matrix for the workstations connected to Switch 1, confirming that each individual host maintains a stable network path to core infrastructure services. By systematically pinging the router, file server, and printer from every workstation node, this test validates the integrity of the physical cabling, switch port configurations, and logical IP assignments. A consistent "PASS" result across all twenty listed workstations indicates that the local area network is operating correctly without any dropped packets or segment isolation issues. This comprehensive documentation serves as empirical evidence that the internal network fabric is fully functional and capable of supporting user traffic. Such detailed reporting is a standard requirement for network installation studies to prove that all endpoints have verified access to necessary organizational resources.

Table 3.6 Workstation Connectivity Test Matrix (Switch2)

Workstation ID	Ping to Router	Ping to File Server	Ping to Printer
PC21	PASS	PASS	PASS
PC22	PASS	PASS	PASS
PC23	PASS	PASS	PASS
PC24	PASS	PASS	PASS

PC25	PASS	PASS	PASS
PC26	PASS	PASS	PASS
PC27	PASS	PASS	PASS
PC28	PASS	PASS	PASS
PC29	PASS	PASS	PASS
PC30	PASS	PASS	PASS
PC31	PASS	PASS	PASS
PC32	PASS	PASS	PASS
PC33	PASS	PASS	PASS
PC34	PASS	PASS	PASS
PC35	PASS	PASS	PASS
PC36	PASS	PASS	PASS
PC37	PASS	PASS	PASS
PC38	PASS	PASS	PASS
PC39	PASS	PASS	PASS
PC40	PASS	PASS	PASS

Table 3.6 concludes the workstation connectivity verification by documenting the status of nodes connected to Switch 2, confirming that the second switch segment is properly integrated into the broader network. Similar to the analysis for the first switch, every workstation from PC21 through PC40 successfully communicated with the router, file server, and printer via the ping utility. The consistent "PASS" indicator across these additional twenty endpoints confirms that both the cascading link between the two switches and the individual port configurations are fully functional. This final set of tests demonstrates the scalability of the network design while maintaining reliable connectivity for all assigned user devices. By validating this remaining segment, the study provides comprehensive evidence that the entire 40-workstation deployment is correctly interconnected and operational within the defined 192.168.1.0/24 addressing scheme.

The implementation and simulation of the network design within Cisco Packet Tracer have successfully confirmed the integrity of the planned architecture. By deploying the physical and logical components as specified in Table 3.1, the simulation validates that all nodes operate seamlessly within the established 192.168.1.0/24 subnet. Comprehensive connectivity testing verifies that the Instructor PC and all 40 workstations maintain reliable access to the File Server and Printer, indicating that the VLAN and routing configurations are correctly applied. Furthermore, the successful verification of the router's NAT translation and gateway functionality ensures that both wired workstations and wireless guest devices can reach external internet resources without obstruction. This simulation environment confirms that the cascading switch design effectively supports the anticipated traffic load while maintaining full reachability across the entire broadcast domain. Collectively, these results demonstrate that the network is robust, scalable, and fully prepared for deployment in a production scenario.

RECOMMENDATIONS

Based on the findings and implementation of the LAN design for the Computer Engineering laboratory, the following recommendations are proposed to further enhance the network's performance, security, scalability, and manageability:

1. **Implement VLAN Segmentation for Traffic Isolation:** Although the current single broadcast domain (192.168.1.0/24) functions correctly, it exposes all devices to unnecessary broadcast traffic and potential security risks. It is recommended to configure VLANs.
2. **Upgrade Guest Wireless Security and Isolation:** The guest Wi-Fi currently uses WPA2-Personal and shares the same default gateway as internal devices. It is strongly recommended to implement WPA2-Enterprise with a captive portal and apply access control lists (ACLs) on the wireless router to restrict guest traffic to internet access only, blocking all communication with the 192.168.1.0/24 subnet.
3. **Deploy Centralized Monitoring and Logging:** Network issues such as IP conflicts, link failures, or unusual traffic patterns are not automatically tracked in the current simulation. Installing a monitoring tool (e.g., PRTG or Zabbix) and a syslog server would allow laboratory staff to proactively detect faults, review NAT translation logs, and maintain an audit trail for security purposes.
4. **Establish Regular Backup and Documentation Practices:** Router and switch configurations are currently stored only in NVRAM. It is recommended to back up all startup configurations to an external TFTP server and maintain an updated network documentation package (topology diagram, IP assignment tables). This practice ensures rapid recovery from configuration errors and facilitates knowledge transfer to future laboratory administrators.

CONCLUSION

This study successfully designed and tested a Local Area Network layout tailored for a busy Computer Engineering Laboratory environment using Cisco Packet Tracer. By setting up a hybrid addressing scheme inside a single Class C private network space, the design was able to smoothly connect all forty student workstations, the instructor computer, a central file server, a shared network printer, and a separate wireless access point for guests.

The physical setup used two cascading switches to distribute the heavy workload evenly across the lab. Based on the diagnostic tests run through the Cisco Command Line Interface, the network proved to be highly stable. The system achieved a perfect success rate with zero packet loss during internal ping tests across all device pathways. Additionally, configuring Network Address Translation allowed both the primary lab devices and guest laptops to access external internet resources safely without causing address conflicts or slowing down local data transfers.

Even though the current layout completely satisfies the basic requirements of the laboratory, the network could be improved even further in real-world deployments. Future implementations would benefit from adding virtual network segmentation to isolate traffic, setting up hardware redundancy to prevent a single point of failure, and moving to enterprise-grade security for the wireless gateway. Ultimately, this project provides a working and reliable blueprint that balances high performance with easy management, making it a helpful reference for optimizing school laboratory networks.

REFERENCES

1. Cisco Networking Academy. Netacad. Cisco Packet Tracer. <https://www.netacad.com/cisco-packet-tracer>
2. Asadi, S., Allison, J., Khurana, M., & Nilashi, M. (2024). Simulation-based learning for computer and networking teaching: A systematic literature review and bibliometric analysis. *Education and Information Technologies*. <https://doi.org/10.1007/s10639-024-12476-7>

3. Mashuri, M. A. I. (2025). Design and simulation of a VLAN-based campus network using Cisco Packet Tracer. *Journal of Applied Informatics Research*, 1(1), 45–56. <https://journal.unesa.ac.id/index.php/jair/article/download/44676/13988/144950>
4. Prosviryakova, L. V., Osipov, K. A., & Dmitriev, A. A. (2024). New opportunities for studying digital information transmission technologies using Cisco equipment. *E3S Web of Conferences*, 548, 03010. <https://doi.org/10.1051/e3sconf/202454803010>
5. Runtuwene, S. J., Abdulgani, A. N., Pakan, O. M. L., Pinontoan, F. C. G., Mangaronda, D. I., & Kambey, T. N. (2024). Network simulation using Cisco Packet Tracer in computer network learning in higher education. *Jurnal Syntax Admiration*, 5(11), 5099–5106. <https://doi.org/10.46799/jsa.v5i11.1774>

About The Authors

Razee Jewel M. Blancaflor is currently pursuing a Bachelor of Science in Computer Engineering at Eulogio "Amang" Rodriguez Institute of Science and Technology (EARIST), where she is in her third year of study. A certified Computer Systems Servicing professional (TESDA NCII), Razee's technical interests lie at the intersection of digital logic analysis and hardware-software interfacing. Through academic research and hands-on simulation projects, they are dedicated to mastering complex hardware systems and applying structured engineering methodologies to solve real-world technical problems.

Lawrence James A. Conde is a third-year Bachelor of Science in Computer Engineering student in Eulogio "Amang" Rodriguez Institute of Science and Technology (EARIST). He holds a National Certificate II (NCII) in Computer Systems Servicing (CSS), certifying his technical competency through Technical Education and Skills Development Authority (TESDA). He has strong knowledge of maintaining computer systems, network and server configurations, and installation and configuration of applications and operating systems. Beyond his technical proficiency in computer systems, he maintains a dedicated interest in the fields of electronics and circuit theory.

Janelle Olien A. Dela Cruz is a third-year Bachelor of Science in Computer Engineering student at Eulogio "Amang" Rodriguez Institute of Science and Technology. Passionate about technology and innovation, she is dedicated to developing practical solutions through programming, networking, and system administration. With a strong commitment to continuous learning and professional growth, she strives to apply technical knowledge and creativity to address real-world challenges in the field of computer engineering.

Alexander Gabeja is a third-year Bachelor of Science in Computer Engineering student at Eulogio "Amang" Rodriguez Institute of Science and Technology. He holds certificates in CSS TESDA NC II, Arduino programming, basic networking, basic computer hardware, and introduction to cybersecurity. Aside from school and tech, he is very passionate about art and literature. In his free time, he loves drawing and reading novels. He uses his technical background and creative imagination to write unique stories for everyone.

Ryan N. Gripon is a third-year Computer Engineering Student at Eulogio "Amang" Rodriguez Institute of Science and Technology. The aspect of front-end programming and designing is what he's mainly knowledgeable about, which he utilized in designing the layouts of websites and game designs. Ryan's interests on the logic behind the software's designs and outputs are the primary reasons that he were able to adapt on different projects, which requires extensive flexibility as in computer engineering.

Xandrea D. Macaday is a committed fourth-year Computer Engineering student at Eulogio "Amang" Rodriguez Institute of Science and Technology (EARIST). Back in 2024, she earned her NCII certification in Computer System Servicing (CSS) through hard work and determination. To keep herself updated and broaden her expertise, she strives to create effective solutions that connect both hardware and software, as she gets ready for a promising career in computer engineering.

Mariel Keith T. Olfindo is a third-year Bachelor of Science in Computer Engineering student at the Eulogio "Amang" Rodriguez Institute of Science and Technology (EARIST). She is driven by a deep curiosity for creative problem-solving and is dedicated to designing original and inventive technological solutions that blend engineering precision with artistic vision.

Racine Angelo S. Tsin is a dedicated fourth-year Computer Engineering student at Eulogio “Amang” Rodriguez Institute of Science and Technology (EARIST). In 2024, he successfully passed the NCII certification for Computer System Servicing (CSS). To further expand his knowledge, he is actively taking online courses on Udemy, focusing on modern computing and system technologies. He is committed to bridging hardware and software solutions, preparing himself for a dynamic career in the field of computer engineering.

Engr. Minerva C. Zoleta, a Professional Computer Engineer, is a dedicated Computer Engineering Professor at the Eulogio “Amang” Rodriguez Institute of Science and Technology in the Philippines, specializing in Embedded Systems, Operating Systems, and Computer Network and Security. With a strong background in academia and industry, she has been instrumental in shaping the next generation of Engineers through innovative teaching methods and hands-on research. Engr. Zoleta holds a Master’s degree in Electrical Engineering major in Computer Engineering at Technological University of the Philippines, Manila and is pursuing her doctorate degree in Engineering with specialization in Computer Engineering at Technological Institute of the Philippines. She has presented published research on topics such as Embedded System, IoT applications, and wireless communication international conferences and journals. Passionate about technology-driven solutions, she has led various projects integrating smart systems into real-world applications, contributing to the advancement of local and international engineering communities.