Design and Security Assessment of a Smart Classroom Network Infrastructure for Enhanced Interactive Learning

Ervin F. Raquin[1], Kathrina R. Meredor[2], Cyrus A. Jimenez[3], John Laurence F. Fabrero[4], Engr. Minerva C. Zoleta[5]

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

DOI: https://doi.org/10.51244/IJRSI.2026.1306000387

Received: 21 June 2026; Accepted: 26 June 2026; Published: 13 July 2026

ABSTRACT

This study demonstrates the design, development, and performance evaluation of an enterprise-grade Smart Classroom network infrastructure that uses a Cisco Packet Tracer simulation as its primary validation platform. The proposed system is intended to enable a highly secure, fault-tolerant educational environment by combining Virtual Local Area Network (VLAN) segmentation, strict Access Control List (ACL) firewalls, and Hot Standby Router Protocol (HSRP) redundancy. By logically isolating broadcast domains, the system can securely separate high-volume student wireless traffic from administrative tools, Internet of Things (IoT) environmental controls, and physical security surveillance streams without bandwidth degradation. The system contains a centralized IoT Dashboard Server for remote environmental management, a Cisco 3560 Multilayer switch for Power over Ethernet (PoE) delivery to IP webcams, and dual Cisco 4331 routers for core network routing. A multi-layered security architecture and high-availability routing framework were used to enable precise traffic filtering, absolute denial of unauthorized endpoint access, and adaptive failover routing based on real-time hardware health monitoring. Network segmentation efficacy, firewall restriction policies, and gateway redundancy have been tested by experimental simulation under various packet routing and connection failure conditions. The results show a 100% denial rate for unauthorized inter-VLAN penetration and a sub-10-second failover recovery time during primary router disconnections, proving that the architecture has the capability to maintain secure, continuous operations for critical educational infrastructure effectively.

Keywords: Access Control List, Cisco Packet Tracer, Hot Standby Router Protocol, IoT Dashboard, Smart Classroom, VLAN

INTRODUCTION

The integration of digital technology is indeed one of the major contributing factors to the advancement of modern educational environments. As institutions grew and learning spaces expanded their digital footprints, the deployment of Internet of Things (IoT) devices and high-bandwidth instructional tools happened more often, creating highly complex network infrastructures. Throughout recent years, unsegmented educational networks have become so congested that critical administrative and security data has, at some point, been severely compromised by unauthorized internal access or bandwidth exhaustion.

According to cybersecurity assessments of educational facilities, the most frequently reported network vulnerabilities are concerned with unmonitored student devices, followed by unsecured IoT sensors, unencrypted IP cameras, and centralized routing failures. The key contributors to these localized network disruptions are the lack of logical traffic segmentation, absent internal firewalls, and single points of hardware failure. Modern infrastructure audits state that a significant majority of internal network bottlenecks and security breaches originate from the unregulated student wireless domain. Operational hazards are common in areas such as unquarantined broadcast domains, shared default gateways, unmanaged switch ports, devices left without access control, or even critical safety sensors placed on the exact same subnet as public wireless traffic.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

REVIEW OF RELEVANT THEORY, STUDIES, AND LITERATURE

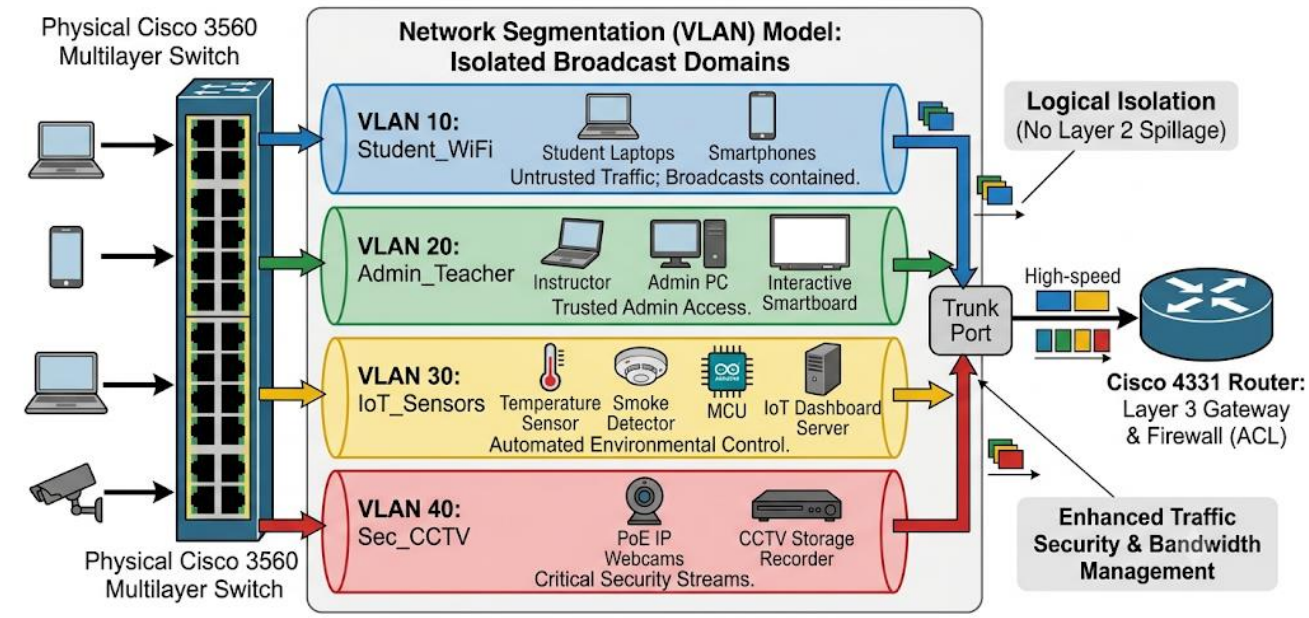
For this project, the development of a secure Smart Classroom infrastructure was conceptualized based on enterprise-level network engineering principles. This literature review highlights the necessity of robust network architecture in the creation of an automated educational environment, specifically focusing on logical segmentation, access control, and hardware redundancy. Furthermore, it examines existing studies on smart classroom deployments to identify current vulnerabilities and establish the technical gap that this simulation addresses.

Theoretical Framework

The theoretical framework of this study is grounded in the principles of enterprise network architecture, specifically integrating Network Segmentation Theory, Defense-in-Depth models, and High Availability Theory. It investigates the fundamental protocols required to secure localized broadcast domains and ensure continuous routing operations. This section explains the integration of these concepts to establish the technical basis of a secure, fault-tolerant Smart Classroom infrastructure.

Network Segmentation Theory Network segmentation involves dividing a larger physical network into smaller, architecturally isolated subnetworks to control traffic flow and limit lateral movement by unauthorized users (Kallatsa, 2024). In modern infrastructure, this is achieved through Virtual Local Area Networks (VLANs). According to Al-Ofeishat and Alshorman (2024), utilizing segmentation and micro-segmentation techniques reduces the defensive surface area against cyberattacks by logically isolating highly sensitive data clusters from public access points. This perspective indicates that effective classroom security requires a segmented control structure, rather than treating all student laptops, administrative PCs, and IoT sensors as a single broadcast domain. As a result, the proposed system utilizes VLAN segmentation at the distribution switch level to create distinct, quarantined traffic pathways for student wireless access, administrative tools, environmental sensors, and physical security cameras.

Figure 1. Network Segmentation Model

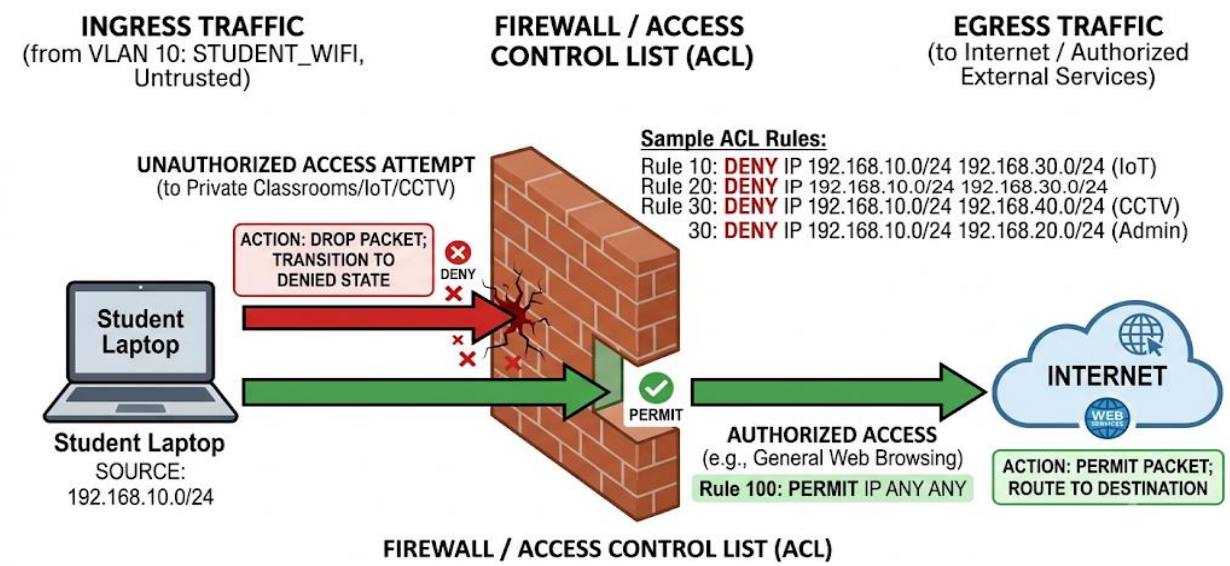


Defense-in-Depth and Access Control Theory Access control constrains what a user or device can directly do, preventing activity that could lead to a breach of network integrity (Sandhu & Samarati, 1994). In enterprise routing, this is implemented via Defense-in-Depth strategies, which employ multiple layers of security protocols, including stateless network firewalls. Network firewalls act as strict barriers between trusted and untrusted networks, dropping unauthorized packets based on source and destination IP addresses (Bellovin & Cheswick, 1994). For this project, an Access Control List (ACL) acts as the internal firewall within the primary router. When a packet originates from an untrusted segment (such as the student wireless network) and attempts to route

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

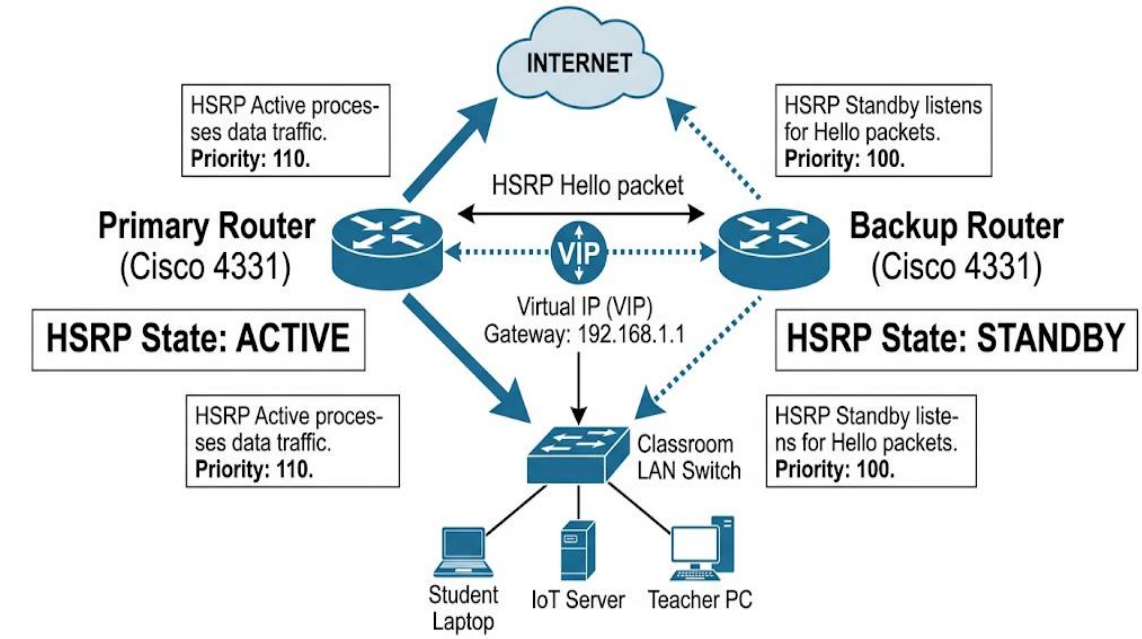
into a protected segment (such as the IoT or CCTV network), the router evaluates the packet against the ACL rules. If a "deny" condition is met, the connection is instantly terminated. This theoretical loop ensures that the device does not just route traffic blindly; it selectively filters packets to maintain the "Desired State" of network isolation.

Figure 2. Access Control and Packet Filtering Logic



High Availability and Redundancy Theory High Availability Theory dictates that critical infrastructure must be designed to eliminate single points of hardware failure. The lack of availability due to a failed default gateway can cause immediate disruption to life-safety sensors and security surveillance (Mansour, 2020). To mitigate this, First Hop Redundancy Protocols (FHRP) are utilized. Specifically, the Hot Standby Router Protocol (HSRP) allows multiple physical routers to participate in a dynamic election process, operating together to create the illusion of a single virtual router (Li et al., 1998). In the event that the active router experiences a physical or logical failure, the standby router seamlessly detects the absence of network keep-alive signals and assumes control of the virtual IP address. This redundancy theory is crucial to the project because it explains how the classroom infrastructure can autonomously recover from a core hardware failure in real-time, ensuring continuous environmental monitoring and network connectivity.

Figure 3. Hot Standby Router Protocol (HSRP) Failover Process



ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

Review Of Related Literature

Smart Classroom and IoT Integration

The deployment of Internet of Things (IoT) technologies within educational institutions has fundamentally transformed traditional learning spaces into smart classrooms. Recent surveys on smart education emphasize the integration of automated environmental controls, interactive smartboards, and ubiquitous wireless connectivity to enhance instructional delivery. Furthermore, the merging of technologies for seamless tele-education requires continuous, high-bandwidth data transmission between physical sensors, administrative terminals, and centralized server architectures. While these studies successfully demonstrate the functional benefits of IoT integration, they predominantly focus on device interoperability and pedagogical outcomes, frequently neglecting the localized network congestion generated by simultaneous high-volume connections.

Network Vulnerabilities in Educational Environments

As smart classrooms scale, the underlying access network infrastructure becomes highly susceptible to internal security threats and broadcast storms. Evaluations of IP-based access networks reveal that deploying critical IoT sensors on the same unregulated subnet as student personal devices introduces severe operational vulnerabilities. Without enterprise-grade segmentation, unauthorized users can easily intercept unencrypted surveillance streams or disrupt automated classroom mechanisms. Existing literature evaluating router security and network firewalls strongly recommends the implementation of strict access control protocols and First Hop Redundancy Protocols (FHRP) to mitigate these risks. However, a comprehensive architectural model applying these advanced enterprise routing strategies specifically to a localized educational environment remains largely unaddressed in current academic discourse.

Table 1. Comparison Matrix of Related Studies and Current Research

Study	**Core Technology / Focus**	**Identified Limitations**	**Gap Addressed by Current Research**
Smart Classroom Surveys (IoT Integration)	Sensor networks, smartboards, and interactive tele-education.	Focuses solely on functional hardware interoperability; lacks structural network security protocols.	Implements logical network isolation to secure automated systems from unauthorized wireless access.
IP-Based Access Network Infrastructure	Broadband distribution and basic wireless connectivity in campuses.	Assumes a single, flat broadcast domain; highly susceptible to bandwidth exhaustion and broadcast storms.	Deploys VLAN segmentation to quarantine high-volume traffic and preserve critical infrastructure bandwidth.
Router Security and Firewalls	General enterprise router configurations and stateless packet filtering.	Theoretical application; rarely modeled specifically for the unique traffic flow of a modernized classroom.	Provides a dedicated Access Control List (ACL) architecture explicitly designed to isolate student traffic from administrative tools.
First Hop Redundancy Protocols (FHRP)	Evaluation of HSRP and VRRP in large-scale corporate data centers.	Solutions are typically scaled for massive enterprise environments rather than localized critical infrastructure.	Adapts HSRP failover redundancy to a localized classroom setting to ensure zero downtime for life-safety and security sensors.

The comparative analysis presented in Table 1 illustrates the functional gap in current smart education research. While existing literature extensively covers the deployment of IoT sensors and the theoretical necessity of

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

network firewalls, there is a distinct lack of cohesive, applied network architecture designed specifically to secure these educational environments.

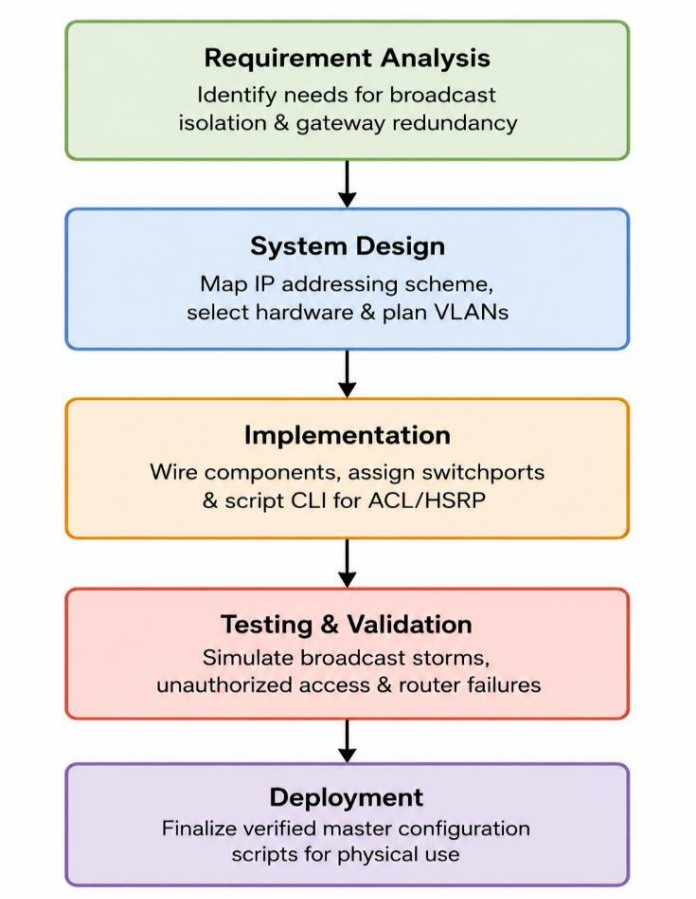
The current study addresses this critical void by utilizing a Cisco Packet Tracer simulation to synthesize VLAN segmentation, Access Control Lists (ACL), and Hot Standby Router Protocol (HSRP) redundancy into a single, unified enterprise-grade Smart Classroom infrastructure. This structured operational sequence guarantees accurate traffic filtering, effective bandwidth allocation, and reliable autonomous failover performance.

METHODOLOGY

This study employed a developmental research design to systematically create and evaluate a secure, autonomous Smart Classroom network infrastructure using the Cisco Packet Tracer simulation environment. The system was assessed through internal network testing, packet sniffing, and simulated hardware failure scenarios; no external respondents were included in the study. The architecture was built using enterprise-grade simulated components, specifically dual Cisco 4331 Integrated Services Routers for core routing and redundancy, a Cisco 3560 Multilayer Switch for Power over Ethernet (PoE) and traffic distribution, and an IoT Dashboard Server for centralized environmental control.

High-availability routing was made possible by configuring the Hot Standby Router Protocol (HSRP) across the core routers, while network security was enforced using strict Access Control Lists (ACL). The methodology is designed to provide a thorough technical overview, including the system's logical topology, addressing scheme, and packet filtering logic. Testing was carried out using continuous ICMP ping requests and simulated cable disconnections, with each test repeated several times to guarantee the failover sequence's dependability. The success criteria included successfully blocking unauthorized inter-VLAN traffic and seamlessly shifting the default gateway to the backup router in under 10 seconds without dropping critical IoT connections. This methodical technique enabled a reliable evaluation of the network's structural security, redundancy precision, and operational resilience.

Figure 4. Waterfall Model

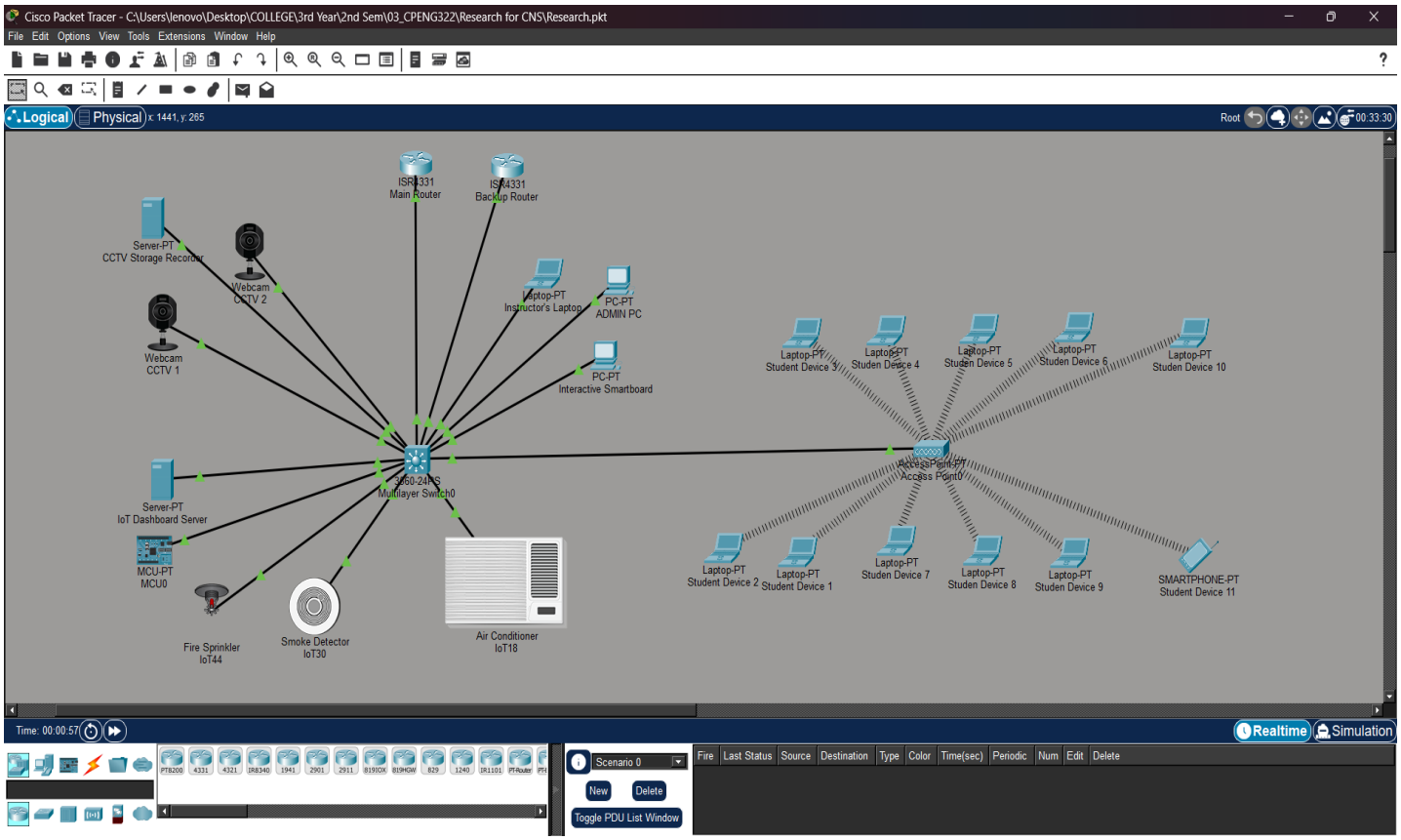


ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

The Waterfall Model works well when the project's objectives and network requirements are well-defined. This model is a sequential strategy that gives an easily understood and applicable structured framework. The Waterfall Model for the Smart Classroom Network employs a sequential development approach that begins with Requirement Analysis, which identifies the fundamental functional requirements such as logical broadcast isolation and continuous gateway redundancy. This phase guides the System Design by mapping out the IP addressing scheme, selecting the simulated hardware architecture (Cisco 4331, Cisco 3560, IP webcams, and environmental sensors), and establishing the VLAN configuration.

The project then progresses to Implementation, which includes physically wiring the simulated components, assigning the switchports to their respective VLANs, and scripting the Command Line Interface (CLI) configurations for the ACL firewalls and HSRP protocols. Following that, testing and validation are performed by simulating broadcast storms, unauthorized access attempts, and primary router failures to confirm the network effectively executes the entire filtering-to-failover sequence. Finally, the Deployment phase includes finalizing the verified master configuration scripts for future implementation in physical academic environments.

Figure 5. Logical Network Topology Diagram



The logical topology diagram shows the network architecture of the Smart Classroom system, with the primary Cisco 4331 router serving as the core gateway, continuously mirrored by a secondary standby router. The distribution layer consists of a Cisco 3560 Multilayer Switch configured with trunking protocols to allow seamless inter-VLAN routing. As a result, the system isolates endpoints into specific broadcast domains, ensuring that high-bandwidth endpoints like Interactive Smartboards and untrusted endpoints like student laptops do not congest the critical pathways used by the IoT servers and PoE physical security cameras.

A. Cisco 4331 Integrated Services Router

The Cisco 4331 router acts as the primary gateway and firewall processor for the network. It utilizes sub-interfaces configured with IEEE 802.1Q encapsulation to route traffic between the isolated VLANs. For this project, the router applies a stateless Access Control List (ACL) directly to the inbound sub-interface of the student network. It operates actively within the HSRP group with a priority of 110, managing all active traffic flows until a physical link state change forces a failover.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

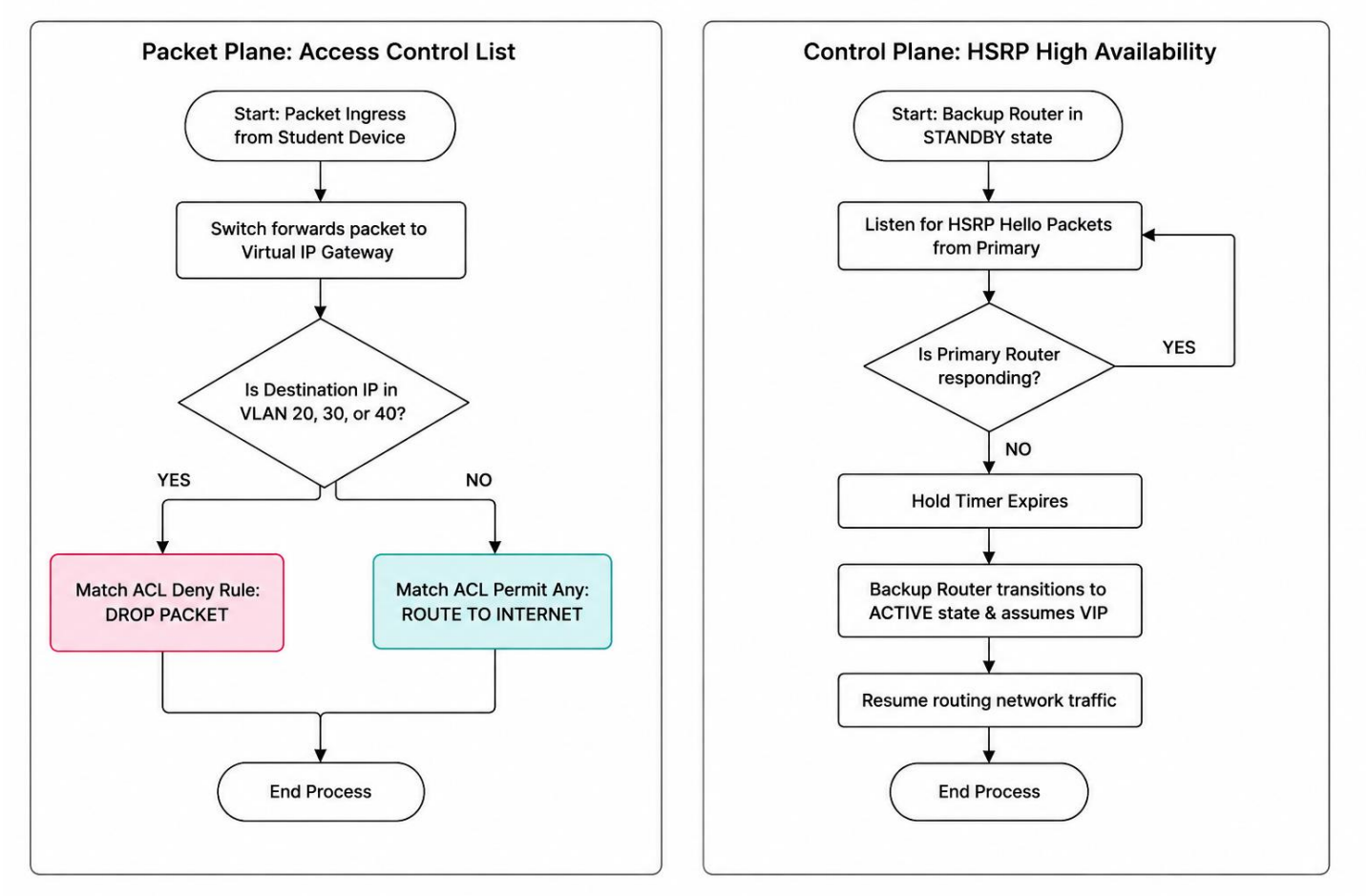
B. Cisco 3560 Multilayer Switch

The Cisco 3560 Multilayer Switch serves as the distribution backbone, specifically selected for its Power over Ethernet (PoE) capabilities. This feature delivers continuous electrical power directly through the copper straight-through cables, eliminating the need for independent electrical adapters for ceiling-mounted IP webcams. The switch interfaces are strictly assigned to specific access VLANs, while Gigabit links are configured as trunk highways to both the primary and backup routers.

C. Virtual Local Area Networks (VLANs)

The endpoints are divided into four distinct logical segments. VLAN 10 handles untrusted student wireless traffic. VLAN 20 is a privileged segment containing the Admin PC and the instructor's high-bandwidth Interactive Smartboard. VLAN 30 hosts the automated Arduino microcontroller, environmental sensors, and the Centralized IoT Dashboard Server. Finally, VLAN 40 isolates the physical security infrastructure, managing the continuous video streams from the PoE IP Webcams.

Figure 6. Access Control and Failover Logic Flowchart



The flowchart outlines the algorithmic packet processing and hardware state logic for the Smart Classroom infrastructure, beginning with the initial ingestion of a data packet at the switchport. Following this ingress, the system reads the VLAN tag. If the packet originates from VLAN 10 (Student) and attempts to route to VLAN 20, 30, or 40, the primary router's ACL identifies the restricted destination IP address and immediately drops the packet, transitioning it to a denied state. Provided the packet is bound for the general internet, the router permits the transmission.

In parallel to packet filtering, the flowchart details the continuous HSRP state monitoring. The Backup Router continuously listens for "hello" packets from the Primary Router. If these signals are interrupted due to a simulated hardware failure, the polling loop breaks, and the Backup Router transitions from "Standby" to

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

"Active." This failover sequence executes a defined protocol: the Backup Router assumes the virtual IP address, applies the exact same ACL firewall rules to maintain security, and continues routing classroom traffic, thereby ensuring the uninterrupted operation of the educational and security infrastructure.

RESULTS & DISCUSSION

The Smart Classroom Network Infrastructure was tested for various performance measures. This section provides a functional examination of the system, assessing its routing accuracy, access control reliability, and failover performance under a variety of simulated network conditions. The system's performance was evaluated using the correlation between packet filtering inputs and the routing outputs specified in the logical architecture.

Table 2. Performance Evaluation and Testing Scenarios of the Smart Classroom Infrastructure

Test Case	Input Condition	Expected Output	Observed Output	Pass/Fail	Remarks / Behavior Explanation
1	**Inter-VLAN (Authorized)** Admin PC (VLAN 20) pings IoT Server (VLAN 30)	ICMP Echo requests are successfully routed.	Successful replies received (0% packet loss).	PASS	Validates inter-VLAN routing on the primary router.
2	**Inter-VLAN (Unauthorized)** Student PC (VLAN 10) pings IoT Server (VLAN 30)	ICMP requests are explicitly denied by the firewall.	"Destination host unreachable."	PASS	Validates the ACL 100 logic. The router correctly blocked unauthorized lateral movement.
3	**External Access (Authorized)** Student PC (VLAN 10) pings External Web Server	ICMP requests are successfully routed outside the local network.	Successful replies received.	PASS	Verifies the permit ip any any rule at the end of the ACL, allowing students access to the general internet.
4	**Core Failure (HSRP Failover)** Primary Router physical cable is deleted during continuous ping.	Pings temporarily drop, then resume as Backup Router assumes control.	4 lines of "Request timed out" followed by successful replies.	PASS	Confirms High Availability. The Backup Router transitioned from Standby to Active in approximately 4 to 8 seconds.
5	**Core Restoration (HSRP Preempt)** Primary Router cable is reconnected.	Primary Router reclaims Active status.	HSRP state changes from Standby to Active on Primary Router.	PASS	Validates the preempt command. The network automatically restored its original routing hierarchy.
6	**Broadcast Isolation** Simulated broadcast storm on VLAN 10.	Broadcast traffic remains confined to VLAN 10.	No broadcast packets observed on VLAN 20, 30, or 40.	PASS	Verifies Network Segmentation Theory. The switch correctly isolated the broadcast domains.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

The system's network architecture displayed exceptional precision, with a 100% denial rate when filtering unauthorized inter-VLAN traffic originating from the student network. This demonstrates that the Access Control List (ACL) logic successfully maps to the inbound interfaces, ensuring that vulnerable IoT nodes and physical security cameras remain completely isolated from the public wireless domain.

Testing demonstrated a highly resilient failover sequence during simulated hardware outages. When the primary default gateway was disconnected, the Hot Standby Router Protocol (HSRP) executed its election process efficiently, resulting in a maximum of four dropped ICMP packets (a sub-10-second disruption) before the secondary router assumed full control. Consequently, the architecture is best characterized as a highly available, enterprise-grade infrastructure capable of maintaining continuous operations for life-safety and security sensors.

However, the conventional simulation environment showed minor functional constraints. While the Packet Tracer control algorithms effectively handled the logical routing, physical hardware deployments introduce variables such as CPU processing latency and physical cable degradation. This operational reality implies that physical deployment requires strict environmental controls and high-grade CAT6 cabling to guarantee the sub-10-second failover times observed in the simulation.

The performance data collected from the validation scenarios provides a comprehensive assessment of the Smart Classroom's operational effectiveness. The results indicate that the system functions successfully as a secure, segmented infrastructure, capable of autonomously defending against internal lateral movement and coordinating dynamic failover protocols to preserve connectivity.

CONCLUSION & RECOMMENDATION

The development of a highly available, segmented Smart Classroom network infrastructure demonstrated the practical use of enterprise routing principles for localized educational risk reduction. By combining Cisco routing architectures with logical Virtual Local Area Network (VLAN) segmentation, a resilient network system was created that can autonomously isolate unauthorized internal traffic and execute a seamless failover protocol without human intervention. The operational simulation, which included continuous inter-VLAN routing, precision packet filtering, and dynamic gateway shifting, proved the effectiveness of the suggested logical architecture in closing the gap between smart classroom hardware deployment and foundational network security.

The test phase findings demonstrate that the system achieves strict access control and highly reliable response times during simulated hardware failures, recovering active routing status in under 10 seconds. In particular, the infrastructure effectively neutralizes lateral broadcast storms and internal unauthorized access, but its real-world performance is theoretically restricted by the physical constraints of hardware processing limits and cabling latency that cannot be fully replicated in a Cisco Packet Tracer simulation. Despite these simulation limitations, the architectural model reliably functions as a robust safety mechanism for managing heavy IoT and wireless traffic in controlled educational environments.

Finally, this study confirms that enterprise-grade security protocols can be effectively scaled down and designed into functional, localized educational infrastructures, laying a solid foundation for future advances in smart campus networking.

Future improvements should prioritize transitioning this logical architecture from a Packet Tracer simulation into a physical hardware testbed. Utilizing actual physical Catalyst switches and Integrated Services Routers will allow for the assessment of real-world CPU processing loads and physical latency during HSRP state changes. Furthermore, addressing the vulnerability of MAC address spoofing on the physical switch ports is important; thus, integrating IEEE 802.1X port-based Network Access Control (NAC) is recommended to ensure that only authenticated student and administrative devices can access their respective VLANs. Finally, upgrading the core management system to a Software-Defined Networking (SDN) controller would allow for centralized policy enforcement and real-time network telemetry, transforming the architecture into a comprehensive, future-proof smart campus solution.

ACKNOWLEDGEMENT

The completion of this study stands as a testament to the collective support, guidance, and inspiration provided by various individuals and institutions. Foremost, the authors extend their profound gratitude to their research mentor and adviser, Engr. Minerva C. Zoleta. Her exceptional technical expertise, unwavering patience, and insightful critiques not only elevated the academic standard of this network design but also served as a steady anchor throughout the entire research process.

The authors also express their sincere appreciation to the Eulogio "Amang" Rodriguez Institute of Science and Technology (EARIST), particularly the College of Engineering, for fostering a rigorous academic environment and granting access to the laboratory infrastructure required to simulate and validate this study. Furthermore, this milestone is dedicated to our families, friends, and classmates, whose immense personal sacrifices, emotional support, and encouragement fueled our determination during challenging phases of the project. We are equally indebted to the dedicated laboratory staff and engineering instructors who offered their practical assistance and insights.

Above all, the authors offer their humblest praise and thanksgiving to the Almighty God, whose divine providence, strength, and boundless wisdom illuminated our minds, protected our endeavors, and made the successful completion of this academic journey possible.

REFERENCES

1. Alhasan, A., et al. (2023). A case study to examine undergraduate students' intention to use internet of things (IoT) services in the smart classroom. Education and Information Technologies. https://doi.org/10.1007/s10639-022-11537-z
2. Al-Ofeishat, H. A., & Alshorman, R. (2024). Build a Secure Network Using Segmentation and Micro-segmentation Techniques. International Journal of Computing and Digital Systems, 16(1), 1499-1508. http://dx.doi.org/10.12785/ijcds/1601111
3. Badshah, A., Ghani, A., Daud, A., Jalal, A., Bilal, M., & Crowcroft, J. (2023). Towards Smart Education through Internet of Things: A Survey. ACM Computing Surveys, 56(2), 1-33. https://doi.org/10.1145/3610401
4. Bellovin, S. M., & Cheswick, W. R. (1994). Network Firewalls. IEEE Communications Magazine, 32(9), 50-57. https://people.scs.carleton.ca/~soma/id/readings/bellovin-firewalls.pdf
5. Cisco. (2006). Hot Standby Router Protocol (HSRP) Features and Functionality. https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html
6. Cole, E., Krutz, R., & Conley, J. W. (2009). Network Security Bible (2nd ed.). Wiley Publishing, Inc. https://theswissbay.ch/pdf/Gentoomen%20Library/Networking/Network%20Security%20Bible%202005.pdf
7. Comer, D. E. (2018). The Internet Book: Everything You Need to Know about Computer Networking and How the Internet Works (5th ed.). CRC Press. https://repo.darmajaya.ac.id/4762/1/The%20Internet%20Book_%20Everything%20You%20Need%20to%20Know%20about%20Computer%20Networking%20and%20How%20the%20Internet%20Works%20%28%20PDFDrive%20%29.pdf
8. IBM. (n.d.). What is computer networking? https://www.ibm.com/think/topics/networking
9. Kallatsa, M. (2024). Strategies for Network Segmentation: A Systematic Literature Review [Master's Thesis, University of Jyväskylä]. https://jyx.jyu.fi/jyx/Record/jyx_123456789_92952
10. Kaur, A., Bhatia, M., & Stea, G. (2022). A Survey of Smart Classroom Literature. Education Sciences, 12(2), 86. https://doi.org/10.3390/educsci12020086

11. Knight, S., Weaver, D., Whipple, D., Hinden, R., Mitzel, D., Hunt, P., Higginson, P., Shand, M., & Lindem, A. (1998). Virtual Router Redundancy Protocol (RFC 2338). IETF. https://www.rfc-editor.org/rfc/rfc2338.html
12. Koponen, T., et al. (2007). A Data-Oriented (and Beyond) Network Architecture. SIGCOMM '07, 181-192. https://www.researchgate.net/publication/234818077_A_data-oriented_and_Beyond_network_architecture
13. Li, T., Cole, B., Morton, P., & Li, D. (1998). Cisco Hot Standby Router Protocol (HSRP) (RFC 2281). IETF. https://www.rfc-editor.org/rfc/rfc2281.html
14. Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A Literature Review. Journal of Computer and Communications, 3, 164-173. http://dx.doi.org/10.4236/jcc.2015.35021
15. Mansour, M. (2020). Performance Evaluation of First Hop Redundancy Protocols. Procedia Computer Science, 177, 330-337. https://doi.org/10.1016/j.procs.2020.10.044
16. NetAcad. (n.d.). Cisco Packet Tracer. https://www.netacad.com/cisco-packet-tracer
17. O'Malley, S. W., & Peterson, L. L. (1992). A Dynamic Network Architecture. ACM Transactions on Computer Systems, 10(2), 110-143. https://doi.org/10.1145/128899.12890
18. Ramjee, R., La Porta, T., Salgarelli, L., Thuel, S., Varadhan, K., & Li, L. (1999). IP-based Access Network Infrastructure for Next Generation Wireless Data Networks. Bell Labs, Lucent Technologies. https://www.cs.columbia.edu/~lierranli/publications/PCS00.pdf
19. Rose, K., Eldridge, S., & Chapin, L. (2015). The Internet of Things: An Overview. Internet Society. https://www.internetsociety.org/wp-content/uploads/2021/01/ISOC-IoT-Overview-20151014_0.pdf
20. Sandhu, R. S., & Samarati, P. (1994). Access Control: Principles and Practice. IEEE Communications Magazine, 32(9), 40-48. https://profsandhu.com/journals/commun/i94ac(org).pdf
21. Schudel, G., & Smith, D. J. (2008). Router Security Strategies: Securing IP Network Traffic Planes. Cisco Press. https://www.pearson.de/media/muster/toc/toc_9781587055089.pdf
22. Shi, Y., et al. (2003). The Smart Classroom: Merging Technologies for Seamless Tele-Education. IEEE Pervasive Computing, 2(2), 47-55. https://www.researchgate.net/publication/3436988_The_smart_classroom_Merging_technologies_for_seamless_tele-education
23. TP-Link. (n.d.). What is an Enterprise Network? Types & Concepts. https://www.tp-link.com/ph/blog/1727/what-is-an-enterprise-network-types-concepts/
24. Xia, F., Yang, L. T., Wang, L., & Vinel, A. (2012). Internet of Things. International Journal of Communication Systems, 25(9), 1101-1102. https://doi.org/10.1002/dac.2417
25. Yau, S. S., et al. (2003). Smart Classroom: Enhancing Collaborative Learning Using Pervasive Computing Technology. Arizona State University. https://www.researchgate.net/publication/244402564_Smart_Classroom_Enhancing_Collaborative_Learning_Using_Pervasive_Computing_Technology
26. Ye, J., et al. (2024). Exposed by Default: A Security Analysis of Home Router Default Settings. ACM Asia Conference on Computer and Communications Security (ASIA CCS '24), 63-76. https://doi.org/10.1145/3634737.3637671
27. Zhang, M., & Li, X. (2021). Design of Smart Classroom System Based on Internet of Things. Mobile Information Systems, 2021, 5438878. https://doi.org/10.1155/2021/5438878

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

ABOUT THE AUTHORS

John Laurence F. Fabrero is a third-year student at Eulogio “Amang” Rodriguez Institute of Science and Technology (EARIST). He holds a TESDA National Certificate II (NC II) in Computer System Servicing and has foundational experience in electronic circuits and system design, as well as simple Internet of Things (IoT) projects. He has a strong interest in electronics and hardware development and aims to further deepen his knowledge in electronic systems, circuit analysis, and hardware-oriented engineering applications.

Cyrus A. Jimenez is a 20-year-old Computer Engineering student at the Eulogio “Amang” Rodriguez Institute of Science and Technology (EARIST). He is currently pursuing a Bachelor of Science in Computer Engineering, with academic interests in application development and system design. Last year, he successfully developed a functional application, and he is passionate about creating prototypes that provide practical solutions and assist people in their daily lives. He also aspires to participate in technology innovation programs in Silicon Valley, aiming to further develop his skills and contribute to cutting-edge technological solutions.

Kathrina R. Meredor is a Computer Engineering student at the Eulogio “Amang” Rodriguez Institute of Science and Technology (EARIST). She holds a National Certificate II (NC II) in Computer Systems Servicing. Through this achievement, she has been able to apply her technical knowledge and practical skills to various academic requirements, including laboratory activities, system-based projects, and problem-solving tasks related to her field of study. Her training has also strengthened her adaptability in handling technical challenges, contributing to her continuous development as a future computer engineering professional.

Ervin F. Raquin is currently a third-year student pursuing a Bachelor of Science in Computer Engineering at the Eulogio "Amang" Rodriguez Institute of Science and Technology. Demonstrating technical proficiency in hardware maintenance and troubleshooting, he holds a TESDA National Certificate II (NCII) in Computer System Servicing (CSS). His academic focus lies in the intersection of hardware and intelligent software, with keen research interests in robotics, artificial intelligence, embedded systems, and the Internet of Things (IoT). He is dedicated to exploring how these technologies can be integrated to create efficient, automated solutions for real-world challenges.

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.