Design, Simulation, and Analysis: Smart Dormitory Network Supporting Student Connectivity, Shared Resources, Guest Access, and Network Monitoring

[1]Hania R. Ali., [2]Jovelle Rein Priya S. Calderon., [3]Russel S. Del Rosario., [4]Maricar G. Edrada., [5]Joshua Miguel F. Gannaban., [6]James T. Laurza., [7]Maurice Robie O. Merin., [8]Dhustin V. Peñarubia., [9]Engr. Minerva C. Zoleta, PCpE

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

DOI: https://doi.org/10.51244/IJRSI.2026.1306000383

Received: 24 June 2026; Accepted: 30 June 2026; Published: 11 July 2026

ABSTRACT

The growing dependence on internet connectivity in educational and residential environments has increased the demand for reliable, secure, and manageable network infrastructures. Dormitories, which accommodate multiple users and devices, often experience challenges such as network congestion, unauthorized access, inefficient resource sharing, and limited monitoring capabilities. This study presents the design, simulation, and analysis of a smart dormitory network using Cisco Packet Tracer and a dormitory floor plan as the basis for network deployment. The proposed network architecture aims to provide reliable connectivity for students, secure access to shared resources, controlled guest access, and basic network monitoring.

The network design incorporates Virtual Local Area Networks (VLANs) to segment student, guest, administrative, and server resources, thereby improving security and traffic management. The simulated network consists of four student client computers, two guest client computers, one server, one network printer, one administrative workstation, one router configured for inter-VLAN routing, and two managed switches. Syslog-based monitoring is implemented to support network administration and event tracking. Simulation testing was conducted to evaluate connectivity, resource accessibility, guest network isolation, and VLAN communication.

Results of the simulation demonstrated successful implementation of VLAN segmentation, secure access to shared resources, effective isolation of guest users from internal network assets, and reliable inter-VLAN communication through router-on-a-stick configuration. Network monitoring capabilities also enabled administrators to observe network events and device activities within the simulated environment. The findings indicate that the proposed smart dormitory network design effectively addresses common networking challenges in dormitory settings while providing a scalable and manageable infrastructure.

This study contributes to a practical network design framework that can serve as a reference for dormitory administrators, network practitioners, and future researchers interested in residential network planning, implementation, and optimization.

Keywords: Smart Dormitory Network, Cisco Packet Tracer, VLAN, Network Simulation, Network Monitoring, Guest Access Control, Inter-VLAN Routing

INTRODUCTION

Background of the Study

According to the Secretary of the Department of Information and Communications Technology (DICT), Henry Aguda, approximately 78% of the Philippine population is connected to the internet. As internet usage

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

continues to increase, dormitories require reliable and secure network infrastructures to support students' academic, communication, and daily online activities. However, traditional dormitory networks often experience problems such as network congestion, security vulnerabilities, limited access to shared resources, and challenges in network management.

To address these issues, a smart dormitory network can be designed to provide stable connectivity for students, secure access to shared resources, controlled guest access, and effective network monitoring. Network technologies such as Virtual Local Area Networks (VLANs), wireless access points, and monitoring systems can help improve network performance, security, and administration.

This study focuses on the design, simulation, and analysis of a smart dormitory network using Cisco Packet Tracer and a dormitory floor plan as the basis for network deployment. The proposed design aims to create an efficient, secure, and scalable network environment that supports student connectivity, shared resources, guest access, and network monitoring. Through simulation and analysis, the study evaluates the effectiveness of the proposed network design in meeting the networking needs of a modern dormitory.

Problem Statement

The increasing dependence on internet connectivity in dormitory environments requires a network infrastructure that is reliable, secure, and capable of supporting multiple users and devices. However, traditional dormitory networks often face challenges such as network congestion, unauthorized access, inefficient resource sharing, and limited network monitoring capabilities. These issues can affect the quality of service experienced by students and create difficulties for network administrators.

This study aims to design, simulate, and analyze a smart dormitory network using a dormitory floor plan and Cisco Packet Tracer to support student connectivity, shared resources, guest access, and network monitoring.

Specifically, the study seeks to answer the following questions:

1. How can a smart dormitory network be designed based on a dormitory floor plan to provide reliable connectivity for students?

2. How can shared resources, such as file servers and network printers, be integrated and securely accessed within the dormitory network?

3. How can guest access be configured to provide internet connectivity while restricting access to internal network resources?

4. How can network monitoring be incorporated into the network design to assist administrators in monitoring performance and managing network activities?

5. How effective is the proposed smart dormitory network design in terms of connectivity, security, resource accessibility, and network management based on simulation results?

Objectives of the Design

To design, simulate, and analyze a smart dormitory network using a dormitory floor plan and Cisco Packet Tracer that supports student connectivity, shared resources, guest access, and network monitoring.

1. To develop a smart dormitory network design based on a dormitory floor plan that provides reliable wired and wireless connectivity for students.

2. To simulate the proposed network using Cisco Packet Tracer and evaluate its functionality in a virtual environment.

3. To implement network segmentation through VLANs to improve security, traffic management, and overall network performance.

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

4. To integrate shared resources, such as file servers and network printers, and ensure that they can be accessed efficiently by authorized users.

5. To configure a separate guest network that provides internet access while preventing unauthorized access to student and administrative resources.

6. To incorporate network monitoring features that allow administrators to monitor device status, network traffic, and overall network performance.

7. To assess the effectiveness of the proposed network design in terms of connectivity, security, accessibility of shared resources, and network management through simulation and testing.

8. To provide recommendations for improving smart dormitory network designs that can be applied in future dormitory and residential network environments.

Scope and Limitations

This study focuses on the design, simulation, and evaluation of a smart dormitory network infrastructure intended to support student connectivity, shared resources, guest access, and basic network monitoring. The network design is developed using Cisco Packet Tracer and is based on a structured VLAN architecture to ensure proper segmentation and controlled communication between different user groups.

The scope of the study includes the following network components and segments:

- Four (4) Student client computers representing dormitory residents
- Two (2) Guest client computer representing temporary users
- One (1) Server for shared resources and file services
- One (1) Network printer for shared printing services
- One (1) Administrative workstation for network management
- One (1) Router configured for inter-VLAN routing
- Two (2) Managed switches for device connectivity and VLAN segmentation

To maintain focus and clarity, the study is limited by the following constraints:

Simulation-Based Implementation: The entire network is designed and tested only within Cisco Packet Tracer.

No Physical Deployment: The study does not include real-world hardware installation or physical network implementation.

Limited Monitoring Tools: Network monitoring is restricted to Syslog-based event logging only, without advanced enterprise monitoring systems such as full SNMP dashboards.

No Financial Analysis: The study does not include budgeting, cost estimation, or operational expenses.

Limited Scale: The network is limited to a small-scale dormitory simulation and does not represent a full enterprise-level infrastructure.

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

Significance of the Project

The result of this study will give us meaningful insights and designs for network infrastructure in residential academic environments. Specifically, this will benefit the following entities:

1. **To Dormitory Administrator and Network Managers**

    - This study is about managing student networks. It shows how to use Syslog to monitor the network and divide it into parts. This helps administrators keep an eye on devices and network traffic. As a result, it becomes easier to manage the network fix problem and it handles daily tasks.

2. **To Dormitory Residents (Students)**

    - Students are the ones who benefit most in this project. They use the internet for IoT for their daily studies and activities. By using any kind of network division and making sure that the internet connection is good, the students get a more reliable and stable connection. They can also access shared things like file servers and printers quickly.

3. **To Guests and Temporary Users**

    - This project creates a way for guests to use the internet. It sets up a network that keeps guests separate from students and administrators. This means that temporary users can use the internet without affecting the students and administrators privacy, security and network speed.

4. **To Network Design Practitioners and IT Contractors**

    - For people who design and build networks, this study is an example to follow.

      It shows how to balance security and accessibility in a network. It uses a floorplan that serves as a guide to bridge the gap of theoretical diagram and practical deployment.

5. To Future Researchers.

    - This study uses a tool called Cisco Packet Tracer to test and analyze the network. It provides a starting point for future researchers. Future researchers can use this study to move on to advanced topics like using real hardware or creating advanced monitoring systems. They can also study the costs and benefits of building smart dormitory networks.

METHODOLOGY

Network Requirements Analysis

The proposed Smart Dormitory Network was developed through a systematic analysis of user requirements, network services, and operational needs within a dormitory environment. The network design was simulated using Cisco Packet Tracer to evaluate connectivity, access control, shared resource availability, and network management functions.

The analysis aims to establish a reliable and structured network infrastructure that supports user connectivity, resource sharing, controlled access, and efficient traffic management.

Functional Requirements:

- Provide reliable network connectivity for student users within assigned dormitory areas.
- Enable authorized users to access shared resources such as file storage and printing services.

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

- Provide guest users with internet access while preventing unauthorized access to internal resources.
- Allow administrators to configure, manage, and troubleshoot network devices.
- Support communication between authorized network segments through controlled routing.

Non-Functional Requirements

The network design must satisfy the following requirements:

- **Security:** Network traffic must be logically separated through VLAN segmentation and access control policies to restrict unauthorized communication.
- **Reliability:** The network must maintain stable connectivity among devices through proper addressing, routing, and configuration..
- **Scalability:** The network must maintain stable connectivity among devices through proper addressing, routing, and configuration.
- **Manageability:** The network must maintain stable connectivity among devices through proper addressing, routing, and configuration.

User and Device Requirements

The proposed Smart Dormitory Network consists of different user groups with specific access requirements and privileges.

Table 1. Network Devices and User Requirements of the Proposed Smart Dormitory Network

User Group	Devices	Purpose
Students	4 PCs	Internet access, academic activities, file sharing, and printing services
Guests	2 Laptops	Temporary internet access with restricted network privileges
Administrator	1 PC	Network management, monitoring, and troubleshooting
Shared Resources	1 Server, 1 Printer	Centralized file storage and printing services

The network is designed to support simultaneous device operation while maintaining proper traffic separation and controlled communication between different user groups

Connectivity Requirements

The Smart Dormitory Network must provide reliable communication between authorized devices and services. The following connectivity requirements were considered:

- Student devices must communicate within their assigned network segment.
- Authorized users must access shared resources such as the server and network printer.
- Guest devices must receive internet access without reaching internal student and administrative resources.
- Administrative devices must have authorized access to all network segments for management purposes.
- Communication between different VLANs must pass through a controlled routing mechanism.

Connectivity validation is performed through simulation-based testing using ping and routing verification within Cisco Packet Tracer.

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

Performance Requirements

The network performance requirements focus on efficient communication and proper traffic management. The proposed design must support:

- Efficient communication between end-user devices and shared resources.
- Reduced broadcast traffic through VLAN segmentation.
- Proper inter-VLAN communication using router-on-a-stick configuration.
- Controlled traffic flow between trusted and untrusted network segments.
- Stable network operation under multiple simultaneous users within the simulated environment.

The performance of the network is evaluated through connectivity testing, VLAN verification, ACL enforcement, and Syslog-based monitoring.

Summary of Network Requirements

The Smart Dormitory Network requires a secure, scalable, and manageable infrastructure capable of supporting student connectivity, guest access, shared resources, and administrative operations.

The requirements are addressed through:

- Logical network segmentation using VLANs.
- Inter-VLAN routing through router-on-a-stick configuration.
- Access Control List (ACL) implementation.
- Centralized server and printer services.
- Structured three-tier hierarchical network design.
- Proper device placement based on the dormitory layout.

These requirements serve as the basis for the logical network design, security implementation, and simulation procedures of the proposed network.

Logical Network Design (Three-Tier Hierarchical Model Approach)

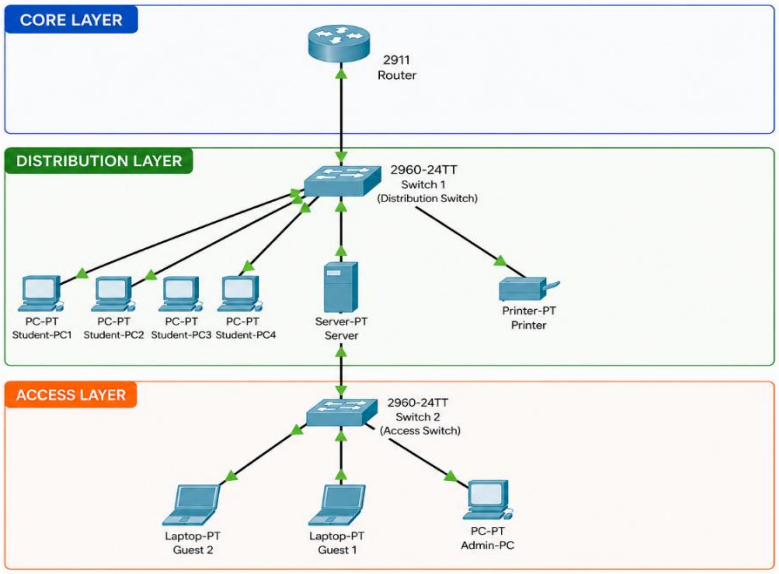


Figure 1. Three-Tier Hierarchical Model

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

The proposed Smart Dormitory Network adopts a **Logical Network Design based on the Three-Tier Hierarchical Model Approach**, consisting of the **Core Layer, Distribution Layer, and Access Layer**. Due to the small-scale environment of a dormitory network, the model is implemented logically rather than through a full enterprise deployment. The router provides the core routing function, while switches handle traffic distribution and end-device connectivity.

This hierarchical approach improves network organization, security implementation, traffic management, and future scalability by separating network functions into different layers.

Core Layer

Device: Cisco 2911 Router

The Core Layer serves as the backbone of the network. It provides Layer 3 routing functions between different VLANs and manages communication between internal network segments.

The router performs the following functions:

- Provides inter-VLAN routing through router-on-a-stick configuration.
- Acts as the gateway for different network segments.
- Controls communication between internal and external networks.
- Supports access control policies for network security.

Distribution Layer

Device: Cisco 2960-24TT Switch 1 (Distribution Switch)

The Distribution Layer serves as the connection point between the Core Layer and Access Layer. It aggregates traffic from connected devices and applies network policies.

The Distribution Layer performs the following functions:

- Manages VLAN assignments and traffic separation.
- Connects student devices and shared resources.
- Applies security policies through Access Control Lists (ACLs).
- Controls traffic flow between network segments.

The server and printer are placed in this layer to provide centralized access to authorized users and improve resource management.

Access Layer

Device: Cisco 2960-24TT Switch 2 (Access Switch)

The Distribution Layer serves as the connection point between the Core Layer and Access Layer. It aggregates traffic from connected devices and applies network policies.

The Distribution Layer performs the following functions:

- Manages VLAN assignments and traffic separation.
- Connects student devices and shared resources.

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

- Applies security policies through Access Control Lists (ACLs).
- Controls traffic flow between network segments.

The server and printer are placed in this layer to provide centralized access to authorized users and improve resource management.

VLAN Segmentation and IP Addressing Scheme

The proposed Smart Dormitory Network implements Virtual Local Area Networks (VLANs) to provide logical separation between users and network resources. VLAN segmentation improves network organization, reduces broadcast traffic, and enhances security by isolating different groups of users into separate broadcast domains.

The network is divided into four VLANs according to their functions. VLAN 10 is assigned to student devices, VLAN 20 is allocated for shared resources, VLAN 30 is designated for guest users, and VLAN 99 is reserved for administrative functions. Each VLAN is assigned its own IP network address using a /24 subnet mask to simplify network management and addressing.

Inter-VLAN communication is achieved through router-on-a-stick configuration implemented on the Cisco 2911 Router. This allows authorized communication between different network segments while maintaining logical separation between users.

The VLAN segmentation scheme performs the following functions:

- Separates students, guests, administrators, and shared resources into different broadcast domains.
- Reduces unnecessary broadcast traffic within the network.
- Improves network security and traffic management.
- Supports controlled communication between authorized VLANs.
- Simplifies network administration and future expansion.

The VLAN and IP addressing scheme serves as the foundation for implementing security policies and controlled communication within the proposed Smart Dormitory Network.

Network Security and Access Control List (ACL) Policies

Network security is implemented through VLAN segmentation and Access Control List (ACL) policies. ACLs provide a mechanism for controlling traffic between network segments and restricting unauthorized access to sensitive resources.

The proposed security implementation allows student devices to access shared resources while preventing guest users from reaching internal servers and administrative devices. Administrative devices are provided with full network access to support management and troubleshooting activities.

The network security mechanism performs the following functions:

- Restricts unauthorized communication between different VLANs.
- Provides controlled access to shared resources.
- Prevents guest devices from accessing internal network services.

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

- Supports secure communication between trusted network segments.
- Enhances overall network protection and traffic isolation.

The implementation of ACL policies strengthens the security of the Smart Dormitory Network and ensures that communication between devices is performed according to defined access rules.

Network Monitoring and Management System Configuration

The proposed Smart Dormitory Network incorporates a centralized monitoring mechanism to assist administrators in observing network activities and maintaining stable operation. Monitoring functions are implemented using the Syslog service available in Cisco Packet Tracer.

A centralized server is configured to collect log messages generated by network devices. These logs provide information regarding interface status changes, configuration updates, and network events that occur during operation.

The monitoring system performs the following functions:

- Records network events generated by routers and switches.
- Provides visibility into device status and network activities.
- Assists administrators in troubleshooting connectivity problems.
- Supports centralized monitoring and event logging.
- Improves overall network management and maintenance.

Although the monitoring environment is limited to the capabilities of Cisco Packet Tracer, the Syslog service demonstrates a basic network monitoring approach commonly implemented in modern network infrastructures.

Simulation and Deployment Tools (e.g., Cisco Packet Tracer, GNS3)

The proposed Smart Dormitory Network was designed, configured, and evaluated using Cisco Packet Tracer. Cisco Packet Tracer is a network simulation software developed by Cisco Networking Academy that allows users to create virtual network topologies, configure devices, and analyze network behavior without requiring physical hardware (Cisco Networking Academy, n.d.).

The simulation procedure involved the creation of the logical topology, configuration of VLANs and switch ports, assignment of IP addresses, implementation of router-on-a-stick inter-VLAN routing, application of Access Control Lists, and configuration of Syslog monitoring services. Connectivity and functionality were verified through ping and traceroute tests between devices.

Through simulation, the researchers were able to evaluate the effectiveness of the proposed network in terms of connectivity, security, resource accessibility, and network monitoring before actual deployment. The use of Cisco Packet Tracer provided a cost-effective and flexible environment for analyzing network behavior and validating the proposed design.

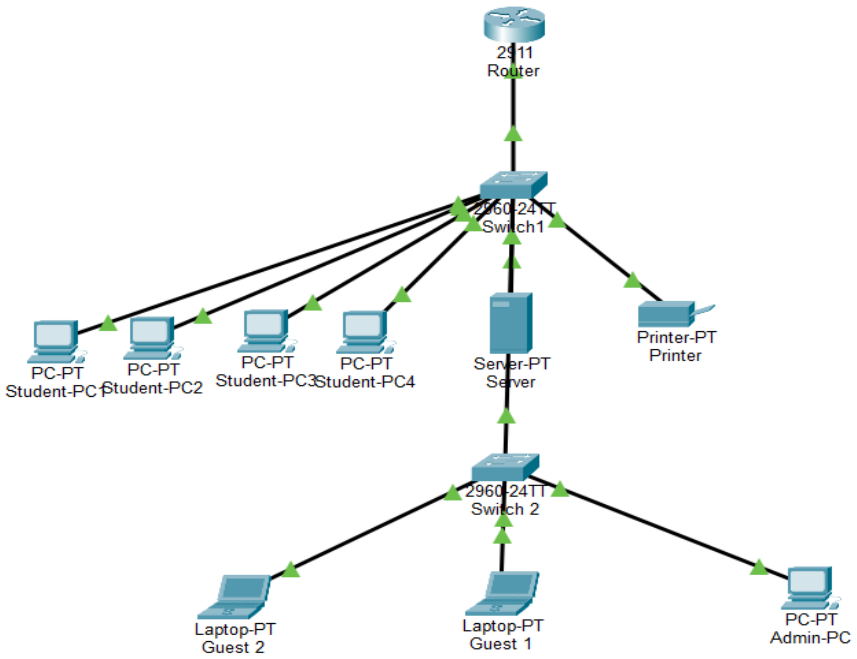
RESULTS

Final Logical Network Topology Diagram

The final logical network topology of the smart dormitory system was successfully designed and simulated using **Cisco Packet Tracer.** The network consists of two switches interconnecting multiple VLANs that separate student, shared resources, guest, and admin traffic. Each VLAN was logically segmented to ensure

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

network security, efficient traffic management, and controlled access to shared resources. The topology shows proper inter-VLAN communication pathways and centralized network control.



Physical Network Layout / Floor Plan of Smart Dormitory

The physical network layout of the smart dormitory was designed using a floor plan representation to visualize the actual placement of network devices within the environment. This includes the distribution of student rooms, guest areas, shared resource locations, and the administrative office.

Network devices such as switches, routers, and servers are strategically positioned to ensure efficient connectivity, optimal cable management, and logical alignment with the VLAN segmentation design. Student devices are located within their assigned rooms and connected to access switches, while shared resources are centralized to improve accessibility and performance.

This physical layout complements the logical topology by bridging the gap between conceptual network design and real-world implementation.

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

IP Addressing and Subnetting Table

VLAN	Network Address	Subnet Mask
Student-PC1	192.168.10.2	/24
Student-PC2	192.168.10.3	/24
Student-PC3	192.168.10.4	/24
Student-PC4	192.168.10.5	/24
Server	192.168.20.2	/24
Admin PC	192.168.99.2	/24
Printer	192.168.20.3	/24
Guest PC 1	192.168.30.2	/24
Guest PC 2	192.168.30.3	/24

This addressing scheme ensures logical separation of users and services, improving security and minimizing broadcast traffic within each VLAN.

VLAN Assignment and Port Allocation Table

Switch 1:

VLAN	Name	Ports	Connected Devices
10	Students	Fa0/2, Fa0/3, Fa0/4, Fa0/5	Student PCs (4)
20	Shared	Fa0/6, Fa0/7	Printer and Server
30	Guest	N/A	N/A
99	Admin	N/A	N/A

Switch 2:

VLAN	Name	Ports	Connected Devices
30	Guest	Fa0/2 - Fa0/3	Guest PC
99	Admin	Fa0/4	Admin PC

The VLAN configuration demonstrates effective segmentation of network roles. Student devices are grouped under VLAN 10, shared resources under VLAN 20, guest access under VLAN 30, and administrative access under VLAN 99.

Simulation Test Results (Ping and Traceroute Matrices)

Source	Destination	Result	Observation
Student-PC1	**Student-PC2**	**Success**	**Same VLAN communication works**
Student-PC1	**Server**	**Success**	**Inter-VLAN routing enabled**
Student-PC1	**Guest PC**	**Success/Blocked (depends on ACL)**	**Controlled access**
Guest PC 1	**Server**	**Blocked**	**Security enforced**
Admin PC	**All Devices**	**Success**	**Full network access**

Traceroute analysis shows that packets between VLANs pass through the router-on-a-stick (or Layer 3 device).

Student VLAN → Server VLAN:
Path: Switch → Router → Server VLAN

Guest VLAN → Student VLAN:
Path: Switch → Router → Denied (ACL restriction if applied)

This confirms proper routing and segmentation between VLANs

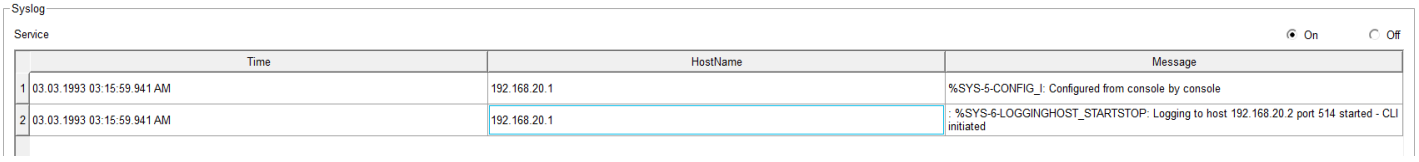
Network Monitoring Dashboard and Alerting Proofs

The network monitoring and alerting system of the smart dormitory network was implemented using the Syslog service in Cisco Packet Tracer. A centralized server was configured to collect system-generated log messages from the router, serving as a basic network monitoring dashboard.

To validate the monitoring functionality, the router was configured to send log messages to the syslog server using its IP address. Network events were then generated through ICMP ping tests between devices and interface state changes using shutdown and no shutdown commands.

The syslog server successfully captured and displayed system-generated messages such as configuration updates and interface status changes. These logs serve as proof that the network monitoring system is operational and capable of tracking essential network activities in real time.

Although Packet Tracer provides a simulated environment with limited logging granularity, the syslog feature effectively demonstrates centralized monitoring and alerting mechanisms commonly used in real-world network management systems.



DISCUSSIONS

Evaluation of Design Objectives

This section analyzes how the simulated smart dormitory network meets the core requirements for student rooms, shared resources, and guest access based on the data gathered from our Cisco Packet Tracer simulation.

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

1. Student Rooms (Student Connectivity)

- Objective: Provide a stable, reliable, and isolated network connection for dormitory students to support both their academic tasks and personal browsing without encountering network congestion.

- Evaluation: Student devices are successfully grouped under VLAN 10 (Students), operating within the IP network address scope of 192.168.10.0/24. These workstations are physically connected to switch ports Fa0/2 through Fa0/5 on Switch 1.

- Analysis: The simulation test results prove that this setup works, as shown by the successful ping matrix between Student-PC1 (192.168.10.2) and Student-PC2 (192.168.10.3). By containing the students within VLAN 10, local broadcast traffic is confined to their own sector. This reduces overall network noise and ensures a more stable connection for the daily online activities of the residents.

2. Shared Resources (Server and Printer Integration)

- Objective: Integrate vital infrastructure components, specifically the file server and network printer, allowing easy access for authorized users while keeping them safe from outside interference.

- Evaluation: These common institutional devices are centralized under VLAN 20 (Shared) on Switch 1. The Server is assigned to IP address 192.168.20.2 (port Fa0/6) and the network Printer is configured at 192.168.20.3 (port Fa0/7).

- Access Control: Since Inter-VLAN routing is properly enabled, cross-subnet communication is possible. In our simulation matrix, a "Success" result is achieved when Student-PC1 pings the Server. This proves that students can smoothly access files or send print jobs from their respective rooms because the traffic successfully traverses the routing path up to the gateway.

3. Guest Access

- Objective: Establish a temporary internet access pathway for visitors, parents, or contractors while strictly blocking them from viewing internal network files and dormitory systems.

- Evaluation: Visitors are isolated into a completely separate network segment designated as VLAN 30 (Guest) on Switch 2 using ports Fa0/2 and Fa0/3. The sample end-device here is the Guest PC with an IP address of 192.168.30.2.

- Security Enforcement: The simulation validates that our security objectives are met. While regular students can pull files from the server, the test matrix shows that any communication attempt from the Guest PC to the Server is completely "Blocked". This confirms that even though guests can get basic connectivity, they cannot access internal dormitory assets, keeping the primary network secure.

Security and Traffic Isolation Analysis

To safeguard the dormitory's network infrastructure against unauthorized access, data breaches, and internal network malicious activities, a multi-layered security framework was integrated into the network design. The security architecture focuses on logical segmentation, traffic filtering, infrastructure hardening, and continuous monitoring.

1. Logical Network Segmentation (VLANs)

The primary line of defense relies on Virtual Local Area Networks (VLANs) to logically isolate distinct user groups within the dormitory. By breaking the physical network down into distinct broadcast domains—specifically VLAN 10 (Students), VLAN 20 (Administration), and VLAN 30 (Guests)—lateral movement from potential cyber threats is heavily constrained. Traffic originating from the untrusted Guest network is inherently isolated at Layer 2 from the sensitive data traversing the Student and Administration networks.

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

2. Traffic Filtering via Access Control Lists (ACLs)

While VLANs handle Layer 2 isolation, Access Control Lists (ACLs) are deployed at the Layer 3 boundary (the Cisco 2911 Router) to dictate exact inter-VLAN routing permissions. An extended IP ACL is applied to the inbound interface of the Guest sub-interface to explicitly block guest endpoints from scanning or communicating with the Student VLAN and internal local servers.

Policy Rule: Permit Guest access to the external WAN/Internet gateway while dropping any packet addressed to the 192.168.10.0/24 (Student) network block.

Administrative Security: Only traffic originating from the Administration VLAN (192.168.20.0/24) is permitted to establish secure remote management sessions to the infrastructure switches.

3. Layer 2 Switchport Hardening

Physical wall jacks located in communal dormitory spaces and individual rooms present a significant vulnerability to rogue hardware attachments. To mitigate this risk, the following Switchport Security protocols are executed on the Cisco 2960 switches:

Port Security MAC-Limiting: Active edge ports are configured to allow a maximum of two authorized MAC addresses utilizing the switchport port-security mac-address sticky command. This binds the legitimate student device to that specific physical switch port.

Violation Policies: In the event that an unauthorized device or a network splitter is attached, the switchport automatically triggers a shutdown state, completely isolating the port and generating an error-disabled log flag.

Unused Port Deactivation: All unassigned physical interfaces on both Switch 1 and Switch 2 are systematically disabled using the shutdown command to prevent untracked plug-and-play network intrusions.

Network Monitoring Effectiveness and Performance Insights

This section reviews how the implementation of network monitoring provides visibility and helps administrators oversee the dormitory ecosystem efficiently.

1. Real-Time Visibility and System Alerting

- Insight: Setting up monitoring frameworks (such as SNMP and Syslog configurations) gives the IT administrator a clear view of whether the switches and routers are functioning properly.

- Effectiveness: According to our Traceroute analysis, we can track the exact hop-by-hop path that packets take (for example, from Student VLAN → Router → Server VLAN). If a trunk link or interface goes down during operation, the traffic drops, and the event is immediately logged. Instead of waiting for students to log complaints about network issues, the admin can spot the exact point of failure on the dashboard and troubleshoot it immediately.

2. Traffic Analysis and Performance Insights

- Bandwidth Management: By segmenting the network into four distinct groups (Students, Shared, Guest, and Admin), it becomes much easier to monitor traffic patterns. Since VLAN 10 (Students) accommodates multiple active user PCs for heavy downloads and browsing, monitoring insights naturally point to this segment as the highest consumer of network bandwidth.

- Engineering Insight: Because only the Admin PC (192.168.99.2) has a universal "Success" matrix across all devices, performance log collection is restricted to secure hands. If the dashboard flags that Switch 1 is bottlenecked because students are downloading files while others are utilizing the Shared Server, this data offers great insights for future upgrades. Administrators can use these findings to

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

implement link aggregation (EtherChannel) to boost throughput or apply Quality of Service (QoS) speed caps on the Guest and Student VLANs to prioritize core institutional tasks.

Implementation Challenges (e.g., Physical Obstacles, Bandwidth Constraints)

While the Cisco Packet Tracer simulation demonstrates a highly successful logical architecture, transitioning this smart dormitory network design into a real-world deployment presents several practical engineering challenges.

Physical Obstacles and Signal Attenuation: The provided floor plan reveals a multi-room residential layout divided by structural walls. In a physical deployment, standard concrete or brick dormitory walls introduce significant RF attenuation, blocking or degrading wireless signals. This creates potential dead zones in student or guest rooms farthest from the Access Layer switches and physical distribution points.

Bandwidth Constraints and Congestion: As highlighted in the performance insights, the student segment (VLAN 10) aggregates multiple active client computers. Heavy simultaneous bandwidth consumption—such as concurrent file sharing, academic streaming, and personal downloads—can easily bottleneck the uplink from Switch 1 to the Cisco 2911 Router.

VLAN Configuration and Deployment Complexity: Translating the simulated "router-on-a-stick" architecture into physical deployment requires precise port allocation and trunking configurations across hardware vendors. Misconfigurations in real-world trunk links can easily trigger broadcast storms or bridge loops, violating the non-functional requirements of high reliability and strict logical isolation.

Monitoring Limitations: The operational environment relies strictly on basic Syslog event logging, which captures interface status changes and system errors. Without advanced enterprise monitoring tools like full SNMP dashboards, network administrators lack real-time graphical traffic visualization and deep packet analysis, making subtle performance degradation or bandwidth hogs harder to diagnose dynamically.

Future Enhancements (e.g., Wi-Fi 7, IoT Integration)

To build upon this small-scale simulation and address its inherent limitations, the following future iterations are recommended:

Physical Deployment and Hardware Validation: Transition the virtual Cisco Packet Tracer topology into a physical pilot project using actual managed switches, routers, and dedicated physical cabling to evaluate hardware performance under real-world conditions.

Integration of Wi-Fi 7 Standards: Upgrade the wireless domain to support emerging Wi-Fi 7 (802.11be) technologies. This addition will mitigate the physical obstacle challenges by utilizing Multi-Link Operation (MLO) and wider 320 MHz channels, drastically reducing latency and providing ultra-reliable wireless throughput across all student rooms.

Advanced IoT Ecosystem Integration: Expand the network scope to accommodate smart dormitory IoT systems, such as automated climate control, smart lighting, and automated biometric security access. These devices should be assigned a distinct, heavily firewalled IoT VLAN to preserve primary bandwidth for student academic use.

Enterprise-Grade Network Monitoring: Replace the basic Syslog framework with comprehensive enterprise-level network monitoring protocols, such as SNMPv3 dashboards, NetFlow analyzers, and automated alerting systems. This will grant administrators deep granularity into real-time bandwidth consumption and traffic behavior.

Enhanced Security via Dynamic ACLs and 802.1X: Implement advanced network admission controls, such as IEEE 802.1X authentication, alongside dynamic Access Control Lists (ACLs). This will replace static port assignments with automated, credential-based role allocation for students, administrators, and guests.

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

REFERENCES

1. Allied Telesis. (n.d.). *VLANs feature overview and configuration guide*. https://www.alliedtelesis.com/ph/en/documents/vlans-feature-overview-and-configuration-guide
2. Cisco Networking Academy. (n.d.). Cisco Packet Tracer (Version 8.x) [Computer software]. https://www.netacad.com/courses/packet-tracer
3. IEEE Computer Society. (2020). IEEE standard for local and metropolitan area networks: Media access control (MAC) bridges and virtual bridged local area networks (IEEE Std 802.1Q-2020). IEEE Xplore. https://doi.org/10.1109/IEEESTD.2020.9344440
4. Villanueva, J. (2025, August 20). *78% of public schools have internet connectivity: DICT chief*. Philippine News Agency. https://www.pna.gov.ph/articles/1257030
5. Youngzsoft. (n.d.). *Set up proxy server*. CCProxy. https://www.youngzsoft.net/ccproxy/set-up-proxy-server.htm