Smart College Network with Automation & Security using Cisco Packet Tracer

Submitted in partial fulfillment of the requirements of

Computer Network (CE11P)

for

Second Year (SEM-IV) of Computer Engineering

By

Sheshank Singh 23102A0017
Ayush Mayekar 23102A0018
Parag Jadhav 23102A0019
Prachee Patil 23102A0020
Om Nanaware 23102A0021

Under the Guidance of

Prof. Suvarna Bhat

Department of Computer Engineering

Vidyalankar Institute of Technology
Wadala(E), Mumbai-400437

University of Mumbai

2024-25

CERTIFICATE OF APPROVAL

This is to certify that the project entitled

"Smart College Network with Automation & Security using Cisco Packet Tracer"

is a bonafide work of

Sheshank Singh 23102A0017
Ayush Mayekar 23102A0018
Parag Jadhav 23102A0019
Prachee Wakode 23102A0020
Om Nanaware 23102A0021

submitted to the University of Mumbai in partial fulfillment of

Computer Network (CE11P)

for

Second Year (SEM-IV) of Computer Engineering

Guide	Head of Department	Principal
Prof. Pankaj Vanwari	Dr. Ravindra Sangle	Dr. Sangeeta Joshi

Mini Project Report Approval

This project report entitled **Smart College Network with Automation & Security using Cisco Packet Tracer** by

1. ***Sheshank Singh 23102A0017***
2. ***Ayush Mayekar 23102A0018***
3. ***Parag Jadhav 23102A0019***
4. ***Prachee Wakode 23102A0020***
5. ***Om Nanaware 23102A0021***

is approved for Computer Network (CE11P) for Second Year of Computer Engineering.

Internal Examiner External Examiner

Date:

Place:

Declaration

I declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Name of student	Roll No.	Signature
1) Sheshank Singh	23102A0017	
2) Ayush Mayekar	23102A0018	
3) Parag Jadhav	23102A0019	
4) Prachee Wakode	23102A0020	
4) Om Nanaware	23102A0021	

Date:

Place:

Acknowledgements

This Project wouldn't have been possible without the support, assistance, and guidance of a number of people whom we would like to express our gratitude to. First, we would like to convey our gratitude and regards to our mentor **Prof. Pankaj Vanwari** for guiding us with his constructive and valuable feedback and for his time and efforts. It was a great privilege to work and study under his guidance.

We would like to extend our heartfelt thanks to our Head of Department, **Dr. Ravindra Sangle,** for overseeing this initiative which will in turn provide every Vidyalankar student with a distinctive competitive edge over others.

We appreciate everyone who spared time from their busy schedules and participated in the survey. Lastly, we are extremely grateful to all those who have contributed and shared their useful insights throughout the entire process and helped us acquire the right direction during this research project.

Abstract

The **Smart College Network with Automation and Security using Cisco Packet Tracer project** aims to simulate and demonstrate a modern, secure, and automated networking infrastructure tailored for educational institutions. Leveraging the capabilities of **Cisco Packet Tracer 8.2,** the system showcases the integration of **IoT devices, firewall security, RFID-based access control**, and **zone-based segmentation** to replicate a **real-world smart campus environment.**

The simulated network architecture is logically divided into four key zones: **Academic Labs, IoT-enabled Control Room, Server Infrastructure,** and a **Malicious Network Zone**. Each zone serves a specific function ranging from educational usage to automation control and threat simulation interconnected using **VLANs, static routing**, and enforced through **Cisco ASA Firewall** configurations. The firewall plays a pivotal role by implementing **Access Control Lists (ACLs),** and intrusion prevention mechanisms to ensure only legitimate traffic can access critical resources.

The automation components include **fire detection systems, motion-triggered fans and lights,** and **RFID-controlled smart doors**, all of which are responsive to real-time triggers via embedded IoT scripts. These systems simulate environmental awareness and safety mechanisms typical of a smart infrastructure.

Furthermore, the simulation incorporates a **malicious network zone** to emulate real-world cyber threats and penetration attempts. These are used to validate the firewall's ability to detect, block, and alert on unauthorized access attempts, thereby reinforcing network robustness and security posture.

The project effectively demonstrates how smart automation, coupled with structured network segmentation and security enforcement, can transform traditional college networks into **intelligent, responsive,** and **resilient ecosystems**. It serves as a valuable learning tool for understanding the practical application of **IoT, cybersecurity protocols**, and enterprise **networking principles** in academic environments.

Table of Contents

1. Introduction

With rapid developments in smart infrastructure and networking, educational institutions are increasingly transitioning to intelligent systems for resource management and operational efficiency. These systems require robust, secure, and automated networks to manage day-to-day activities while being resilient to internal and external cyber threats.

This project showcases a virtual **smart college campus** network that integrates **automation**, **security**, and **scalability** using Cisco Packet Tracer. Through the inclusion of various IoT elements and network protection mechanisms, the simulation aims to model a secure, highly functional, and user-responsive campus environment.

2. Problem Definition

Traditional campus networks often lack integrated automation and are vulnerable to unauthorized access and inefficiencies in real-time monitoring. This fragmentation leads to delays, manual operations, and increased security risks.

The problem being addressed is the **lack of a unified and secure automated infrastructure** in educational institutes. By designing a virtual network environment with clearly defined **zones**, **automated device control**, and **centralized access management**, this project presents a scalable and secure smart campus blueprint.

3. Literature Survey

The development of smart campuses has seen global momentum. Literature on network simulation and automation in educational setups emphasizes the following:

- **Cisco Networking Academy** introduces VLANs, ASA firewalls, and IoT components as part of its standard curriculum.
- **IEEE papers** highlight real-time use of motion sensors and RFID in university campuses.
- Online repositories and simulators focus on either automation or security, but few incorporate both with IoT and firewall systems.

This project integrates lessons from academic and professional resources to design a holistic, real-time network simulation.

4. Proposed System

The network architecture is logically divided into the following segments:

Zone	IP Address Range	Description
Academic Labs	192.168.0.0/24	PCs for students and faculty
IoT Control Room	192.168.10.0/24	Smart sensors and actuators
Server Infra	10.101.1.0/24	Internal servers and cloud nodes
Malicious Zone	10.102.1.0/24	Simulated attacker network

Key features include:

- **VLAN-based segmentation** ensuring compartmentalized access and communication.
- **IoT modules** simulating environmental response: fire alarms, door controls, motion-triggered systems.
- **RFID-based access control** for sensitive areas like server rooms.
- **Cisco ASA Firewall** setup with ACLs, NAT policies, and traffic filtering.

5. Implementation

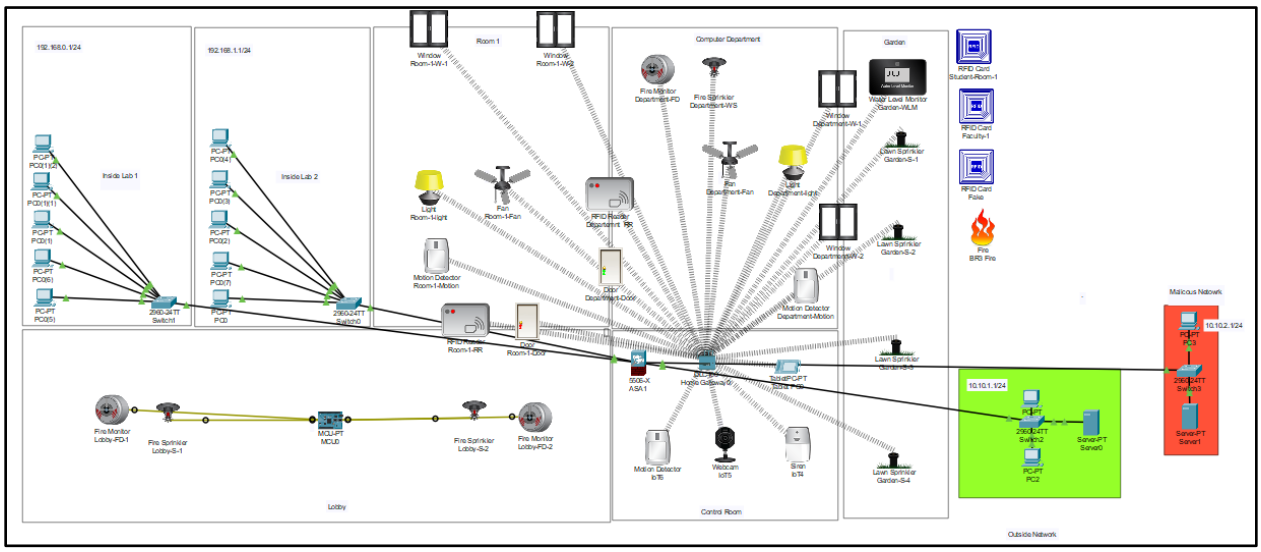
The network was modeled and tested using **Cisco Packet Tracer 8.2**, and included:

- **Topology Design**: Using routers, switches, servers, PCs, ASA firewall, and IoT devices.
- **Static Routing & VLAN Configuration**: Configured for each network zone using Layer-3 switches.
- **IoT Logic**: Sensors scripted to detect conditions and trigger actuators.
    - **Fire Sensor**: Detects heat; triggers alert, shuts RFID door.
    - **Water Level Sensor**: Triggers motor pump when below threshold.
    - **Motion Sensor**: Activates smart fan/light in presence of motion.
- **Firewall Rules**:
    - ACLs deny traffic from the malicious zone.

- **RFID Authentication**: Access granted only to authorized RFID tags.

Testing Scenarios:

- Unauthorized access from malicious zone blocked by ASA firewall.
- IoT system functionality verified via triggered events and alerts.
- HTTP and DNS access tested between labs and servers.



6. Conclusion and Future Scope

The simulated **Smart College Network** demonstrates the ability to integrate automation, security, and manageability into a single cohesive system. Through VLAN segmentation, firewall implementation, and IoT-triggered control mechanisms, it ensures safety, reliability, and efficiency.

Challenges Encountered:

- Complexity in ASA firewall CLI configuration.
- Timing sync for sensor-actuator scripting.
- DHCP-static IP conflicts during inter-VLAN routing.

7. References

1. Cisco Networking Academy – IoT & Packet Tracer Labs
2. Cisco ASA Configuration Documentation
3. IEEE Smart Campus Research Publications
4. YouTube: Cisco Smart Campus Simulations
5. Official Cisco Packet Tracer 8.2 Documentation
6. GitHub Projects on Smart Network Security