PROJECT TITLE
Secure Network Configuration using Cisco Packet Tracer (CAN Network)

The domain of the Project:
Network & System Security

COURSE NAME
Cyber Security

Team Mentor:
Mr. Derick Johnson

Team Members:
Ms. Diksha Santosh Hire

Period of the project:

October 2025 – December 2025

Declaration

The project titled **Secure Network Configuration using Cisco Packet Tracer (CAN Network)** has been mentored by Mr. Derick Johnson, organised by SURE Trust, from June 2025 to December 2025, for the benefit of the educated unemployed rural youth for gaining hands-on experience in working on industry relevant projects that would take them closer to the prospective employer. I declare that to the best of my knowledge the members of the team mentioned below, have worked on it successfully and enhanced their practical knowledge in the domain.

Team Members:

Ms. Diksha Santosh Hire

Mentor's Name:
Mr. Derick Johnson
Pentester, Tech Speaker

Mentor's Name:
Mr. Nishchay Gabba
Security Researcher

Prof. Radhakumari
Executive Director & Founder
SURE Trust

Table of contents

Executive Summary

● *This project focuses on designing and implementing a secure Campus Area Network (CAN) using Cisco Packet Tracer. The network is divided into Admin, IT, HR, and Guest departments using* ***VLANs*** *to improve security and management.*

● *A* ***core switch and access switches*** *are used to connect all departments, ensuring structured and organized network connectivity.*

● ***Switch port security*** *is implemented on access ports to restrict unauthorized devices and protect the network from MAC-based attacks.*

● *An* ***ASA firewall*** *is configured between the internal network and an* ***ISP router*** *to provide perimeter security and control network traffic.*

● ***Network Address Translation (NAT)*** *is implemented on the ASA firewall to allow internal users to securely access the internet.*

● *A* ***centralized DHCP server*** *is configured to automatically assign IP addresses to devices based on their VLAN, reducing manual configuration errors.*

● *The final result is a secure and well-structured network where all departments receive IP addresses automatically, internal resources are protected, and guest users are restricted while still having internet access.*

● *This project demonstrates real-world networking and security practices used in organizations and helps build practical skills relevant to network and cybersecurity roles.*

Introduction

● ***Background and context of the project:***
With the increasing use of computer networks in organizations, there is a strong need for secure and well-structured networks. Campus Area Networks (CAN) are commonly used in colleges and companies, and they require proper security, segmentation, and management to protect data and resources.

● ***Problem statement or goals of the project:***
Many networks lack proper security and traffic separation, which can lead to unauthorized access and network misuse. The main goal of this project is to design a secure network that separates departments, controls access, and provides safe internet connectivity using industry-standard networking practices.

● ***Scope and limitations of the project:***
The project covers VLAN configuration, switch port security, ASA firewall setup, NAT configuration, and DHCP implementation using Cisco Packet Tracer. The project is limited to a simulation environment and does not include real hardware deployment.

● ***Innovation component in the project:***
The project combines VLAN-based network segmentation with centralized DHCP and firewall-based security. Using an ASA firewall with an ISP router for controlled internet access adds a realistic enterprise-level security approach to the network design.

Project Objectives

- *To design a secure Campus Area Network (CAN) using Cisco Packet Tracer that represents a real organizational network.*

- *To implement VLAN-based network segmentation for Admin, IT, HR, and Guest departments to improve security and traffic management.*

- *To configure inter-VLAN routing using a router so that authorized departments can communicate securely.*

- *To apply switch port security on access ports to restrict unauthorized devices and prevent MAC-based attacks.*

- *To configure an ASA firewall to protect the internal network and control traffic between the internal network and the internet.*

- *To implement Network Address Translation (NAT) on the ASA firewall to provide secure internet access using an ISP router.*

- *To configure a centralized DHCP server to automatically assign IP addresses to devices based on their VLAN.*

- *To design a structured network topology using core and access switches to ensure scalability and easy network management.*

- *To restrict guest network access to internal departmental resources while allowing controlled internet connectivity for guest users.*

- *To test and verify network security and connectivity using ping and device status commands to ensure the network works as intended.*

Methodology and Results

Methodology/Technology Used:

● VLAN configuration is used to divide the network into Admin, IT, HR, and Guest departments.

● Inter-VLAN routing is implemented using a router to allow controlled communication between VLANs.

● Switch port security is applied on access ports to restrict unauthorized devices using MAC address limitations.

● An ASA firewall is configured to provide network security between the internal network and the internet.

● Network Address Translation (NAT) is implemented on the ASA firewall to allow secure internet access.

● A centralized DHCP server is used to automatically assign IP addresses based on VLAN configuration.

Tools/Software Used:

● Cisco Packet Tracer for network simulation and configuration.

● Cisco IOS Command Line Interface (CLI) for configuring router and switches.

● ASA CLI for firewall and NAT configuration.

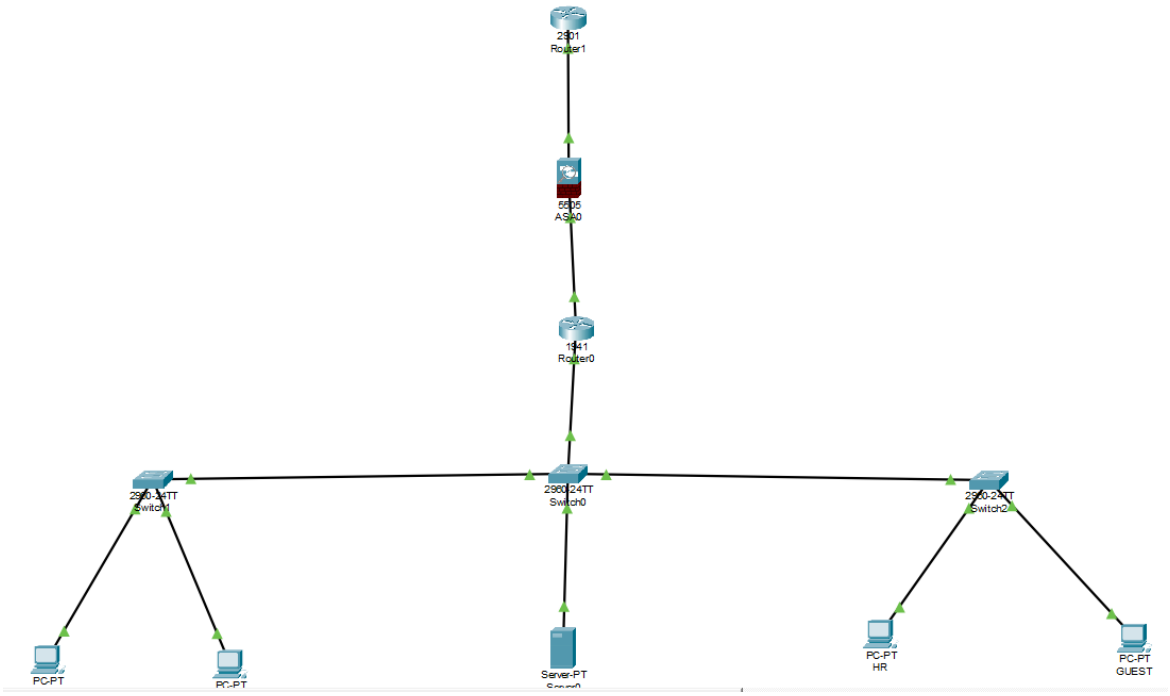
● End devices such as PCs and server provided within Cisco Packet Tracer.

Project Architecture:

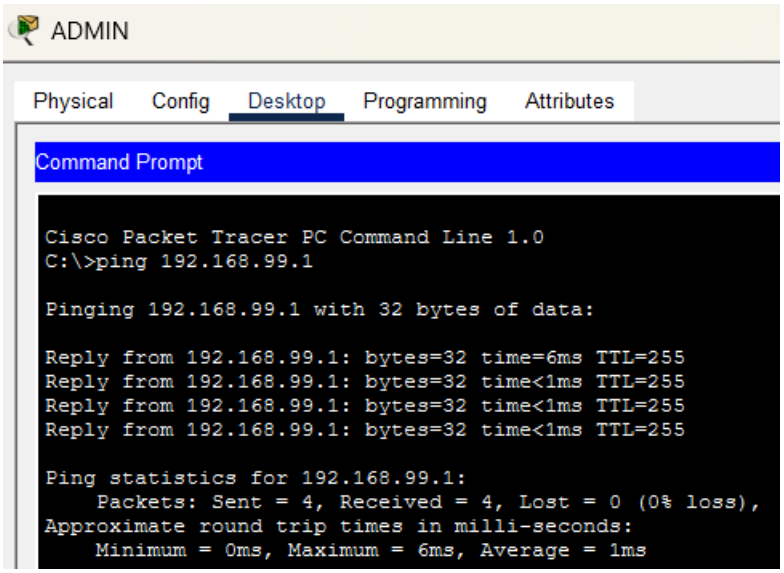
The network architecture consists of an ISP router connected to an ASA firewall, which acts as the security gateway. The ASA firewall is connected to a core switch that manages VLAN traffic. Two access switches are used to connect departmental PCs. A centralized server provides DHCP services to all VLANs. The router handles inter-VLAN routing, allowing secure communication between departments while maintaining isolation.

Final Project working Screenshots:

Entire Network Topology:



Server successfully pinged:



PCs successfully connected to the network:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	ADMIN	Server0	ICMP		0.000	N	0
	Successful	IT	Server0	ICMP		0.000	N	1
	Successful	Server0	HR	ICMP		0.000	N	2
	Successful	Server0	GUEST	ICMP		0.000	N	3

Project GitHub Link:

Learning and Reflection

Document every team member's new learnings (in terms of technology, management, etc):

● *Learned how to design a complete network topology from scratch using Cisco Packet Tracer.*

● *Gained practical understanding of VLAN creation and network segmentation for different departments.*

● *Learned how inter-VLAN routing works and how data flows between networks.*

● *Understood the purpose and configuration of switch port security to protect access ports.*

● *Learned how to configure an ASA firewall and control traffic between internal and external networks.*

● *Gained hands-on experience in implementing Network Address Translation (NAT) for internet access.*

● *Learned how to configure a centralized DHCP server and automate IP address assignment.*

● *Developed a clear understanding of why network security is important and how it is implemented in real-world environments.*

Team Member Experience:

● As a single team member, I independently planned, built, and configured the entire network.

● The project helped me understand network flow, including how devices communicate within and outside the network.

● Gained confidence in configuring routers, switches, firewalls, and servers from the beginning.

● The hands-on work strengthened my foundation in networking concepts and security principles.

● Learned how to identify and fix configuration issues during the project.

● This project provided valuable practical experience, beyond theoretical knowledge.

● The experience improved my problem-solving and technical skills.

● Overall, the project played an important role in preparing me for real-world networking and cybersecurity roles.

Conclusion and Future Scope

Recap objectives and achievements:

● The main objective of this project was to design and implement a secure Campus Area Network (CAN) using Cisco Packet Tracer.

● VLAN-based segmentation was successfully implemented for Admin, IT, HR, and Guest departments to improve security and traffic management.

● Inter-VLAN routing was configured, allowing controlled communication between authorized departments.

● Switch port security was applied to restrict unauthorized devices from accessing the network.

● An ASA firewall was successfully configured to secure the internal network and control traffic flow.

● Network Address Translation (NAT) was implemented to provide secure internet access using an ISP router.

● A centralized DHCP server was configured to automatically assign IP addresses to all VLANs.

● All configurations were tested and verified, and the network worked as expected in the simulation environment.

Future scope of this project:

● Advanced security features such as Intrusion Detection and Prevention Systems (IDS/IPS) can be added.

● Virtual Private Network (VPN) configuration can be implemented for secure remote access.

● More departments and users can be added to test network scalability.

● Advanced Access Control Lists (ACLs) can be applied for stricter traffic control.

● Network monitoring tools such as SNMP and Syslog can be integrated.

● The project can be extended to real hardware implementation for real-world deployment experience.