# Cisco Packet Tracer Project Report

## Project Title:

LAN Threat Detection Using Access Control Lists and Port Security

## Objective:

This project simulates a LAN environment in Cisco Packet Tracer to demonstrate how ACLs (Access Control Lists) and switch-level Port Security can be used to detect and block unauthorized devices or malicious access attempts.

## Devices Used:

• 1 Router (1841)  
• 1 Switch (2960)  
• 2 PCs (User and Attacker)

## Topology Overview:

The network topology consists of PC0 and PC1 connected to a switch, which is connected to a router. IP addressing and port security configurations are applied to simulate access control.

## Key Configurations:

Router Configuration:  
- IP: 192.168.1.1/24 on FastEthernet0/0  
- ACL: Blocks access from PC1 (192.168.1.3)  
  
Switch Port Security:  
- PC0 is allowed on Fa0/1  
- PC1 triggers a security violation on Fa0/2 (MAC address not recognized)

## Results:

- PC0 can successfully ping the router.  
- PC1 is blocked by ACL and switch security rules.  
- Network threat is simulated and contained using Cisco best practices.

## Conclusion:

This simulation shows how simple Cisco configurations like ACLs and Port Security can prevent unauthorized access and secure local area networks effectively.