# SAVEETHA SCHOOL OF ENGINEERING

**CAPSTONE PROJECT**

**Design and Implementation of a Secure and Efficient Network Infrastructure for a Police Station**

**NAME:** Akash. S

**REGISTER NUMBER:** 192324298

**COURSE CODE:** CSA0747

**COURSE NAME:** Computer Network for IOT

## INTRODUCTION:

### In the digital age, efficient communication and collaboration within organizations like police stations rely heavily on robust network infrastructures. The design and implementation of a multi-mode network topology are essential for supporting diverse communication needs, ensuring secure data handling, and optimizing resource allocation. The project aims to create a comprehensive network design for a police station, incorporating secure VLANs, multiple routing protocols, and unified communication tools like IP telephony and video conferencing to improve operational efficiency. Additionally, stringent security measures will be implemented to prevent unauthorized access to sensitive police records and ensure the network's reliability.

### Objective:

* Design a multi-mode network topology.
* Implement a secure VLAN structure and configure routing protocols.
* Showcase web services and unified communication systems in a police station environment.
* Analyse the advantages and limitations of the network design.

## LITERATURE REVIEW

## Network topologies have evolved to meet the growing demands of modern organizations, including law enforcement agencies. Multi-mode networks, which blend wired and wireless technologies, offer flexibility and reliability. VLAN segmentation is widely adopted to isolate network traffic, optimize performance, and enhance security. Routing protocols like OSPF and RIP allow seamless communication across VLANs, while Access Control Lists (ACLs) control traffic flow, ensuring unauthorized users cannot access sensitive data. Unified communications, including IP-based telephony and video conferencing, are increasingly essential for enhancing real-time collaboration in organizations like police stations.

## Research has shown that segmented networks using VLANs and ACLs can drastically reduce the attack surface, limiting exposure to common network attacks like Denial-of-Service (DoS) and unauthorized access. Additionally, deploying IP-based communication systems in critical environments ensures both redundancy and seamless communication during emergencies.

# METHODOLOGY

**Software:**

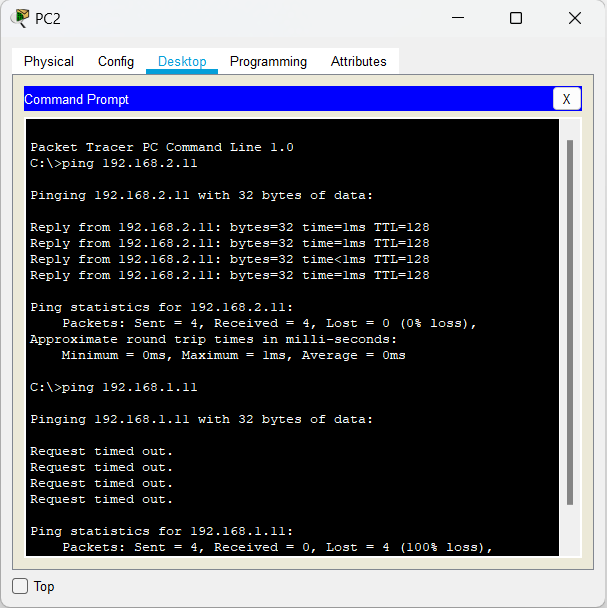
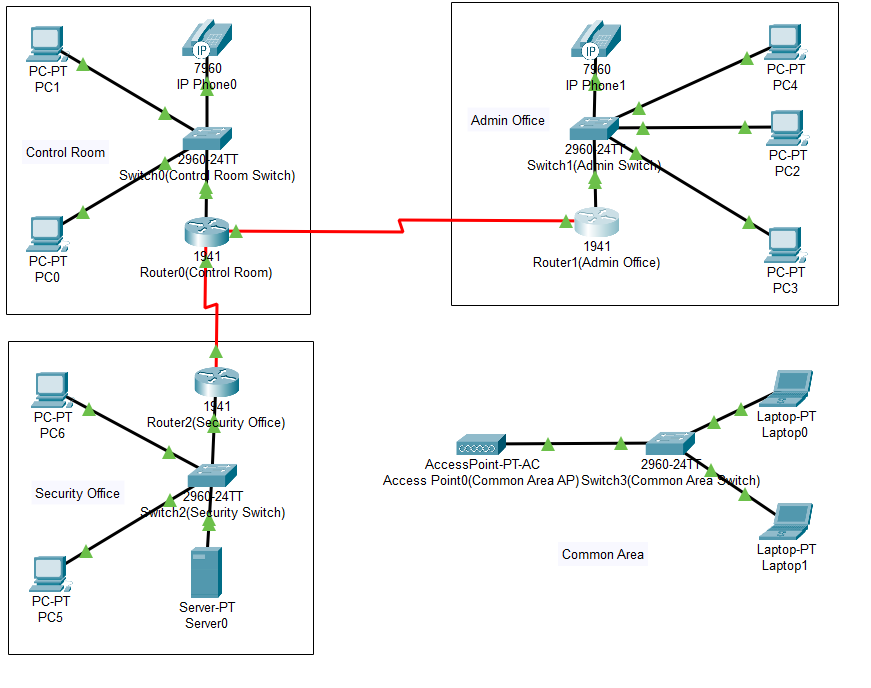
* Cisco Packet Tracer

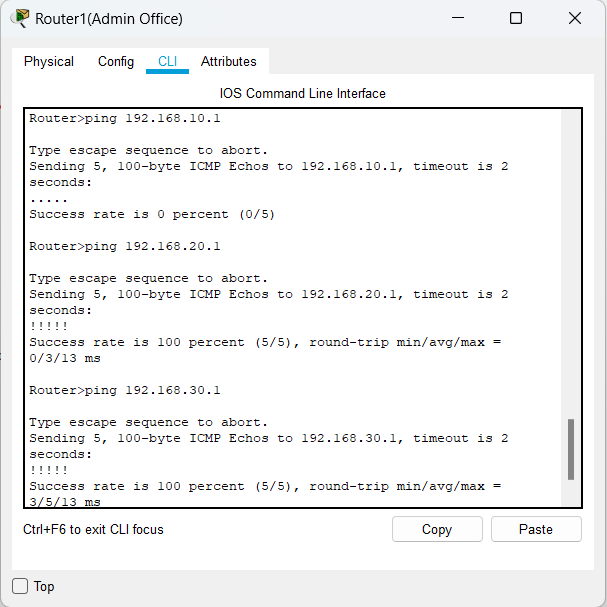
**Network Design:**

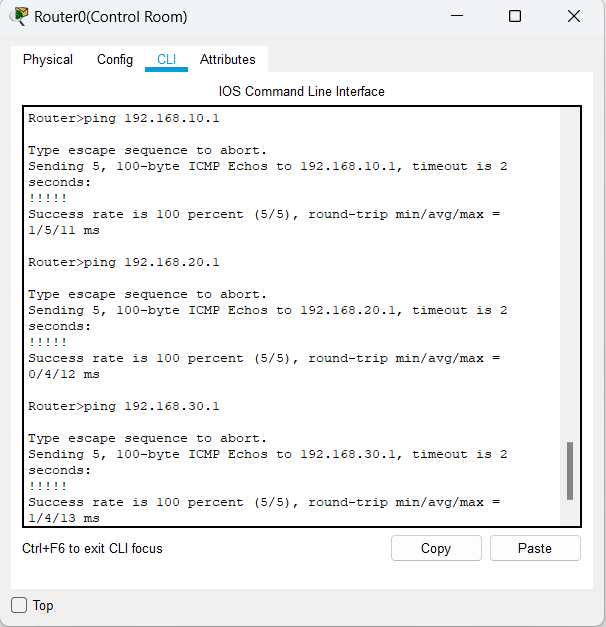
1. **VLAN Creation:**
   * We created four VLANs: Admin, Security, Common Area, and Server VLAN, to segment traffic and enhance security.
2. **IP Address Allocation:**
   * Assigned IP addresses for each VLAN:
     + Admin VLAN: 192.168.10.0/24
     + Security VLAN: 192.168.20.0/24
     + Common Area VLAN: 192.168.30.0/24
     + Server VLAN: 192.168.40.0/24
   * Configured IP addresses for routers and devices within each VLAN.
3. **Inter-VLAN Routing:**
   * Implemented router-on-a-stick configuration to allow communication between VLANs.
   * Configured sub-interfaces on the router for each VLAN.
4. **Routing Protocol Configuration:**
   * Enabled **RIP** routing between routers to ensure dynamic routing across the network.
5. **Access Control Lists (ACLs):**
   * Configured ACLs to restrict access between the Admin and Security VLANs while allowing access between the Admin and Common Area VLANs.
6. **Testing and Verification:**
   * Ping tests were performed between devices in different VLANs to ensure routing and ACLs were working as intended.
   * Web services on servers were accessed through HTTP to verify connectivity.
7. **Unified Communications Setup:**
   * Deployed IP telephony and video conferencing tools across VLANs to enable efficient department communication.

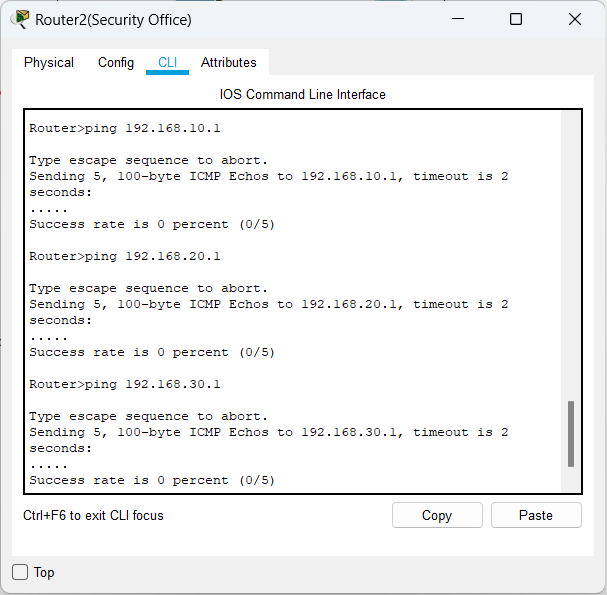
**RESULT:**

### Network Design:









The network was successfully designed and configured in **Cisco Packet Tracer**. The VLANs effectively segmented traffic, and the routing between VLANs allowed for controlled communication. Access Control Lists ensured that sensitive departments like Security were protected from unauthorized access, while unified communication tools worked efficiently across the network.

1. **Network Configuration:**
   * Accurate configuration of VLANs and sub-interfaces.
   * Successful communication between VLANs through inter-VLAN routing.
   * IP telephony and video conferencing were operational, facilitating real-time collaboration between departments.
2. **Security:**
   * ACLs successfully blocked unauthorized access to the Security VLAN while allowing necessary traffic between other VLANs.
   * Sensitive police records were hosted securely on the servers, accessible only by authorized personnel.

## CONCLUSION:

Cisco Packet Tracer provides a valuable platform for simulating network designs, especially in critical environments like police stations.  It enables users to visualize and test the interaction between various network components, ensuring efficient communication and data flow. By simulating real-world scenarios, it helps identify potential issues and optimizes network performance before actual implementation.

* The tool effectively demonstrates multi-mode network topologies, VLAN configurations, and communication protocols like HTTP.
* Access Control Lists (ACLs) were successfully implemented, ensuring secure data segregation and preventing unauthorized access.

Although Packet Tracer does not support real-world web service deployment, it offers essential insights into network security, optimization, and functionality in virtual environments. Real deployment would require dedicated server software.