**SAVEETHA SCHOOL OF ENGINEERING**

**CAPSTONE PROJECT**

**Ensuring Secure Data Transmission and Access Control over VPN Tunnels**

**NAME:** K.Sanjai

**REGISTER NUMBER:** 192325139

# COURSE CODE: CSA0747

**COURSE NAME:** Computer Network for IOT

INTRODUCTION

In today's digital landscape, safeguarding sensitive data during transmission across insecure networks, such as the internet, is paramount for organizations. This project focuses on implementing and enforcing security measures within Virtual Private Network (VPN) tunnels to protect the confidentiality, integrity, and privacy of network communications. By utilizing encryption, authentication, and access control mechanisms, VPN tunnels ensure that data remains secure from unauthorized access or tampering as it moves between remote users or sites and the central network infrastructure. This project aims to explore the essential techniques required to establish secure, trustworthy VPN connections that comply with regulatory requirements while maintaining the privacy of critical information.

LITRATURE REVIEW

A Virtual Private Network (VPN) is a critical technology for securing communications over untrusted networks, such as the internet. Extensive research has highlighted the importance of encryption, authentication, and access control in ensuring the confidentiality, integrity, and privacy of data transmitted through VPN tunnels. Studies emphasize the role of encryption algorithms like AES and RSA in preventing unauthorized access to sensitive information. Additionally, various VPN protocols, such as IPsec and SSL, incorporate robust authentication mechanisms, including digital certificates and pre-shared keys, to verify user identities. Literature also points to the necessity of enforcing access control policies to restrict connectivity to authorized users, safeguarding sensitive network resources. VPNs not only protect data from tampering or interception but also help organizations comply with regulatory requirements related to data protection and privacy, such as GDPR and HIPAA. Overall, VPN technology serves as a foundation for secure and trustworthy communication in modern network infrastructures.

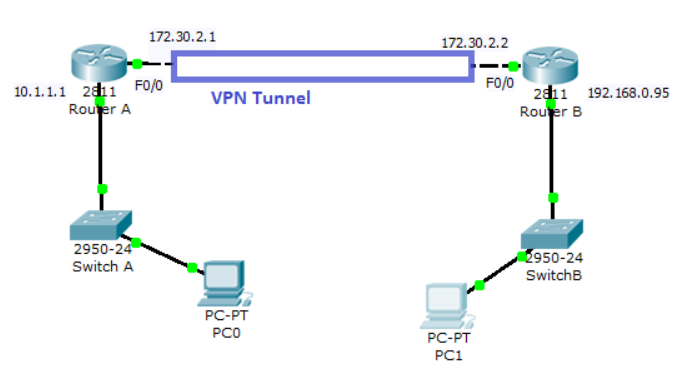
**Methodology**

1. **Network Topology Design**:
   * **Objective**: Create a simulated network environment to establish a VPN.
   * **Steps**: Design a network with at least two remote sites and a central network infrastructure using routers, switches, and PCs. Include relevant network components to simulate a real-world VPN scenario.
2. **VPN Configuration**:
   * **Objective**: Configure VPN protocols to ensure secure communication.
   * **Steps**:
     + On each router, configure IPsec VPN by setting up encryption, authentication, and tunneling protocols.
     + Define encryption (e.g., AES), hashing (e.g., SHA), and Diffie-Hellman groups to ensure data confidentiality and integrity.
     + Establish VPN tunnels between remote sites and the central site.
3. **Authentication and Access Control Setup**:
   * **Objective**: Implement strong authentication mechanisms.
   * **Steps**: Configure pre-shared keys or digital certificates for user and device authentication. Set up access control lists (ACLs) to restrict VPN access to authorized devices and define what network resources they can access.
4. **Data Transmission and Verification**:
   * **Objective**: Test secure data transmission through the VPN.
   * **Steps**: Use Packet Tracer to send data packets between the remote sites and the central network. Verify encryption and the integrity of data by observing the VPN tunnel status and ensuring that packets are successfully delivered without tampering.
5. **Testing and Troubleshooting**:
   * **Objective**: Ensure the VPN is functioning as expected.
   * **Steps**: Use Packet Tracer's simulation tools to monitor packet flow, detect possible issues, and troubleshoot misconfigurations. Test various failure scenarios, such as unauthorized access attempts, to ensure the VPN's security mechanisms are working properly.

This methodology ensures a secure VPN setup and data transmission between remote and central network sites using Cisco Packet Tracer.

**RESULT:**

Network design:



**CONCLUSION:**

In this project, we successfully implemented a secure VPN configuration using Cisco Packet Tracer, ensuring encrypted communication between remote sites and a central network. By setting up IPsec VPN tunnels, we safeguarded data confidentiality, integrity, and privacy during transmission. Additionally, the use of authentication mechanisms and access control policies helped prevent unauthorized access to sensitive network resources. This project demonstrated the effectiveness of VPN technology in protecting network communications over untrusted networks, highlighting its importance for maintaining secure and reliable remote access in real-world scenarios.