# SAVEETHA SCHOOL OF ENGINEERING

**CAPSTONE PROJECT**

**LAN (Local Area Network) and WAN ( Wide Area Network)**

**NAME:** B. Ramya Sri

**REGISTER NUMBER:** 192324262 **COURSE CODE:** CSA0747

**COURSE NAME:** Computer Network for IOT

## INTRODUCTION:

## To achieve seamless data collection and communication, the nodes will be interconnected using a robust network infrastructure, configured either through Local Area Network (LAN) or Wide Area Network (WAN) setups. This network will facilitate efficient routing of information from the field to central data processing units, enabling real-time monitoring and analysis. Each node will be assigned a unique IP address to ensure that data transmission is both secure and organized. This addressing scheme will support reliable communication and prevent data loss or misrouting.

### Objective:

* design a network consist of server
* make a server to provide service to its clients
* showcase the web service
* analysis the pros and cons

## LITERATURE REVIEW

## The deployment of networked monitoring systems in dense forests typically involves the installation of nodes that collect and transmit data regarding wildlife activity. These nodes can be configured in various network architectures, including Local Area Networks (LAN) and Wide Area Networks (WAN). LAN configurations are often used for more localized deployments, where nodes are closely spaced and interconnected to create a network that supports high-speed data transfer and low latency communication. WAN configurations, on the other hand, are employed in broader deployments where nodes are distributed over larger areas, requiring the integration of long-range communication technologies to bridge the distance between nodes.

# METHODOLOGY

**Software:**

* Cisco Packet Tracer

### Network Design:

Network consist of

* + 1 routers
  + 2 switches
  + 2 PC
  + 2 servers

All routers were connected to one another, and each two routers connected two switches, with the third router connecting to a single switch. The first four switches connected two PCs, and the third switch connected two servers.

### IP Address Allocation:

### Step 1:

### • Each node in the wildlife monitoring system will be allocated a unique IP address to facilitate secure and efficient communication. This unique identification is crucial for.

### Step 2:

### Ensuring that data from each node is correctly routed to the central server or other nodes (Hershey et al., 2018).

### Step 3:

### • Allowing for the monitoring and management of individual nodes, including performance metrics, status updates, and fault detection.

### Step 4:

### • Implementing access control and encryption protocols specific to each node based on its IP address to protect against unauthorized access.

### Step 5:

### • For nodes with fixed locations and roles, static IP addressing can be used. This simplifies network management and troubleshooting.

### Step 6:

### • In cases where nodes are mobile or their locations are not fixed, dynamic IP addressing through protocols such as DHCP (Dynamic Host Configuration Protocol) can be utilized to allocate IP addresses as needed.

.

### Protocol:

### 1. Encryption

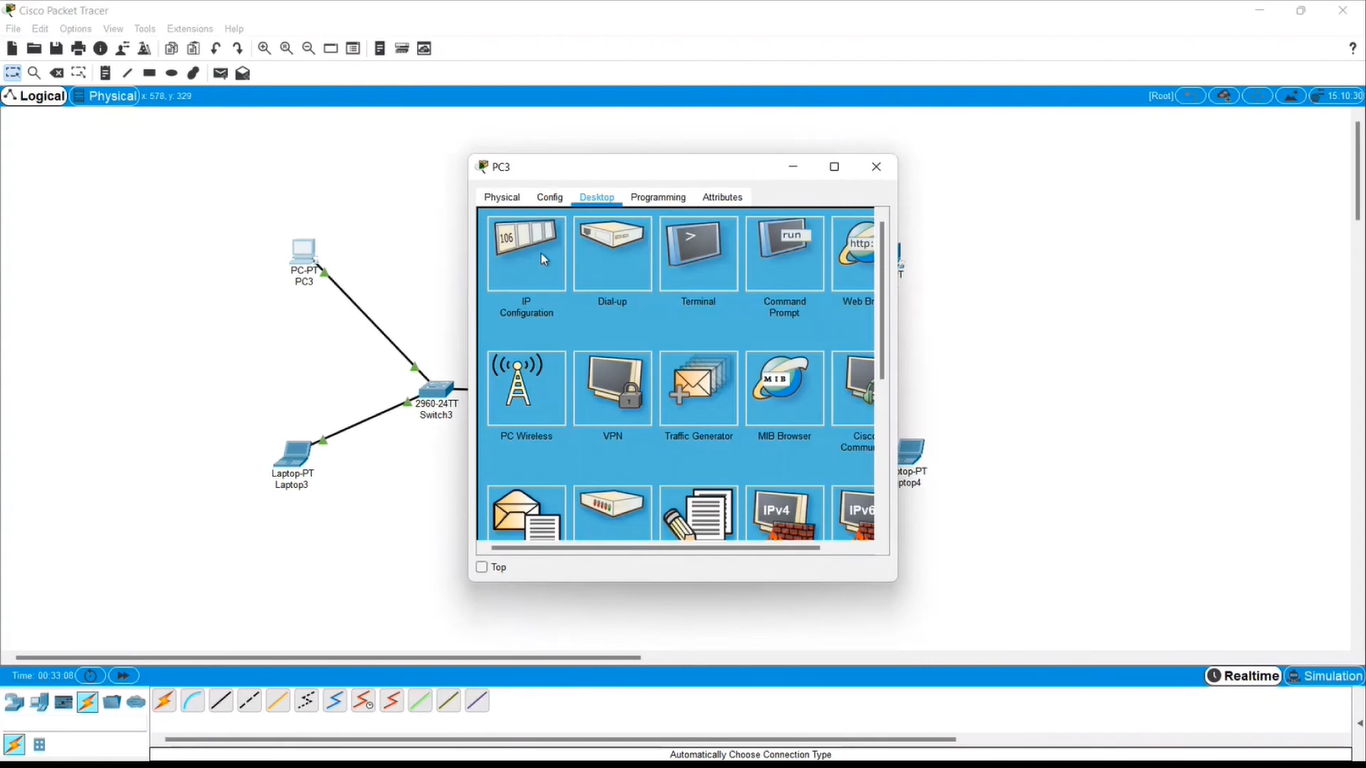
### 2. Authentication

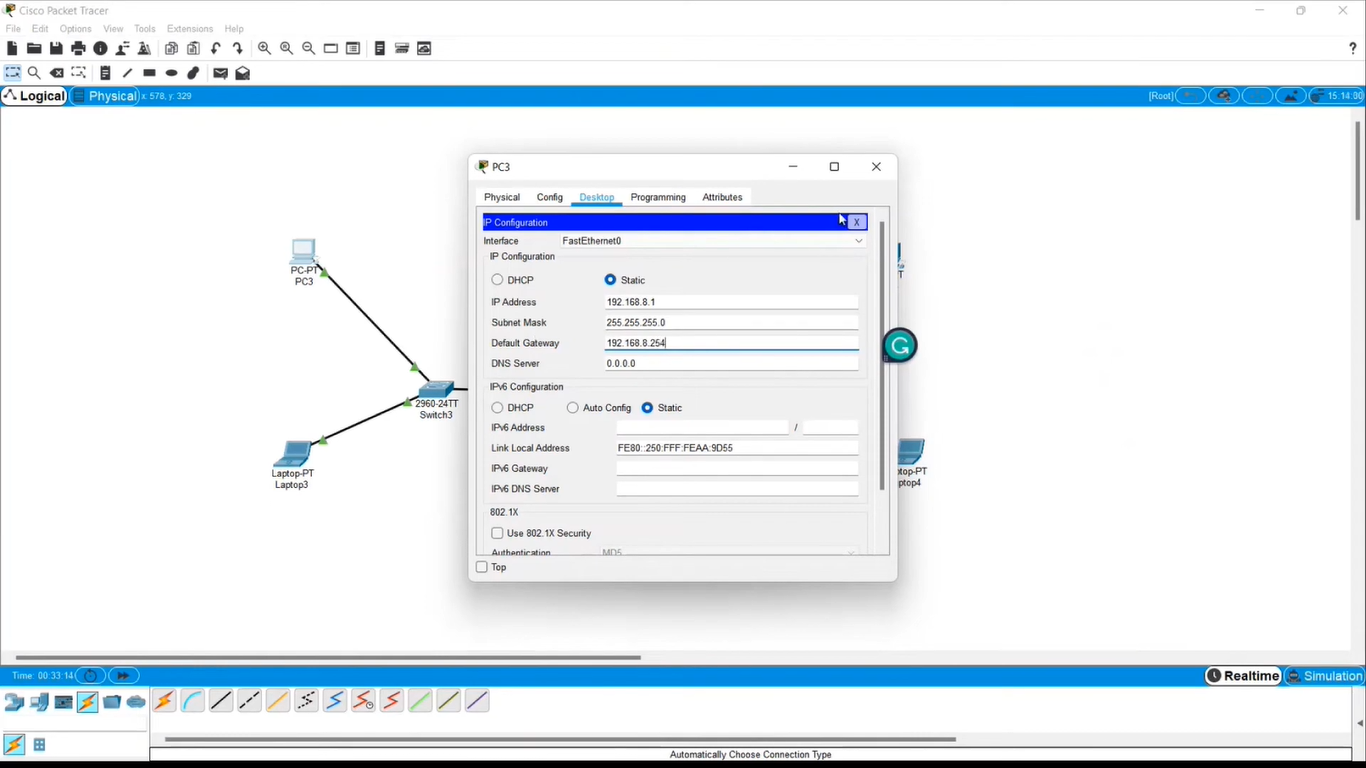
### 3. Access Control

**RESULT:**

### Network Design:

### 



****

## CONCLUSION:

## The deployment of sophisticated wildlife monitoring systems in dense forests represents a significant advancement in the field of conservation technology. This literature review has explored the critical components of network design necessary for effective wildlife tracking, including node placement, network configuration, IP addressing, and security protocols. Strategic placement of monitoring nodes is essential for maximizing coverage and data accuracy in forest environments. The choice between LAN and WAN configurations depends on the specific requirements of the monitoring system, with LANs offering high-speed communication for localized areas and WANs providing extensive coverage for larger, dispersed networks. Both configurations have distinct advantages that impact system performance and data transmission efficiency.

* **Practice Network Design for Web Services:** Packet Tracer helps visualize how web servers, clients, and other network devices interact. This is useful for designing and troubleshooting real-world web service deployments.

Cisco Packet Tracer does not run real web server software, but it does provide a useful platform for learning and experimenting with online services in a virtual network. Real-world web service deployment requires dedicated web server software running on adequate hardware.