

# **SOHO Network Design Project**

## **A PROJECT REPORT**

*Submitted by*

**Ajay Kumar**

**23MCA20225**

*Submitted to*

**Ms. Gagandeep Kaur**

*in partial fulfillment for the award of the degree of*

**MASTER OF COMPUTER APPLICATIONS**



**University Institute of Computing**

**Chandigarh University**

**April 2025**

# Chapter 1: Introduction

## 1.1 Overview

In today's digital world, even small organizations require reliable and secure networks to carry out daily operations. This project involves designing and simulating a **SOHO (Small Office Home Office) Network** using Cisco Packet Tracer. The network is structured to support **three departments** — IT, Finance, and Customer Service — by implementing **VLANs** for segmentation, **router-on-a-stick** for inter-VLAN communication, and **DHCP** for automated IP management. The goal is to provide a scalable and secure environment that supports both **wired and wireless** connectivity.

## 1.2 Features

- **Departmental Segmentation** using VLANs
- **Inter-VLAN Communication** using sub-interfaces on a single router
- **Dynamic IP Addressing** using router-based DHCP pools
- **Secure Wireless Access** with password-protected access points
- **Support for Wired and Wireless Devices** including PCs, laptops, and smartphones
- **Network Simulation and Testing** using Cisco Packet Tracer

## 1.3 Objectives

- To design a scalable network architecture suitable for small businesses
- To segment the network using VLANs for enhanced security and performance
- To enable communication between departments using inter-VLAN routing
- To implement dynamic IP allocation using DHCP
- To integrate wireless networks for mobility and flexibility
- To test the network using simulation tools and validate its performance

# Chapter 2: Requirements

## 2.1 Hardware Requirements

Device	Quantity	Description
Cisco Router (e.g., 2911)	1	For routing and DHCP server configuration
Cisco Switch (e.g., 2960)	1	Layer 2 switch for VLANs and port assignment
Wireless Access Points	3	One per department (IT, Finance, Customer)
PCs	3	Wired clients representing each department
Smartphones/Laptops	3	Wireless devices representing mobile users
Ethernet Cables	As needed	For physical connections (straight-through and crossover)

## 2.2 Software Requirements

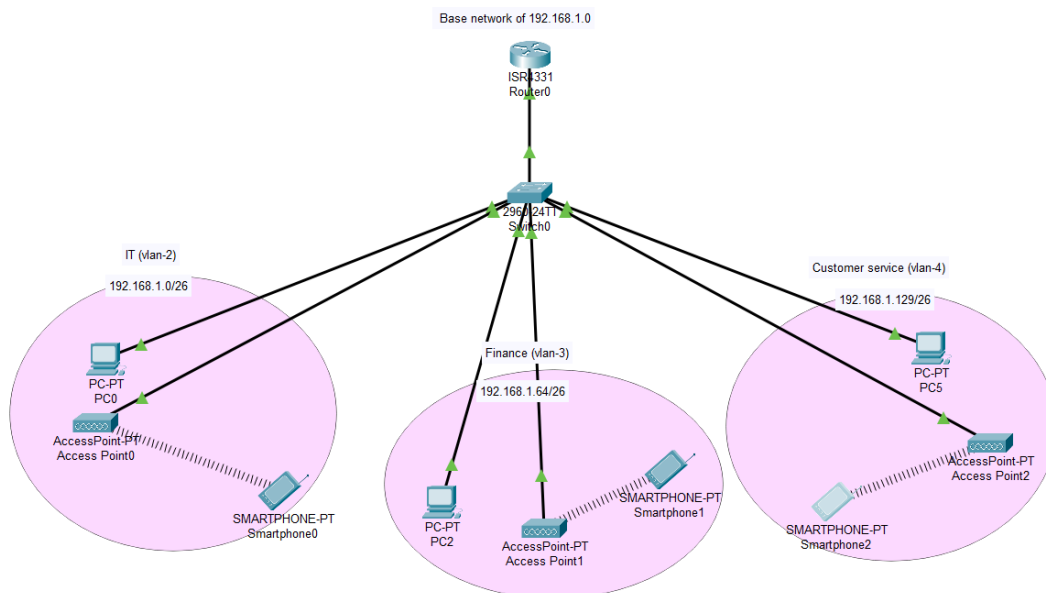
- **Cisco Packet Tracer** (version 8.0 or above)
- Operating systems on end devices with support for IP configuration

- Router and switch IOS with support for VLANs, DHCP, and 802.1Q trunking
- GUI access or command-line knowledge for configuration

## Chapter 3: Implementation and Result

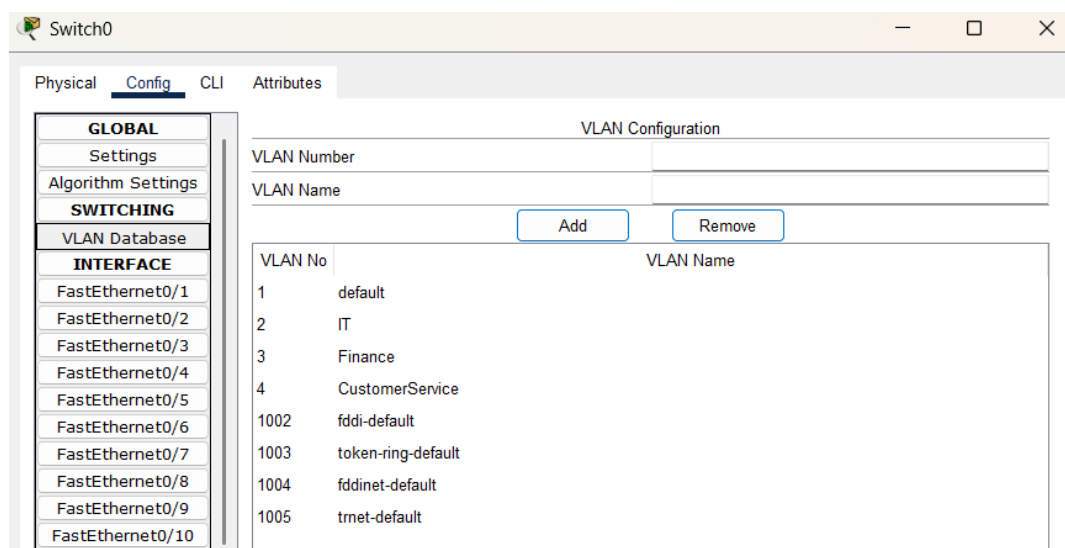
### 3.1 Network Design

The network is divided into **three subnets**, each representing a department. Each department is assigned a **VLAN**, and a subnet is allocated using **CIDR** and subnetting principles. The router interfaces use **802.1Q encapsulation** to support multiple VLANs over a single physical interface.



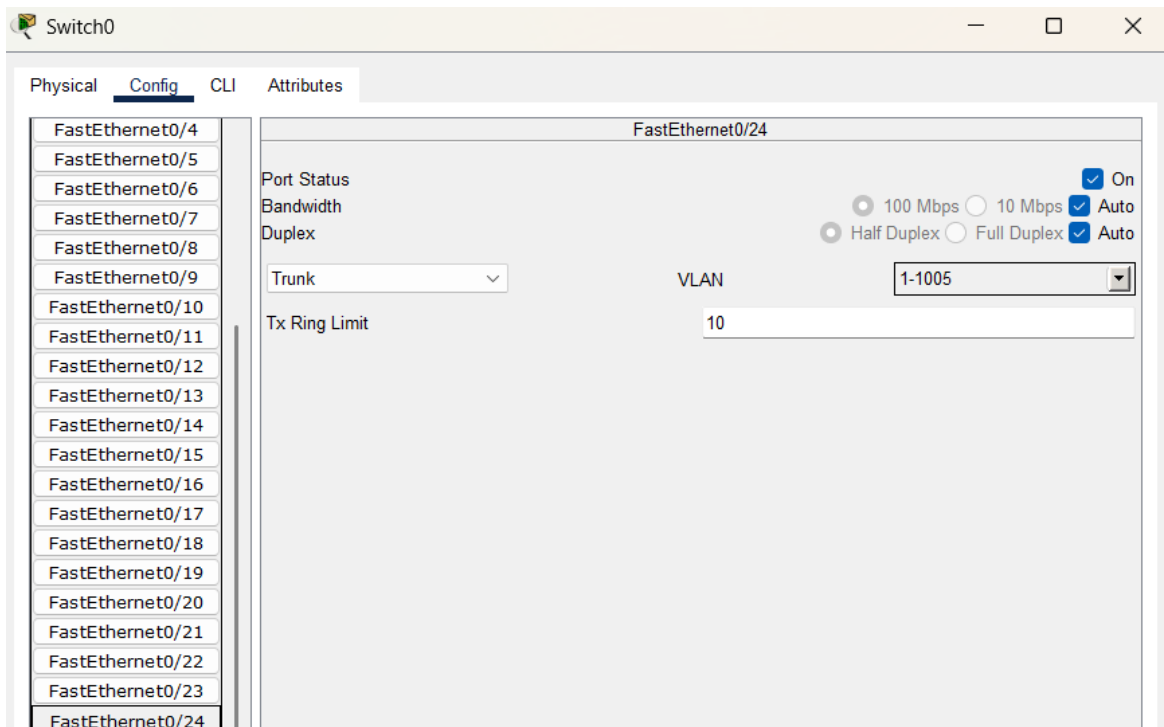
### 3.2 VLAN and IP Addressing Plan

VLAN	Department	Subnet	Default Gateway	IP Range
2	IT	192.168.1.0/26	192.168.1.1	192.168.1.1 – 192.168.1.62
3	Finance	192.168.1.64/26	192.168.1.65	192.168.1.65 – 192.168.1.126
4	Customer Service	192.168.1.128/26	192.168.1.129	192.168.1.129 – 192.168.1.190



### 3.3 Switch Configuration

Ports on the switch were manually assigned to their respective VLANs. One port (Fa0/24) was configured as a **trunk port** to carry VLAN traffic to the router.



### PC Configuration (Wired Clients)

We'll assume each PC is connected to a **VLAN-assigned port on the switch** and will receive its IP from the **router-based DHCP server**.

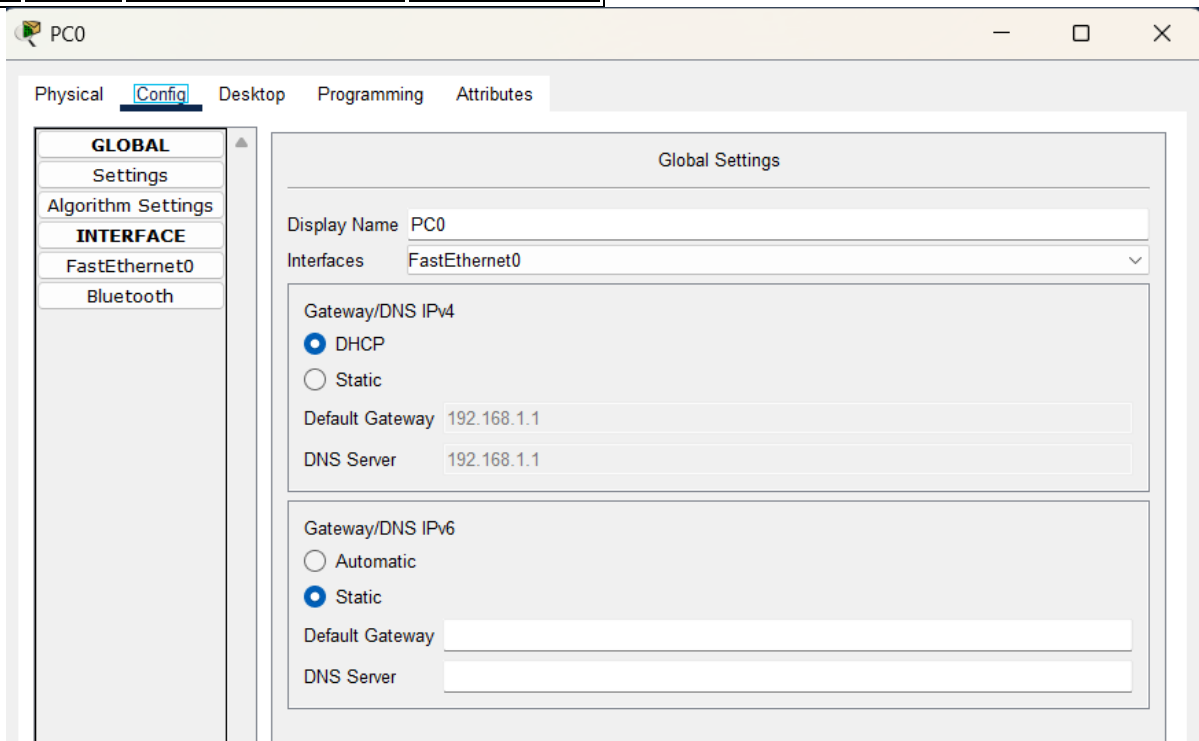
◆ **Step-by-step for each PC:**

- 1. Click on the PC (e.g., **PC\_IT**).
- 2. Go to **Desktop > IP Configuration**.
- 3. Set to **DHCP**.

**Expected IPs (Auto-assigned):**

PC	VLAN	Expected IP Range	Gateway
PC_IT	2	192.168.1.2 – .62	192.168.1.1
PC_Finance	3	192.168.1.66 – .126	192.168.1.65

PC	VLAN	Expected IP Range	Gateway
PC_Customer	4	192.168.1.130 – .190	192.168.1.129



## 🔑 Access Point Configuration (Per Department)

Each Access Point is configured with:

- Unique **SSID**
- **WPA2-PSK security**
- **Static IP** from its department's subnet

### ◆ Access Point – IT Department

1. Click **AccessPoint\_IT**
2. Go to **Config tab**
3. Under **Wireless**:
  - **SSID**: IT\_WiFi
  - **Security**: WPA2-PSK
  - **Passphrase**: it123456
4. Under **FastEthernet**:
  - IP Address: 192.168.1.6
  - Subnet Mask: 255.255.255.192
  - Default Gateway: 192.168.1.1

### ◆ Access Point – Finance Department

1. SSID: Finance\_WiFi
2. Passphrase: fin123456
3. IP Address: 192.168.1.70
4. Subnet Mask: 255.255.255.192
5. Gateway: 192.168.1.65

### ◆ Access Point – Customer Service

1. SSID: Customer\_WiFi
2. Passphrase: cust12345
3. IP Address: 192.168.1.134
4. Subnet Mask: 255.255.255.192
5. Gateway: 192.168.1.129

## Wireless Phone Configuration (Smartphones)

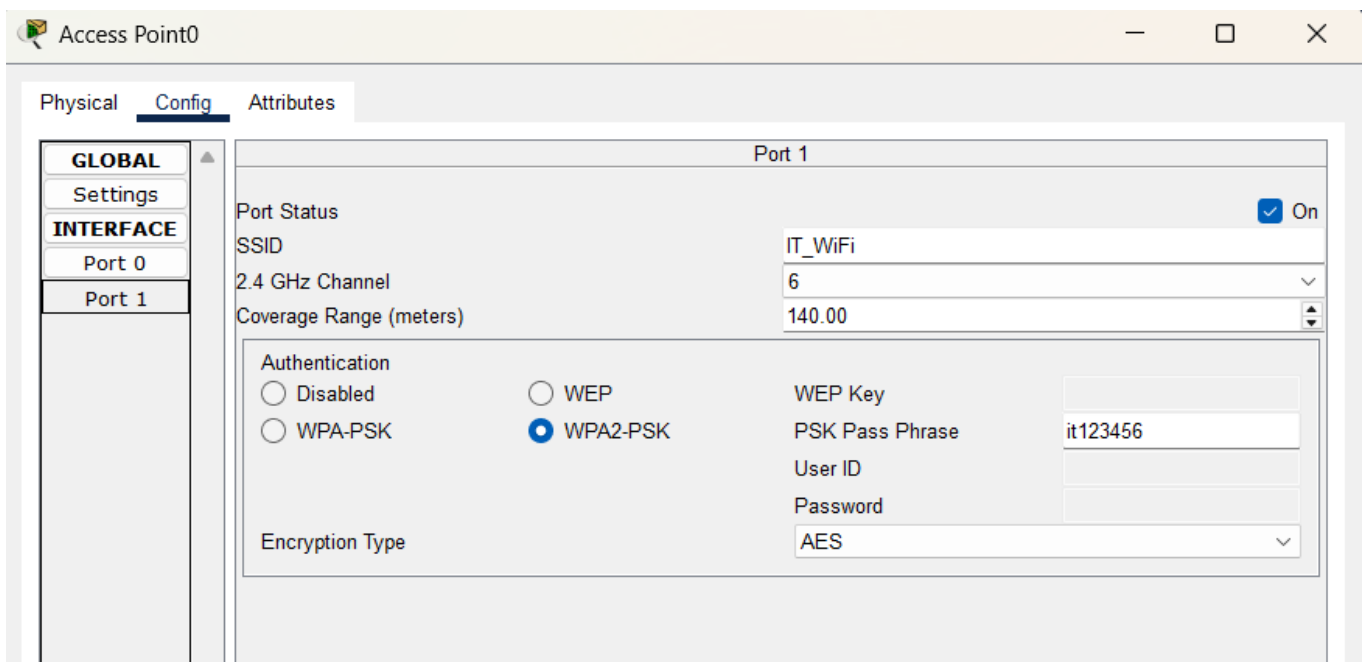
Phones will connect via **GUI Wireless Settings** and use **DHCP**.

### ◆ Step-by-Step:

1. Click on **Smartphone (e.g., Smartphone\_IT)**
2. Go to **Config > Wireless0**
3. Click **Connect**:
  - Choose **SSID**: e.g., IT\_WiFi
  - Enter **password**: it12345
4. Once connected:
  - Go to **Desktop > IP Configuration**
  - Select **DHCP**

### Expected IPs:

Smartphone	VLAN	SSID	IP Range	Gateway
Smartphone_IT	2	IT_WiFi	192.168.1.2 – .62	192.168.1.1
Smartphone_Finance	3	Finance_WiFi	192.168.1.66 – .126	192.168.1.65
Smartphone_Customer	4	Customer_WiFi	192.168.1.130 – .190	192.168.1.129



Access Point0

Physical Config Attributes

**GLOBAL**

Settings

**INTERFACE**

Port 0

Port 1

Port 1

Port Status ☒ On

SSID IT\_WiFi

2.4 GHz Channel 6

Coverage Range (meters) 140.00

Authentication

☐ Disabled ☐ WEP ☒ WPA2-PSK

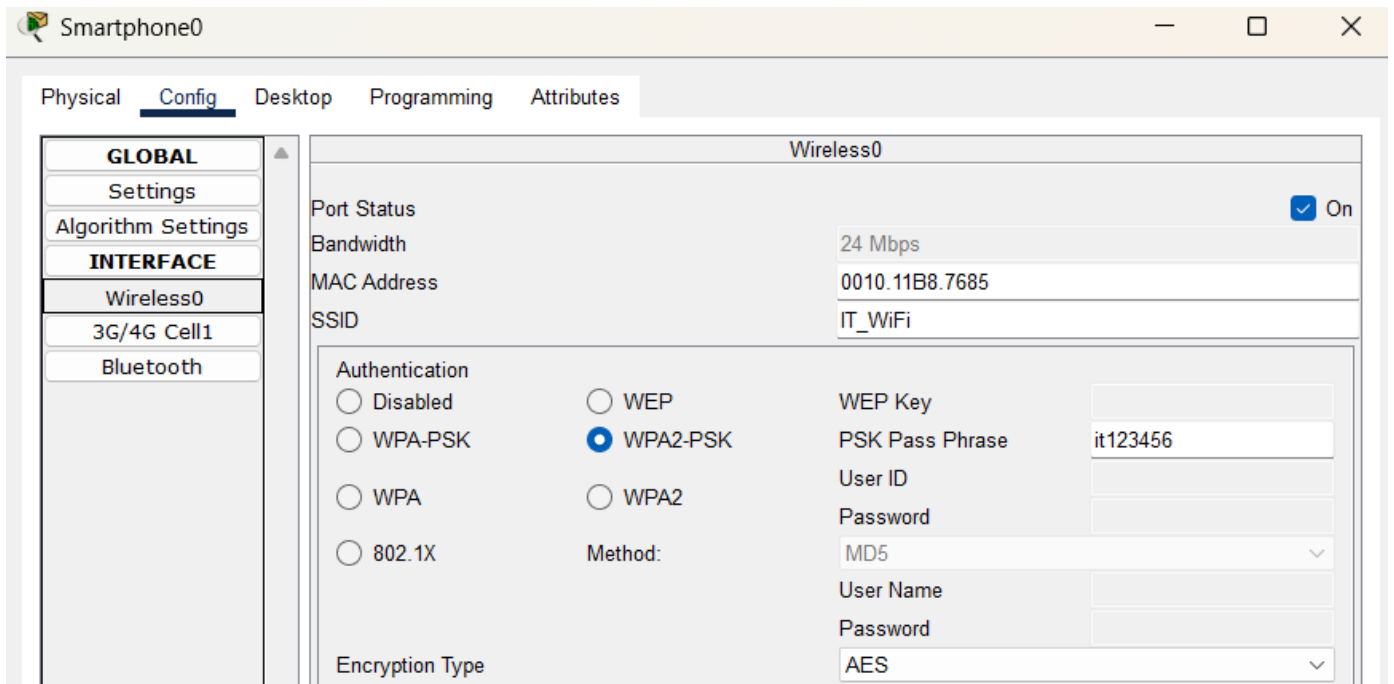
WEP Key

PSK Pass Phrase it123456

User ID

Password

Encryption Type AES

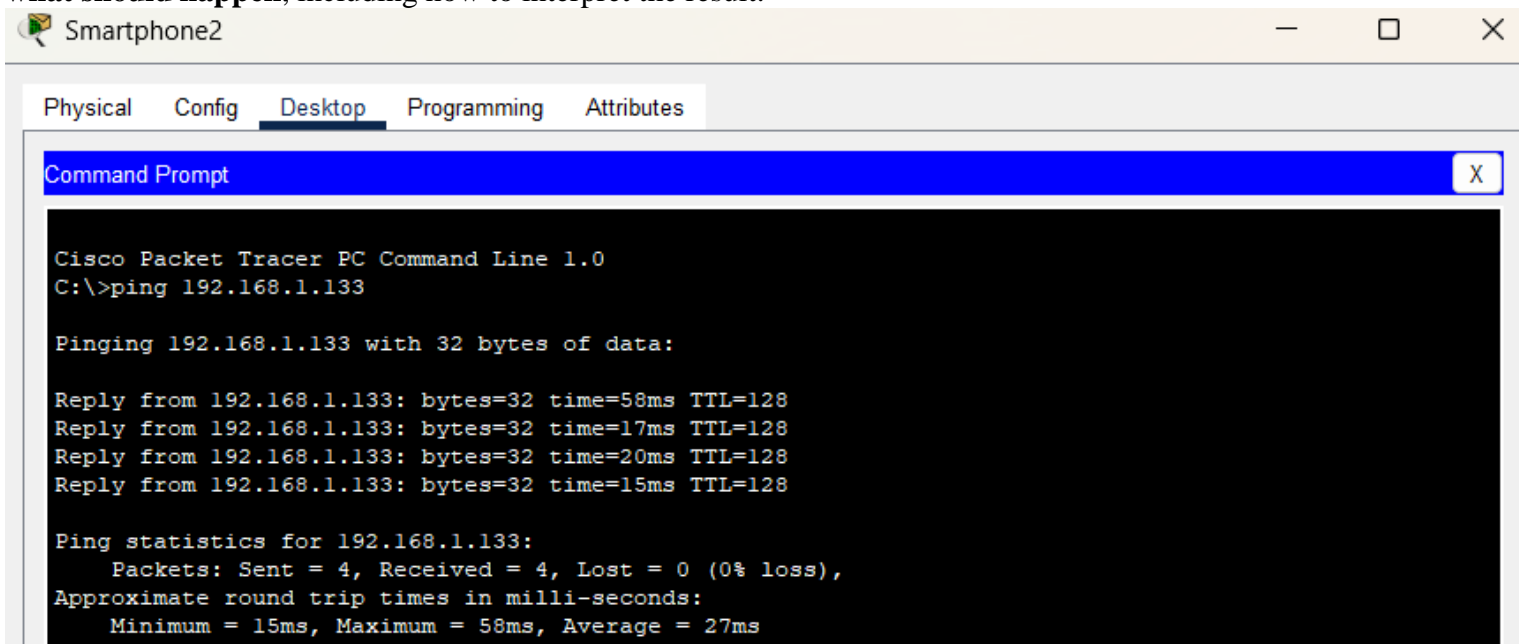


## ✓ Simulation and Connectivity Testing Results

The following tests were conducted using **Cisco Packet Tracer Simulation Mode** and real-time ping tests to verify the network functionality:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Smart...	Smartpho...	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC0	PC2	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC2	PC5	ICMP		0.000	N	3	(edit)	(delete)

Let's walk through the **ping test from Smartphone3 (IP: 192.168.1.133) to Smartphone2** and explain what should happen, including how to interpret the result.



## Result Summary

- **Dynamic IP Assignment:** All devices (PCs and phones) successfully obtained IP addresses from the correct DHCP pool.
- **Wireless Security:** Devices could only connect with correct **WPA2-PSK** credentials.
- **Inter-VLAN Routing:** All departments could communicate as required.
- **Access Point Connectivity:** Each AP was reachable and bridged correctly to VLANs.
- **Segmentation:** Devices in one VLAN couldn't access other VLANs unless routing was enabled.
- **Ping Tests:** Latency was simulated, and all pings returned replies confirming end-to-end communication.
- **Visualization:** Packet Tracer visually confirmed all packets followed the expected path, respecting VLAN tagging and trunk links.



# Chapter 1: Introduction

## 1.1 Overview

In today's digital world, even small organizations require reliable and secure networks to carry out daily operations. This project involves designing and simulating a **SOHO (Small Office Home Office) Network** using Cisco Packet Tracer. The network is structured to support **three departments** — IT, Finance, and Customer Service — by implementing **VLANs** for segmentation, **router-on-a-stick** for inter-VLAN communication, and **DHCP** for automated IP management. The goal is to provide a scalable and secure environment that supports both **wired and wireless** connectivity.

## 1.2 Features

- **Departmental Segmentation** using VLANs
- **Inter-VLAN Communication** using sub-interfaces on a single router
- **Dynamic IP Addressing** using router-based DHCP pools
- **Secure Wireless Access** with password-protected access points
- **Support for Wired and Wireless Devices** including PCs, laptops, and smartphones
- **Network Simulation and Testing** using Cisco Packet Tracer

## 1.3 Objectives

- To design a scalable network architecture suitable for small businesses
- To segment the network using VLANs for enhanced security and performance
- To enable communication between departments using inter-VLAN routing
- To implement dynamic IP allocation using DHCP
- To integrate wireless networks for mobility and flexibility
- To test the network using simulation tools and validate its performance

# Chapter 2: Requirements

## 2.1 Hardware Requirements

Device	Quantity	Description
Cisco Router (e.g., 2911)	1	For routing and DHCP server configuration
Cisco Switch (e.g., 2960)	1	Layer 2 switch for VLANs and port assignment
Wireless Access Points	3	One per department (IT, Finance, Customer)
PCs	3	Wired clients representing each department
Smartphones/Laptops	3	Wireless devices representing mobile users
Ethernet Cables	As needed	For physical connections (straight-through and crossover)

## 2.2 Software Requirements

- **Cisco Packet Tracer** (version 8.0 or above)
- Operating systems on end devices with support for IP configuration
- Router and switch IOS with support for VLANs, DHCP, and 802.1Q trunking
- GUI access or command-line knowledge for configuration

## Chapter 3: Implementation and Result

### 3.1 Network Design

The network is divided into **three subnets**, each representing a department. Each department is assigned a **VLAN**, and a subnet is allocated using **CIDR** and subnetting principles. The router interfaces use **802.1Q encapsulation** to support multiple VLANs over a single physical interface.

### 3.2 VLAN and IP Addressing Plan

VLAN	Department	Subnet	Default Gateway	IP Range
2	IT	192.168.1.0/26	192.168.1.1	192.168.1.1 – 192.168.1.62
3	Finance	192.168.1.64/26	192.168.1.65	192.168.1.65 – 192.168.1.126
4	Customer Service	192.168.1.128/26	192.168.1.129	192.168.1.129 – 192.168.1.190

### 3.3 Switch Configuration

Ports on the switch were manually assigned to their respective VLANs. One port (Fa0/24) was configured as a **trunk port** to carry VLAN traffic to the router.

### 3.4 Router Configuration

The router's single interface was divided into **three sub-interfaces**, each corresponding to a VLAN. **DHCP pools** were configured for each VLAN to provide dynamic IP addresses. The router acted as the default gateway for each department and also handled address distribution.

Sample DHCP Config: