SIMPLE OFFICE NETWORKING USING DHCP

***Submitted by***

# M.Abraham Martin – RA2211028010224

**B.Sasikiran–RA2211028010227 Akshaykumar – RA2211028010229**

***for the course***

***21CSC302J – COMPUTER NETWORKS***

***in partial fulfillment of the requirements for the degree of BACHELOR OF TECHNOLOGY***



**DEPARTMENT OF NETWORKING AND**

**COMMUNICATIONSSCHOOL OF COMPUTING FACULTY OF ENGINEERING AND TECHNOLOGY SRM INSTITUTE OF SCIENCE AND TECHNOLOGYKATTANKULATHUR - 603 203.**

**NOVEMBER 2024**



# Abstract

This case study details the design and implementation of a network for an Enterprise, focused on operating independently from headquarters while meeting essential communication and security needs. Using Cisco Packet Tracer, the network integrates a router, switch, and wireless access points, creating a structured, scalable environment. The network is segmented into VLANs for three departments— Admin/IT, Finance/HR, and Customer Service/Reception—enabling secure data separation and optimized management. DHCP is configured for automatic IPv4 address allocation, and inter-VLAN routing allows for secure inter-departmental communication. Wireless connectivity within each department enhances flexibility, while VLAN configuration strengthens security. The network was tested and validated using Cisco Packet Tracer, ensuring that the design meets performance and security standards. This implementation demonstrates a practical, scalable approach for small business networking, addressing the branch's current operational needs and providing a foundation for future growth.

**Table of Contents**

[Abstract………………………………………………………………….. 3](#_TOC_250006)

1. [Introduction………………………………………………………… 5](#_TOC_250005)
2. [Network Design……………………………………………………. 6](#_TOC_250004)
3. Setting Access Points in each Department………………………… 8
4. Switching Configuration…………………………………………... 11
5. Routing Configuration…………………………………………….. 13
6. Dynamic Host Configuration Protocol (DHCP)………………….. 17
7. [Results and Evaluation…………………………………………..... 20](#_TOC_250003)
8. [Conclusion………………………………………………………… 21](#_TOC_250002)
9. [References…………………………………………………………. 22](#_TOC_250001)
10. [Appendices………………………………………………………... 22](#_TOC_250000)
11. Course Completion Certificate…………………………………… 23

**Table of Figure: -**

Fig2.1 – Topology of full network \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 6

Fig3.1 – WIFI 10

Fig3.2 – WIFI 10

Fig3.3 – WIFI 11

Fig5.1 – router config 13

Fig6.1 – PC0 desktop 17

Fig6.2 – printer config 18

Fig6.3 – smartphone 19

Fig7.1 – ping command 20

# CHAPTER 1

# Introduction

* 1. **Background**

In today’s rapidly evolving network landscape, the "Branch Network Deployment" project addresses the essential need for a dedicated and secure network infrastructure for an Enterprise’s office, focused on buying and selling goods. The office is designed to operate independently from the headquarters, ensuring uninterrupted local operations and secure data management. This network aims to support key business functions for three departments— Admin/IT, Finance/HR, and Customer Service/Reception—each with distinct requirements for connectivity and data security. Leveraging Cisco technology for routers and switches, this project prioritizes an organized, resilient, and future-ready network to meet the demands of this growing branch office.

# Objectives

The primary objectives of the "Branch Network Deployment" project are to design efficient, scalable network infrastructure tailored to the specific needs of a small branch office. The project focuses on implementing VLANs to isolate each department, ensuring data segmentation and security, while establishing wireless access for user mobility. Key goals include configuring DHCP for automatic IP allocation, enabling seamless inter-department communication via inter-VLAN routing, and applying necessary security protocols. This network design aims to provide a reliable, secure, and adaptable infrastructure that supports current operations while preparing for potential expansions and technological advancements as the branch grows.

# CHAPTER 2

# Network Design

* 1. **Topology**

The network configuration designed for the "Branch Network Deployment" project adopts a simplified hierarchical topology to achieve efficiency, manageability, and security for a small branch office. This design includes two primary layers: the core and access layers. At the core layer, a single router facilitates centralized routing, inter-VLAN communication, and manages internet access for the branch. A switch operates at the access layer, connecting different departments and organizing them into distinct Virtual Local Area Networks (VLANs) for Admin/IT, Finance/HR, and Customer Service/Reception. Each VLAN provides logical segmentation to ensure data privacy and network efficiency.

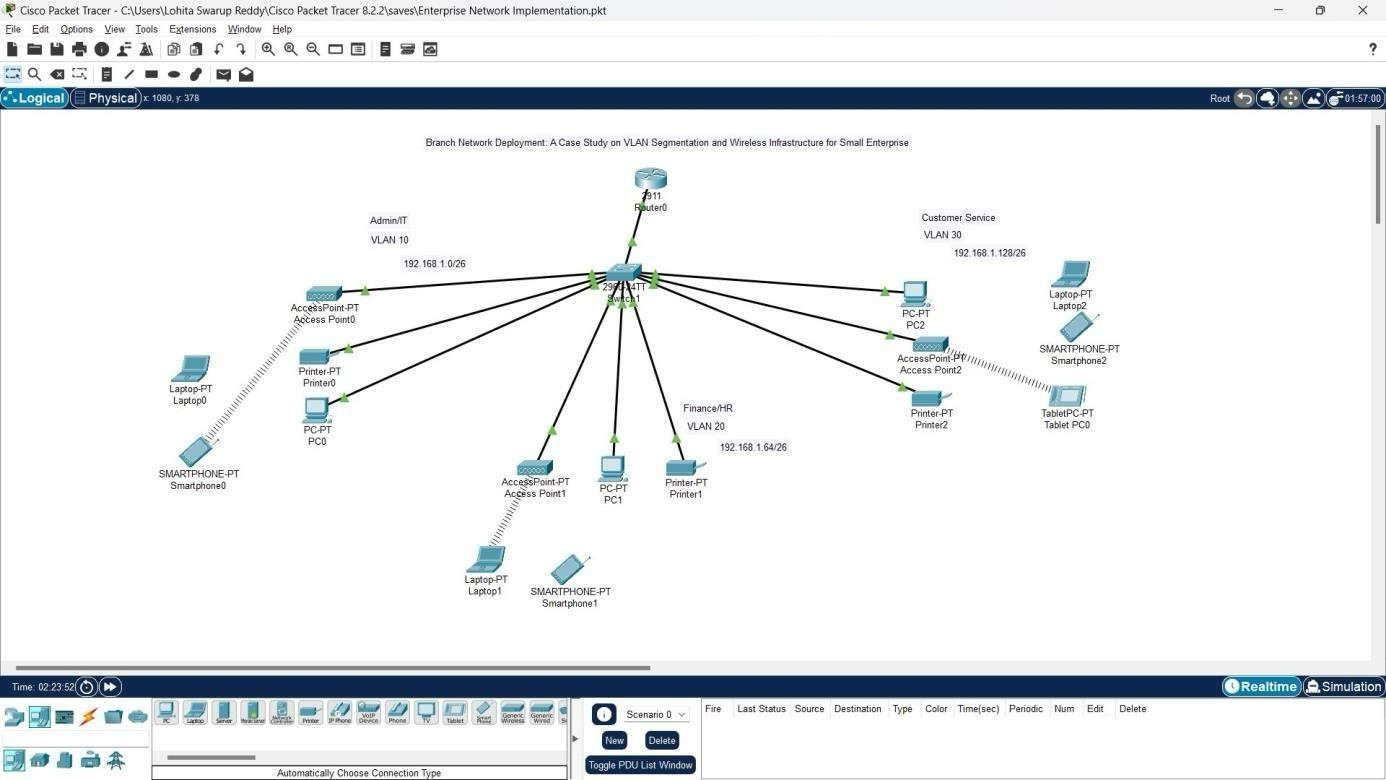
The access layer supports end-user devices, including PCs and wireless access points for each department, connecting to the central switch to ensure seamless connectivity and mobility. DHCP configuration on the router allows automatic IP assignment across all VLANs, reducing manual configuration. This Figure 2.1 topology provides a structured, scalable layout, suitable for the branch's needs, and facilitates smooth communication between departments while maintaining data segregation and security.

Figure 2.1: Topology of full network

# COMPONENTS

The network design for the "Branch Network Deployment" project incorporates the following essential devices:

## Router (1):

1. **Switch (1):**
2. **Printers (3):**
   * A single 2911 Router is deployed at the core layer to manage inter-VLAN communication,DHCP services, and internet connectivity.
   * Configured to enable dynamic IP allocation and inter-departmental routing.
   * Positioned at the access layer, the 2960-24TT Switch connects all wired devices and provides VLAN segmentation for the three departments: Admin/IT, Finance/HR, and Customer Service/Reception.
   * Configured to support VLANs for data separation and security
   * Each department has a dedicated printer connected to the network, configured to operate within its respective VLAN to maintain data privacy.

## Access Points (Aps):

* + Three wireless access points, one for each department, are deployed to provide wireless connectivity for mobile devices.
  + Configured with separate SSIDs to align with departmental VLANs, ensuring secure and isolatedaccess for wireless devices.

## End -User Devices (PCs):

* + Three PCs, one assigned to each department, are deployed for essential departmental operationsand communication.
  + Each PC connects to the designed VLAN, allowing secure departmental data sharing.

## Wireless End Devices (Mobile, Laptop, Tablet):

* + Wireless devices such as laptops, tablets, and mobile phones connect through the department-specific wireless access points.
  + DHCP ensures these devices receive dynamic IP addresses for seamless wireless connectivity.

These components form a streamlined, well-structured network, optimizing connectivity, security, and ease of management. This architecture meets the branch office’s requirements, allowing inter- departmental communication while maintaining data integrity and scalability for future growth.

# IP Addressing Scheme

## Base Network: 192.168.1.0 Number of Subnets: 3

**Subnet Mask After Borrowing 2 Bits: 255.255.255.192 Block Size: 64**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Department** | **Network ID** | **Subnet Mask** | **Host Address Range** | **Broadcast Address** |
| **Admin/IT** | 192.168.1.0 | 255.255.255.192 | 192.168.1.1 - 192.168.1.62 | 192.168.1.63 |
| **Finance/HR** | 192.168.1.64 | 255.255.255.192 | 192.168.1.65 - 192.168.1.126 | 192.168.1.127 |
| **Customer Service** | 192.168.1.128 | 255.255.255.192 | 192.168.1.129 -192.168.1.190 | 192.168.1.191 |

*Table 2.3.1*

In this *Table 2.3.1* IP addressing scheme provides dedicated network segments for each department, ensuringsecure data separation and efficient management within the branch network.

**CHAPTER 3**

# Setting Access Points in each Department

To enable wireless communication for each department, set up dedicated wireless access points configured with unique SSIDs and secure passphrases. Here’s how each department's wireless setup was implemented:

# Admin/IT Department:

* **SSID**: Admin-WIFI
* **Security Protocol**: WPA2-PSK (Wi-Fi Protected Access 2 with Pre-Shared Key)
* **Passphrase**: Admin@123

This SSID and security configuration ensure that only authorized Admin/IT users with the passphrase can connect to the network.

# Finance/HR Department:

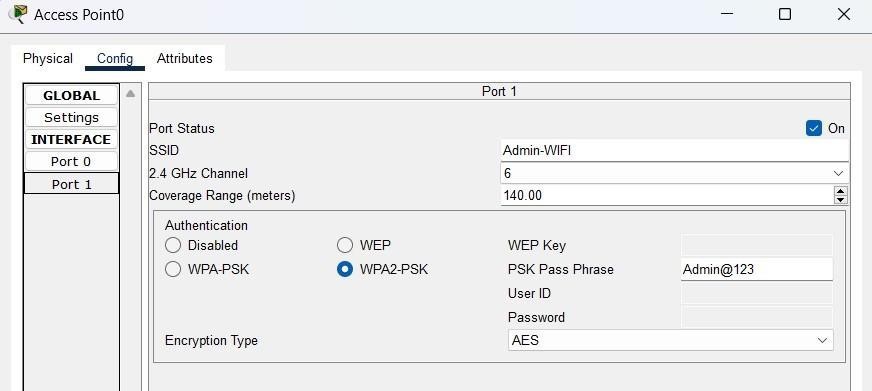
* + - **SSID**: Finance-WIFI
    - **Security Protocol**: WPA2-PSK
    - **Passphrase**: Finance@123
    - Similarly, this secure setup allows only Finance/HR users to connect, ensuring department-specific access and protecting sensitive financial data.

# Customer Service/Reception Department

* + - **SSID**: CS-WIFI
    - **Security Protocol**: WPA2-PSK
    - **Passphrase**: CustomerService@123
    - The Customer Service/Reception team has its own SSID and passphrase, ensuring that guests and employees in this department can connect without accessing the internal networks of other departments

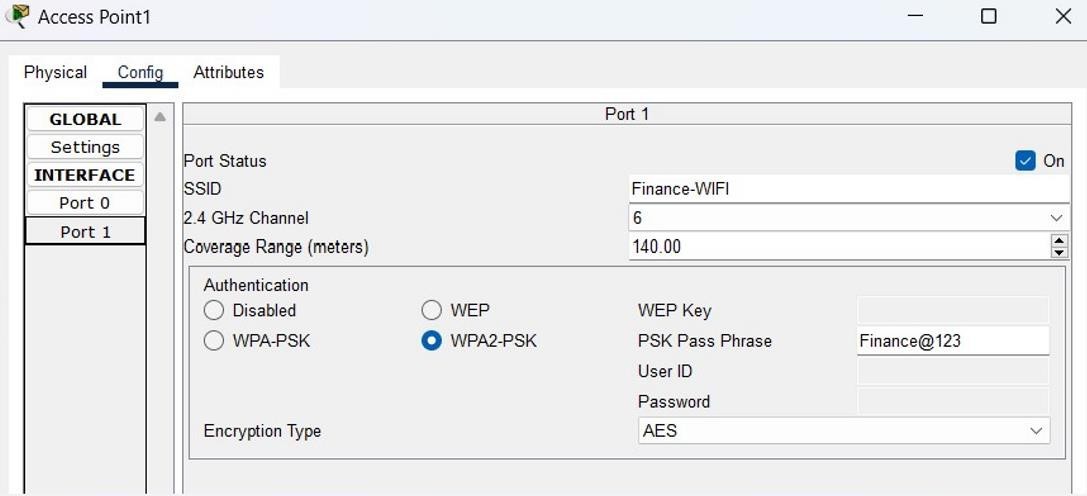
These configurations meet the company’s requirement for secure, department-specific wireless networks, allowing each department to operate independently yet securely within the overall network. By using WPA2-PSK, you’ve ensured strong encryption, which protects against unauthorized access and data breaches.

This Figure 3.1 shows the configuration settings for an Access point0, including SSID, channel, coverage range, and WPA2-PSK authentication with AES encryption. The passphrase "Admin@123" is set for network security.



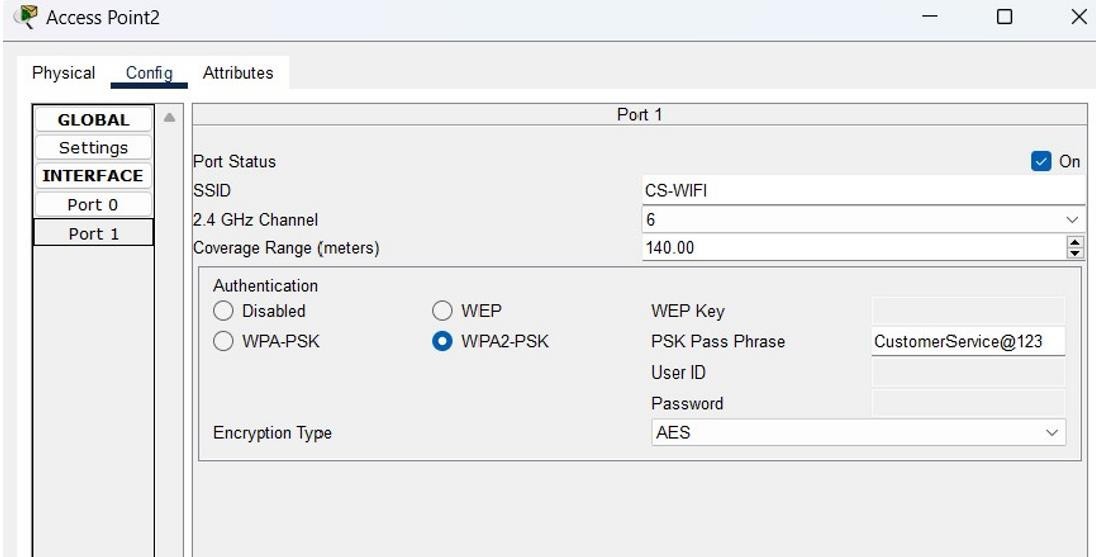
*Figure 3.1 - WIFI*

This Figure 3.2 shows the configuration settings for an access point 01, including SSID, channel, coverage range, and WPA2-PSK authentication with AES encryption. The passphrase "Finance@123" is set for network security.



*Figure 3.2 -WIFI*

This Figure 3.3 shows the configuration settings for an access point 02, including SSID, channel, coverage range, and WPA2-PSK authentication with AES encryption. The passphrase "CustomerService@123" is set for network security.



*Figure 3.3- WIFI*

**CHAPTER 4**

# 4.1Switch Configuration

To configure VLANs on the switch, VLAN 10 is created for Admin/IT, VLAN 20 for Finance/HR, and VLAN 30 for Customer Service, with specific access ports assigned to each VLAN.

# Commands:

Switch (config) #int range fa0/2-4Switch (config-if- range) fa

& Incomplete command.

Switch (config-if-range) #switchport mode access Switch (conf1g-1f-range) #switchport access VLAN 103 Access VLAN does not exist. Creating VLAN 10 Switch (config-if-range) #

Switch (config-if-range) #int range fa0/5-7 Switch (config-if-range) #switchport mode access

Switch (contig-11-range) #switchport access VLAN 20 Access VLAN does not exist. Creating

VLAN20

Switch (config-if-range) # Switch (config-if-range) #

Switch (config-if-range) $int range fa0/8-

10 Switch (config-if-range) #switchport mode access

Switch (config-if-range) #switchport access VLAN 30

\* Access VLAN does not exist. Creating VLAN 30Switch (contig-11-range) #do wr

Building configuration...(OK]

Switch (config-if-range) #exit Switch (config) do show start Using 1539 bytes

version 15.0

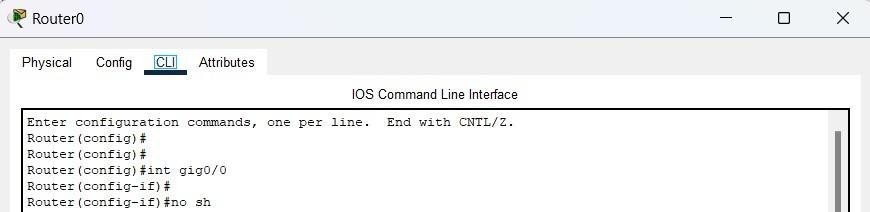
no service timestamps log datetime msec no service timestamps debug datetime me no service password-encryptionhostname Switch

spanning-tree mode spanning-tree extend system-idinterface FastEthernet0/1 interface FastEchernet0/2

# CHAPTER 5

# Router Configuration

* 1. **Router Configuration**

Figure 5.1 shows the command line interface (CLI) configuration for Router0, where the `gig0/0` interface is accessed and enabled with the `no shutdown` command.

*Figure 5.1-router config*

# Interface Configuration and VLANs

Sub-interfaces have been configured on the main GigabitEthernet0 interface (e.g., gig0/0.10, gig0/0.20, and gig0/0.30) to represent VLANs for each department. This setup isolates each department within its own VLAN while enabling inter-VLAN communication through the router. Each sub-interface is tagged with VLAN encapsulation using dot1Q, followed by a VLAN ID (e.g., dot1Q 10 for Admin, dot1Q20 for Finance, and dot1Q 30 for Customer Service), allowing the router to identify and manage traffic foreach VLAN across the network.

# IP Address Assignment for VLANs:

Each sub-interface is assigned an IP address within its own subnet to serve as the default gateway for devices in each VLAN. For example, VLAN 10 uses 192.168.1.1, VLAN 20 uses 192.168.1.65, and VLAN 30 uses 192.168.1.129, all with a subnet mask of 255.255.255.192.

This configuration enables devices in each VLAN to receive IP addresses and settings like gateway andDNS automatically via DHCP, simplifying network management

# Commands:

Router (config-if) # Router (config-if) #exit Router (config) f Router (config) #

Router (config) fint gig0/0.10 Router (Conf1g-gub1f) #

SLINK-5-CHANGED: Interface GigabitEtherneto/0.10, changed state to up

SLINEPROTO-S-UPDOWN: Line protocol on Interface GigabitEcherneco/0.10, changed state to up Router (config-subif) #

Router (contig-subif) fencapaulation dot 1Q

\* Incomplete command.

Router (config-subif) #encapsulation dot10 10

Router (config-subif) #ip address 192.168.1.1 255.255.255.192 Router (conf1g-sub1f) $

Router (config-subif) exit Router (config) #

Router (config) #int g1g0/0.20 Router (contig-subif) +

&LINK-S-CHANGED: Interface GigabitEthernet0/0.20, changed state to up

ALINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEcherneto/0.20, changed state to up Router (contig-aubif) #encapaulation dot10 20

Router (config-subif) $

Router (config-subif) #ip address 192.168.1.65 255.255.255.192 Router (config-subif) fdo wr

Building configuration... [OK]

Router (config-subif) # Router (config-sub1f) $ex

Router (config) #

Router (config) Fint 0100/0.30 Router （contig-sub2f）

SLINK-5-CHANGED: Interface GigabitEtherneto/0.30, changed state to up

#LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEchernet0/0.30, changed state to up Router (config-subif) #encapsulation dot10 30

Router （contig-subit） #ip address 192.268.1.129 255.255.255.192 Router (config-subif) fdo wr

interface GigabitEthernet0/0

no ip address duplex auto speed auto intertace GigabitEthernet0/0.10 encapsulation dotiQ 10

ip address 192.168.1.1 255.255.255.192

Interface GigabitEtherneto/0.20 encapsulation dot10 20

ip address 192.168.1.65 255.255.255.192

interface GigabitEthernet0/0.30 encapsulation dot10 30

1p address 192.168.1.129 255.255.255.192

interface GigabitEthernet0/1

no 1p address duplex auto speed auto shutdown

interface GagabatEtherneto/2

no ip address duplex auto speed auto shutdown

interface VLAN no id addressshutdown

# Commands for router:

Router (config) # Router (config) #

Router (config) #ip dhep pool Admin-Pool Router (dhcp-config) #

Router (dhcp-config) #network 192.168.1.0 255.255.255.192 Router (dhcp-config) #default-router 192.168.1.1

Router (dhcp-conf1g) #dng-sexver 192.168.1.2 Router (dhcp-config) #domain-name Admin.com Router (dhcp-config) #exit

Router (config) f Router (config) # Router (dhcp-config) ex Router (config) #

Router (contig) #ip dhcp pool CS-pool

Router (dhcp-config) #network 192.168.1.128 255.255.255.192

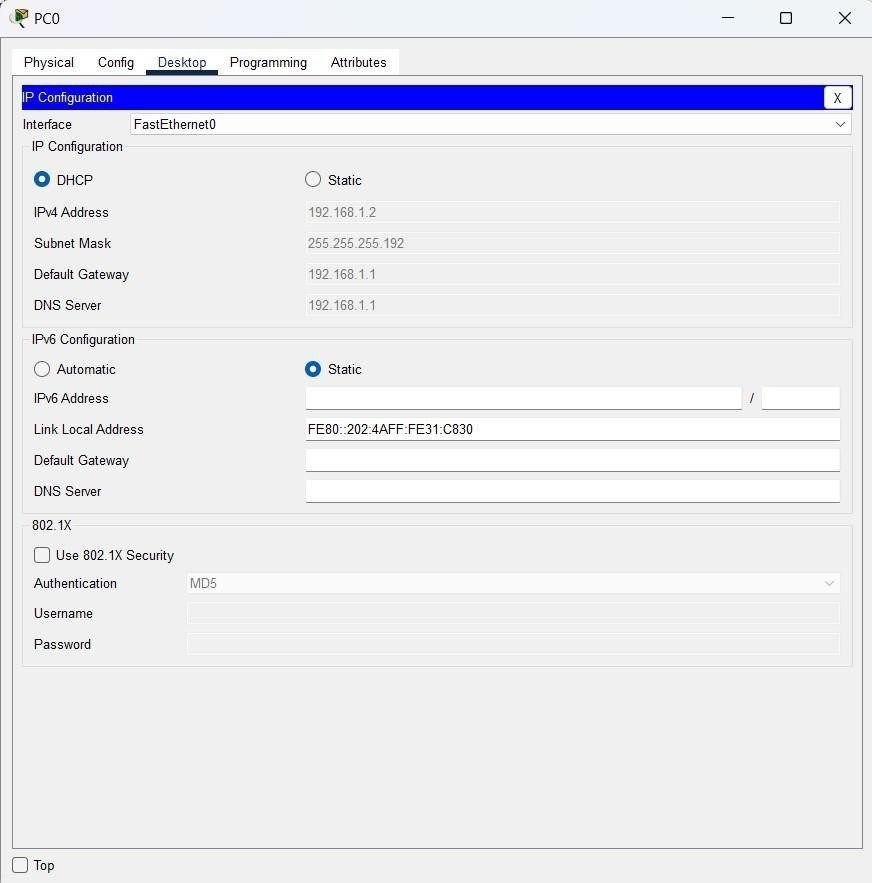
Route (dhcp-config) default 192. 162.15021- 129Router (dhcp-contig) fdomain-name cs.com Router (dhcp-config) #

Router (dhcp-config) #

# CHAPTER 6

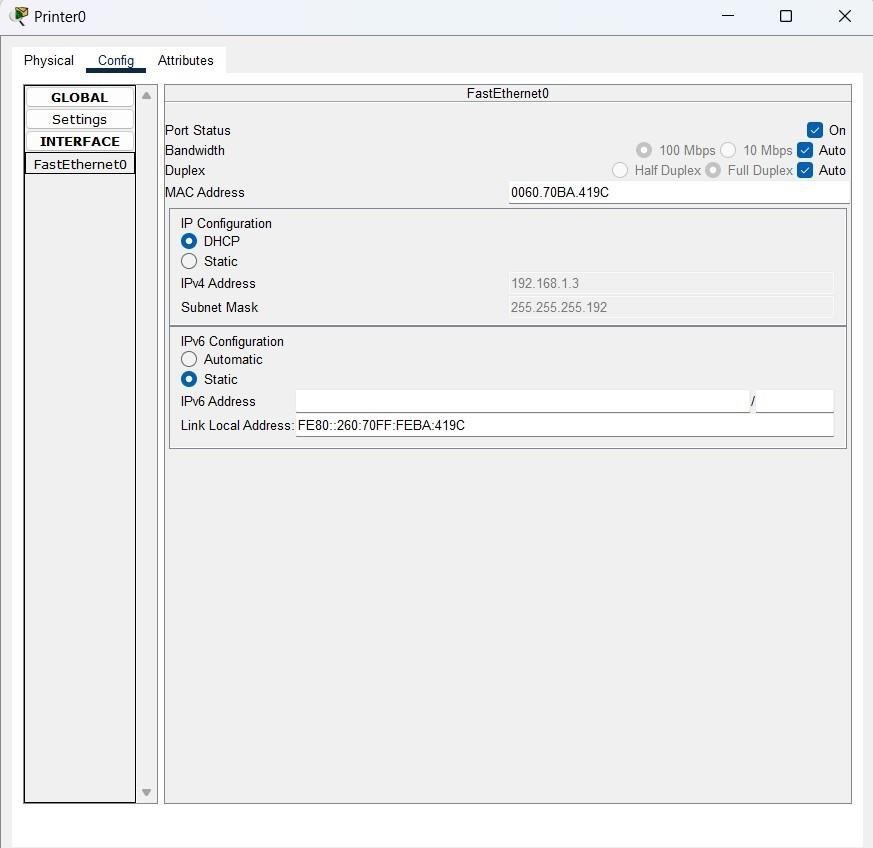
# DHCP (Dynamic Host Configuration Protocol):

Figure 3.1 shows the IP configuration settings for PC0, including a static IPv4 address, subnet mask, default gateway, and DNS server. IPv6 is also set to static, with a link-local address specified.



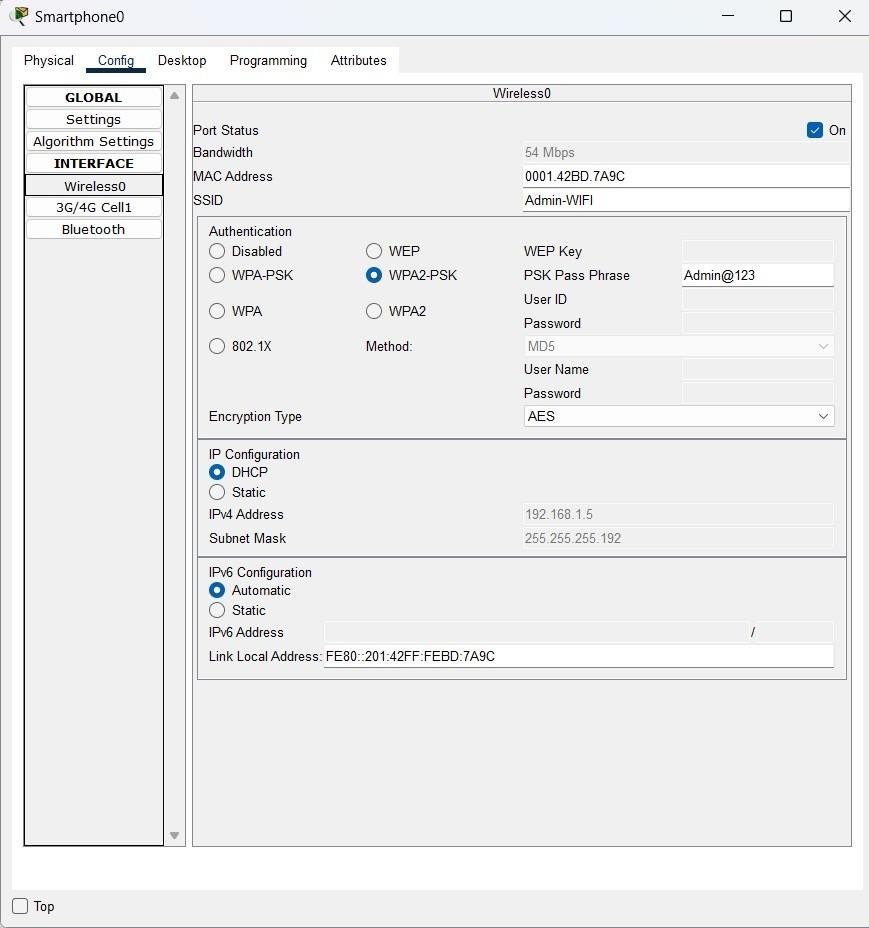
*Figure 6.1- pc0desktop*

Figure 6.2 shows the configuration settings for a network printer interface in Cisco Packet Tracer. It displays the IP and MAC address details, as well as settings for IPv4, IPv6, and duplex mode.



*Figure 6.2- printer config*

Figure 6.3 displays the wireless configuration settings for a smartphone interface in Cisco Packet Tracer. It includes network details like SSID, authentication type, encryption, and IP settings using DHCP.



*Figure 6.3- smartphone*

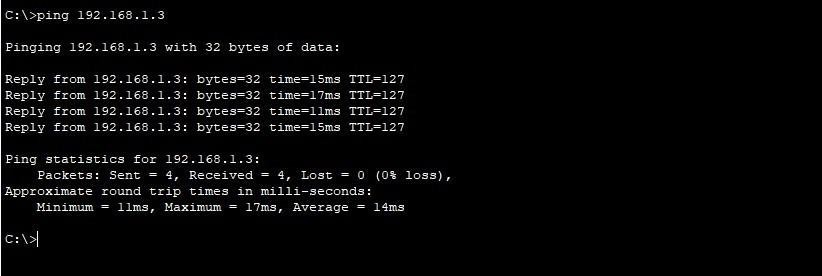
# CHAPTER 7

# Results and Evaluation

* 1. **Performance Metrics**

Performance metrics, including network latency, throughput, redundancy testing, DHCP response time, inter-VLAN routing performance were measured during testing to ensure optimal network operation.

Figure 7.1 shows the results of a ping test to the IP address 192.168.1.3. It indicates successful connectivity, with all packets received and no packet loss, showing response times between 11ms and 17ms.



*Figure 7.1- ping command*

**CHAPTER 8**

# Conclusion

* 1. **Summary**

In summary, the network design and implementation for the company’s network have been successfully executed. Key accomplishments include a well-structured network that meets the organization’s requirements for departmental segmentation, wireless connectivity, secure IP addressing through DHCP, and VLAN-based isolation for different departments. The setup allows for seamless inter-VLAN communication, robust security through WPA2-PSK for wireless networks, and automatic IP distribution to host devices. Testing in Cisco Packet Tracer confirmed the functionality of each configuration, ensuring the network meets project specifications. The resulting network is secure, efficient, and scalable, aligned with the needs of the company’s operations.

# Lessons Learned

Throughout the project, several valuable lessons were learned:

* + - **Importance of VLANs**: Effective VLAN segmentation simplifies network management, enhancessecurity, and aligns with departmental organization.
    - **Wireless Security**: Implementing WPA2-PSK with strong passphrases for each department’sSSID is essential for securing wireless communication.
    - **DHCP Efficiency**: Configuring DHCP pools for each VLAN streamlined IP address managementand reduced manual configuration.
    - **Testing is Essential**: Testing all configurations using Cisco Packet Tracer is crucial for identifying potential issues and ensuring reliability before deployment.
    - **Scalability for Future Growth**: Designing the network with scalability in mind ensures that futureexpansion can be handled smoothly without extensive redesign.

**CHAPTER 9**

# References

1. Cisco Networking Academy, *Routing and Switching Essentials v6 Companion Guide*, Cisco Press,2016.
2. Cisco Systems, *Cisco Packet Tracer User Guide*, Cisco Press, 2020.
3. IEEE Standards Association, *IEEE Standards for Local and Metropolitan Area Networks*, IEEE,2018.

**CHAPTER 10**

# Appendices

Abbreviations:

* DHCP - Dynamic Host Configuration Protocol
* IP - Internet Protocol
* SSID - Service Set Identifier
* VLAN - Virtual Local Area Network
* WPA2-PSK - Wi-Fi Protected Access 2 - Pre-S

**CHAPTER 11**

**COURSE COMPLETION CERTIFICATES:**

****

**RA2211028010227**

**RA2211028010224**

****

**RA2211028010229**

