Protecting Transactions in a Coffee Shop with Free Wi-Fi

In Partial Fulfilment of the Requirements in IT11/L

Submitted by:

Navallo, Christian Kerby N.

Toylo, Vincent Ray

Submitted to:

Lloyd Ryan Largo

Abstract

In today’s service-oriented businesses such as cafés and coffee shops, networking plays a critical role in daily operations. A coffee shop relies heavily on its network to process customer payments through POS terminals, manage administrative tasks in the manager’s office, support staff connectivity, and provide free Wi-Fi access for guests. A reliable and secure network infrastructure is essential to ensure smooth business operations, protect sensitive financial data, and maintain customer trust while delivering convenient internet access.

The primary networking issues identified in this scenario include the use of a flat network where all devices share the same broadcast domain, the absence of inter-VLAN routing for controlled communication, and weak wireless security configurations. POS terminals handling sensitive payment data are exposed to the same network as guest devices, increasing the risk of data interception and unauthorized access. Additionally, the Manager’s Office cannot securely access sales data due to the lack of proper routing between network segments.

To address these challenges, a redesigned network architecture was proposed using Virtual Local Area Networks (VLANs) to logically separate POS, Management, Staff, and Guest networks. Inter-VLAN routing was implemented using a router-on-a-stick configuration to allow controlled communication where necessary, particularly between the POS and Management VLANs. Secure wireless configurations were also applied by assigning separate SSIDs for Staff and Guest Wi-Fi and enabling strong encryption to prevent unauthorized access.

This design was motivated by the need to enhance security, improve network performance, and ensure compliance with best practices in network segmentation. By isolating sensitive systems from public access and enforcing controlled routing, the coffee shop benefits from reduced security risks, improved reliability, and better manageability of its network infrastructure while still offering free Wi-Fi services to customers.

Table of Contents

Problem Statement

Problem Statement 1 – Lack of VLAN Segmentation

The coffee shop currently operates on a flat network where POS terminals, manager PCs, staff devices, and guest Wi-Fi users are connected to the same network. This lack of segmentation exposes sensitive financial transactions to unnecessary security risks and increases broadcast traffic, negatively affecting network performance.

Problem Statement 2 – No Inter-VLAN Routing

The absence of inter-VLAN routing prevents secure and controlled communication between departments. Specifically, the Manager’s Office cannot access POS sales data because there is no routing mechanism to allow traffic between separate network segments.

Problem Statement 3 – Insecure Wireless Configuration

The wireless routers are configured with default SSIDs and weak passwords. This makes the network vulnerable to unauthorized access, allowing attackers or unintended users to connect easily and potentially intercept sensitive data.

Goal and Objectives

Overall Goal

To design and implement a secure and efficient network infrastructure for a coffee shop using Cisco Packet Tracer by applying VLAN segmentation, inter-VLAN routing, and secure wireless configurations.

Specific Objective 1

To implement VLAN segmentation that separates POS terminals, Management computers, Staff Wi-Fi devices, and Guest Wi-Fi devices into distinct broadcast domains, reducing security risks and improving network performance.

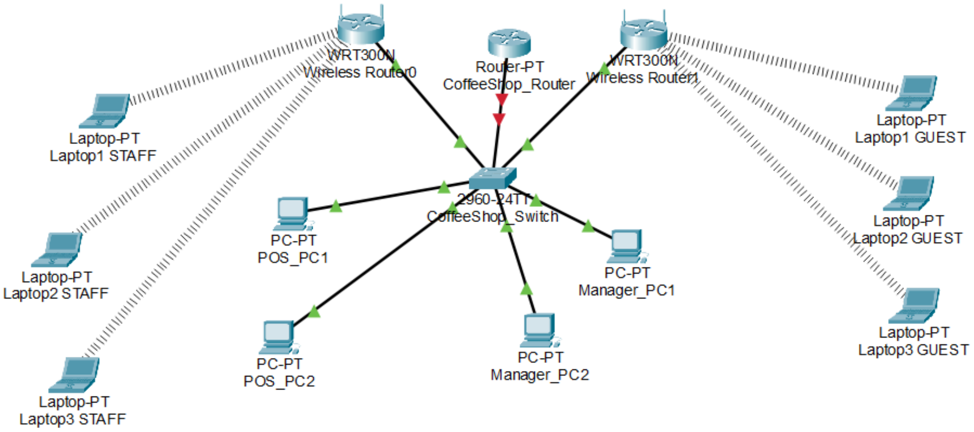
Specific Objective 2

To enable inter-VLAN routing that allows controlled communication between selected VLANs, particularly enabling the Manager’s Office to securely access POS transaction data.

Specific Objective 3

To configure secure wireless networks by creating separate SSIDs for Staff and Guest users and applying strong encryption and passwords to prevent unauthorized access.

Network Design/Topology



Devices Used

- 1 Router with inter-VLAN routing capability
- 2 Wireless Routers (Staff Wi-Fi and Guest Wi-Fi)
- 1 Cisco 2960 Switch
- 2 POS PCs
- 2 Manager Office PCs
- 3 Staff Laptops
- Multiple Guest Laptops

VLAN Assignments

VLAN ID	**VLAN Name**	**Purpose**
10	POS	Payment processing terminals
20	MANAGEMENT	Manager’s office computers
30	STAFF	Employee wireless devices

VLAN ID	VLAN Name	Purpose
40	GUEST	Customer Wi-Fi access

Configuration & Testing

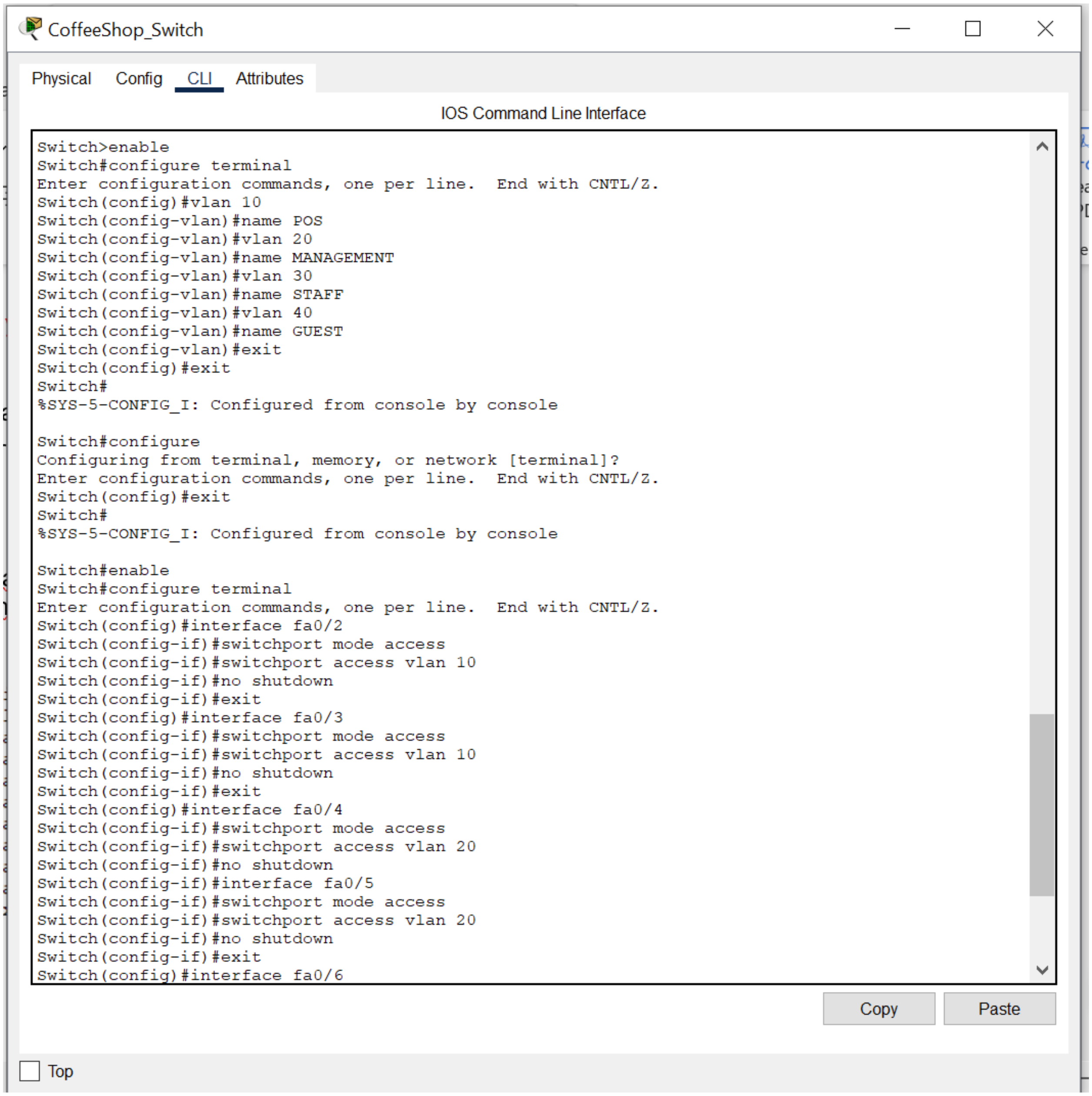
Provide details of your configuration and test results in the following structured format:

Example:

1. VLAN Configuration

Insert the configuration commands and screenshots for creating VLANs on the switch.
Example:

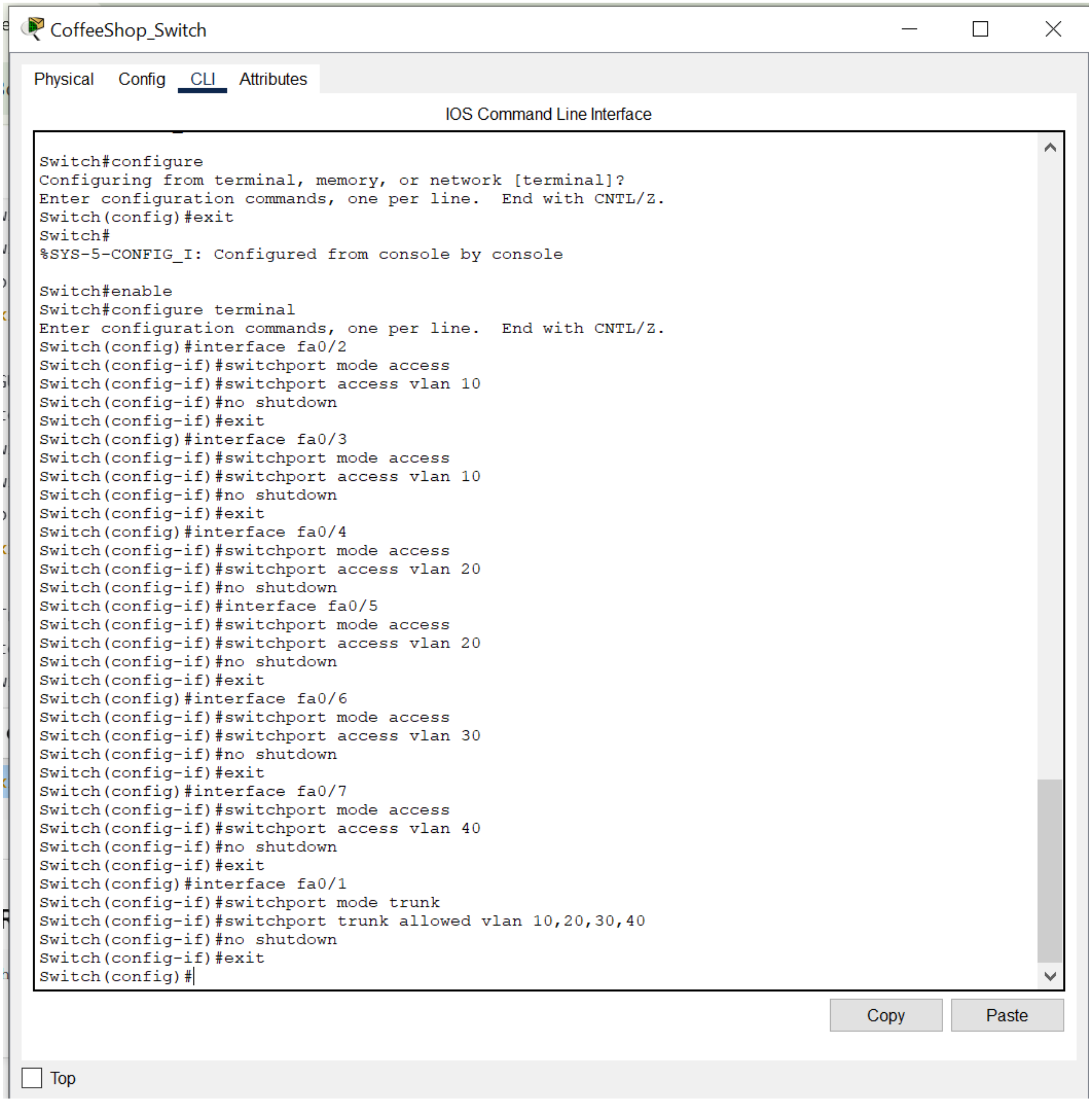
```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name Faculty
```



```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name POS
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name MANAGEMENT
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name STAFF
Switch(config-vlan)#vlan 40
Switch(config-vlan)#name GUEST
Switch(config-vlan)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#interface fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#interface fa0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#no shutdown
Switch(config-if)#interface fa0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#interface fa0/6
```



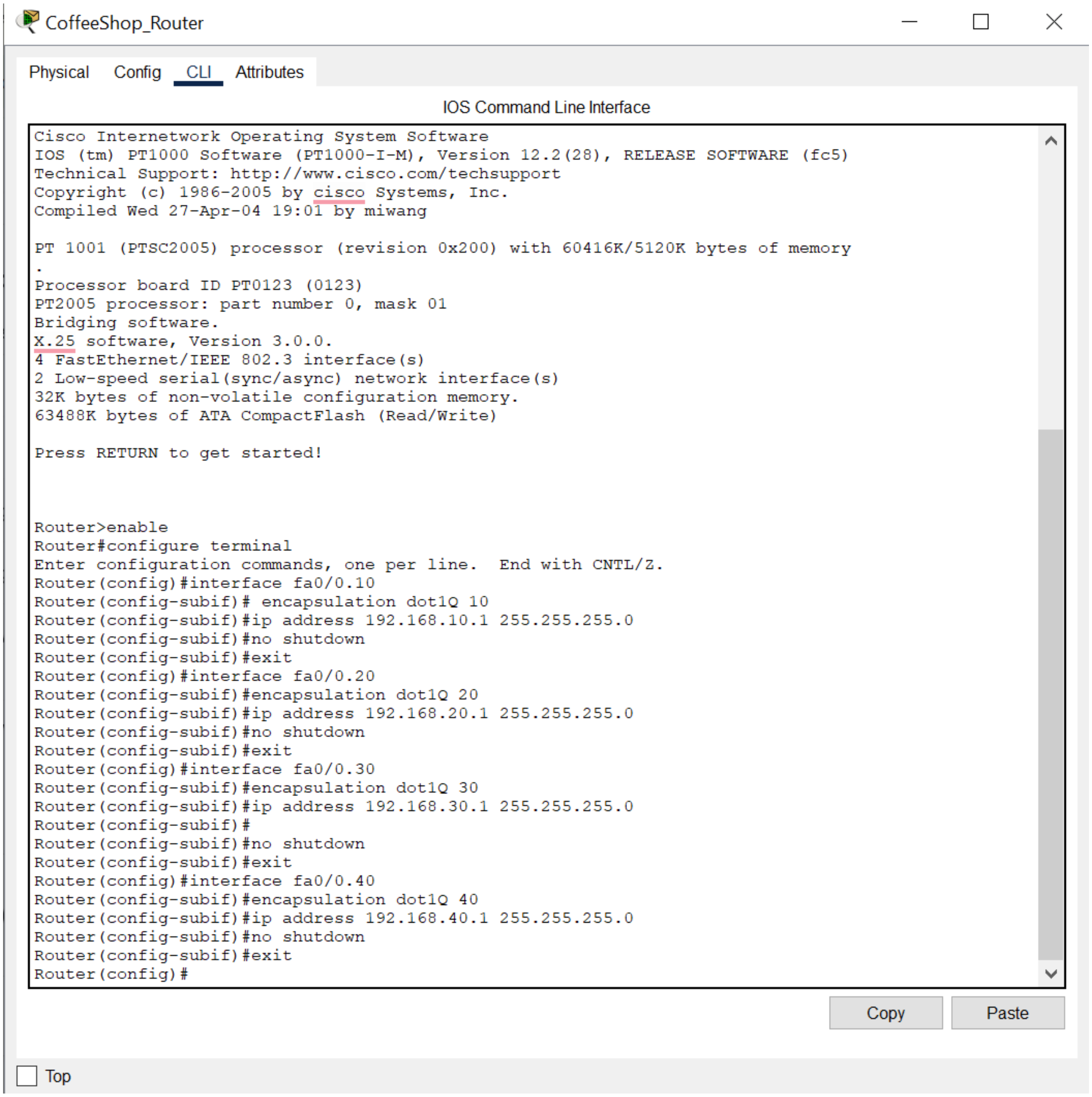
```
Switch#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#interface fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#interface fa0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#no shutdown
Switch(config-if)#interface fa0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#interface fa0/6
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#interface fa0/7
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 40
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10,20,30,40
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#
```

2. Router Configuration (Inter-VLAN + Wireless)

Insert the configuration commands for enabling inter-VLAN routing and setting up wireless. Example:

```
Router> enable
Router# configure terminal
Router(config)# interface g0/0.10
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.0
```



```
Cisco Internetwork Operating System Software
IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory
.
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

Press RETURN to get started!



Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fa0/0.10
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#interface fa0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#interface fa0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#interface fa0/0.40
Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip address 192.168.40.1 255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#
```

3. IP Addressing Scheme

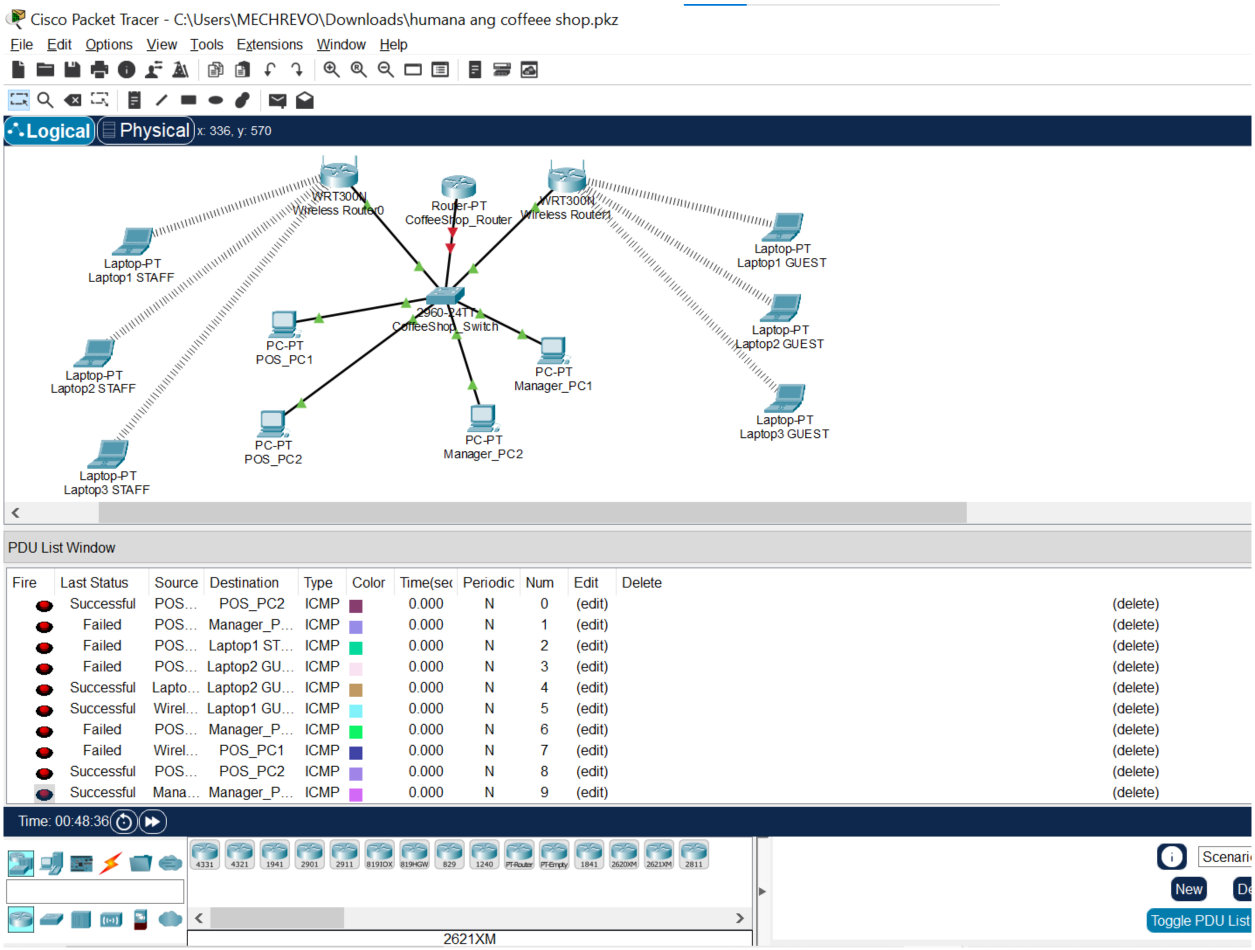
Fill in the table below to show your complete IP addressing plan:

Department / VLAN	Network Address	Subnet Mask	Default Gateway
POS(VLAN 10)	192.168.10.0/24	255.255.255.0	192.168.10.1
MANAGEMENT (VLAN 20)	192.168.20.0/24	255.255.255.0	192.168.20.1
STAFF(VLAN 30)	192.168.30.0/24	255.255.255.0	192.168.30.1
GUEST(VLAN40)	192.168.30.0/24	255.255.255.0	192.168.40.1

4. Connectivity Test Results

Provide proof of successful connectivity:

- Ping tests between VLANs (screenshots)
- Verification that access restrictions are working as intended



Fire	Last Status	Source	Destination	Type	Color	Time(sec	Periodic	Num	Edit	Delete
●	Successful	POS…	POS_PC2	ICMP	🟪	0.000	N	0	(edit)	(delete)
●	Failed	POS…	Manager_P…	ICMP	🟪	0.000	N	1	(edit)	(delete)
●	Failed	POS…	Laptop1 ST…	ICMP	🟩	0.000	N	2	(edit)	(delete)
●	Failed	POS…	Laptop2 GU…	ICMP	⬜	0.000	N	3	(edit)	(delete)
●	Successful	Lapto…	Laptop2 GU…	ICMP	🟫	0.000	N	4	(edit)	(delete)
●	Successful	Wirel…	Laptop1 GU…	ICMP	🟦	0.000	N	5	(edit)	(delete)
●	Failed	POS…	Manager_P…	ICMP	🟩	0.000	N	6	(edit)	(delete)
●	Failed	Wirel…	POS_PC1	ICMP	🟦	0.000	N	7	(edit)	(delete)
●	Successful	POS…	POS_PC2	ICMP	🟪	0.000	N	8	(edit)	(delete)
●	Successful	Mana…	Manager_P…	ICMP	🟪	0.000	N	9	(edit)	(delete)

References

Cisco Networking Academy. (2021). *Introduction to networks companion guide*. Cisco Press.

Cisco. (2024, March 15). *How to configure a wireless router in Packet Tracer*. Cisco Networking Academy. https://www.netacad.com/resources/labs