Project Report
On
Computer Networking: Concepts (CSE3751)

Scalable Hotel Management Network Design

Submitted by:

BHABASHIS MISHRA

B. Tech. CSIT 5th Semester

INSTITUTE OF TECHNICAL EDUCATION AND RESEARCH
(FACULTY OF ENGINEERING)
SIKSHA 'O' ANUSANDHAN (DEEMED TO BE UNIVERSITY), BHUBANESWAR, ODISHA

Declaration

We, the undersigned students of B. Tech. of Computer Science and Information Technology Department hereby declare that we own the full responsibility for the information, results etc. provided in this PROJECT titled "**Scalable Hotel Management Network Design**" submitted to **Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar** for the partial fulfillment of the subject **Computer Networking: Concepts (CSE 3751)**. We have taken care in all respect to honor the intellectual property right and have acknowledged the contribution of others for using them in academic purpose and further declare that in case of any violation of intellectual property right or copyright we, as the candidate(s), will be fully responsible for the same.

BHABASHIS MISHRA.

Date:

Place:

Abstract

This project focuses on designing a **secure, scalable, and efficient hotel network** using Cisco Packet Tracer. The network segments departments—Reception, Finance, Restaurant, Sales, and Guest Wi-Fi—using **VLANs** to ensure data isolation and secure communication. **Access Control Lists (ACLs)** control inter-departmental access, allowing only authorized communication, such as between Reception and Finance for billing. A **centralized server** hosts shared resources, and a dedicated **Guest VLAN** ensures internet-only access for guests while isolating internal networks.

Key features include **Inter-VLAN Routing**, **DHCP** for automated IP assignment, and **STP** for redundancy. The design is tested for secure communication, guest isolation, and scalability, ensuring reliable hotel operations and readiness for future expansion. This solution provides a robust IT infrastructure tailored to the modern hospitality industry's needs.

Contents

1. Introduction

In today's hospitality industry, technology plays a crucial role in streamlining operations and enhancing guest experiences. Hotels rely heavily on robust IT infrastructures to manage departmental communication, secure sensitive data, and provide seamless services to guests. However, designing a network that meets these demands while maintaining scalability and security poses significant challenges.

This project focuses on creating a **Scalable Hotel Management Network** that ensures efficient communication, secure data handling, and operational reliability across various hotel departments—Reception, Finance, Restaurant, and Sales. Using **Cisco Packet Tracer**, the network is designed to isolate departmental traffic using **VLANs**, enable controlled communication via **Inter-VLAN Routing**, and enforce security policies through **Access Control Lists (ACLs)**. Additionally, a **Guest VLAN** provides internet-only access, safeguarding internal systems from unauthorized access.

The network also incorporates redundancy through **Spanning Tree Protocol (STP)** to maintain service availability during hardware failures. Designed with scalability in mind, the infrastructure supports future growth, such as adding new departments or expanding to additional branches. This project aims to deliver a secure, scalable, and efficient network that meets the hotel's current and future operational needs.

2. Problem Statement

The hotel requires a secure and scalable network to support its daily operations while isolating sensitive data and ensuring controlled communication between departments. Each department has specific operational and security requirements:

1. **Reception (VLAN 10)**:
    - Handles guest check-ins, reservations, and billing.
    - Needs direct communication with the Finance department for billing but must remain isolated from other departments.
2. **Finance (VLAN 20)**:
    - Manages sensitive financial data such as payroll, invoices, and transactions.
    - Must be isolated from all departments except Reception to maintain data security.
3. **Restaurant (VLAN 30)**:
    - Manages food orders, inventory, and room service.
    - Occasionally collaborates with the Sales department for promotions but operates independently otherwise.
4. **Sales (VLAN 40)**:
    - Focuses on marketing, online bookings, and promotions.
    - Needs access to Restaurant data but must remain isolated from Finance.
5. **Centralized Server (VLAN 50)**:
    - Hosts shared resources like promotional materials, sales reports, and customer feedback.
    - Access is strictly controlled to prevent unauthorized use.
6. **Guest Wi-Fi (VLAN 60)**:
    - Provides internet-only access for hotel guests.
    - Must be isolated from all internal hotel networks to ensure data security.

Requirements

- **Secure departmental communication** via VLANs and inter-VLAN routing.
- **Access Control Lists (ACLs)** to restrict inter-departmental access.
- **Guest network isolation** to prevent unauthorized access to internal resources.
- **Centralized resource sharing** using a dedicated server VLAN.
- **Redundancy** for high availability and uninterrupted operations.
- **Scalability** to support future expansions, such as adding new departments or branches.

Objects to Be Considered for Implementation in Cisco Packet Tracer

1. **Router**:
    - Perform inter-VLAN routing using sub-interfaces.
    - Implement ACLs for securing sensitive data and controlling inter-departmental communication.

2. **Switches**:
    - **Switch 1**: Supports VLANs 10 (Reception) and 20 (Finance).
    - **Switch 2**: Supports VLANs 30 (Restaurant) and 40 (Sales).
    - **Switch 3**: Dedicated to VLAN 50 (Server).
    - **Switch 4**: Dedicated to VLAN 60 (Guest Wi-Fi).
    - Configure VLANs and trunk links for efficient data flow.
3. **VLANs**:
    - Create VLANs for each department to ensure logical segmentation and security.
4. **Access Control Lists (ACLs)**:
    - Define and apply ACLs to control and restrict communication between VLANs.
5. **DHCP Server**:
    - Configure DHCP for dynamic IP allocation within each VLAN to simplify management.
6. **Devices**:
    - PCs, servers, and access points for simulating real-world hotel operations.
    - Access Point for Guest Wi-Fi.
7. **Redundant Links and STP**:
    - Use Spanning Tree Protocol (STP) to prevent loops and ensure redundancy for critical links.

Constraints

1. **Security Constraints**:
    - Finance VLAN (20) must be accessible only by Reception VLAN (10); other departments must not access it.
    - Guest VLAN (60) must not have access to internal VLANs to protect sensitive data.
2. **Performance Constraints**:
    - The network must handle high data traffic during peak hours without compromising speed or reliability.
3. **Scalability Constraints**:
    - The network must allow seamless addition of new departments, devices, or branches without significant reconfiguration.
4. **Cost Constraints**:
    - The design must balance between meeting technical requirements and maintaining cost-efficiency for the hotel.

3. Methodology

This section provides a step-by-step methodology for implementing the **Scalable Hotel Management Network** using Cisco Packet Tracer. The methodology covers **designing the topology**, **configuring the devices**, and the corresponding **CLI instructions** to achieve the project objectives.

1. Designing the Topology

The network topology consists of a **single router** (Router H1) connected to **four switches**, each supporting specific VLANs:

1. **Router H1**:
    - Performs **inter-VLAN routing** using sub-interfaces.
    - Implements **Access Control Lists (ACLs)** for secure communication.
2. **Switches**:
    - **Switch 1**: VLAN 10 (Reception) and VLAN 20 (Finance).
    - **Switch 2**: VLAN 30 (Restaurant) and VLAN 40 (Sales).
    - **Switch 3**: VLAN 50 (Centralized Server).
    - **Switch 4**: VLAN 60 (Guest Wi-Fi).
3. **VLANs**:
    - VLAN 10: Reception (192.168.10.0/24)
    - VLAN 20: Finance (192.168.20.0/24)
    - VLAN 30: Restaurant (192.168.30.0/24)
    - VLAN 40: Sales (192.168.40.0/24)
    - VLAN 50: Server (192.168.50.0/24)
    - VLAN 60: Guest Wi-Fi (192.168.60.0/24)
4. **Connections**:
    - The router connects to each switch via trunk links.
    - Each VLAN has its assigned PCs/devices, which connect to their respective switches.

2. Configuring the Devices

Router Configuration (Router H1):

- Configure sub-interfaces for each VLAN to enable inter-VLAN communication.
- Apply ACLs to restrict access between sensitive VLANs.

Switch Configurations:

- Create and assign VLANs to ports.
- Configure trunk ports to facilitate VLAN traffic between switches and the router.

Server and Guest Wi-Fi:

- Assign the centralized server to VLAN 50.
- Configure VLAN 60 for isolated guest internet access using an access point.

3. CLI Instructions

Router H1 Configuration

```
enable
configure terminal

# Sub-interfaces for inter-VLAN routing
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0
exit

interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0
exit

interface GigabitEthernet0/0.30
encapsulation dot1Q 30
ip address 192.168.30.1 255.255.255.0
exit

interface GigabitEthernet0/0.40
encapsulation dot1Q 40
ip address 192.168.40.1 255.255.255.0
exit

interface GigabitEthernet0/0.50
encapsulation dot1Q 50
ip address 192.168.50.1 255.255.255.0
exit

interface GigabitEthernet0/0.60
encapsulation dot1Q 60
ip address 192.168.60.1 255.255.255.0
exit
```

```
# Create an ACL to block traffic from VLANs 10 and 20 to
VLANs 30 and 40
ip access-list extended BLOCK_10_20_TO_30_40
deny ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
deny ip 192.168.10.0 0.0.0.255 192.168.40.0 0.0.0.255
deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
deny ip 192.168.20.0 0.0.0.255 192.168.40.0 0.0.0.255
permit ip any any

# Apply the ACL to the respective sub-interfaces
interface GigabitEthernet0/0.10
ip access-group BLOCK_10_20_TO_30_40 out
exit

interface GigabitEthernet0/0.20
ip access-group BLOCK_10_20_TO_30_40 out
exit

write memory
```

Switch 1 Configuration

```
enable
configure terminal

# Create VLANs
vlan 10
name RECEPTION
exit

vlan 20
name FINANCE
exit

# Assign ports to VLANs
interface FastEthernet0/1
switchport mode access
switchport access vlan 10
exit

interface FastEthernet0/2
switchport mode access
switchport access vlan 20
```

```
exit

# Configure trunk port to router
interface GigabitEthernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
exit

write memory
```

Switch 2 Configuration

```
enable
configure terminal

# Create VLANs
vlan 30
name RESTAURANT
exit

vlan 40
name SALES
exit

# Assign ports to VLANs
interface FastEthernet0/1
switchport mode access
switchport access vlan 30
exit

interface FastEthernet0/2
switchport mode access
switchport access vlan 40
exit

# Configure trunk port to router
interface GigabitEthernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
exit

write memory
```

Switch 3 Configuration

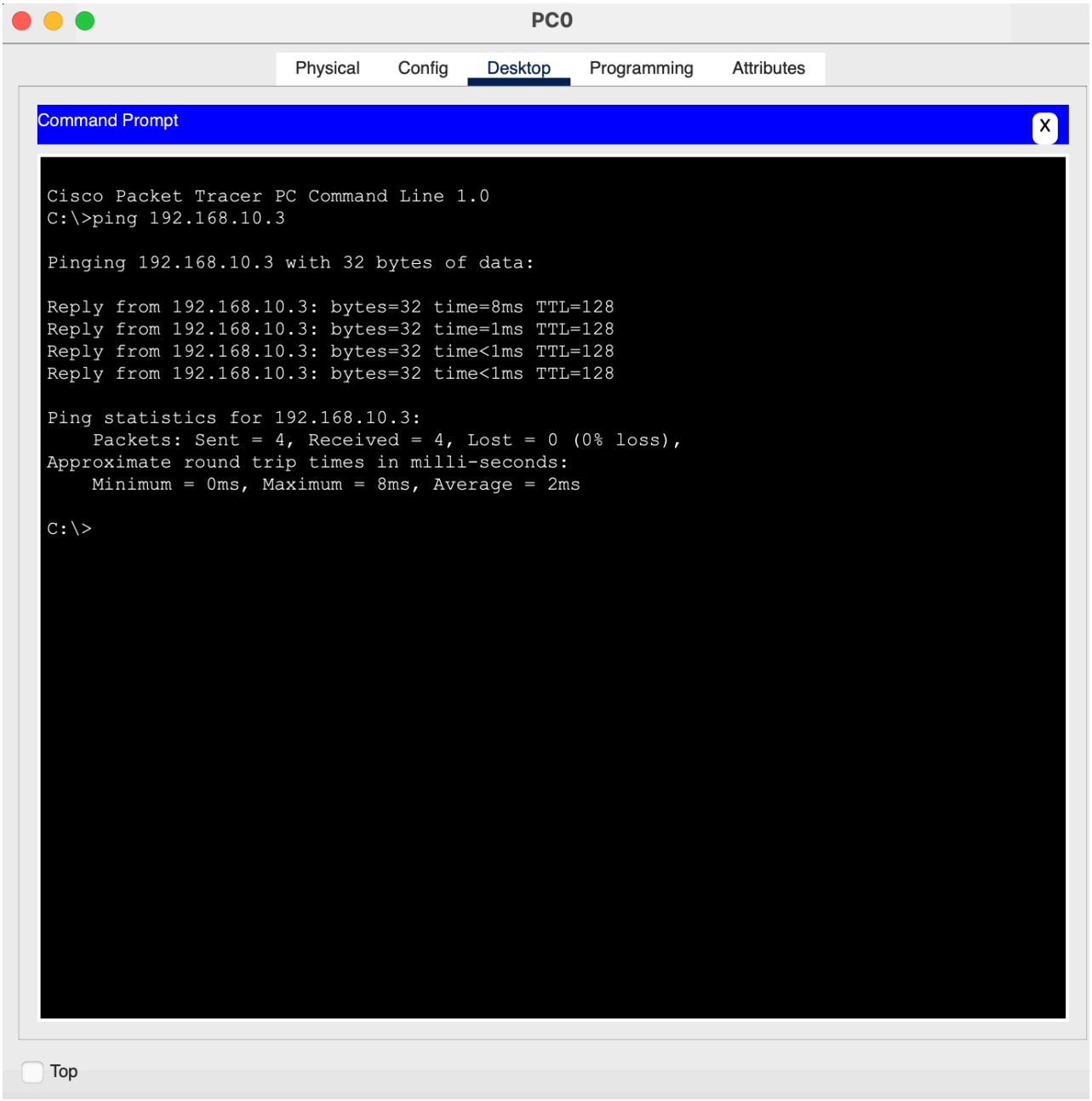
```
enable
configure terminal
# Create VLAN 50 for Server
vlan 50
name SERVER
exit

# Assign port to VLAN 50
interface FastEthernet0/1
switchport mode access
switchport access vlan 50
exit

# Configure trunk port to router
interface GigabitEthernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
exit
write memory
```

Switch 4 Configuration

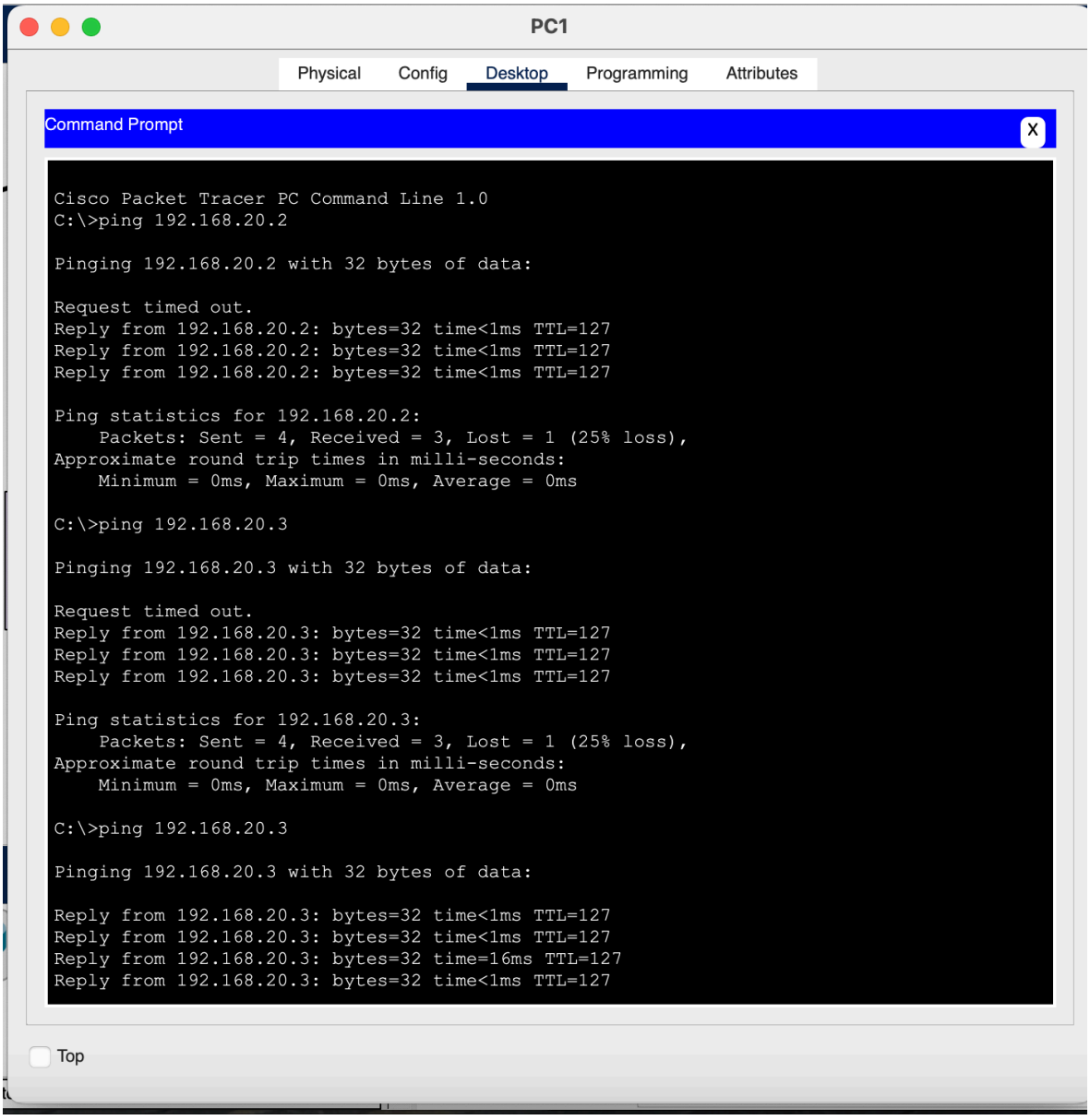
```
enable
configure terminal

# Create VLAN 60 for Guest Wi-Fi
vlan 60
name GUEST_WIFI
exit

# Assign port to VLAN 60
interface FastEthernet0/1
switchport mode access
switchport access vlan 60
exit

# Configure trunk port to router
interface GigabitEthernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
exit
```

4. Testing and Verification

1. **Ping Tests**:
    - Test communication between devices within the same VLAN

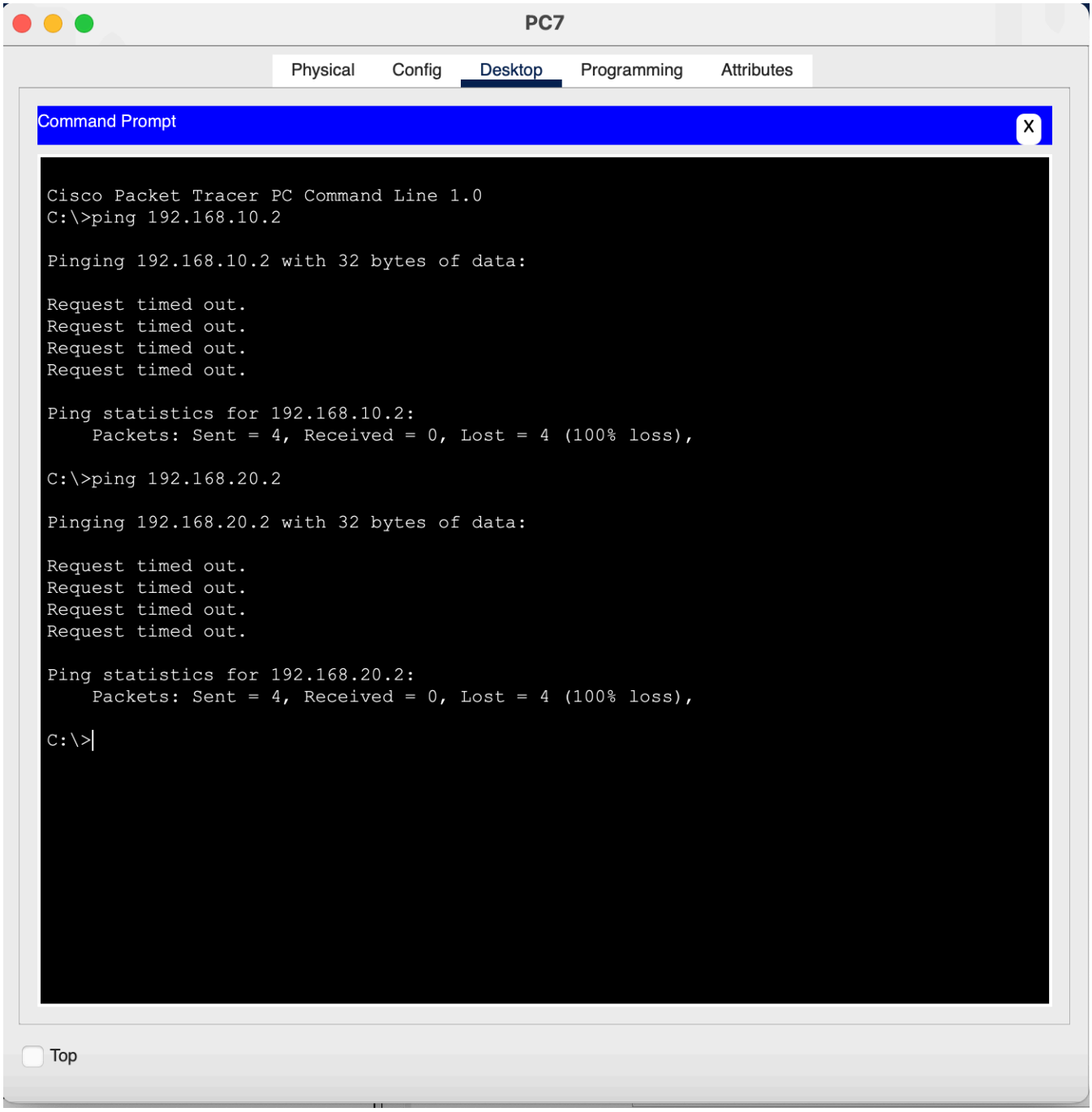


- Test inter-VLAN communication to ensure proper routing.



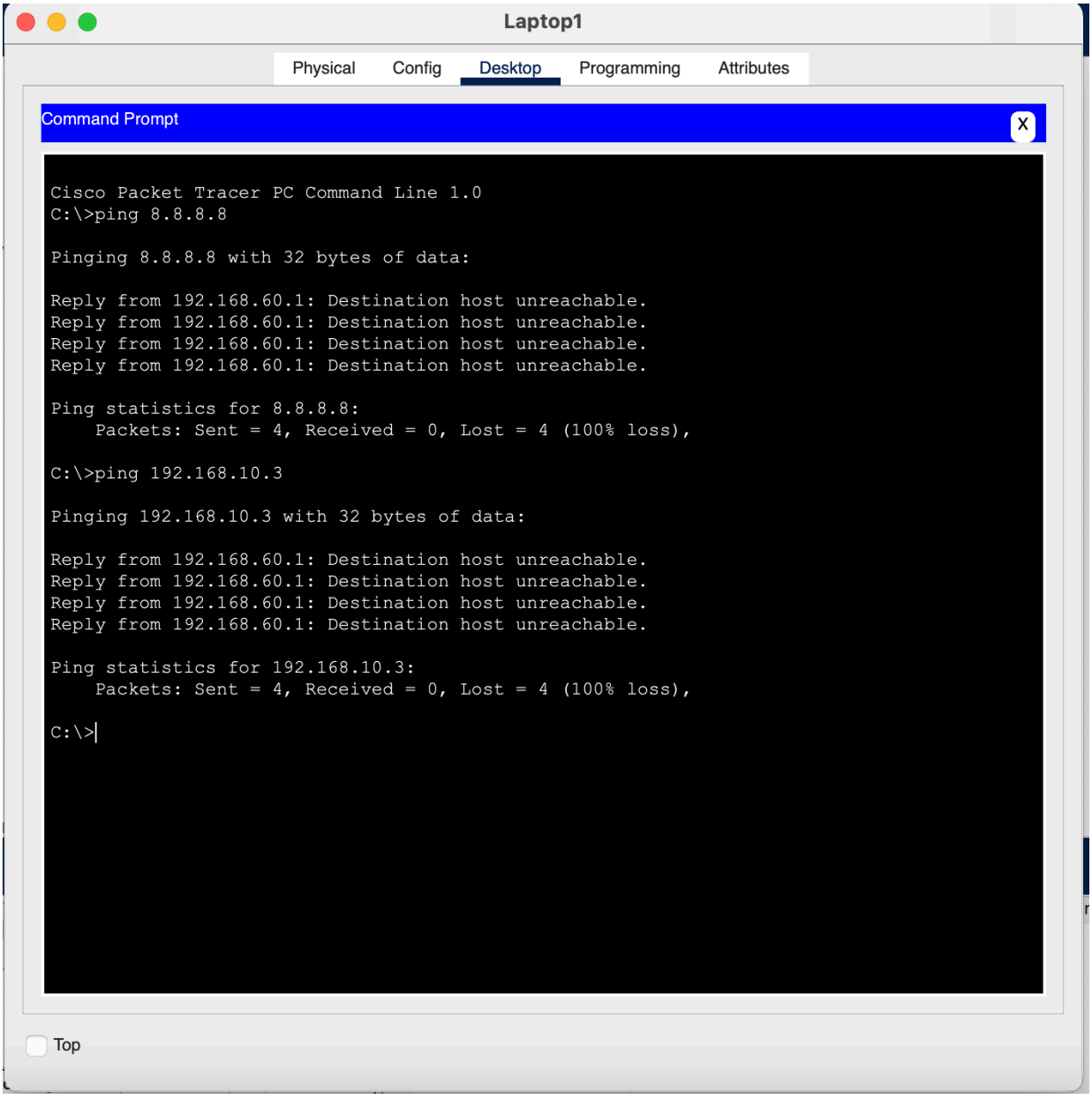
2. **ACL Verification**:

   - Confirm that unauthorized VLANs (e.g., Sales) cannot access Finance.



3. **Guest Network Isolation**:

   - Verify that the Guest VLAN cannot access internal VLANs but can access the internet.



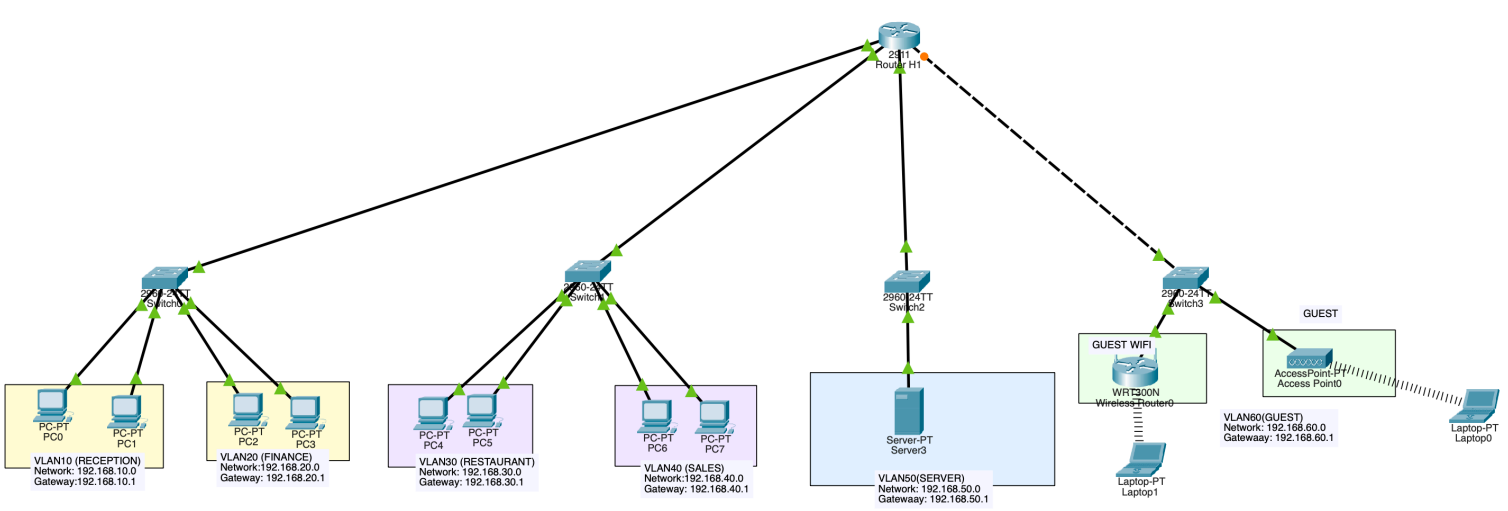
4. Results & Interpretation

Results & Interpretation

The following section provides screenshots and descriptions to demonstrate the successful implementation of the **Scalable Hotel Management Network Design**. The results include packet transmission, testing of inter-VLAN communication, and outputs of both **ping** and **traceroute** commands, along with CLI configurations.

1. Designed Network Topology

Screenshot of the Topology



This screenshot shows the completed network topology in **Cisco Packet Tracer**, including:

- **Router H1** connected to four switches (Switch 1, 2, 3, 4).
- VLAN assignments for each switch.
- End devices (PCs, servers, and access points) connected to their respective VLANs.

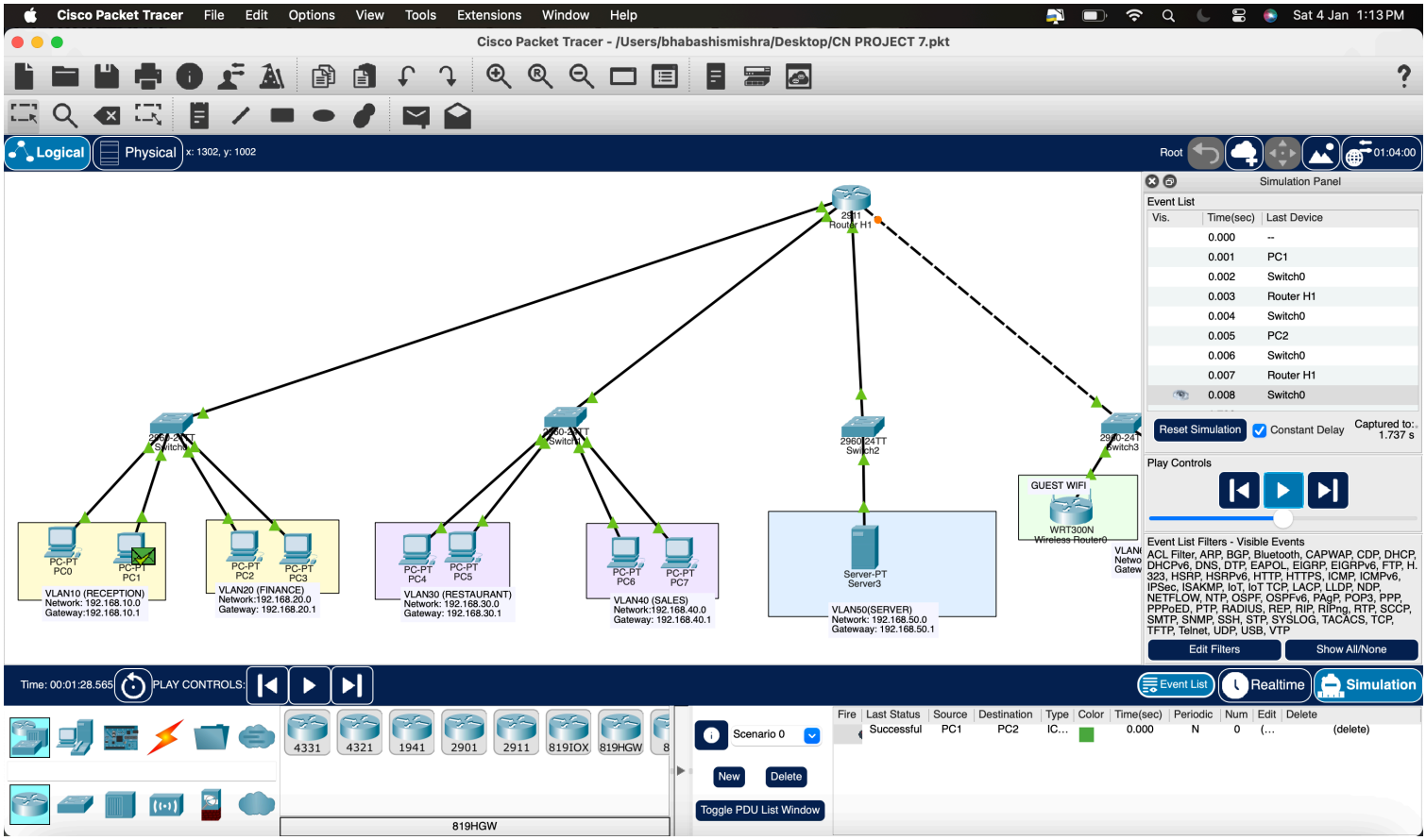
Description:
The topology reflects the logical separation of departments into VLANs and the physical connections between devices and switches.

2. Successful Transmission of Packets

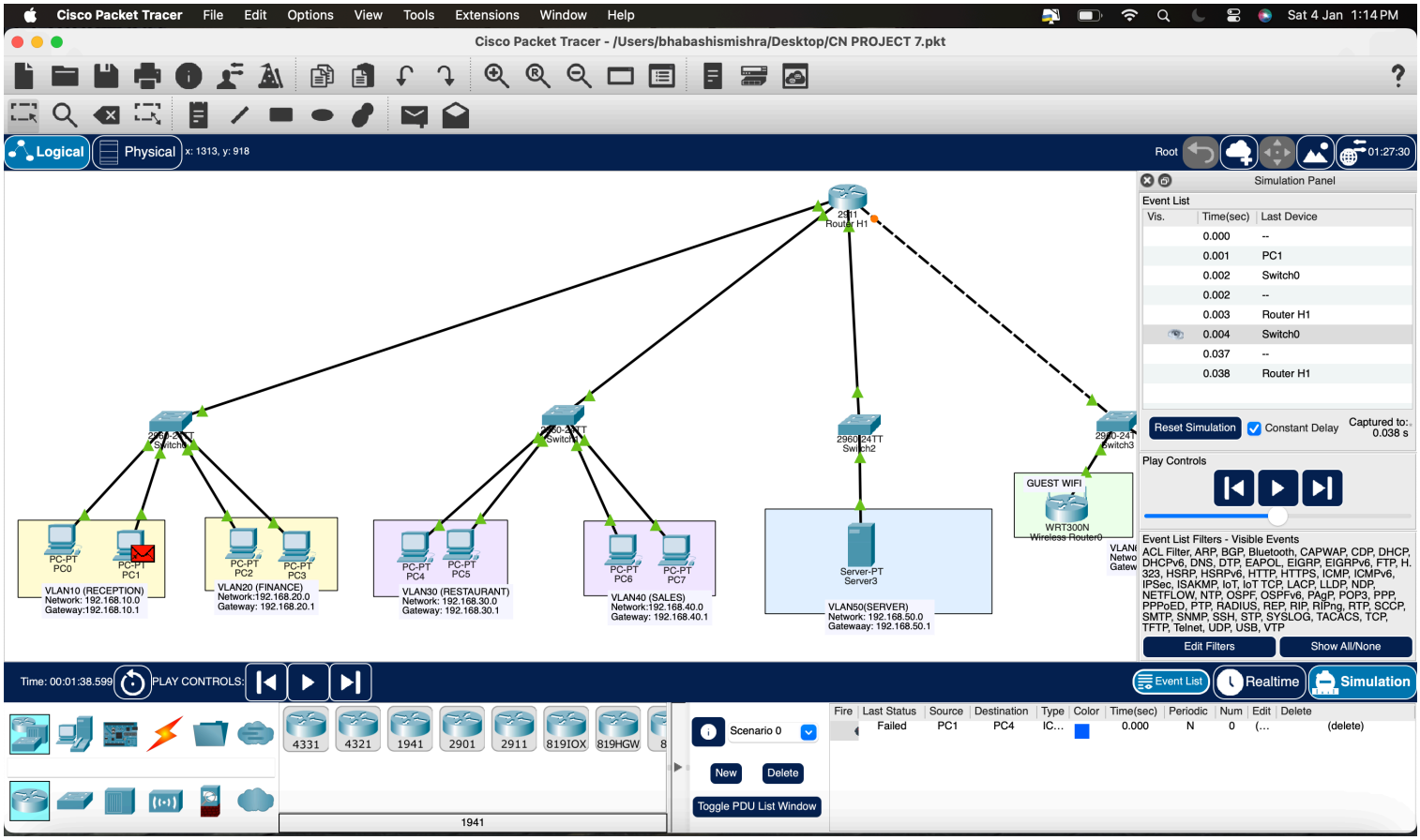
Screenshot of Packet Transmission

A screenshot of the **Packet Tracer Simulation Mode** with successful packet transmissions between:

- Devices within the same VLAN.



- Devices across different VLANs (using inter-VLAN routing).



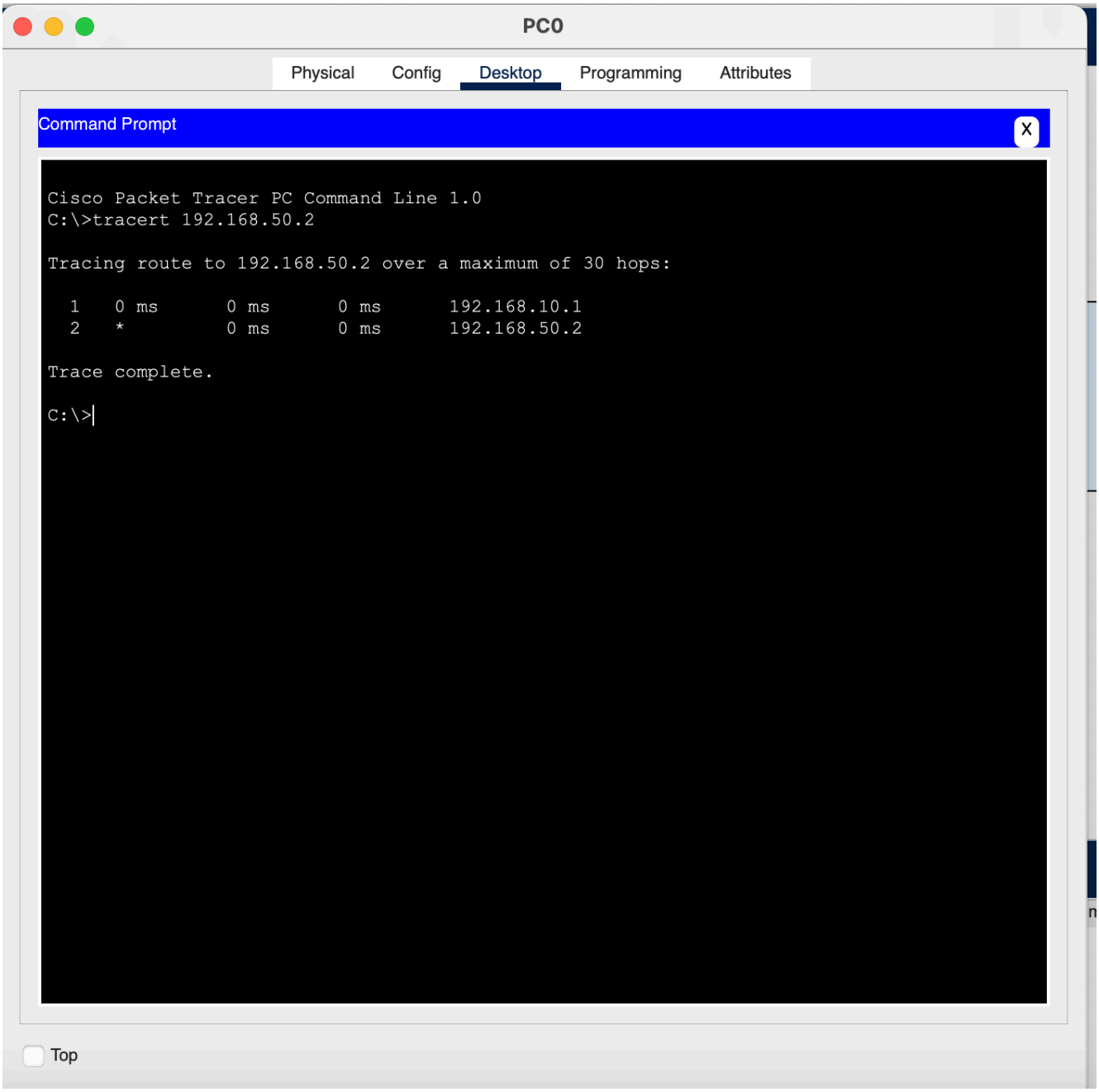
Description:
This confirms that packets are transmitted without loss or errors, and inter-VLAN communication is operational.

3. Successful Ping and Traceroute Commands

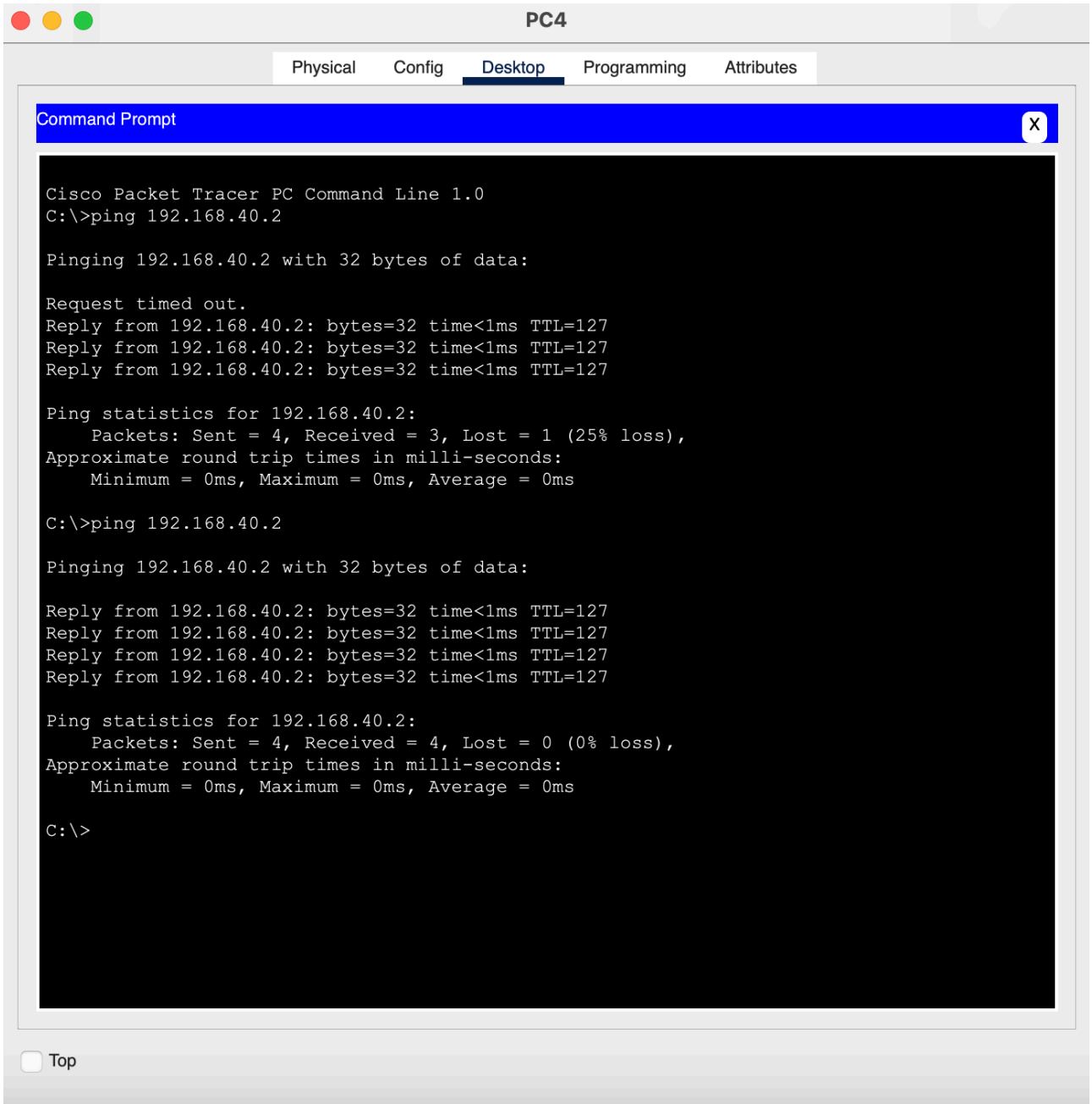
Ping Test:

A screenshot showing the **ping** command from:

- **PC in VLAN 10 (Reception)** to **PC in VLAN 20 (Finance)**
-



- **PC in VLAN 30 (Restaurant)** to **PC in VLAN 40 (Sales)**.

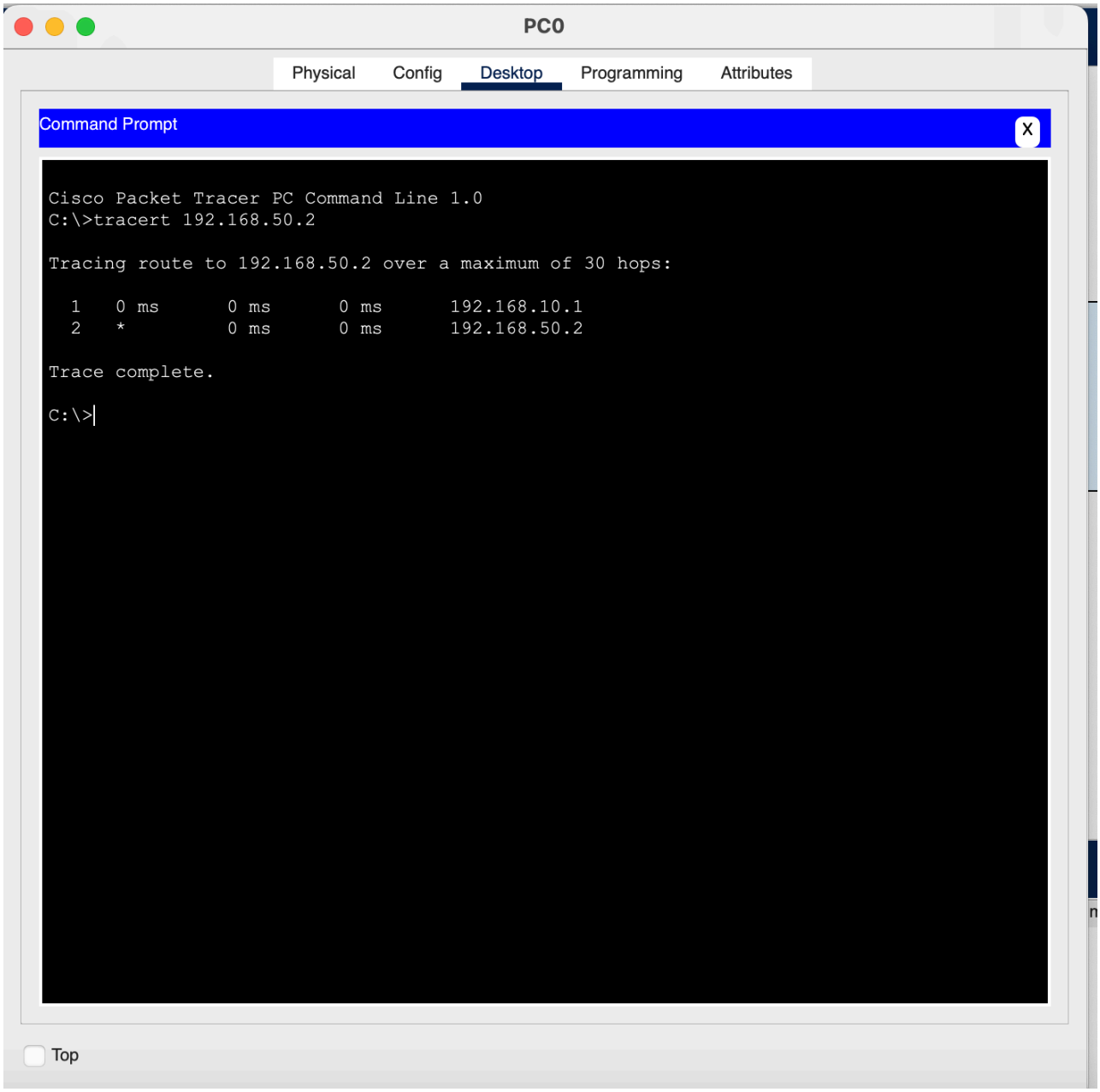


Description:
The ping results confirm successful communication between authorized VLANs, verifying that inter-VLAN routing is working as expected.

Traceroute Test:

A screenshot of the **traceroute** command from:

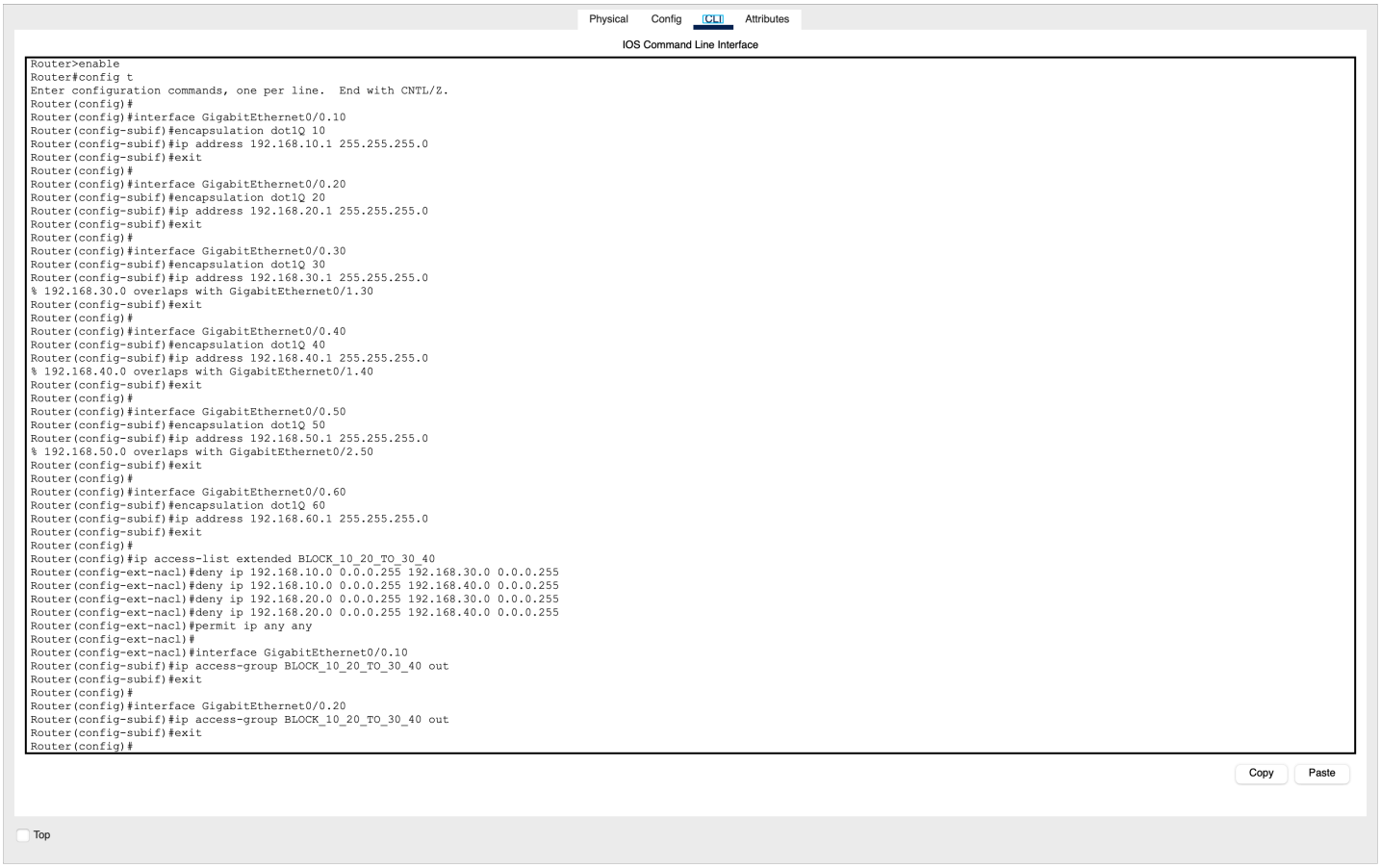
- **PC in VLAN 10 (Reception)** to **Centralized Server in VLAN 50**.



Description:
The traceroute results demonstrate the packet's path through the router, confirming proper routing and connectivity.

4. CLI Instructions and Results

Router H1 CLI Configuration:

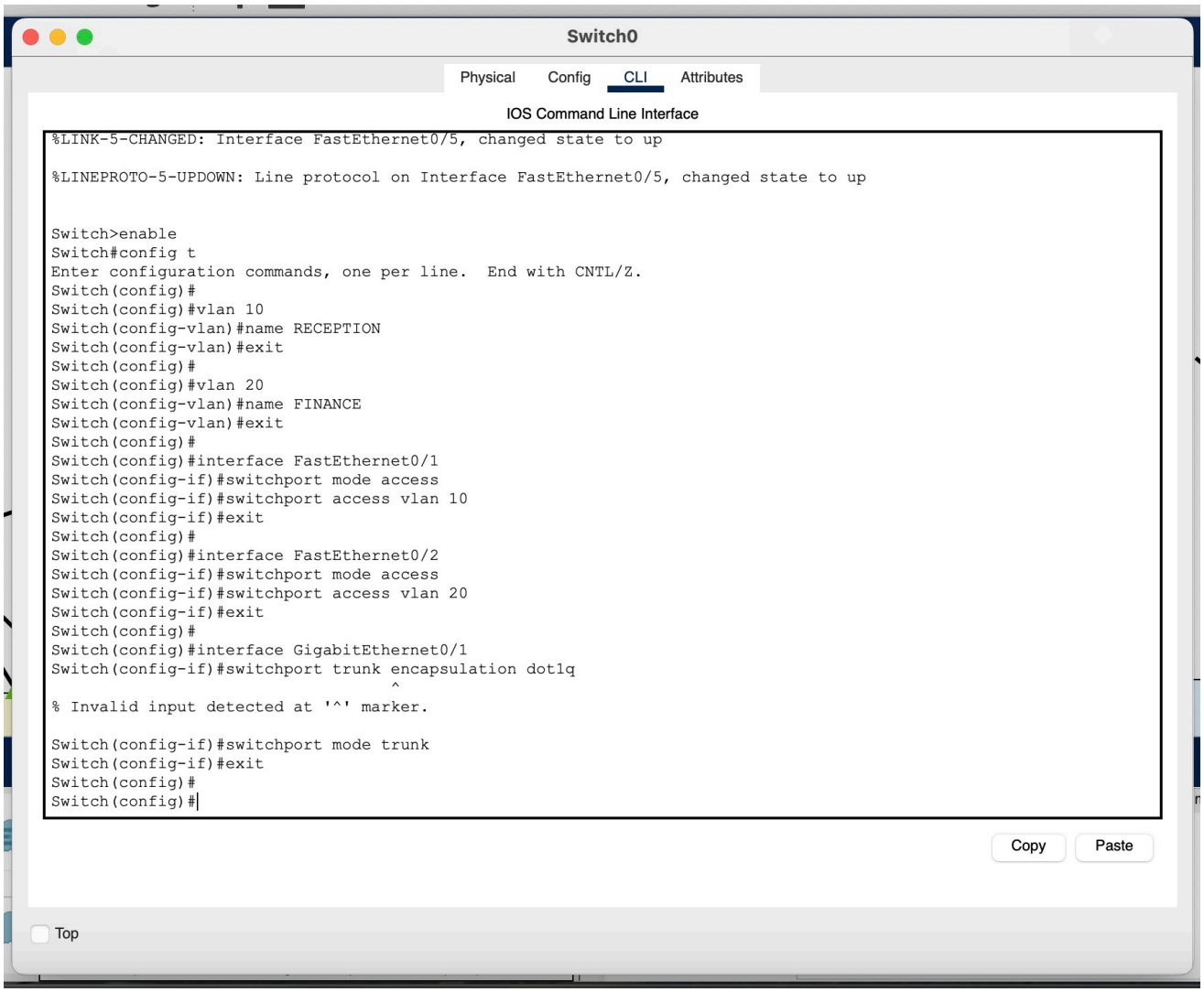


A screenshot of the CLI configuration for **Router H1**, including:

- Sub-interface configurations for VLANs.
- Application of ACLs to restrict access to the Finance VLAN.

Description:
The CLI output shows the successful configuration of sub-interfaces and ACLs, ensuring secure communication and data isolation.

Switch 0 CLI Configuration

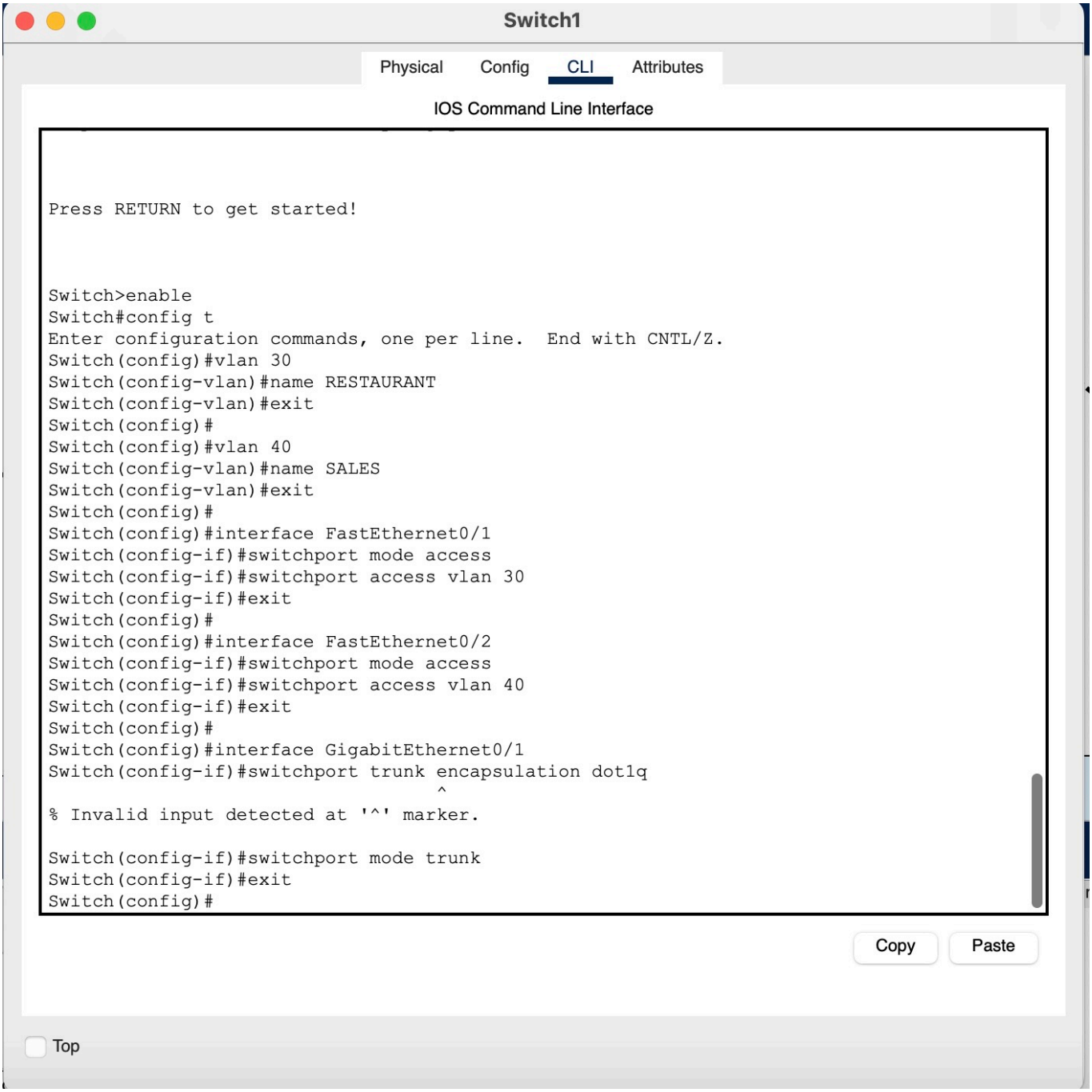


A screenshot of **Switch 1**'s CLI showing:

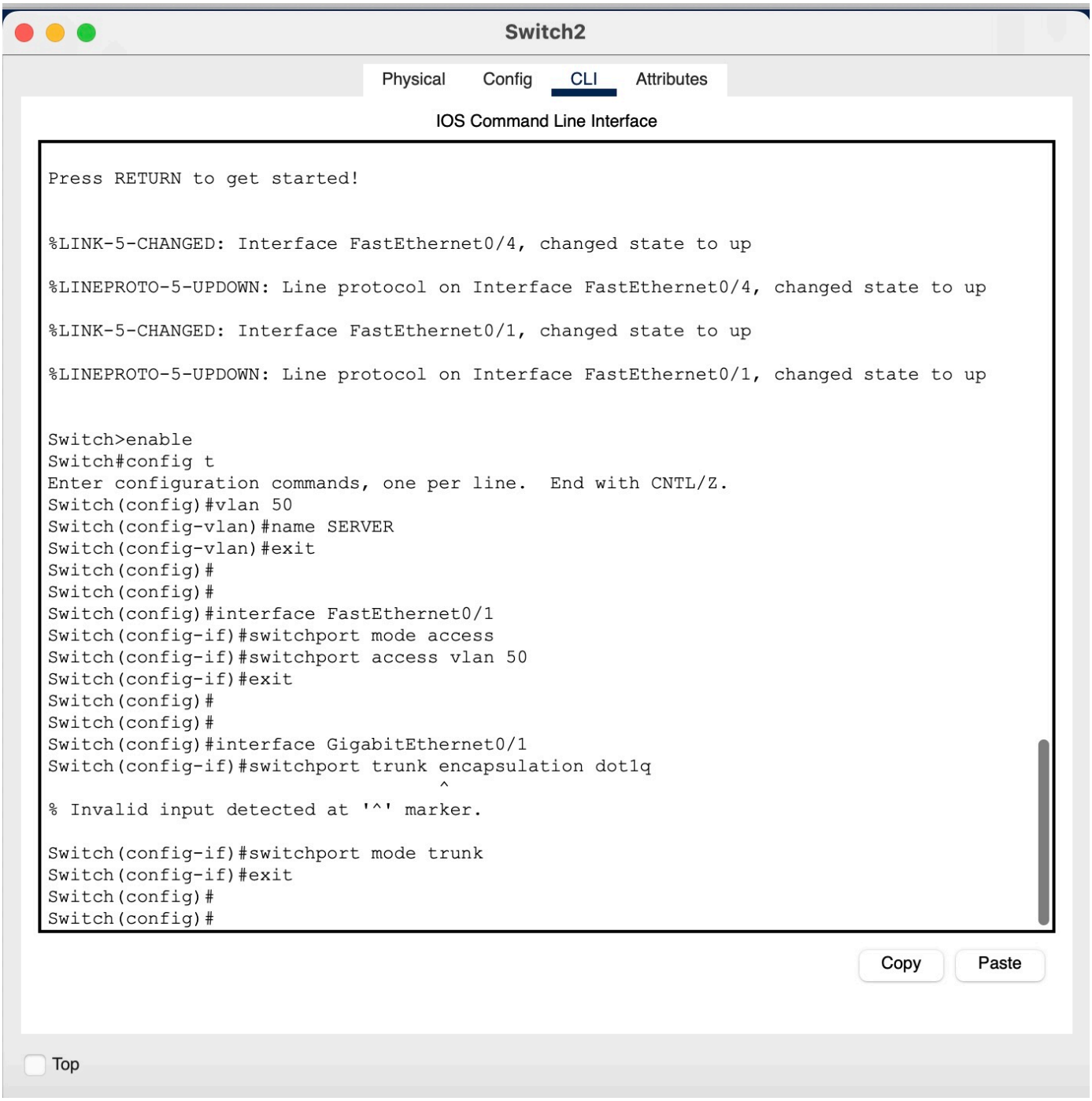
- Creation of VLANs 10 and 20.
- Assignment of ports to respective VLANs.
- Configuration of the trunk port.

Description:
The CLI output confirms that VLANs are properly configured, and the switch is ready for communication with other devices.

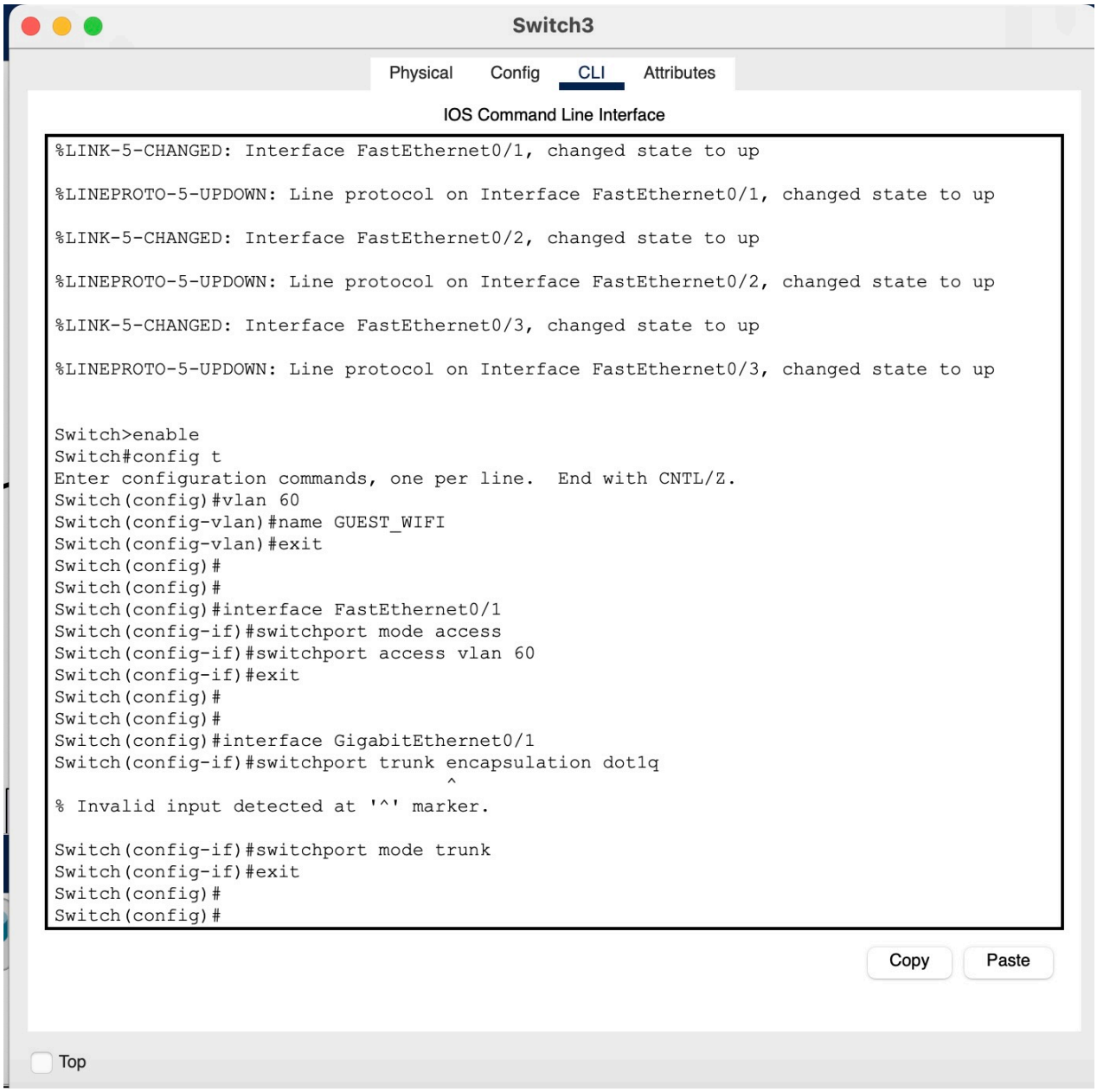
Switch 1 CLI Configuration:



Switch 2 CLI Configuration:



Switch 3 CLI Configuration:



5. Conclusion

The **Scalable Hotel Management Network Design** project successfully demonstrates the implementation of a secure, efficient, and scalable network infrastructure tailored to meet the operational needs of a modern hotel. By leveraging **Cisco Packet Tracer**, the network provides robust communication, data isolation, and resource sharing among the hotel's critical departments—Reception, Finance, Restaurant, Sales, and Guest Wi-Fi.

The design ensures that each department operates within its own **VLAN**, safeguarding sensitive data while allowing controlled inter-departmental communication through **Inter-VLAN Routing**. The **Access Control Lists (ACLs)** applied on the router enhance the security framework by restricting unauthorized access, especially to the Finance VLAN, which handles sensitive financial data. Moreover, the **Guest Wi-Fi VLAN** provides internet-only access to hotel guests, ensuring isolation from internal networks and maintaining data confidentiality.

The centralized server VLAN enables efficient resource sharing, allowing departments to access common files like promotional materials and sales reports, with strict access control. Furthermore, the network is designed with **redundancy** through **Spanning Tree Protocol (STP)**, ensuring uninterrupted service in case of device or link failures.

Project Highlights

1. **Secure Network Design**:
    - VLAN-based isolation ensures data security and operational independence for each department.
    - ACLs enforce strict access policies, protecting sensitive data.
2. **Efficient Communication**:
    - Inter-VLAN Routing provides seamless communication between authorized departments, improving workflow efficiency.
3. **Guest Network Isolation**:
    - A separate VLAN for guest Wi-Fi guarantees complete isolation of internal systems from guest devices, enhancing security.
4. **Scalability and Flexibility**:
    - The network's modular design allows for the seamless addition of new departments, devices, or branches without major reconfiguration.
5. **Redundancy for Reliability**:
    - Redundant links and STP prevent network loops and ensure failover capabilities, maintaining high availability.
6. **Cost-Effective Implementation**:
    - The use of VLANs and a single router with sub-interfaces optimizes resource utilization and reduces costs while meeting the project's technical requirements.

Testing and Verification

The project was rigorously tested to ensure the following:

- Devices within the same VLAN could communicate without issues.
- Controlled inter-VLAN communication was achieved through router sub-interfaces.
- ACLs effectively restricted unauthorized access to sensitive VLANs.
- The Guest VLAN provided internet-only access with no connectivity to internal networks.
- STP successfully handled link failures, ensuring network redundancy.

Project Benefits

The implemented network design delivers several tangible benefits to the hotel:

- Enhanced **security** by isolating sensitive data and applying controlled access.
- Improved **operational efficiency** by facilitating seamless communication between authorized departments.
- **Scalability** to accommodate future growth, ensuring long-term viability.
- **Reliability** through redundancy, reducing downtime and improving the guest experience.

References

(as per the IEEE recommendations)

[1] CompTIA Network+ N10-008 Certification Guide by Glen D. Singh, 2*nd* Edition, Packt publication.

[2] Cisco Systems. (2023). *Cisco Packet Tracer 8.2.0 User Guide*. Retrieved from Cisco Networking Academy.

[3] Tanenbaum, A. S., & Wetherall, D. J. (2021). *Computer Networks* (5th Edition). Pearson Education.

[4] Oppenheimer, P. (2019). *Top-Down Network Design* (4th Edition). Cisco Press.

[5] Lammle, T. (2021). *CCNA Certification Study Guide* (8th Edition). Wiley.

[6] ChatGPT