Project Documentation:

Secure Enterprise Network Setup

# 1. Introduction

This project demonstrates the setup of a secure enterprise network involving VLANs, Inter-VLAN Routing, and effective IP addressing.   
The network setup is designed to meet the requirements of different departments within an organization: HR, IT, and Finance.

# 2. Objective

The primary goal of this project was to:  
Design and implement a network structure with separate VLANs for different departments.  
Set up Inter-VLAN Routing to allow communication between devices across different VLANs.  
Ensure the network is secure by segmenting traffic through VLANs.  
Test connectivity between devices in different VLANs.

# 3. Network Design

The network consists of the following components:  
- One Router for routing traffic between VLANs.  
- Three Layer 2 Switches to manage traffic within each VLAN.  
- Nine PCs, distributed across three VLANs:  
 - HR VLAN: 192.168.10.0/24  
 - IT VLAN: 192.168.20.0/24  
 - Finance VLAN: 192.168.30.0/24  
  
Each department is isolated within its own VLAN, and communication between VLANs is facilitated by Inter-VLAN Routing on the router.

# 4. IP Addressing Scheme

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| VLAN Name | VLAN ID | Subnet IP Range | Gateway IP | PCs IP Addresses |
| HR | 10 | 192.168.10.0/24 | 192.168.10.1 | 192.168.10.5, 192.168.10.10, 192.168.10.15 |
| IT | 20 | 192.168.20.0/24 | 192.168.20.1 | 192.168.20.5, 192.168.20.10, 192.168.20.15 |
| Finance | 30 | 192.168.30.0/24 | 192.168.30.1 | 192.168.30.5, 192.168.30.10, 192.168.30.15 |
|  |

# 5. Configuration Details

**Router Configuration:**  
- Sub-interfaces created for each VLAN (HR, IT, Finance).  
- IP addresses assigned to each sub-interface (Gateway IP for each VLAN).  
- Routing enabled to allow communication between VLANs.  
  
Example router configuration:

*interface GigabitEthernet0/0.10  
 encapsulation dot1Q 10  
 ip address 192.168.10.1 255.255.255.0  
  
interface GigabitEthernet0/0.20  
 encapsulation dot1Q 20  
 ip address 192.168.20.1 255.255.255.0  
  
interface GigabitEthernet0/0.30  
 encapsulation dot1Q 30  
 ip address 192.168.30.1 255.255.255.0*

**Switch Configuration**:  
- Each switch is configured with the appropriate VLAN IDs (10, 20, 30).  
- Ports assigned to their respective VLANs based on device location.  
  
Example switch configuration:

*vlan 10  
 name HR  
!  
vlan 20  
 name IT  
!  
vlan 30  
 name Finance*

# 6. Network Connectivity and Testing

After completing the configuration, tests were performed to verify connectivity:  
- Ping tests were conducted between PCs in different VLANs (HR to IT, Finance to IT) to ensure Inter-VLAN Routing was functional.  
- HR-PC1, IT-PC1, and Finance-PC1 were successfully able to ping each other after inter-VLAN routing was enabled.  
  
Test results:  
*- HR-PC1 (192.168.10.5) successfully pinged IT-PC1 (192.168.20.5) and Finance-PC1 (192.168.30.5).*

*- IT-PC1 (192.168.20.5) successfully pinged HR-PC1 (192.168.10.5) and Finance-PC1 (192.168.30.5).*

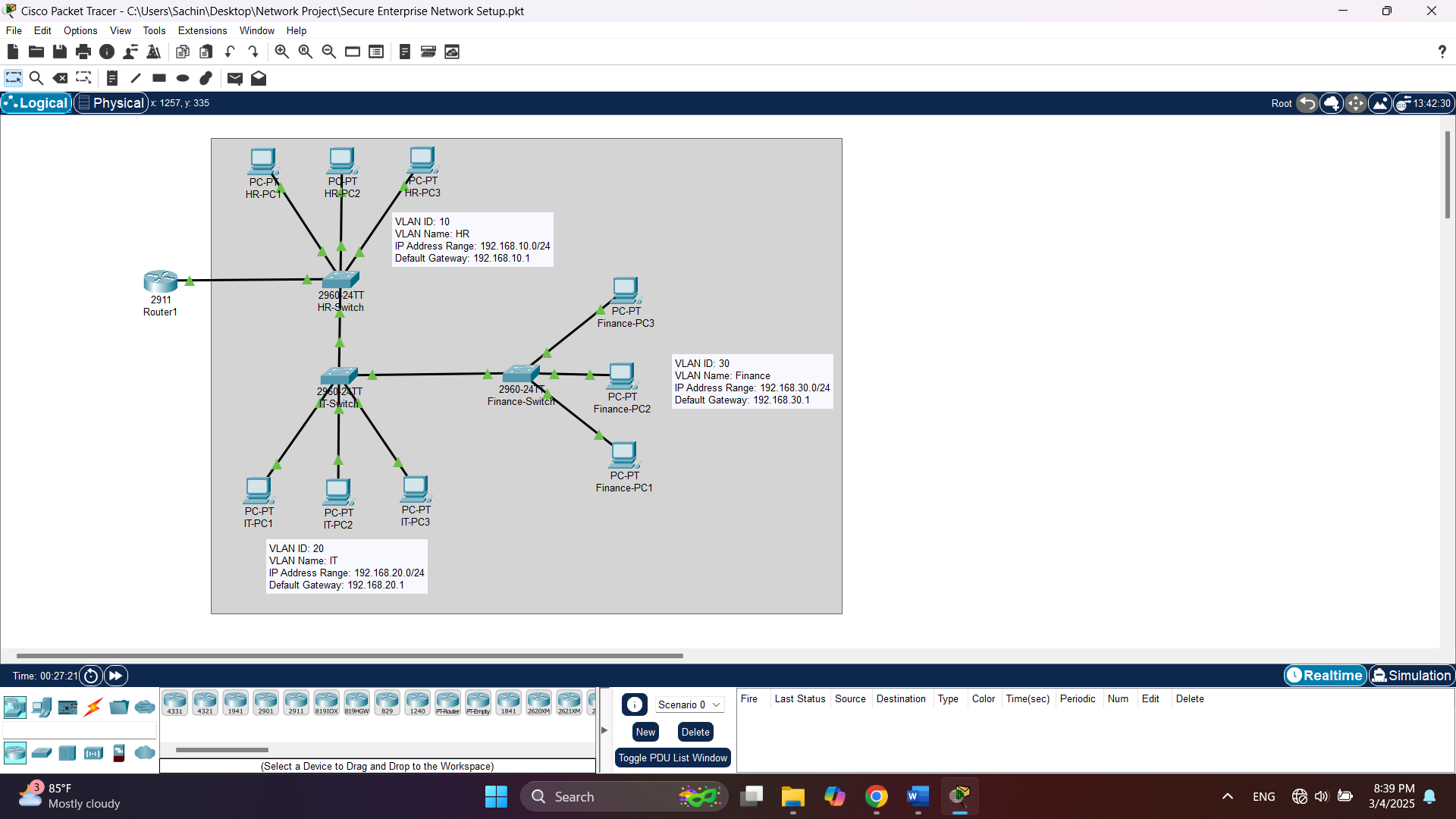
*- Finance-PC1 (192.168.30.5) successfully pinged HR-PC1 (192.168.10.5) and IT-PC1 (192.168.20.5).*

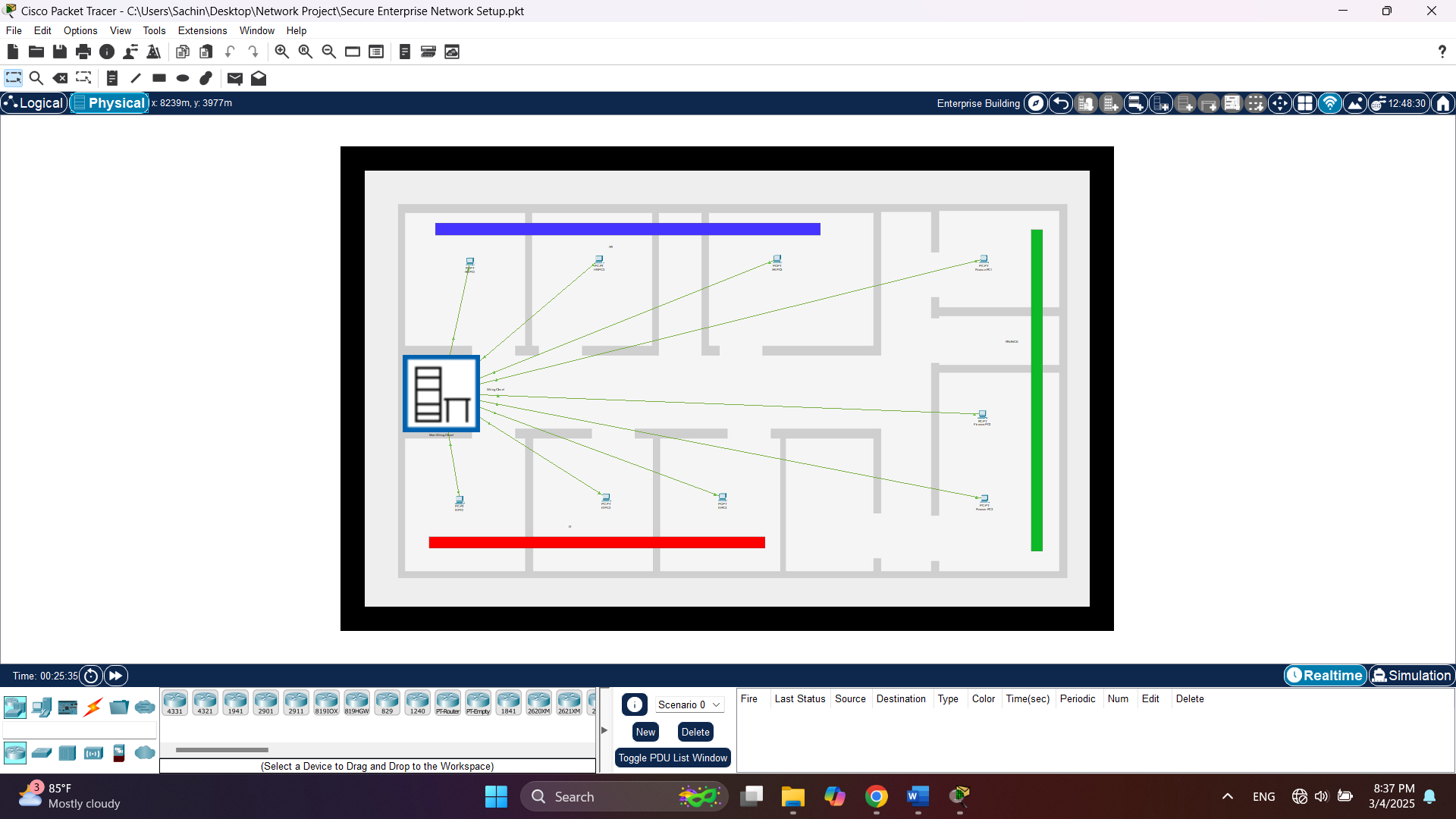
# 7. Conclusion

This project successfully demonstrated the ability to create and configure a secure enterprise network using VLANs for different departments,   
Inter-VLAN Routing for communication, and appropriate IP addressing. The network setup ensures proper segmentation, with each department   
isolated in its own VLAN and able to communicate with others as needed.

# 8. Screenshots

relevant screenshots for the following:  
**1. Network Topology:**

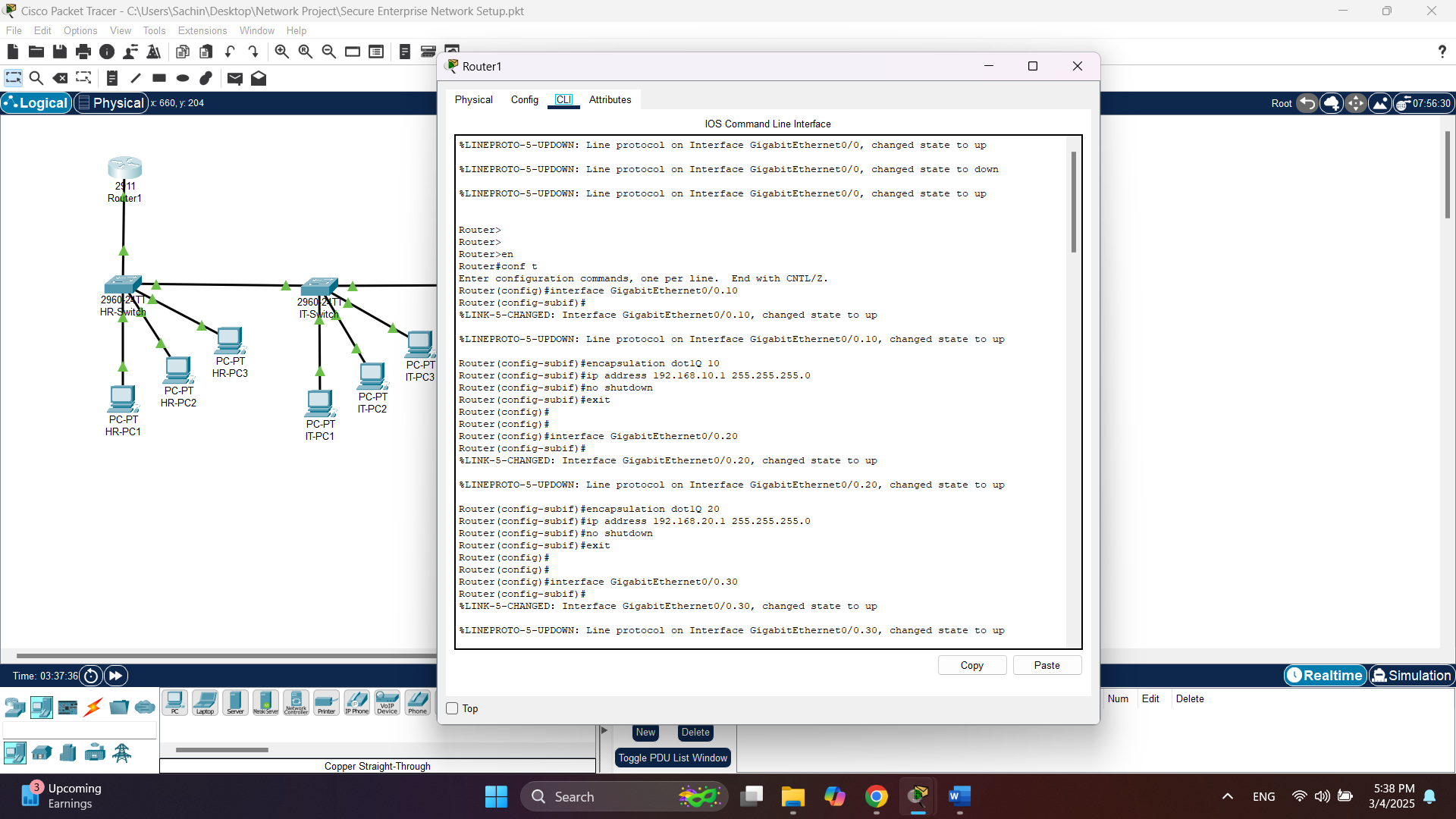
1. **Diagram of the network setup.**

**II. Physical Setup**

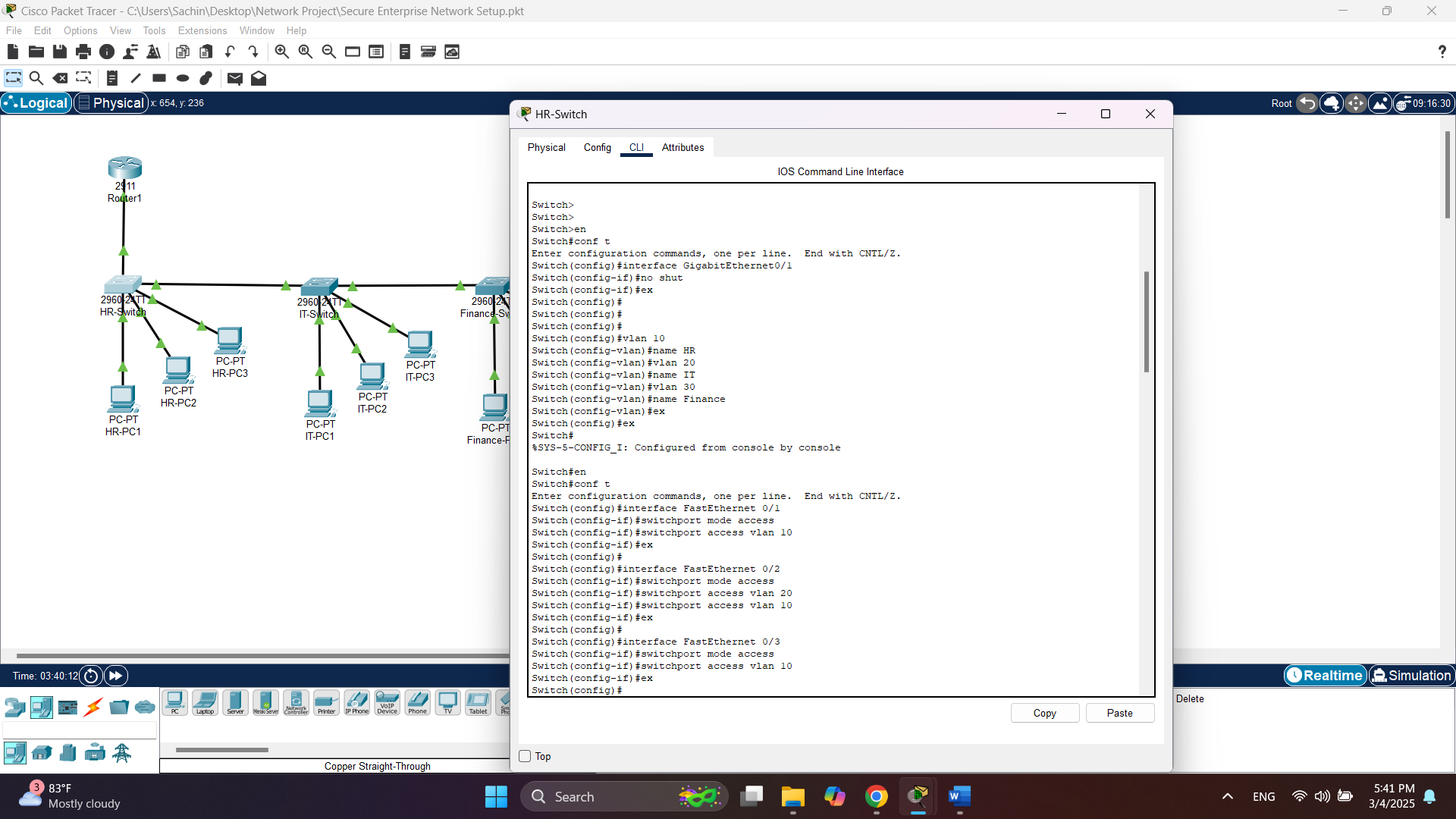
**III. Main Wiring Setup**

****

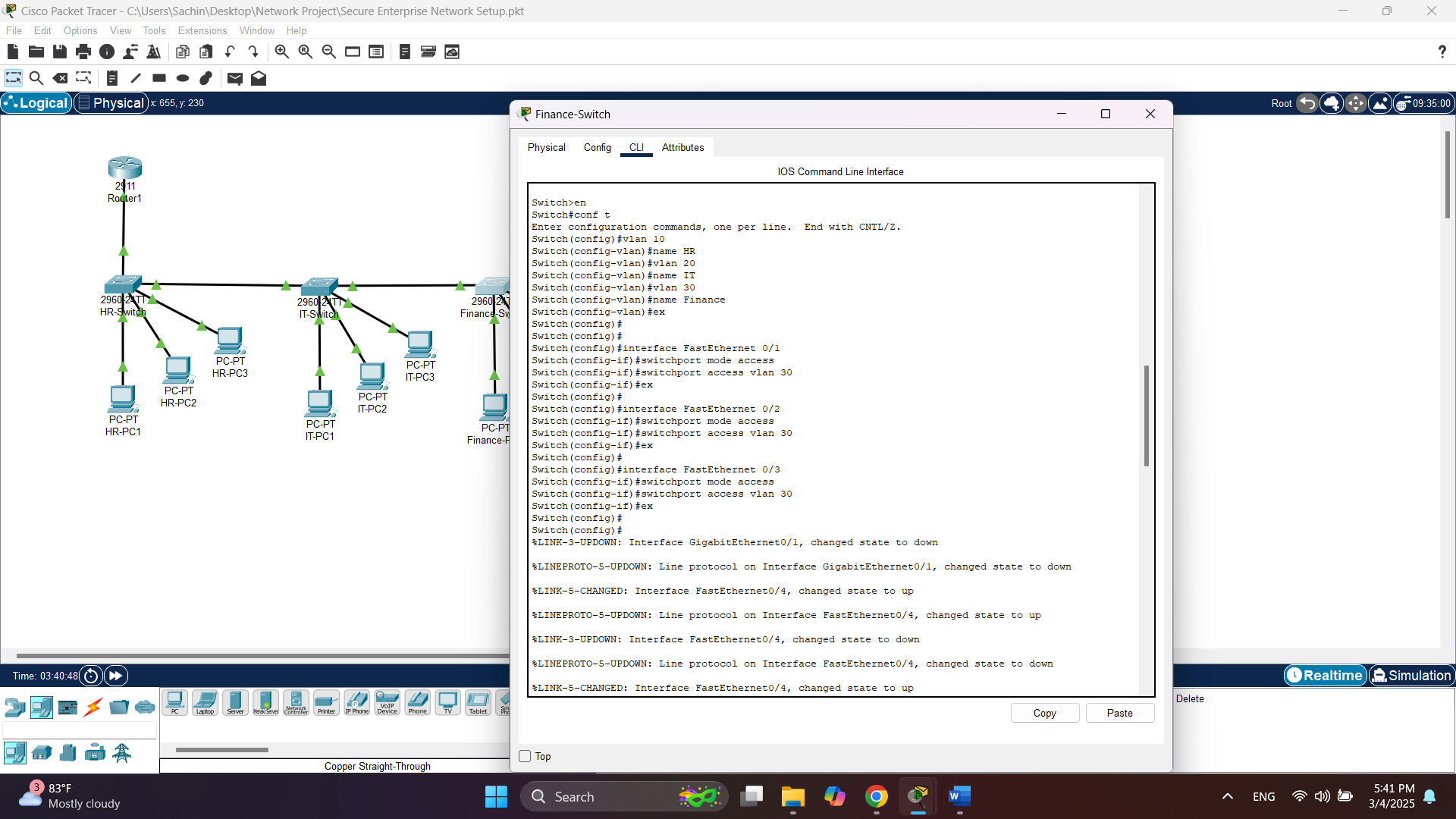
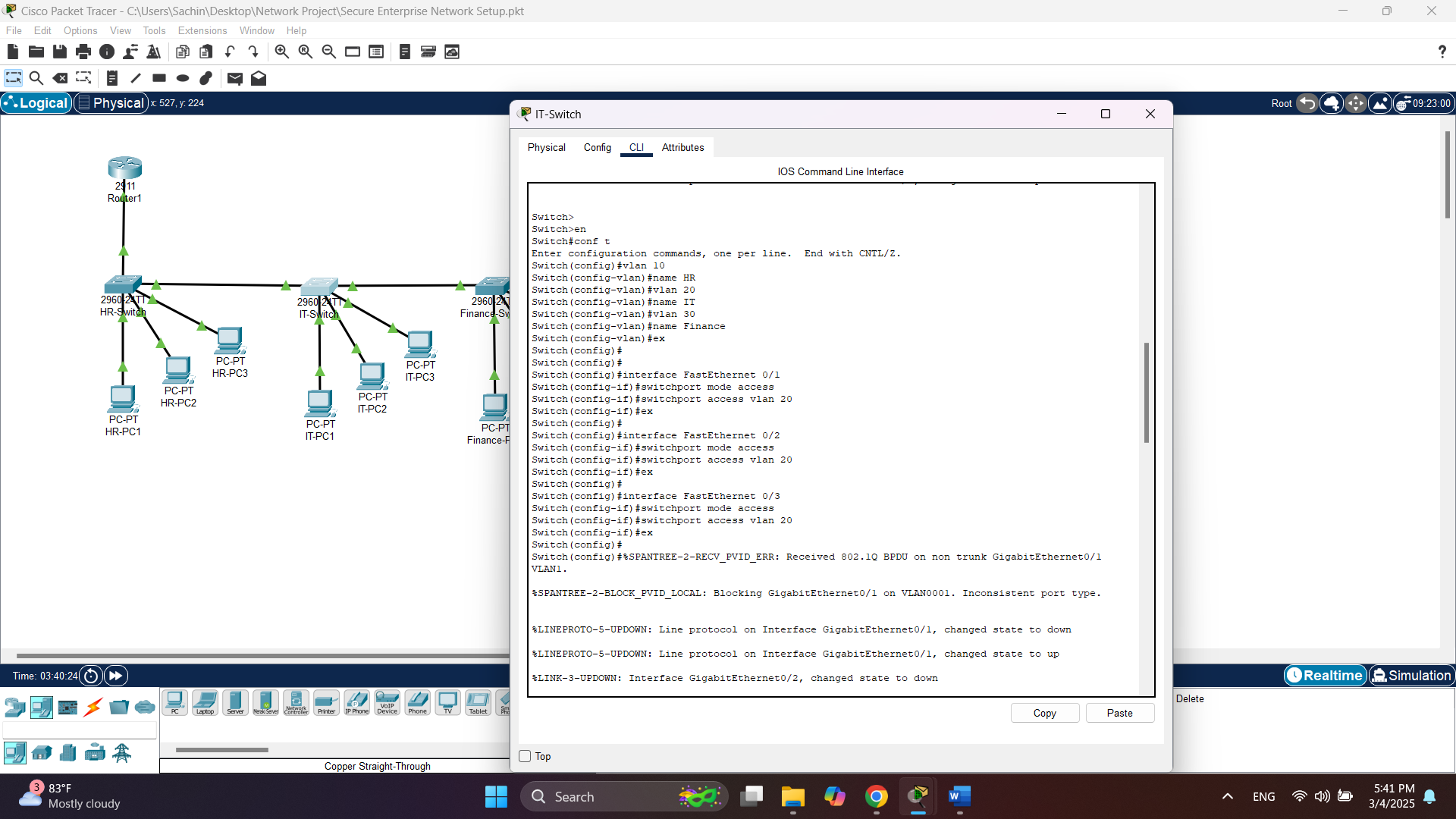
**2. Router Configuration: Screenshot of the router interface configuration.**

****

**3. Switch Configuration: Screenshot of the switch VLAN configuration.**

****

HR Switch

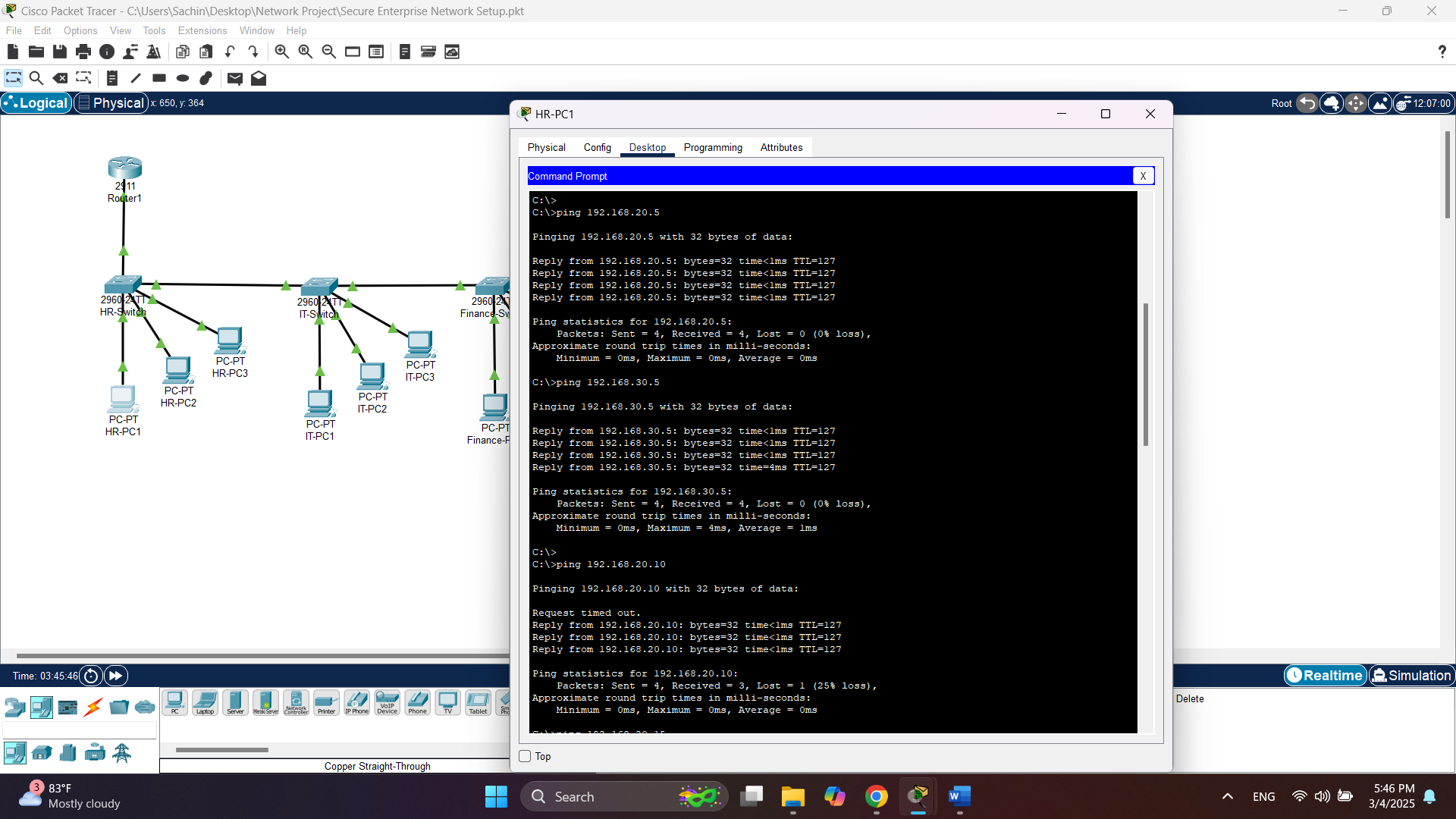
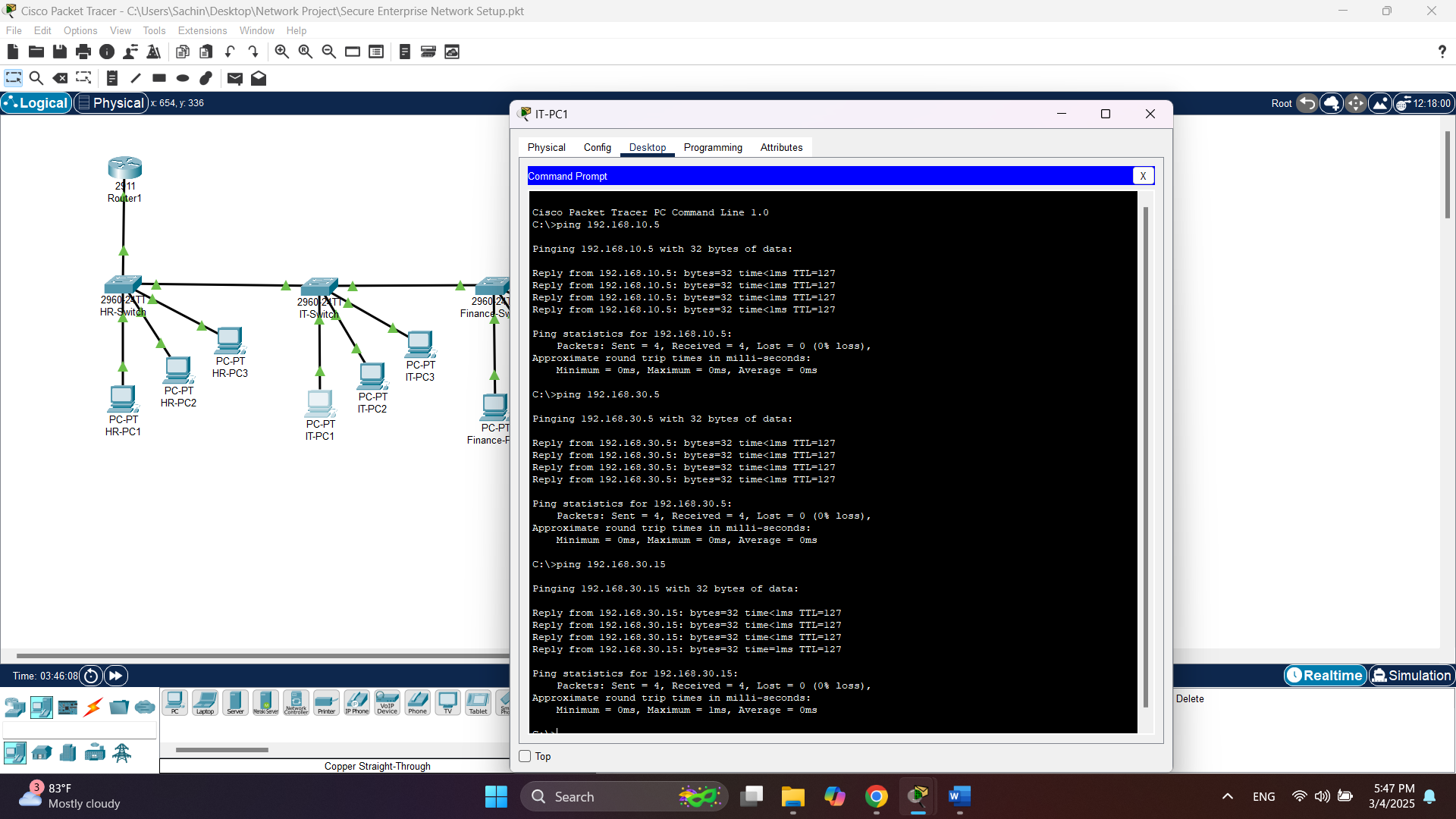
****

IT Switch

Finance Switch

Finance Switch

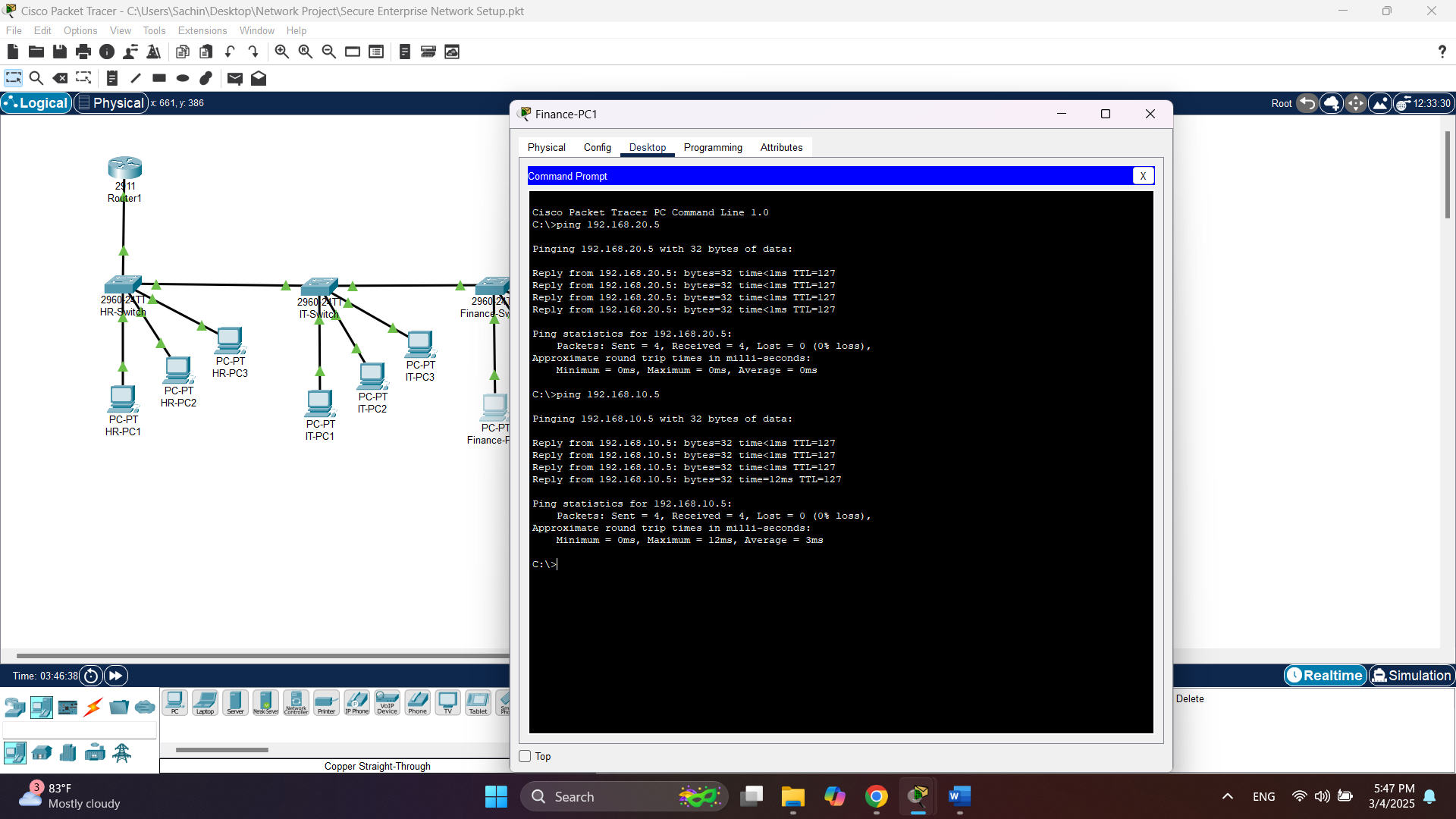
**4. Ping Test Results: Screenshots of successful ping tests between PCs in different VLANs.**

****

IT- PC1

HR-PC1

HR-PC

****

Finance- PC1

# 9. Future Enhancements

**Firewall Integration for Improved Security:** In the current setup, traffic between VLANs is routed without any restriction. To enhance the security of the network, integrating a firewall between VLANs would allow for better control over traffic flow. A firewall could filter traffic, block unauthorized access, and allow only the required traffic based on pre-defined rules.

**Virtual Private Network (VPN) Setup:** To provide remote access to employees while maintaining security, a VPN could be implemented. A VPN would allow authorized users to securely access the corporate network from outside the office environment. This feature is particularly useful for remote employees or branch offices that need to connect securely to the main network.