NETWORKING SIMULATION

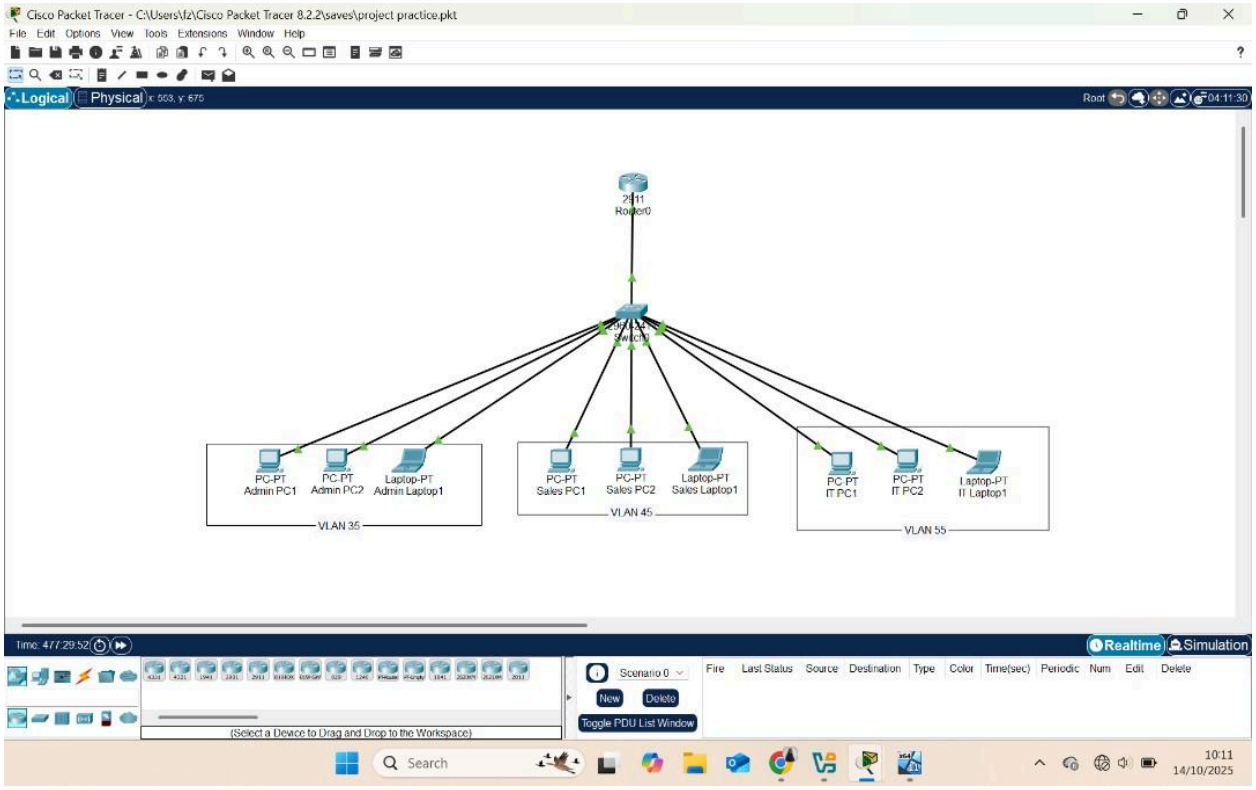
Tool Used: CISCO PACKET TRACER

INTRODUCTION

This project simulates a branch office network for a mid-sized financial services company. My goal is to design a secure small enterprise network with VLAN segmentation, inter-VLAN routing, and Access Control Lists (ACLs) to regulate communication between departments. I also configured SSH to enable secure device management while disabling Telnet for better security.

NETWORK DESIGN and TOPOLOGY

To begin the project, I designed a simple and secure branch office network using Cisco Packet Tracer. The network connects three core departments; Administration, Sales, and IT Support. I assigned each department to a separate VLAN (35,45, 55 respectively) to ensure proper segmentation and control of network traffic. Each department has three end devices (two PCs and one laptop) connected to a central switch, which links to a router through a trunk port. This design enables inter-VLAN routing and controlled communication between departments through Access Control Lists (ACLs).



Explanation of Components:
Router: Performs inter-VLAN routing (Router-on-a-Stick) and applies ACLs.
Switch: Connects all end devices and manages VLAN assignments.
Admin PCs & Laptop: Devices used by the administration team (VLAN 35).
Sales PCs & Laptop: Devices used by the Sales department (VLAN 45).
IT PCs & Laptop: Devices used by the IT Support department (VLAN 55).

This topology forms the foundation for VLAN configuration, inter-VLAN routing, and network security through ACLs and SSH.

STEP-BY-STEP CONFIGURATION AND EXPLANATION
After the preparatory steps above, my goal is to build a secure, segmented branch network and then harden it for safe management. I will:

- configure VLANs on the switch and assign ports so each department (Admin, Sales, IT).
- trunk the switch uplink to the router so multiple VLANs travel over a single link.
- configure Router-on-a-Stick subinterfaces with 802.1Q encapsulation and assign each VLAN a dedicated gateway (IP addressing using the 10.10.x.0/24 scheme).
- apply extended ACLs on the router to enforce the policy (Admin → Sales allowed, Admin → IT denied; Sales → IT allowed, Sales → Admin denied; IT unrestricted).
- enable SSH on network devices (generate RSA keys, create local admin account, set VTY to SSH only) and explicitly disable Telnet.
- verify the design with show commands and connectivity tests (ping, show ip interface brief, show vlan brief, show interfaces trunk, show access-lists)

Step 1: Vlan Configuration

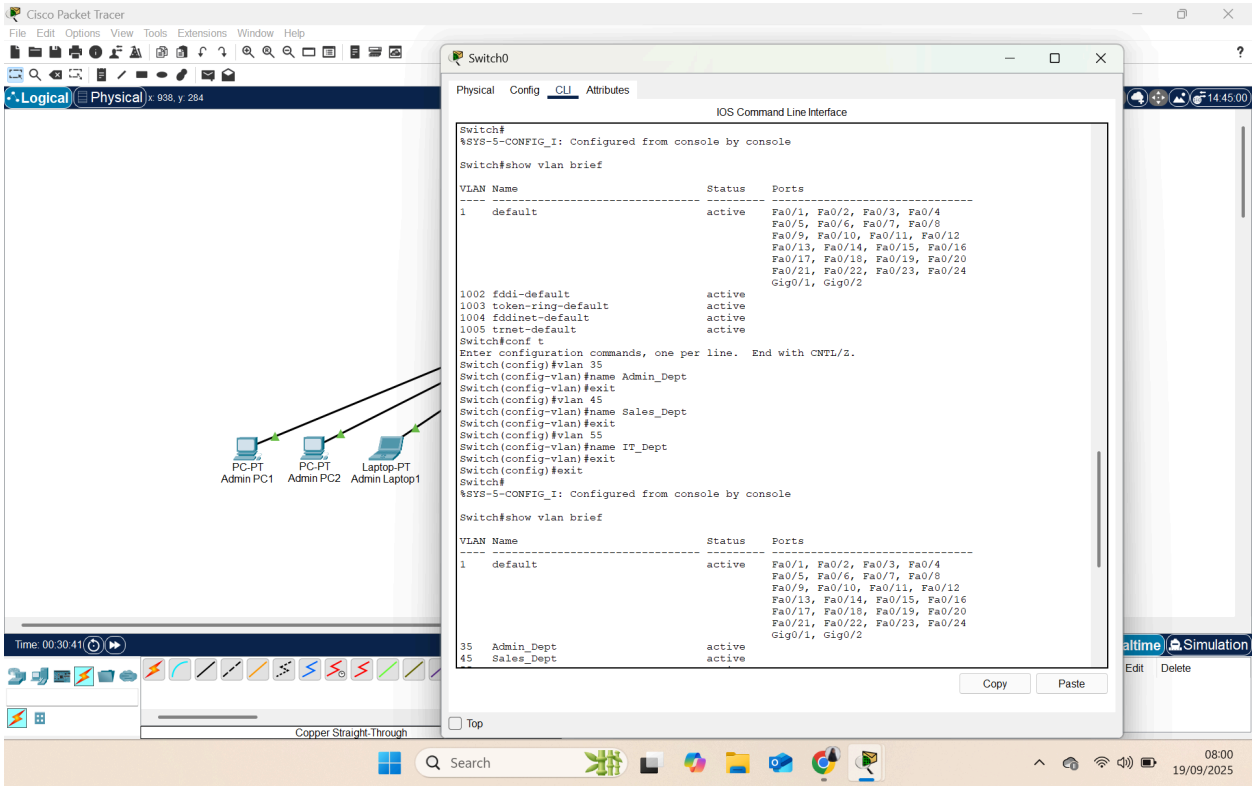
I created three VLANs (35, 45, 55,) named them Admin_Dept, Sales_Dept and IT_Dept.

Commands used: on the switch
```
enable
conf t
 vlan 35
 name Admin_Dept
```

exit
 vlan 45
 name Sales_Dept
exit
 vlan 55
 name IT_Dept
exit

Then I showed the vlan brief to confirm configuration.

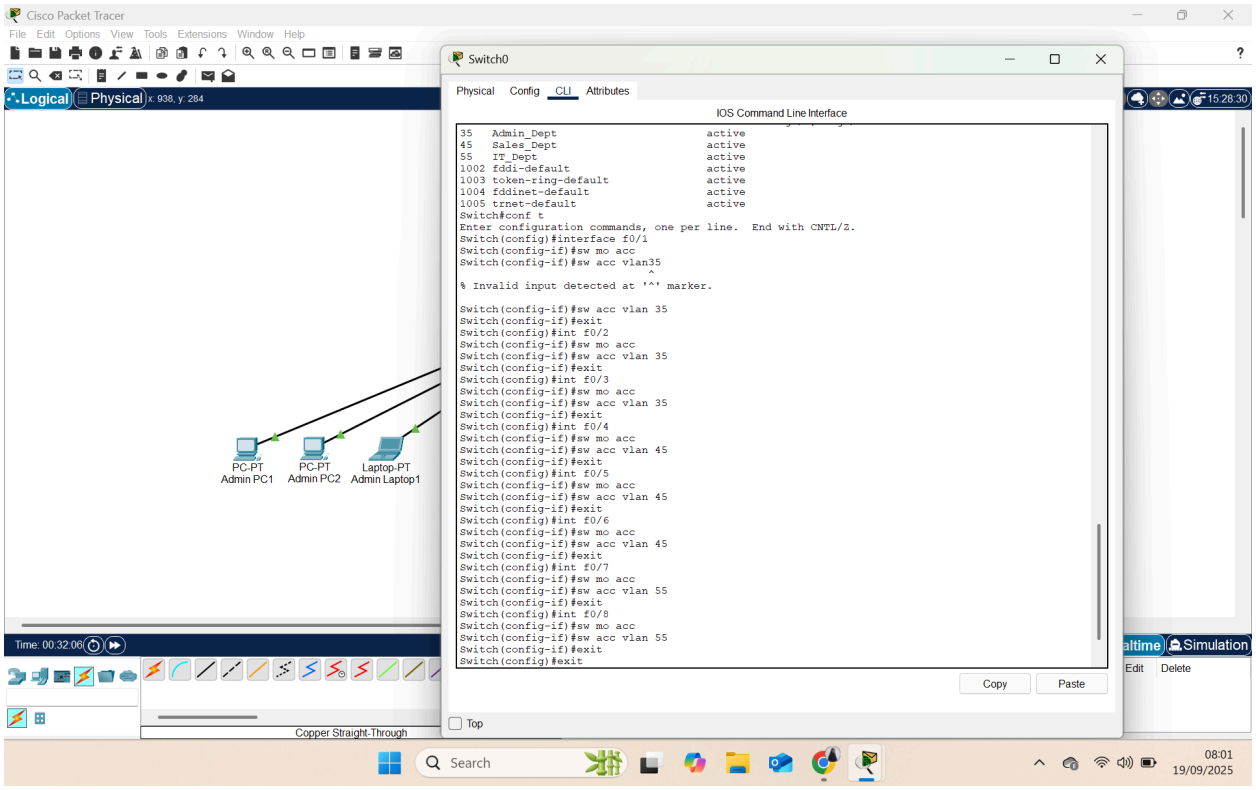
Command used: show vlan brief



Then, I assigned switch access ports for each department (3 devices per VLAN).

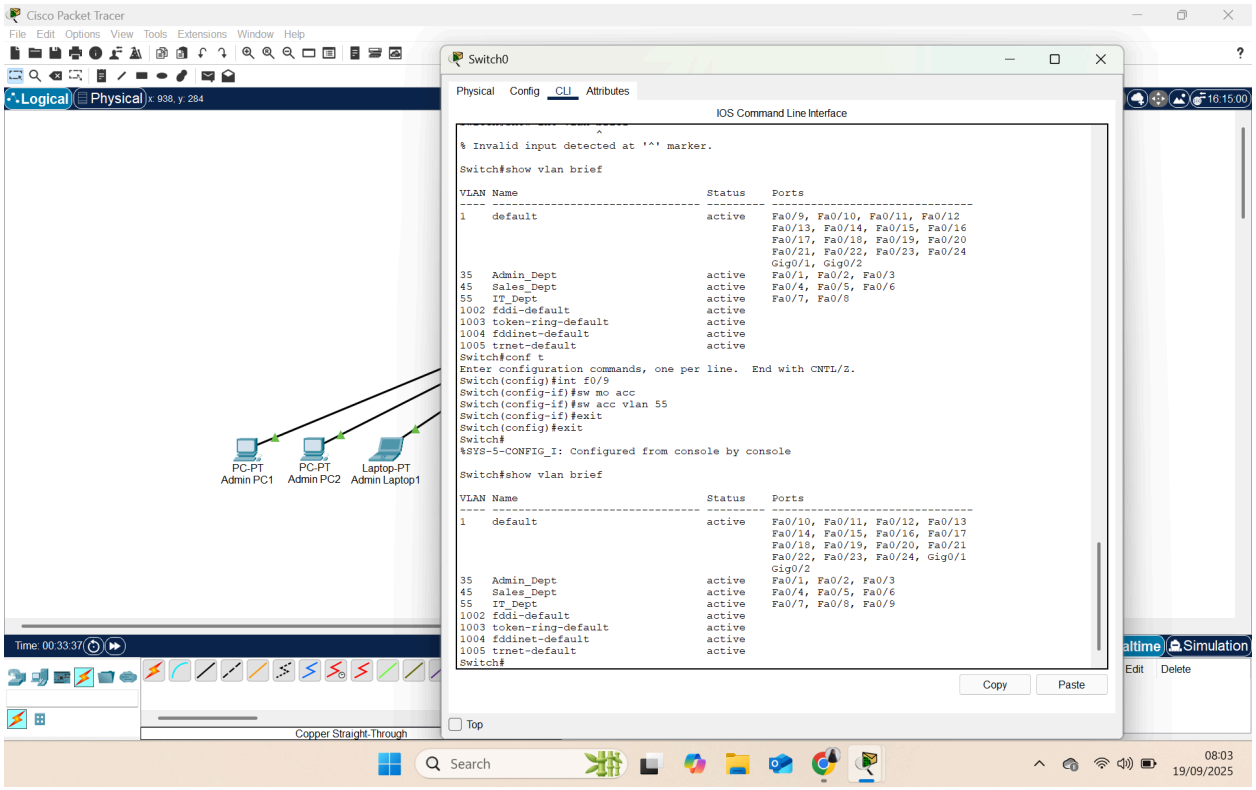
Commands used: on the switch
conf t
 interface f0/1
 sw mo acc
 sw acc vlan 35
exit

```
 int f/02
 sw mo acc
 sw acc vlan 35
exit
 int f/03
 sw mo acc
 sw acc vlan 35
exit
 int f/04
 sw mo acc
 sw acc vlan 45
exit
 int f/05
 sw mo acc
 sw acc vlan 45
exit
 int f/06
 sw mo acc
 sw acc vlan 45
exit
 int f/07
 sw mo acc
 sw acc vlan 55
exit
 int f/08
 sw mo acc
 sw acc vlan 55
exit
 int f/09
 sw mo acc
 sw acc vlan 55
exit
```



Then I showed the vlan brief to confirm configuration.

Command used: show vlan brief



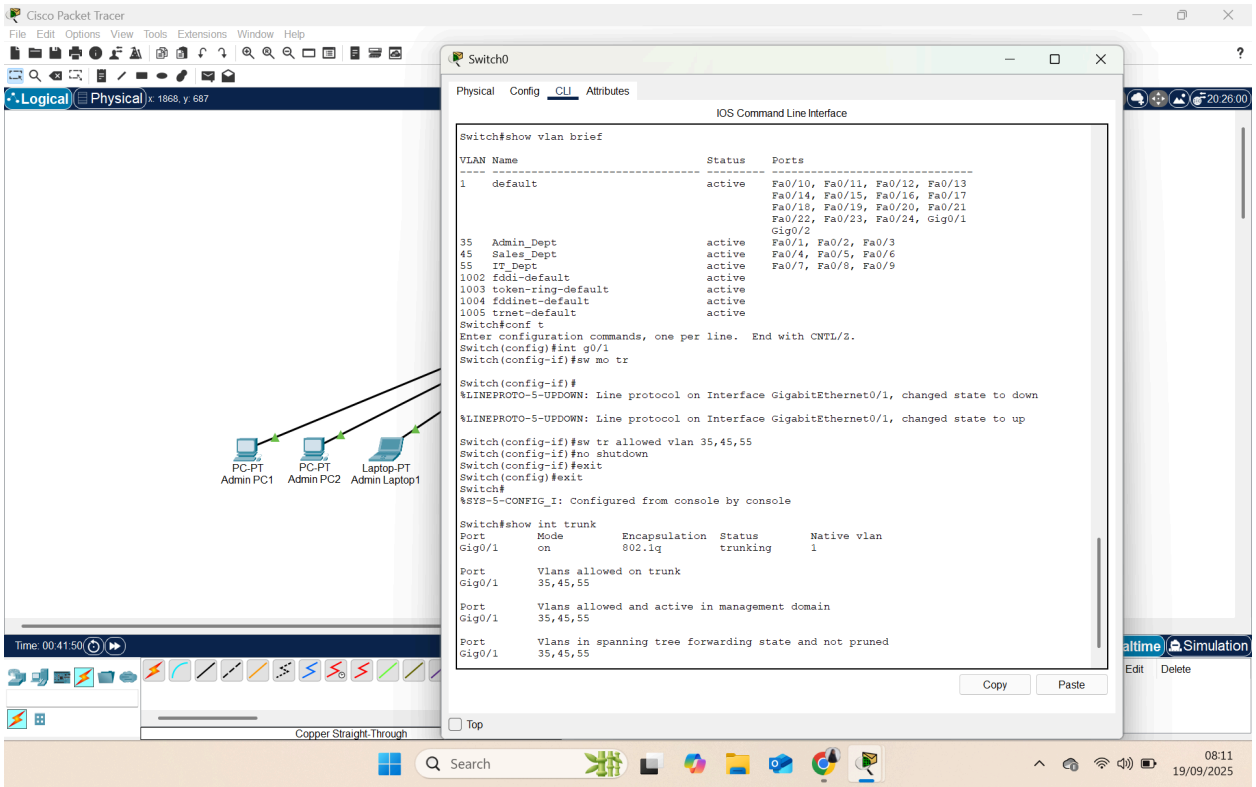
Step 2: Configuring Trunking on the Switch Uplink

In this step, I configured trunking on the switch uplink interface to allow multiple VLANs to be carried over a single physical link to the router. This enables inter-VLAN communication through Router-on-a-Stick.

Commands used: on the switch
enable
conf t
 int g0/1
 sw mo tr
 sw tr allowed vlan 35,45,55
 no shutdown
exit

Then I showed the interface trunking for confirmation.

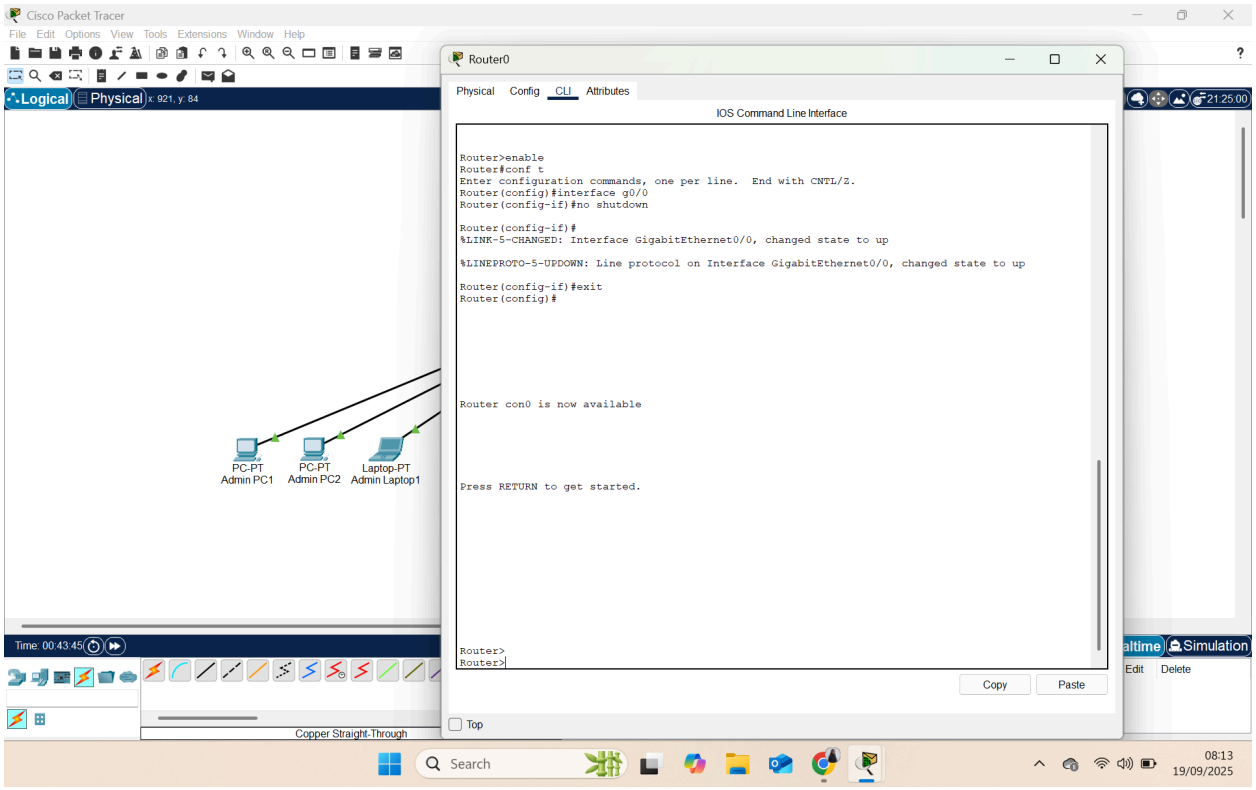
Command used: show int tr



Step 3: Connecting Switch to the Router

I connected the switch to the router using the GigabitEthernet0/0 interface. This physical link will carry traffic from all VLANs through the trunk port to the router for inter-VLAN routing.

Commands used: on the router
en
conf t
 interface g0/0
 no shutdown
exit



Step 4: Configuring Router-on-a-Stick (Subinterfaces)

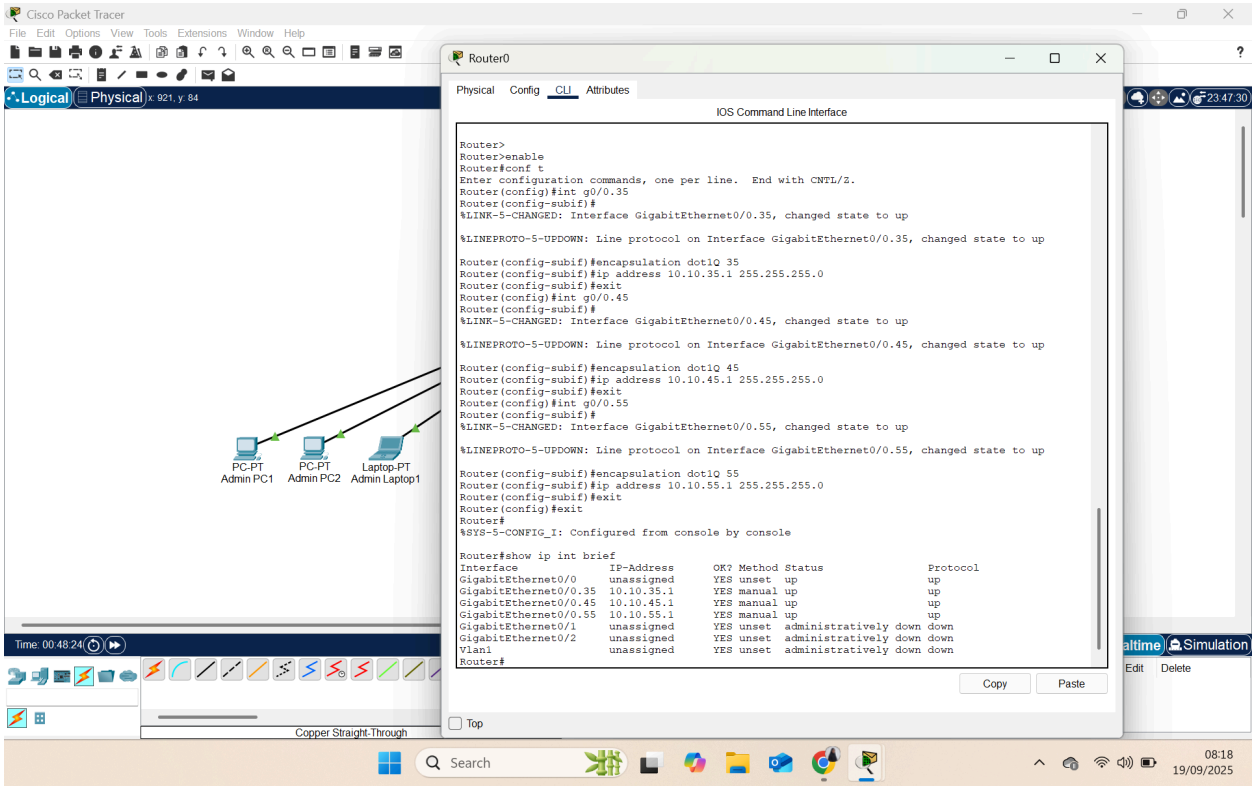
In this step, I configured subinterfaces on the router's GigabitEthernet0/0 interface to enable inter-VLAN routing. I used 802.1Q encapsulation to allow traffic from multiple VLANs to travel through a single physical interface. Each subinterface was assigned to a specific VLAN and configured with a default gateway IP address from the 10.10.x.0/24 addressing scheme. This allows devices in different VLANs to communicate through the router while maintaining logical network segmentation.

For Vlan 35, I assigned 10.10.35.1 as the default gateway.
For Vlan 45, I assigned 10.10.45.1 as the default gateway.
For Vlan 55, I assigned 10.10.55.1 as the default gateway.

Commands used: on the router
enable
conf t
 int g0/0.35
 encapsulation dot1Q 35
 ip address 10.10.35.1 255.255.255.0
exit
 int g0/0.45
 encapsulation dot1Q 45
 ip address 10.10.45.1 255.255.255.0
exit
 int g0/0.55
 encapsulation dot1Q 55
 ip address 10.10.55.1 255.255.255.0
exit

Then I showed the IP interface brief for confirmation

Command used: show ip int brief



Step 5: Assigning IP Addresses to End Devices

In this step, I manually assigned IP addresses to each end device (PCs and laptops) in their respective VLAN networks. This ensures that each device can communicate with other devices within the same VLAN and with other VLANs through the router's subinterfaces (default gateways).

Each device's IP address falls within the corresponding subnet:

Admin VLAN (35): 10.10.35.0/24
Sales VLAN (45): 10.10.45.0/24
IT VLAN (55): 10.10.55.0/24

The default gateway for each device is set to the router subinterface IP assigned to its VLAN. This is essential for inter-VLAN communication.

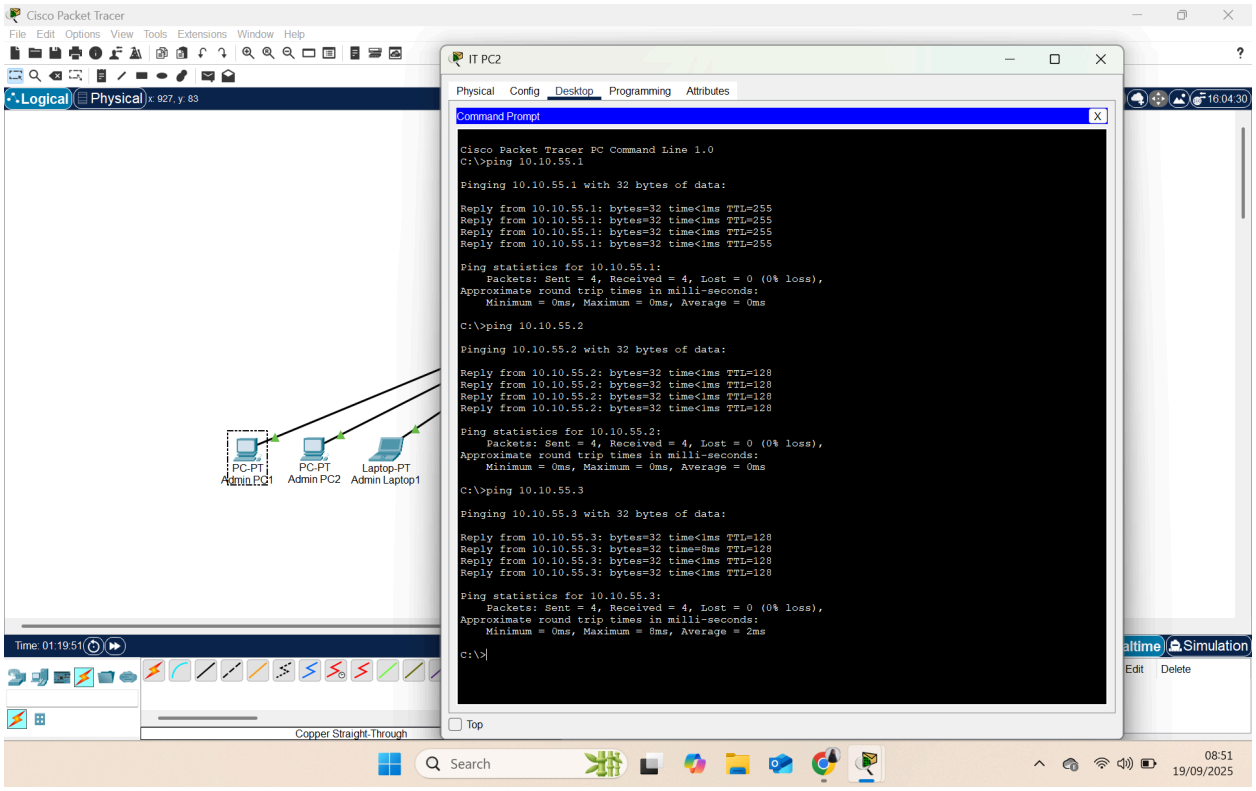
List of IP addresses I used;

Name of Device	**IP Address**	**Subnet mask**	**Default Gateway**
Admin PC1	10.10.35.2	255.255.255.0	10.10.35.1
Admin PC2	10.10.35.3	255.255.255.0	10.10.35.1
Admin Laptop1	10.10.35.4	255.255.255.0	10.10.35.1
Sales PC1	10.10.45.2	255.255.255.0	10.10.45.1
Sales PC2	10.10.45.3	255.255.255.0	10.10.45.1
Sales Laptop1	10.10.45.4	255.255.255.0	10.10.45.1
IT PC1	10.10.55.2	255.255.255.0	10.10.55.1
IT PC2	10.10.55.3	255.255.255.0	10.10.55.1
IT Laptop1	10.10.55.4	255.255.255.0	10.10.55.1

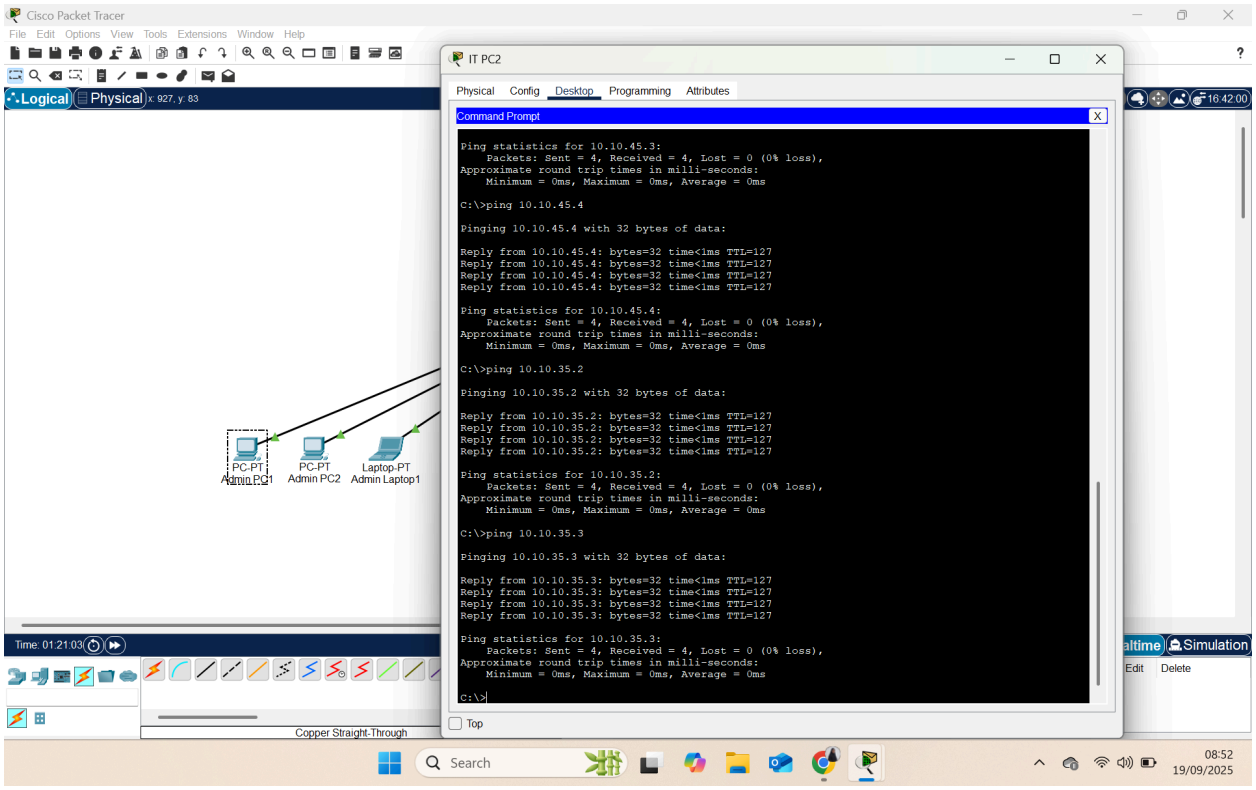
Step 6: Testing Network Connectivity

In this step, I verified that devices in each VLAN were properly configured and could communicate with each other and with the router. I used the **ping** command from the end devices to test basic connectivity:

Firstly, I tested connectivity within the same VLAN to confirm that devices could communicate locally through the switch. I also pinged the default gateways to ensure each device could reach the router.



Then, I tested connectivity between different VLANs to confirm that inter-VLAN routing was working correctly through the router subinterfaces.



Successful ping replies indicated that the IP addresses, VLAN assignments, trunking, and Router-on-a-Stick configuration were all correctly set up.

Step 7: Configuring Extended ACLs on the Router

In this step, I applied **Extended Access Control Lists (ACLs)** on the router to control and secure communication between the different VLANs based on the company's security policy.

The policy states:

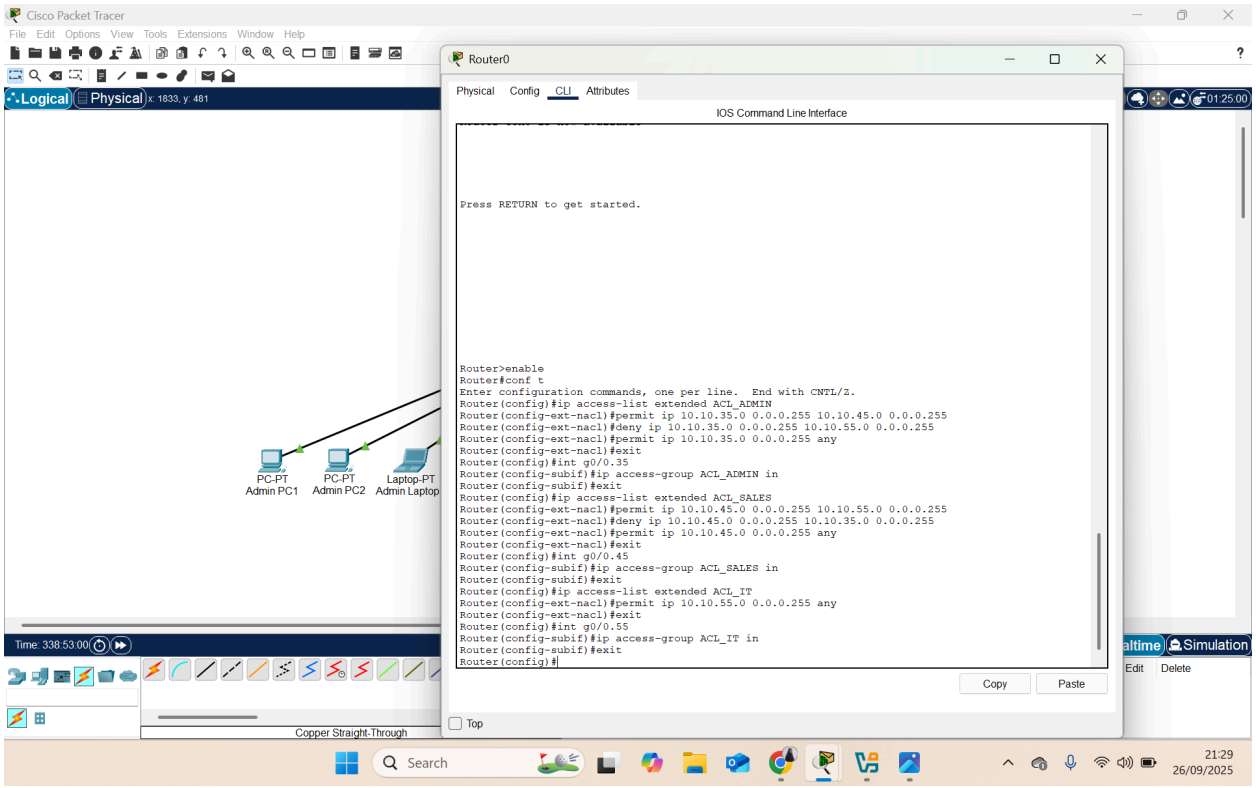
- Admin VLAN should be able to access **Sales VLAN** only (for reporting purposes) but not IT VLAN.
- Sales VLAN should be able to access **IT VLAN** (for support) but should not access Admin VLAN.
- IT VLAN should have **unrestricted access** to all VLANs for administrative purposes.

Extended ACLs were chosen because they provide more granular control allowing me to specify source and destination IP addresses as well as the type of traffic. I applied the ACLs inbound on

each VLAN’s subinterface, which is more efficient and limits unwanted traffic at the point of entry.

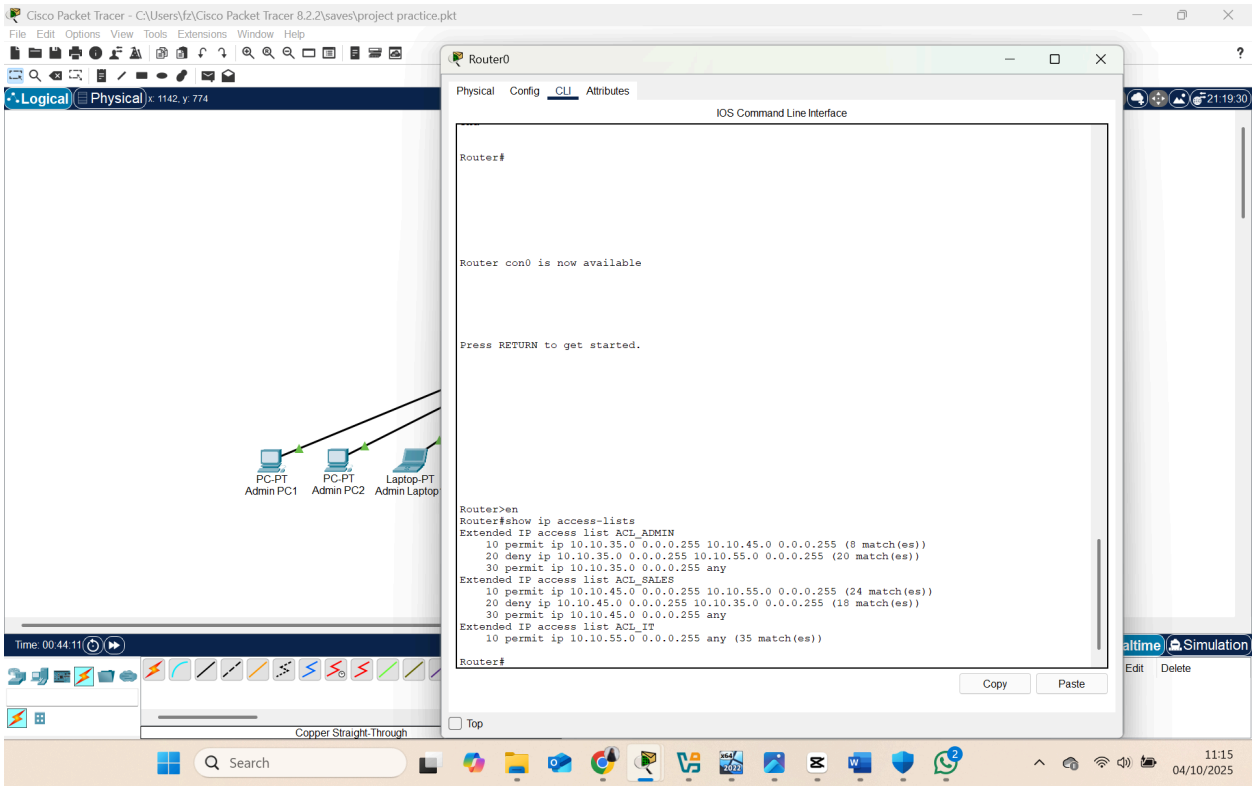
Commands used: on the router

```
en
conf t
 ip access-list extended ACL_ADMIN
 permit ip 10.10.35.0 0.0.0.255 10.10.45.0 0.0.0.255
 deny ip 10.10.35.0 0.0.0.255 10.10.55.0 0.0.0.255
 permit ip 10.10.35.0 0.0.0.255 any
exit
 int g0/0.35
 ip access-group ACL_ADMIN in
exit
 ip access-list extended ACL_SALES
 permit ip 10.10.45.0 0.0.0.255 10.10.55.0 0.0.0.255
 deny ip 10.10.45.0 0.0.0.255 10.10.35.0 0.0.0.255
 permit ip 10.10.45.0 0.0.0.255 any
exit
 int g0/0.45
 ip access-group ACL_SALES in
exit
 ip access-list extended ACL_IT
 permit ip 10.10.55.0 0.0.0.255 any
exit
 int g0/0.55
 ip access-group ACL_IT in
exit
```



Then I showed the IP access-lists for confirmation that the ACL rules were actively applied and traffic was being filtered as intended.

Command used: show ip access-lists



This configuration enforces the principle of least privilege, ensuring each department can only access what it truly needs.

Step 7: Testing and Verifying ACL Configuration

After applying the ACLs, I tested connectivity between devices in different VLANs to ensure the security policy was enforced correctly. The goal of this step is to confirm that:

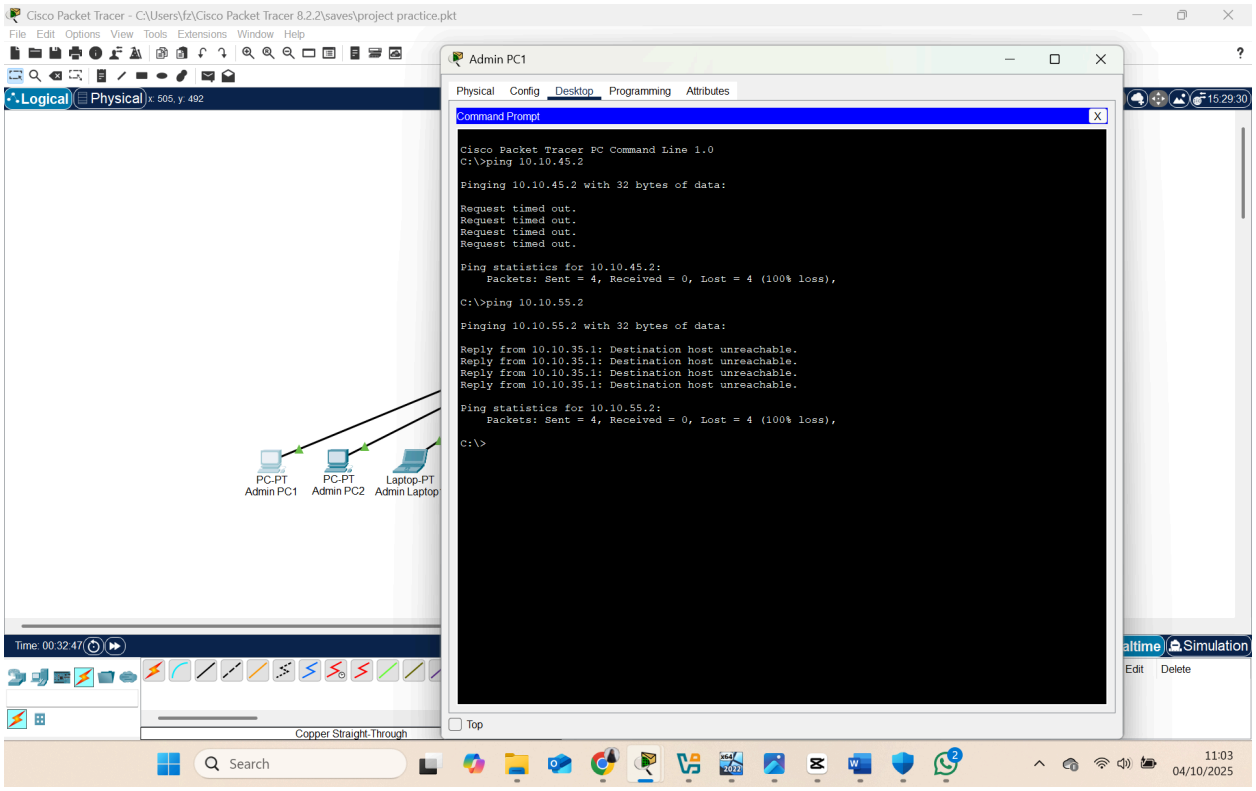
- Admin VLAN can reach Sales VLAN but cannot reach IT VLAN.
- Sales VLAN can reach IT VLAN but cannot reach Admin VLAN.
- IT VLAN can reach both Admin and Sales VLANs without restrictions.

Ping Test Results and Explanation

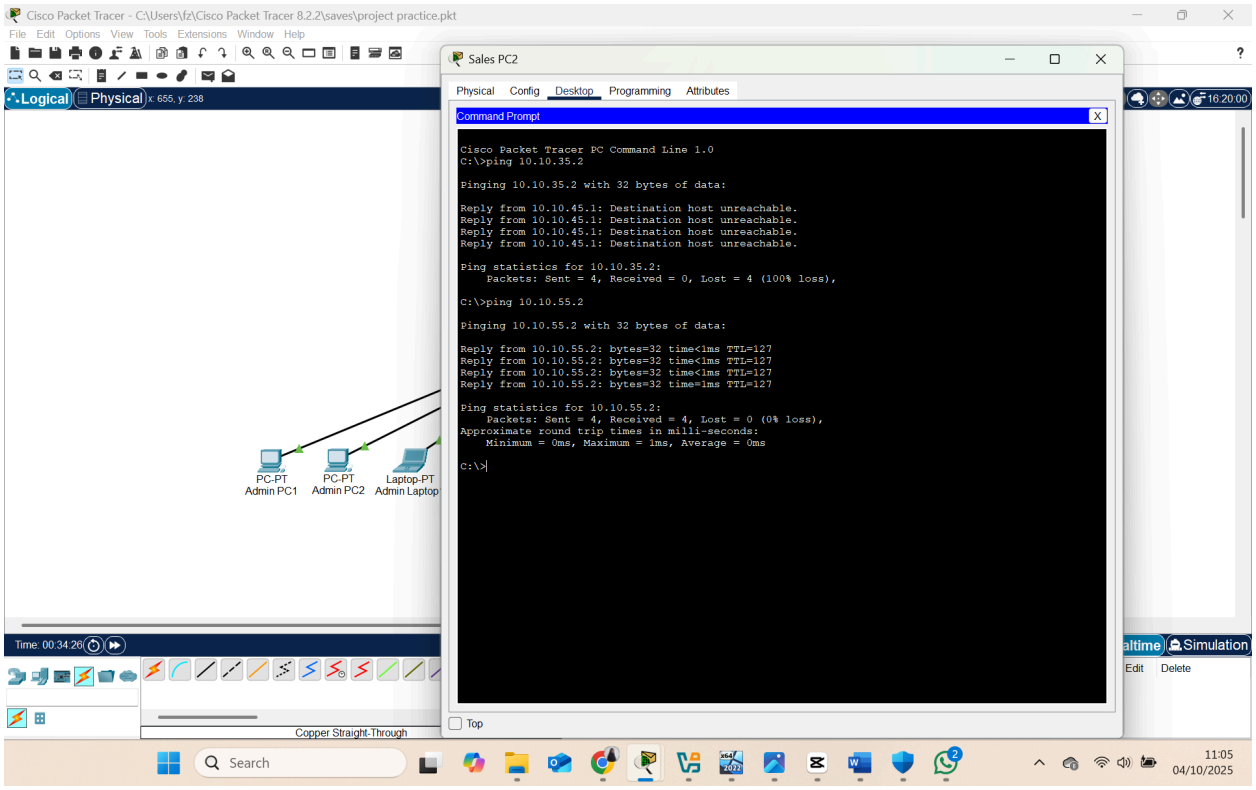
During testing, I verified how the Access Control Lists (ACLs) affected communication between the VLANs by using the ping command.

Admin to Sales: When I pinged a Sales device from Admin(ping 10.10.45.2), I received a “Request timed out” response. This happened because ping uses ICMP echo requests, which require a two-way handshake. Admin could reach Sales, but Sales was not allowed to reply (due to the ACL rule blocking Sales from reaching Admin), resulting in a timeout.

Admin to IT: When I pinged IT from Admin(ping 10.10.55.2), the response was “Destination host unreachable.” This is because Admin traffic was explicitly denied from reaching IT, so the echo request itself could not pass through.

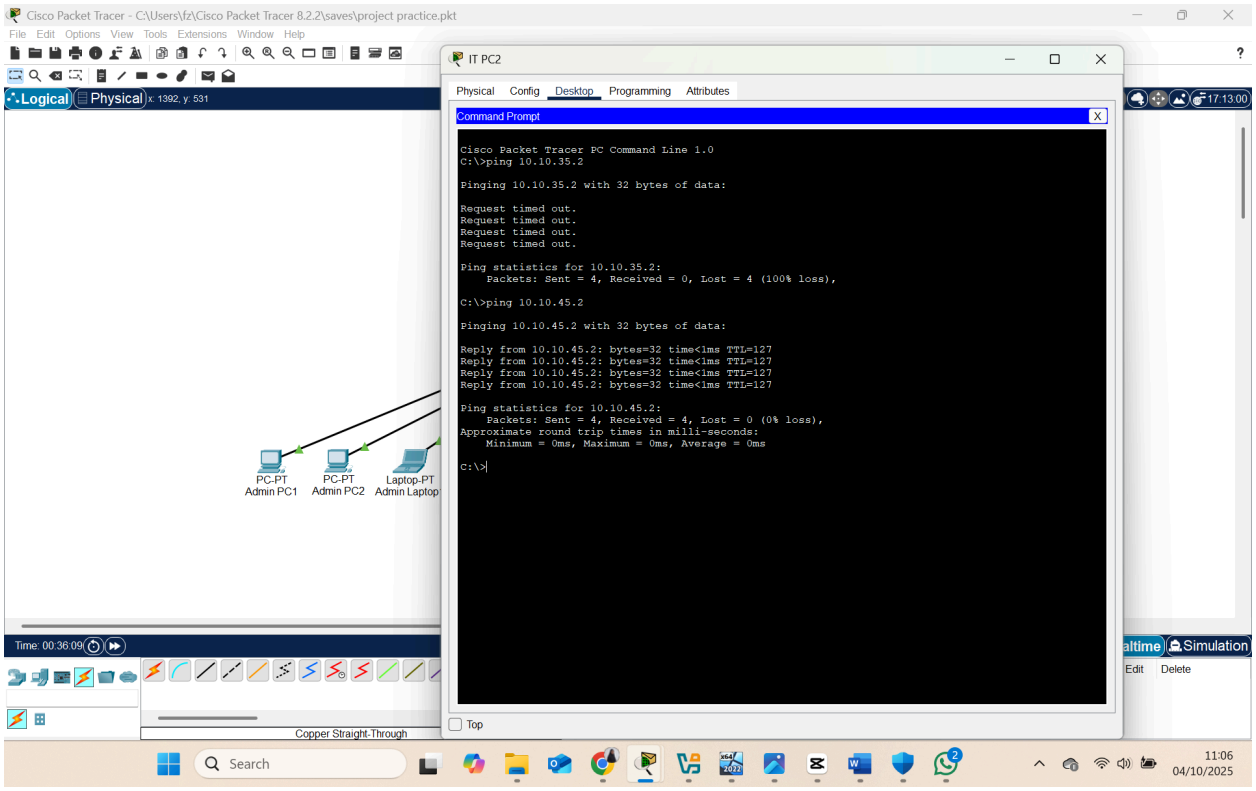


Sales to Admin: When I pinged Admin from Sales(ping 10.10.35.2), the result was “Destination host unreachable.”
This is because Sales traffic was explicitly denied from reaching Admin, so the echo request itself could not pass through.
Sales to IT: When I pinged IT from Sales(ping 10.10.55.2), the ping was successful. This confirms that Sales has permission to communicate with IT as there are no ACL restrictions preventing the traffic in that direction.



IT to Admin: Pinging Admin from IT(ping 10.10.35.2) also resulted in “Request timed out.” IT was able to send the request, but Admin could not reply because Admin-to-IT traffic was blocked by the ACL.

IT to Sales: When I pinged Sales from IT, the ping was also successful. IT VLAN has unrestricted access, so it can reach both Sales and Admin without any restrictions.



Security Justification:

- The successful and failed pings prove that traffic is filtered based on department needs.
- Sensitive Admin resources are protected from unauthorized access.
- IT retains full access for administrative tasks.
- ACL match counts validate that the filtering is active and effective, ensuring the principle of least privilege is maintained.

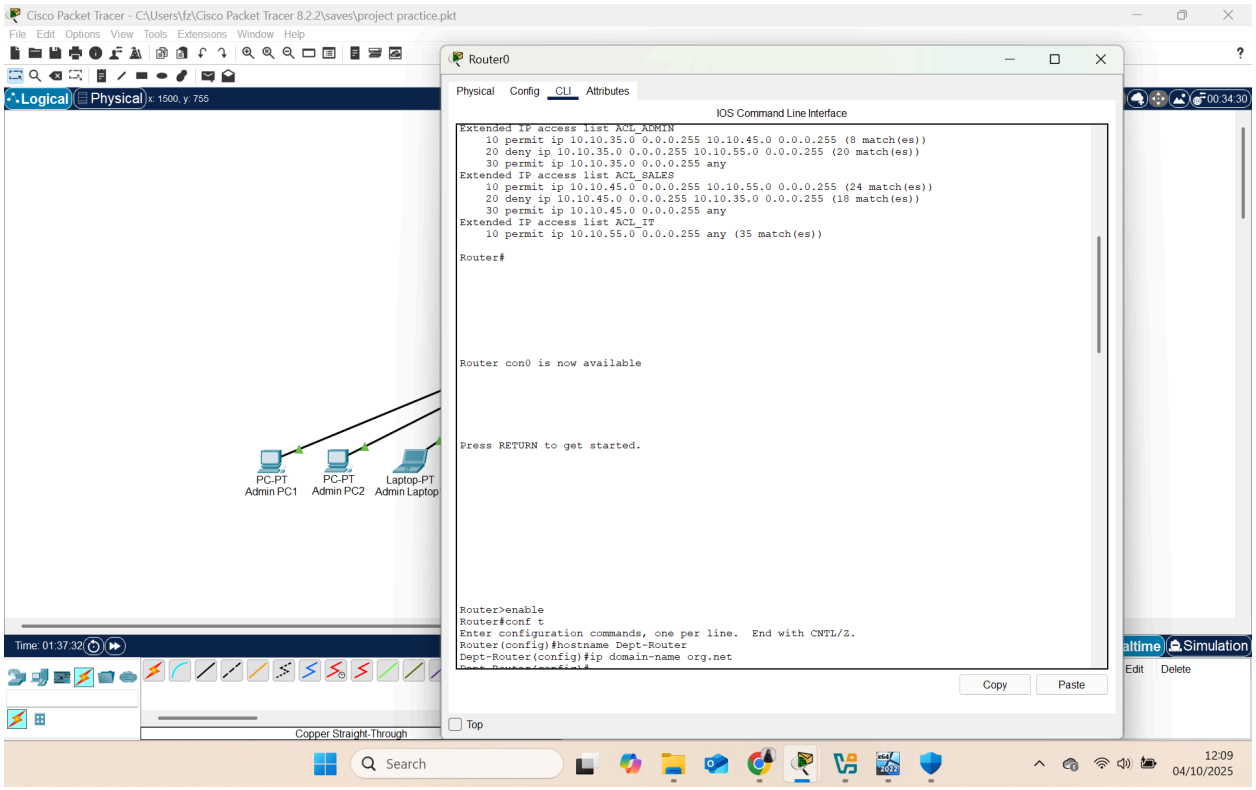
Step 8: Enabling Secure Remote Access (SSH)

In this step, I secured remote management of the network devices by enabling **Secure Shell (SSH)** and disabling insecure protocols like Telnet. I generated RSA encryption keys, created a local administrative user account, and configured the VTY lines to accept SSH connections only. This ensures encrypted communication between administrators and the network devices.

Firstly, I started with the basic device configuration and domain name setup.

Commands used: on router
enable

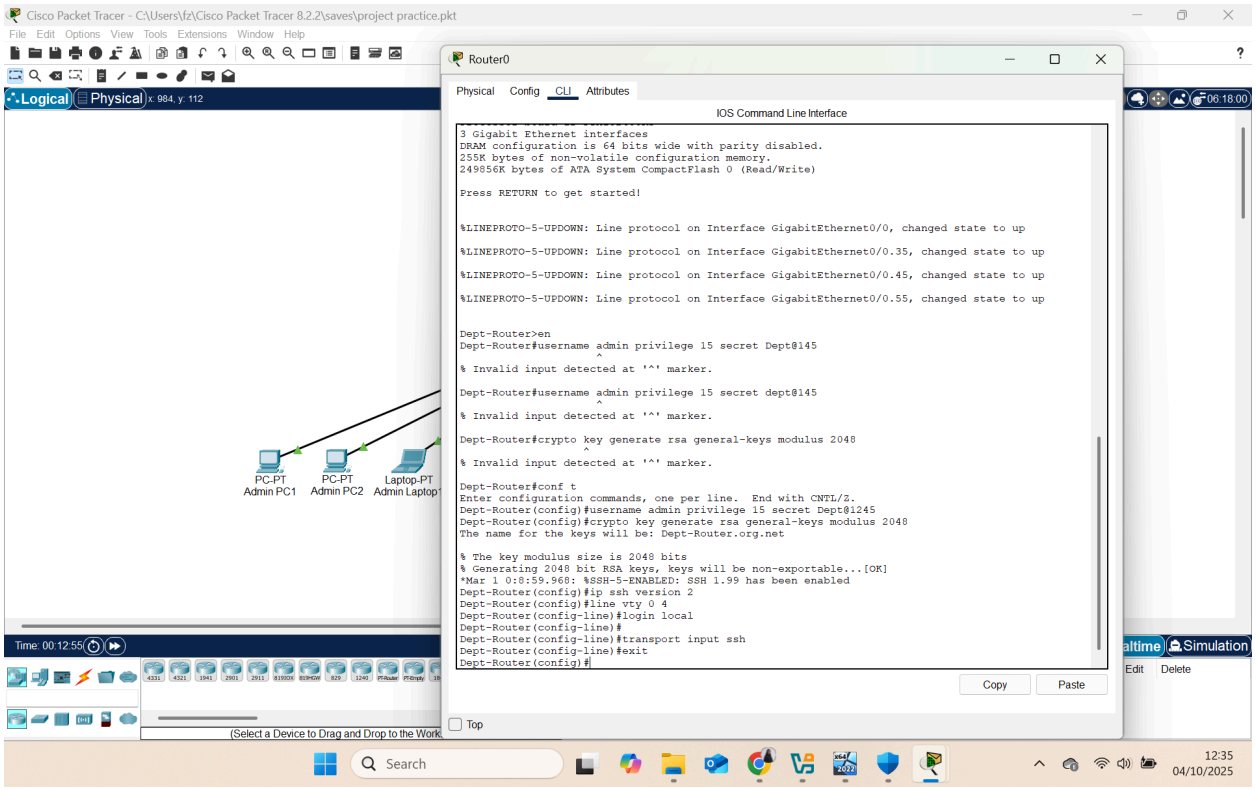
conf t
 hostname Dept-Router
 ip domain-name org.net
exit



Then, I enabled SSH authentication and encryption. I then configured VTY lines for SSH-only access while disabling Telnet.

Commands used: on router
en
conf t
 username admin privilege 15 secret Dept@1245
 crypto key generate rsa general-keys modulus 2048
 ip ssh version 2
 line vty 0 4
 login local
 transport input ssh

exit



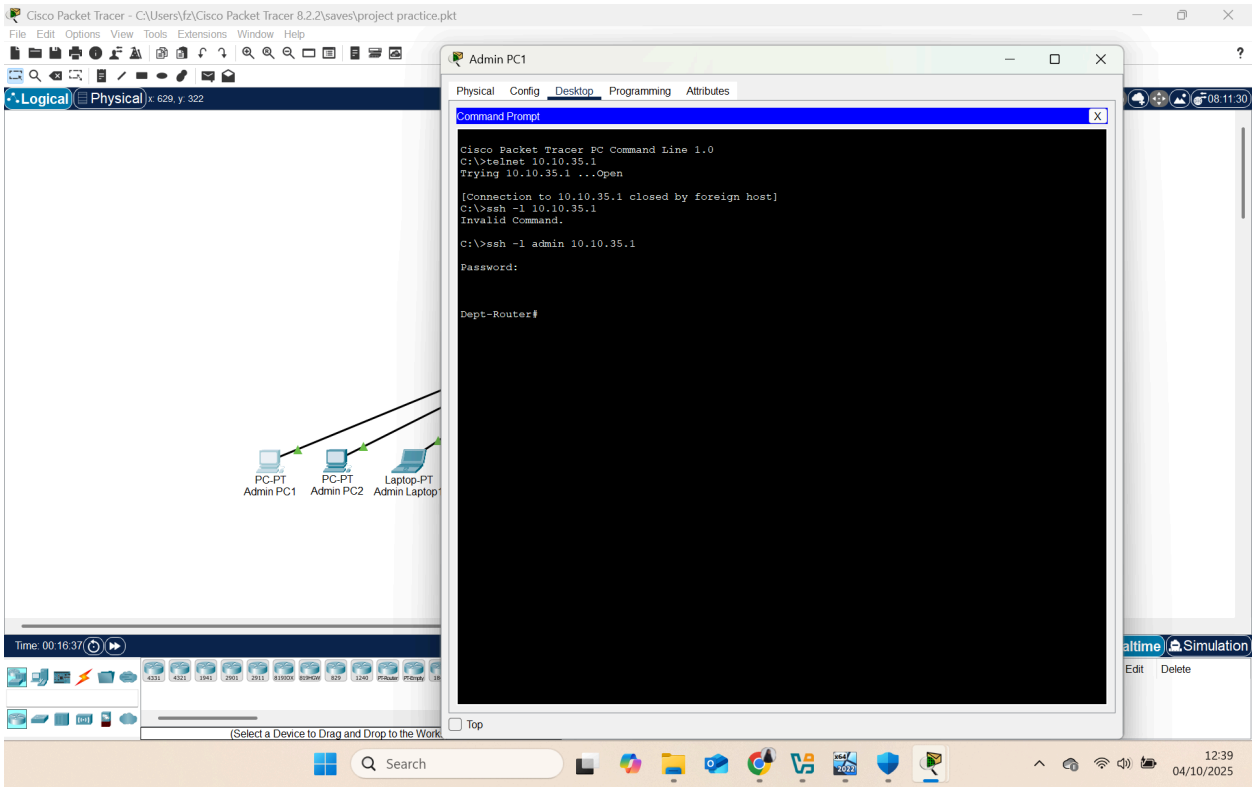
Step 9: Verifying SSH Configuration

In this step, I confirmed that the settings are working correctly to ensure that only secure remote access (SSH) is allowed and that Telnet is disabled.

To verify, I accessed the CLI of one of my end devices(Admin PC1) and used the following command: **telnet 10.10.35.1**
I got the response;
Trying 10.10.35.1 ... Open
Connection to 10.10.35.1 closed by foreign host
This confirms that the Telnet service was rejected, confirming that Telnet has been successfully disabled on the router.

Then I ran the command: **ssh -l admin 10.10.35.1**
I was prompted to enter my password, and after that I got
Dept-Router#

This indicates that the SSH configuration was successful and I have gained access to the router securely.



SECURITY IMPLICATIONS OF MISCONFIGURATION

A misconfigured network can expose sensitive resources to unauthorized access. For example, if ACLs are not properly applied, the Sales department could access Admin resources containing HR and financial data. If Telnet is not disabled, attackers could intercept login credentials sent in plain text. Similarly, an unsegmented network would allow unrestricted access across departments, increasing the risk of insider threats or lateral movement in case of a breach.

CONCLUSION

This project successfully demonstrated how I designed and secure a small enterprise network. I segmented the network using VLANs, enabled inter-VLAN routing with Router-on-a-Stick, and applied ACLs to enforce communication policies between departments. I also configured SSH for secure remote access while disabling Telnet to reduce vulnerabilities. Overall, the implementation improved network security, controlled traffic flow, and ensured proper access between different departments.