#### Network Infrastructure Design and Implementation for a Small Business

*Jan 2025 - Present*

***Freelance Network & IT Support | Small Business Project***

NOTE:

This is a simulated real-world project based on work I’ve done for a small business. For privacy and security reasons, IPs and topology have been modified while keeping the configurations and challenges realistic.

This project involved designing and implementing a secure and scalable network infrastructure for a small business using Cisco networking technologies. It was completed as part of freelance technical support for a small business aiming to improve its internal network reliability, security, and segmentation. The goal was to optimize communication between departments while ensuring basic network security.

#### Business Overview

The business has 8 employees spread across four departments: Sales, Inventory, Management, and Owner. The premises also include a CCTV system.

#### Requirements

1. Internal communication between departments
2. Internet access for all users
3. Segregation of departments via VLANs
4. Secure access to CCTV
5. Scalability for future devices

#### Network Devices

Sales– 2 PCs (Billing and Inventory updates)

Inventory – 1 PC

Management – 2 PCs (Admin + Accounts)

Owner – 1 PC

CCTV – 1 DVR

Printer – Shared via Management VLAN

**Total:**

5 PCs

1 Printer

1 DVR

1 Router

1 Switch

#### IP addressing

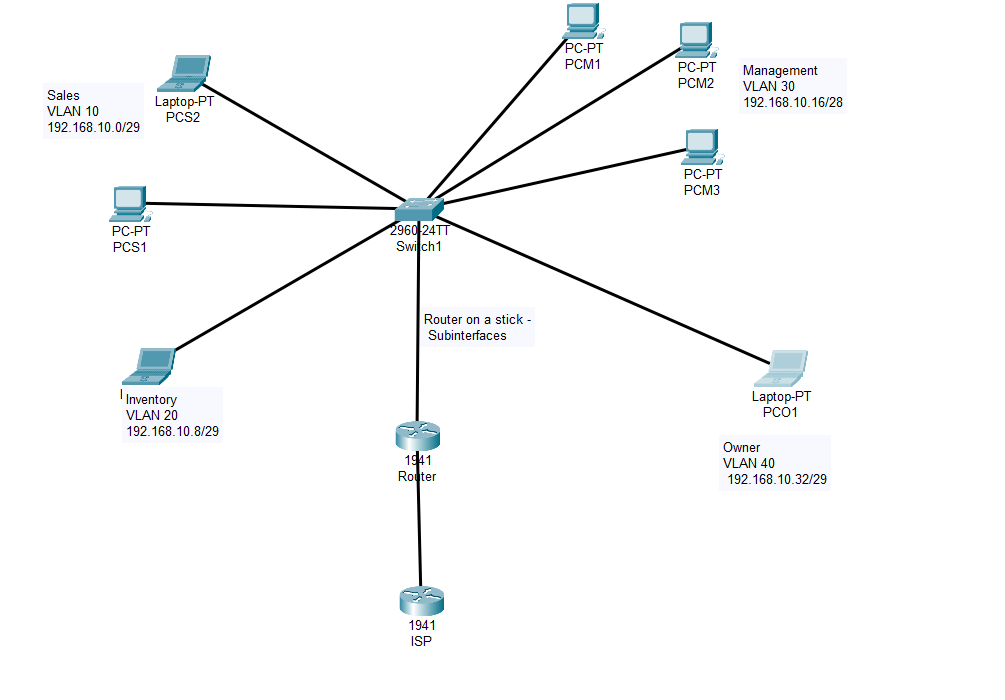
Purchased Public IP: 74.125.50.10/30

The internal IP addressing was designed using private IPv4 ranges optimized with subnetting to reduce wastage. The router uses a single physical interface configured with multiple sub-interfaces for inter-VLAN routing, ensuring departmental isolation and security. Each department is allocated just enough IP addresses with room for slight future expansion.

Private IP addressing:

| VLAN | Dept | Needed | Subnet | Usable IPs | Gateway | Available hosts |
| --- | --- | --- | --- | --- | --- | --- |
| 10 | Sales | 2 | 192.168.10.0/29 | .1 to .6 | 192.168.10.1 | 6 |
| 20 | Inventory | 1 | 192.168.10.8/29 | .9 to .14 | 192.168.10.9 | 6 |
| 30 | Management | 3 + printer | 192.168.10.16/28 | .17 to .30 | 192.168.10.17 | 14 |
| 40 | Owner | 1 | 192.168.10.32/29 | .33 to .38 | 192.168.10.33 | 6 |

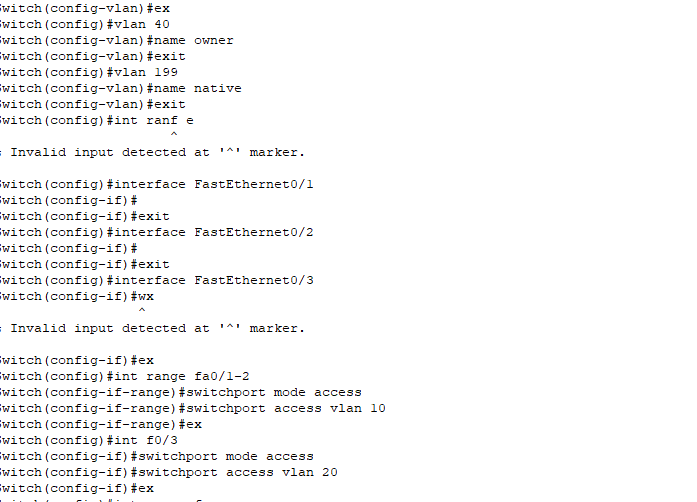
#### Network Topology



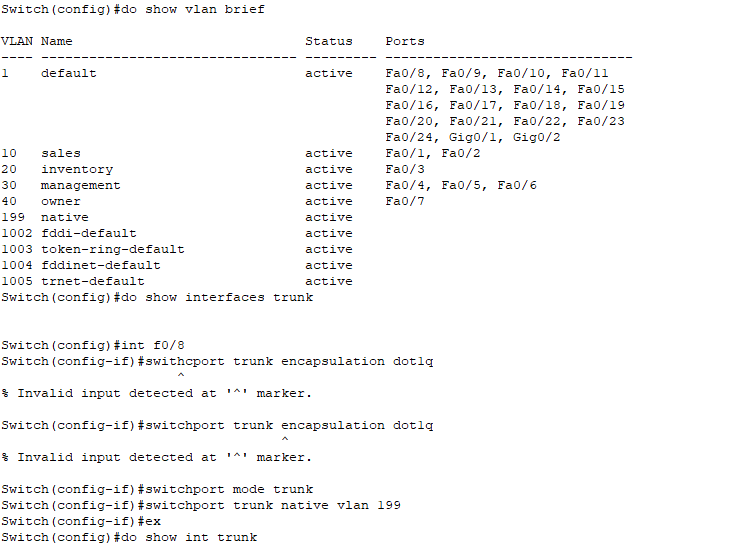
#### Configuration

Initially, for clarification purposes I configured the IP addresses of PCs statically.

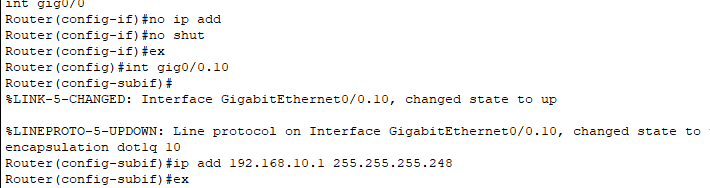
I proceeded to configure the various vlans on the switch.

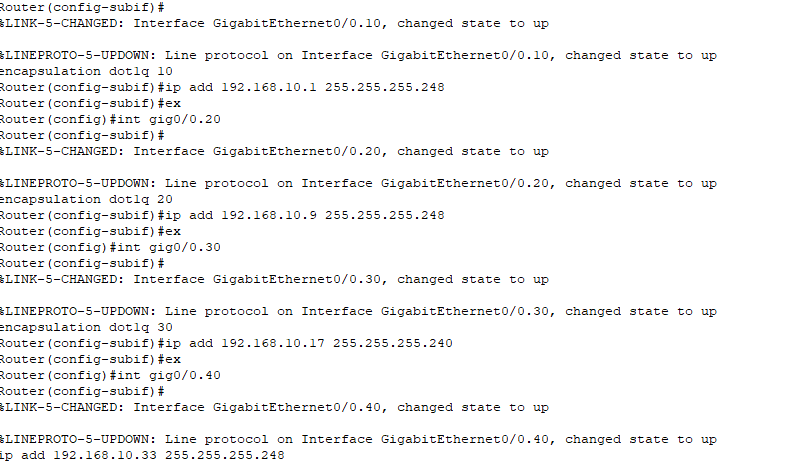


The final vlan table is as follows:

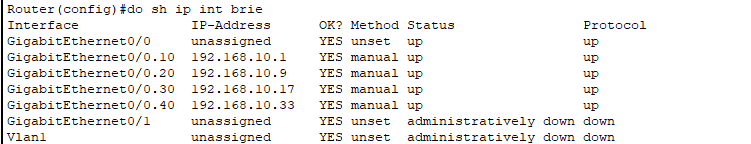


What remained was the router configuration, since we are using router on a stick configuration, I added sub interfaces and assigned them the addresses that will act as default gateways for the PCs.



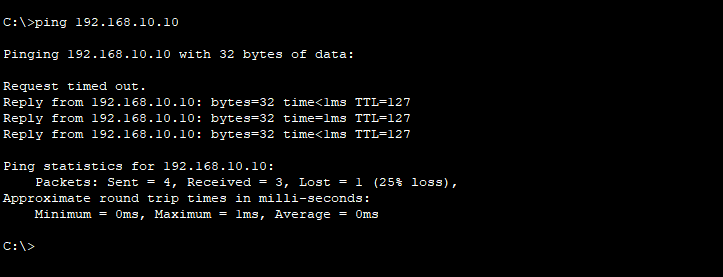


The final interface table

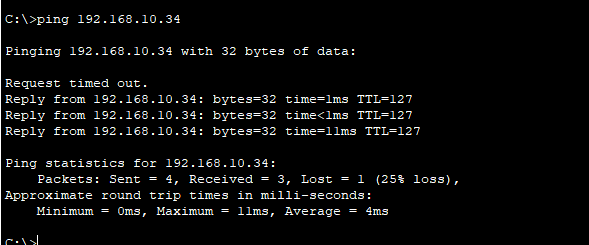


#### Checking connectivity

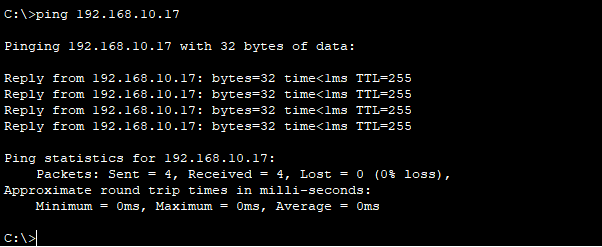
Pinging inventory pc from sales



Sales to owner



Sales to management



After a few more different pings from different PCS, I concluded that the topology is fully connected.

#### NAT for internet access

The public IP purchased by the business is 74.125.50.10/30 . Due to the greater number of PCs, I decided to use PAT.

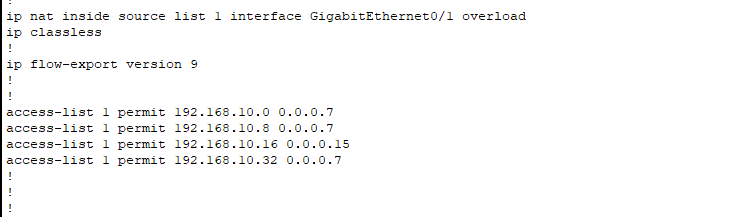
Int gig0/1 has IP 74.125.50.10

ISP has taken IP 74.125.50.9

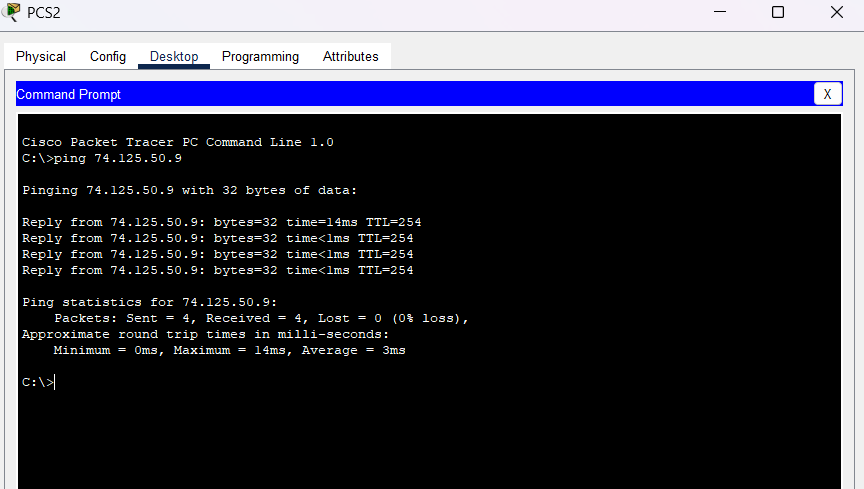
I configured nat normally, on all the sub interfaces as “ip nat inside”

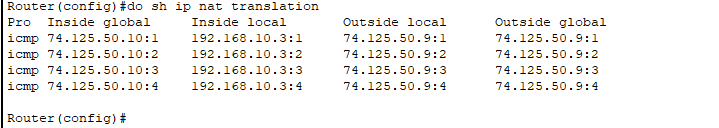
Configured public IP on interface of router gig0/1. Applied “ip nat outside”.

The ACL1 was configured for nat. It included all the users that need to be natted (inside users).



Then I added a default route on our router to the ISP and checked internet connectivity of all PCs. It worked.



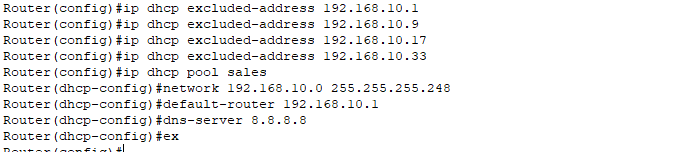


Now NAT works and every device has internet connectivity.

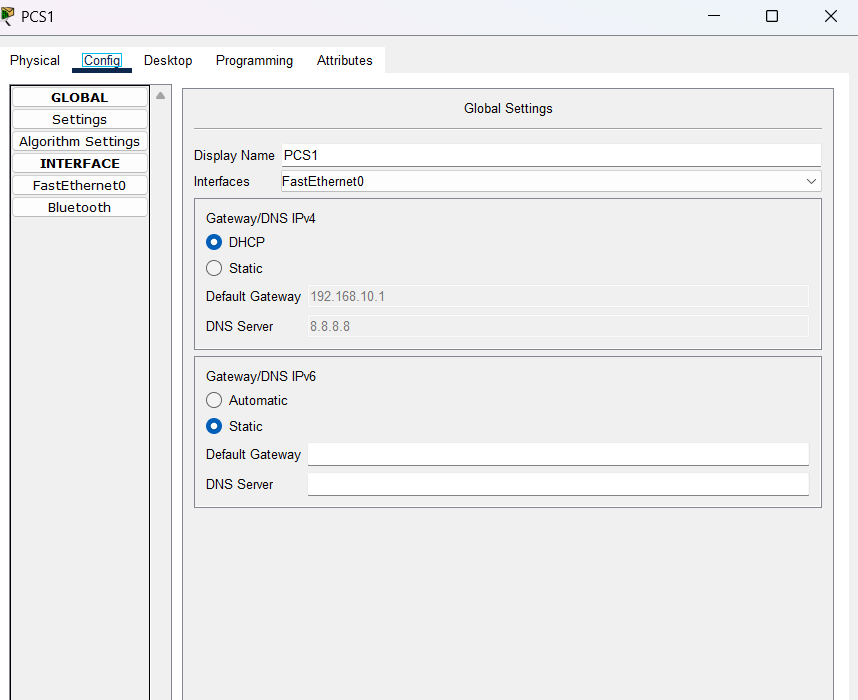
#### DHCP

Although VLANs were implemented from the beginning to ensure logical segmentation and improved network management, static IP addressing was initially applied to end devices for greater control during early configuration and troubleshooting phases. However, maintaining static IPs across multiple VLANs quickly becomes impractical in due to increased administrative overhead and the risk of misconfiguration. To reflect a scalable and efficient design typical of small business networks, the router was configured to act as a centralized DHCP server. Separate DHCP pools were created for each VLAN, allowing client devices to receive IP configurations dynamically. This approach reduces manual effort, minimizes errors, and supports future growth without the need for readdressing.

IP addresses assigned to key infrastructure devices such as router interfaces were manually excluded from DHCP allocation using ip dhcp excluded-address to prevent address conflicts.



Similarly, I configured the other pools for other vlans and then proceeded to change the configurations on the PCs to DHCP.



### Network Security

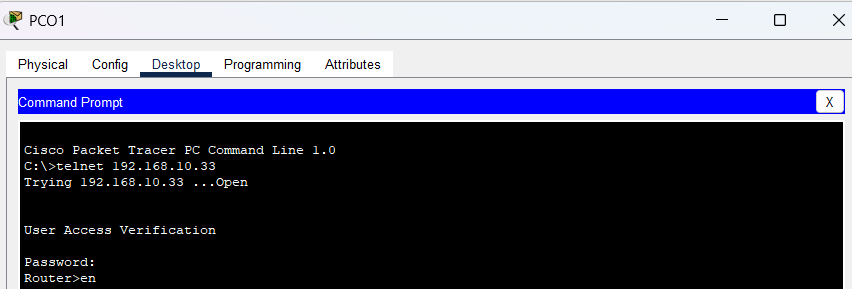
#### ACLs

Access Control Lists were introduced according to the business needs for added security.

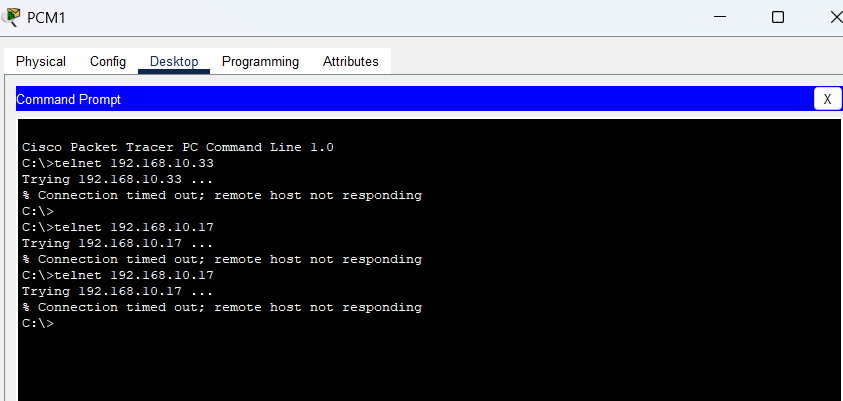
1. Only the Owner and Admin (me) can access the router using Telnet  
   To avoid anyone playing around with the router settings, Telnet access is only allowed from the Owner VLAN and my remote IP. This way, only trusted devices — mine and the Owner’s — can manage the router.

I had to include the whole owner dhcp pool in the acl to avoid any future conflicts.

The owner can telnet to the router



The other PCs cannot telnet to the router

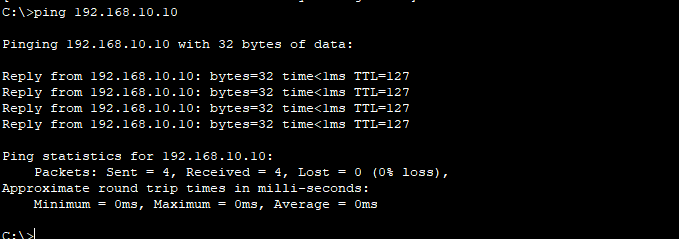


1. Limit Access to Inventory VLAN (VLAN 20).

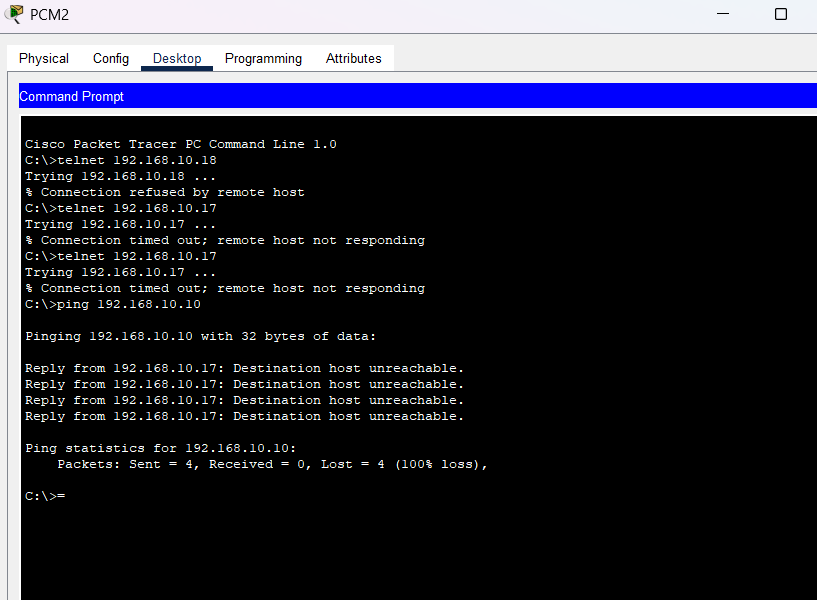
ACL Number: 120  
Objective:  
To restrict access to sensitive inventory systems so that only authorized departments — Sales (VLAN 10) and Owner (VLAN 40) — are able to access it.

Sales and the Owner are the only ones who actually need to interact with inventory data. Blocking other VLANs helps keep things clean, organized, and prevents unnecessary access.

We can see that owner can now ping inventory



We can see, management PC cannot ping the inventory

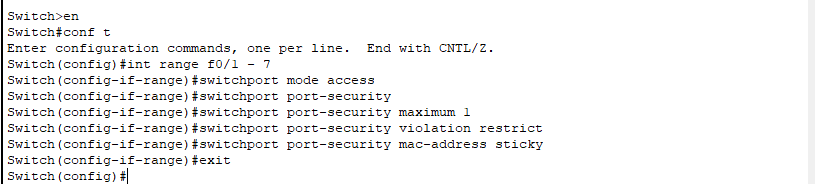


#### Port Security

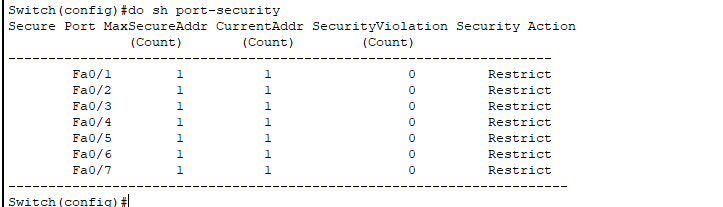
Port security was implemented on access layer switch ports to ensure that only authorized devices can connect to the network. Since each department has a fixed number of devices, this helps prevent unauthorized access in case someone tries to plug in an unknown device into a free Ethernet port. For example, the Sales department has three PCs, so only three MAC addresses are allowed per relevant port. If more are detected, the port will shut down as a security measure.

This adds a basic but effective layer of protection to the internal network and aligns with the business's need for better access control without requiring major infrastructure changes.

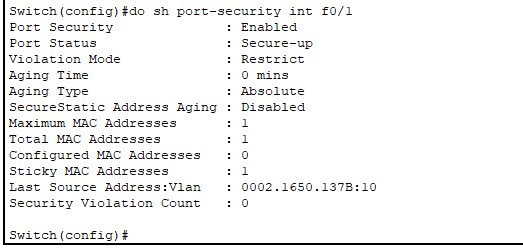
Configuration



Verification



Verification per interface



#### Conclusion

This project was designed to replicate the kind of network infrastructure and security implementation typically required by small businesses, with a focus on practicality, scalability, and realistic constraints. Every decision — from subnetting to ACLs to NAT — was made with the goal of balancing performance and manageability, while maintaining security.

Though the environment was simulated, the setup reflects real-world standards, especially for businesses operating on a modest scale without dedicated IT staff. The network supports multiple departments with clear segmentation, ensures internet access for all users, and protects sensitive systems like inventory and the router itself from unauthorized access.

Security measures such as **access control lists**, **port security**, and a **centralized DHCP setup** bring the network in line with best practices, while keeping it lightweight enough for a small business to maintain. The design also leaves room for scalability — both in terms of additional users and the possibility of cloud integration or future redundancy.

Going forward, improvements such as intrusion detection systems (IDS), SIEM integration, or extending services to the cloud can further enhance security and resilience. However, as it stands, this project represents a solid, production-ready network model for small businesses and acts as a personal proof-of-capability in secure network design and implementation.