

SMALL OFFICE HOME OFFICE (SOHO)

Network Design and Implementation

### 

### **📘 Overview**

This project focuses on designing and implementing a Small Office/Home Office (SOHO) network to provide efficient and secure connectivity for a small business environment. The network is designed to support essential business operations, including internet access, file sharing, and communication between employees.

The main objective of this project is to create a reliable and cost-effective network infrastructure that ensures seamless connectivity, data security, and ease of management. The network includes devices such as routers, switches, wireless access points, computers, and network printers.

The design involves IP addressing, subnetting, configuration of DHCP and NAT services, and implementation of wireless network security protocols (WPA2). The network topology was tested to ensure performance, scalability, and fault tolerance.

Upon completion, the SOHO network provides users with stable internet connectivity, secure data transmission, and efficient resource sharing, meeting the functional needs of a small office environment.

### **🎯 Objectives**

* **Segment the network** into four VLANs — Administration, HR, IT, and Guest — for organized and secure communication.
* **Enable inter-VLAN routing** among Administration, HR, and IT VLANs while **restricting Guest VLAN** to Internet-only access.
* **Provide reliable Internet connectivity** through a WAN link between the internal router and ISP router.
* **Implement core services** like DHCP, NAT, and basic firewall rules for automated addressing and security.
* **Test and validate** VLAN communication, Internet access, and access control policies.
* **Document** topology, configurations, and results for reproducibility and learning.

### **🧠 Scope & Description**

The project focuses on designing, configuring, and testing a **layered SOHO network** suitable for a small organization environment.

**In Scope:**

* VLAN creation and configuration on switches.
* Inter-VLAN routing via Router-on-a-Stick.
* DHCP and NAT configuration on Router.
* WAN link setup between Router and ISP.
* Guest VLAN restricted to Internet access only.
* Network validation through connectivity and security testing.

**Out of Scope:**

* Enterprise-level routing protocols (OSPF, BGP)
* Redundancy, load balancing, or advanced IDS/IPS systems.

## ⚙️ Technologies & Protocols Used

* **Devices:** Cisco 2811 Routers, 2960 Switches, Access Point, PCs, Laptops, Smartphones
* **Protocols:** VLAN, IEEE 802.1Q, DHCP, NAT, Inter-VLAN Routing, Static Routing
* **Security:** VLAN isolation, Guest access restriction, Basic ACLs
* **Software:** Cisco Packet Tracer (for simulation)

### **🧩 Network Topology**

### **🌐 IP Addressing Plan**

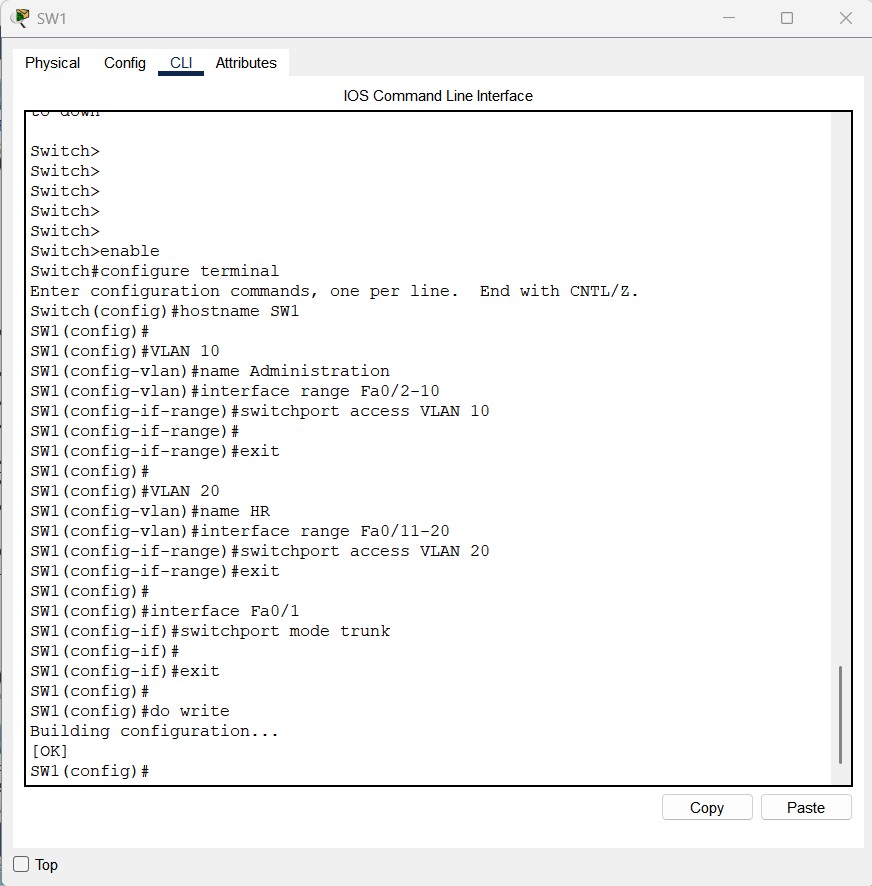
Since the Internet Service Provider (ISP) has provided a single public IP address — **15.0.0.1** — we will utilize a private IP range, **192.168.10.0/24**, to create our internal network. To efficiently organize and manage network traffic, we will perform **subnetting** on this range.

Given that the network design includes **four distinct VLANs**, the **192.168.10.0/24** network will be divided into **four separate subnets**, each corresponding to a specific VLAN.

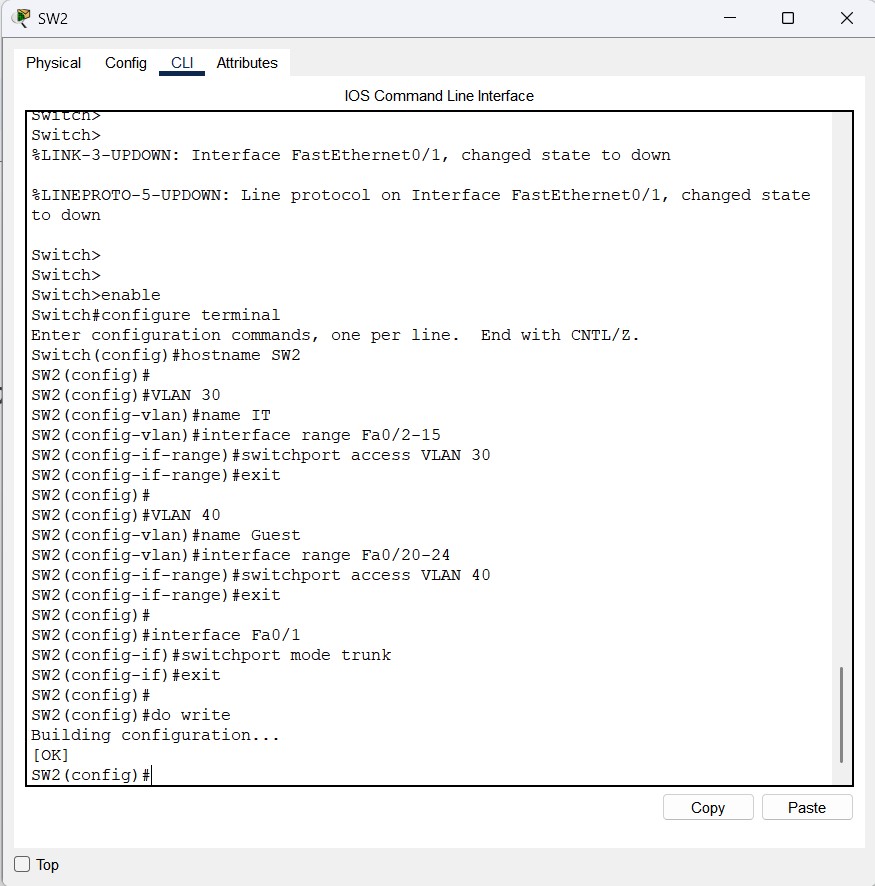
| **VLAN** | **Network/Subnet** | **Gateway** |  | **Access** |
| --- | --- | --- | --- | --- |
| VLAN 10 | 192.168.10.0/26 | 192.168.10.1 |  | Inter-VLAN + Internet |
| VLAN 20 | 192.168.10.64/26 | 192.168.10.65 |  | Inter-VLAN + Internet |
| VLAN 30 | 192.168.10.128/26 | 192.168.10.129 |  | Inter-VLAN + Internet |
| VLAN 40 | 192.168.10.192/26 | 192.168.10.193 |  | Internet Only |

### **🧩Configuration**

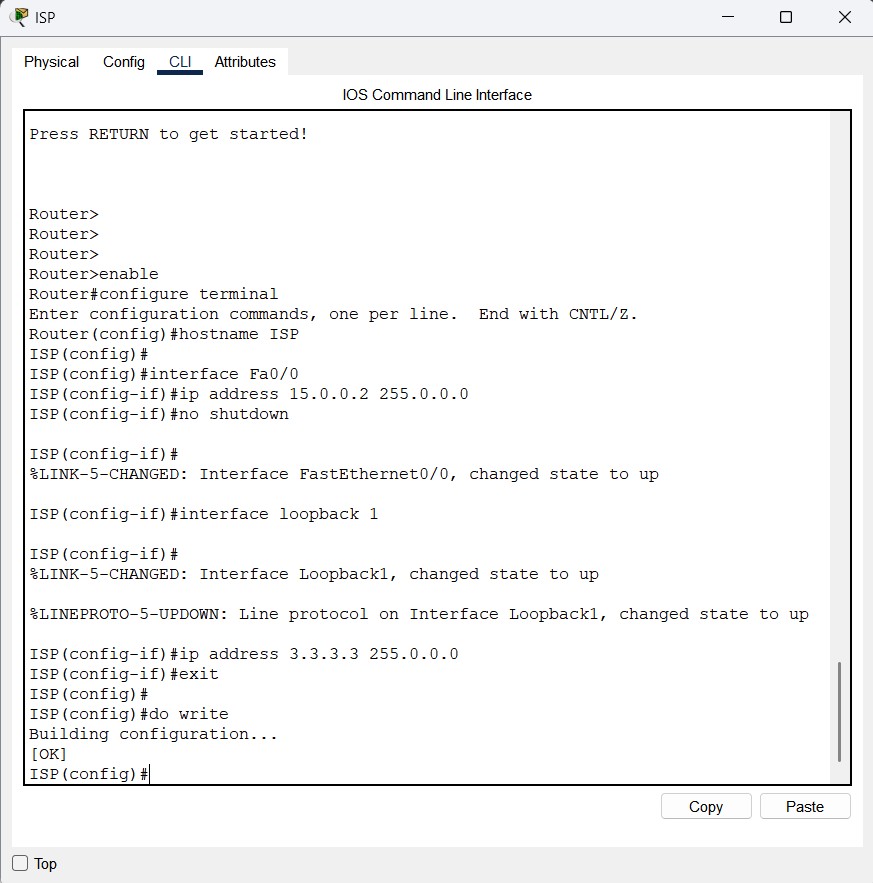
Switch - SW1



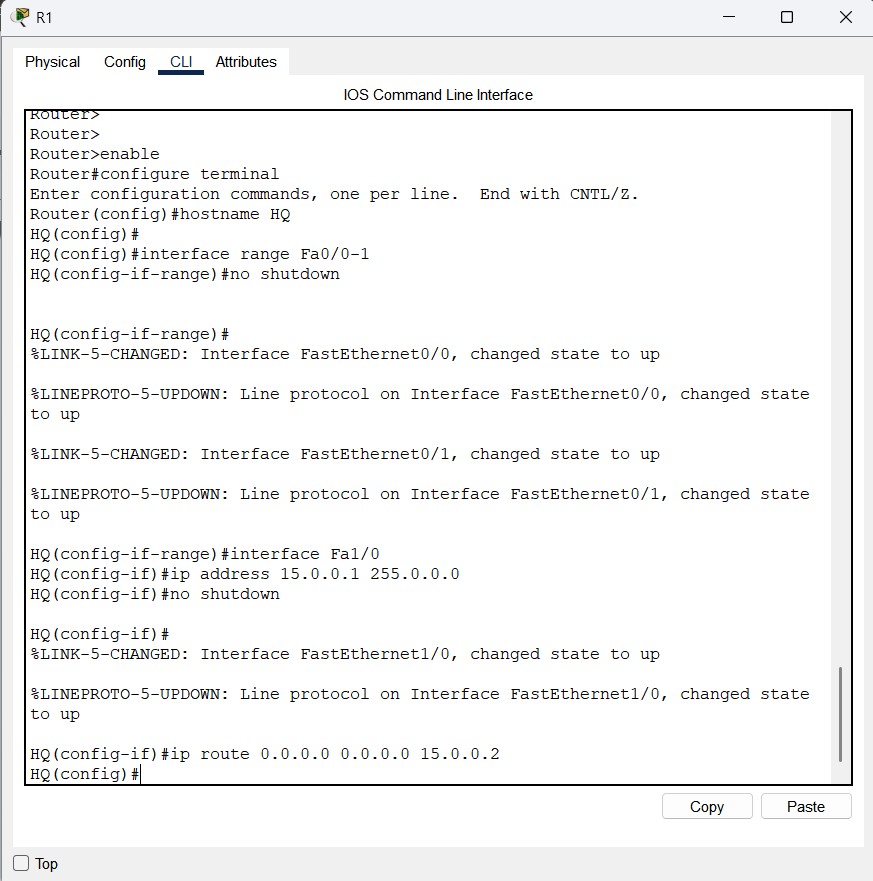
Switch SW2

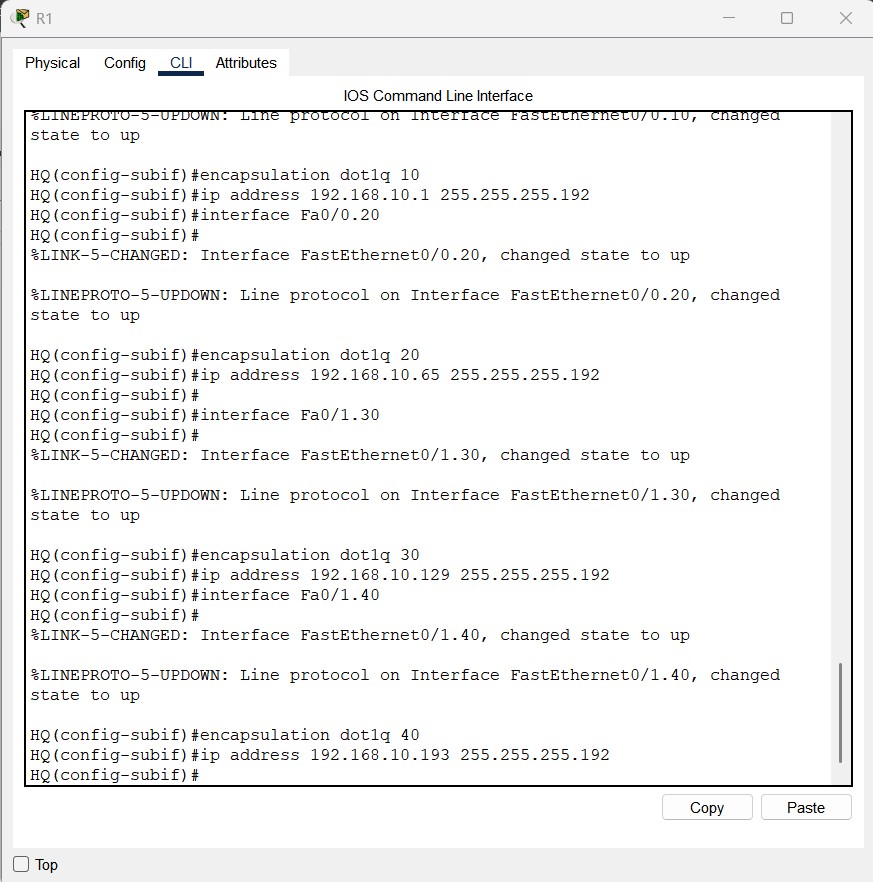


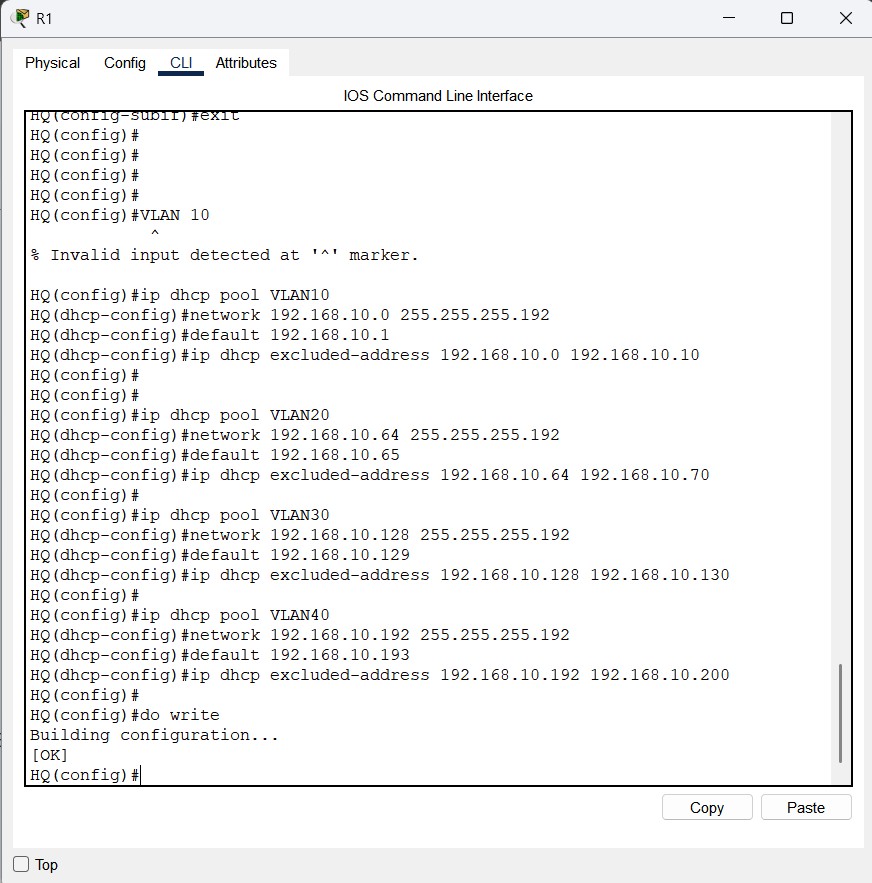
Router - ISP

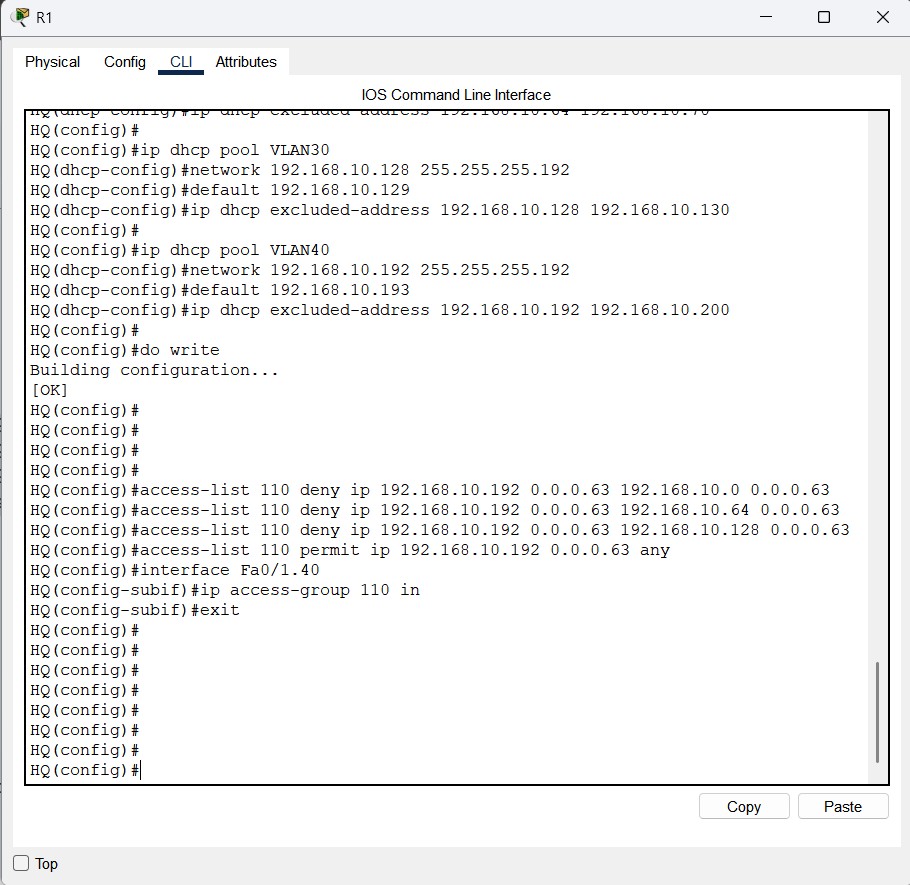


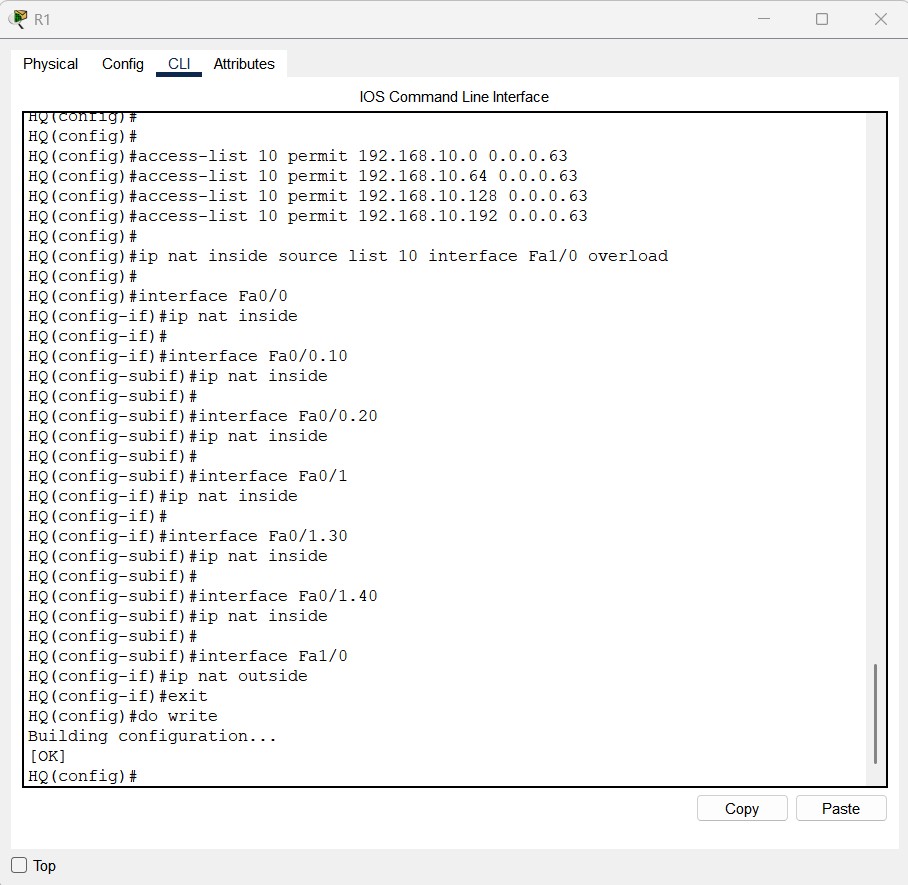
Router - HQ

Initial Config

Inter-VLAN Config

DHCP Config

ACL Config

NAT Config

I am also sharing a document that contains all the configurations implemented in this project.

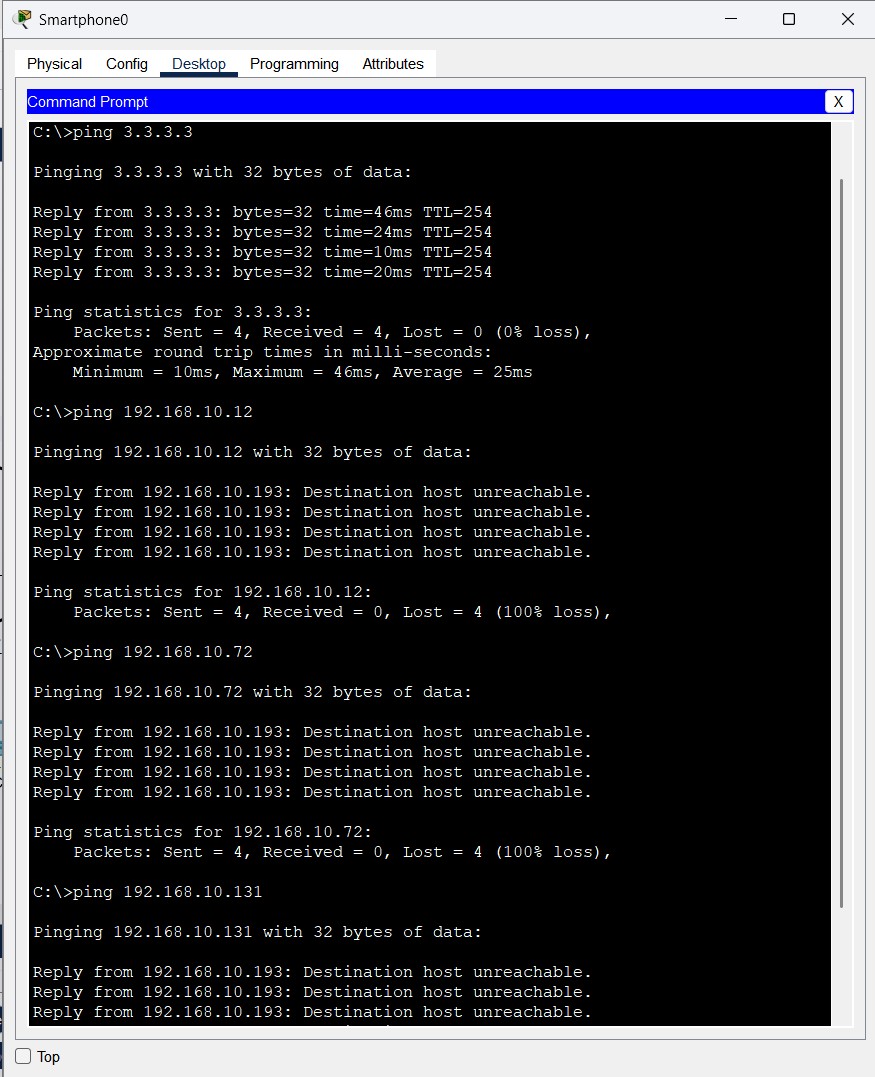
[Project\_SOHO\_Config](https://docs.google.com/document/d/1w4UBQmEKcKKQCfoJOvhCZsZ-khrRRSHqe5TR5dPnHqc/edit?usp=sharing)

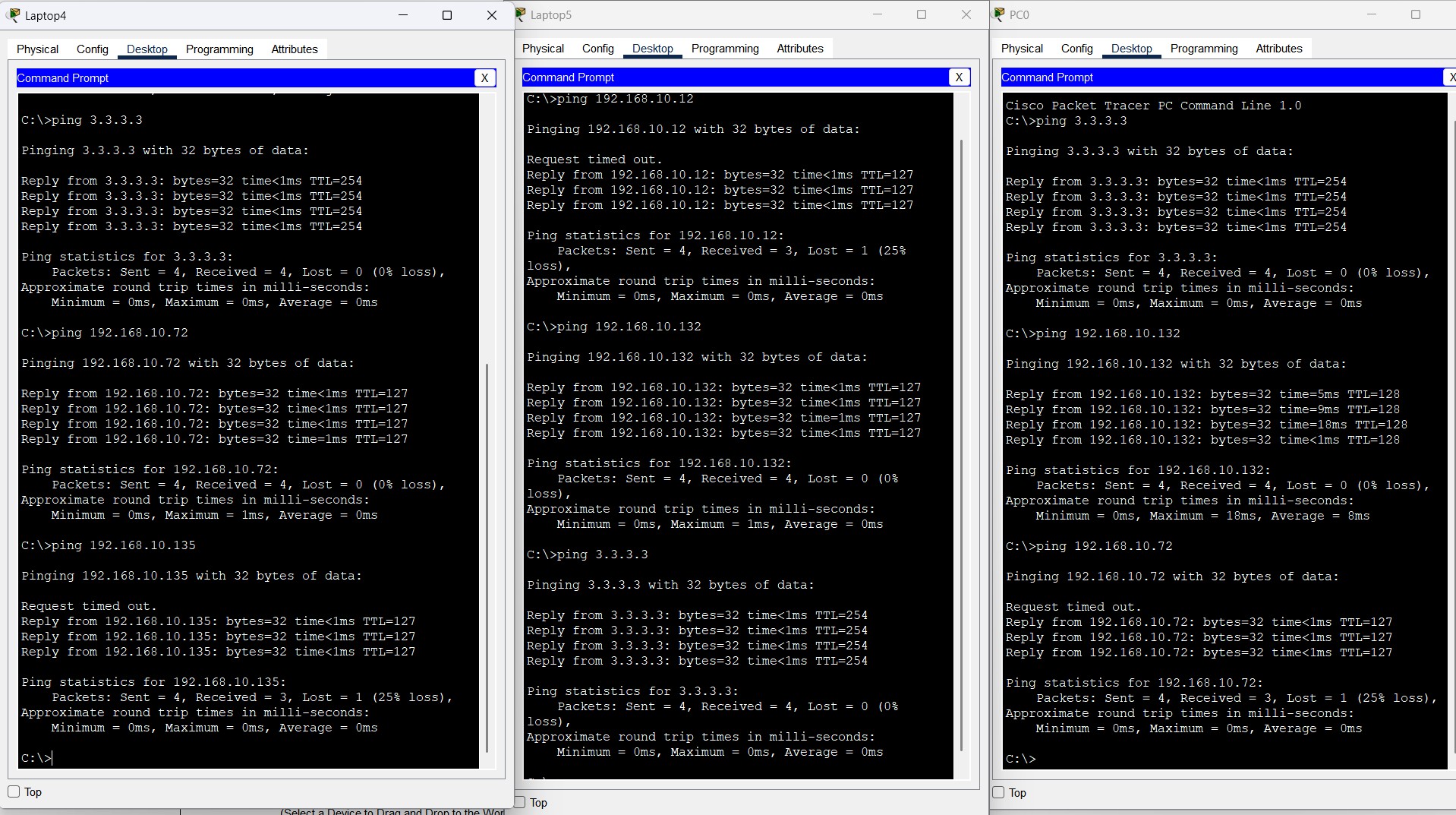
### **🔧 Implementation Steps**

1. **Created VLANs (10, 20, 30, 40)** and assigned ports on switches.
2. **Configured trunk ports** between switches and router (802.1Q encapsulation).
3. **Set up Router-on-a-Stick** for inter-VLAN routing on R1.
4. **Assigned IP addresses** and gateways for each VLAN.
5. **Enabled DHCP** for automatic IP assignment per VLAN.
6. **Configured NAT** and WAN link for Internet connectivity.
7. **Applied ACLs** to restrict Guest VLAN to Internet access only.
8. **Tested connectivity** using ping and browser simulation between VLANs and Internet.

### **🧪 Testing & Validation**

* Verified inter-VLAN communication between VLAN 10, 20, and 30.
* Confirmed Guest VLAN users could only reach Internet hosts.
* DHCP leases validated for all VLANs.
* NAT translation tested with successful Internet access.
* ACL verification ensured Guest VLAN isolation.

VLAN 40 

VLAN - 10,20,30

### 

### 

### 

### 

### 

### 

### **🔐 Security Considerations**

* VLAN-based segmentation reduces broadcast traffic and limits lateral movement.
* ACLs on R1 prevent Guest VLAN access to internal subnets.
* NAT hides internal IPs from external networks.
* WPA2/3 encryption configured on Guest Wi-Fi.

### **🚀 Results & Observations**

* All VLANs successfully connected as per design.
* Internet access functional through R1–ISP link.
* Guest VLAN isolated from internal networks.
* Network achieved stable performance and security goals.

### **🔮 Future Enhancements**

* Introduce **VPN access** for remote employees.
* Implement **VLAN-based QoS** for bandwidth optimization.
* Add **redundancy and monitoring tools** (SNMP, Syslog).
* Configure **static routing or OSPF** for scalability.

### **🏁 Conclusion**

The SOHO network successfully delivers a secure, scalable, and efficient multi-department setup. VLAN segmentation, routing, and access control have been effectively implemented, providing a robust foundation for small-scale organizational networking.