**Project Title:**

**Network Segmentation and Security in Enterprise Environments**

**Project Overview:**

This project focuses on creating a segmented network architecture that enhances security by segmentation, isolating sensitive data, limiting unauthorized access, and controlling network traffic within an enterprise. By using technologies like VLANs (Virtual Local Area Networks), firewalls, and access control lists (ACLs), this project will ensure that different segments of the network will have appropriate security policies such as firewalls, VPN, IPSec implementations in place.

**Project Objectives:**

- Implement network segmentation to isolate critical systems and departments.
- Enhance security through firewalls, VLANs, and access control mechanisms.
- Reduce the attack surface area by limiting access to sensitive data and systems.
- Monitor and manage inter-segment traffic to ensure security compliance.
- Document network topologies, security policies, and configurations.

**Tools and Technologies:**

- **Network Devices**: Layer 2 Switches, Routers and Firewalls.
- **Software**: Cisco Packet Tracer, GNS 3.
- **Protocols**: TCP/IP, VLAN, Access Control Lists (ACLs), IPSec VPN, and SNMP.
- **Hardware**: Network Interface Cards, Servers, and Devices for testing.

**Project Phases:**

1. **Planning and Design:**

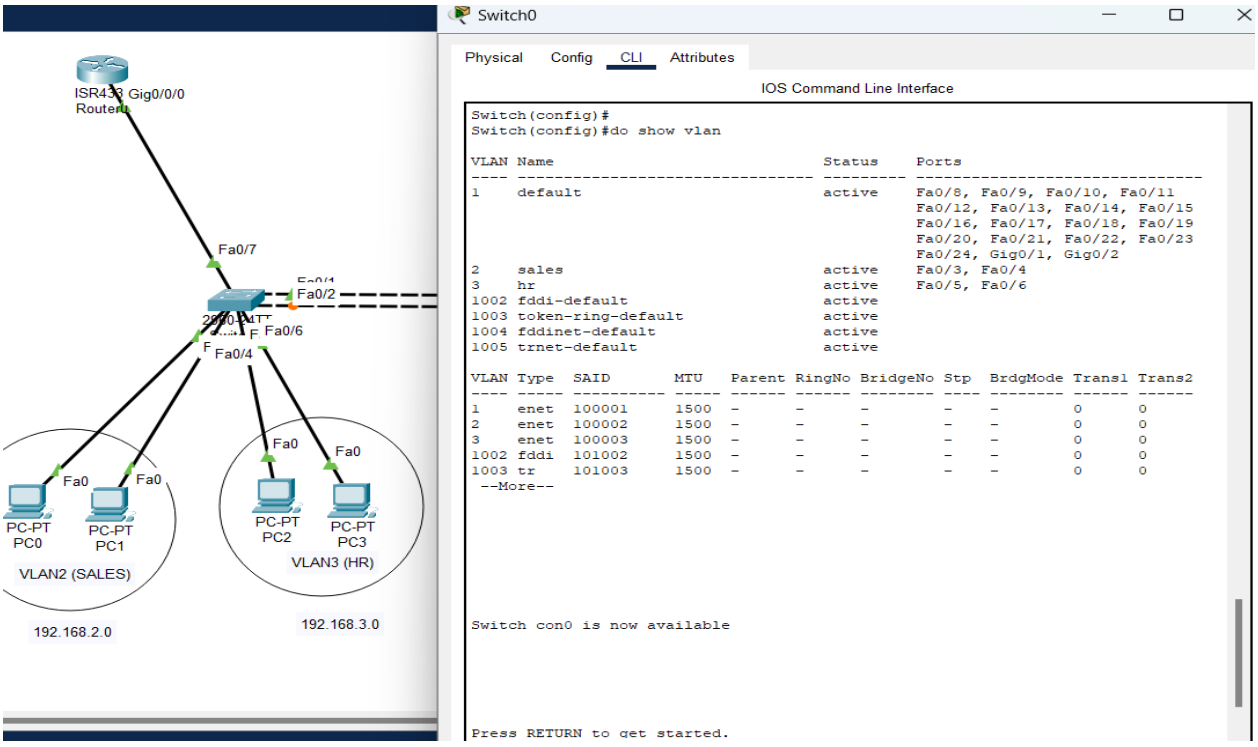
- **Assess Network Requirements**: Understand the existing network infrastructure and identify needs (e.g., isolating finance or HR departments).
- **Define Segmentation Strategy**:
    - **VLANs**: Create logical segments for different departments, such as **HR Dept**, **Sales Dept**, **and Guest Network**.
    - **Subnets**: Design subnets based on the size of each department, ensuring proper IP address allocation.

    - **Traffic Flow**: Define how traffic should be allowed or blocked between different segments using routing and firewall rules.
- **Security Objectives**: Determine security objectives for each network segment, such as access control, monitoring, and data protection.

**2. Network Segmentation Implementation:**

- **VLAN Configuration**: Implement VLANs on switches to logically separate traffic.
    - VLAN 2: SALES Department (fa0/3, fa0/4)
    - VLAN 3: HR Department (fa0/5, fa0/6)

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 2
Switch(config-vlan)# name SALES
Switch(config-vlan)# exit
Switch(config)# vlan 3
Switch(config-vlan)# name HR
Switch(config-vlan)# exit
Switch(config)# interface range fa0/3-4
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config)# exit
Switch(config)# interface range fa0/5-6
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 3
Switch(config)# end
Switch(config)# wr
```



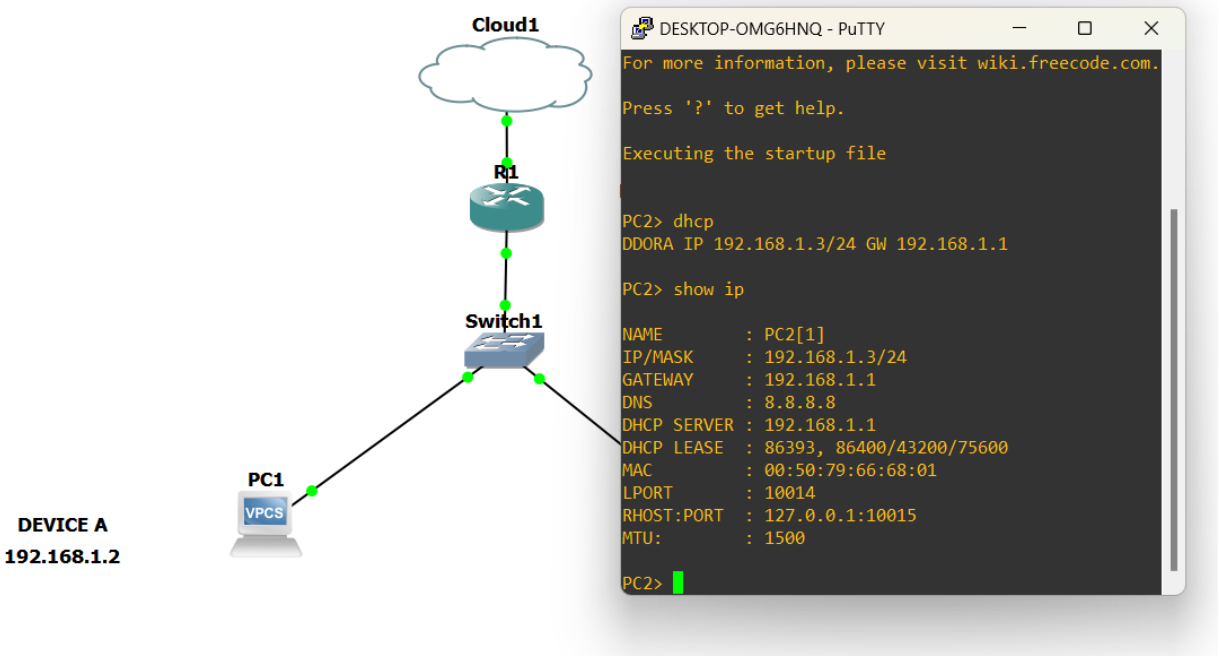

- **DHCP (on GNS 3):** Dynamic Host Configuration Protocol is a network protocol used to automatically assign IP addresses and other network configuration settings to devices (clients) on a network. It simplifies the process of configuring devices to communicate over IP networks.

  **DHCP CONFIG ON ROUTER**

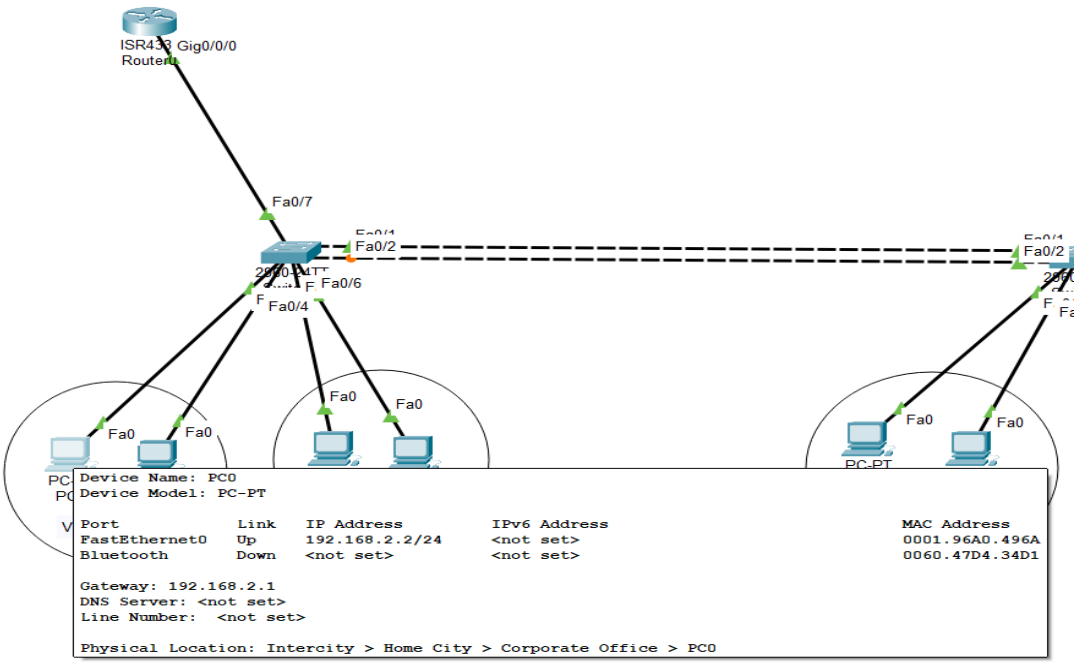
  ip dhcp pool head-office(name of your choice)

  network 192.168.1.0 255.255.255.0

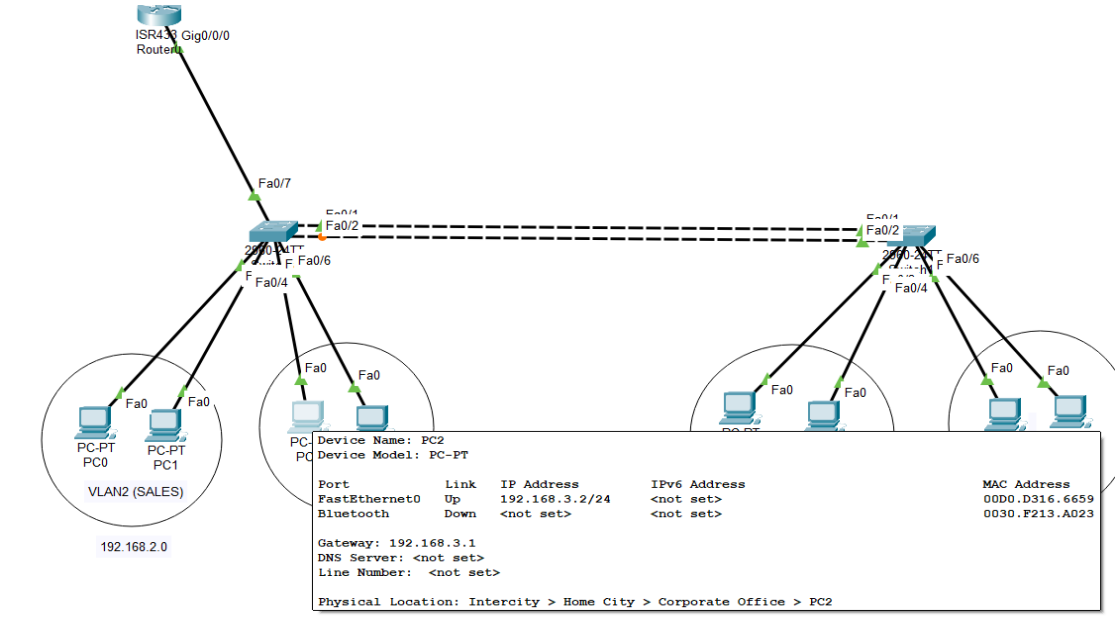
default-router 192.168.1.1
dns-server 8.8.8.8
exit
ip dhcp excluded-address 192.168.1.1 192.168.1.100



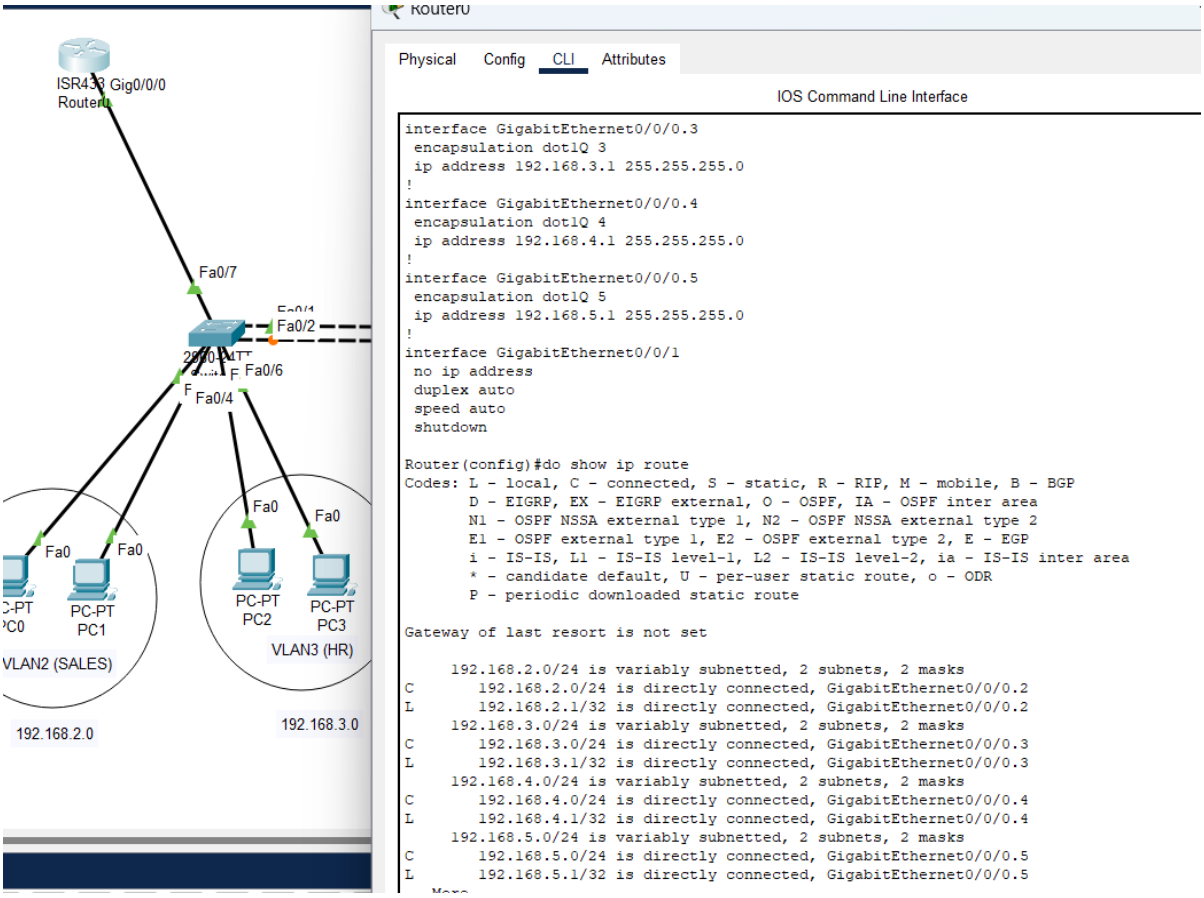

- **Subnetting**: Divide IP address ranges into smaller subnets to manage and limit network traffic. Assign IP address ranges
    - **Sales Dept: 192.168.2.0/24**

- 


  - **HR Dept: 192.168.3.0/24**


ISR433 Gig0/0/0
Router
Fa0/7
Fa0/2
Fa0/2
Fa0/6
Fa0/4
Fa0/6
Fa0/4
Fa0
Fa0
Fa0
Fa0
Fa0
Fa0
Fa0
Fa0
PC-PT
PC0
PC-PT
PC1
VLAN2 (SALES)
192.168.2.0
Device Name: PC2
Device Model: PC-PT
Port Link IP Address IPv6 Address MAC Address
FastEthernet0 Up 192.168.3.2/24 <not set> 00D0.D316.6659
Bluetooth Down <not set> <not set> 0030.F213.A023
Gateway: 192.168.3.1
DNS Server: <not set>
Line Number: <not set>
Physical Location: Intercity > Home City > Corporate Office > PC2

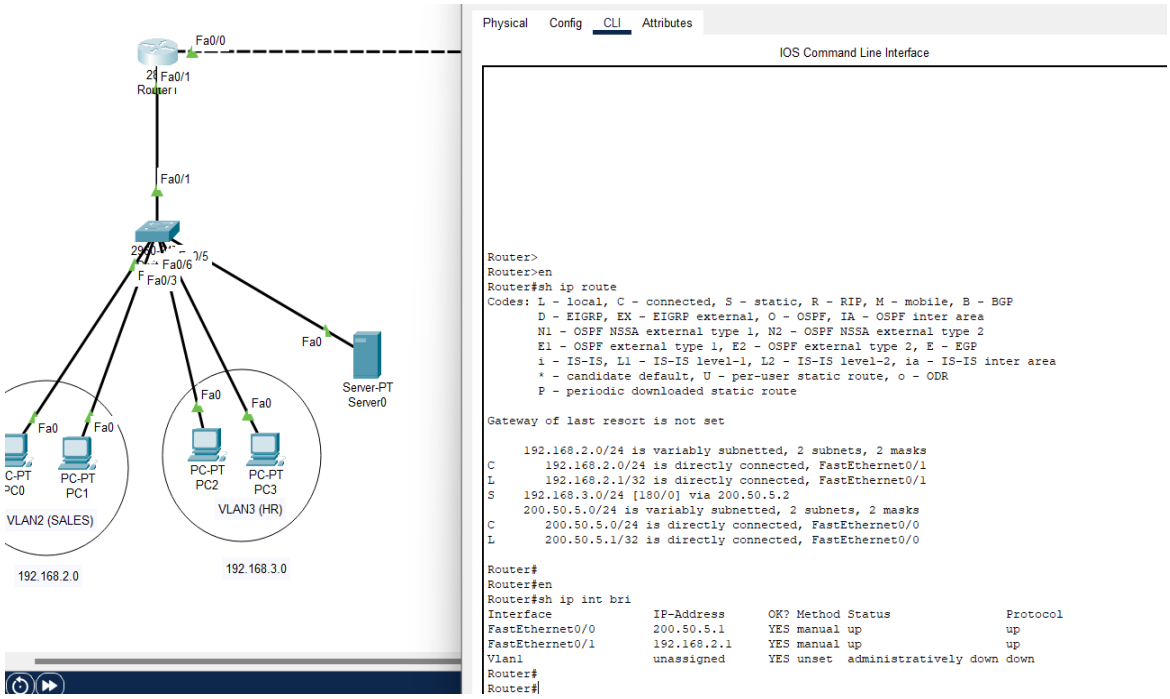
- **Inter-VLAN Routing**: Configure devices (Routers or Layer 3 switches) to enable routing between VLANs when necessary.




- **Routing protocol** using an administrative distance of 180, for the head office router and devices to be able to reach the branch office router or devices and vice versa. using the verification command of '**show ip route**' on each router to see the routing

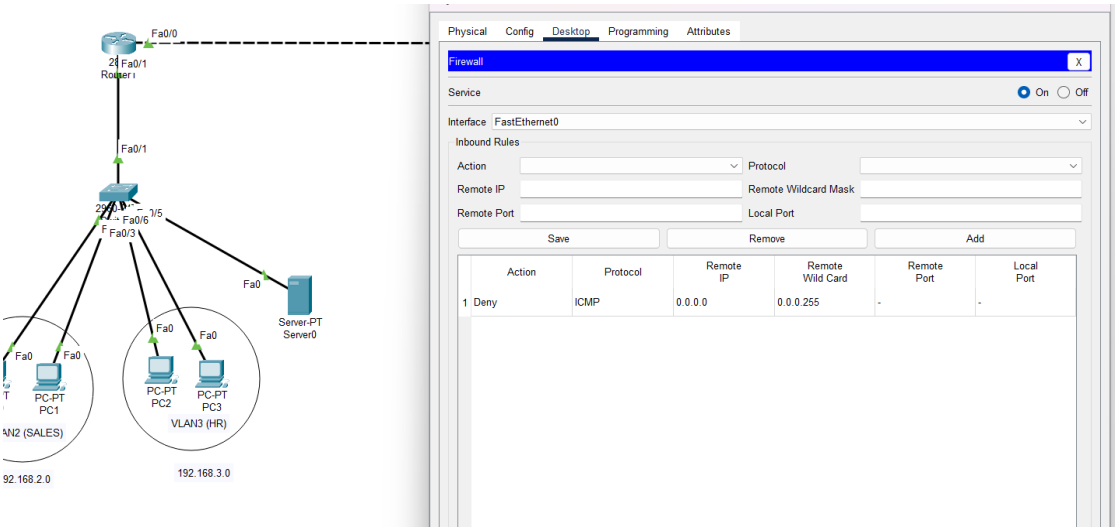
configuration table already done by the network administrator. A static routing config was used for the topology in this project.

*Router#*
*Router#en*
*Router#show ip route*

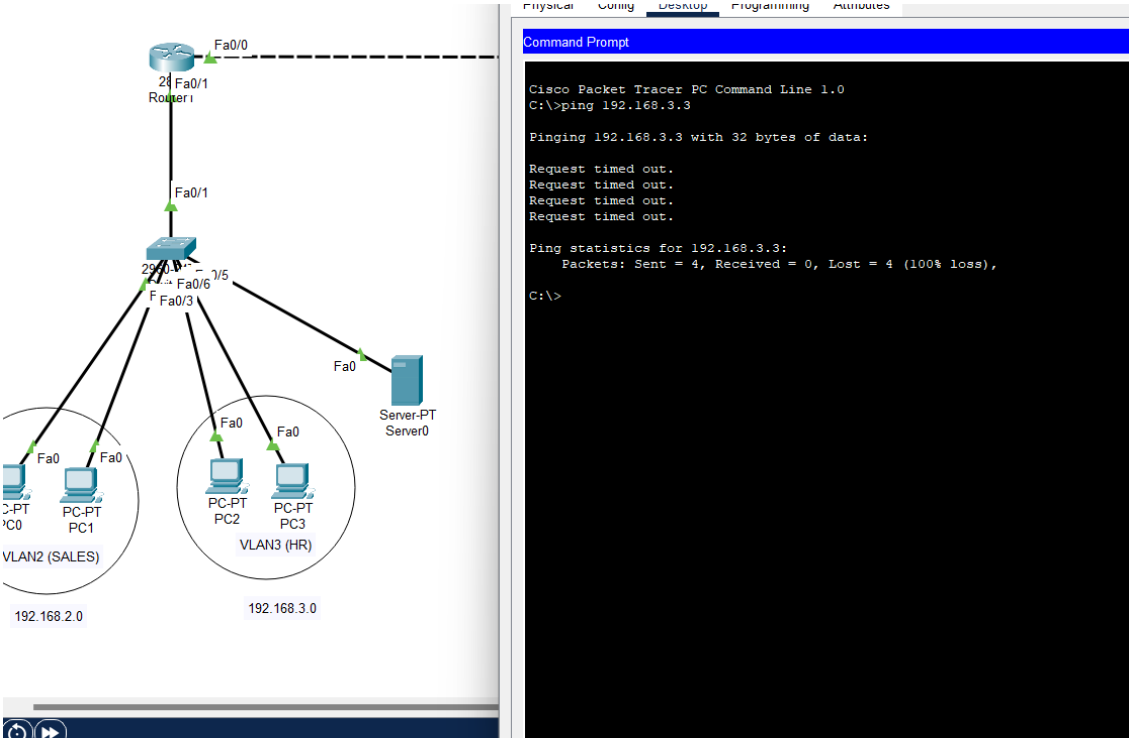
- 


### 3. Security Configuration

- **Firewall Setup**: Implement firewalls between network segments to control traffic.
  - Firewall setups on cisco lab comprises of configuring inbound rules, that means denying any of these services between devices (1) ICMP (2) TCP (3) IP (4) UDP.
  - For example, in our topology, i implemented a firewall setup to deny ICMP on device with the ip add of **192.168.3.3** as shown below.

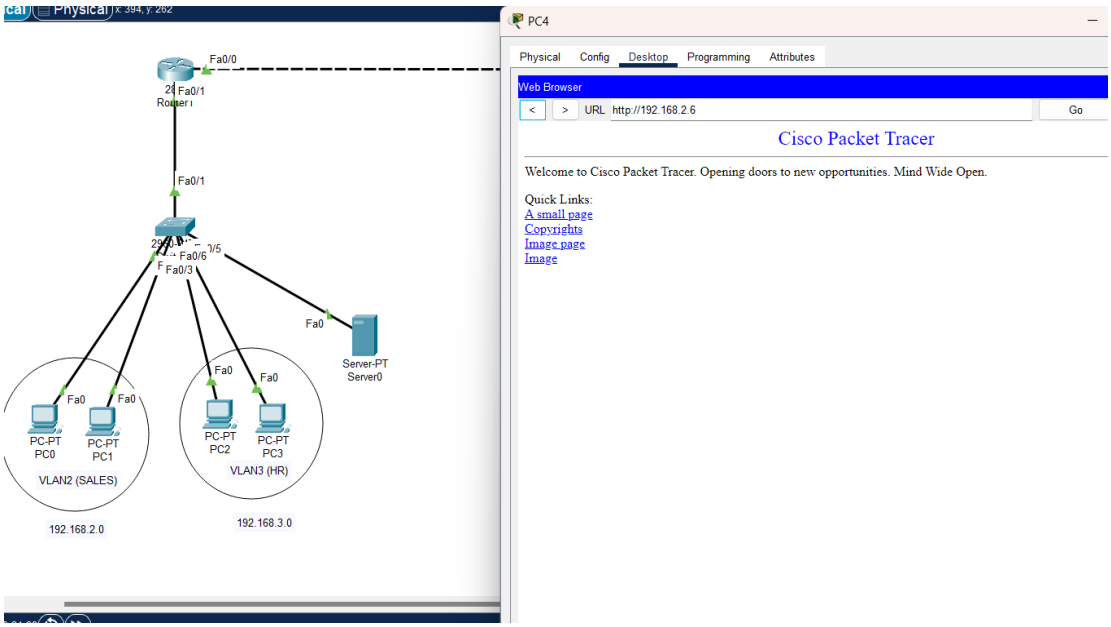
- 

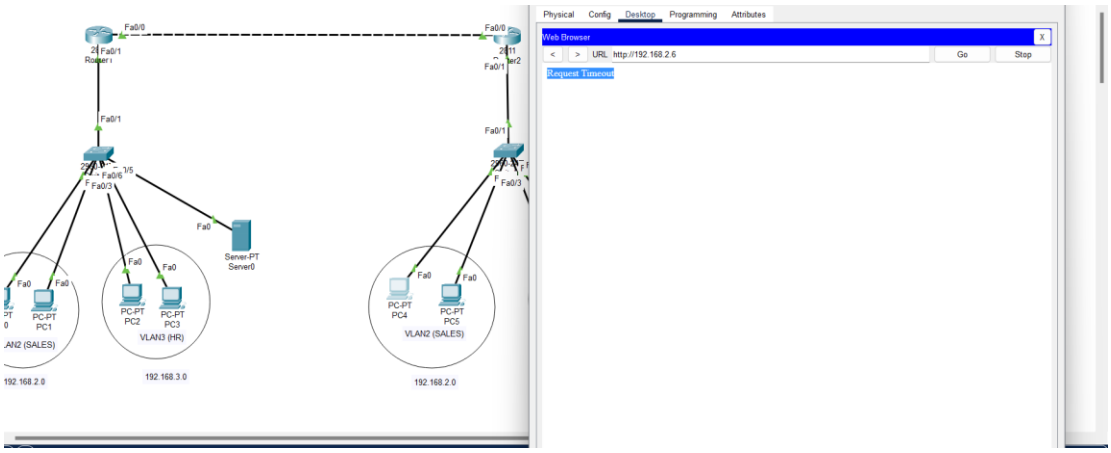

**ICMP Denial on 192.168.3.3**

- 


- **Access Control Lists (ACLs)**: Use ACLs on routers and Layer 3 switches to enforce policies on which traffic is allowed between segments. Using ACLs the devices on the branch office will be permitted or denied access to the websites running on the head office server. Here we are using extended access-list config to block/deny access from branch office router. However, the devices on the branch office (192.168.3.0) can still gain access to other services in the head office (192.168.2.0) by configuring permit any any.

- **Example**: Allow traffic from VLAN 2 (SALES) to VLAN 3 (HR) but block all traffic from the Guest network or multi-cast address.
- Illustrating how traffic is being denied from branch office (192.168.3.0) network from accessing the website running in head office (192.168.2.0) server (192.168.2.6)




- 


- **VPNs (Virtual Private Networks) / IPSec:** Implementing an **IPsec VPN** establishes a secure site-to-site connection between two networks over an untrusted medium like the internet. Below is a brief narration of the process to configure a site-to-site IPsec VPN, focusing on a simple topology with two Cisco routers connecting two LANs.

  If remote access is required, implement secure VPNs to allow employees to connect securely to specific network segments.

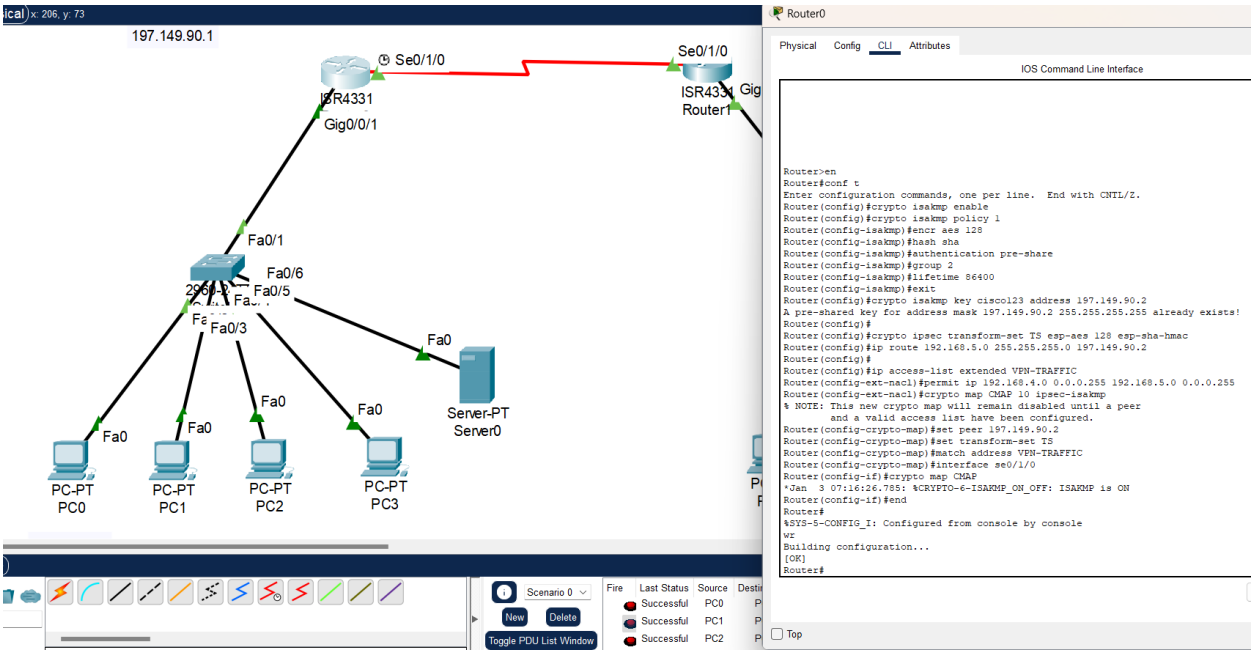
**Site-to-Site VPN Config:**

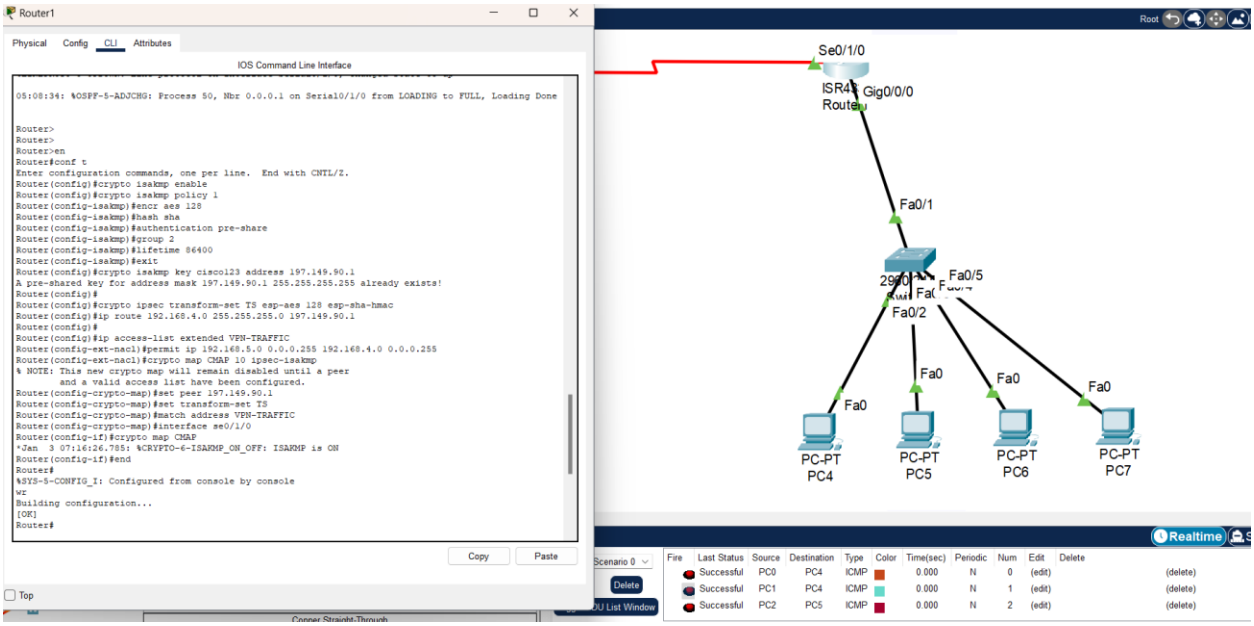
```
en
conf t
crypto isakmp enable
crypto isakmp policy 1
encr aes 128
hash sha
authentication pre-share
group 2
lifetime 86400
exit
crypto isakmp key cisco123 address 197.149.90.2

crypto ipsec transform-set TS esp-aes 128 esp-sha-hmac
ip route 192.168.5.0 255.255.255.0 197.149.90.2

ip access-list extended VPN-TRAFFIC
permit ip 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255
crypto map CMAP 10 ipsec-isakmp
set peer 197.149.90.2
set transform-set TS
match address VPN-TRAFFIC
interface se0/1/0
crypto map CMAP
end
Wr
```

## ROUTER 1 CONFIG



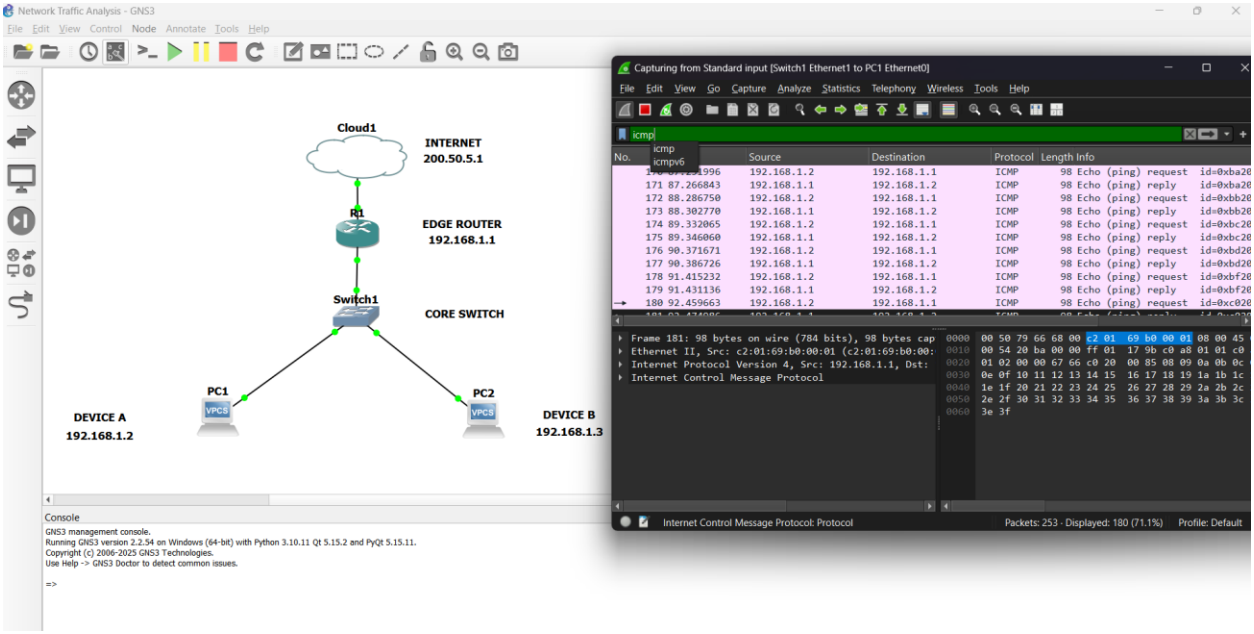




## ROUTER 2 CONFIG.

**Intrusion Detection and Prevention Systems (IDPS)**: Set up systems to monitor for suspicious activity or unauthorized access attempts between segments.

## Monitoring and Management

- **Network Monitoring**: This involves the use of tools like Wireshark or Nagios to monitor network traffic and identify potential issues or security threats. Here we made use of GNS 3 software and Wireshark for network monitoring.




- **Log Management**: Set up centralized logging (e.g., with Syslog or Splunk) for network devices to track all access attempts and unusual activities.

## Challenges and Solutions

- **Challenge**: Managing inter-VLAN communication while maintaining strict security.
  - **Solution**: Use firewalls and ACLs to limit access between VLANs and allow communication only when necessary (e.g., HR can communicate with Finance but not with Development).
- **Challenge**: Ensuring proper routing between subnets while protecting sensitive data.
  - **Solution**: Implement strict ACLs and monitoring systems to detect any unauthorized access attempts.

**Expected Outcomes:**

- **Improved Security**: By isolating sensitive data and controlling access between segments, the risk of unauthorized access and data breaches is reduced.
- **Optimized Network Performance**: With segmentation, network traffic is reduced in individual segments, leading to more efficient data flow and better performance.
- **Easier Management**: Smaller network segments are easier to manage and troubleshoot, with clear boundaries and rules for each department or system.

**Conclusion**

We have successfully implemented a segmented network architecture that enhances security and improves network performance. This project will help you understand how to configure network devices, implement security measures, and monitor network activities to ensure a safe and efficient IT environment.