CAVITE STATE UNIVERSITY
Don Severino de las Alas Campus
Indang, Cavite

COLLEGE OF ENGINEERING AND INFORMATION TECHNOLOGY
Department of Information Technology

College of Engineering and Information Technology

Cavite State University - Don Severino Delas Alas Campus

Indang, Cavite, Philippines

Bandal, Princess Jade S.

Placio, Hannah Pauline

Ramos, Mikaela

Instructor:

Ms. Gerami M. Benedicto

June 18, 2025

This network design is a small to medium-sized enterprise setup that incorporates several essential networking technologies, including VLANs, EIGRP routing, extended access control lists (ACLs), and static NAT. The primary purpose of this network is to segment internal departments, manage traffic efficiently, allow secure remote access via Telnet, and enable communication between internal users and external networks such as the internet or a public server.

The network is designed for structured departmental communication and secure data flow within an organization. It ensures that different segments of the company, such as administration, finance, and technical departments, can operate efficiently without unnecessary traffic interference or security risks. It also supports remote management, internal services, and limited internet exposure through controlled NAT.

This design works by combining several technologies to handle different aspects of communication. VLANs segment the local network by department, which reduces broadcast traffic and increases security. Routers use EIGRP to exchange routing information and ensure that each VLAN can reach other VLANs and external networks. ACLs filter and permit specific traffic, while static NAT allows internal devices to communicate with external networks using a mapped public IP. Telnet enables administrators to access and manage routers remotely.

The network incorporates several core technologies. VLANs are used to separate network traffic by department and are assigned on switch ports. EIGRP is configured on routers to dynamically share routing information between subnets. Static NAT is applied on routers to map private internal IPs to a public address, enabling internet access or public service exposure. Extended ACLs control traffic flow by defining which IPs and services are allowed or denied. Telnet is configured on Router1 to allow remote command-line access from PC1. Each device connects via switches, and inter-VLAN routing occurs through routers. PCs connect to switches, switches connect to routers, and the server connects directly to Router1.

To implement this design, each networking component was configured using Cisco Packet Tracer. VLANs were created and assigned to appropriate switch ports using the following commands: "vlan 10", "name Admin", then "interface FastEthernet0/1" followed by "switchport mode access" and "switchport access vlan 10". On the routers, IP addresses were configured on interfaces, for example: "interface FastEthernet0/0", "ip address 192.168.10.1 255.255.255.0", and enabled with "no shutdown". EIGRP was enabled using: "router eigrp 100", "network 192.168.10.0", and "network 192.168.20.0". Static NAT was configured using: "ip nat inside source static 192.168.10.2 200.0.0.2" with the inside and outside interfaces labeled appropriately. ACLs were applied using: "access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq 80" and applied to the interface using "ip access-group 100 in". Telnet access was enabled on Router1 by configuring the VTY lines with "line vty 0 4", "login local", and "transport input telnet", after setting a username and password with "username admin password adminpass". PC1 was tested by accessing Router1 using the command "telnet 192.168.10.1" in the command prompt.

In conclusion, this network demonstrates a functional and scalable enterprise-level design, showcasing multiple key networking technologies in action. It offers efficient traffic management, security through segmentation and filtering, and remote administration capability. The use of VLANs, EIGRP, ACLs, NAT, and Telnet ensures a robust environment that supports both internal communication and limited external access, providing a strong foundation for future growth or real-world implementation.

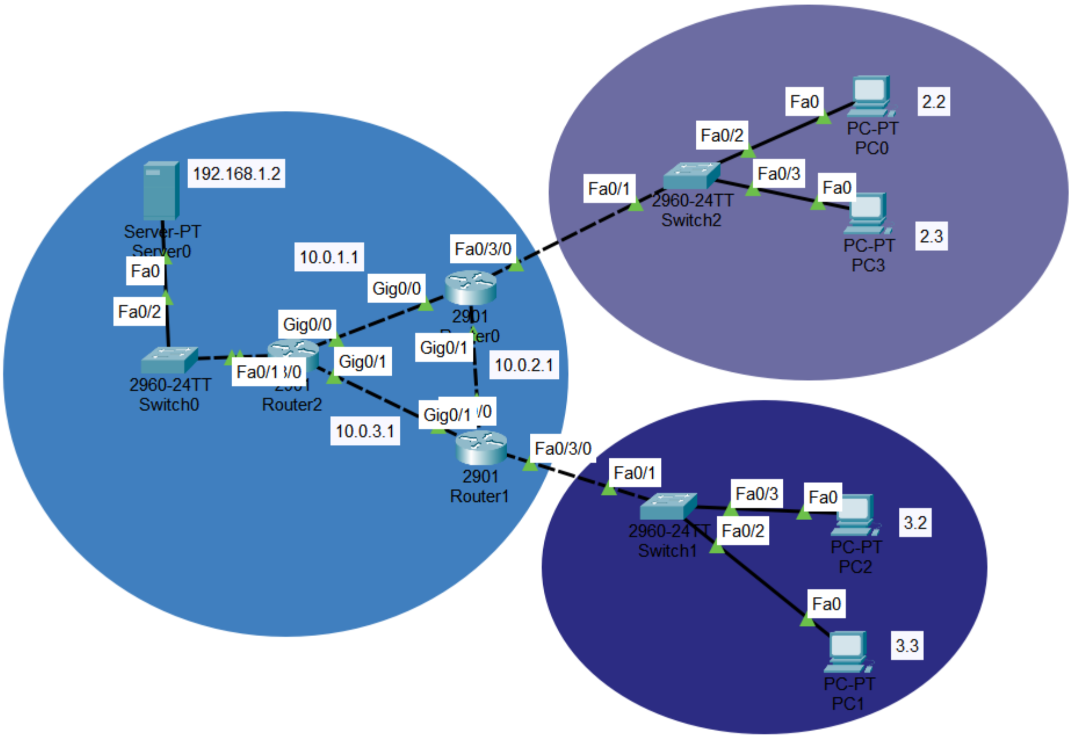

Figure 1. The Network Topology