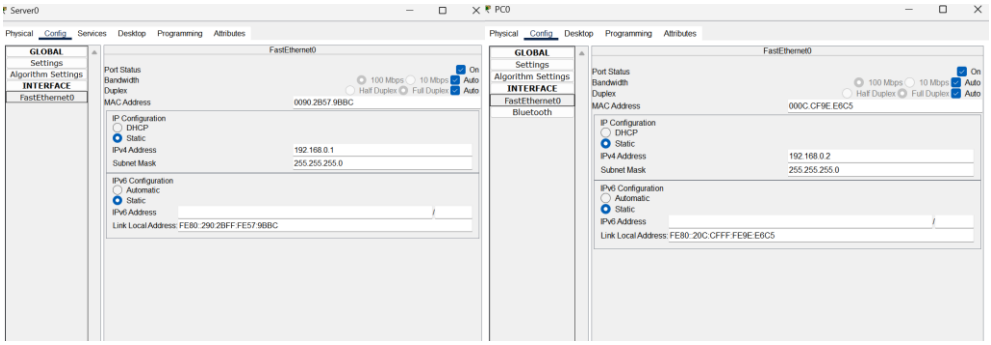
A REPORT ON THE BASIC SWITCH AND END DEVICE CONFIGURATION

In this project, I built a simple network and end device configuration using Cisco Packet Tracer.

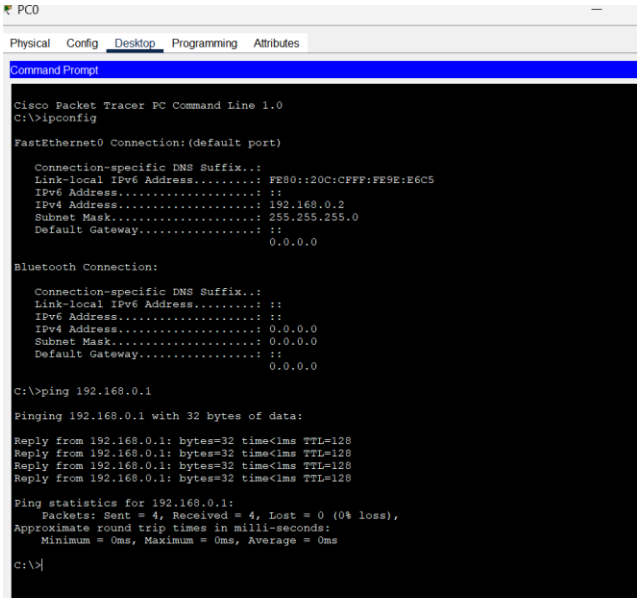
Setting Up a Basic Network

First, I created a basic network by connecting a **PC and a server** using a **copper cross-over cable** and selecting fastethernet0.

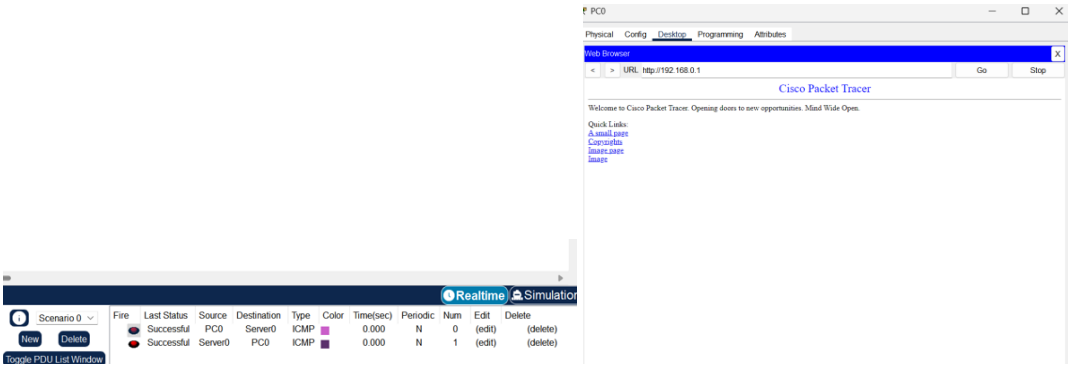
After establishing the connection, I configured the **IP addresses** for the PC and server.



To verify connectivity, I ran the **“ipconfig”** command on the PC, followed by the command **“ping 192.168.0.1”**, which confirmed successful communication between the two devices.

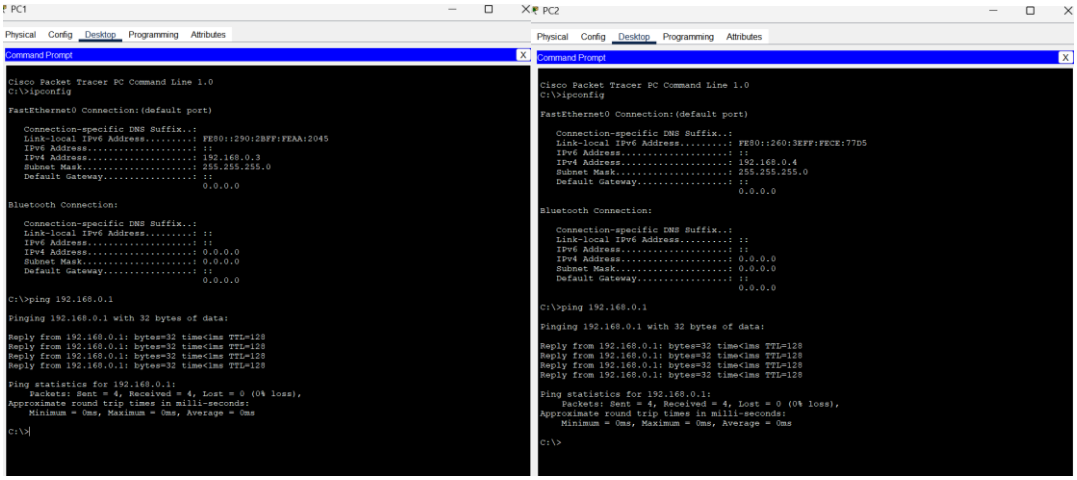


Additionally, I used the **Simple PDU tool** to send a one-time ping message from the PC to the server. The server's response further demonstrated that the connection was successfully established.



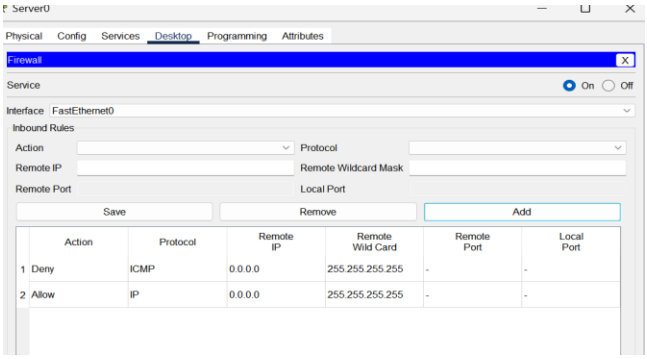
Building the Complete Network Topology

Next, I expanded the network by adding two more **PCs and a switch**. After making the necessary connections between all devices, I assigned **IP addresses** to the newly added PCs and verified connectivity between all PCs and the server.

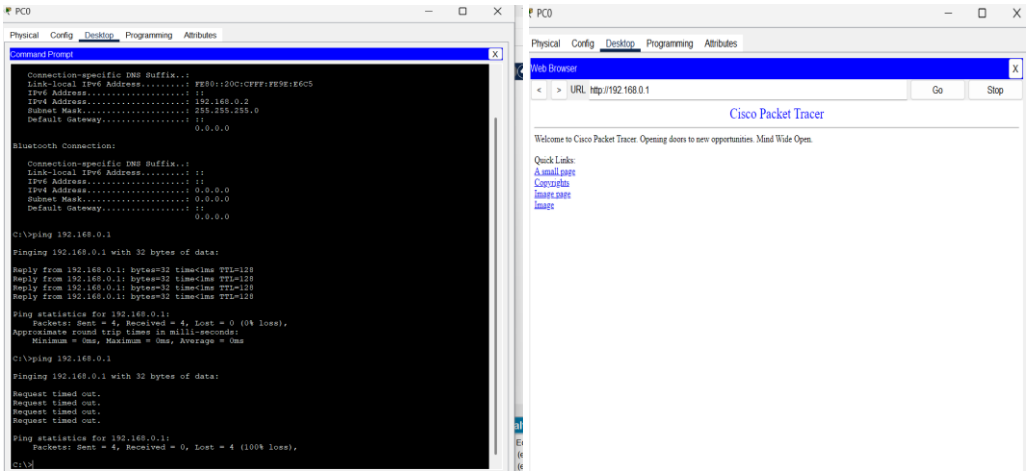


Configuring the Firewall on the Server

To configure a firewall on the server. I enabled firewall services and denied the **ICMP protocol traffic** and set the **Remote IP:** 0.0.0.0 and set the **Remote Wildcard Mask:** 255.255.255.255. Additionally, I allowed **IP protocol traffic** and set the same **remote IP and wildcard mask settings as the ICMP protocol.**



To verify that ICMP traffic was successfully blocked, I attempted to ping the server again, which resulted in **no response**. However, to confirm that IP traffic was still permitted, I used the web browser on the **desktop feature** to access the server's IP address, which connected.



Conclusion:

This project successfully demonstrated the process of building and securing a simple network using Cisco Packet Tracer. Starting with a basic PC-to-server connection, the network was expanded by integrating additional devices through a switch. The final step involved configuring the server's firewall to block ICMP traffic while allowing IP traffic, effectively verifying both connectivity and security.