Ryan Hatch  
April 16 2023

**Network Configuration Simulation**

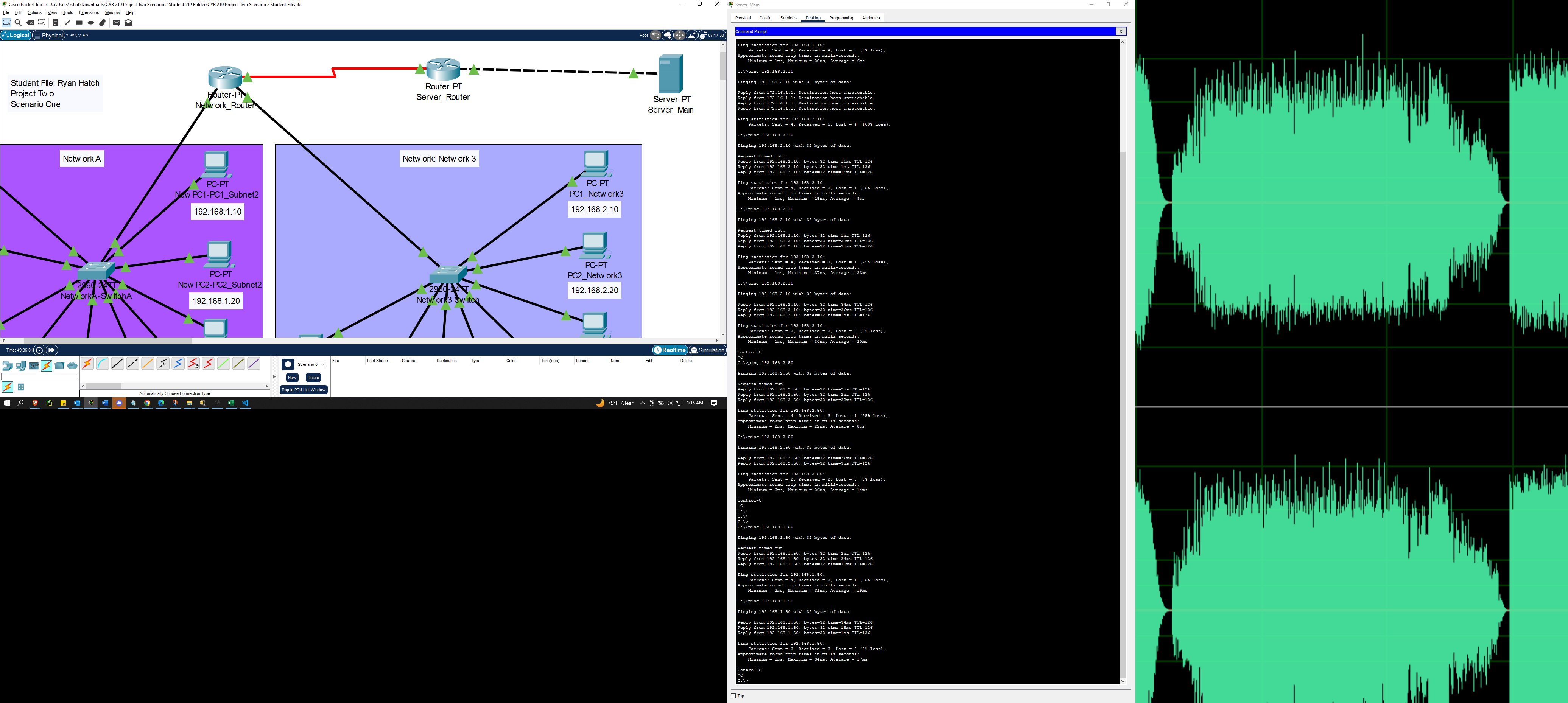
IP networking is the process of configuring network devices to communicate with each other using IP addresses. In this project, I configured the network devices to use IP addresses in the range of 192.168.1.0/24 and 192.168.2.0/24.

Subnet masks are used to divide a network into smaller subnetworks or subnets. In this project, I used a subnet mask of 255.255.255.0, which allowed me to create subnets with up to 254 hosts.

Before incorporating Network 3, I had to remove Subnet 2 and combine it with Subnet 1. To do this, I reconfigured the network devices to use the subnet mask 255.255.254.0, which allowed me to create a single subnet that included both Subnet 1 and Subnet 2.

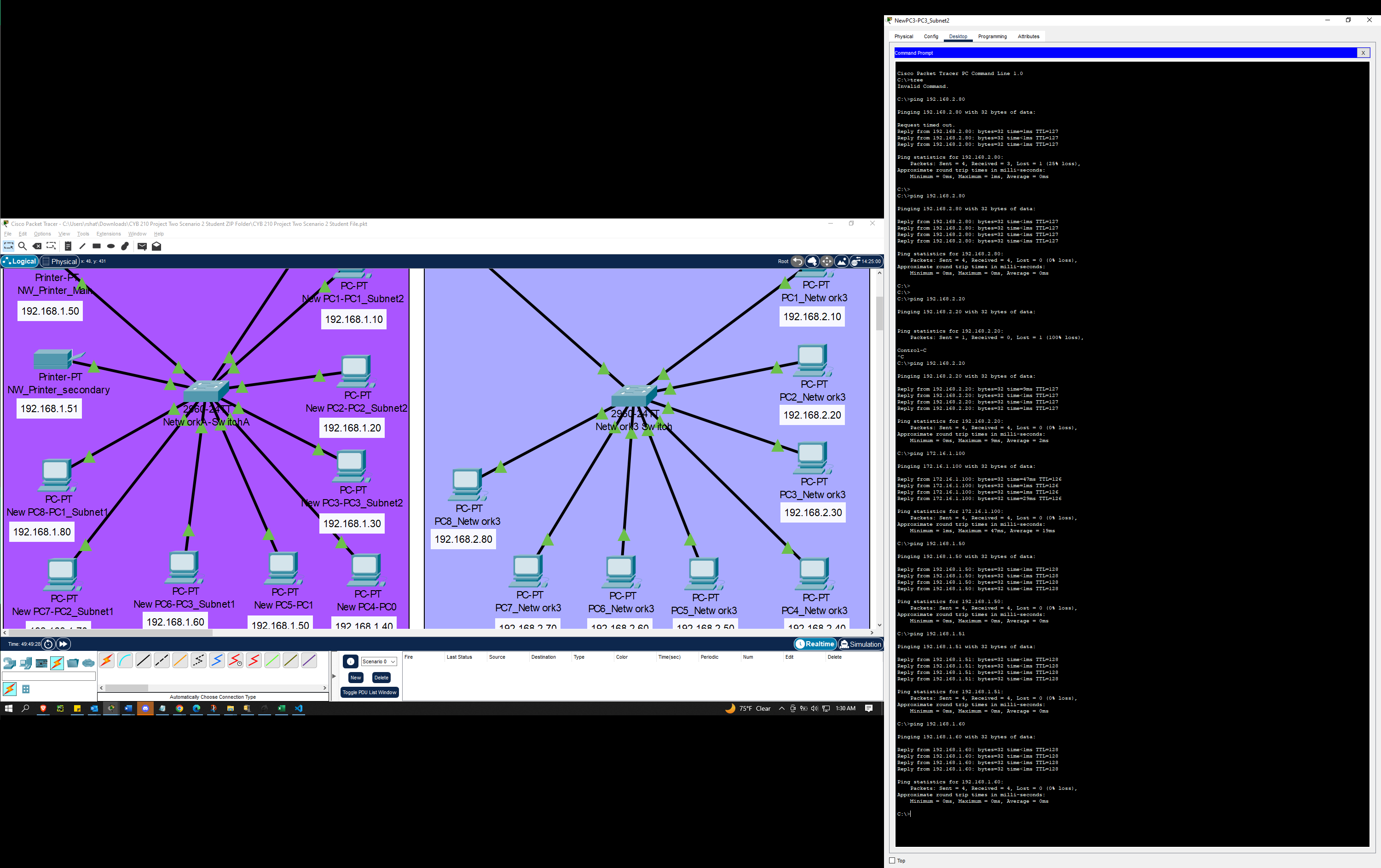
Once I had created the new subnet, I incorporated Network 3 by configuring the router to connect the two networks. I assigned the IP address 192.168.1.1 to one side of the router as Network A and 192.168.2.1 to the other side as Network 3.

Throughout the process, I monitored the network to ensure that it was functioning correctly and that there were no issues with IP address conflicts or routing. I also made sure to document the network configuration for future reference and troubleshooting purposes.

In the screenshot below, I was testing the connectivity between different networks using the ping command from the main server. I first established a strong connection with a PC in Network A and then with a PC in Network 3. After getting two successful pings with 0% loss, I tested the connectivity with a PC in Network 3 and then with a PC in Network A. 

**I: Successful pings**

To verify the connection status of the network, I used the ping command on a computer in Network A called PC3 (192.168.1.30). First, I tested if PC8 and PC2 in Network 3 were working, then I tested if the server was working. Once I confirmed the server was working, I tested both printers on Network A.

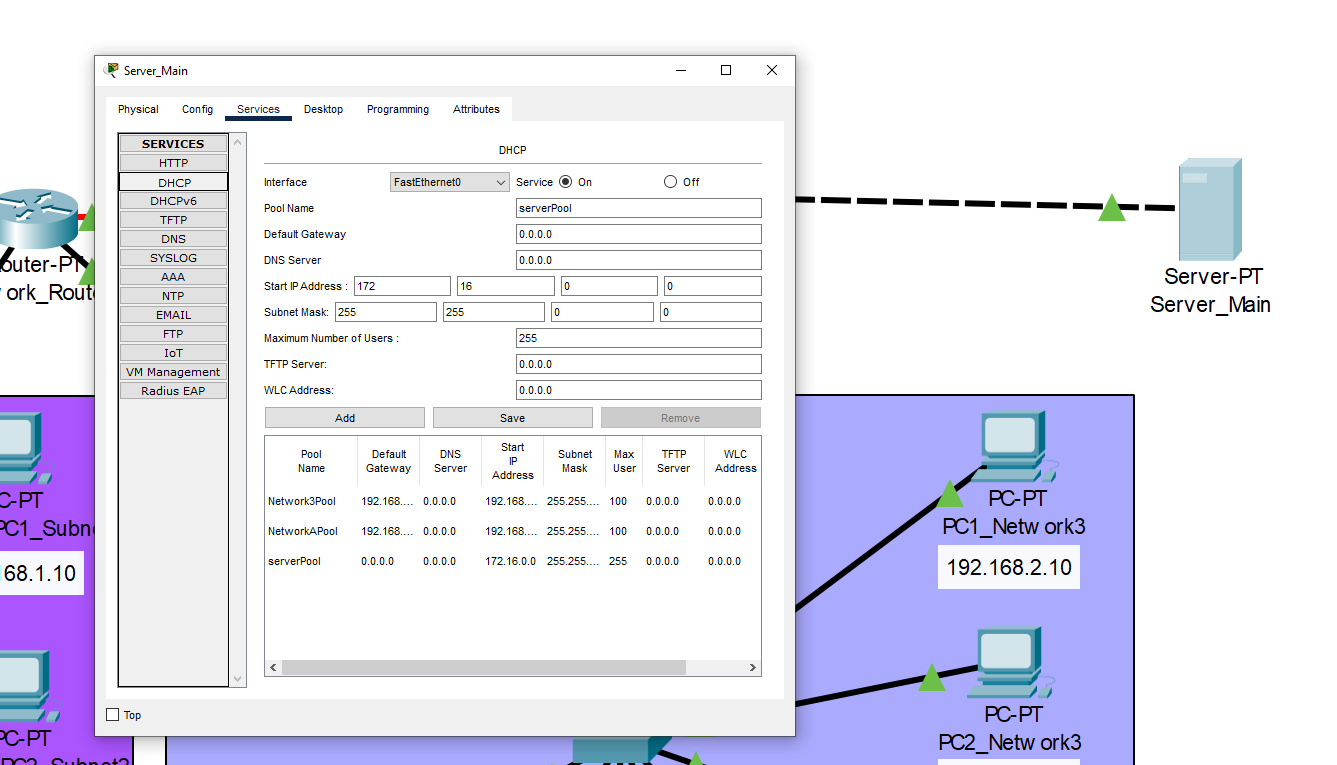


**II: Successful pings**

DHCP (Dynamic Host Configuration Protocol) is a network protocol used to automatically assign IP addresses and other network configuration parameters to devices on a network. I used DHCP in this project to simplify the management of IP addresses and reduce the chances of address conflicts. To configure DHCP, I used the Cisco Packet app to set up a DHCP server on the network. I ensured that the DHCP server had a pool of available IP addresses to assign to devices on the network. I also set up the DHCP server to distribute other network configuration parameters, such as the default gateway, DNS servers, and subnet mask.

Once the DHCP server was set up, I configured the network devices to obtain their IP addresses and other network configuration parameters from the DHCP server automatically. This made it easier to manage the network, as devices could be added or removed without needing to manually configure their network settings.

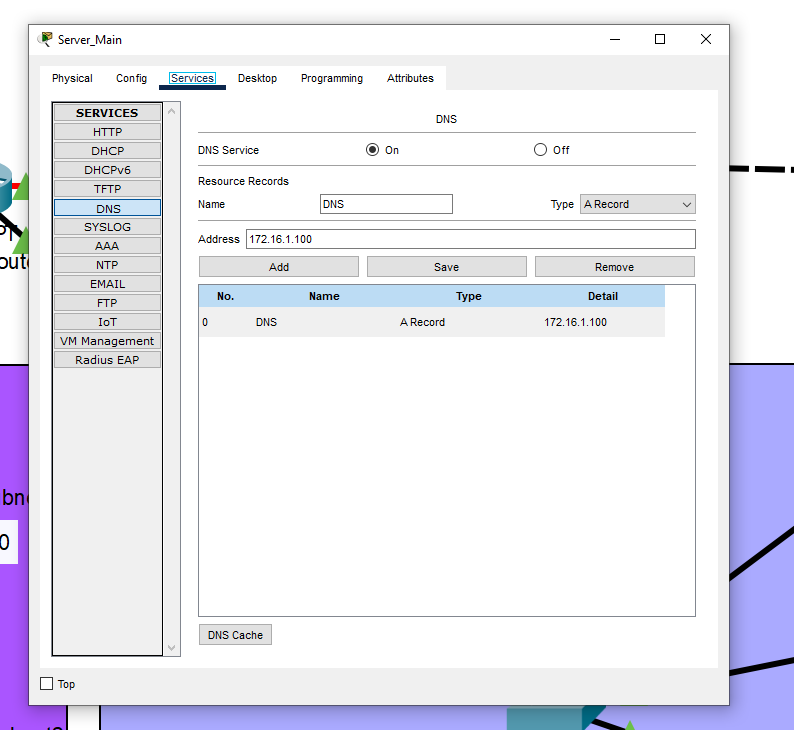
Throughout the process, I monitored the DHCP server to ensure that it was functioning correctly and was not assigning duplicate IP addresses. I also made sure to regularly review the DHCP lease times to ensure that they were appropriate for the network and prevented IP address conflicts.  
Overall, using DHCP simplified the management of the network and reduced the chances of address conflicts, making it easier to add or remove devices from the network as needed.

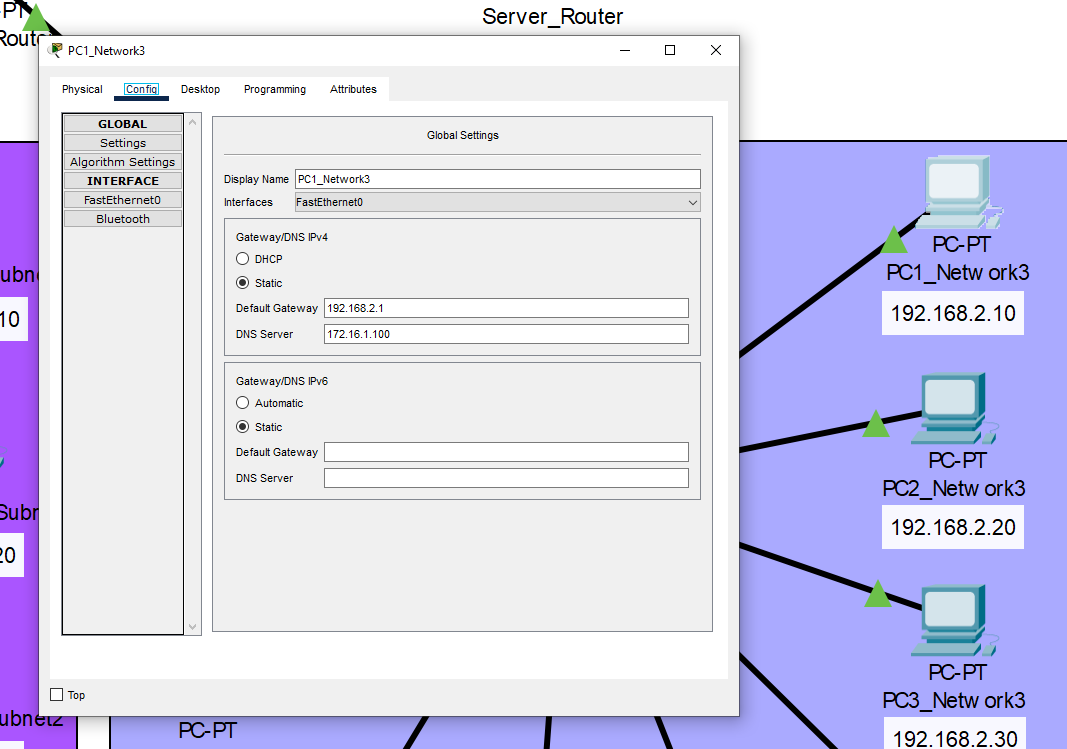


**III: DHCP**

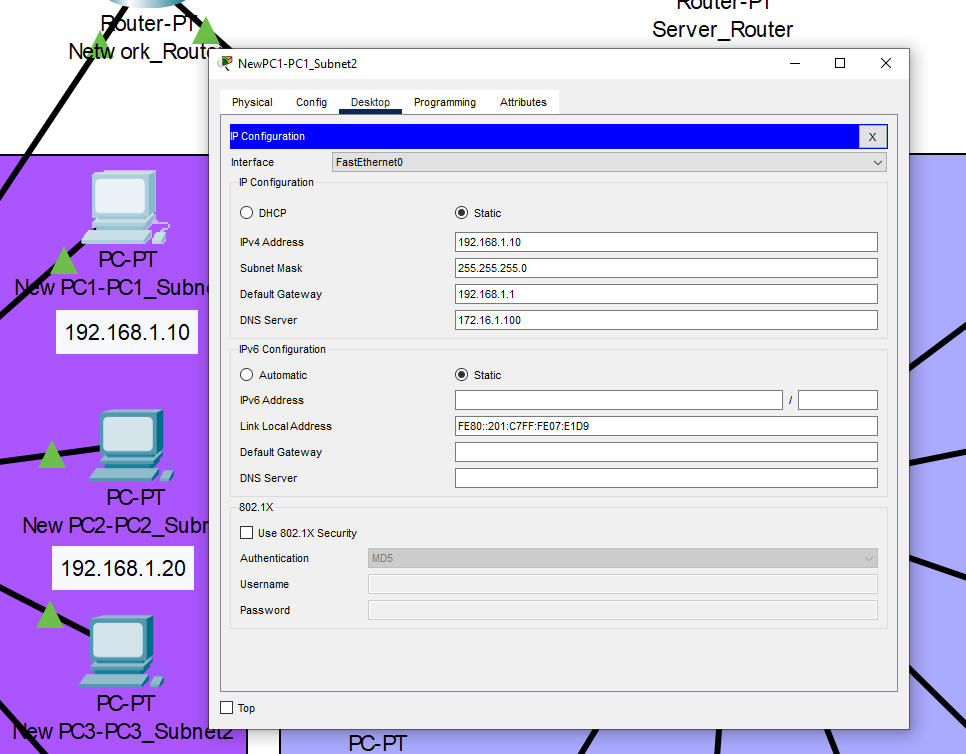
DNS (Domain Name System) is a hierarchical decentralized naming system for computers, services, or other resources connected to the internet or a private network. It translates domain names to IP addresses, allowing users to access resources using human-readable names rather than having to remember numerical IP addresses.  
In this project, I used DNS to allow users on the internal network to access resources on the internet using domain names instead of IP addresses. I set up a DNS server on the network, which served as a central repository for resolving domain names to IP addresses.

To configure DNS, I used the Cisco Packet app to set up the DNS server and configured the necessary DNS records, including A records for mapping domain names to IP addresses and MX records for mapping domain names to email servers. I also ensured that the DNS server was properly configured with the correct forwarders and root hints to allow it to resolve domain names that were not in its local zone.  
  
Throughout the process, I tested the DNS configuration to ensure that it was working correctly and resolved domain names to the correct IP addresses. I also monitored the network traffic to detect any issues that might have arisen from the use of DNS and made any necessary adjustments to the configurations.



**IV: DNS**  


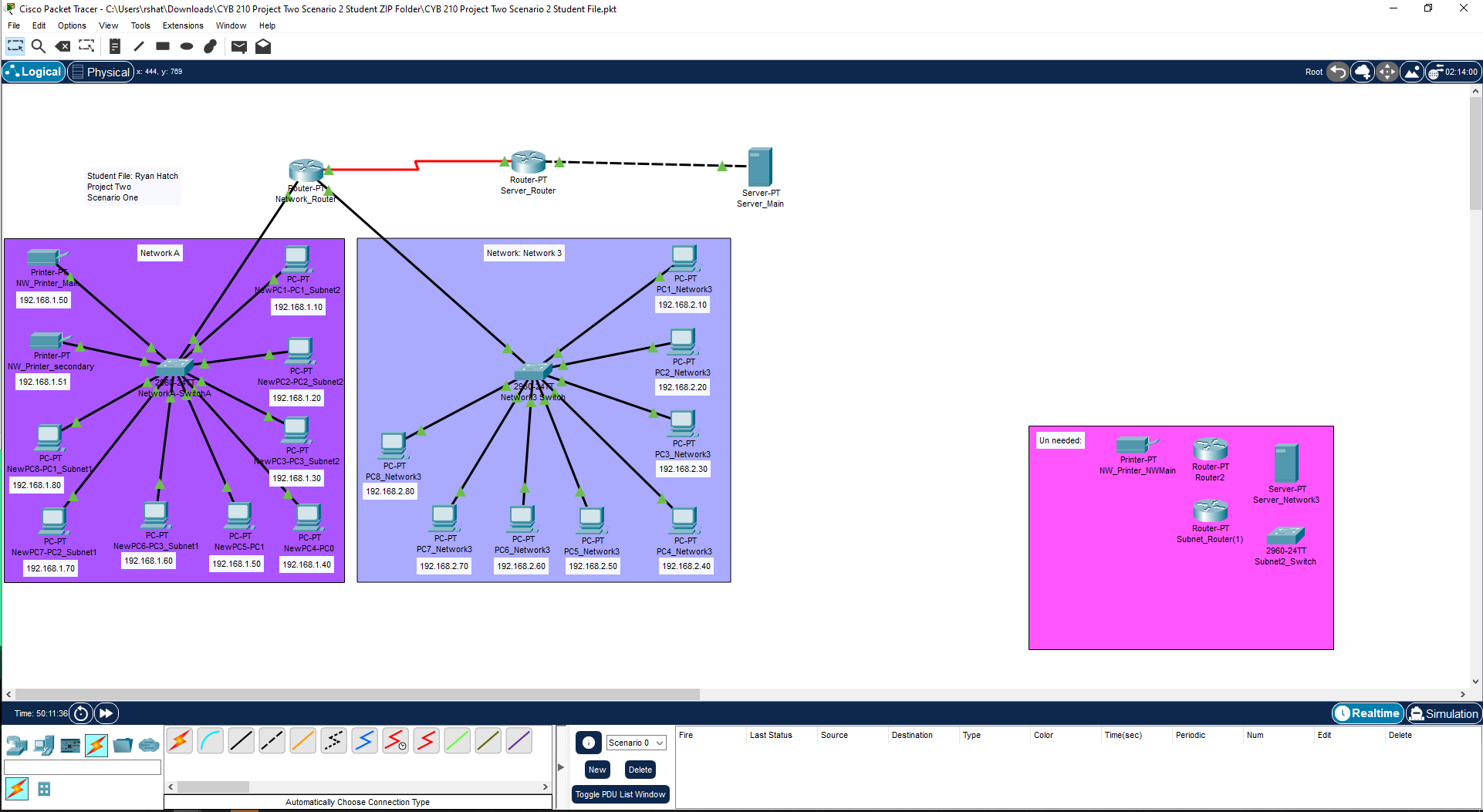
**V: Path**



**VI: NAT/ PAT**

NAT (Network Address Translation) is a technique used to map an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device. I used NAT in this project to allow hosts on the internal network with private IP addresses to communicate with hosts on the external network with public IP addresses.  
  
PAT (Port Address Translation) is a variant of NAT that maps multiple private IP addresses to a single public IP address by using different port numbers to distinguish between them. I used PAT in this project to allow multiple hosts on the internal network to share a single public IP address when accessing the internet.

To configure NAT and PAT, I used the Cisco Packet app to set up the appropriate rules and mappings on the network devices, such as routers or firewalls. I ensured that the NAT and PAT configurations were correctly applied to the network topology to enable the proper translation of IP addresses and ports.  
  
Throughout the process, I tested the NAT and PAT configurations to ensure that they were working correctly and did not introduce any unwanted network issues. I also monitored the network traffic to detect any issues that might have arisen from the use of NAT and PAT and made any necessary adjustments to the configurations.

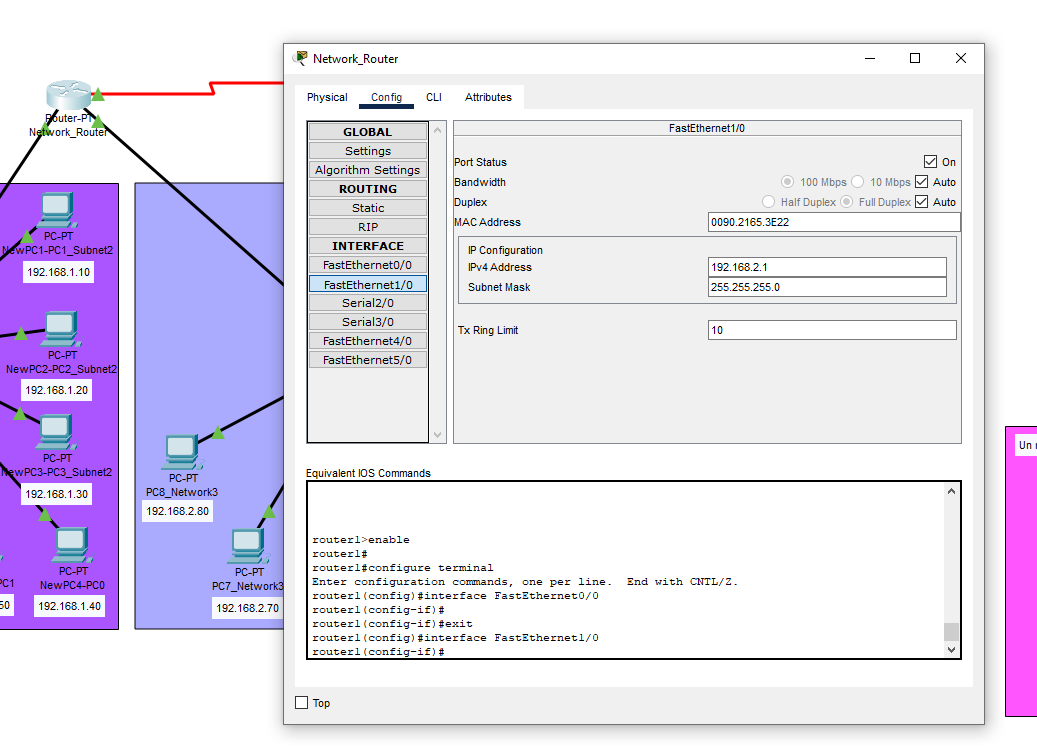


**VII: subnets and configuration**

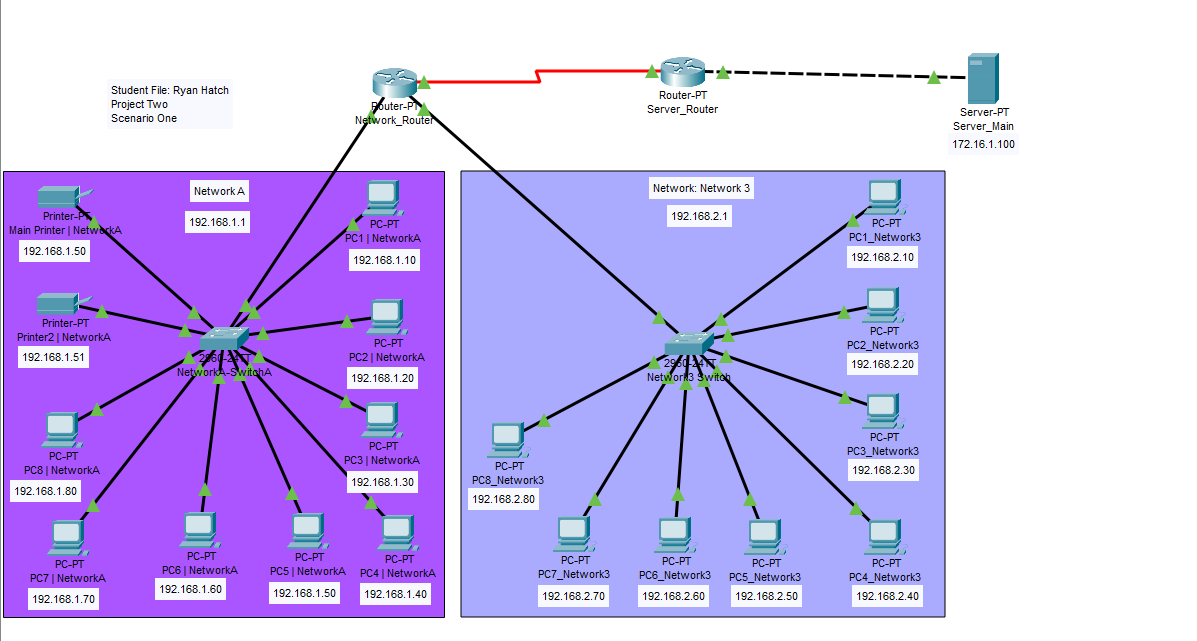
To create the subnets, I used the subnet mask 255.255.255.0, which allows for up to 254 hosts per subnet. I divided the available IP address range into subnets based on the number of hosts that each subnet would need to accommodate.

For example, if I needed to create a subnet for a small office with 20 computers, I would allocate a range of 20 IP addresses within the available range and configure the devices on that subnet to use those addresses.

To assign static IP addresses to specific devices, I configured those devices to use a specific IP address within the range of the subnet. I ensured that the static IP addresses did not conflict with any other IP addresses on the network and were within the appropriate subnet.  
  
To assign dynamic IP addresses, I configured a DHCP server on the network, as I mentioned earlier. The DHCP server would automatically assign IP addresses to devies on the network as they connect. Throughout the process, I monitored the network to ensure that all devices were communicating correctly and that there were no IP address conflicts. If I detected any issues, I would adjust the subnet configurations or IP address assignments as necessary to resolve the issue.



**VIII: subnets/ Network 3**



**IX: Network Diagram**