Lab 5: Basic DHCP and NAT Configuration.

Student Name: -------------------------------------

Student ID: ----------------------------------------

Student Section: ------------------------------------

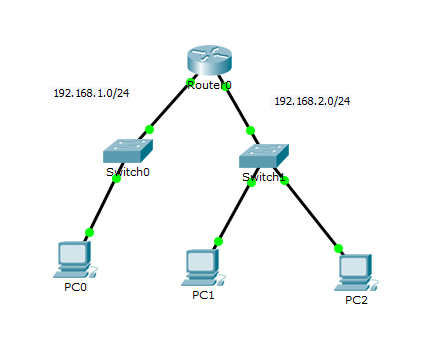
Part 1: DHCP

This part demonstrates how to configure DHCP on a Cisco router instead of a server. As you know by now, the Dynamic Host Configuration Protocol (DHCP) is a network protocol used to automatically configure network devices with IP addresses.

DHCP allows a computer to join an IP-based network without having a pre-configured static IP address. DHCP is a protocol that assigns unique IP addresses to devices, then releases and renews these addresses as devices leave and re-join the network.

Internet Service Providers (ISPs) usually use DHCP to allow customers to join the Internet with minimum effort. The DHCP server maintains a database of available IP addresses and configuration information. When it receives a request from a client, the DHCP server determines the network to which the DHCP client is connected, and then allocates an IP address.

**Topology Diagram**



* **Configure a DHCP Server**

Cisco IOS software supports a DHCP server configuration called Easy IP. The goal for this lab is to have devices on the networks 192.168.1.0/24 and 192.168.2.0/24 request IP addresses via DHCP from R0.

* **Exclude statically assigned addresses**

The DHCP server assumes that all IP addresses in a DHCP address pool subnet are available for assigning to DHCP clients. You must specify the IP addresses that the DHCP server should not assign to clients. These IP addresses are usually static addresses reserved for the router interface, switch management IP address, servers, and local network printer. The **ip dhcp excluded-address** command prevents the router from assigning IP addresses within the configured range (Specifies the IP addresses that the DHCP Server should not assign to DHCP clients). The format for this command is:

* **Router(config)#ip dhcp excluded-address firstIP lastIP**
* **Configure the DHCP pool:**
* **Router(config)#ip dhcp pool POOLNAME**
* Creates a name for the DHCP Server address pool and places you in DHCP pool configuration mode (identified by the dhcp-config# prompt).
* **Router(dhcp-config)# network NETWORKID MASK**
* Specifies the subnet network number and mask of the DHCP address pool.
* **Router(dhcp-config)# dns-server IPaddress**
* Specifies the IP address of a DNS server that is available to a DHCP client.
* **Router(dhcp-config)# default-router IPaddress**
* Specifies the IP address of the default router for a DHCP client
* **Configure Router0 as DHCP Server**

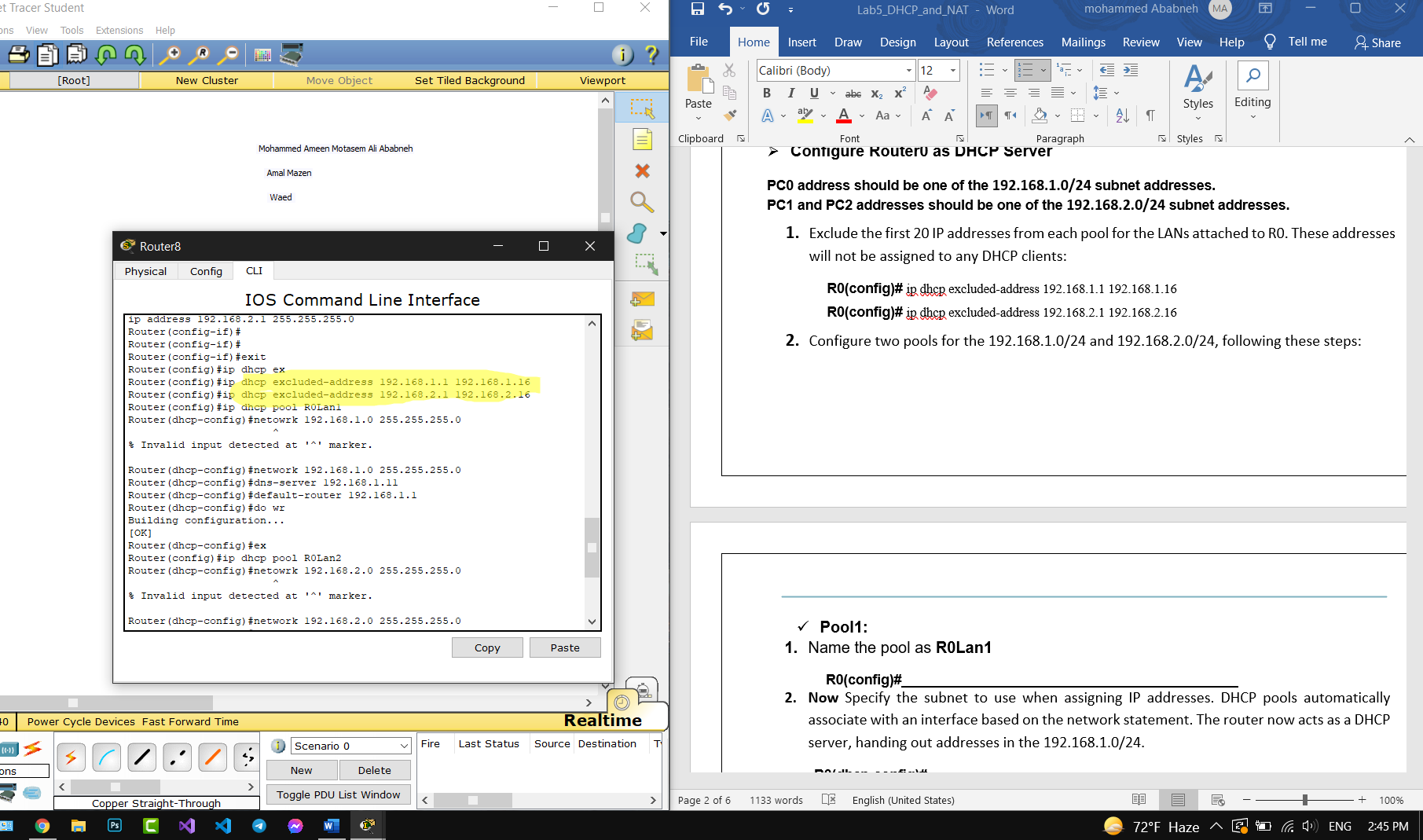
**PC0 address should be one of the 192.168.1.0/24** **subnet addresses.**

**PC1 and PC2 addresses should be one of the 192.168.2.0/24** **subnet addresses.**

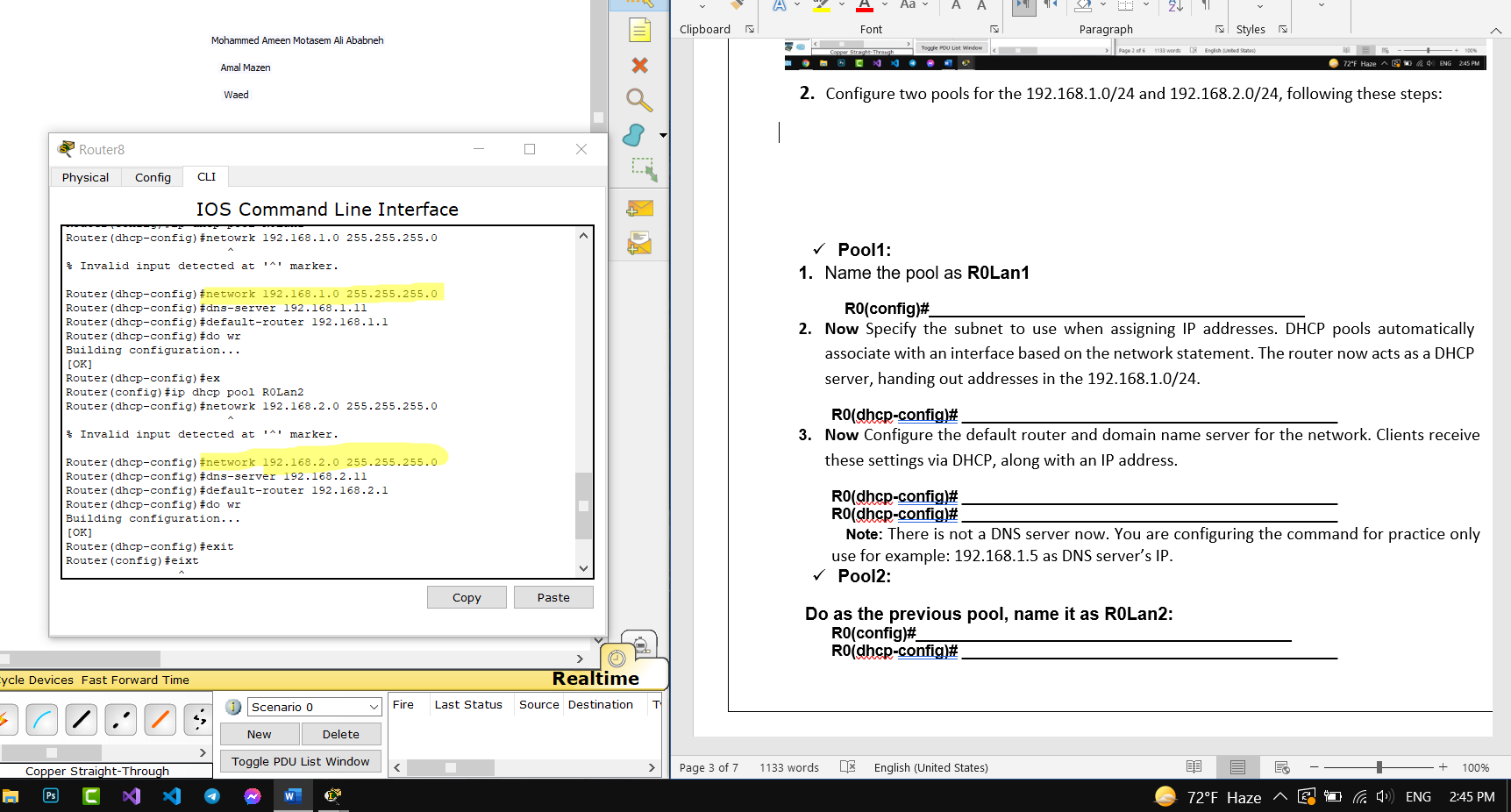
1. Exclude the first 20 IP addresses from each pool for the LANs attached to R0. These addresses will not be assigned to any DHCP clients:

**R0(config)#** ip dhcp excluded-address 192.168.1.1 192.168.1.16

**R0(config)#** ip dhcp excluded-address 192.168.2.1 192.168.2.16



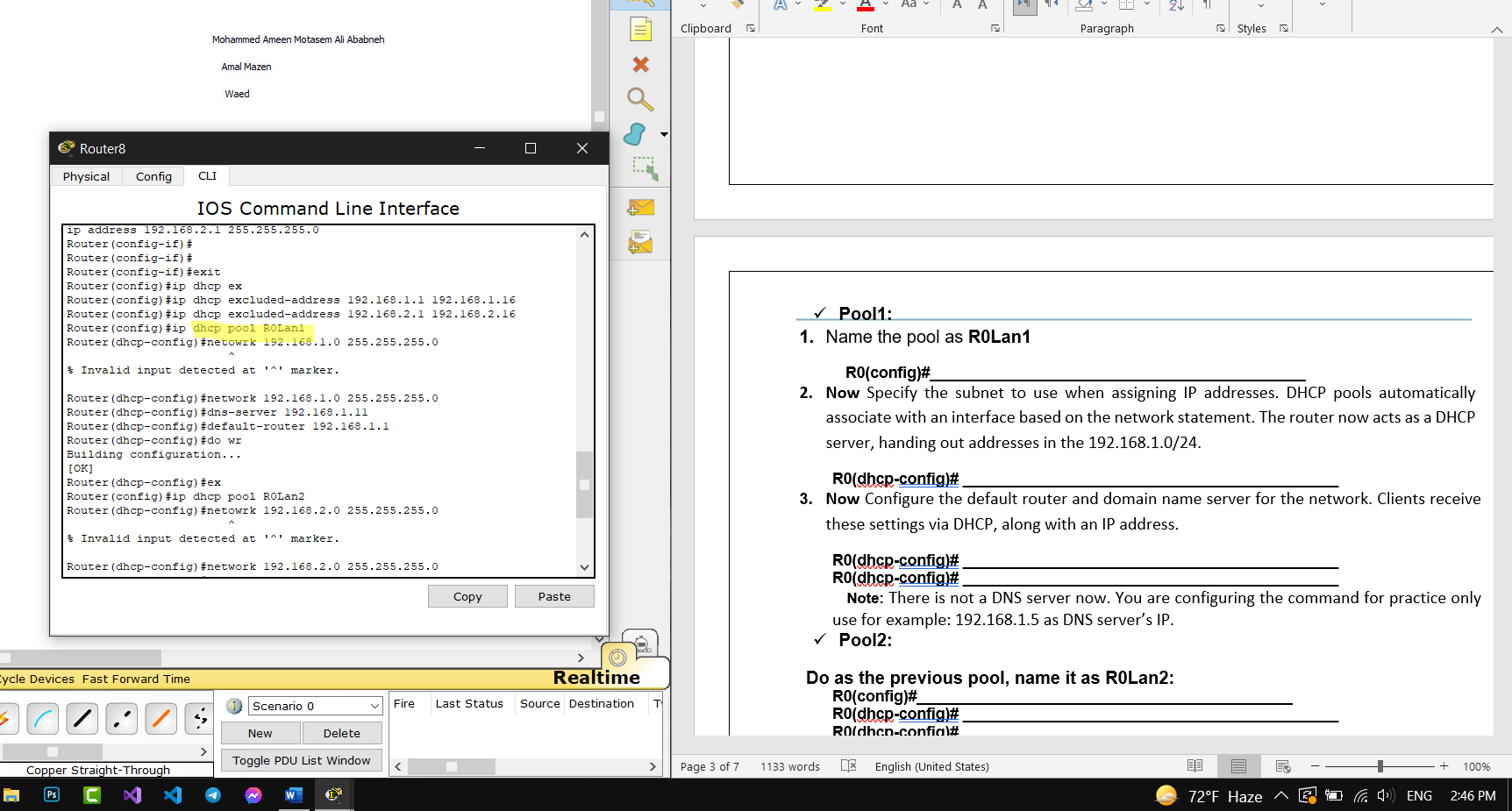
1. Configure two pools for the 192.168.1.0/24 and 192.168.2.0/24, following these steps:



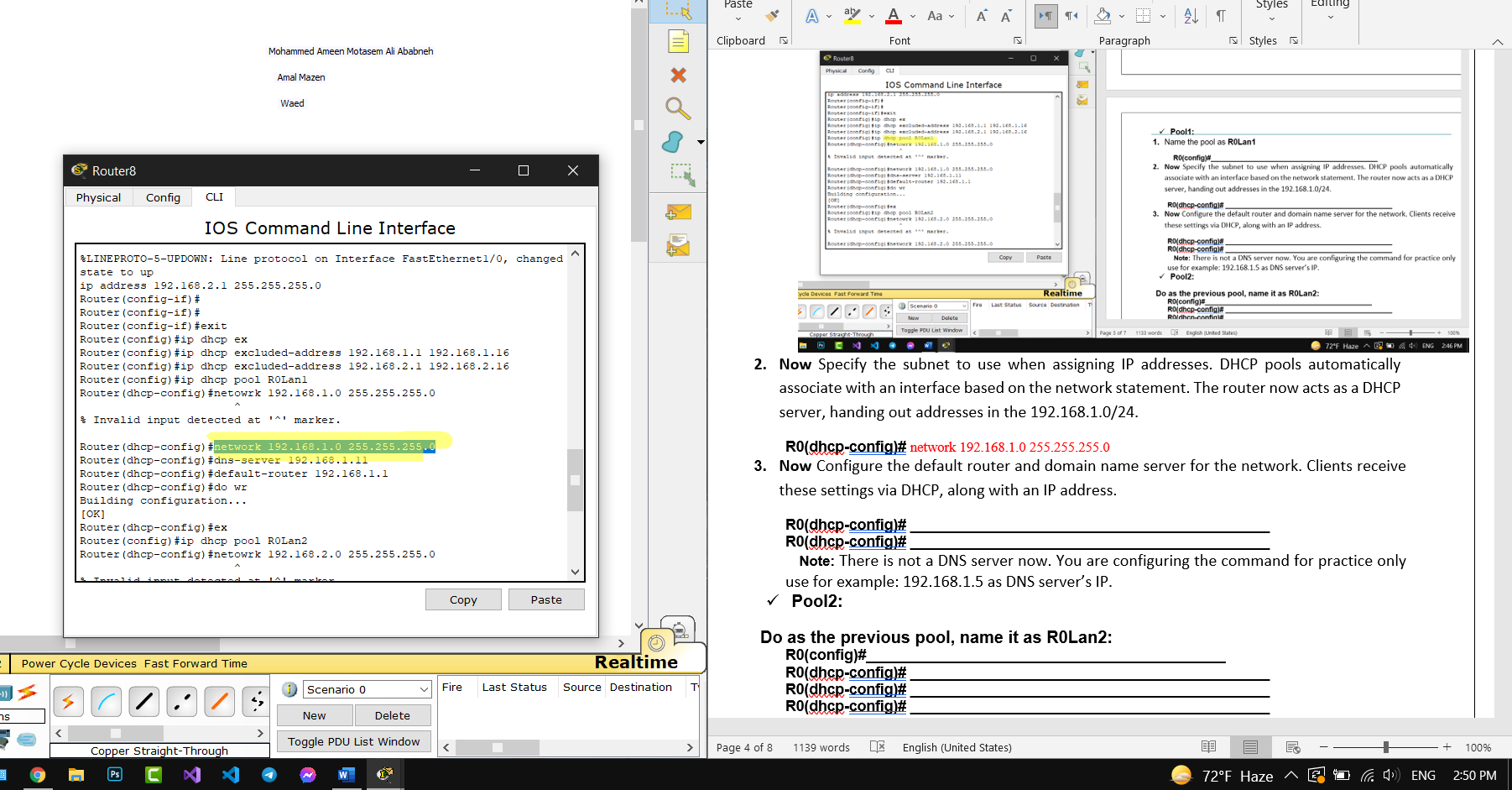
* **Pool1:**

1. Name the pool as **R0Lan1**

**R0(config)#** ip dhcp pool R0Lan1

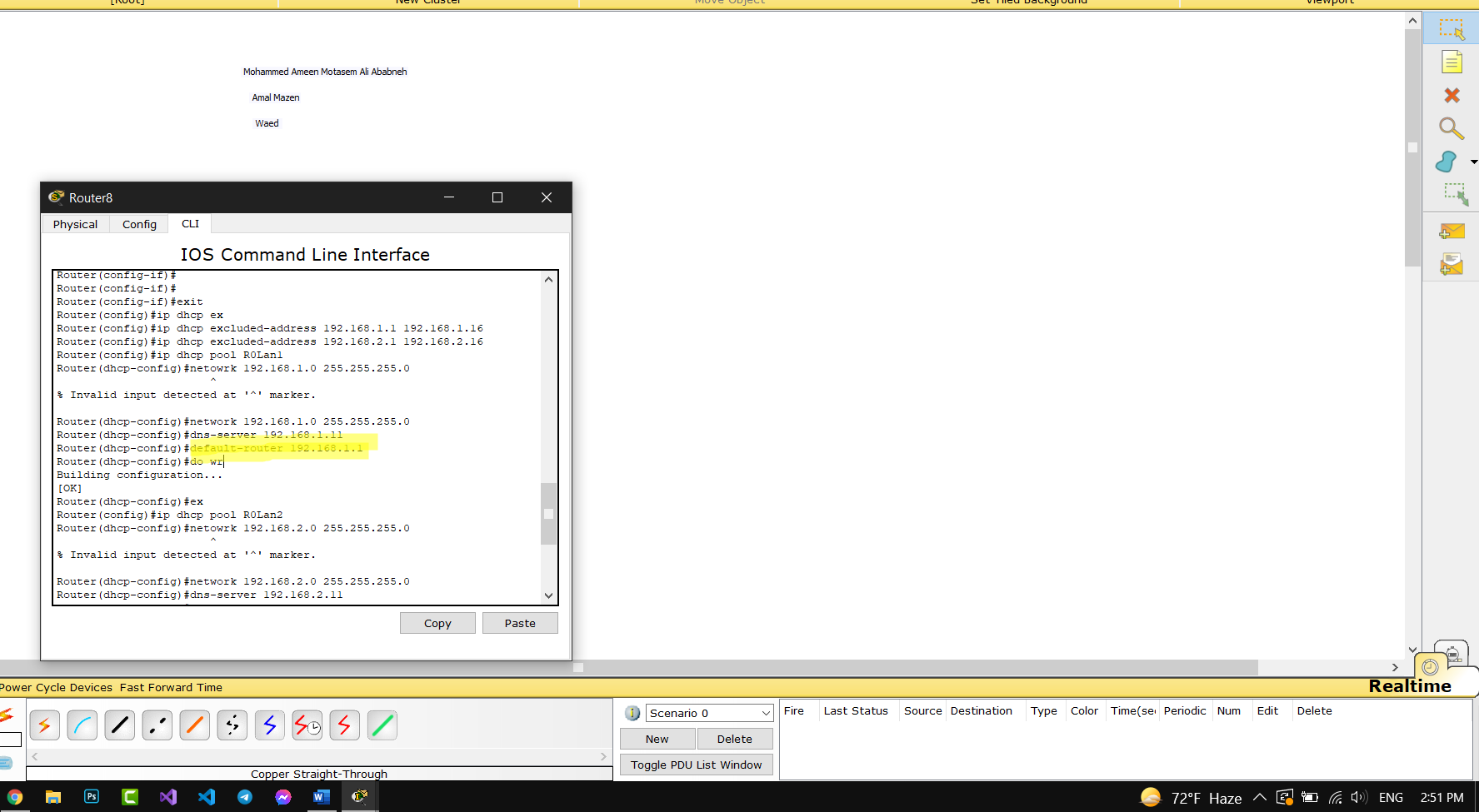


1. **Now** Specify the subnet to use when assigning IP addresses. DHCP pools automatically associate with an interface based on the network statement. The router now acts as a DHCP server, handing out addresses in the 192.168.1.0/24.



**R0(dhcp-config)#** network 192.168.1.0 255.255.255.0

1. **Now** Configure the default router and domain name server for the network. Clients receive these settings via DHCP, along with an IP address.



**R0(dhcp-config)#** default-router 192.168.1.1

**Note:** There is not a DNS server now. You are configuring the command for practice only use for example: 192.168.1.5 as DNS server’s IP.

* **Pool2:**

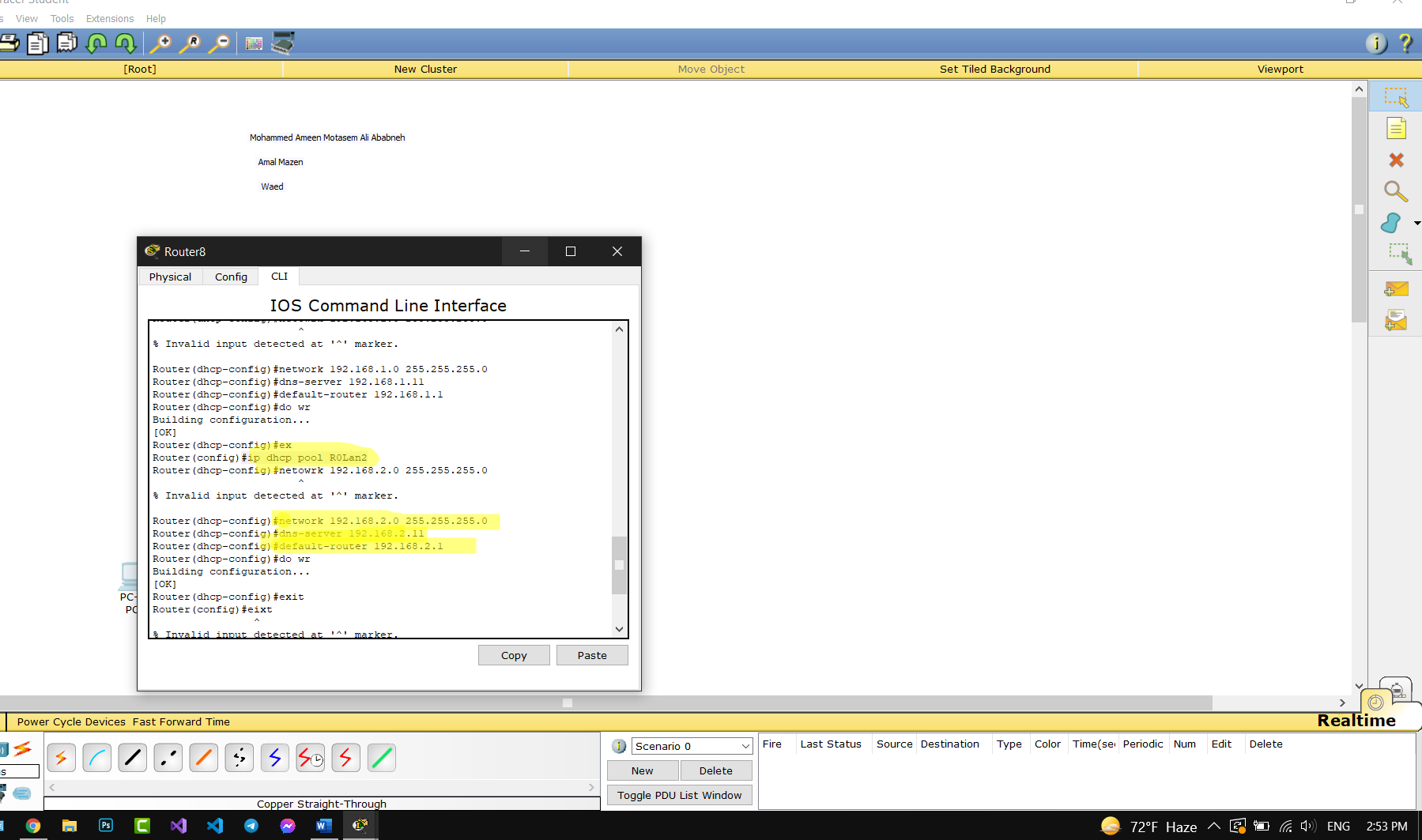
**Do as the previous pool, name it as R0Lan2:**

#ip dhcp pool R0Lan2

Router(dhcp-config)#network 192.168.2.0 255.255.255.0

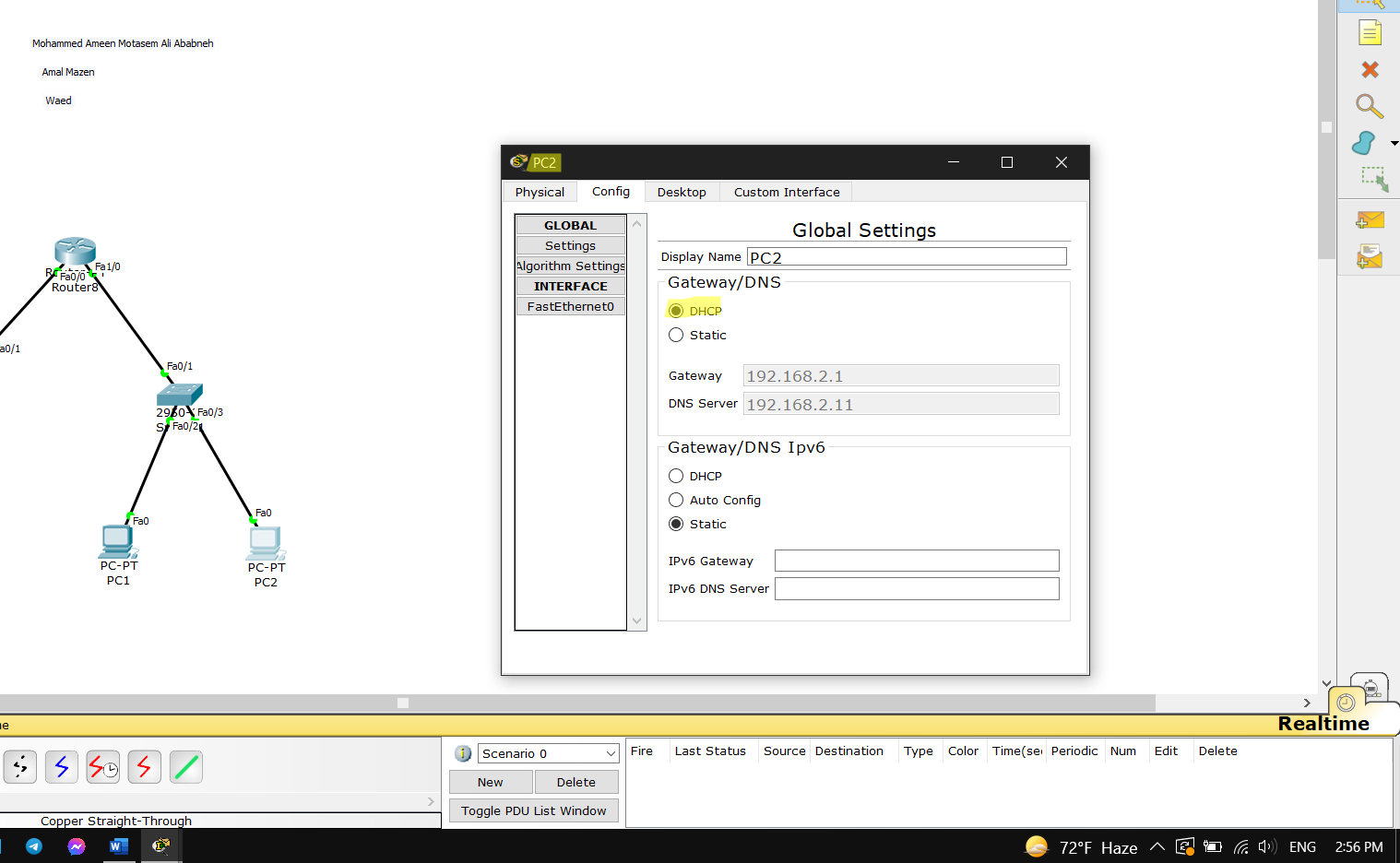
Router(dhcp-config)#dns-server 192.168.2.11

Router(dhcp-config)#default-router 192.168.2.1

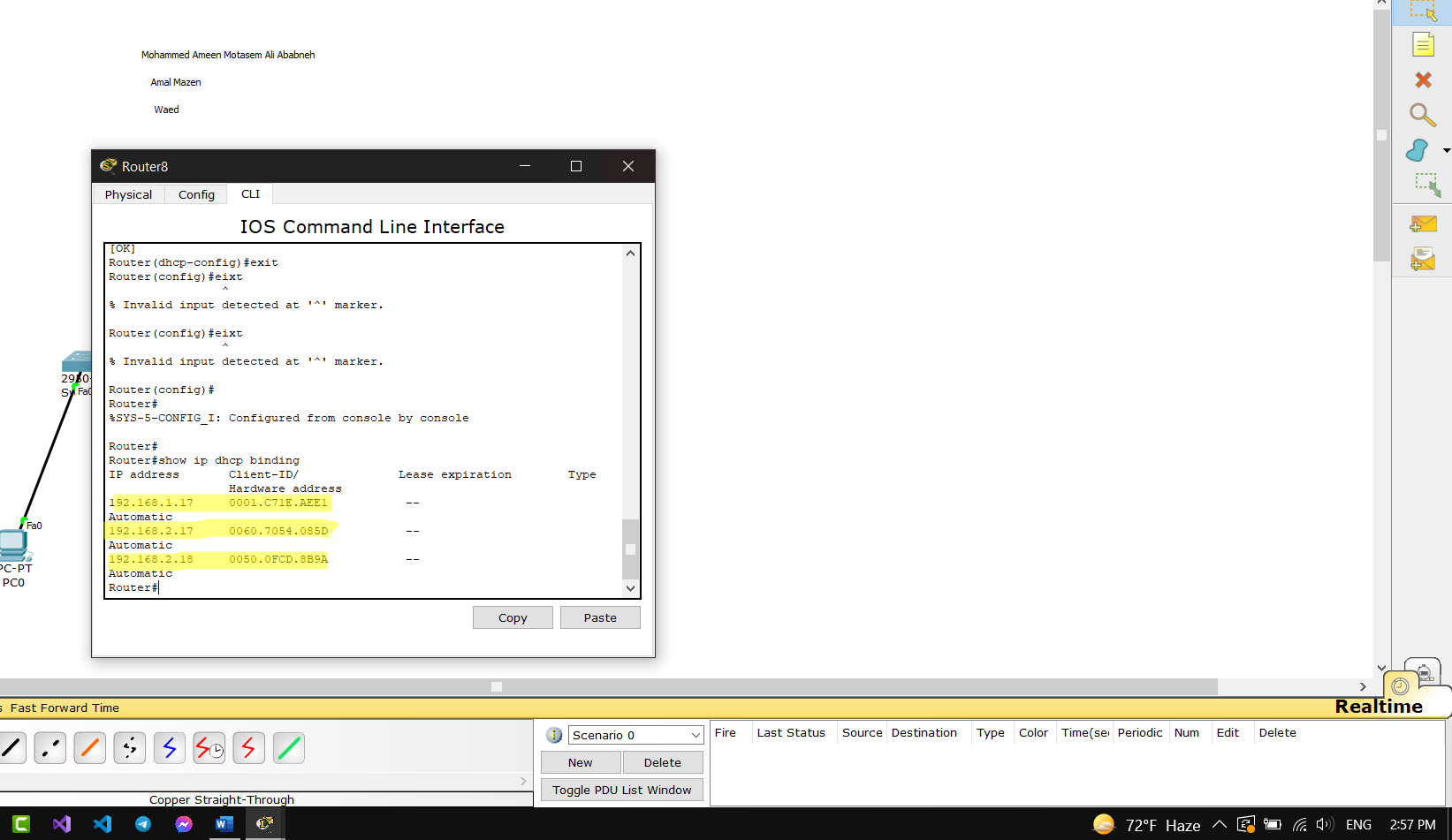


* **Verify the DHCP configuration.**

1. Now go to the IP configuration of the 3 PCs and change the IP configuration mode to DHCP.



1. Use the command **show ip dhcp binding (**Displays a list of all bindings created on a specific DHCP Server). What do you see. Explain.



1. NOW what is the IP address assigned to the PC1, PC2 and PC3?

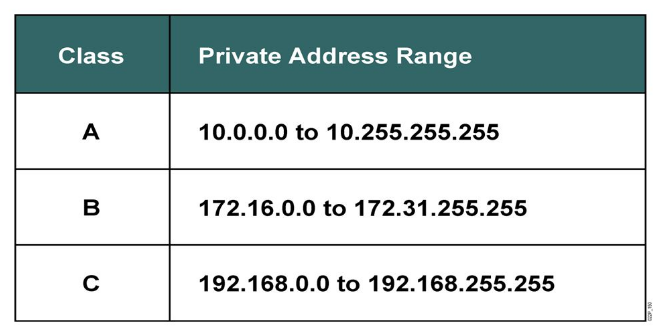
**PC1:** 192.168.1.17

**PC2:** 192.168.2.17

**PC3:** 192.168.2.18

Part 2: Static NAT

**Task2: Configure Static Nat**

The Internet Assigned Numbers Authority (**IANA**) reserves the following IP address blocks for use as private IP addresses:

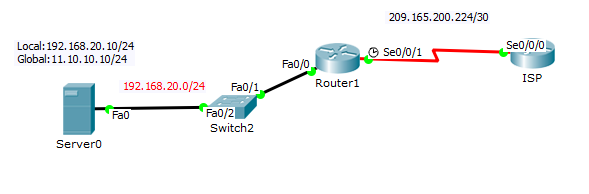
These addresses are for private, internal network use only. Packets containing these addresses are not routed over the Internet and are referred to as non-routable addresses.

Unlike public IP addresses, private IP addresses are a reserved block of numbers that can be used by anyone. That means two networks, or two million networks, can each use the same private addresses. To prevent addressing conflicts, routers must never route private IP addresses.

Network Address Translation (NAT) provides the mechanism to translate private addresses to public addresses.

Before NAT, a host with a private address could not access the Internet. Using NAT, individual companies can address some or all of their hosts with private addresses and use NAT to provide access to the Internet.

**Topology Diagram:**



**Step 1: Statically map a public IP address to a private IP address.**

Statically assign the public IP address 11.10.10.10 as the address for NAT to use to map packets to the private IP address of the inside server.

**R1(config)# ip nat inside source static private Address Public Address**

* Assign the public IP address 11.10.10.10 as the address for NAT to use to map packets to the private IP address of the inside server.

**R1(config)#**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Step 2: Specify inside and outside NAT interfaces.**

Before NAT can work, you must specify which interfaces are inside and which interfaces are outside.

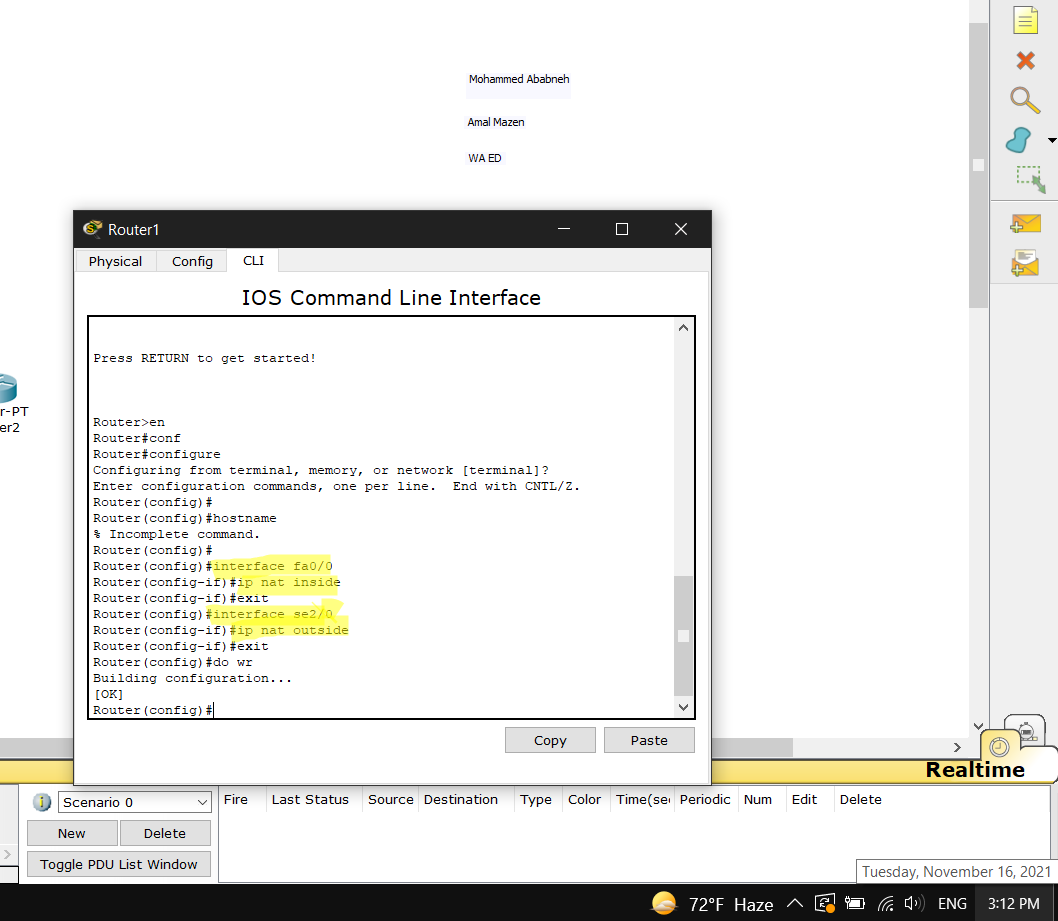
R1(config)#**interface InterName**

R1(config-if)#**ip nat outside**

R1(config-if)#**interface InterName**

R1(config-if)# **ip nat inside**

* Specify the interfaces of R1 as inside and outside interfaces.



**R1(config** # interface fa0/0

**R1(config-if)#** #ip nat inside

**R1(config)#** interface se2/0

**R1(config-if)#** #ip nat outside

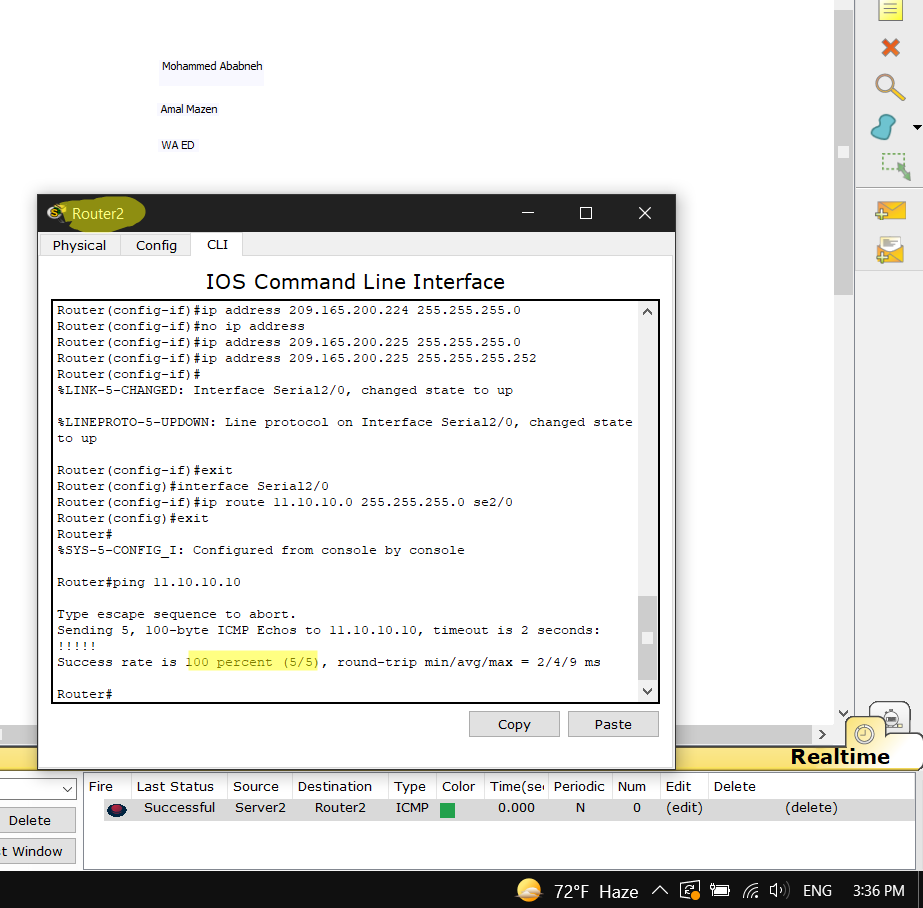
**Task 3: Configure Static Routing**

ISP uses static routing to reach all networks beyond R1. However, R1 translates private addresses into public addresses before sending traffic to ISP. Therefore, ISP must be configured with the public addresses that are part of the NAT configuration on R1. Enter the following static route on ISP:

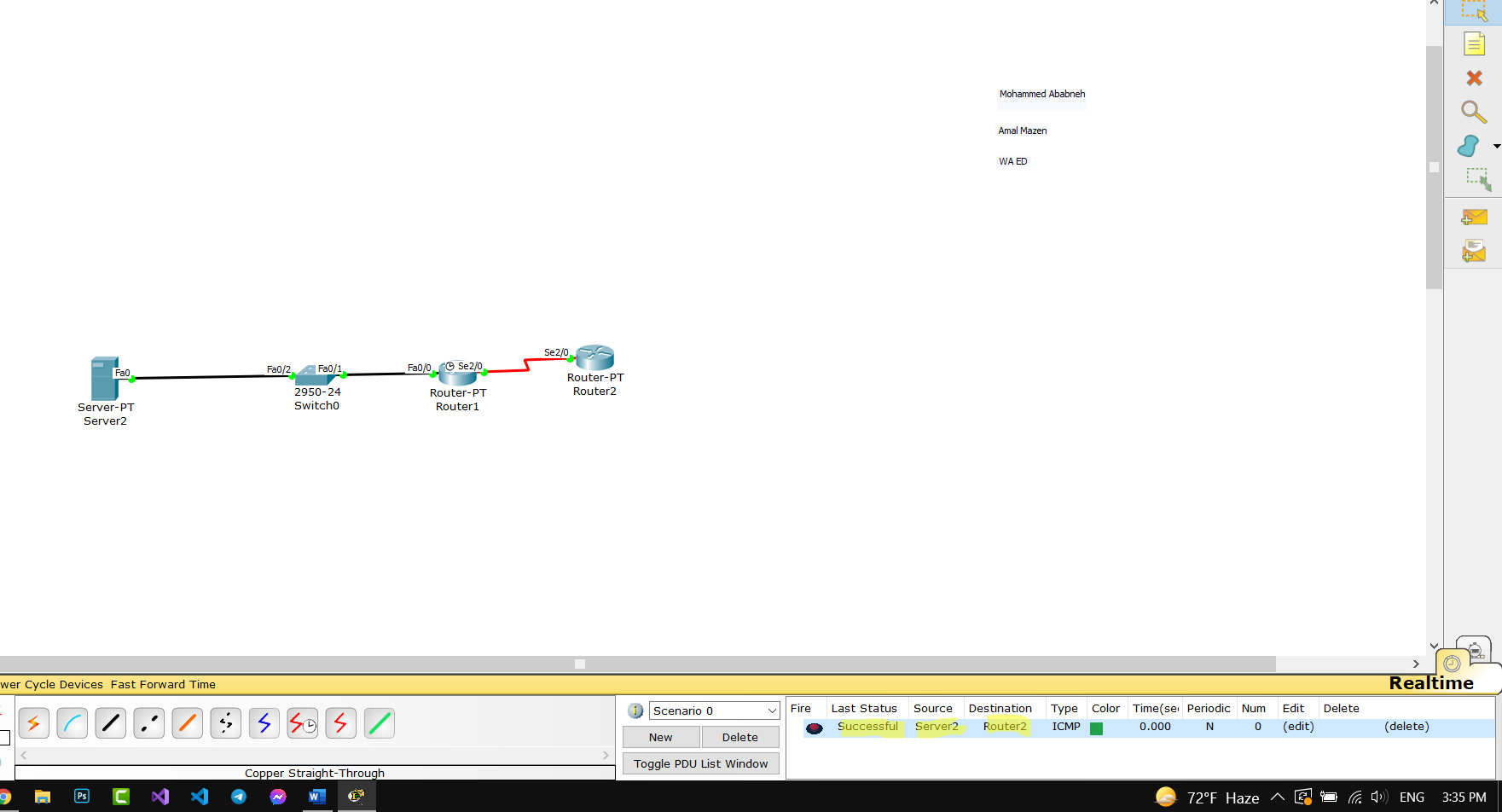
ISP(config)#**ip route 11.10.10.0 255.255.255.0 se 0/0/0**

**Task 4: Verify the static NAT configuration.**

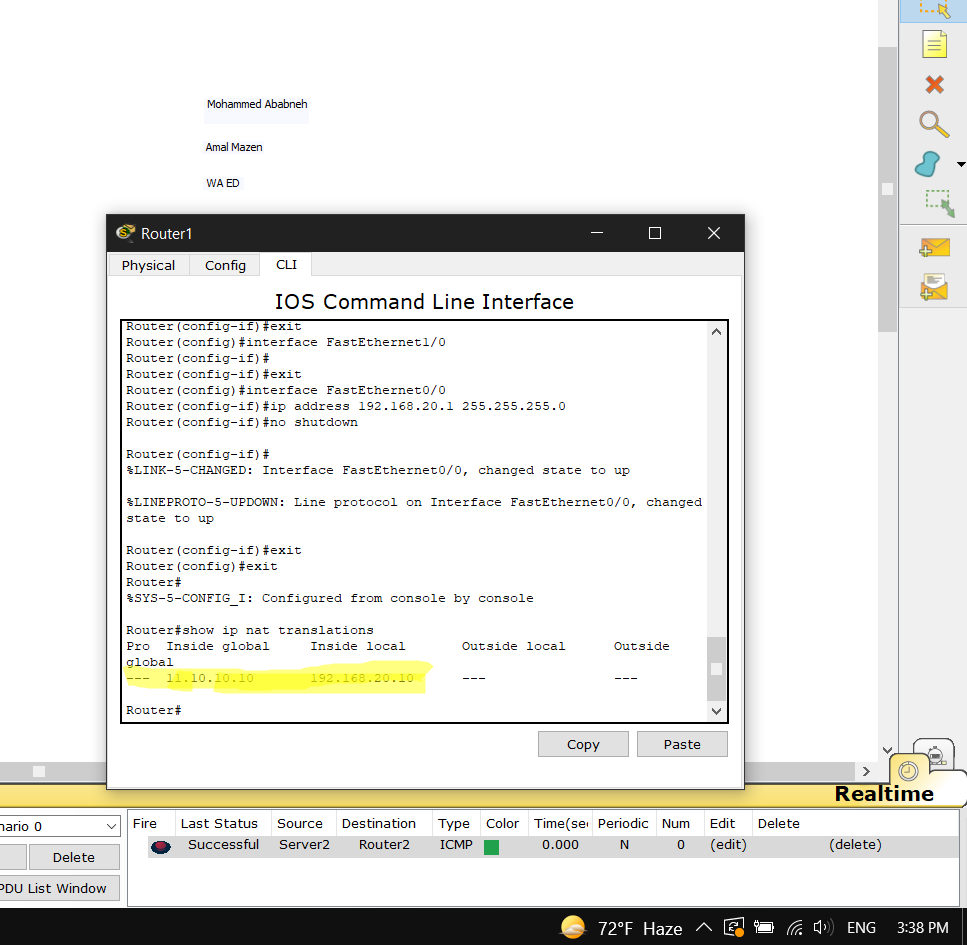
* From ISP, ping the public IP address 11.10.10.10

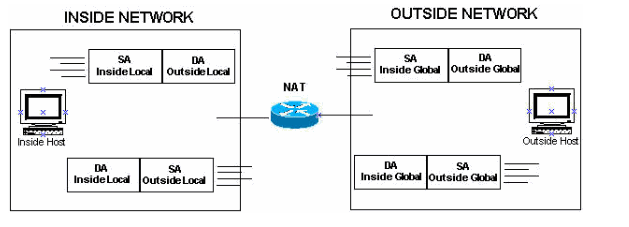


* From Server0, ping ISP.



* Use the command **show ip nat translations**. What do you see?





* **Inside and Outside refer to the IP addresses within the networks**
* **Local and Global refer to the network spaces**

* **Inside Local**

**"IP address that is used to identify my computer** - **Inside IP address",**

**"in the internal network** -**Local",**

* **Inside Global**

**"IP address that is used to identify my computer - Inside IP address",**

**"in the external network - Global",**

* **Outside Global**

**"IP address that is used to identify the computer of the external network - Outside IP address",**

**"within the external network - Global",**

* **6. Outside Local**

**"IP address that is used to identify the computer of the external network - Outside IP address",**

**"within the local network - Local",**