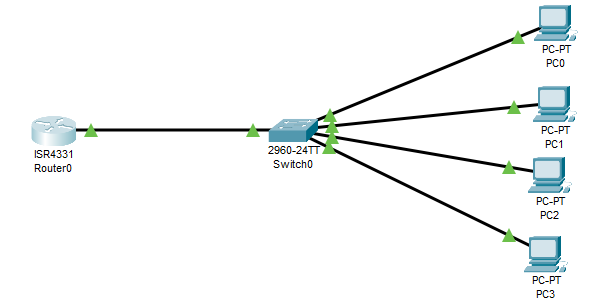
9. Configure a router as DHCP server to allocate IP addresses to network clients.



Aim: To configure a router as DHCP server to allocate IP addresses to the network clients.

Algoirthm:

Step 1: Start the process.

Step 2: Open Cisco packet tracer and place network devices and connect them as per requirement.

Step 3: Configure IP address for the interface of the router and exclude it from the DHCP IP.

Step 4: Assign the range of IP addresses for the DHCP server as dhcp pool.

Step 5: Configure the network, default-router and dns-server for the DHCP router.

Step 6: Configure dynamic IPs for all PCs by clicking DHCP option and verify them with ip dhcp binding command in router.

Step 7: Stop the process.

**Router**

>en

#conf t

#int g0/0/0

#ip add 192.168.1.100 255.255.255.0

#no sh

#exit

#ip dhcp excluded-address 192.168.1.100

#ip dhcp pool 192.168.1.0-192.168.1.254

#network 192.168.1.0 255.255.255.0

#default-router 192.168.1.100

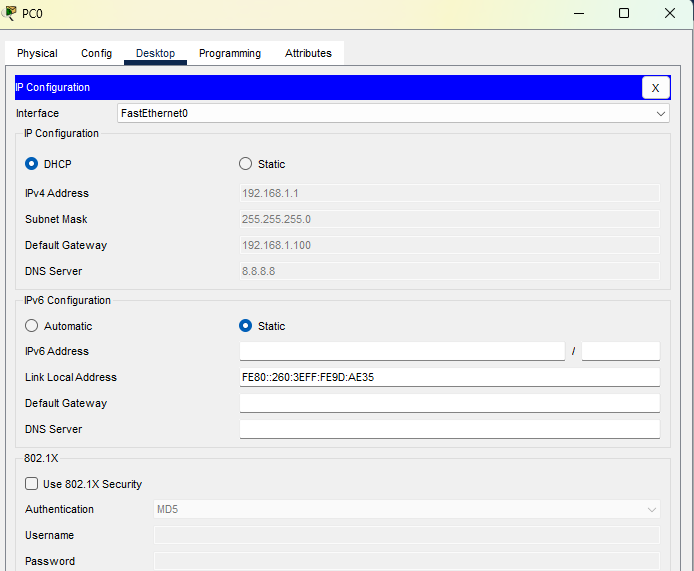
#dns-server 8.8.8.8

#end

Go to ALL PC -> IP Configuration -> Select DHCP

#show ip dhcp binding

Output:



10. Configure and secure TELNET and SSH access.

**Aim:** To configure and secure TELNET and SSH access.

Algorithm:

Step 1: Start the process.

Step 2: Open Cisco Packet tracer and place the network devices and connect them as required.

Step 3: Configure the IP address on interfaces, enable password and line vty passwords of all routers.

Step 4: Specify transport input ssh command to make the Router 3 to listen SSH connections

Step 5: Configure the domain name and crypto key generation rsa in the Router 3.

Step 6: Telnet the Router 2 from Router 1 and then ssh the Router 3.

Step 7: Stop the process.

**Router 1**

>en

#conf t

#hostname R1

#int g0/0/0

#ip add 192.168.1.1 255.255.255.0

#no shut

#exit

#enable secret kasc

#line vty 0 4

#password ctit

#login

#exit

#end

#wr

**Router 2**

Router>en

#conf t

#enable secret kasc

#line vty 0 4

#password ctit

#login

#exit

#int g0/0/0

#ip add 192.168.1.1 255.255.255.0

#no shut

#exit

#int g0/0/0

#ip add 192.168.1.2 255.255.255.0

#no shut

#exit

#int g0/0/1

#ip add 192.168.2.1 255.255.255.0

#no shut

#exit

#end

>wr

**Router 3**

>en

#hostname R3

#conf t

#hostname R3

#int g0/0/0

#ip add 192.168.2.2 255.255.255.0

#no sh

#exit

#

#enable secret kasc

#line vty 0 4

#transport input ssh

#password ctit

#exit

#ip domain-name kasc.ac.in

#crypto key generate rsa

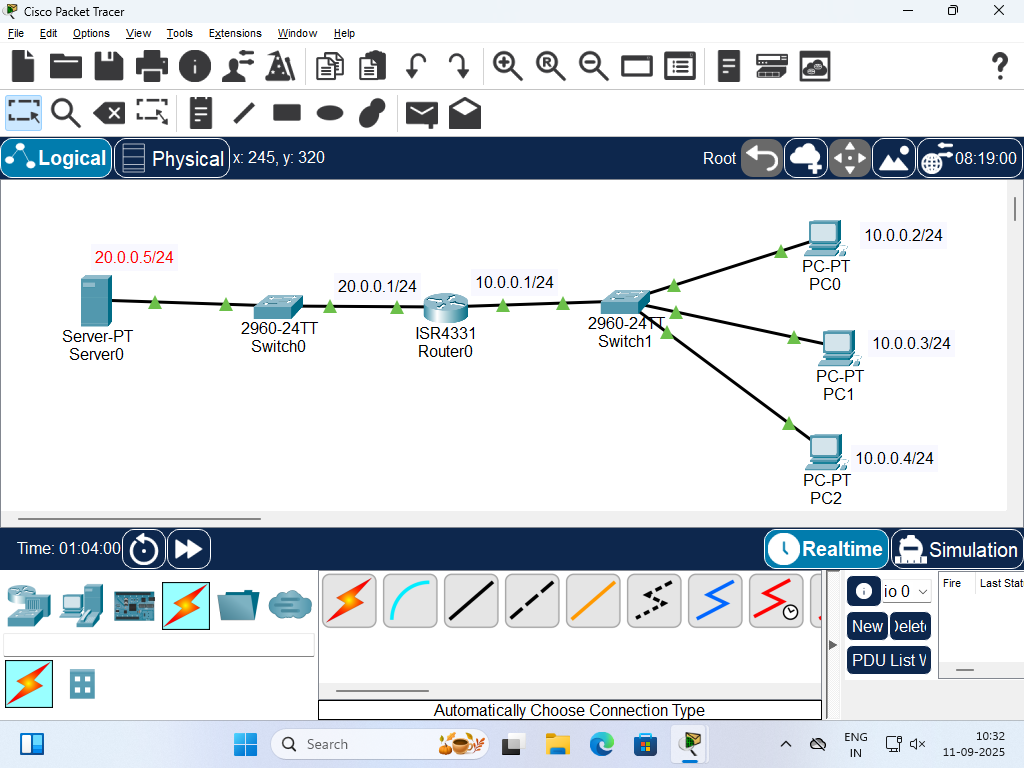
The name for the keys will be: R3.kasc.ac.in

How many bits in the modulus [512]: 512

#end

#wr

11. Write standard access list to restrict network access.



Aim: To write standard access list to restrict network access.

Algorithm:

Step 1: Start the Process

Step 2: Open Cisco packet tracer, place the network devices and connect them as per requirement

Step 3: Configure IP addresses on all devices and interfaces

Step 4: Configure the standard access list to permit PC 1, PC2 and deny PC3 for accessing the server.

Step 5: Specify ip access-group in the router interface.

Step 6: Verify the configuration from all PCs by using ping

Step 7: Stop the process

>en

#conf t

#hostname R1

#int g0/0/0

#ip add 20.0.0.1 255.255.255.0

#no shut

#exit

#int g0/0/1

#ip add 10.0.0.1 255.255.255.0

#no shut

#exit

#ip access-list standard 1

#permit 10.0.0.2 0.0.0.0

#permit 10.0.0.3 0.0.0.0

#deny 10.0.0.4 0.0.0.0

#exit

#int g0/0/0

#ip access-group 1 out

#exit

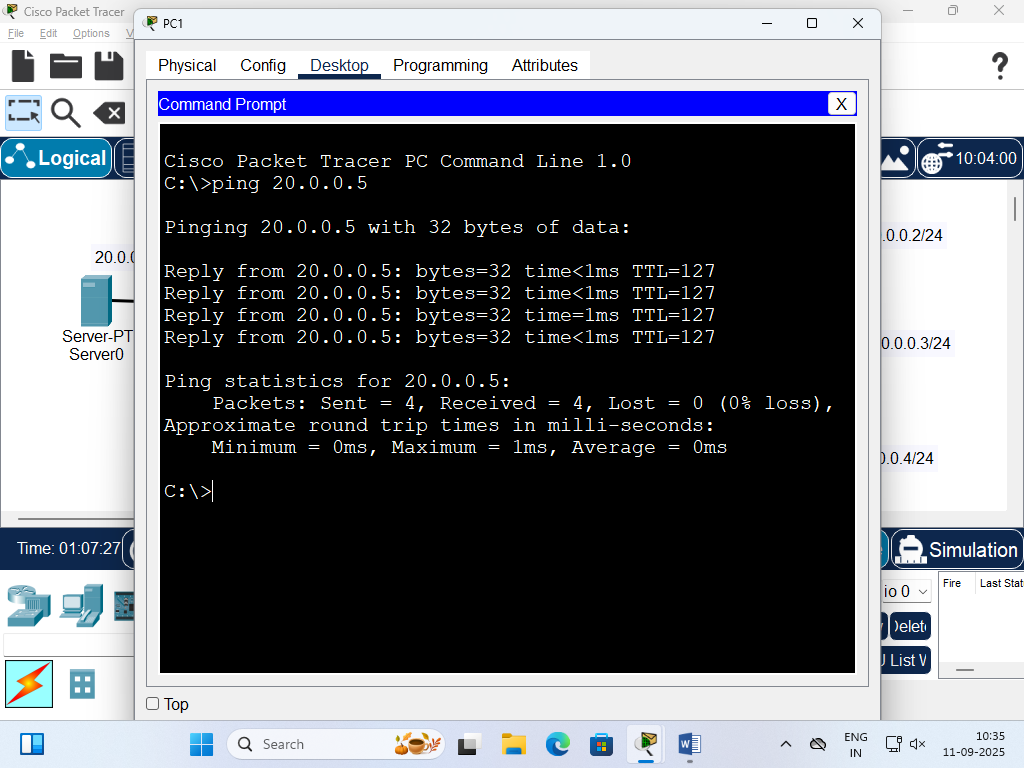
#end

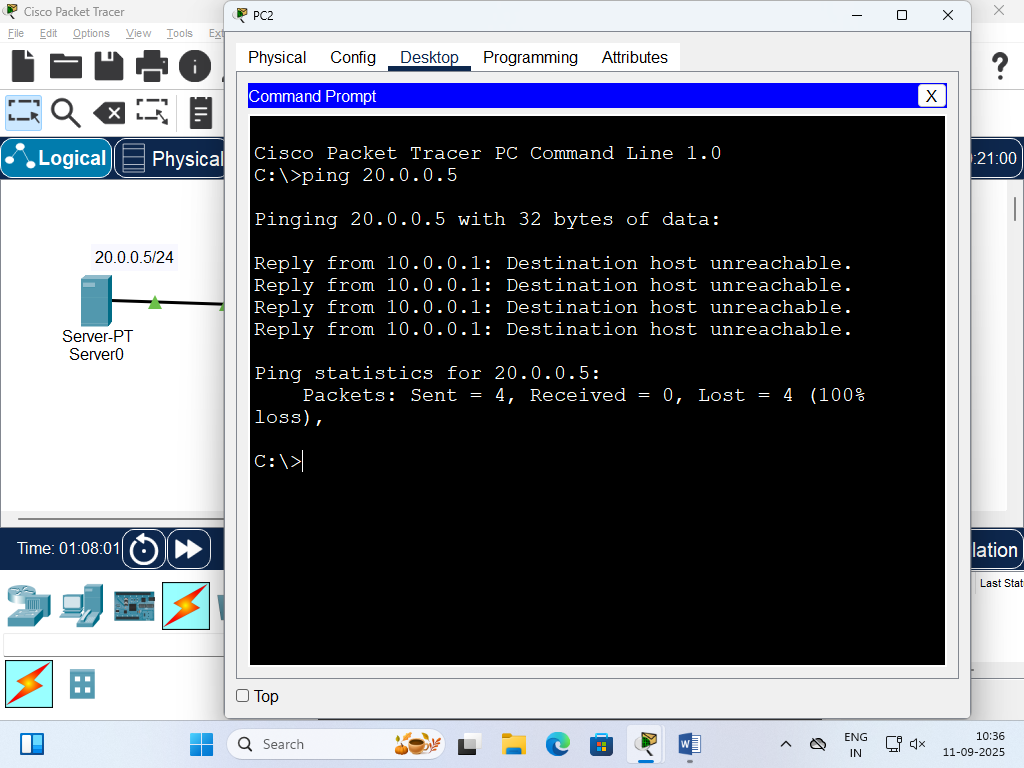
#wr

Output:

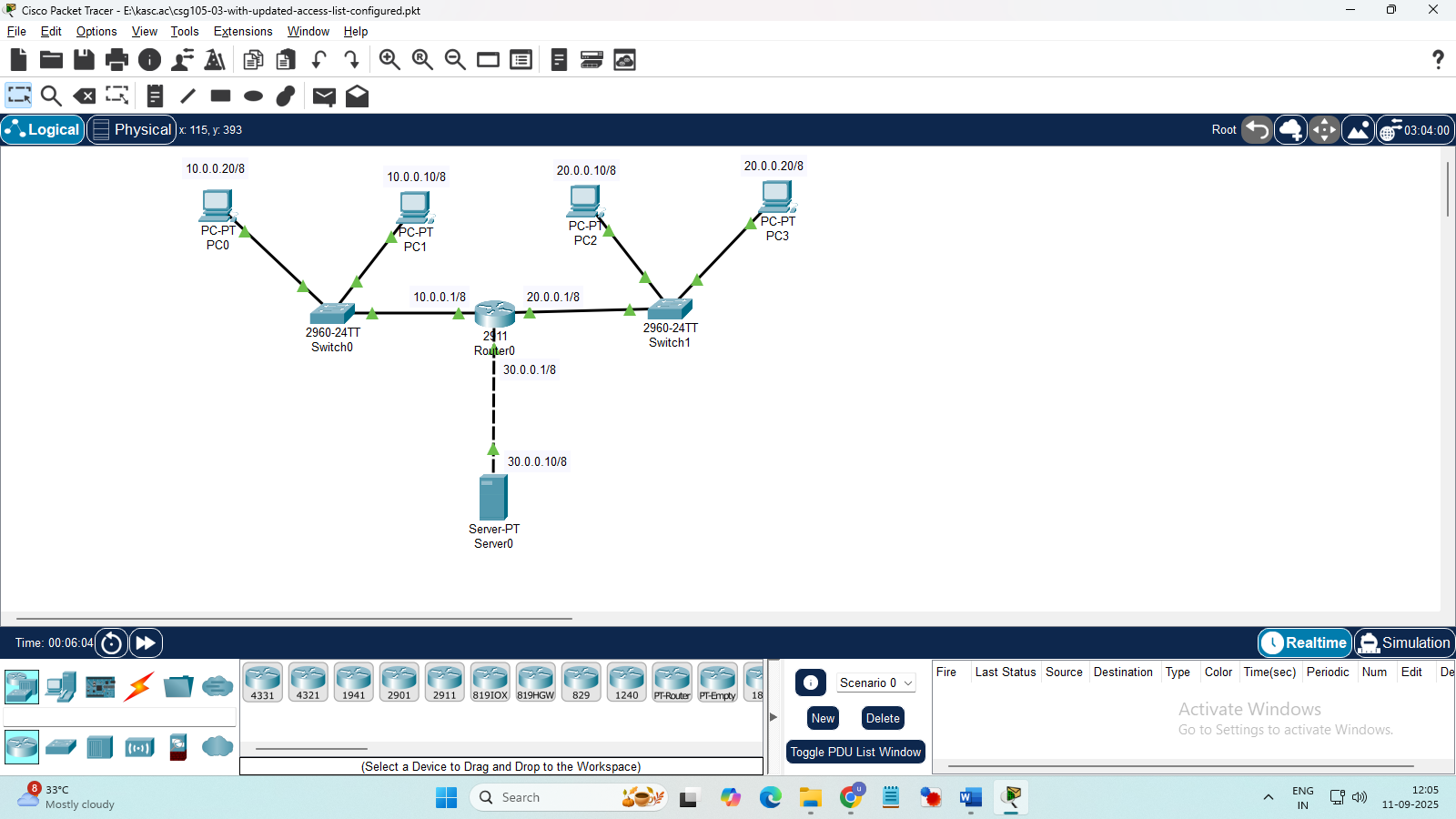
From all PC

Ping 20.0.0.5





12. Write extended access list for advanced traffic filtering.



Aim: To write extended access list for advanced traffic filtering.

Algorithm:

Step 1: Start the Process

Step 2: Open Cisco packet tracer, place the network devices and connect them as per requirement

Step 3: Configure IP addresses on all devices and router interfaces

Step 4: Configure the extended access list to permit tcp, udp access to server from a network, permit access to the other network and deny ip access to the server.

Step 5: Specify ip access-group in the router interface.

Step 6: Verify the configuration from all PCs by using ping

Step 7: Stop the process

>en

#conf t

#int g0/0/0

#ip add 10.0.0.1 255.0.0.0

#no shut

#exit

#int g0/0/1

#ip add 20.0.0.1 255.0.0.0

#no shut

#exit

#int g0/0/2

#ip add 30.0.0.1 255.0.0.0

#no shut

#exit

#ip access-list extended BlockMarketing

#permit tcp 10.0.0.0 0.255.255.255 host 30.0.0.10 eq 80

#permit udp 10.0.0.0 0.255.255.255 host 30.0.0.10 eq 53

#deny ip 10.0.0.0 0.255.255.255 host 30.0.0.10

#permit ip 10.0.0.0 0.255.255.255 20.0.0.0 0.255.255.255

#deny ip 10.0.0.0 0.255.255.255 any

#exit

#int g0/0/0

#ip access-group BlockMarketing in

Output:

Ping the other PCs from PC0

Ping the server from PC0

