

CSE 3502

INFORMATION SECURITY MANAGEMENT



Lab Assessment – 2

L19+L20 | SJT516
Dr. Lavanya K

WINTER SEMESTER 2021-22

by

SHARADINDU ADHIKARI

19BCE2105

Exp 2. Part 1: Cisco Router Show Commands

1.1. INTRODUCTION

- Cisco routers run an operating system, called IOS (Internetwork Operating System). Like any operating system, IOS includes a command language to enable equipment owners to retrieve information and change the device's settings.
- A large number of commands are available on Cisco routers, as well as many different protocols and features that can be used to establish a network.
- The following commands are used to gather information on a Cisco IOS Software-based router when attempting to learn basic information about a router, or possibly troubleshooting protocol-independent problems:
 - show version
 - show running-config
 - show interfaces
 - show logging
 - show tech-support
- One of the most powerful commands in IOS is `show`. This command retrieves information and can be used to examine nearly everything about a Cisco router and its configuration. This part of the assignment revolves around exploring router with the `show` commands.

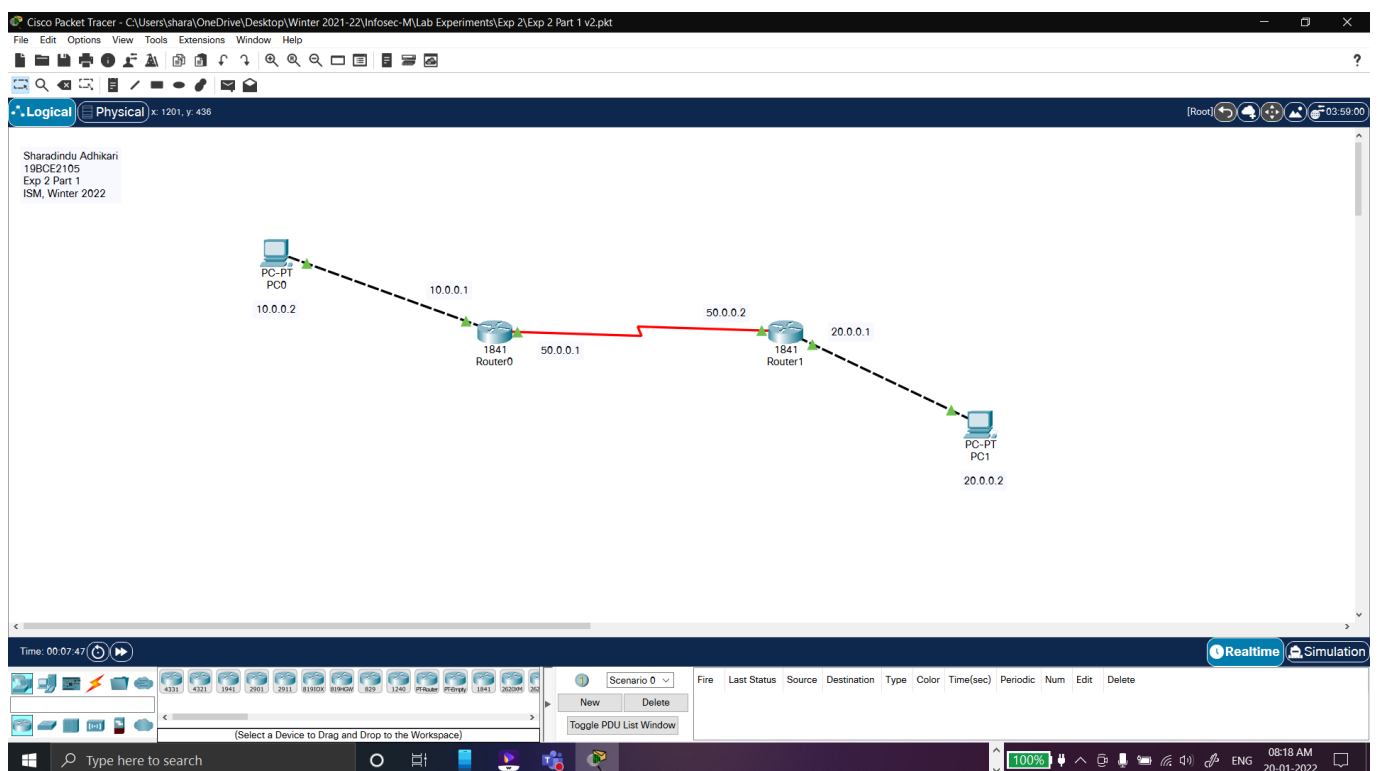
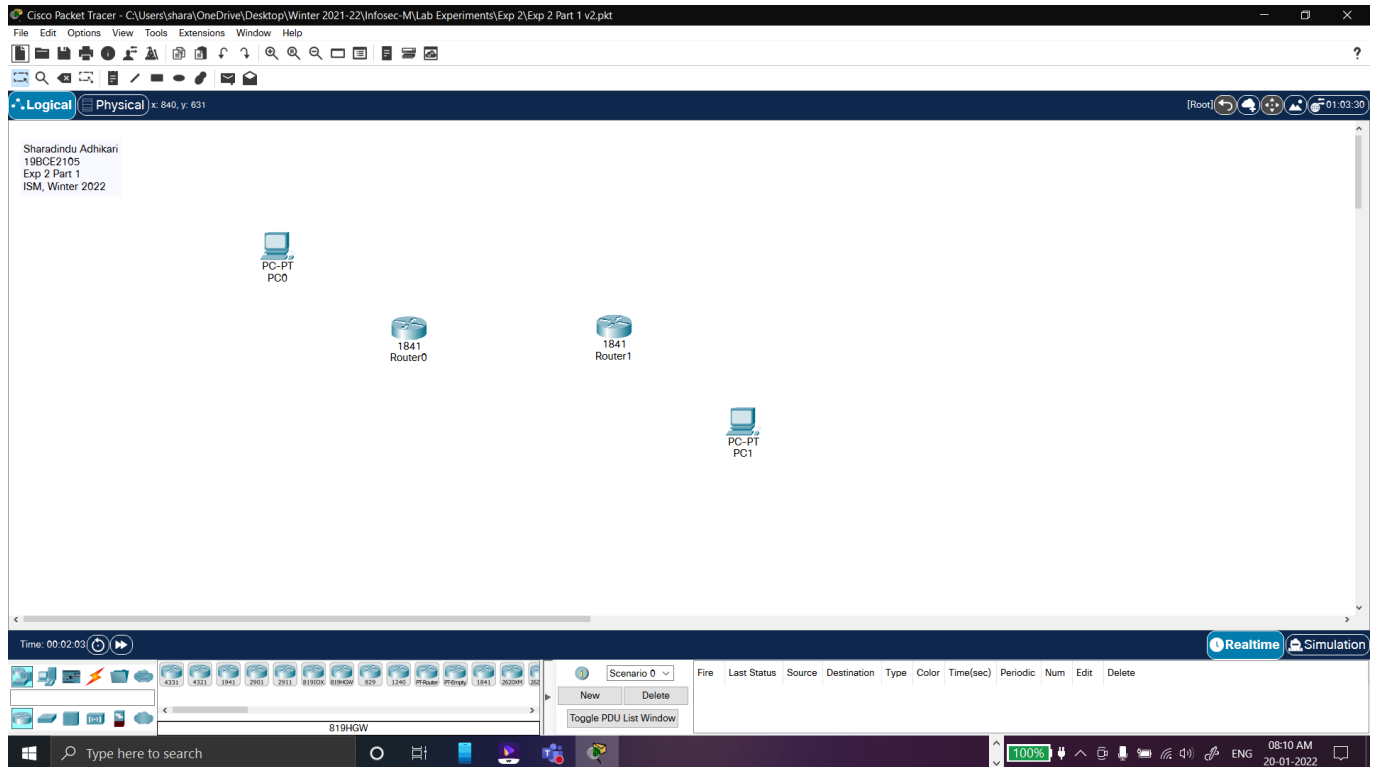
1.2. COMPONENTS

Component / Device / Interface	Connected To	IP Address
PCs		
PC0	FastEthernet0/0 of Router0	10.0.0.2 / 255.0.0.0
PC1	FastEthernet0/0 of Router 1	20.0.0.2 / 255.0.0.0
Routers		
Router0 (FastEthernet0/0)	PC0	10.0.0.1 / 255.0.0.0
Router0 (Serial0/0/0)	Serial0/0/0 of Router1	50.0.0.1 / 255.0.0.0
Router1 (Serial0/0/0)	Serial0/0/0 of Router0	50.0.0.2 / 255.0.0.0
Router 1 (FastEthernet0/0)	PC1	20.0.0.1 / 255.0.0.0

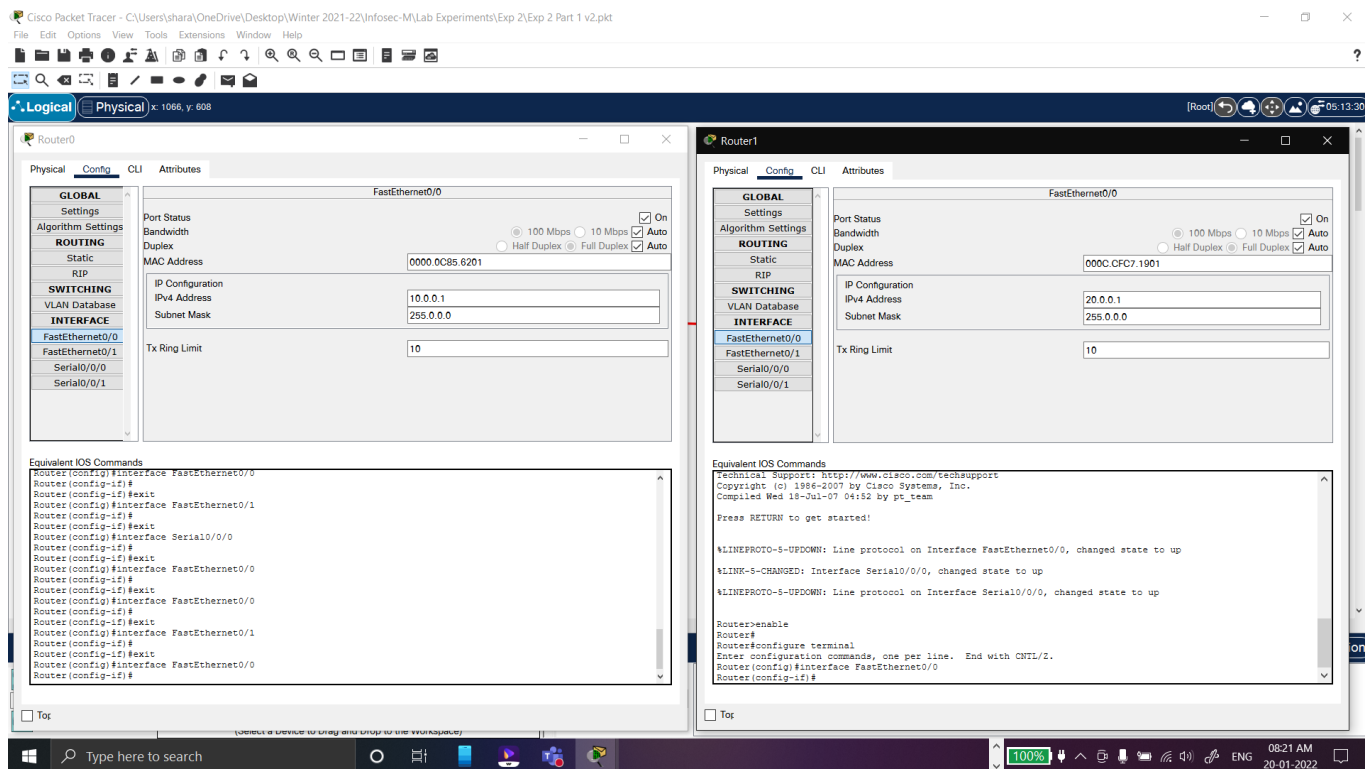
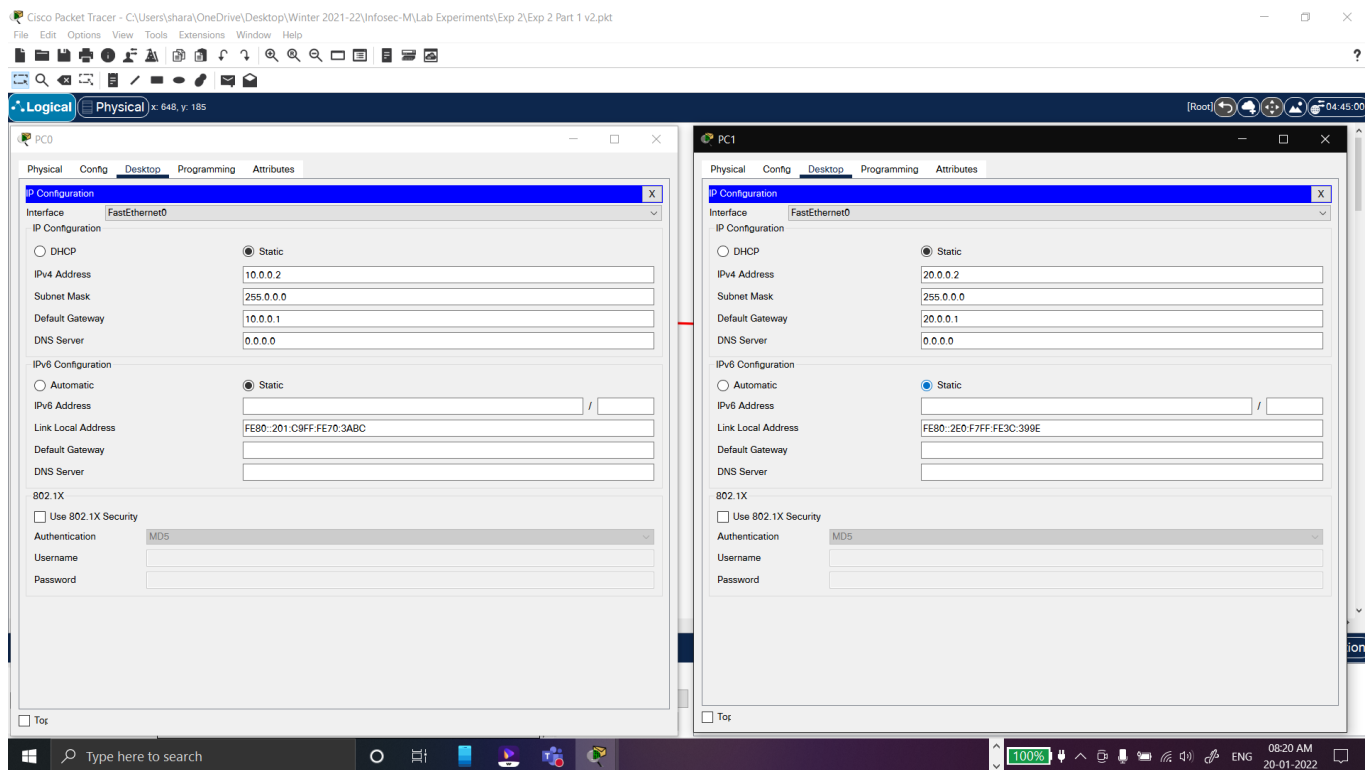
- PC-PTs and 1841 Routers are the only components here.
- RIP Routing Protocol is configured on both routers 0 and 1.
- Clock rate and bandwidth is assigned on the Serial Interface 0/0/0 of Router0.

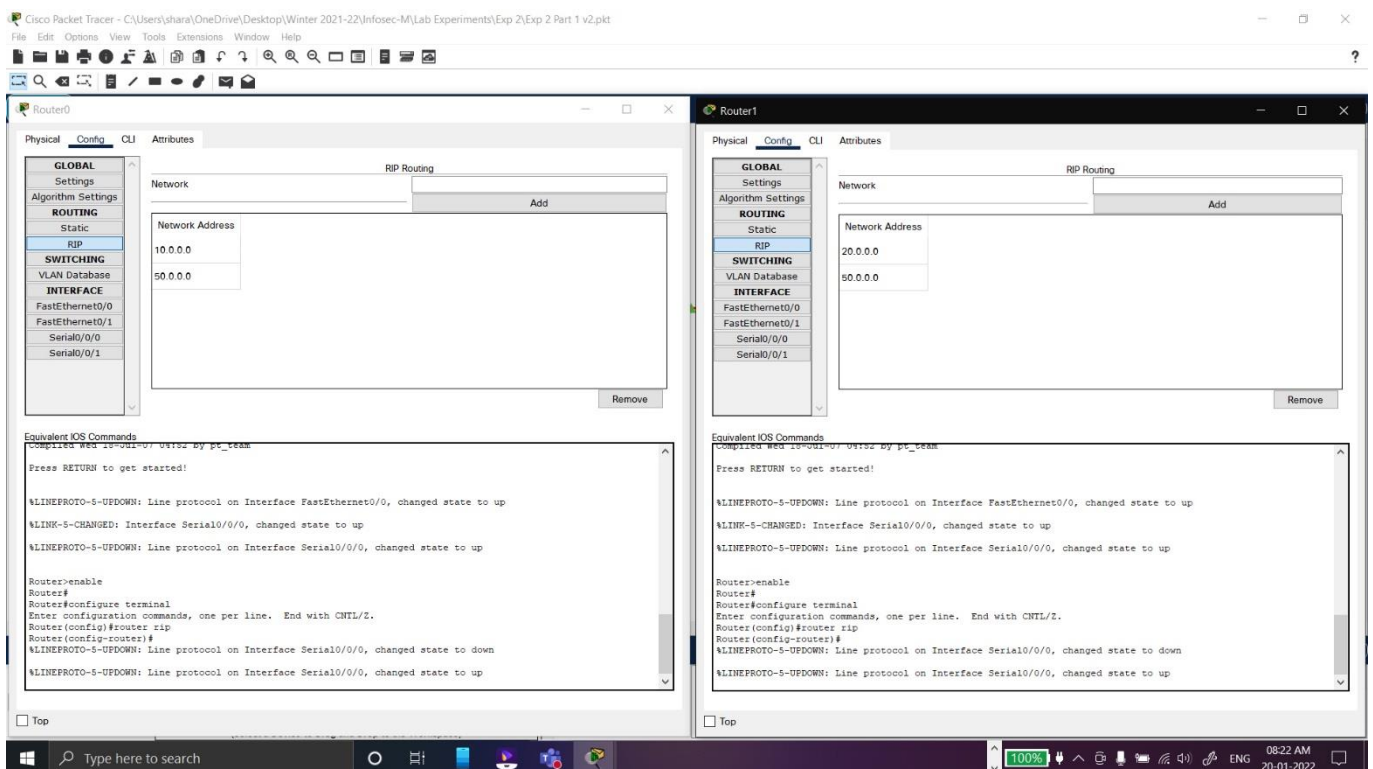
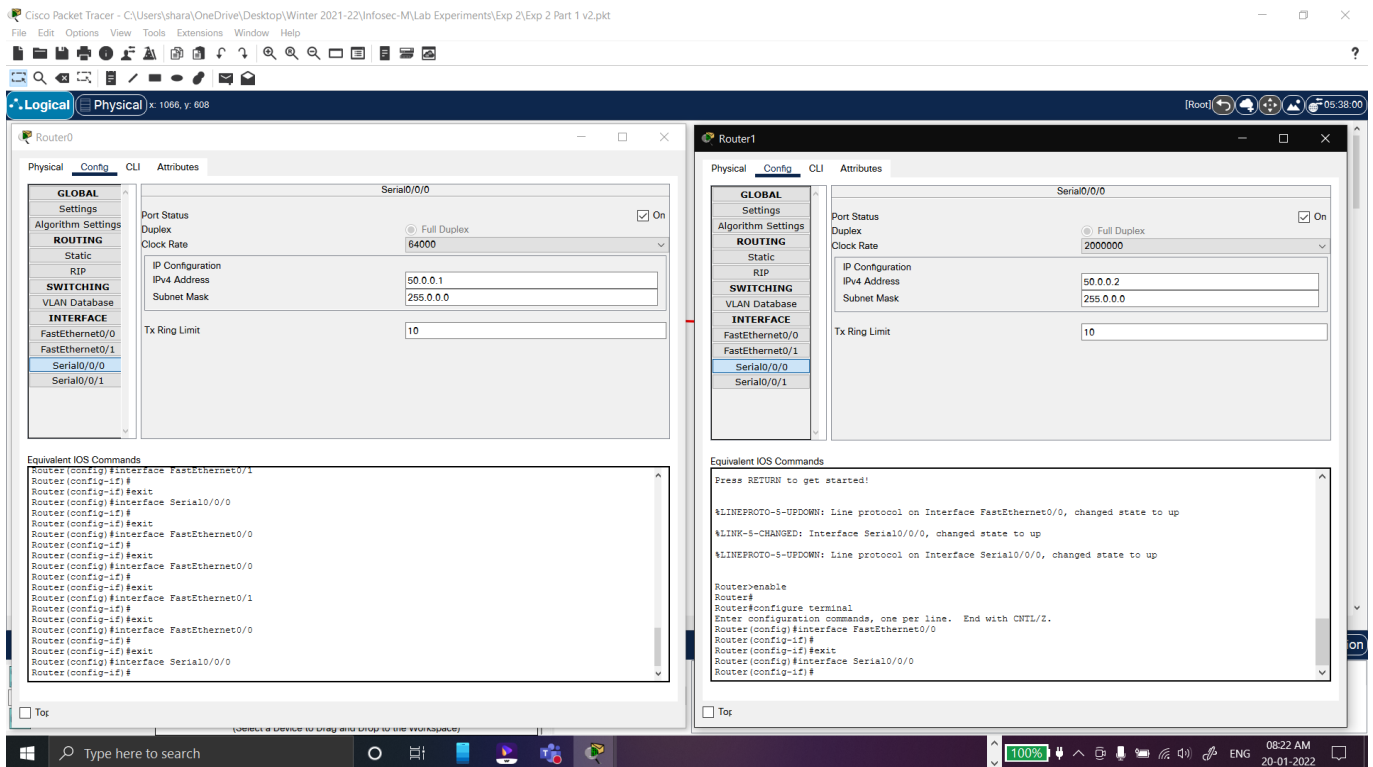
1.3. SNAPSHOTS & COMMANDS

Step 1: Making the Topology



Step 2: Assigning the IPs and Configuring





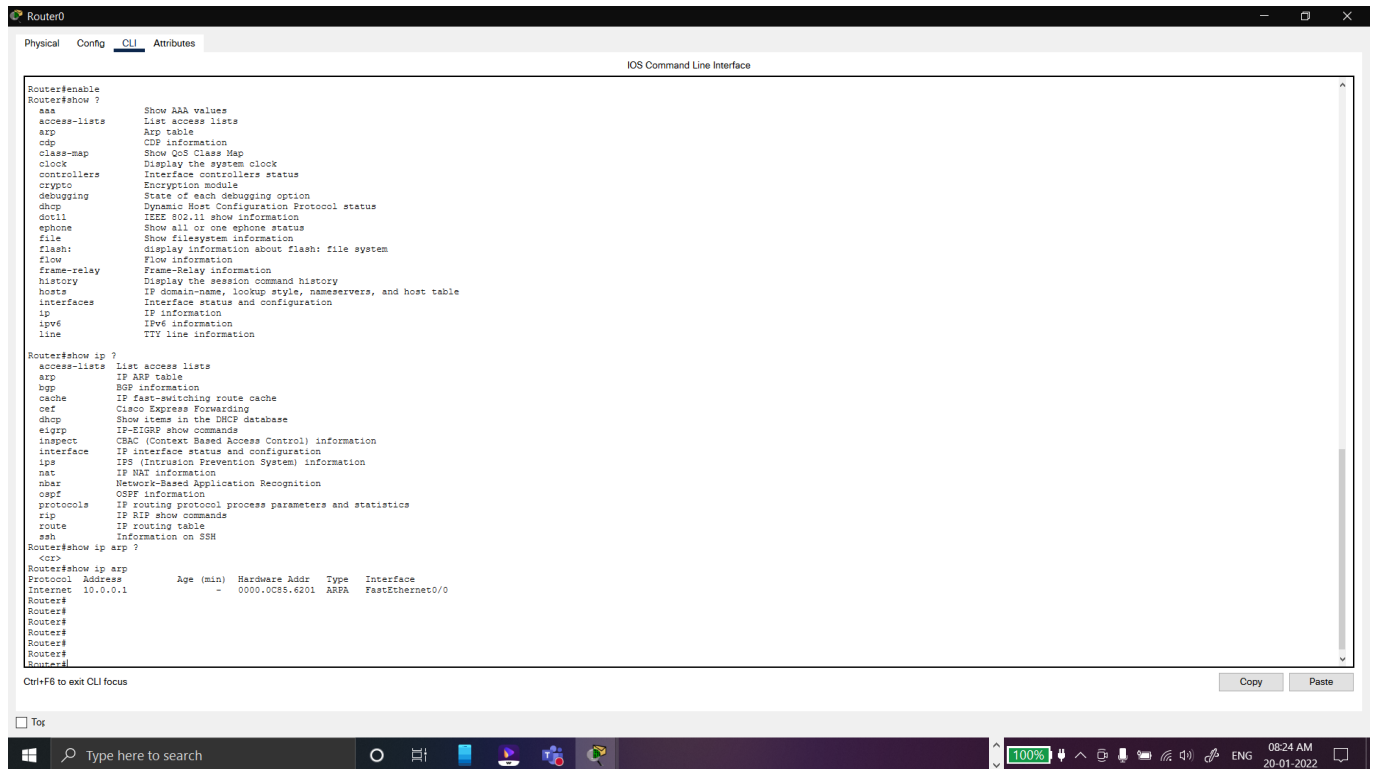
Step 3: Cisco Router Show Commands

First, we type in the `enable` command to enter in privilege exec mode. Then use the `show` command, paired with `?` (Question mark) to list all available commands.

Router#show ip

To display IP configuration data, enter the show ip command in User Exec mode or Privileged Exec mode.

```
Router#show ip [address-table | route | http [server secure]]
```



Router#show interfaces

This command shows the status and configuration of interfaces. By default, it will display all interfaces. But we can limit it to particular interface. To view the detail of specific interface we can use the following command:

```
Router#show interface [type slot_# port_#]
```

For example, to view the detail of serial 0/0/0 interface on Router0, we will use the following command:

```
Router#show interface serial 0/0/0
```

Router#show ip interface brief

This command provides a quick overview of all interfaces on the router including their IP addresses and status.

Router#show controllers [type slot_# port_#]

This command is used to check the hardware statistic of interface including clock rate and cable status such as cable is attached or not. One end of serial cable is physically DTE, and the other end is DCE. If cable is attached, it will display the type of cable.

For example, Router#show controllers serial 0/0/0

```
Router#
Router#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up (connected)
Hardware is HD64570
Internet address is 50.0.0.1/8
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/0/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 48 kilobits/sec
5 minute input rate 15 bits/sec, 0 packets/sec
5 minute output rate 15 bits/sec, 0 packets/sec
30 packets input, 1560 bytes, 0 no buffer
Received 29 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
31 packets output, 1612 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 output buffer failures, 0 output buffers swapped out

Router#show ip interface brief
Interface      IP-Address      OK? Method Status      Protocol
FastEthernet0/0 10.0.0.1        YES manual up          up
FastEthernet0/1 unassigned      YES unset  administratively down down
Serial0/0/0     50.0.0.1        YES manual up          up
Serial0/0/1     unassigned      YES unset  administratively down down
Vlan1           unassigned      YES unset  administratively down down

Router#show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is PowerPC MPC860
DCE V.35, clock rate 64000
IDB at 0x81081AC0, driver data structure at 0x81084AC0
SOC Registers:
General [GSR]=0x210x00000000, Protocol-specific [PSMR]=0x8
Events [SCCE]=0x0000, Mask [SCCM]=0x0000, Status [SCCS]=0x00
Transmit on Demand [TCOR]=0x0, Data Sync [DSR]=0x07FE
Interrupt Registers:
Config [CICR]=0x000007F80, Pending [CIPR]=0x00000000
Mask [CIMR]=0x00000000, In-srv [CISR]=0x00000000
Command register [CR]=0x880
Port A [PADIR]=0x1030, [PARAR]=0x0FFF
[PACOR]=0x0010, [PARAT]=0x00FF
Port B [PBDIR]=0x0800F, [PBPAR]=0x0800E
[PBCOR]=0x00000, [PBAT]=0x03FFD
Port C [PCDIR]=0x00C, [PCPAR]=0x000
[PCOR]=0x0C20, [PCDAT]=0x0DF2, [PCINT]=0x00F
Receive Ring
rmd(68012830): status 9000 length 600 address 3B6DAC4
Transmit Ring
rmd(68012830): status 8000 length 600 address 3B6D444

Ctrl+F6 to exit CLI focus
```

Router#show flash

This command displays the content of flash memory, used space and available space. By default, router stores IOS image file in flash. We can use this command to check the available space in Flash memory while updating / restoring IOS files.

Router#show version

This command displays information about software version of running IOS. It also provides information about configuration setting. It shows current configuration register setting that is used to reset the password of router.

Router#show hosts

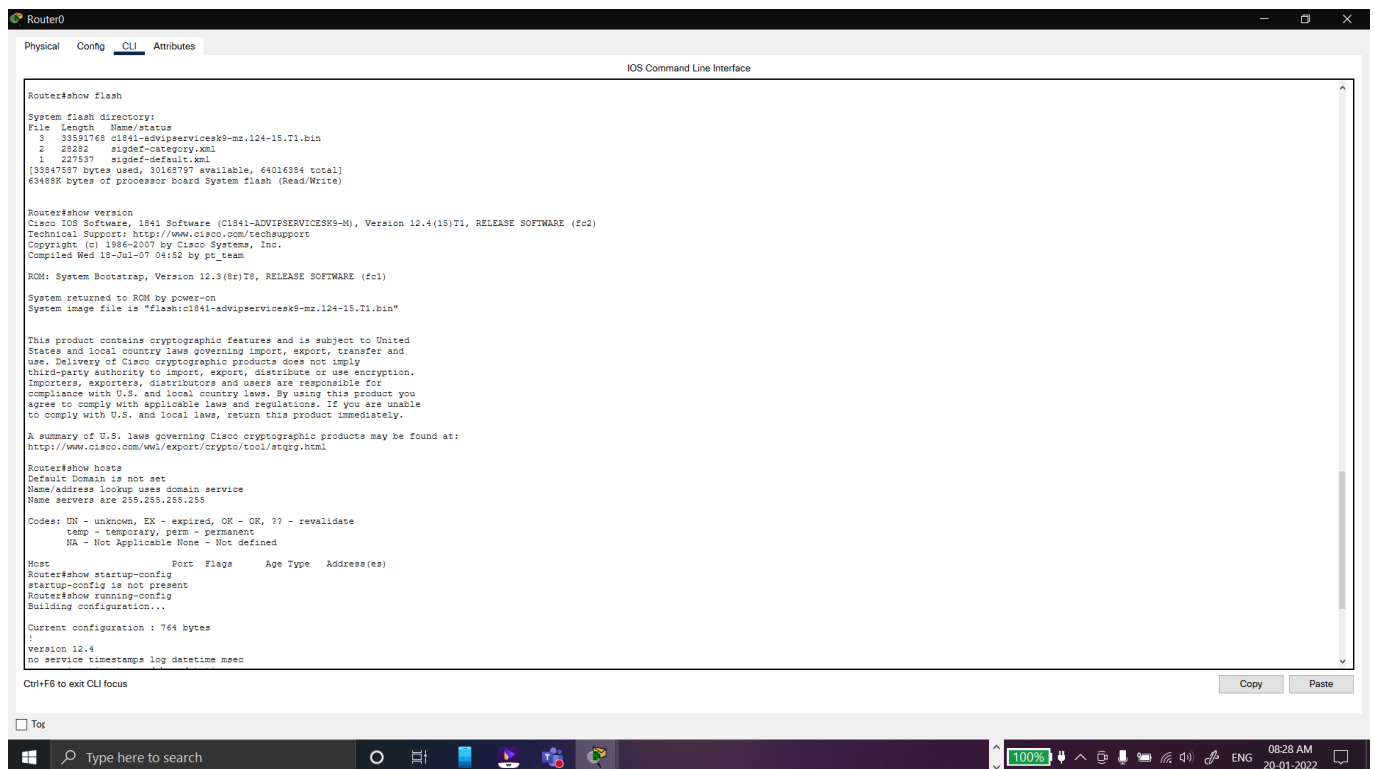
To display the DNS name servers and domain name that our Server Switch uses, we enter the `show host` command in User Exec mode or Privileged Exec mode. This command has no arguments or keywords.

Router#show startup-config

Routers load configuration from NVRAM in start-up. This command will display the configuration stored in NVRAM.

Router#show running-config

Router keeps all running configuration in RAM. This command will display the configuration currently running in RAM.



```
Router0
Physical Config CLI Attributes
IOS Command Line Interface

Router#show flash
System flash directory:
File Length Name/status
  3 33591768 c1841-advip-servicesk9-mz.124-15.T1.bin
  2 25282 sigdef-category.xml
  1 227537 sigdef-default.xml
[33547587 bytes used, 30168797 available, 64016384 total]
63485K bytes of processor board System flash (Read/Write)

Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 16-Jul-07 04:52 by pt_team

ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)
System returned to ROM by power-on
System image file is "flash:c1841-advip-servicesk9-mz.124-15.T1.bin"

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wml/export/crypto/steering.html

Router#show hosts
Default Domain is not set
Name/address lookup uses domain service
Name servers are 255.255.255.255

Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
temp - temporary, perm - permanent
NA - Not Applicable None - Not defined

Host Port Flags Age Type Address(es)
Router#show startup-config
startup-config is not present
Router#show running-config
Building configuration...

Current configuration : 764 bytes
!
version 12.4
no service timestamps log datetime msec

Ctrl+F6 to exit CLI focus
Copy Paste
```

Router#show clock

To display the current system time, we enter the `show clock` command in User Exec mode or Privileged Exec mode.

Router#show users

This command displays users currently connected to the router.

Router#show arp

This command displays ARP cache table. ARP table is used to resolve the hardware MAC addresses.

Router#show protocols

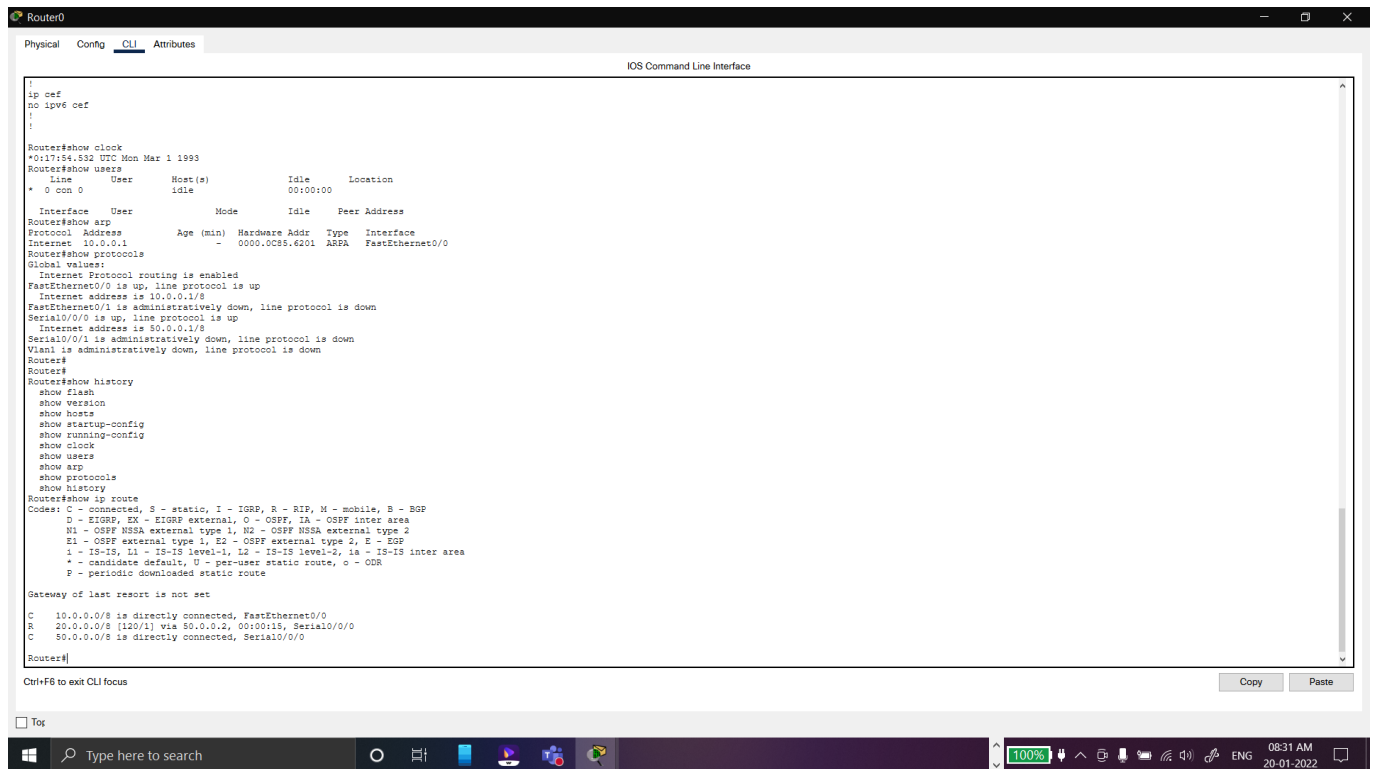
This command shows the status of configured layer three protocols on the device.

Router#show history

Router keeps a history of used command. This command will list the used command on that level.

Router#show ip route

Routers use routing table to take packet forward decision. This command displays routing table.



The screenshot displays the Cisco Router CLI interface with the following content:

```
Router0
Physical Config CLI Attributes
IOS Command Line Interface

!
ip cef
no ipv6 cef
!
!
Router#show clock
*01:17:54.552 UTC Mon Mar 1 1993
Router#show users
  Line      User      Host(s)      Idle      Location
  *  0 con 0
Router#show arp
  Interface      User      Mode      Idle      Peer Address
Router#show asp
Protocol Address      Age (min)  Hardware Addr  Type  Interface
Internet  10.0.0.1
Router#show protocols
Global values:
Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
Internet address is 10.0.0.1/8
FastEthernet0/1 is administratively down, line protocol is down
Serial0/0/0 is up, line protocol is up
Internet address is 50.0.0.1/8
Serial0/0/1 is administratively down, line protocol is down
Vlan1 is administratively down, line protocol is down
Router#
Router#
Router#show history
show flash
show version
show hosts
show startup-config
show running-config
show clock
show users
show arp
show protocols
show history
Router#show ip route
Codes: C - connected, S - static, I - IGRP, B - BGP, M - mobile, S - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, IA - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        S - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/0
R    20.0.0.0/8 [120/1] via 50.0.0.2, 00:00:15, Serial0/0/0
C    50.0.0.0/8 is directly connected, Serial0/0/0

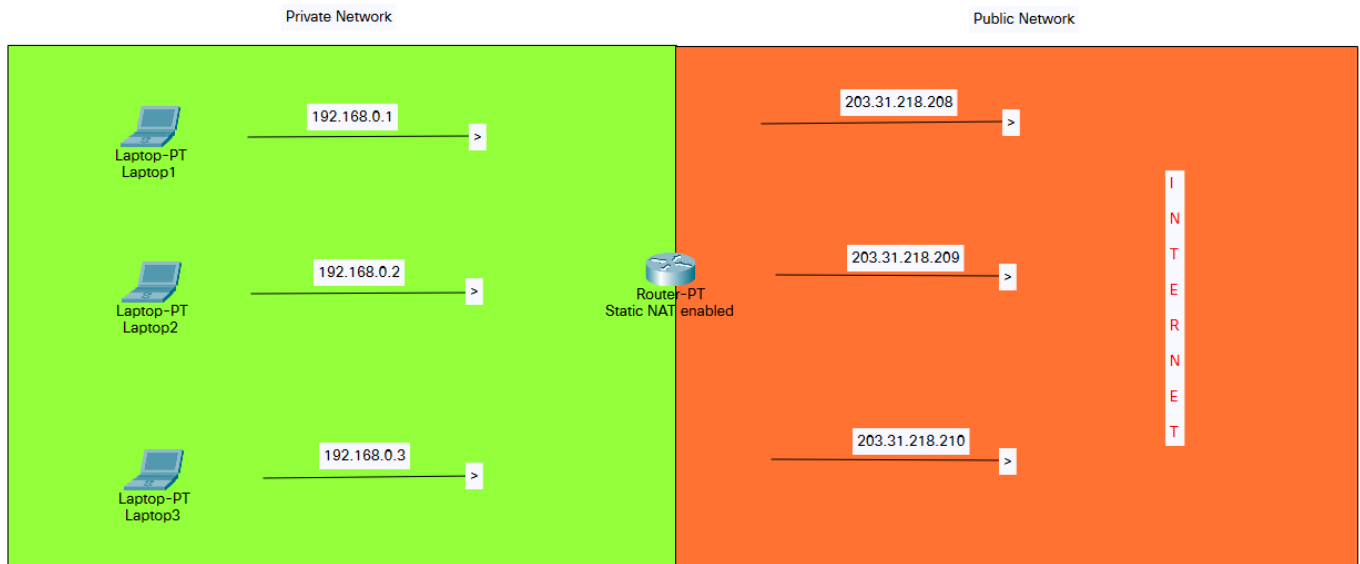
Router#
```

At the bottom of the window, there is a taskbar with a search bar, application icons, and system tray information showing 100% CPU usage and the date 20-01-2022.

Exp 2. Part 2: Static NAT Configuration

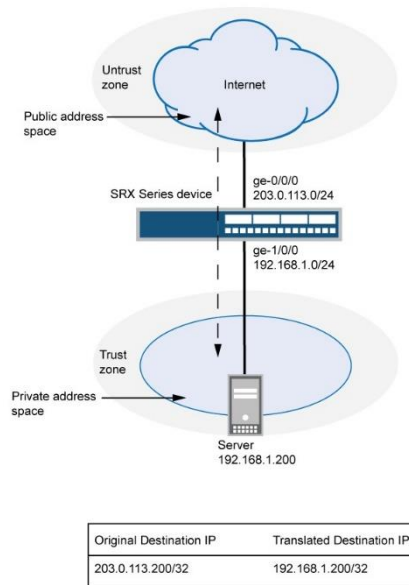
2.1. INTRODUCTION

- A static network address translation (static NAT) is a type of NAT technique that routes and maps network traffic from a static public IP address to an internal private IP address and/or network. It enables providing external network or Internet connectivity to computers, servers or networking devices within a private local area network (private LAN) having an unregistered private IP address.
- A static NAT is primarily used in enterprise networks where many internal servers have unregistered IP addresses and are accessed by a global audience using static public IP addresses. It provides a means to ensure network transparency, security and privacy by hiding the details of internal network usage, architecture and patterns from external or public users.
- A static NAT works by creating a one-to-one relationship between the public and private IP address. This means the private IP address can be mapped to only one public IP address at a time. The end user, on the other hand, has a transparent view of the remote device/network and accesses it using the mapped public IP address.
- Static NAT allows connections to be originated from either side of the network, but translation is limited to one-to-one or between blocks of addresses of the same size. For each private address, a public address must be allocated. No address pools are necessary.
- Static Network Address Translation (NAT) rules specify two layers of match conditions:
 - Traffic direction — Allows you to specify from interface, from zone, or from routing-instance.
 - Packet information — Can be source addresses and ports, and destination addresses and ports.
- Static NAT also supports the following types of translation:
 - To map multiple IP addresses and specified ranges of ports to a same IP address and different range of ports.
 - To map a specific IP address and port to a different IP address and port.
- All IP translations take place within the router's memory and the whole process is totally transparent to both internal and external hosts. When hosts from the Internet try to contact the internal hosts, their packets will either be dropped or forwarded to the internal hosts depending on the router's & firewall configuration.
- In the diagram below, made in Packet Tracer, we can see that we have our private network connected to the Internet via our router, which has been configured for Static NAT mode. In this mode each private host has a single public IP Address mapped to it, e.g., private host 192.168.0.1 has the public IP Address 203.31.218.208 mapped to it. Therefore, any packets generated by 192.168.0.1 that need to be routed to the Internet will have their source IP field replaced with IP Address 203.31.218.208.

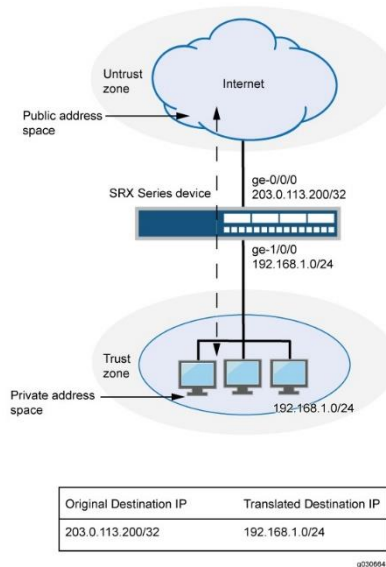


- The main configuration tasks for static NAT are as follows:
 - Configure static NAT rules that align with your network and security requirements.
 - Configure NAT proxy ARP entries for IP addresses in the same subnet of the ingress interface.

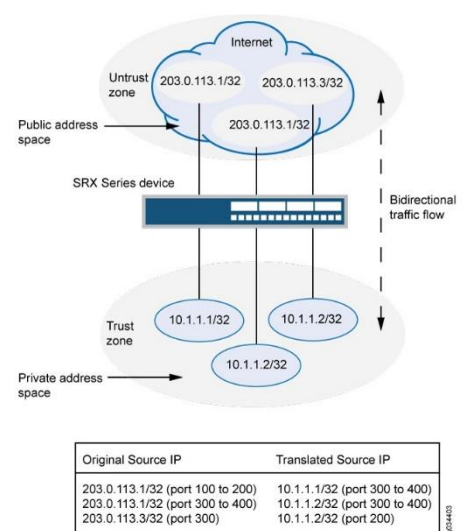
▪ Static NAT Config. for Single Address Translation



Subnet Translation



Port Mapping



- Because static NAT rules do not support overlapping addresses and ports, they should not be used to map one external IP address to multiple internal IP addresses for ALG traffic. For example, if different sites want to access two different FTP servers, the internal FTP servers should be mapped to two different external IP addresses.

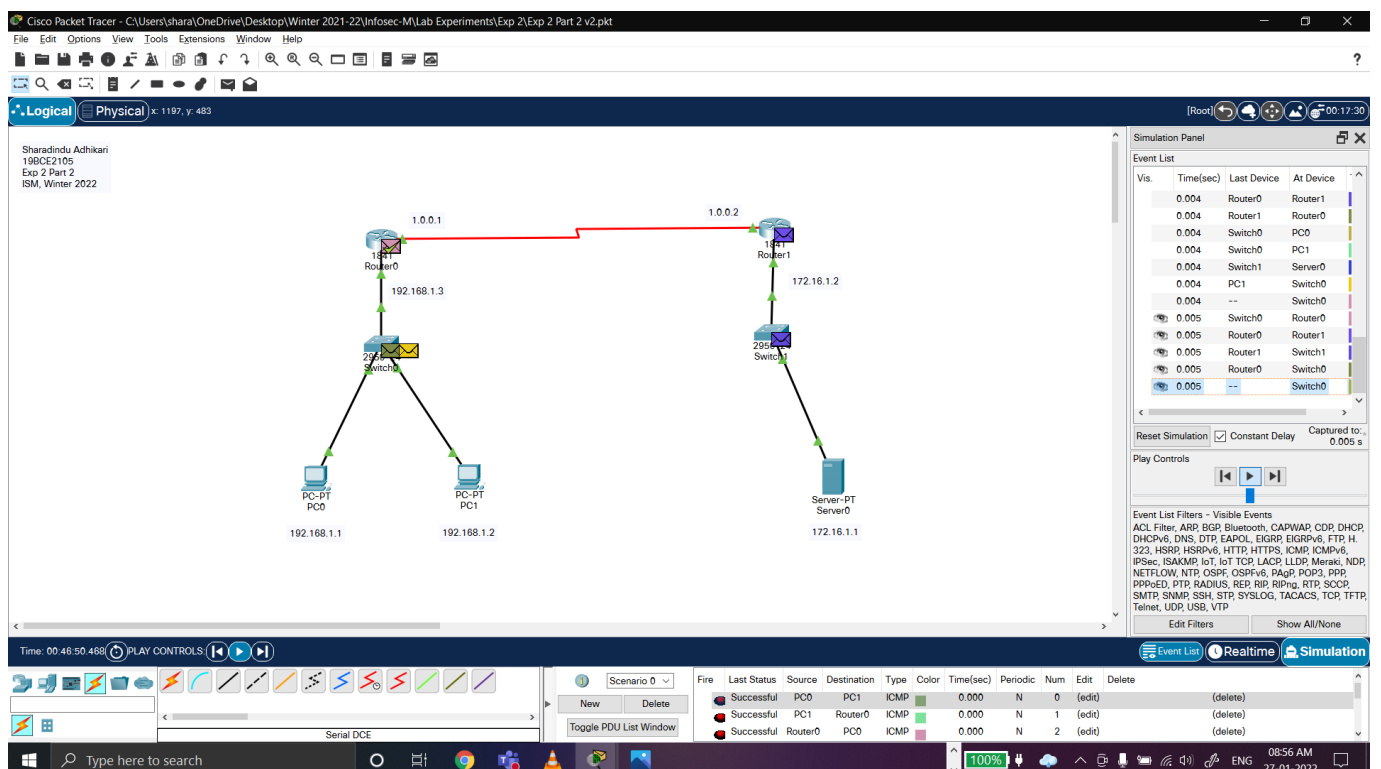
2.2. COMPONENTS

Component / Device / Interface	IP Address	Connected with
PCs		
PC0 (Fa0)	192.168.1.1	Fa0/0 of Router0
PC1 (Fa0)	192.168.1.2	Fa0/0 of Router0
Routers		
Router0 (Se0/0/0)	1.0.0.1	Se0/0/0 of Router1
Router1 (Se0/0/0)	1.0.0.2	Se0/0/0 of Router0
Server		
Server0 (Fa0)	172.16.1.1	Fa0/0 of Router1

- The Components in this Part are the regular PC-PTs, 1841 Routers, 2950-24 Switches, and a Server.
- After assigning IPs to all the components (switches being the obvious exception), and configuring the Routers, Static NAT has been configured.
- All the commands are added separately (from the snapshots) as well, along with their descriptions where necessary.

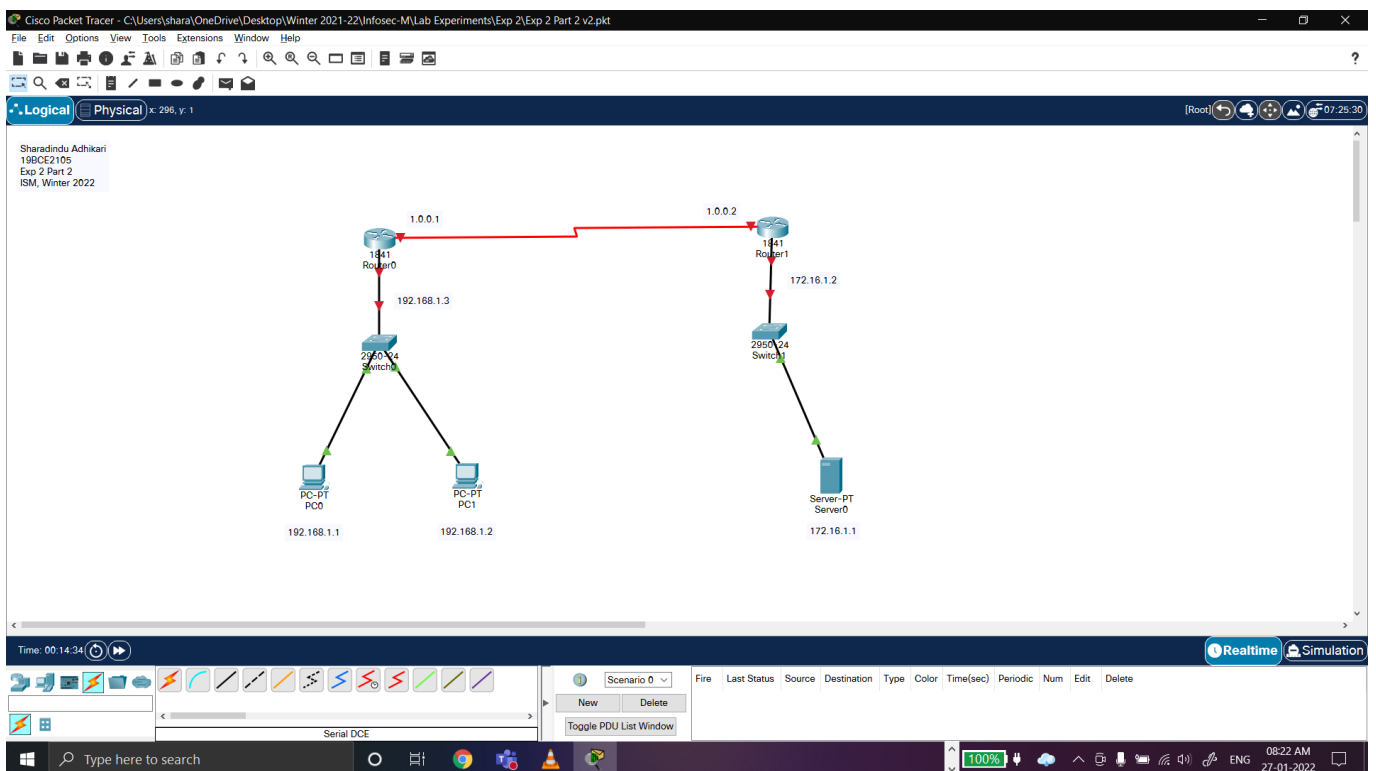
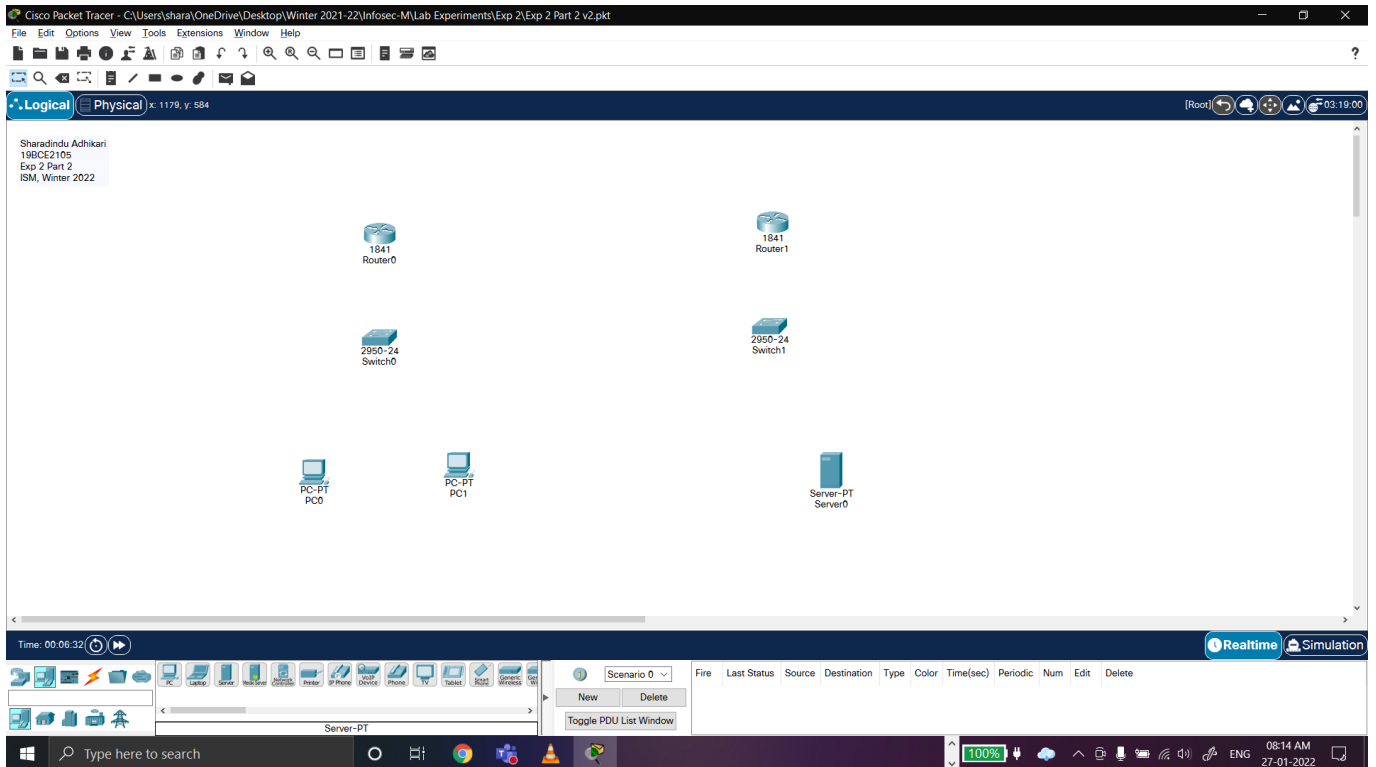
2.3. DIAGRAM

Final Simulation of the entire static NAT setup:

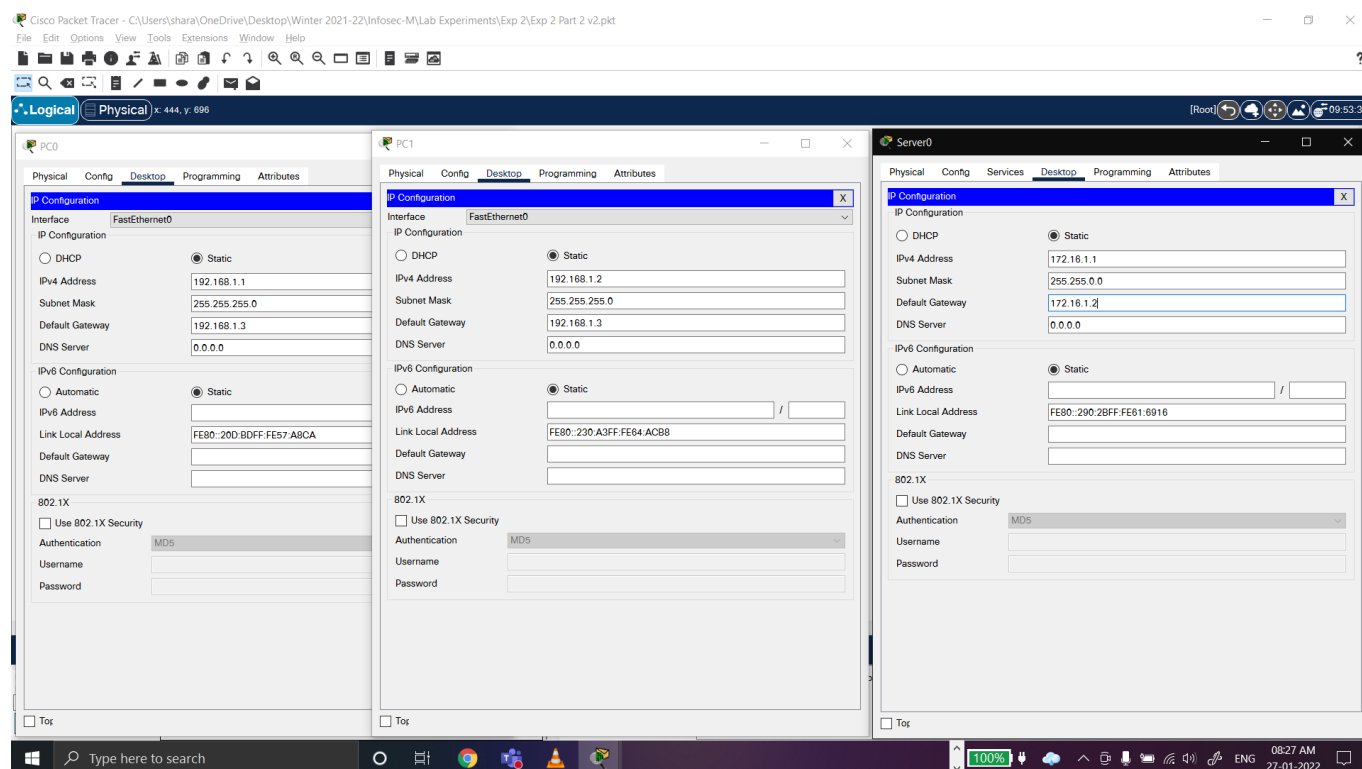


2.4. COMMANDS AND SCREENSHOTS

Step 1: Making the Topology



Step 2: Assigning IP Addresses to the PCs and the Server



Step 3: Configuring IP Addresses in the Routers (using CLI)

Router0

```
Router>en
Router#conf t
Router (config)#int fa0/0
Router (config-if)#ip add 192.168.1.3 255.255.255.0
Router (config-if)#no shut
Router (config-if)#exit

Router (config)#int s0/0/0
Router (config-if)#ip add 1.0.0.1 255.0.0.0
Router (config-if)#clock rate 64000
Router (config-if)#no shut
Router (config-if)#exit
```

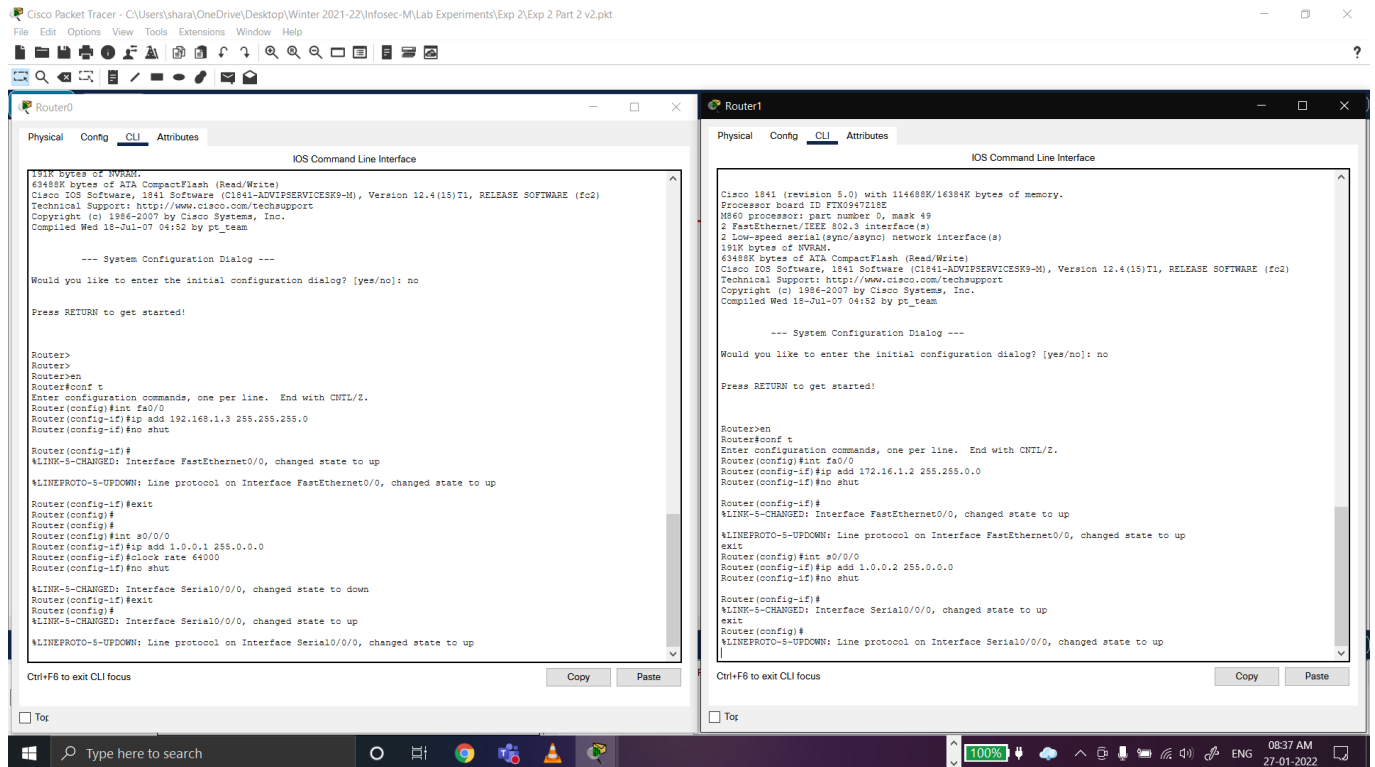
Router1

```
Router>en
Router#conf t
Router (config)#int fa0/0
Router (config-if)#ip add 172.16.1.2 255.255.0.0
Router (config-if)#no shut
Router (config-if)#exit
```

```

Router (config)#int s0/0/0
Router (config-if)#ip add 1.0.0.2 255.0.0.0
Router (config-if)#no shut
Router (config-if)#exit

```



Descriptions with example IP addresses:

- `interface FastEthernet 0/0` command is used to enter in interface mode.
`ip address 10.0.0.1 255.0.0.0` command assigns IP address to interface.
`no shutdown` command is used to bring the interface up.
`exit` command is used to return in global configuration mode.
- `Router(config)#interface serial 0/0/0` command is used to enter in interface mode.
`Router(config-if)#ip address 100.0.0.1 255.0.0.0` command assigns IP to interface.
`Router(config-if)#no shutdown` command brings interface up.
`Router(config-if)#exit` command is used to return in global configuration mode.

Step 4: Configuring Static NAT

```

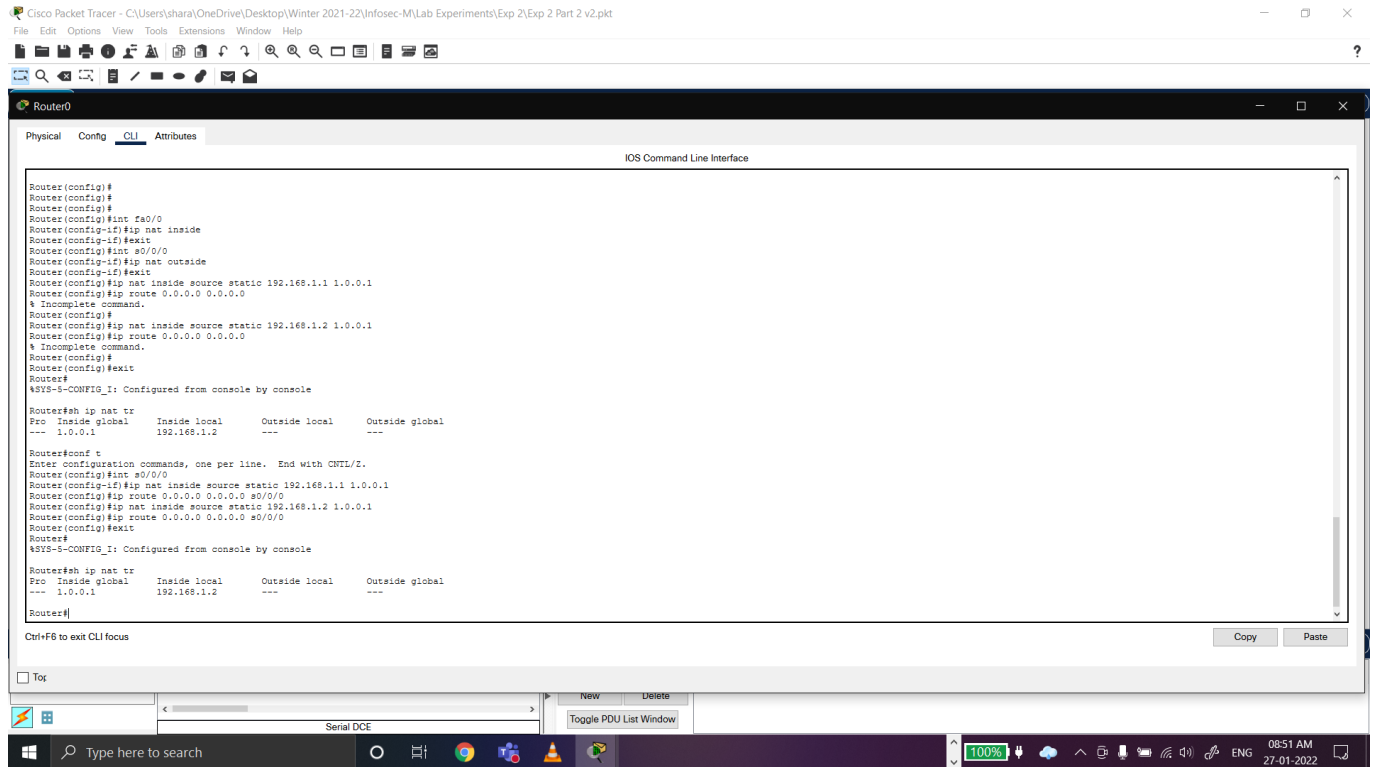
Router (config)#int fa0/0
Router (config-if)#ip nat inside
Router (config-if)#exit
Router (config)#int s0/0/0
Router (config-if)#ip nat outside
Router (config-if)#exit
Router (config)#ip nat inside source static 192.168.1.1 1.0.0.1
Router (config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
Router (config)#ip nat inside source static 192.168.1.2 1.0.0.1
Router (config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
Router (config)#exit

```

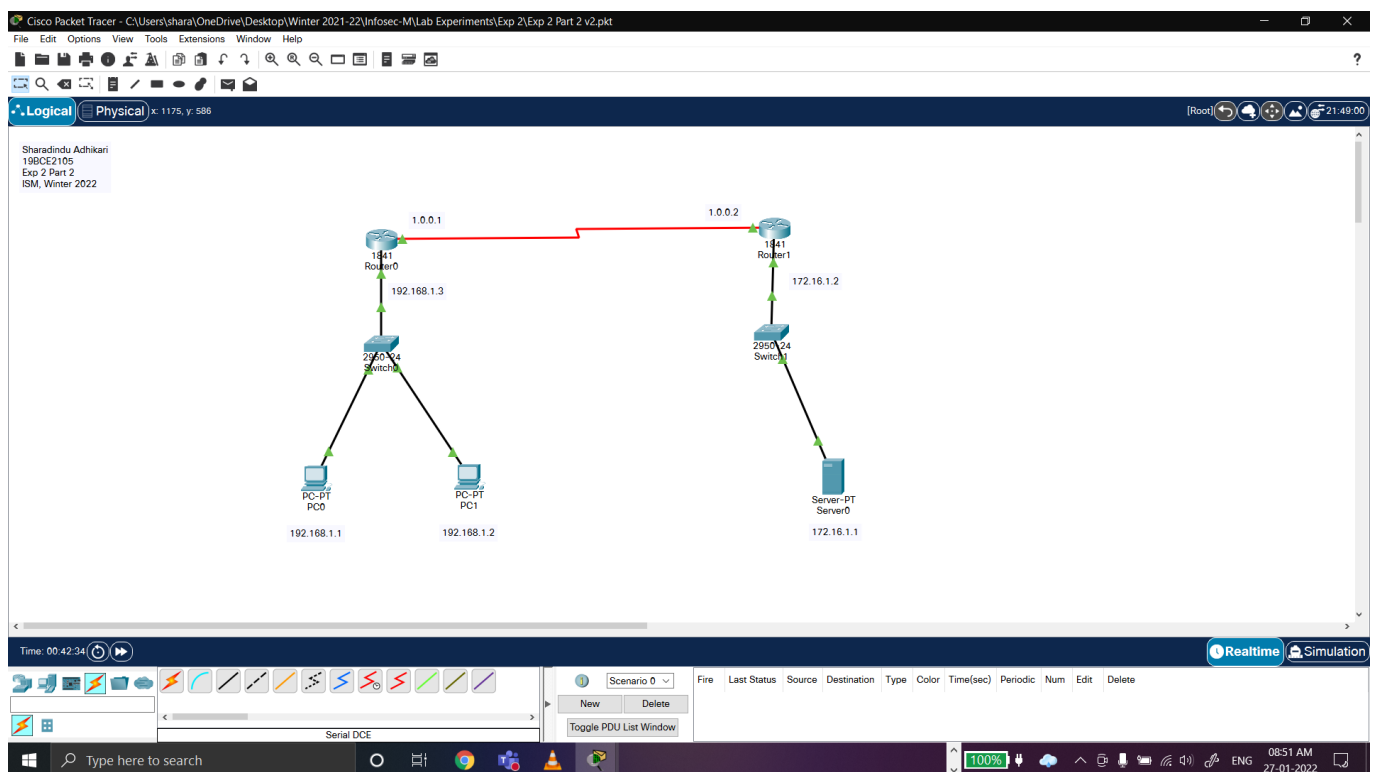
```

Router#
Router#sh ip nat tr
Pro   Inside global   Inside local   Outside local   Outside global
---   1.0.0.1         192.168.1.2   ---           ---
Router#

```



Step 5: Sending PDUs, Simulating the route, etc.



Cisco Packet Tracer - C:\Users\shara\OneDrive\Desktop\Winter 2021-22\Infosec-M\Lab Experiments\Exp 2\Exp 2 Part 2 v2.pkt

File Edit Options View Tools Extensions Window Help

Logical Physical x: 941, y: 671

Sharadindu Adhikari
19BCE2105
Exp 2 Part 2
ISM, Winter 2022

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device
	0.001	Router0	Switch0
	0.001	Server0	Switch1
	0.001	Router1	Router0
	0.001	--	Server0
	0.002	PC0	Switch0
	0.002	PC1	Switch0
	0.002	Server0	Switch1
	0.002	Switch0	PC1
	0.002	Switch0	Router0
	0.002	Switch0	PC0
	0.002	Switch1	Router1
	0.002	Router0	Switch0

Reset Simulation ☒ Constant Delay Captured to: 0.002 s

Play Controls

Event List Filters - Visible Events

ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPsec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PaGP, POP3, PPP, PPPoE, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters Show All/None

Time: 00:48:50.485 PLAY CONTROLS

Scenario 0

New Delete

Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	In Progress	PC0	PC1	ICMP		0.000	N	0	(edit)	(delete)
	In Progress	PC1	Router0	ICMP		0.000	N	1	(edit)	(delete)
	In Progress	Router0	PC0	ICMP		0.000	N	2	(edit)	(delete)

100%

08:56 AM
27-01-2022

PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC1	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC1	Router0	ICMP		0.000	N	1	(edit)	(delete)
	Successful	Router0	PC0	ICMP		0.000	N	2	(edit)	(delete)
	Successful	Server0	Router1	ICMP		0.000	N	3	(edit)	(delete)
	Successful	Router1	Router0	ICMP		0.000	N	4	(edit)	(delete)
	Successful	PC1	Router1	ICMP		0.000	N	5	(edit)	(delete)
	Successful	Server0	Router0	ICMP		0.000	N	6	(edit)	(delete)
	Successful	PC0	Server0	ICMP		0.000	N	7	(edit)	(delete)

Reset Simulation ☒ Constant Delay Captured to: 14.561 s

Play Controls

Event List Filters - Visible Events

ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPsec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PaGP, POP3, PPP, PPPoE, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters Show All/None

Time: 00:47:05.024 PLAY CONTROLS

Scenario 0

New Delete

Toggle PDU List Window

100%

09:01 AM
27-01-2022