DYNAMIC NAT CONFIGURATION, SWITCH AND ROUTER SECURITY CONFIGURATION

Submitted by

FRANCIS ALEX	*18BCE2325*
BAWATHARANY MURALIDHARAN	*18BCE2367*
RAKESH B KRISHNAN	*18BCE2351*
ASTHA CHAUDHARY	*18BCE2145*

Prepared For

ISM – J COMPONENT

Submitted To

MRS LAVANYA K

Senior Professor

VIT®
UNIVERSITY
(Estd. u/s 3 of UGC Act 1956)
VELLORE ■ CHENNAI
www.vit.ac.in

SCOPE

TABLE OF CONTENTS

DYNAMIC NAT CONFIGURATION USING CISCO PACKET TRACER

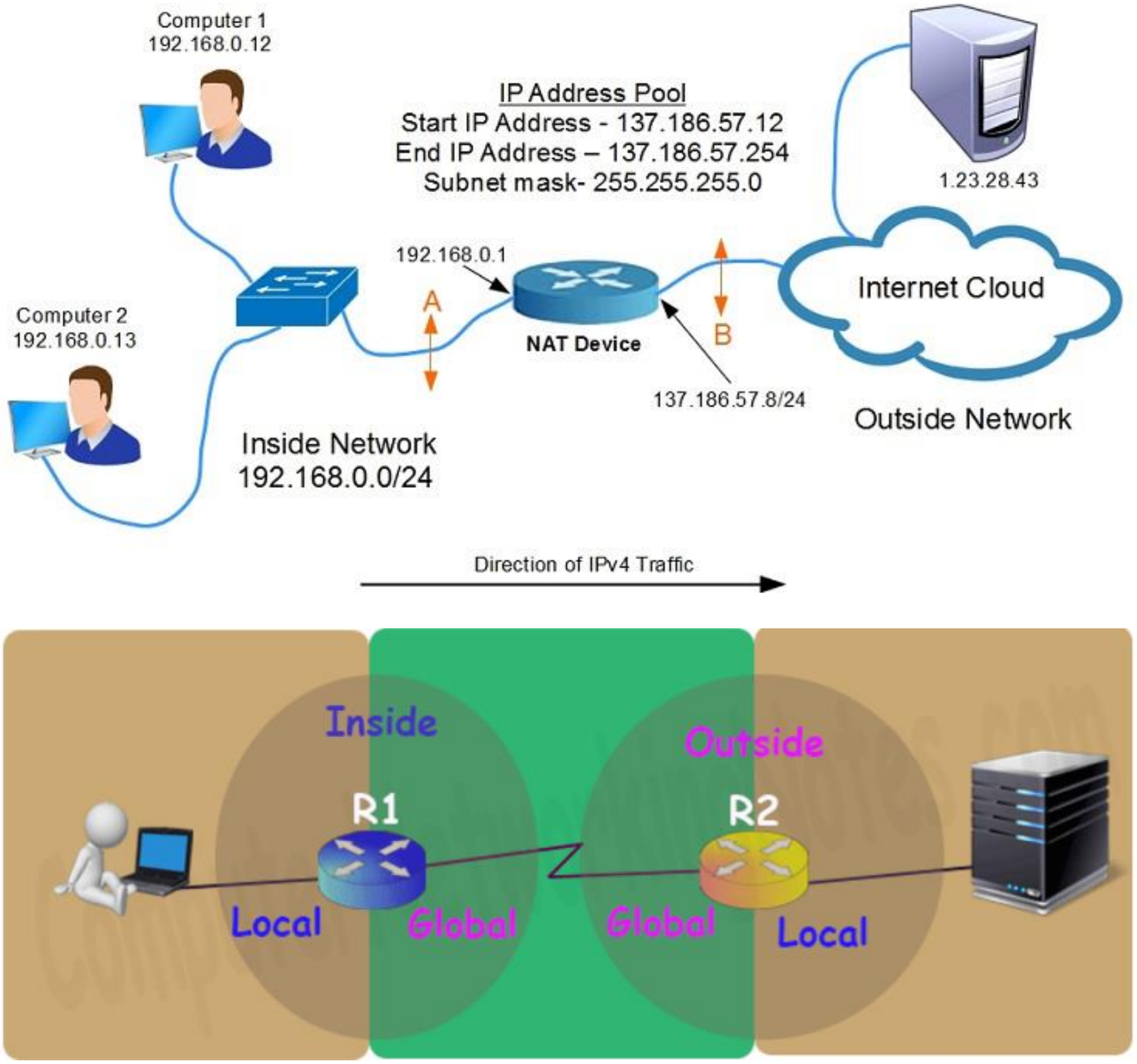
WHAT IS DYNAMIC NAT

Dynamic NAT (Network Address Translation) - Dynamic NAT can be defined as mapping of a private IP address to a public IP address from a group of public IP addresses called as NAT pool. Dynamic NAT establishes a one-to-one mapping between a private IP address to a public IP address. Here the public IP address is taken from the pool of IP addresses configured on the end NAT router. The public to private mapping may vary based on the available public IP address in NAT pool.

BENEFIT OF DYNAMIC NAT

a. The main advantage of NAT (Network Address Translation) is that it can prevent the depletion of IPv4 addresses.
b. NAT (Network Address Translation) can provide an additional layer of security by making the original source and destination addresses hidden.
c. NAT (Network Address Translation) provides increased flexibility when connecting to the public Internet.

FRAMEWORK DESIGN



Framework Diagram

STEP BY STEP EXPLANATION & SCREENSHOTS

1. Creating the basic network topology by connecting the Laptop's, switch, routers and server with connecting wires. The following wires need to be used for connecting devices.

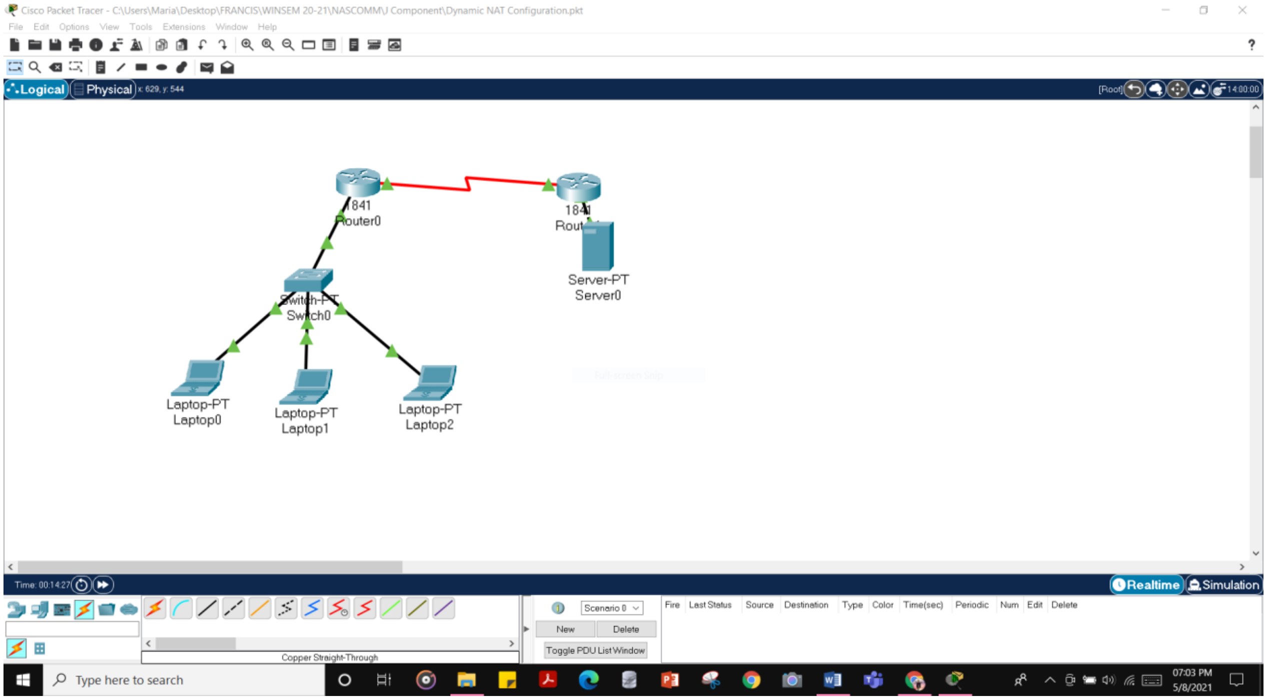
    a. Router-----Router (Serial DCE)

b. Router -------Switch (copper straight through wire)

c. Laptop-------Switch (copper straight through wire)

d. Router -------Server (copper straight through wire)

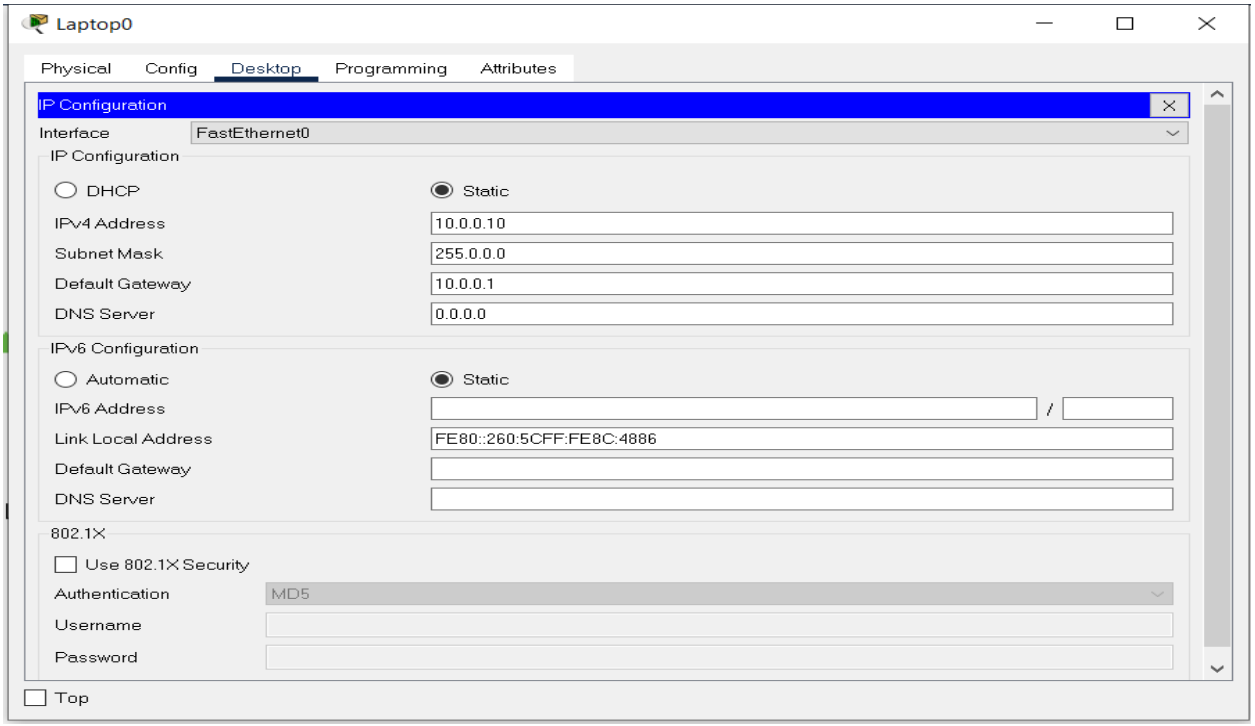
Connection is established and shown below:



Network Topology

2. Next step is to assign IP address to the Laptop, in order to do that we have to click on Laptop and then in top click on desktop followed by IP address and then enter the desired IP address. Here is screenshot of what we have added.

We have added the default IP address of Laptop0 to be 10.0.0.10 with default gateway being 10.0.0.1.



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address	10.0.0.10
Subnet Mask	255.0.0.0
Default Gateway	10.0.0.1
DNS Server	0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address	/
Link Local Address	FE80::260:5CFF:FE8C:4886
Default Gateway	
DNS Server	

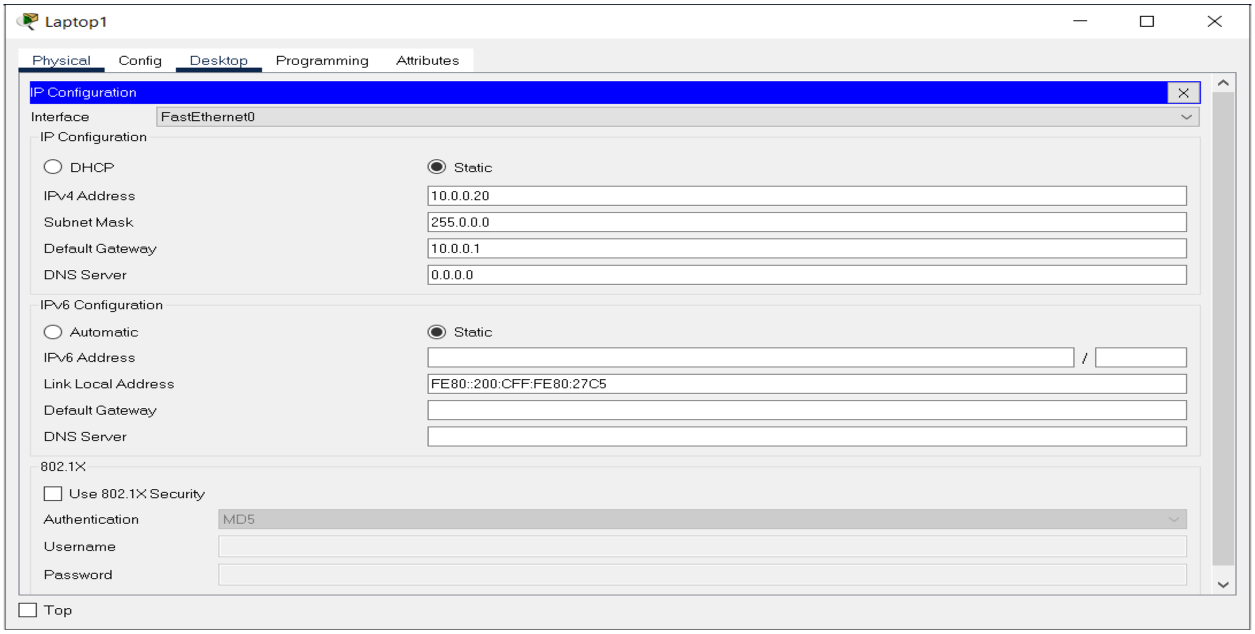
802.1X

□ Use 802.1X Security

Authentication	MD5
Username	
Password	

□ Top

Laptop0 IP address configuration



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address	10.0.0.20
Subnet Mask	255.0.0.0
Default Gateway	10.0.0.1
DNS Server	0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address	/
Link Local Address	FE80::200:CFF:FE80:27C5
Default Gateway	
DNS Server	

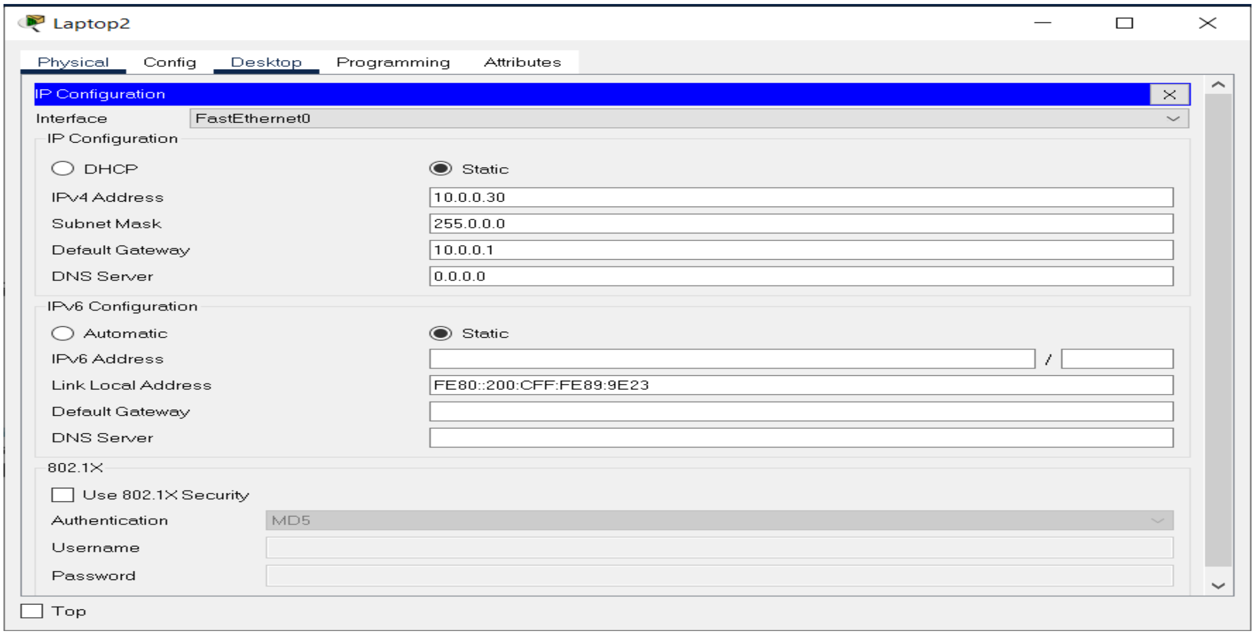
802.1X

□ Use 802.1X Security

Authentication	MD5
Username	
Password	

□ Top

Laptop1 IP address configuration



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 10.0.0.30

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::200:CFF:FE89:9E23

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

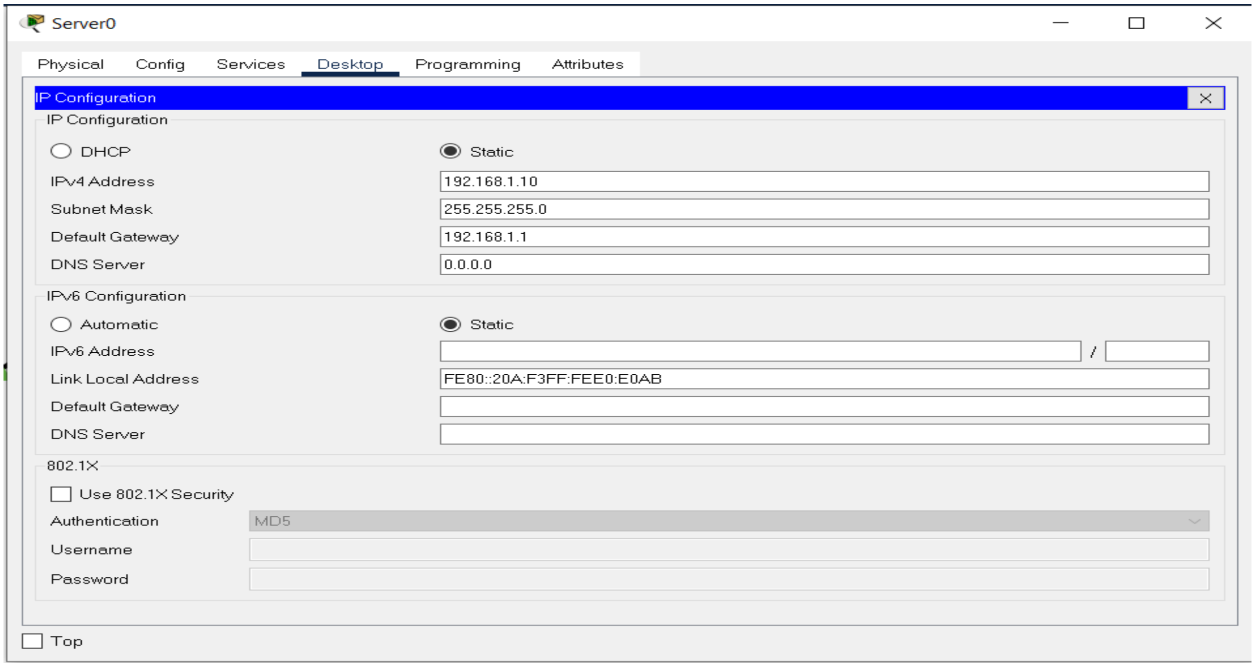
Username:

Password:

Laptop2 IP address configuration

3. Next step is to assign IP address to the Server, in order to do that we have to click on Laptop and then in top click on desktop followed by IP address and then enter the desired IP address. Here is screenshot of what we have added.

   We have added the default IP address of Server to be 192.168.1.10/24 with default gateway being 192.168.1.1



IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.1.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::20A:F3FF:FEE0:E0AB

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

Username:

Password:

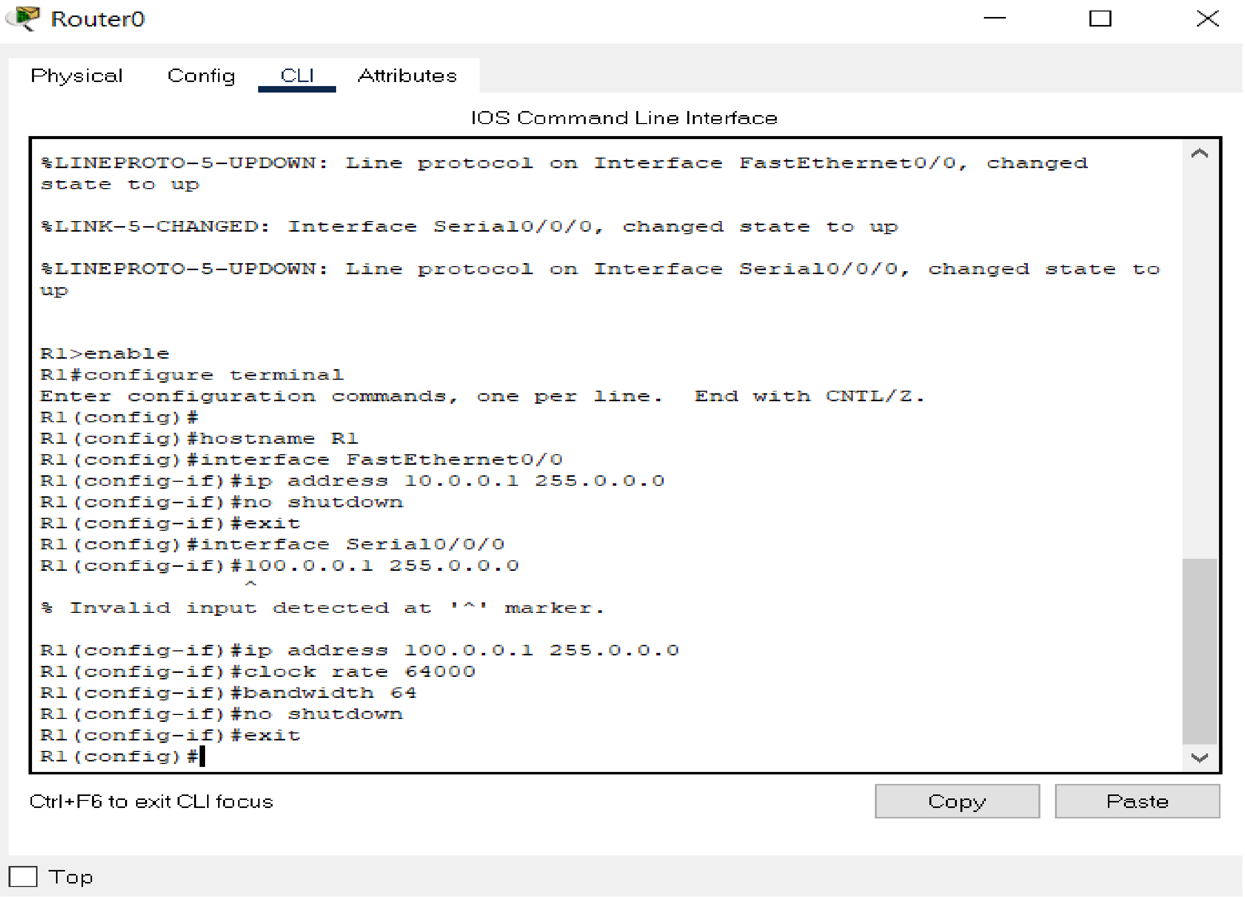
□ Top

Server0 IP address configuration

4. In order to configure the router, we have to click on router followed by clicking on CLI in top right. Then following commands must be entered in order to set up the IP address and host name.

- Router>enable
- Router# configure terminal
- Router(config)#
- Router(config)#hostname R1
- R1(config)#interface FastEthernet0/0
- R1(config-if)#ip address 10.0.0.1 255.0.0.0
- R1(config-if)#no shutdown
- R1(config-if)#exit
- R1(config)#interface Serial0/0/0
- R1(config-if)#ip address 100.0.0.1 255.0.0.0
- R1(config-if)#clock rate 64000
- R1(config-if)#bandwidth 64
- R1(config-if)#no shutdown

- R1(config-if)#exit
- R1(config)#

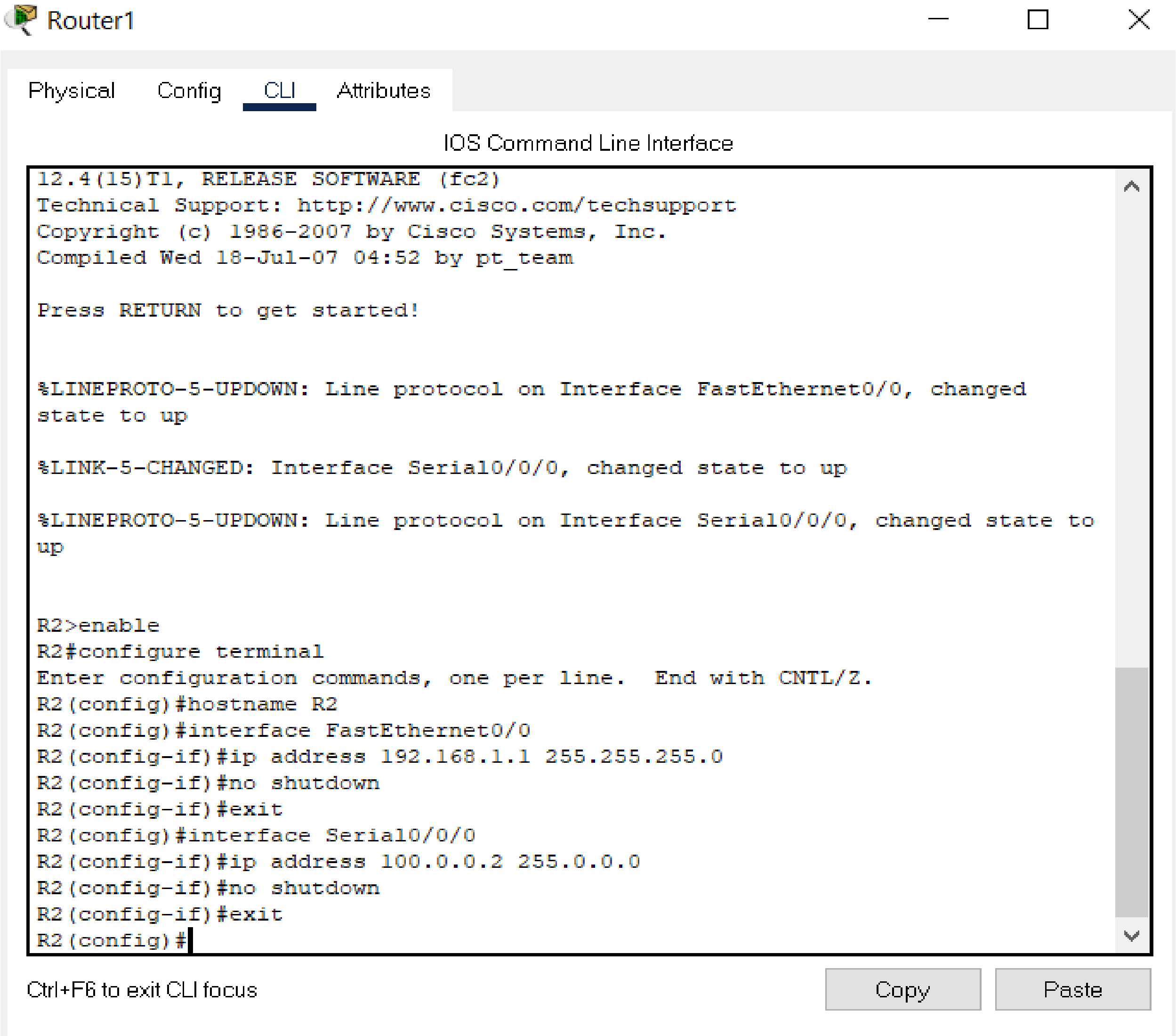


```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to
up


R1>enable
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#
R1(config)#hostname R1
R1(config)#interface FastEthernet0/0
R1(config-if)#ip address 10.0.0.1 255.0.0.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface Serial0/0/0
R1(config-if)#100.0.0.1 255.0.0.0
              ^
% Invalid input detected at '^' marker.

R1(config-if)#ip address 100.0.0.1 255.0.0.0
R1(config-if)#clock rate 64000
R1(config-if)#bandwidth 64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
```

Router 0 setting IP address and hostname

- Router>enable
- Router#configure terminal
- Router(config)#hostname R2
- R2(config)#interface FastEthernet0/0
- R2(config-if)#ip address 192.168.1.1 255.255.255.0
- R2(config-if)#no shutdown
- R2(config-if)#exit
- R2(config)#interface Serial0/0/0
- R2(config-if)#ip address 100.0.0.2 255.0.0.0
- R2(config-if)#no shutdown

- R2(config-if)#exit
- R2(config)#



```
12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

Press RETURN to get started!


%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to
up


R2>enable
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#hostname R2
R2(config)#interface FastEthernet0/0
R2(config-if)#ip address 192.168.1.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface Serial0/0/0
R2(config-if)#ip address 100.0.0.2 255.0.0.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
```

Router 1 setting IP address and hostname

5. Now we are entering dynamic NAT configuration. To do so we have to click on Router and then click on CLI. Then following commands need to be entered.

a. First we have to mention the IP address and then permit and deny the required IP address.

- R1#configure terminal
- Enter configuration commands, one per line. End with CNTL/Z.
- R1(config)#access-list 1 permit 10.0.0.10 0.0.0.0
- R1(config)#access-list 1 permit 10.0.0.20 0.0.0.0
- R1(config)#access-list 1 deny any

b. In next step we define a pool of inside global addresses which are available for translation. Following command is used to define the NAT pool.

```
Router(config)#ip nat pool [Pool Name] [Start IP address] [End IP address] netmask [Subnet mask]
```

c. Now we type the following commands in router for defining the NAT pool.

- R1(config)#ip nat pool ccna 50.0.0.1 50.0.0.2 netmask 255.0.0.0
- R1(config)#ip nat inside source list 1 pool ccna

d. Finally we have to define which interface is connected with local network and which interface is connected with global network.

To define an inside local we use following command.

```
Router(config-if)#ip nat inside
```

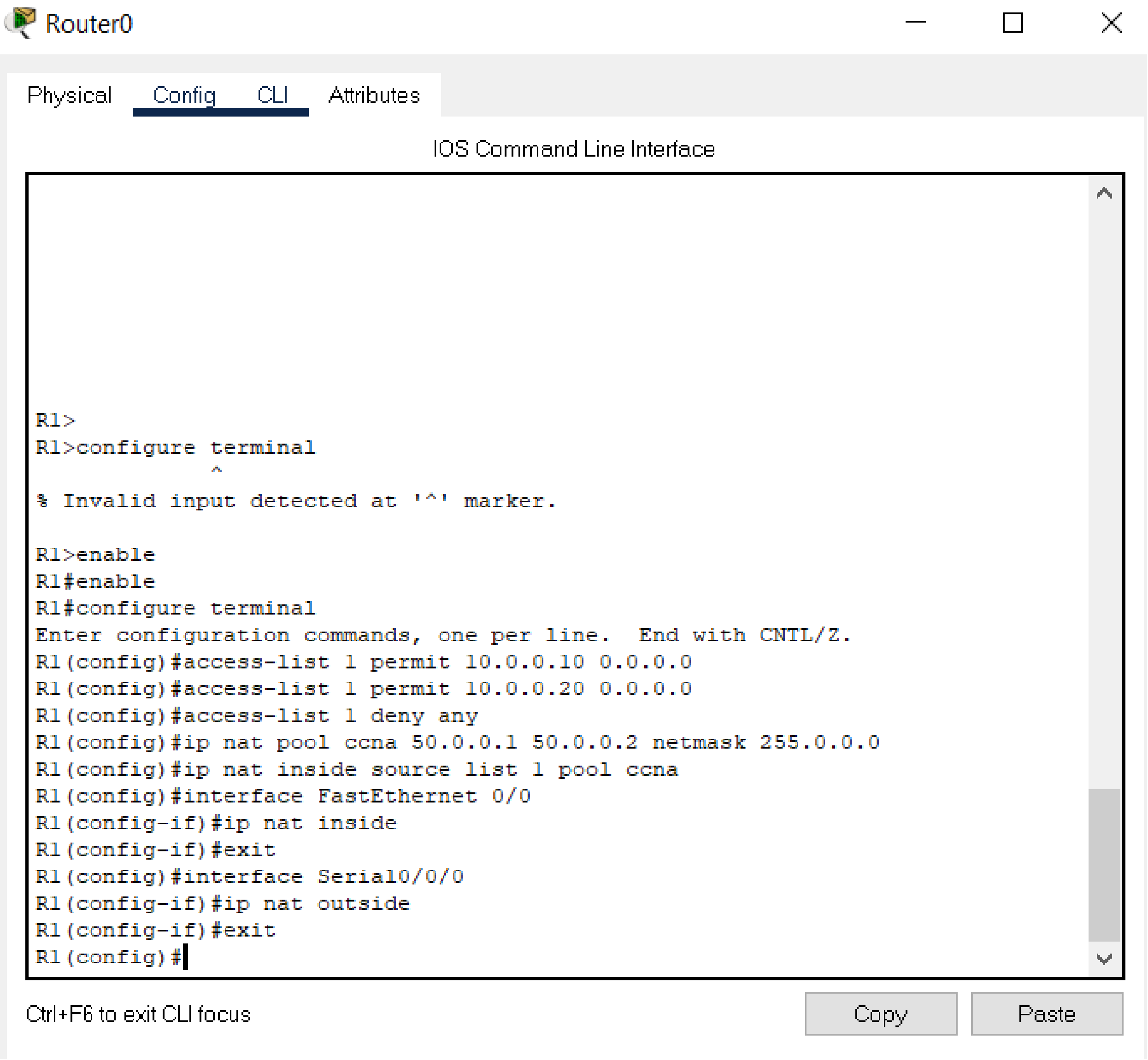
Following command defines inside global

```
Router(config-if)#ip nat outside
```

e. Now we enter the following commands in router.

- R1(config)#interface FastEthernet 0/0
- R1(config-if)#ip nat inside
- R1(config-if)#exit
- R1(config)#interface Serial0/0/0
- R1(config-if)#ip nat outside
- R1(config-if)#exit
- R1(config)#

Overall the screenshots of the dynamic configuration of router0 is shown.

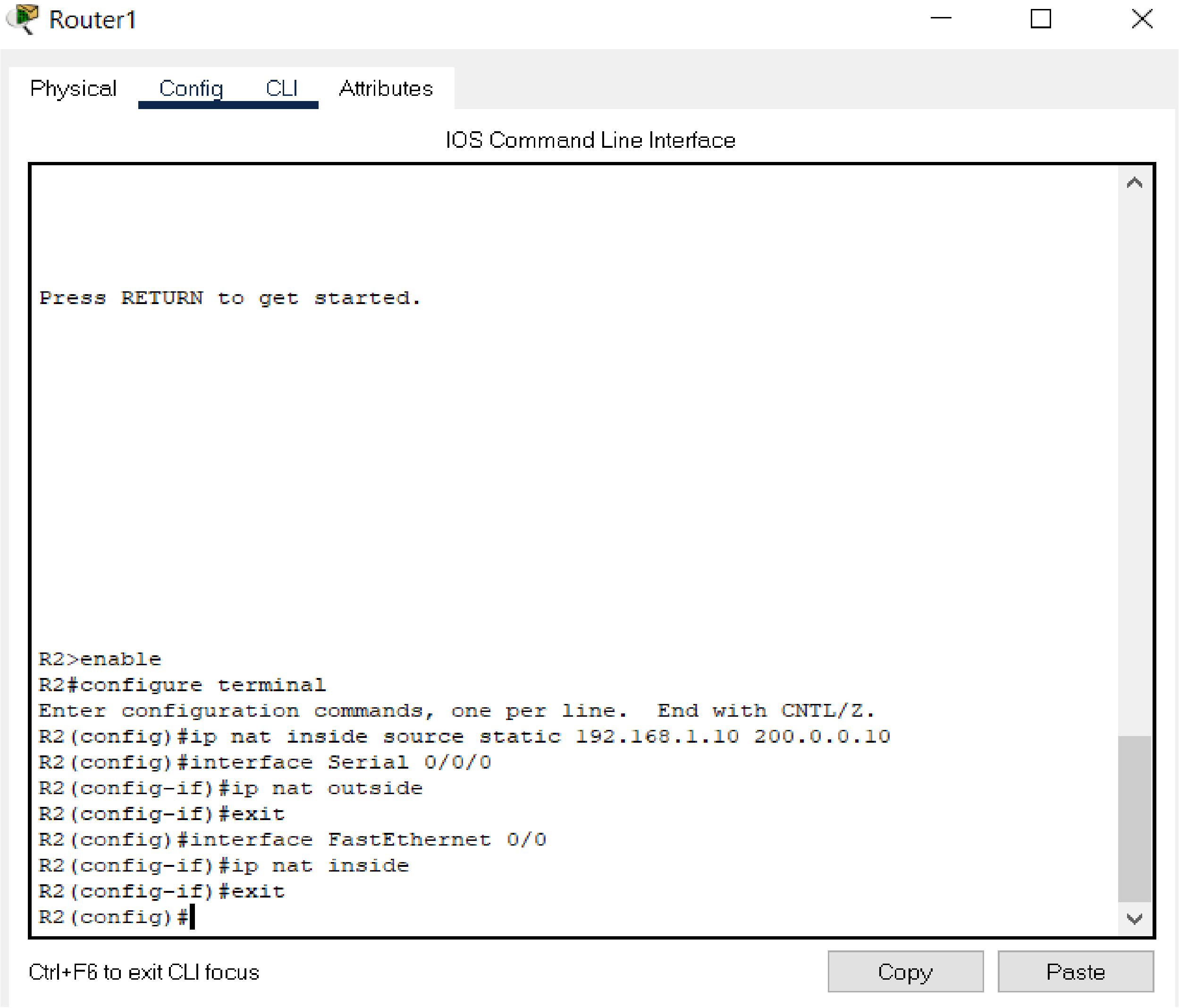


```
R1>
R1>configure terminal
             ^
% Invalid input detected at '^' marker.

R1>enable
R1#enable
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 1 permit 10.0.0.10 0.0.0.0
R1(config)#access-list 1 permit 10.0.0.20 0.0.0.0
R1(config)#access-list 1 deny any
R1(config)#ip nat pool ccna 50.0.0.1 50.0.0.2 netmask 255.0.0.0
R1(config)#ip nat inside source list 1 pool ccna
R1(config)#interface FastEthernet 0/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interface Serial0/0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#
```

Router 0 Dynamic NAT configuration

Similarly we do the configuration with Router1 as well.

```
•   R2>enable
•   R2#configure terminal
•   Enter configuration commands, one per line. End with CNTL/Z.
•   R2(config)#ip nat inside source static 192.168.1.10 200.0.0.10
•   R2(config)#interface Serial 0/0/0
•   R2(config-if)#ip nat outside
•   R2(config-if)#exit
•   R2(config)#interface FastEthernet 0/0
•   R2(config-if)#ip nat inside
•   R2(config-if)#exit
•   R2(config)#
```



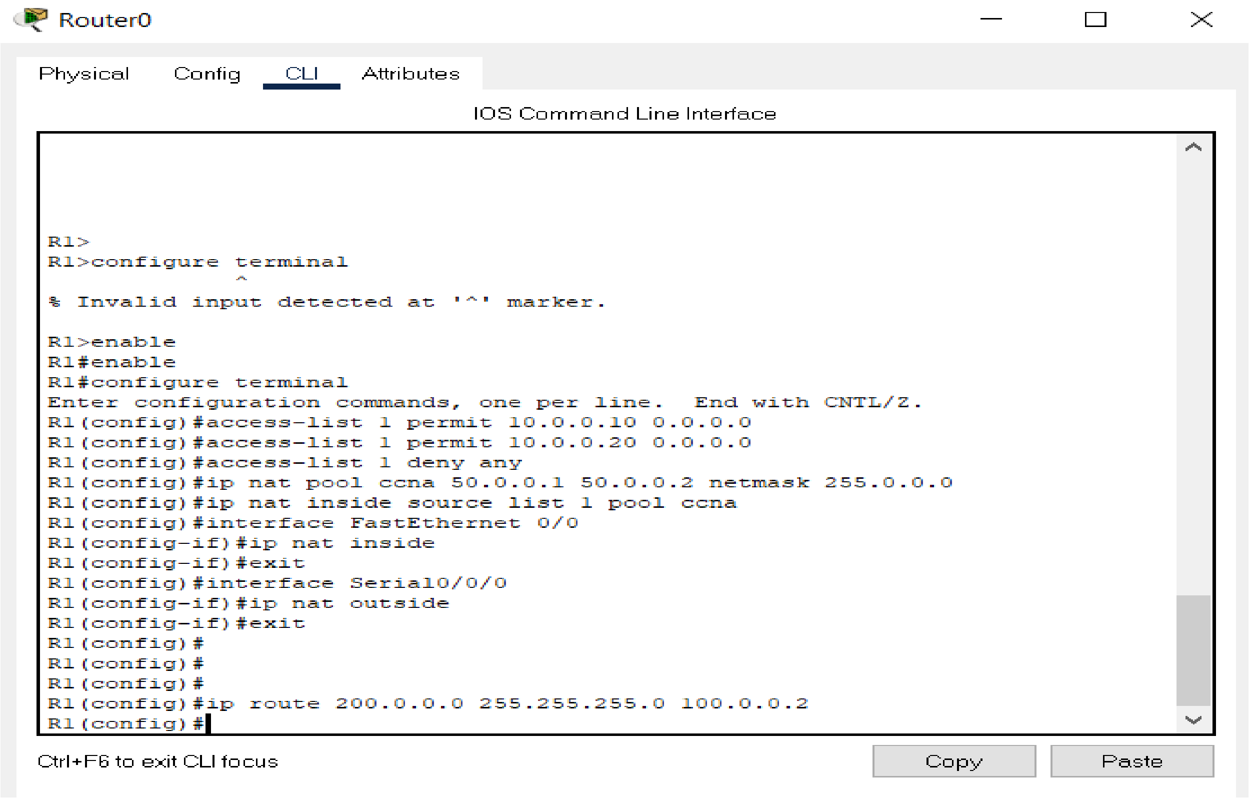
```
Press RETURN to get started.




R2>enable
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip nat inside source static 192.168.1.10 200.0.0.10
R2(config)#interface Serial 0/0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#interface FastEthernet 0/0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#
```

Router 1 Dynamic NAT configuration

In order to configure static routing in Router R0

R1(config)#ip route 200.0.0.0 255.255.255.0 100.0.0.2

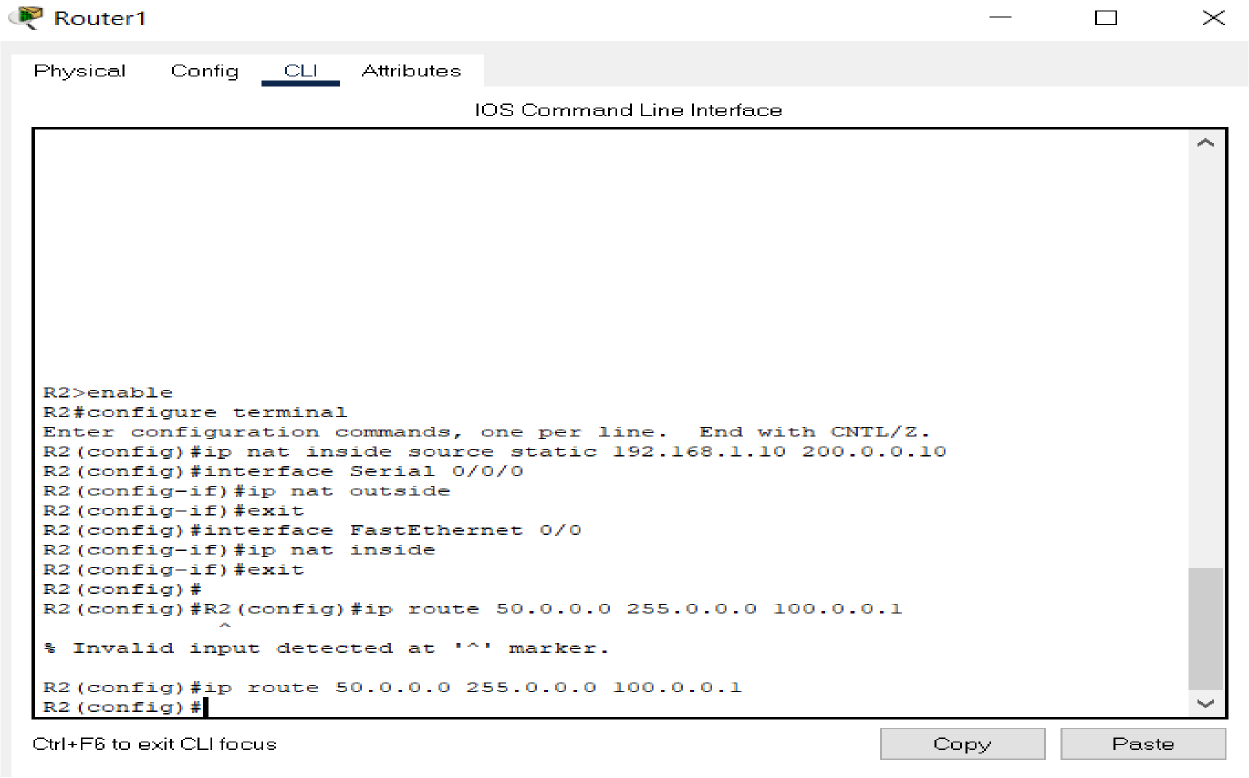
R2(config)#ip route 50.0.0.0 255.0.0.0 100.0.0.1



```
R1>
R1>configure terminal
             ^
% Invalid input detected at '^' marker.

R1>enable
R1#enable
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 1 permit 10.0.0.10 0.0.0.0
R1(config)#access-list 1 permit 10.0.0.20 0.0.0.0
R1(config)#access-list 1 deny any
R1(config)#ip nat pool ccna 50.0.0.1 50.0.0.2 netmask 255.0.0.0
R1(config)#ip nat inside source list 1 pool ccna
R1(config)#interface FastEthernet 0/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interface Serial0/0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#
R1(config)#
R1(config)#
R1(config)#ip route 200.0.0.0 255.255.255.0 100.0.0.2
R1(config)#
```

Ctrl+F6 to exit CLI focus

Static Routing in Router R0



```
R2>enable
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip nat inside source static 192.168.1.10 200.0.0.10
R2(config)#interface Serial 0/0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#interface FastEthernet 0/0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#
R2(config)#R2(config)#ip route 50.0.0.0 255.0.0.0 100.0.0.1
             ^
% Invalid input detected at '^' marker.

R2(config)#ip route 50.0.0.0 255.0.0.0 100.0.0.1
R2(config)#
```

Ctrl+F6 to exit CLI focus

Static Routing in Router R1

6. Now we are testing Dynamic NAT configuration , we configured dynamic NAT on R0 for 10.0.0.10 and 10.0.0.20 and static NAT on R2 for 192.168.1.10

Device	Inside Local IP Address	Inside Global IP Address
Laptop0	10.0.0.10	50.0.0.1
Laptop1	10.0.0.20	50.0.0.2
Server	192.168.1.10	200.0.0.10

To test this setup we click on laptop0 and then desktop followed by Command Prompt.

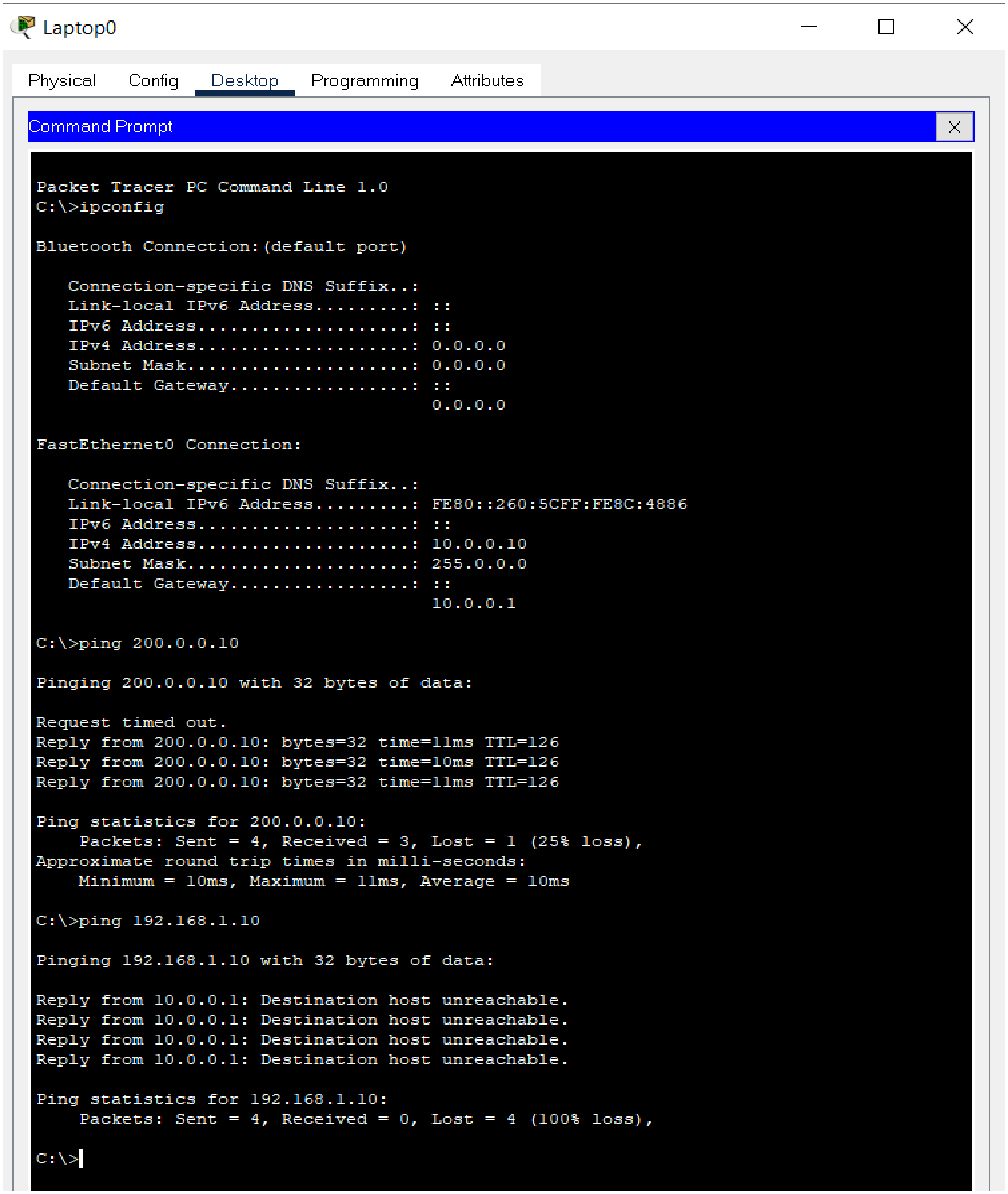
Then we run the following command.

a. Run ipconfig command -> this command is to make sure we are testing correct NAT device.

b. Run ping 200.0.0.10 -> Checks whether we are able to access the remote device or not. A ping reply confirms that we are able to connect with remote device on this IP address.

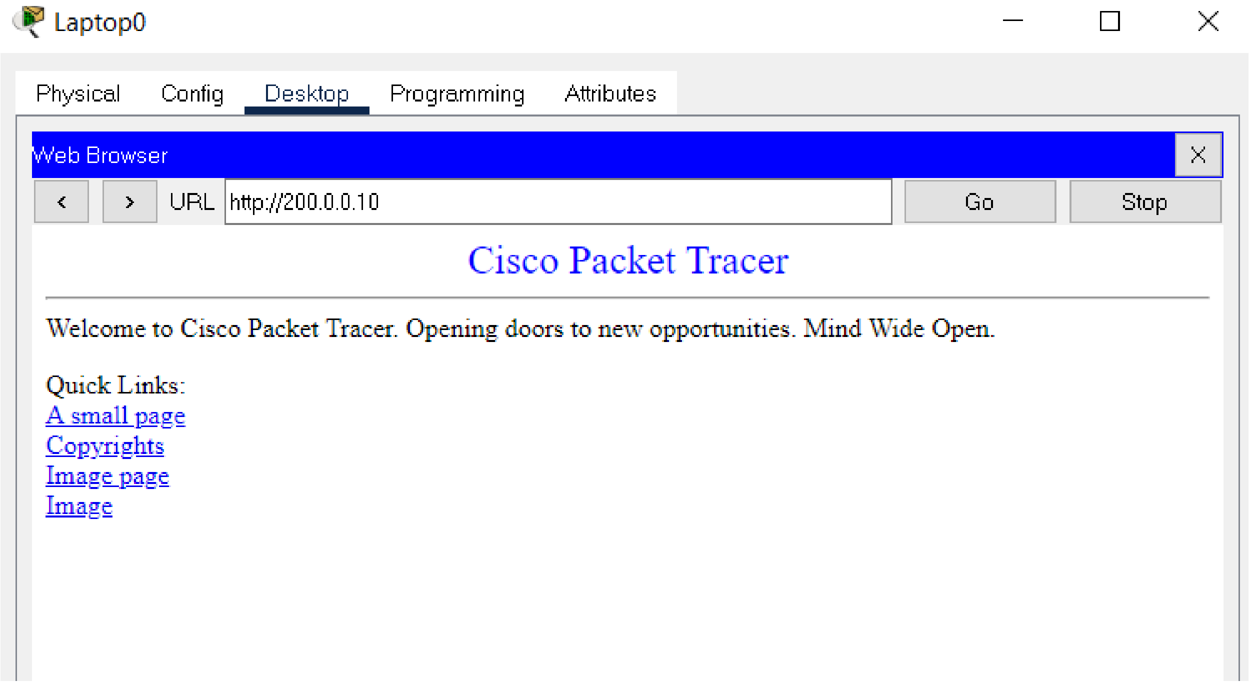
c. Run ping 192.168.1.10 -> Checks whether we are able to access the remote device on its actual IP address or not. A ping error confirms that we are not able to connect with remote device on this IP address.

d. Now we click web server and access 200.0.0.10



```
Packet Tracer PC Command Line 1.0
C:\>ipconfig

Bluetooth Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

FastEthernet0 Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::260:5CFF:FE8C:4886
   IPv6 Address....................: ::
   IPv4 Address....................: 10.0.0.10
   Subnet Mask.....................: 255.0.0.0
   Default Gateway.................: ::
                                     10.0.0.1

C:\>ping 200.0.0.10

Pinging 200.0.0.10 with 32 bytes of data:

Request timed out.
Reply from 200.0.0.10: bytes=32 time=11ms TTL=126
Reply from 200.0.0.10: bytes=32 time=10ms TTL=126
Reply from 200.0.0.10: bytes=32 time=11ms TTL=126

Ping statistics for 200.0.0.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 11ms, Average = 10ms

C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Testing Dynamic NAT configuration



http://200.0.0.10

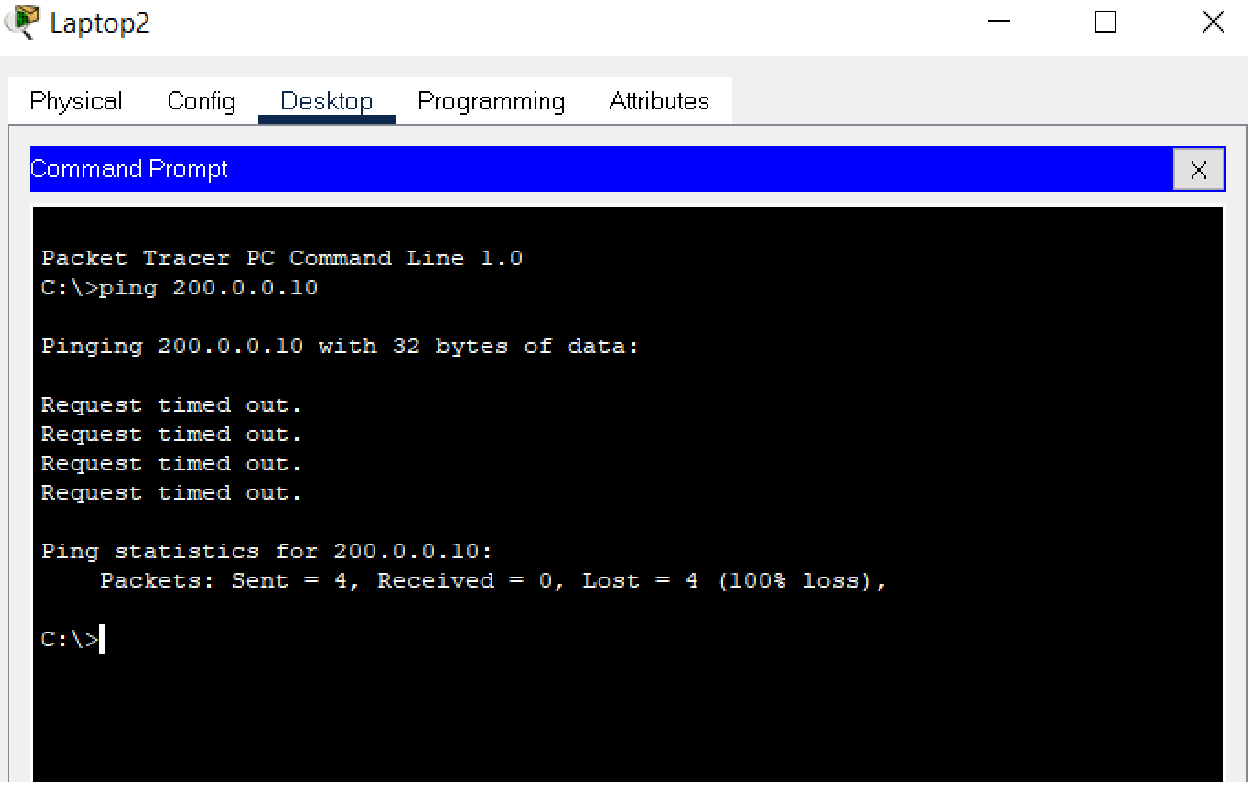
Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

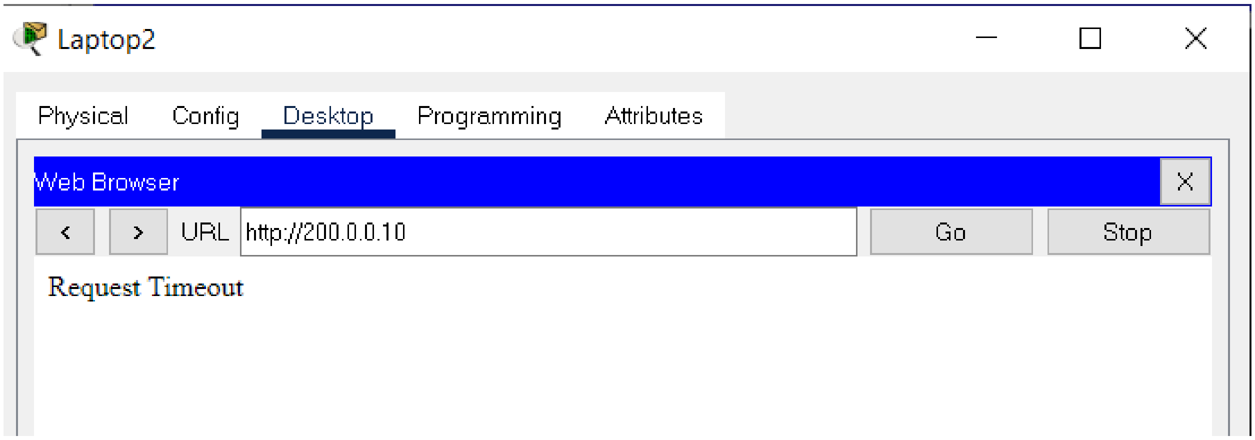
Quick Links:
A small page
Copyrights
Image page
Image

Checking if host 10.0.0.10 is able to access 200.0.0.10.

Now following the same procedure from Laptop 2 as well.



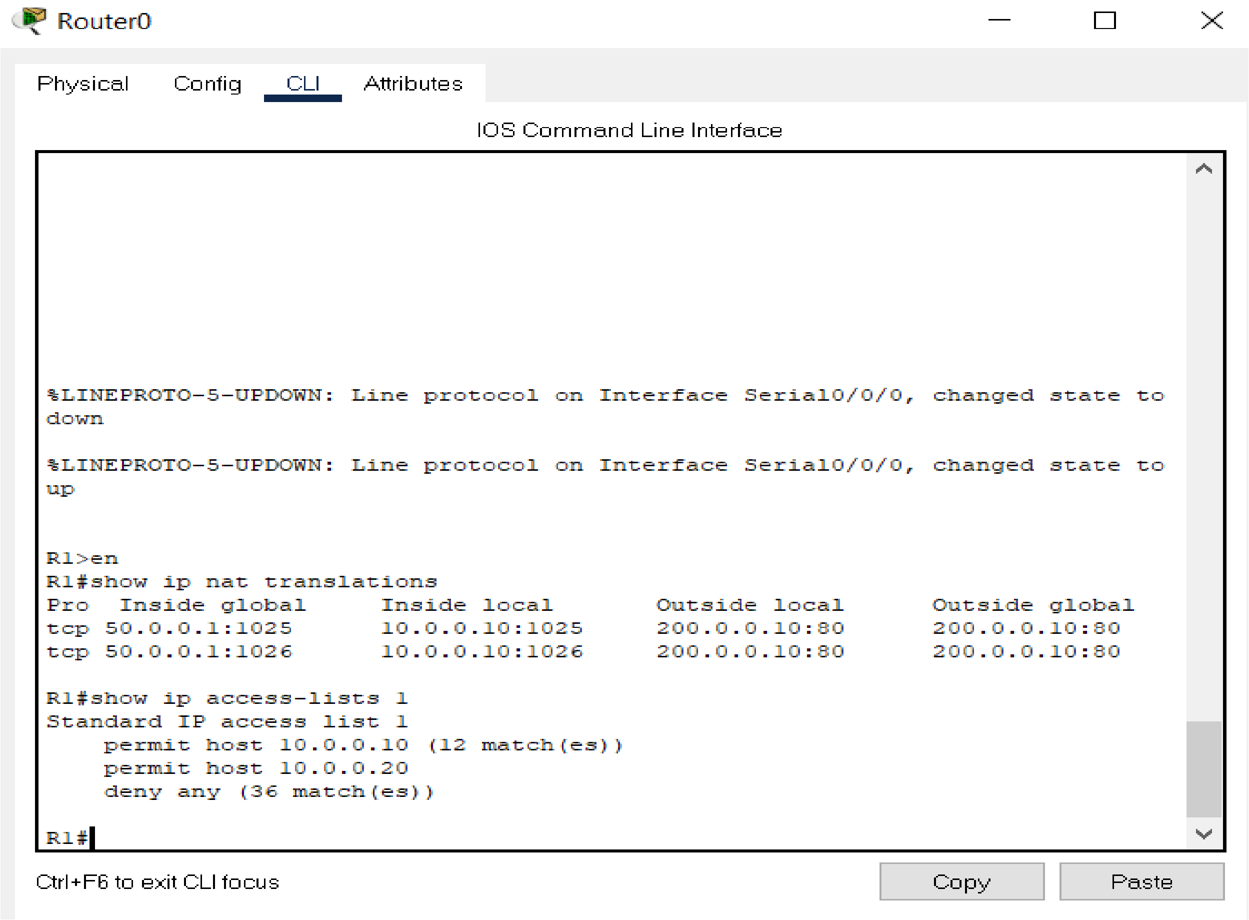
```
Packet Tracer PC Command Line 1.0
C:\>ping 200.0.0.10

Pinging 200.0.0.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 200.0.0.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```



URL http://200.0.0.10

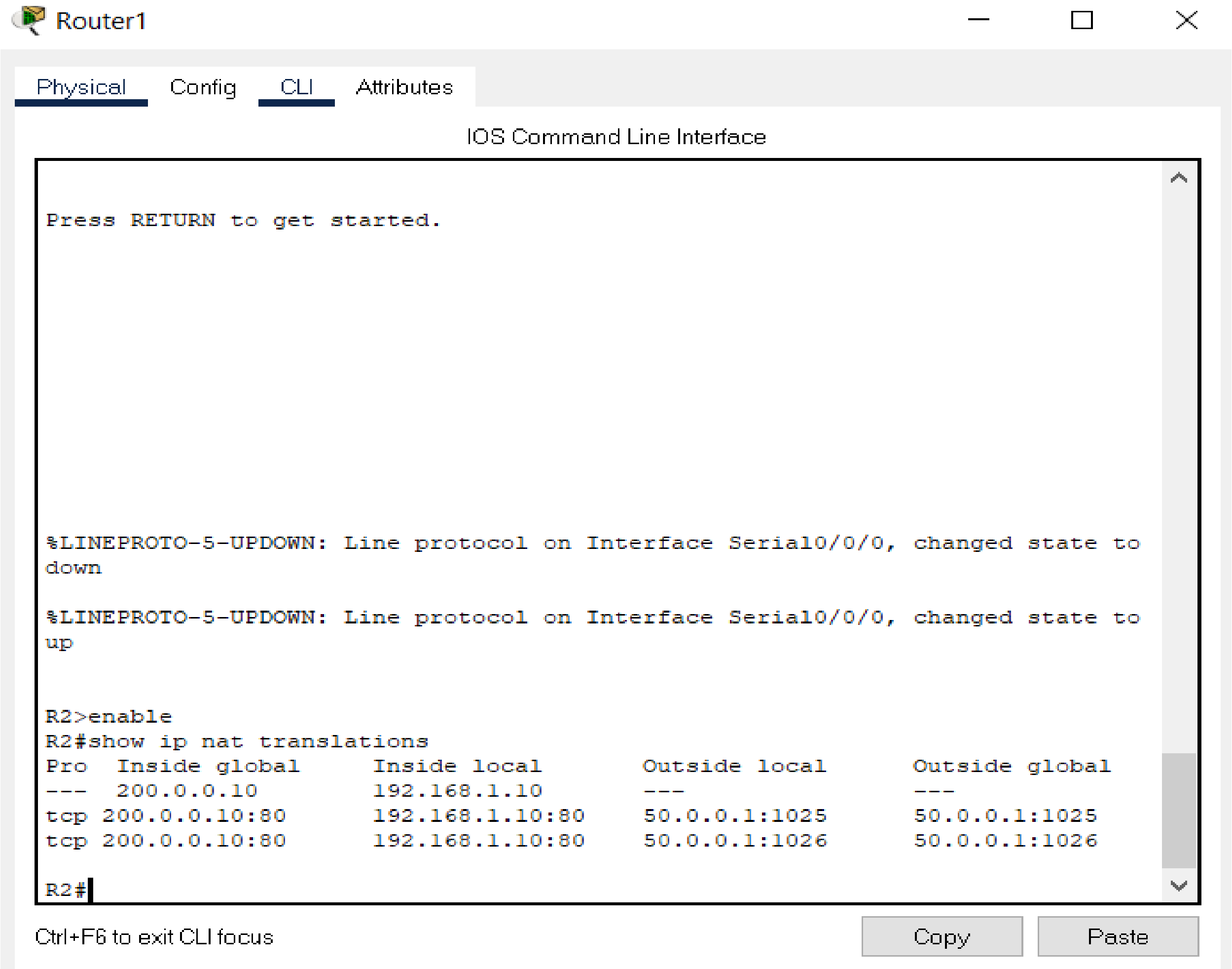
Request Timeout

Note : we are not able to connect with remote device from host is because we configured NAT only for two hosts (Laptop0 and Laptop1) which IP addresses are 10.0.0.10 and 10.0.0.20. So only the host 10.0.0.10 and 10.0.0.20 will be able to access the remote device.



```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to
up


R1>en
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 50.0.0.1:1025      10.0.0.10:1025     200.0.0.10:80      200.0.0.10:80
tcp 50.0.0.1:1026      10.0.0.10:1026     200.0.0.10:80      200.0.0.10:80

R1#show ip access-lists 1
Standard IP access list 1
    permit host 10.0.0.10 (12 match(es))
    permit host 10.0.0.20
    deny any (36 match(es))

R1#
```

Show command using ip nat translations



```
Press RETURN to get started.








%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to
up


R2>enable
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  200.0.0.10        192.168.1.10       ---                ---
tcp 200.0.0.10:80      192.168.1.10:80    50.0.0.1:1025      50.0.0.1:1025
tcp 200.0.0.10:80      192.168.1.10:80    50.0.0.1:1026      50.0.0.1:1026

R2#
```

Nat translations on Router R1

With that the configuration of dynamic NAT is performed. Furthermore successful testing of working is done as well.

SWITCH SECURTIY CONFIGURATION

WHAT IS SWITCH SECURITY CONFIGURATION

A very important part of securing an organizational network involves the layer 2 parts of the network, specifically the switches. Many people can tend to ignore the security vulnerabilities that can be exploited at layer 2, but these devices are just as vulnerable as high layer devices but are just attacked in different ways.

Switch Port Security
The simplest form of switch security is using port level security. When using port level security, the MAC address(es) and/or number of MAC addresses of the connected devices is controlled. There are three different ways that MAC addresses can be configured onto a port:

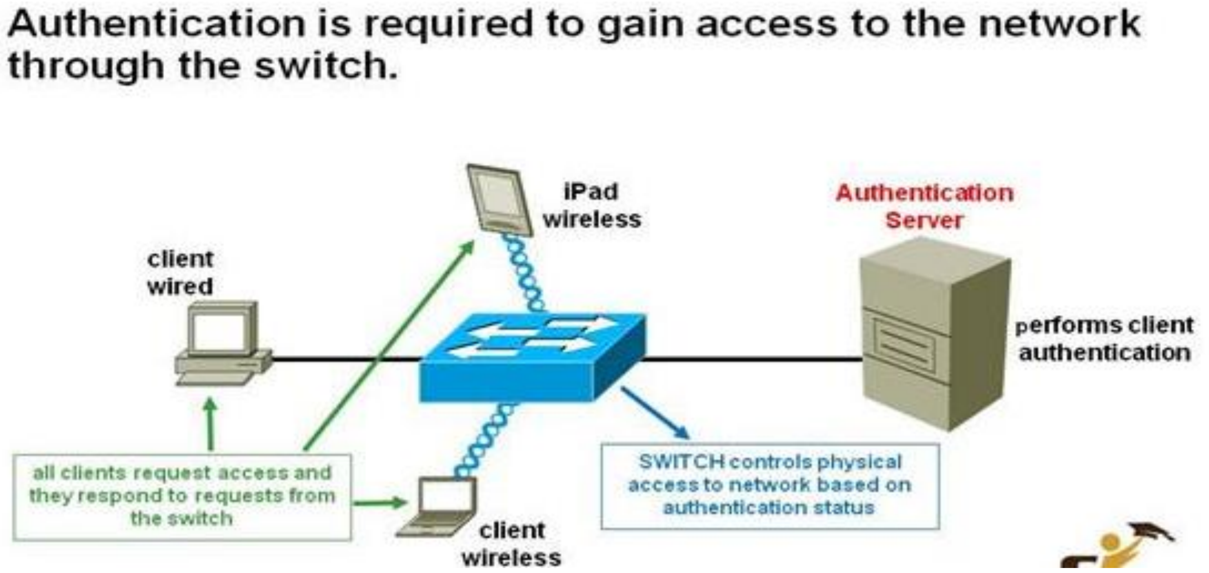
- Statically
- Dynamically
- Sticky

Switch Port Types
When deploying a switched network, one of the first things designed is how the different ports on the switch are connected. There are three main port types:

- Access ports are intended to be connected to a host or group of hosts (but not another switch).
- Trunk ports are intended to be connected to another switch.
- Dynamic ports are able to negotiate themselves as access or trunk ports.

The main difference between access and trunk ports is that access ports are only able to exist within a single Virtual LAN (VLAN) at a time while trunk ports are able to forward traffic from multiple VLANs at once.

FRAMEWORK DESIGN



Authentication is required to gain access to the network through the switch.

iPad
wireless
Authentication
Server
client
wired
performs client
authentication
all clients request access and they respond to requests from the switch
SWITCH controls physical access to network based on authentication status
client
wireless

Framework Design

OBJECTIVES

- Part 1: Create a Secure Trunk
- Part 2: Secure Unused Switchports
- Part 3: Implement Port Security
- Part 4: Enable DHCP Snooping
- Part 5: Configure Rapid PVST PortFast and BPDU Guard

We are enhancing security on two access switches in a partially configured network. We will implement the range of security measures that were covered in this module according to the requirements. Note that routing has been configured on this network, so connectivity between hosts on different VLANs should function when completed.

COMPONENTS USED

- 8 PCS
- 2 SWITCHES
- 1 STATIC TRUNK

STEP BY STEP EXPLANATION AND SCREENSHOTS

Step 1: Create a Secure Trunk.

a. Connect the G0/2 ports of the two access layer switches.

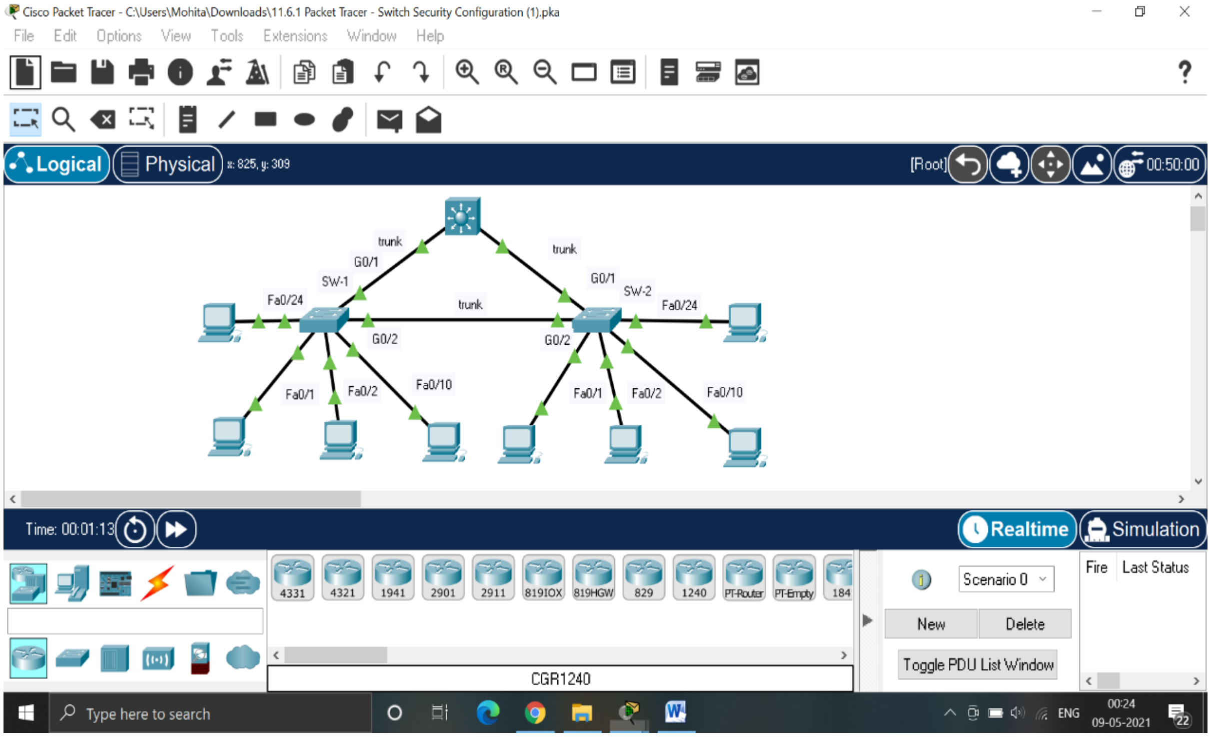
b. Configure ports G0/1 and G0/2 as static trunks on both switches.

c. Disable DTP negotiation on both sides of the link.

d. Create VLAN 100 and give it the name Native on both switches.

e. Configure all trunk ports on both switches to use VLAN 100 as the native VLAN.

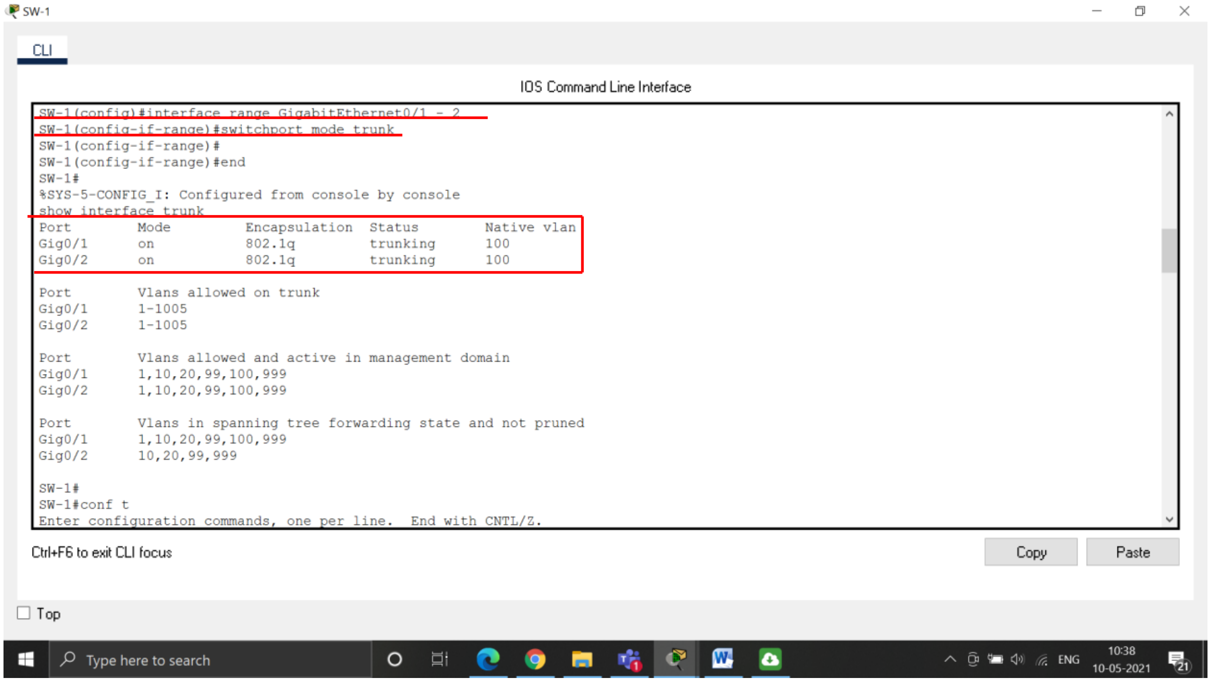
The below diagram shows the setup of the experiment



Network Topology Used

SW-1(config)#interface range GigabitEthernet0/1 - 2

SW-1(config-if-range)#switchport mode trunk



```
SW-1(config)#interface range GigabitEthernet0/1 - 2
SW-1(config-if-range)#switchport mode trunk
SW-1(config-if-range)#
SW-1(config-if-range)#end
SW-1#
%SYS-5-CONFIG_I: Configured from console by console
show interface trunk
Port        Mode             Encapsulation  Status        Native vlan
Gig0/1      on               802.1q         trunking      100
Gig0/2      on               802.1q         trunking      100

Port        Vlans allowed on trunk
Gig0/1      1-1005
Gig0/2      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1,10,20,99,100,999
Gig0/2      1,10,20,99,100,999

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1,10,20,99,100,999
Gig0/2      10,20,99,999

SW-1#
SW-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

SW-1 (config-if-range)#switchport nonegotiate

SW-1 (config-if-range)#

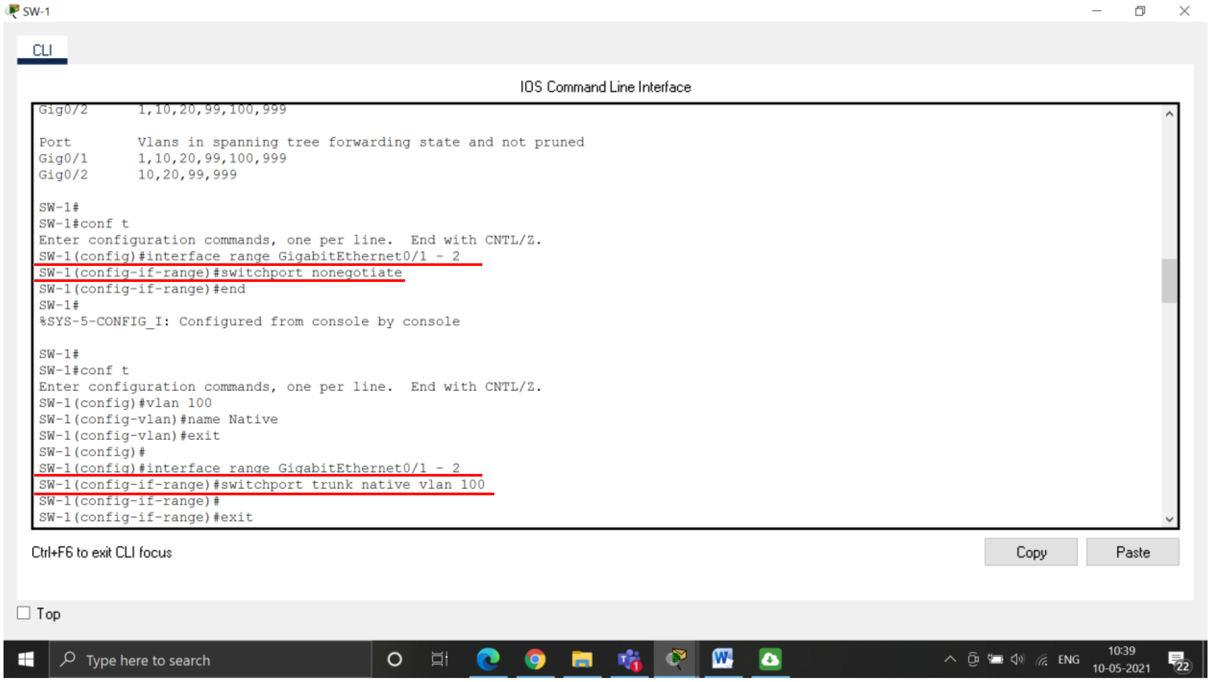
SW-1 (config-if-range)#vlan 100

SW-1 (config-vlan)#name Native

SW-1(config-vlan)#

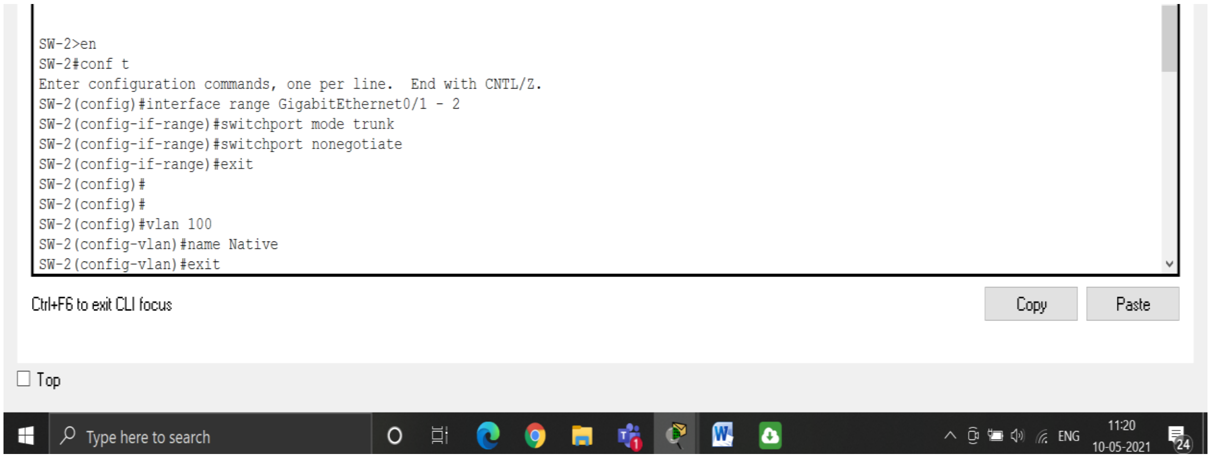
SW-1(config-vlan)#interface range GigabitEthernet0/1 - 2

SW-1(config-if-range)#switchport trunk native vlan 100



```
Gig0/2      1,10,20,99,100,999

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1,10,20,99,100,999
Gig0/2      10,20,99,999

SW-1#
SW-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-1(config)#interface range GigabitEthernet0/1 - 2
SW-1(config-if-range)#switchport nonegotiate
SW-1(config-if-range)#end
SW-1#
%SYS-5-CONFIG_I: Configured from console by console

SW-1#
SW-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-1(config)#vlan 100
SW-1(config-vlan)#name Native
SW-1(config-vlan)#exit
SW-1(config)#
SW-1(config)#interface range GigabitEthernet0/1 - 2
SW-1(config-if-range)#switchport trunk native vlan 100
SW-1(config-if-range)#
SW-1(config-if-range)#exit
```

We execute the same for switch 2(SW-2)



```
SW-2>en
SW-2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-2(config)#interface range GigabitEthernet0/1 - 2
SW-2(config-if-range)#switchport mode trunk
SW-2(config-if-range)#switchport nonegotiate
SW-2(config-if-range)#exit
SW-2(config)#
SW-2(config)#
SW-2(config)#vlan 100
SW-2(config-vlan)#name Native
SW-2(config-vlan)#exit
```

Step 2: Secure Unused Switchports.

a. Shutdown all unused switch ports on SW-1.

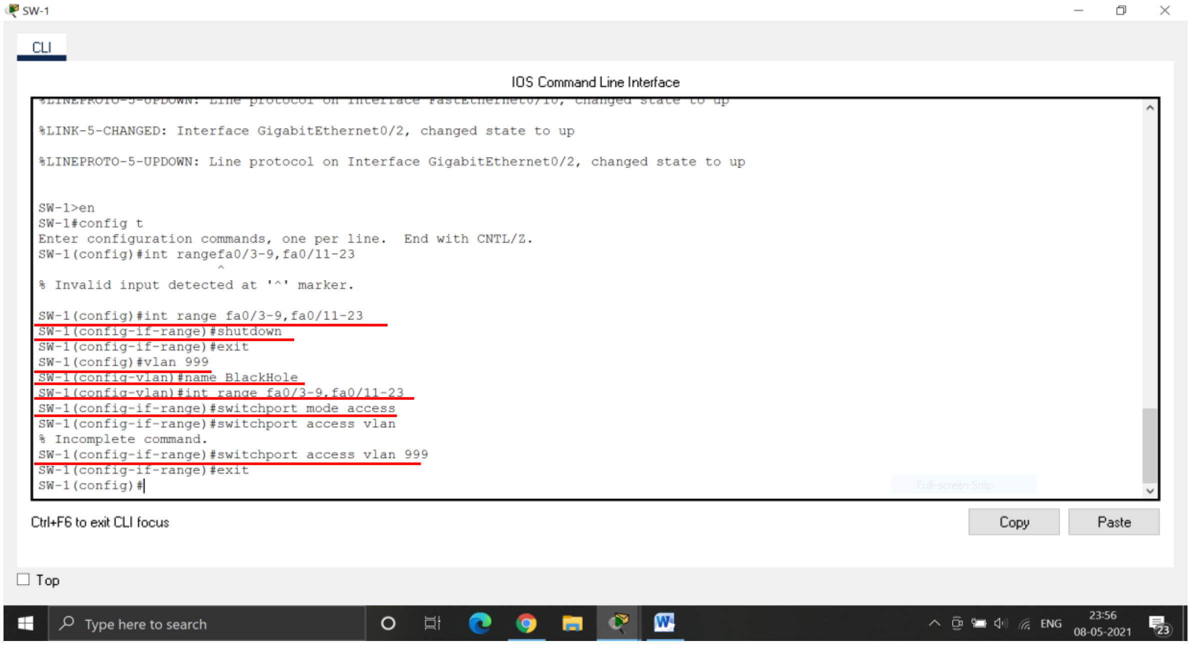
```
SW-1(config)#interface range FastEthernet0/3-9, FastEthernet0/11-23
SW-1(config-if-range)#shutdown
SW-1(config-if-range)#exit
```

b. On SW-1, create a VLAN 999 and name it BlackHole. The configured name must match the requirement exactly.

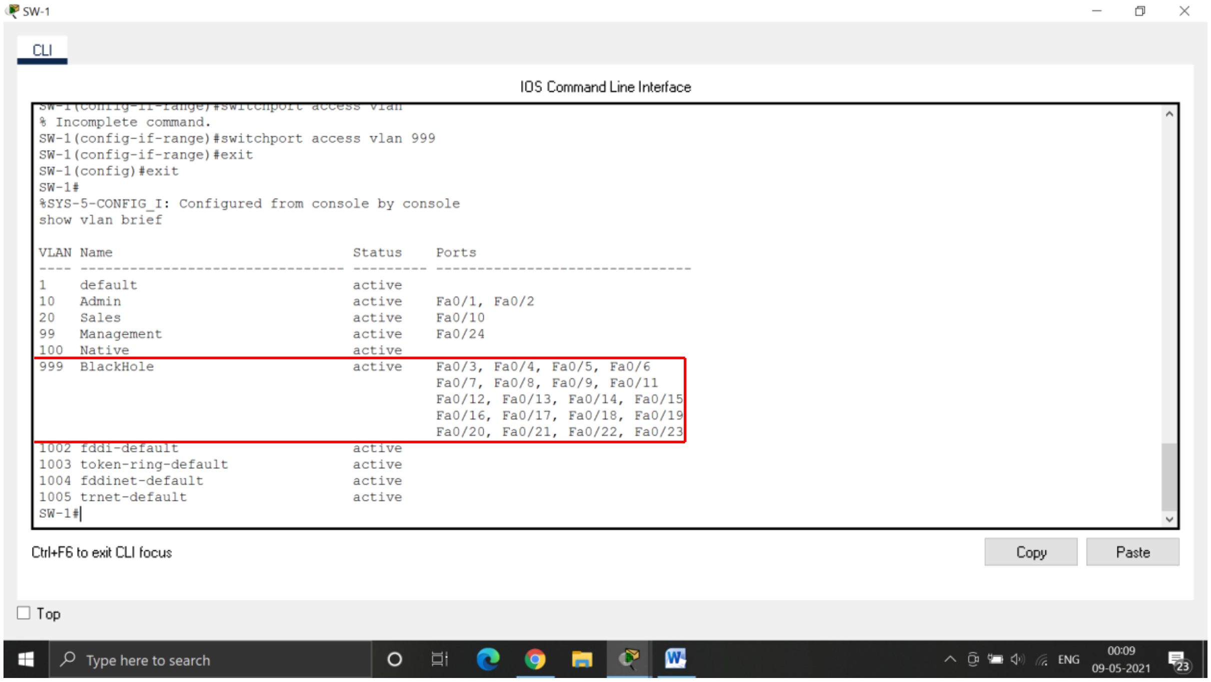
```
SW-1(config)#vlan 999
SW-1(config-vlan)#name BlackHole
SW-1(config-vlan)#exit
```

c. Move all unused switch ports to the BlackHole VLAN.

```
SW-1(config)#interface range FastEthernet0/3-9, FastEthernet0/11-23
SW-1(config-if-range)#switchport access vlan 999
```



```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up


SW-1>en
SW-1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-1(config)#int rangefa0/3-9,fa0/11-23
                          ^
% Invalid input detected at '^' marker.

SW-1(config)#int range fa0/3-9,fa0/11-23
SW-1(config-if-range)#shutdown
SW-1(config-if-range)#exit
SW-1(config)#vlan 999
SW-1(config-vlan)#name BlackHole
SW-1(config-vlan)#int range fa0/3-9,fa0/11-23
SW-1(config-if-range)#switchport mode access
SW-1(config-if-range)#switchport access vlan
% Incomplete command.
SW-1(config-if-range)#switchport access vlan 999
SW-1(config-if-range)#exit
SW-1(config)#
```



```
SW-1(config-if-range)#switchport access vlan
% Incomplete command.
SW-1(config-if-range)#switchport access vlan 999
SW-1(config-if-range)#exit
SW-1(config)#exit
SW-1#
%SYS-5-CONFIG_I: Configured from console by console
show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
10   Admin                            active    Fa0/1, Fa0/2
20   Sales                            active    Fa0/10
99   Management                       active    Fa0/24
100  Native                           active
999  BlackHole                        active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SW-1#
```

Step 3: Implement Port Security.

a. Activate port security on all the active access ports on switch SW-1.

SW-1(config)#interface range FastEthernet0/1, FastEthernet0/2, FastEthernet0/10,FastEthernet0/24

SW-1(config-if-range)#switchport mode access

SW-1(config-if-range)#switchport port-security

b. Configure the active ports to allow a maximum of 4 MAC addresses to be learned on the ports.

SW-1(config)#interface range FastEthernet0/1, FastEthernet0/2, FastEthernet0/10,FastEthernet0/24

SW-1(config-if-range)#switchport port-security maximum 4

c. For ports F0/1 on SW-1, statically configure the MAC address of the PC using port security.

SW-1(config)#interface FastEthernet0/1

SW-1(config-if)#switchport port-security mac-address 0010.11E8.3CBB

d. Configure each active access port so that it will automatically add the MAC addresses learned on the port to the running configuration

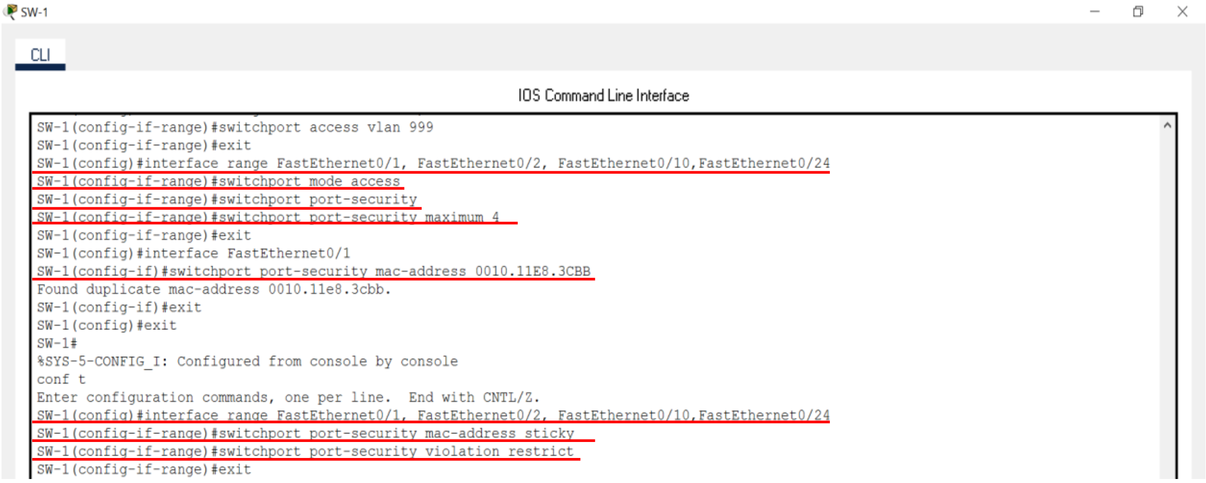
SW-1(config)#interface range FastEthernet0/1, FastEthernet0/2, FastEthernet0/10,FastEthernet0/24

SW-1(config-if-range)#switchport port-security mac-address sticky

e. Configure the port security violation mode to drop packets from MAC addresses that exceed the maximum, generate a Syslog entry, but not disable the ports.

SW-1(config)#interface range FastEthernet0/1, FastEthernet0/2, FastEthernet0/10,FastEthernet0/24

SW-1(config-if-range)#switchport port-security violation restrict



```
SW-1(config-if-range)#switchport access vlan 999
SW-1(config-if-range)#exit
SW-1(config)#interface range FastEthernet0/1, FastEthernet0/2, FastEthernet0/10,FastEthernet0/24
SW-1(config-if-range)#switchport mode access
SW-1(config-if-range)#switchport port-security
SW-1(config-if-range)#switchport port-security maximum 4
SW-1(config-if-range)#exit
SW-1(config)#interface FastEthernet0/1
SW-1(config-if)#switchport port-security mac-address 0010.11E8.3CBB
Found duplicate mac-address 0010.11e8.3cbb.
SW-1(config-if)#exit
SW-1(config)#exit
SW-1#
%SYS-5-CONFIG_I: Configured from console by console
conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-1(config)#interface range FastEthernet0/1, FastEthernet0/2, FastEthernet0/10,FastEthernet0/24
SW-1(config-if-range)#switchport port-security mac-address sticky
SW-1(config-if-range)#switchport port-security violation restrict
SW-1(config-if-range)#exit
```

Step 4: Configure DHCP Snooping.

a. Configure the trunk ports on SW-1 as trusted ports.

SW-1(config)#interface range GigabitEthernet0/1-2

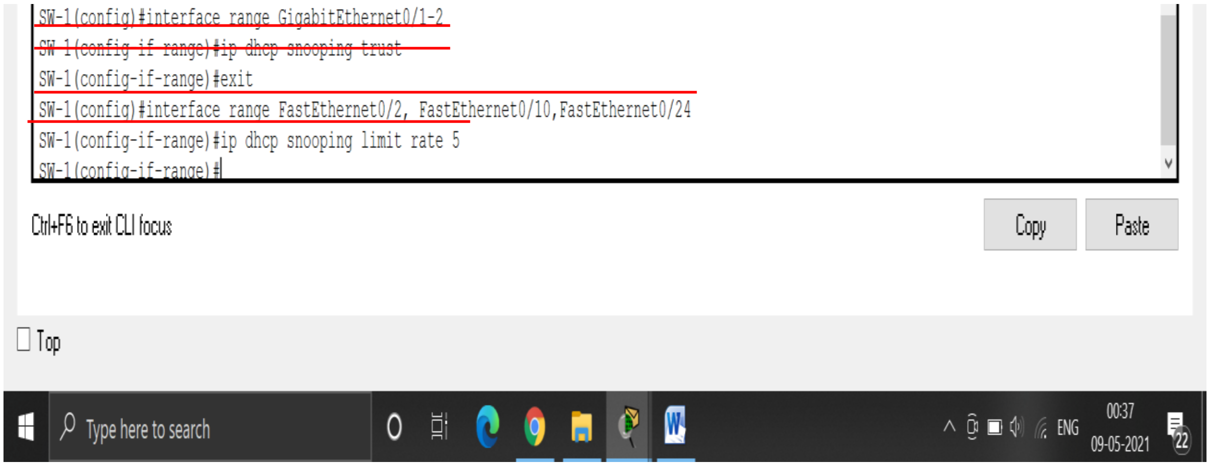
SW-1(config-if-range)#ip dhcp snooping trust

b. Limit the untrusted ports on SW-1 to five DHCP packets per second.

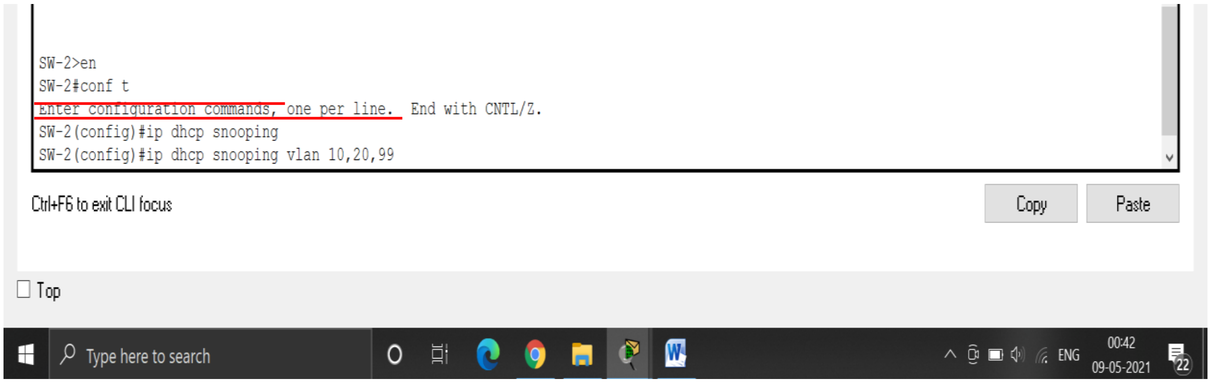
```
SW-1(config)#interface range FastEthernet0/2, FastEthernet0/10,FastEthernet0/24
SW-1(config-if-range)#ip dhcp snooping limit rate 5
```

c. On SW-2, enable DHCP snooping globally and for VLANs 10, 20 and 99.

```
SW-2(config)#ip dhcp snooping
SW-2(config)#ip dhcp snooping vlan 10,20,99
```



```
SW-1(config)#interface range GigabitEthernet0/1-2
SW-1(config-if-range)#ip dhcp snooping trust
SW-1(config-if-range)#exit
SW-1(config)#interface range FastEthernet0/2, FastEthernet0/10,FastEthernet0/24
SW-1(config-if-range)#ip dhcp snooping limit rate 5
SW-1(config-if-range)#
```



```
SW-2>en
SW-2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-2(config)#ip dhcp snooping
SW-2(config)#ip dhcp snooping vlan 10,20,99
```

Step 5: Configure PortFast, and BPDU Guard.

Portfast and BPDU Guard

A feature to disable the delay is called Portfast. When a port is enabled with Portfast, it will immediately transition to a forwarding state.A companion feature is called BPDU guard. Because a port that is intended to be connected to a single host should not receive Bridge Protocol Data Units (BPDUs) from another switch, the BPDU feature will automatically transition the port to an err-disabled state, and manual administrator intervention is required before traffic will be allowed to be forwarded again.

a.Enable PortFast on all the access ports that are in use on SW-1.

b. Enable BPDU Guard on all the access ports that are in use on SW-1.

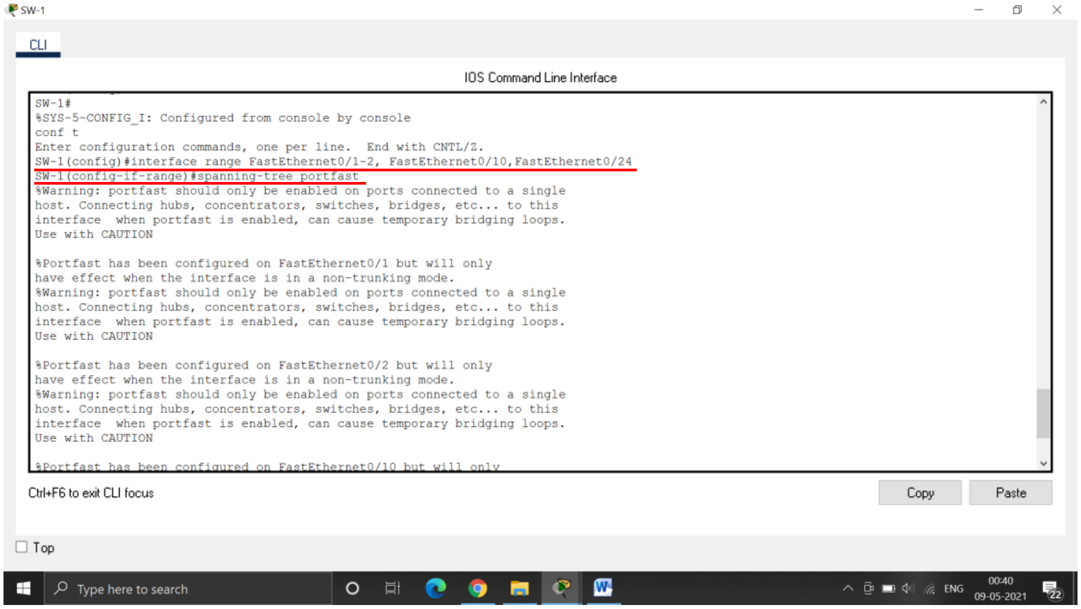
```
SW-1(config)#interface range FastEthernet0/1-2, FastEthernet0/10,FastEthernet0/24
```

```
SW-1(config-if-range)#spanning-tree portfast
```

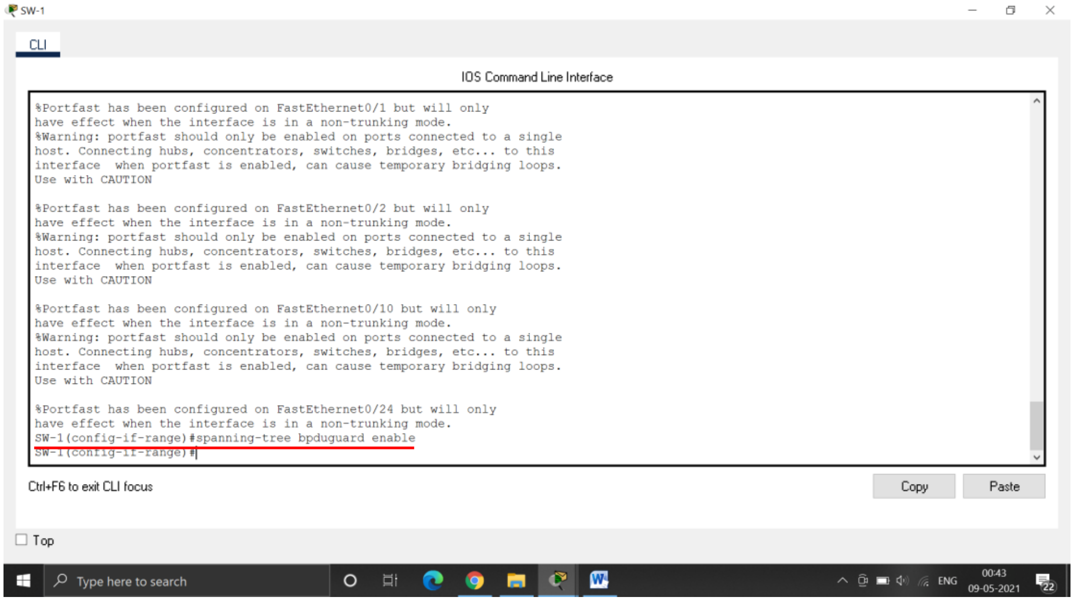
```
SW-1(config-if-range)#spanning-tree bpduguard enable
```

c. Configure SW-2 so that all access ports will use PortFast by default.

```
SW-2(config)#spanning-tree portfast default
```

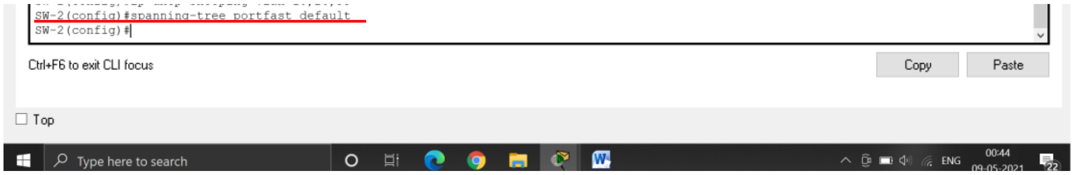


```
SW-1#
%SYS-5-CONFIG_I: Configured from console by console
conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-1(config)#interface range FastEthernet0/1-2, FastEthernet0/10,FastEthernet0/24
SW-1(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/1 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/2 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/10 but will only
```



```
%Portfast has been configured on FastEthernet0/1 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/2 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/10 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/24 but will only
have effect when the interface is in a non-trunking mode.
SW-1(config-if-range)#spanning-tree bpduguard enable
SW-1(config-if-range)#
```

SW-2



```
SW-2(config)#spanning-tree portfast default
SW-2(config)#
```

When all the steps are successfully completed we have configured and enabled the switch security in the system.

ROUTER SECURITY CONFIGURATION

WHAT IS ROUTER SECURITY CONFIGURATION

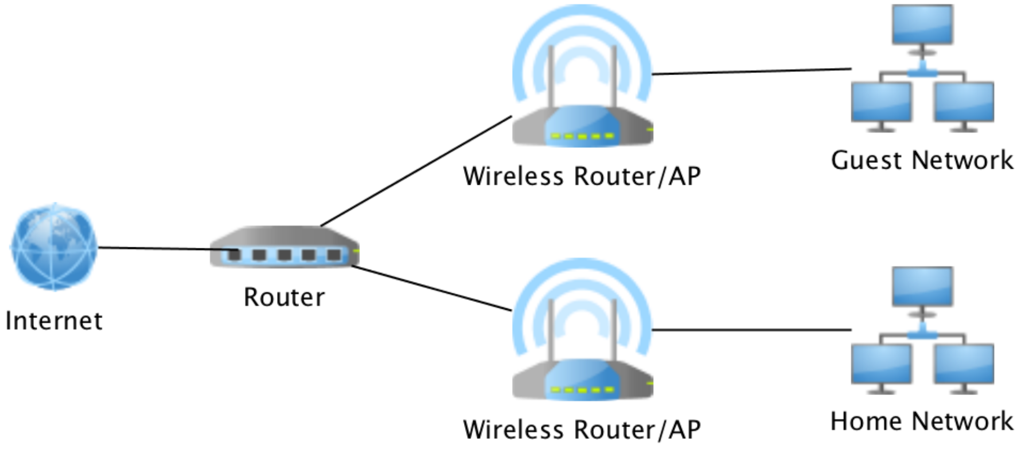
The Router is perhaps the most important gadget in your home. It checks all incoming and outgoing traffic, acting as a sentry to make sure that nothing dangerous comes in and nothing sensitive goes out. It controls access to your home Wi-Fi network and through that all of your phones, tablets, laptops, and more. If someone else gains access to that network—whether a remote hacker or your next-door neighbor—it can be quick work to compromise those devices.

It’s also important to protect your network from attacks over the internet by keeping your router secure. Your router directs traffic between your local network and the internet. So, it’s your first line of defense for guarding against such attacks. If you don't take steps to secure your router, strangers could gain access to sensitive personal or financial information on your device.

Strangers also could seize control of your router, to direct you to fraudulent websites. Change the name of your router from the default. The name of your router (often called the service set identifier or SSID) is likely to be a standard, default ID assigned by the manufacturer. Change the name to something unique that only you know.

Change your router's pre-set password(s). The manufacturer of your wireless router probably assigned it a standard default password that allows you to set up and operate the router, as its “administrator.” Hackers know these default passwords, so change it to something only you know. The same goes for any default “user” passwords. Use long and complex passwords – think at least 12 characters, with a mix of numbers, symbols, and upper and lower case letters.

FRAMEWORK DESIGN



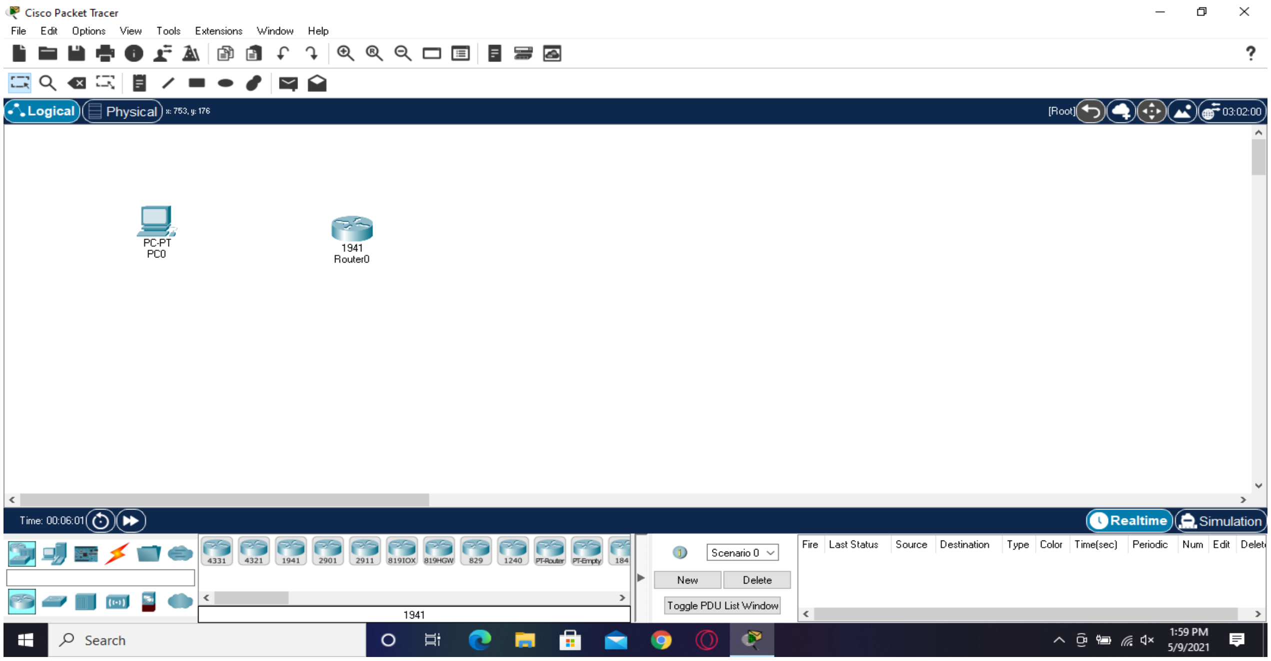
Framework Design

AIM

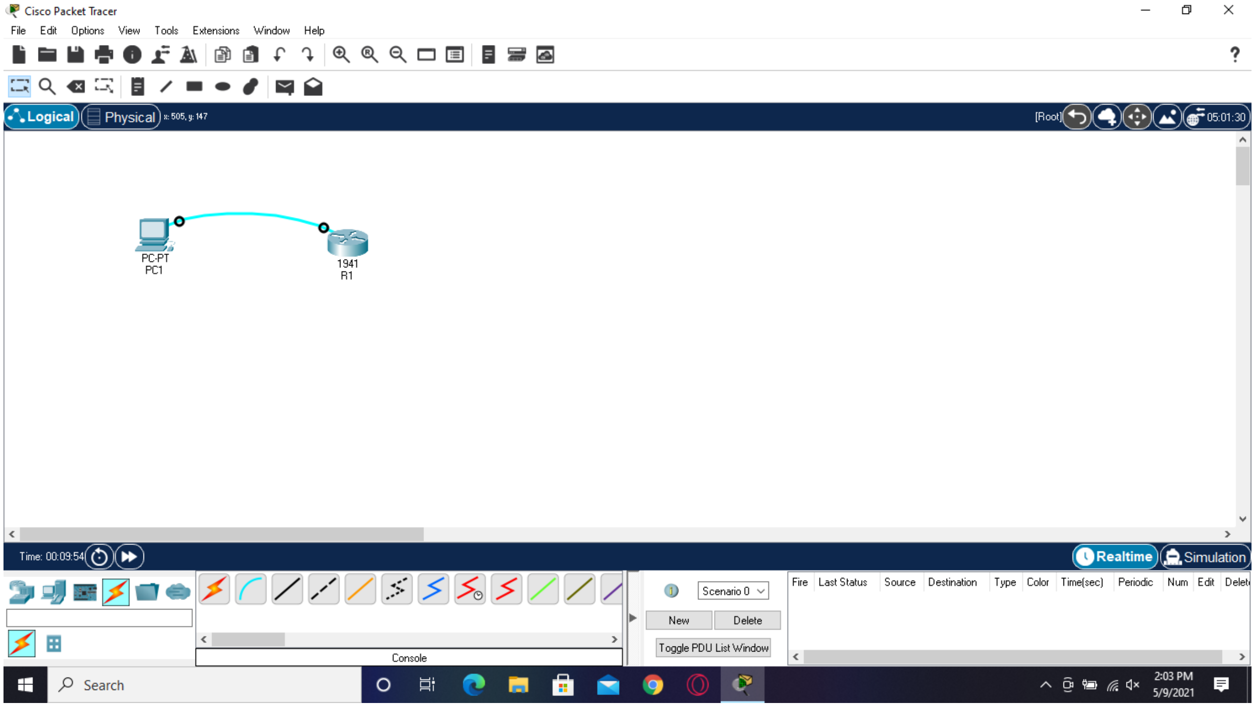
To implement basic router security by enabling a password for router access and performing encryption of the password.

STEP BY STEP EXPLANATION AND SCREENSHOTS

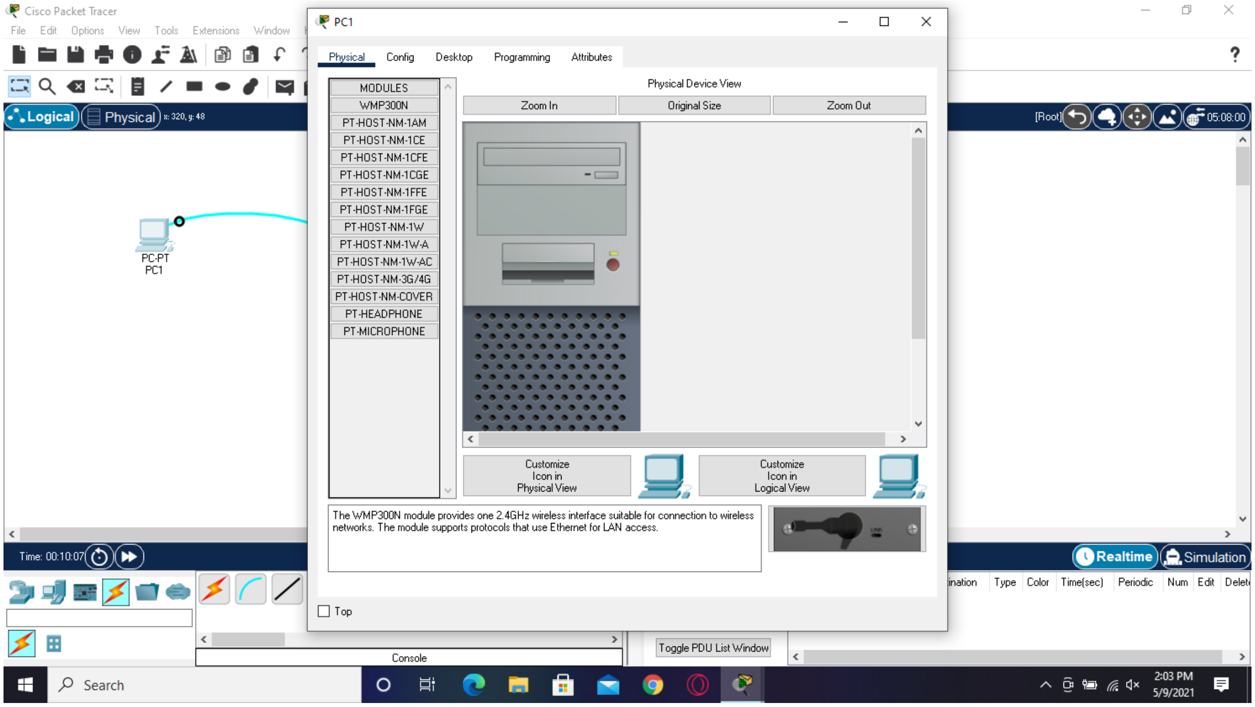
Step 1: Place components PC-PT and Router 1941. Rename PC as PC1 and Router as R1


Cisco Packet Tracer
File Edit Options View Tools Extensions Window Help
Logical
Physical
x: 753, y: 176
[Root]
03:02:00
PC-PT
PC0
1941
Router0
Time: 00:06:01
Realtime
Simulation
4331 4321 1941 2901 2911 819IOX 819HGW 829 1240 PT-Router PT-Empty 184
1941
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
Search
1:59 PM
5/9/2021

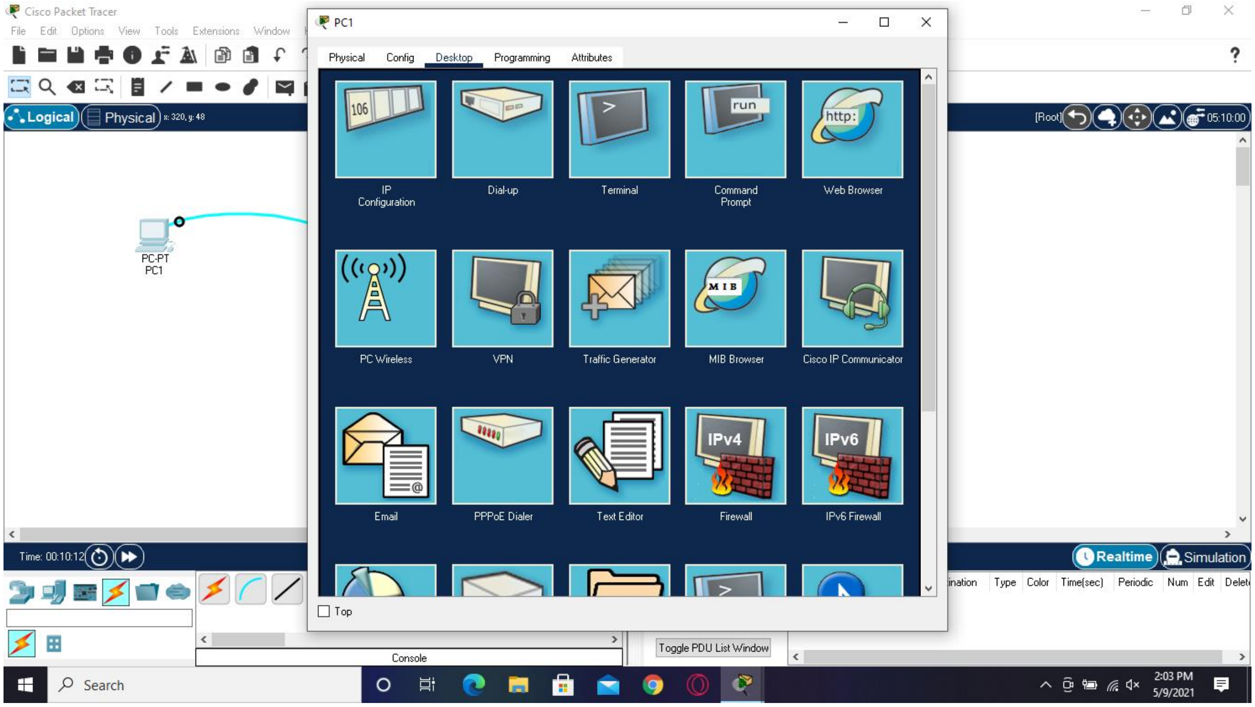
Step 2: Connect PC1's RS-232 port to R1's console port.

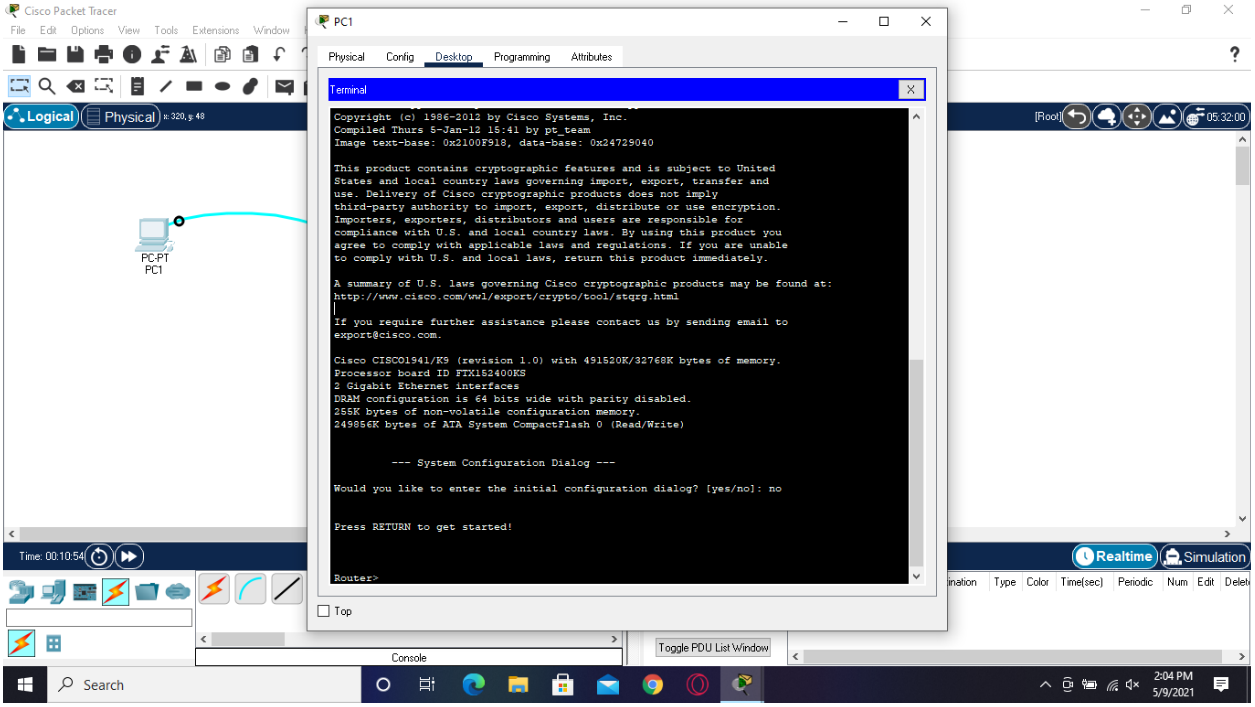


Step 3: Use the console connection to configure the router from PC1. Change the hostname to R1

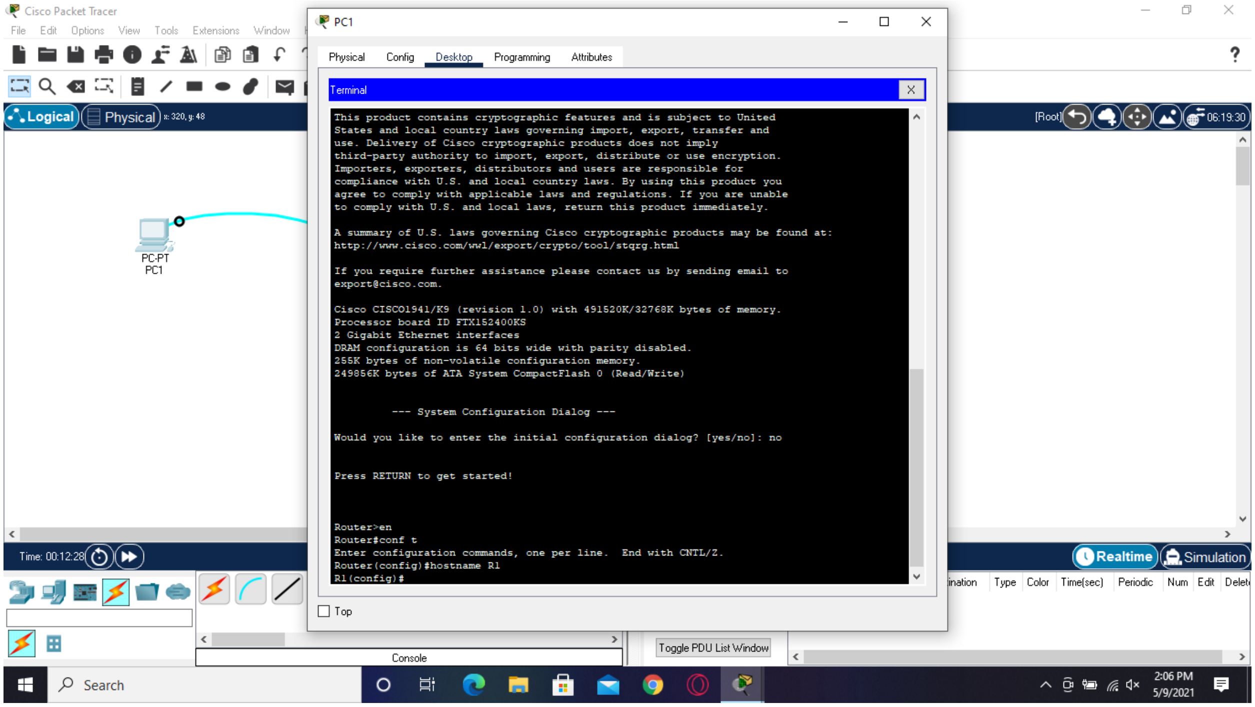


The WMP300N module provides one 2.4GHz wireless interface suitable for connection to wireless networks. The module supports protocols that use Ethernet for LAN access.



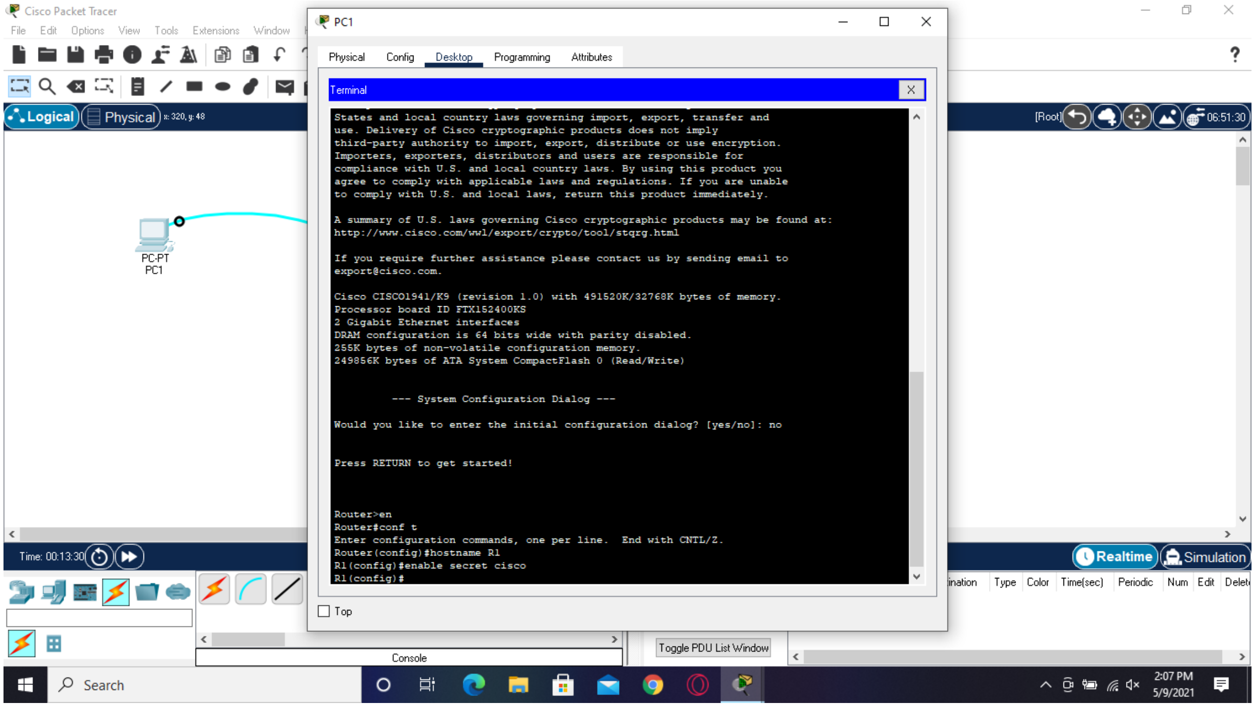


```
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team
Image text-base: 0x2100F918, data-base: 0x24729040

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/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)


         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no


Press RETURN to get started!



Router>
```



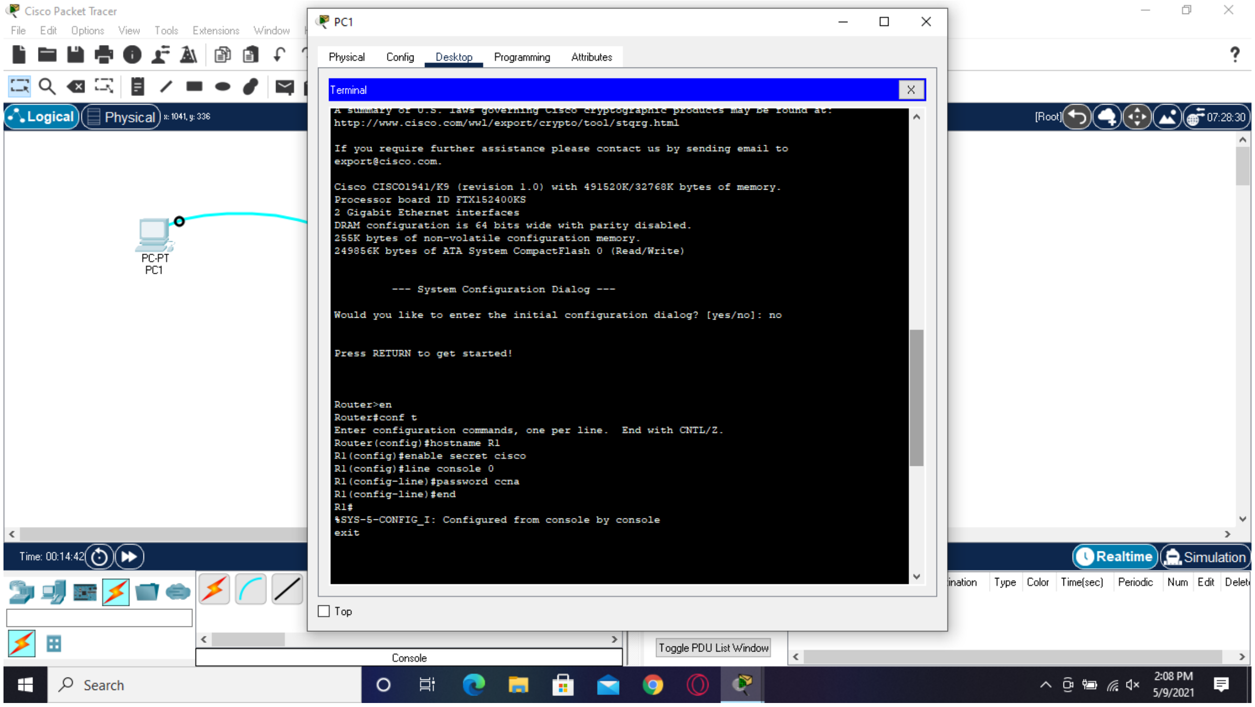
```
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors 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/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)


         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no


Press RETURN to get started!



Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
```

Step 4: Set the enable secret of R1 to cisco

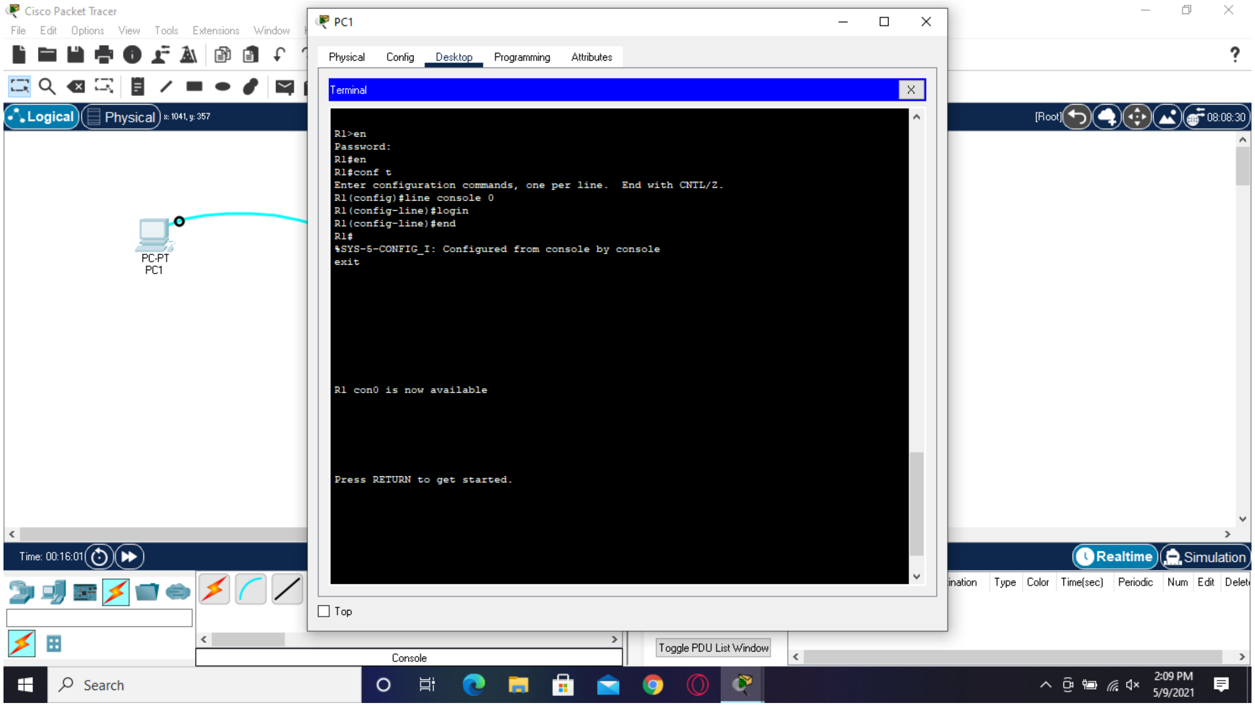


```
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local 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/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)


         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no


Press RETURN to get started!



Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#enable secret cisco
R1(config)#
```

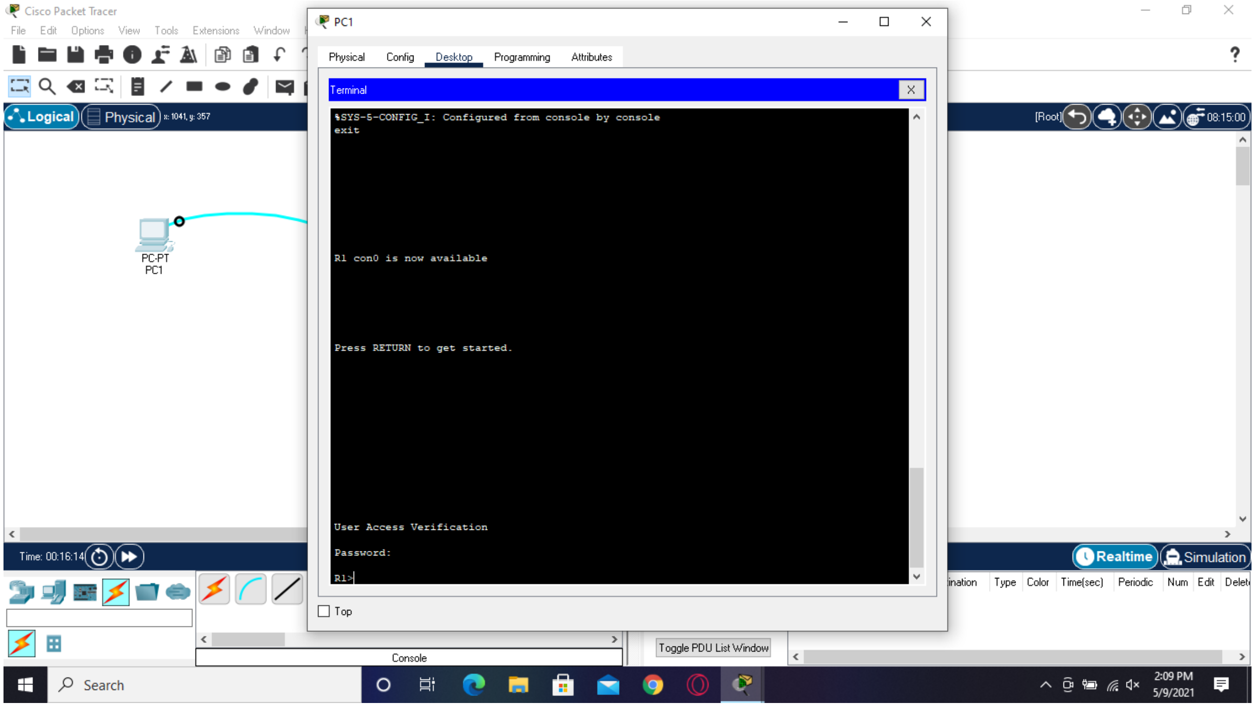
Step 5: Set console password of R1 to “ccna” and make it required to connect to R1 by the console port. Check the running configuration.



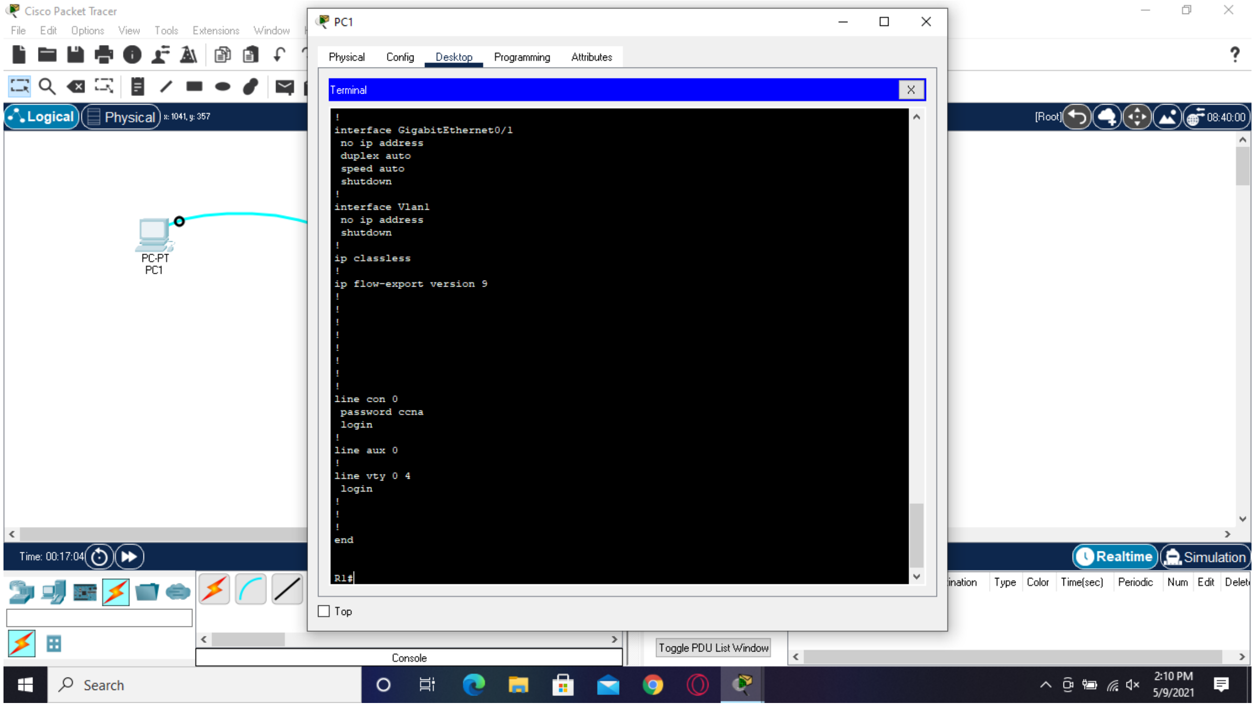
```
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)


         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no


Press RETURN to get started!



Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#enable secret cisco
R1(config)#line console 0
R1(config-line)#password ccna
R1(config-line)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
exit
```



```
R1>en
Password:
R1#en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#line console 0
R1(config-line)#login
R1(config-line)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
exit



R1 con0 is now available



Press RETURN to get started.
```

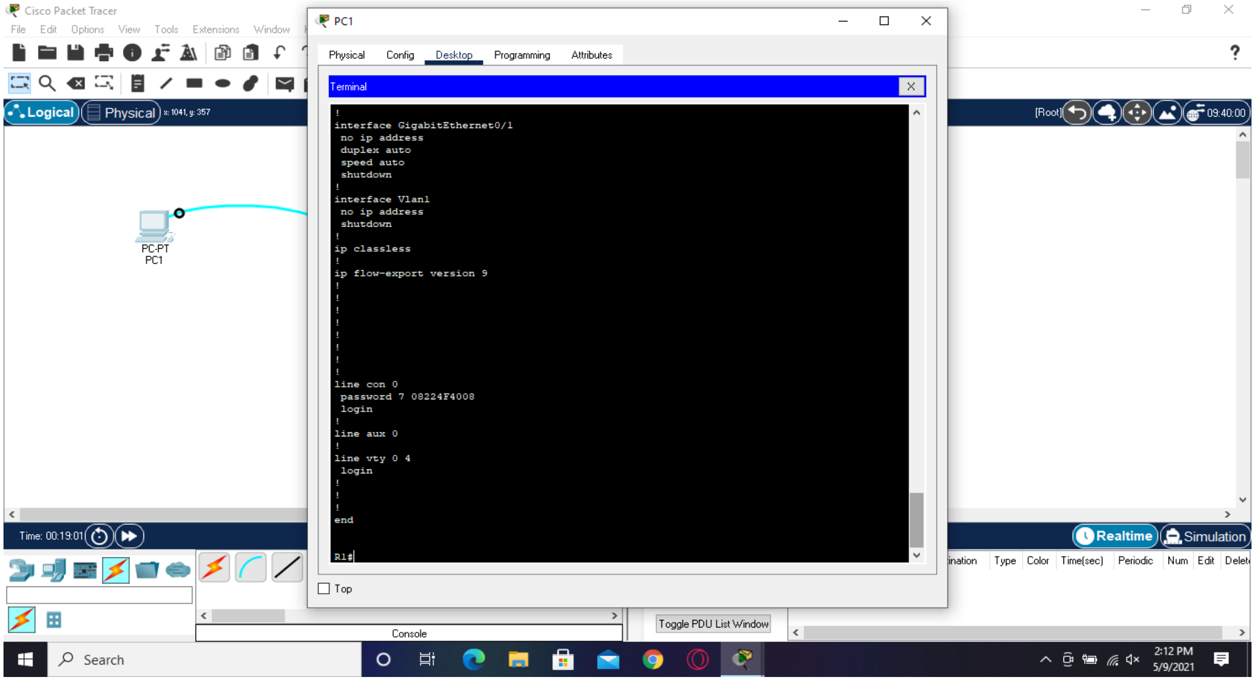


```
%SYS-5-CONFIG_I: Configured from console by console
exit



R1 con0 is now available



Press RETURN to get started.



User Access Verification

Password:

R1>
```



```
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
!
line con 0
 password ccna
 login
!
line aux 0
!
line vty 0 4
 login
!
!
!
end


R1#
```

Step 6: Encrypt the password using service password-encryption command



```
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
!
line con 0
 password 7 08224F4008
 login
!
line aux 0
!
line vty 0 4
 login
!
!
!
end


R1#
```

TERMINAL COMMANDS

```
R1>en
R1#conf t
Router(config)#hostname R1
R1(config)#enable secret cisco
R1(config)#line console 0
R1(config-line)#password ccna
R1(config-line)#login
R1(config-line)#end
R1#exit

User Access Verification

Password: ccna
R1>en
password: cisco
R1#show run

R1#conf t
R1(config)#service password-encryption
R1(config)#exit
R1#show run
```

REFERENCES

1. https://www.computernetworkingnotes.com/ccna-study-guide/how-to-configure-dynamic-nat-in-cisco-router.html

2. https://youtu.be/qmJUzktLGpc

3. https://youtu.be/Gj-8agyq4yQ