

LAB REPORT

COURSE NO. : ICT 4256

COURSE TITLE: DATA COMMUNICATION AND NETWORKS LAB

PREPARED BY

Md. Moniruzzaman Hemal

ID:1801007

Session: 2018-2019

SUPERVISED BY

Md. Habibur Rahman

Lecturer

Department of ICT, BDU



BANGABANDHU SHEIKH
MUJIBUR RAHMAN DIGITAL
UNIVERSITY
(BDU)

Report No: 01

Report Title: Introduction with Network Topology using Cisco Packet Tracer.

Objectives:

- To learn how to create a network topology in PT
- To learn how to configure a network topology using command mode

Discussion:

Network topology is the geometric representation of the relationship of all the links connecting the devices or nodes. Network topology represents in two ways one is physical topology that defines the way in which a network is physically laid out and another one is logical topology that defines how data flows through the network. In this paper we have discussed how to design bus, star and mesh topology networks and provide interfacing and simulation between end points using packet tracer software.

Methodology of my project:

- Create a New Project.
- Create the basic Network topology.
- Configuration of the Network Nodes.
- Choose the Statistics.
- Run the Simulation.
- Analysis of the Results.

Working Procedure:

To implement this practical following network topology is required to be configured using the commands learned in previous practical. After configuring the given network, a packet should be ping from any one machine to another.

Topology

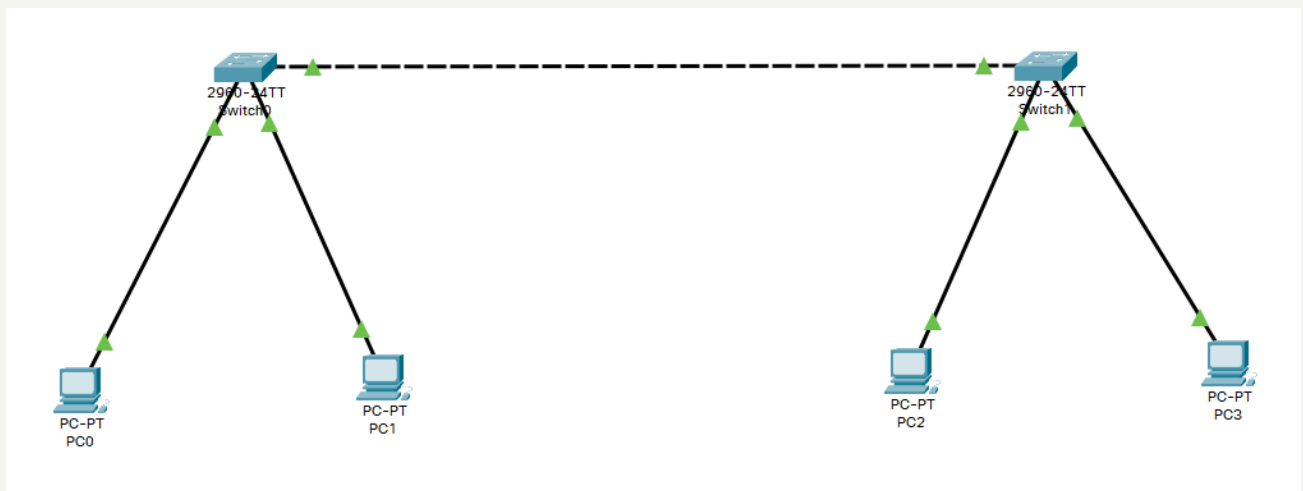


Figure 1.1: Bus Network Topology using Cisco Packet Tracer.

1. Configure PC0, PC1 with following IP address and Subnet Mask:

Host	IP Address	Subnet Mask
PC0	192.168.25.1	255.255.255.0
PC1	192.168.25.2	255.255.255.0

2. Use the ping command to verify the connection from PC0 to PC1.

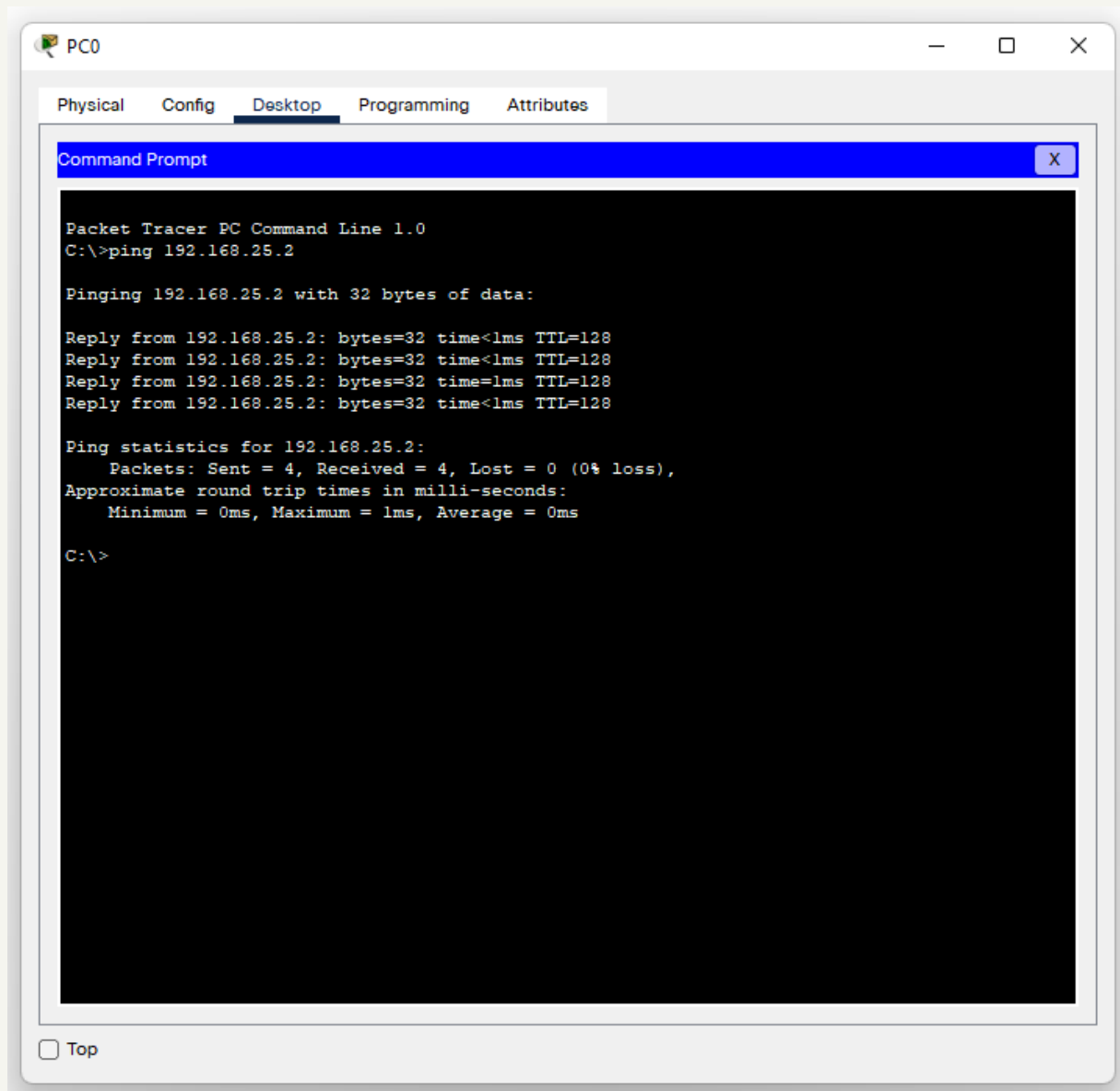


Figure 1.2: ping command to verify the connection from PC0 to PC1.

3. Do the same procedure for PC2 and PC3 with the following IP.

4. Check the connection from PC2 to PC3 using the ping command.

Host	IP Address	Subnet Mask
PC2	192.168.25.3	255.255.255.0
PC3	192.168.25.4	255.255.255.0

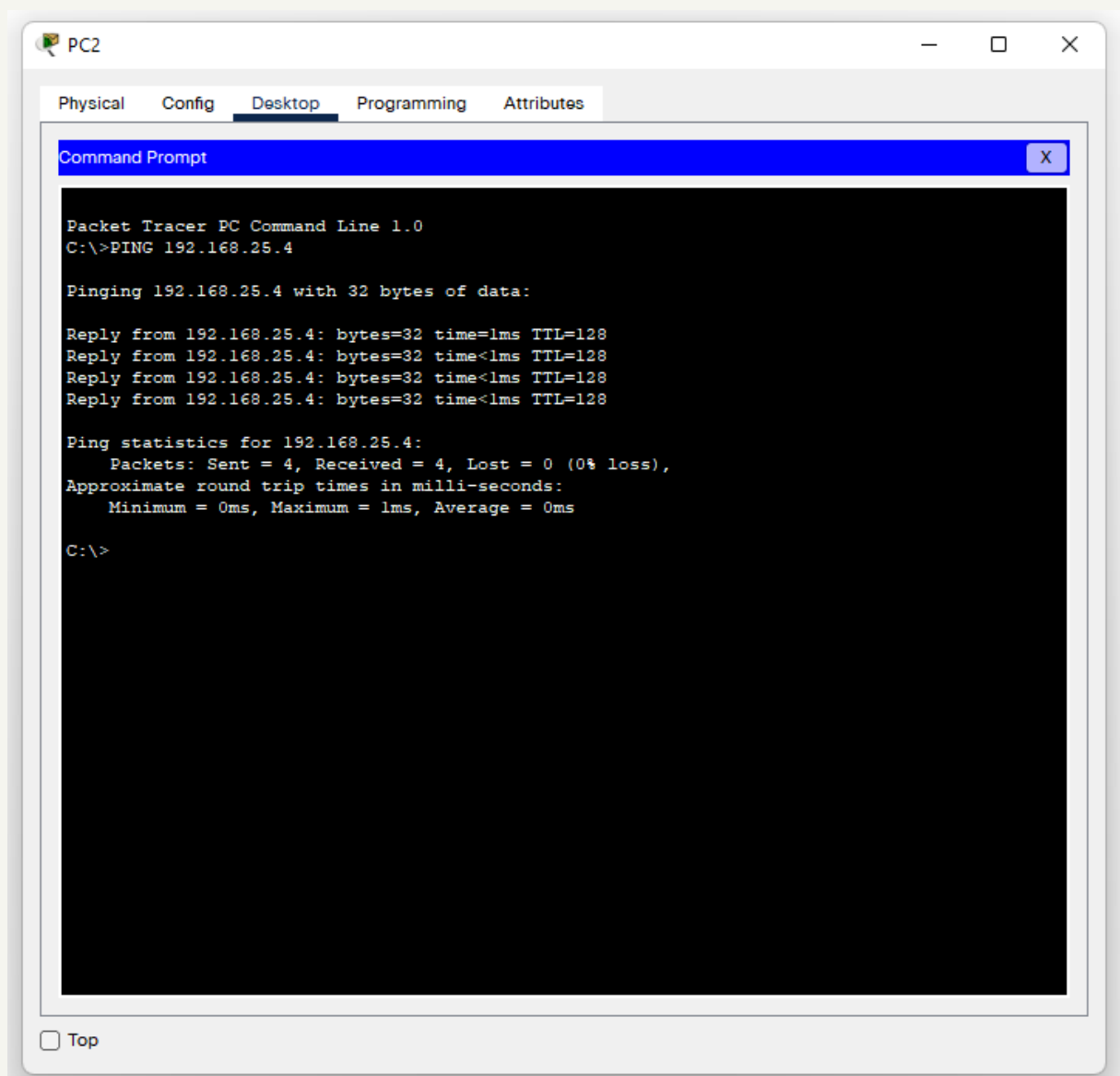


Figure 1.3: ping command to verify the connection from PC2 to PC3.

5. Simulation across PCs









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	PC2	PC3	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC0	PC3	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC1	PC3	ICMP		0.000	N	3	(edit)	(delete)

Figure 1.4: Successful Packets travel across PCs

PDU Information at Device: PC0

OSI Model

Outbound PDU Details

At Device: PC0

Source: PC0

Destination: PC3

In Layers

Out Layers

Layer7

Layer6

Layer5

Layer4

Layer3

Layer2

Layer1

Layer7

Layer6

Layer5

Layer4

Layer 3: IP Header Src. IP: 192.168.25.1, Dest. IP: 192.168.25.4
ICMP Message Type: 8

Layer 2: Ethernet II Header
0006.2A75.A005 >> 0050.0FD4.29D3

Layer 1: Port(s):

1. The Ping process starts the next ping request.
2. The Ping process creates an ICMP Echo Request message and sends it to the lower process.
3. The source IP address is not specified. The device sets it to the port's IP address.
4. The device sets TTL in the packet header.
5. The destination IP address is in the same subnet. The device sets the next-hop to destination.

Challenge Me

<< Previous Layer

Next Layer >>

Figure 1.5: Protocol data unit at PC0.

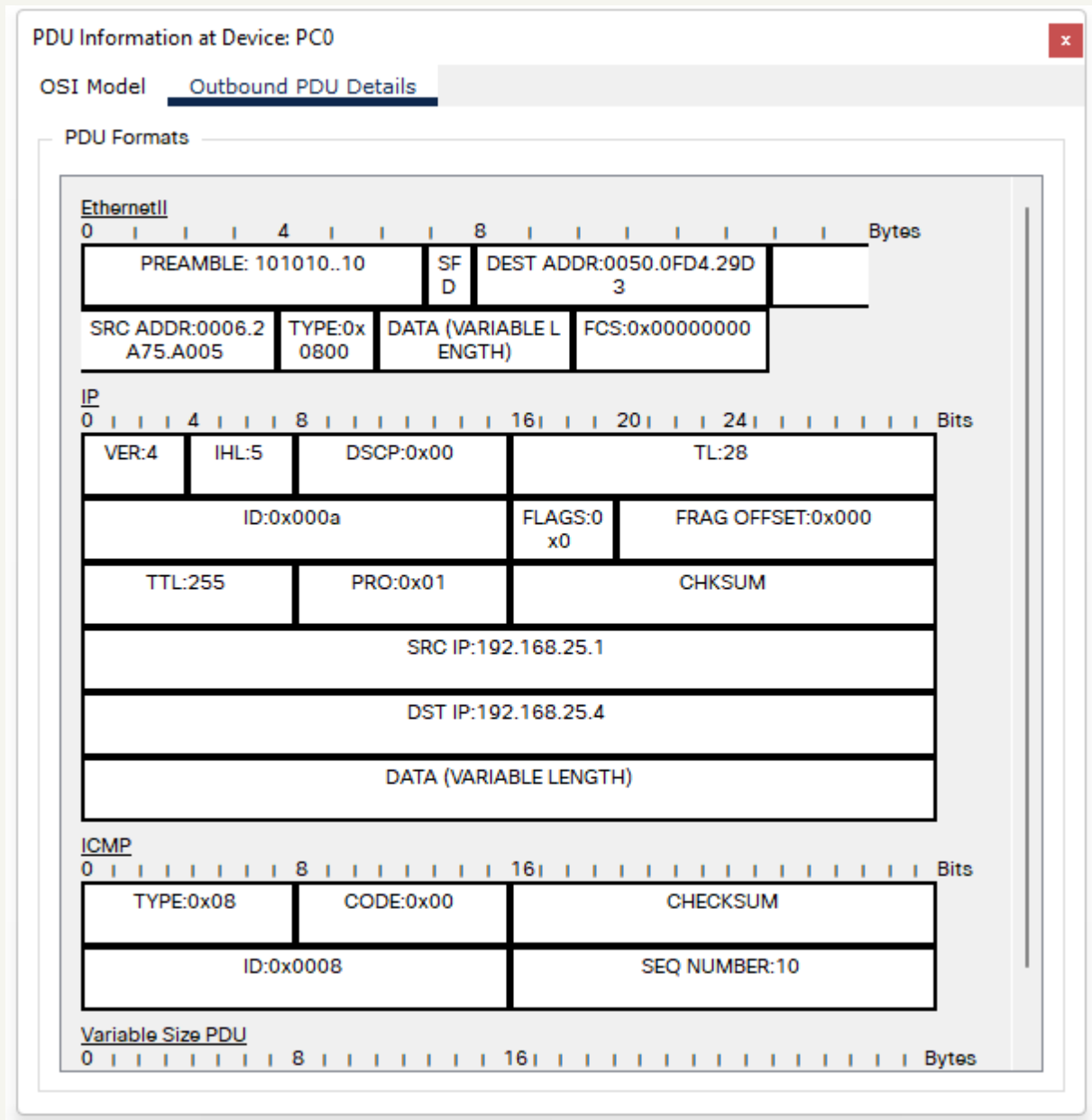


Figure 1.6: Outbound PDU (Protocol data unit) at PC0.

Conclusion:

This network represents the Introduction with Network Topology using Cisco Packet Tracer. Here we have also compared the Check the connection from one PC to another using the ping command.

Report No: 02**Report Title:** Implementation of RIP using Packet Tracer.

Objectives:

The main objectives behind RIP implementation using Cisco packet tracer are:

- Configure routers using basic interface configuration commands.
- Enable RIP.
- Verify the RIP configuration.

Discussion:

The Routing Information Protocol (RIP) is a distance-vector routing protocol, which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is fifteen. Originally each RIP router transmitted full updates every 30 seconds.

RIP version 1: The original specification of RIP uses Classful routing. The periodic routing updates do not carry subnet information, lacking support for variable length subnet masks (VLSM). In other words, all subnets in a network class must have the same size.

RIP version 2: Due to the deficiencies of the original RIP specification, RIP version 2 (RIPv2) was developed. It included the ability to carry subnet information, thus supporting Classless Inter-Domain Routing (CIDR)

Methodology of my project:

- Create a New Project.
- Build the RIP network topology.
- Configuration of the Network Nodes.
- Choose the Statistics.
- Run the Simulation.
- Analysis of the Results.

Working Procedure:

1. Build the network topology.

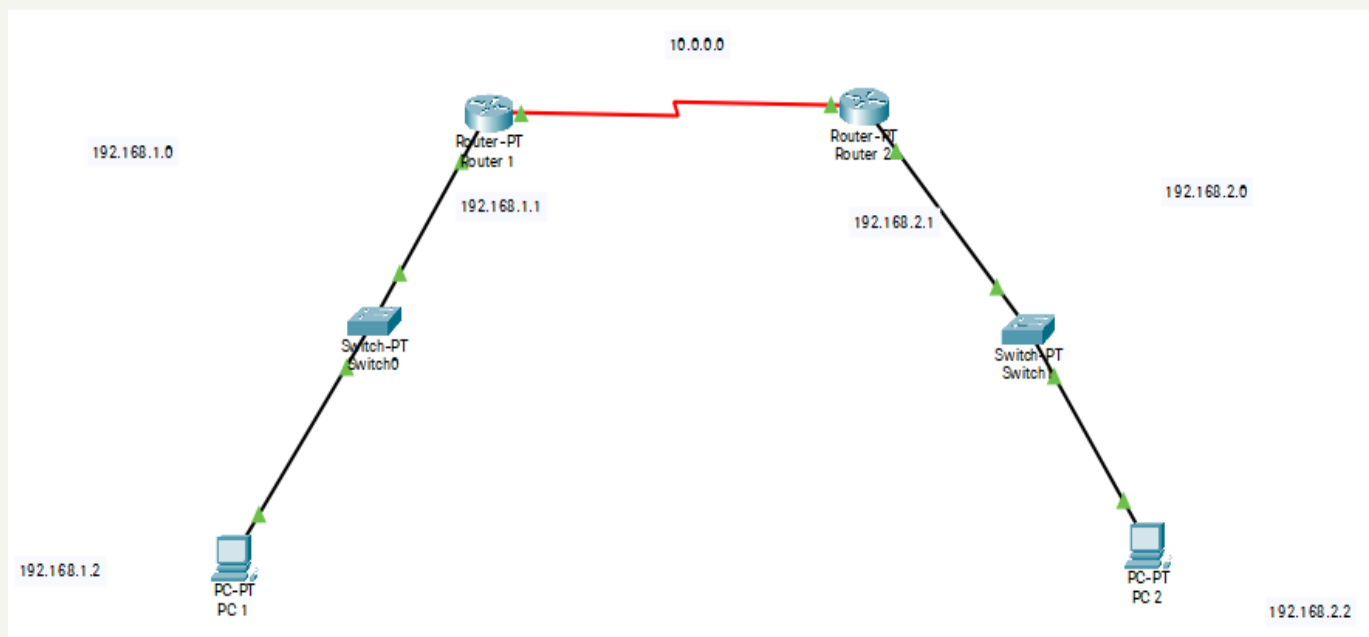


Figure 2.1: Architectural design of the RIP configuration.

2. Configure IP addresses on the PCs and the routers.

Router 1:

```
R1(config)#  
R1(config)#int fa0/0  
R1(config-if)#ip address 192.168.1.1 255.255.255.0  
R1(config-if)#no shut
```

```
R1(config-if)#  
R1(config-if)#interface Serial2/0  
R1(config-if)#ip add 10.0.0.2 255.0.0.0  
R1(config-if)#no shut
```

Router 2:

```
R2(config)#  
R2(config)#int fa0/0  
R2(config-if)#ip add 192.168.2.1 192.168.2.1  
R2(config-if)#no shut
```

```
R2(config-if)#  
R2(config-if)#int serial2/0  
R2(config-if)#ip add 10.10.0.3 255.0.0.0  
R2(config-if)#no shut
```

3. IP configuration on PCs

Click PC->Desktop->IP Configuration. On each PC assign these addresses:

PC1:

IP address: 192.168.1.2 Subnet mask 255.255.255.0 Default Gateway 192.168.1.1

PC2:

IP address: 192.168.2.2 Subnet mask 255.255.255.0 Default Gateway 192.168.2.1

4. Configure RIPv2 on the routers

Router 1:

```
R1(config)#  
R1(config)#router rip  
R1(config-router)#version 2  
R1(config-router)#network 10.0.0.0  
R1(config-router)#network 192.168.1.0
```

Router 2:

```
R2(config)#  
R2(config)#router rip  
R2(config-router)#version 2  
R2(config-router)#network 10.0.0.0  
R2(config-router)#network 192.168.1.0
```

As we can see, to configure rip on each router, we enable RIP using router rip command then advertise the networks directly connected to the router interfaces using network command.

5. Verifying RIP configuration.

To verify that RIP is indeed advertising routes, we can use the **show Ip route** command on R1.

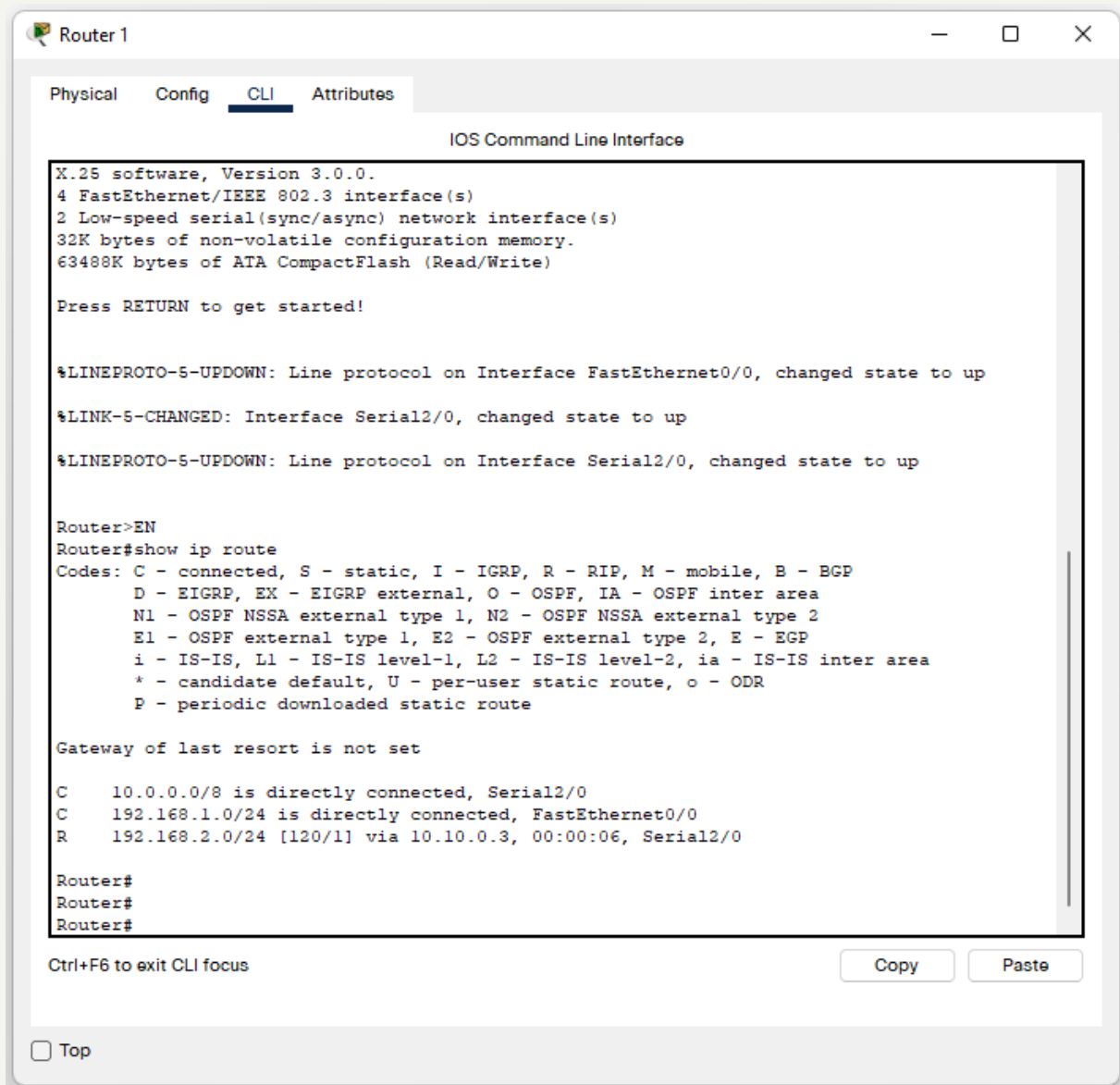


Figure 2.2: Verifying RIP configuration.

we can see that R1 has learned about the 192.168.2.0/24 network. The letter R indicates that the route was learned using RIP. Note the administrative distance of 120 and the metric of 1 in the [120/1] part.

To specifically display routes learnt through RIP use the **show ip route rip** command on the router.

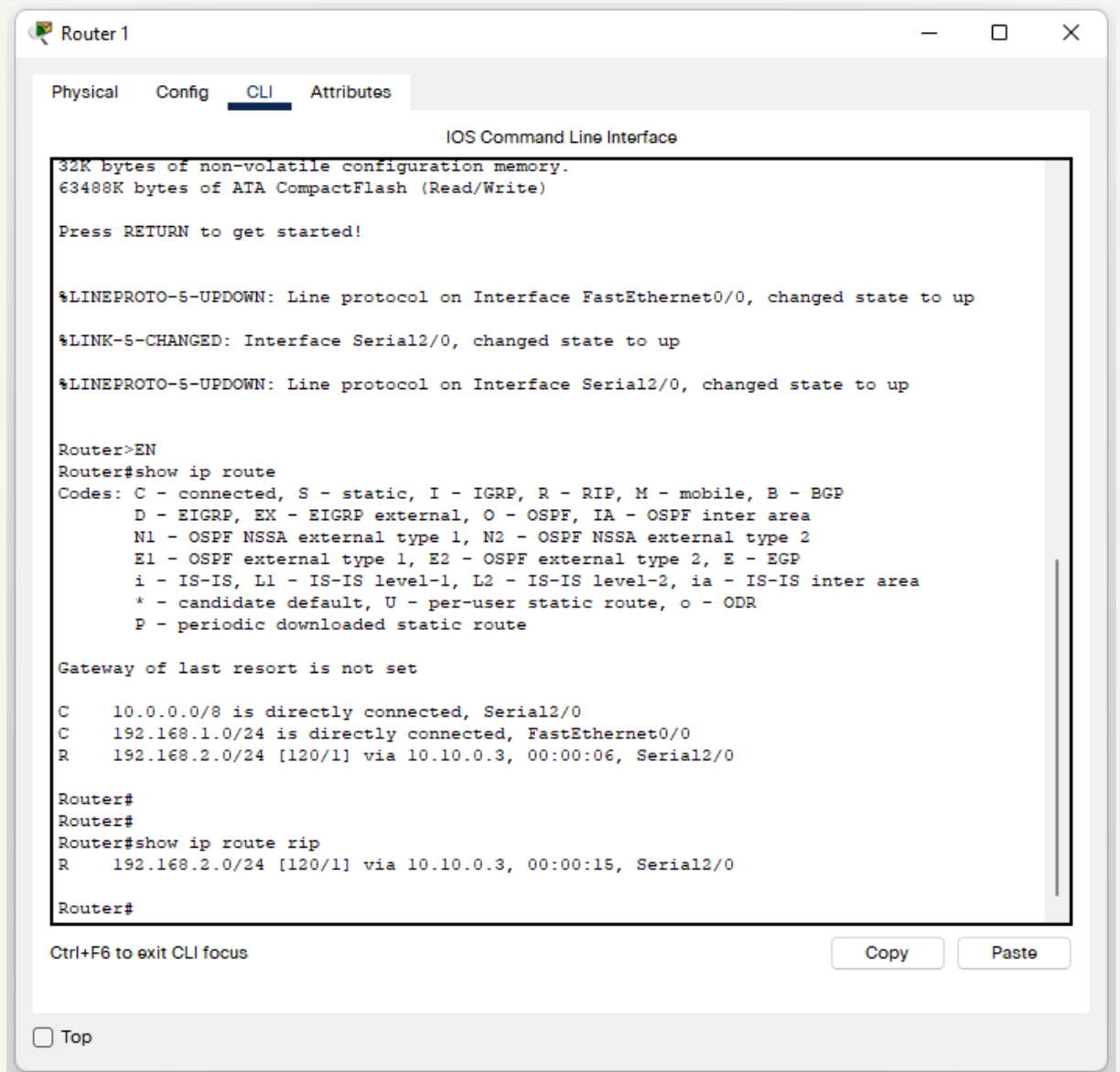


Figure 2.3: specifically display routes of Router 1 learnt through RIP.

Now let's Ping PC2 from PC1 to further confirm that connectivity is really established between the two subnets.

6. Connection test across PCs

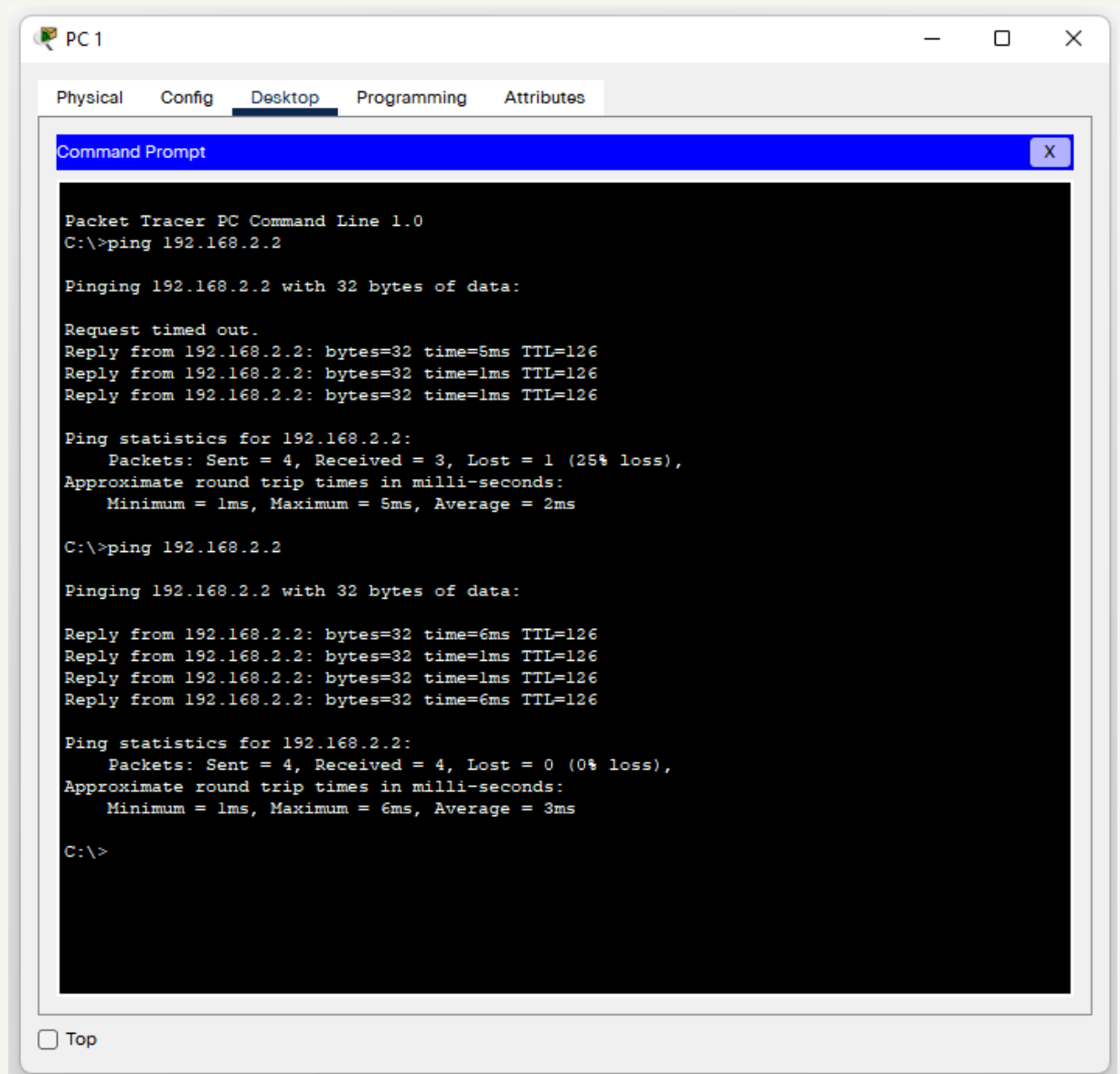
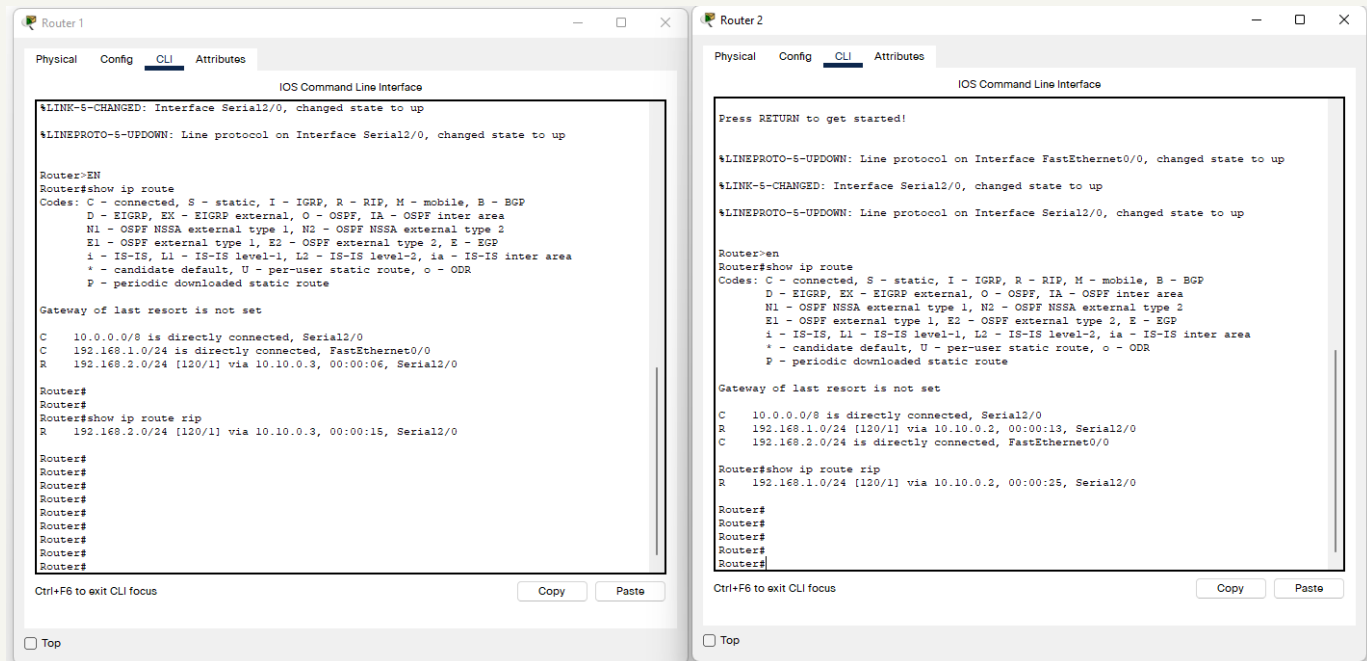


Figure 2.4: Ping PC2 from PC1.

Result:



The image displays two side-by-side screenshots of Cisco IOS Command Line Interface (CLI) windows, labeled Router 1 and Router 2. Both windows show the output of the 'show ip route' command, which lists the IP routes learned through RIP. The output includes the status of the interface (up/down), the protocol (RIP), and the specific IP addresses and metrics (metric, interface) for each route. The Router 1 window shows routes for 10.0.0.0/8, 192.168.1.0/24, and 192.168.2.0/24. The Router 2 window shows routes for 10.0.0.0/8, 192.168.1.0/24, and 192.168.2.0/24. The Router 2 window also shows a message about the line protocol on Interface FastEthernet0/0 being up.

```
Router 1
Physical Config CLI Attributes
IOS Command Line Interface
%LINK-5-CHANGED: Interface Serial2/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
Router>EN
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - 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
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, Serial2/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
R    192.168.2.0/24 [120/1] via 10.10.0.3, 00:00:06, Serial2/0

Router#
Router#
Router#show ip route rip
R    192.168.2.0/24 [120/1] via 10.10.0.3, 00:00:15, Serial2/0
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#

Ctrl+F6 to exit CLI focus
Copy Paste
Top

Router 2
Physical Config CLI Attributes
IOS Command Line Interface
Press RETURN to get started!
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface Serial2/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
Router>en
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - 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
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, Serial2/0
R    192.168.1.0/24 [120/1] via 10.10.0.2, 00:00:13, Serial2/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0

Router#show ip route rip
R    192.168.1.0/24 [120/1] via 10.10.0.2, 00:00:25, Serial2/0
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#

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

Figure 2.5: Output of the display routes learnt through RIP.

Conclusion:

My achievement is to implement RIPv2. RIPv2 is remarkably simple to implement once there are basic classful subnetting skills and enough knowledge of the participating networks. If a network is simple and does not involve different classes of IP address and contains not more than fifteen hop counts, then RIP is the appropriate choice.

Report No: 03

Report Title: Wireless LAN configuration using Cisco Packet Tracer.

Objectives:

- To learn how to create a Wireless LAN configuration in PT
- To learn how to configure a Wireless LAN configuration using command mode

Discussion:

Wireless Local Area Networks (WLAN) have become immensely popular because they are extremely easy to setup and use and have minimal maintenance cost. One or more access points (APs) can cover a building or an area. A WLAN is not completely wireless because the servers in the backbone are fixed.

The WLAN solution allows we to provide the following wireless LAN services to our customers:

- WLAN client connectivity to conventional 802.3 LANs
- Secured WLAN access with different authentication and encryption methods
- Seamless roaming of WLAN clients in the mobility domain

Methodology of my project:

- Create a New Project.
- Create the Wireless LAN configuration.
- Place Wireless Interface Card to Laptops
- IP Check on WLAN Devices
- DHCP Server Configuration
- IP Check on WLAN Devices again
- Analysis of the Results.

Working Procedure:

1. Network diagram

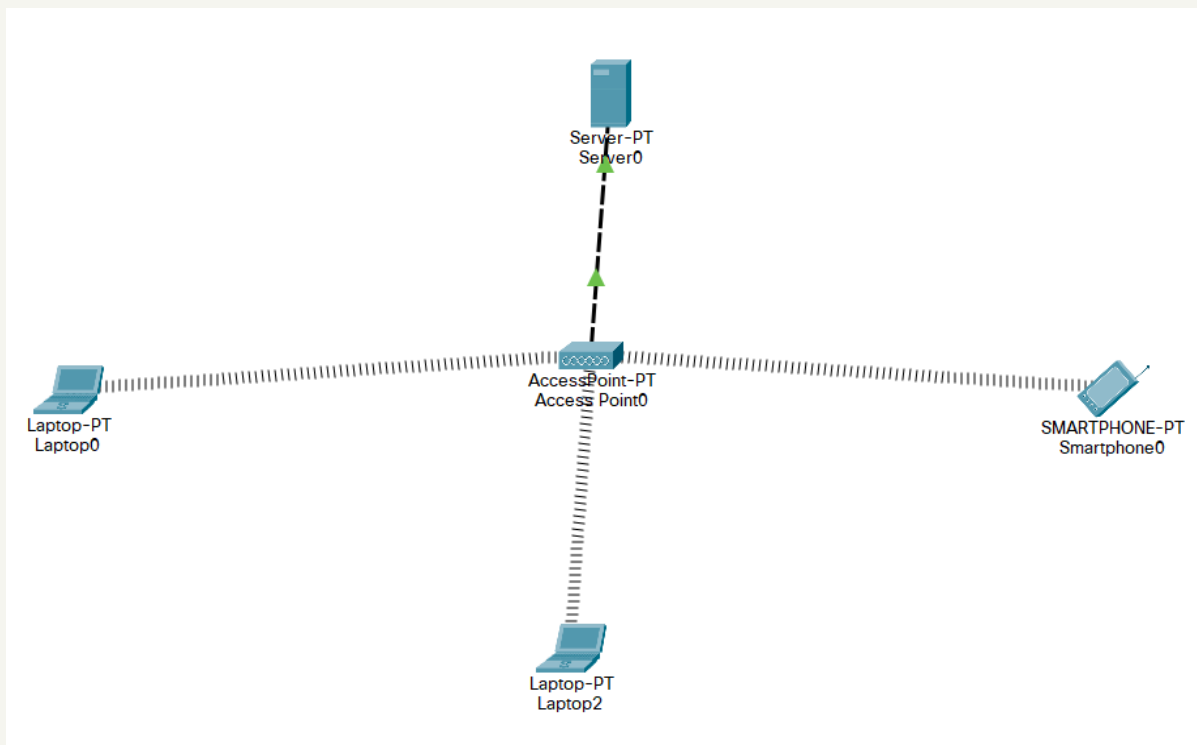


Figure 3.1: Wireless LAN configuration.

2. Place Wireless Interface Card to Laptops

By default, laptops have classic Ethernet cards. To be involved in a wireless network, we should have a wireless interface card. So, in each laptop, we should turn off the laptop, remove the classical Ethernet, instead of it we place Wireless Interface Card (WPC300N). Then, we power on the laptop again.

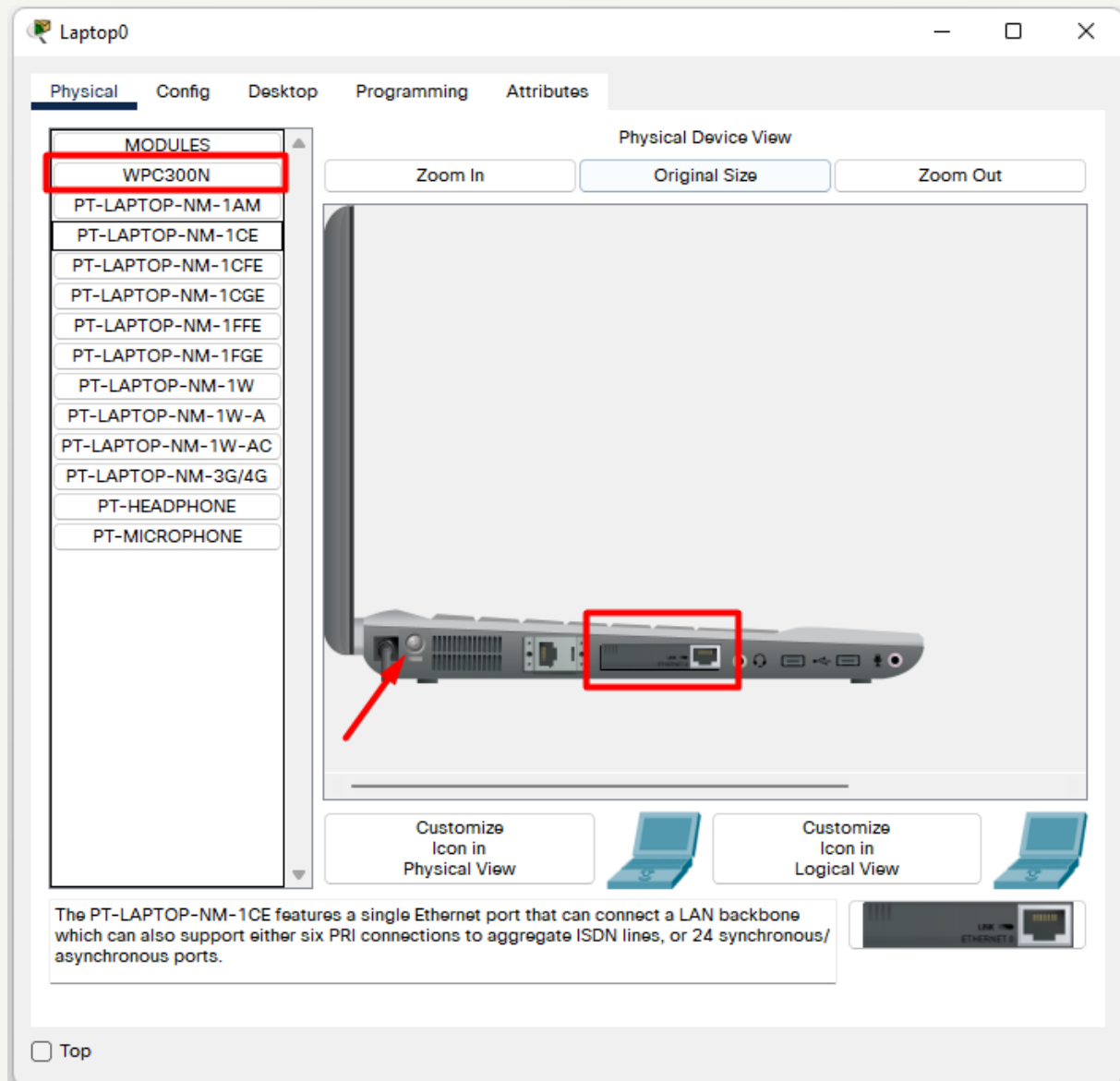


Figure 3.2: By default laptops have classic Ethernet cards.

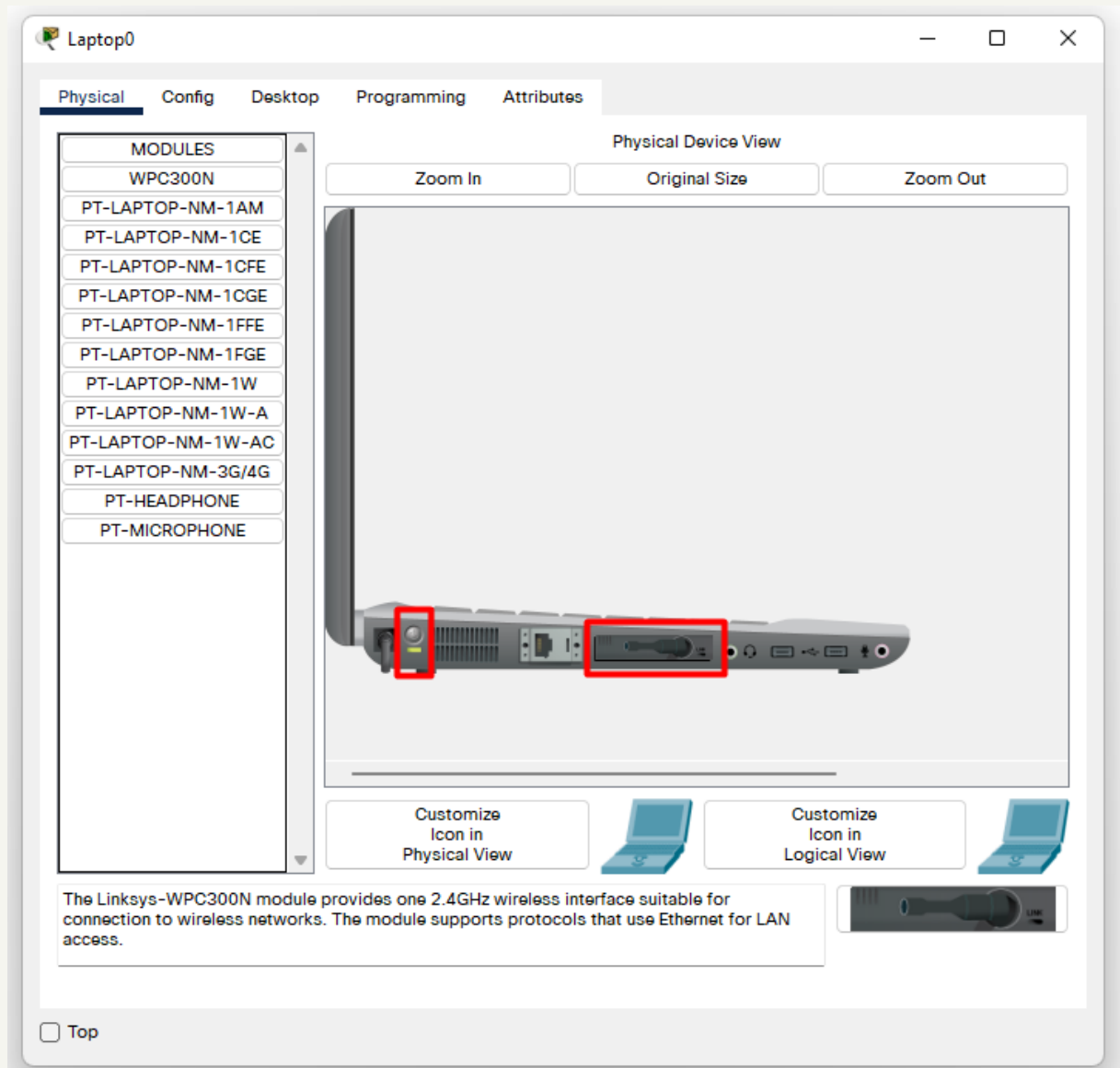


Figure 3.3: Placing Wireless Interface Card to Laptops.

After this process each laptop connects to the wireless Access Point in Packet Tracer. Smartphone devices in Packet Tracer connect to Access Points (AP) by default. So, there is nothing to do on them.

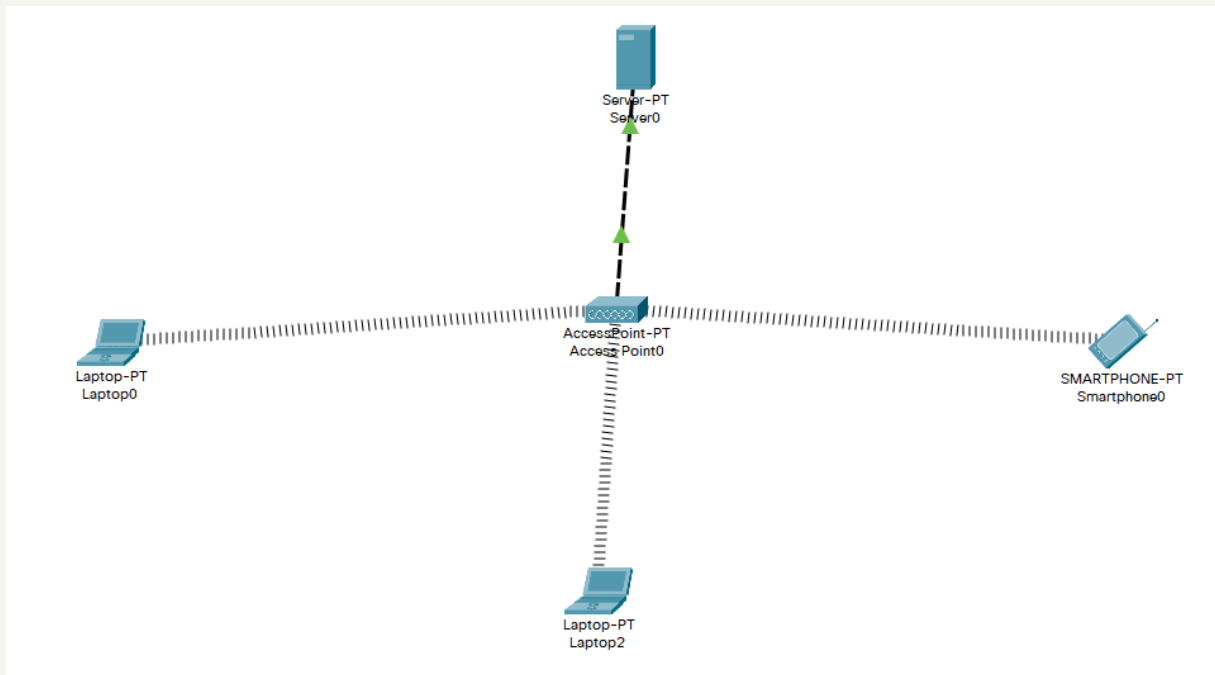


Figure 3.4: wireless connections to the wireless Access Point.

3. IP Check on WLAN Devices

We will check the IP addresses of the laptops. For now, checking only one of them is enough. Because, at the beginning if there is no Static IP Configuration and no DHCP, an IP from a special block is assigned to the devices. This is APIPA (Automatic Private IP Addressing) addresses. These addresses are from the block “169.254.x.x/25”. Simple, when we say this type of IP address in a device, we can say that it has no IP address.

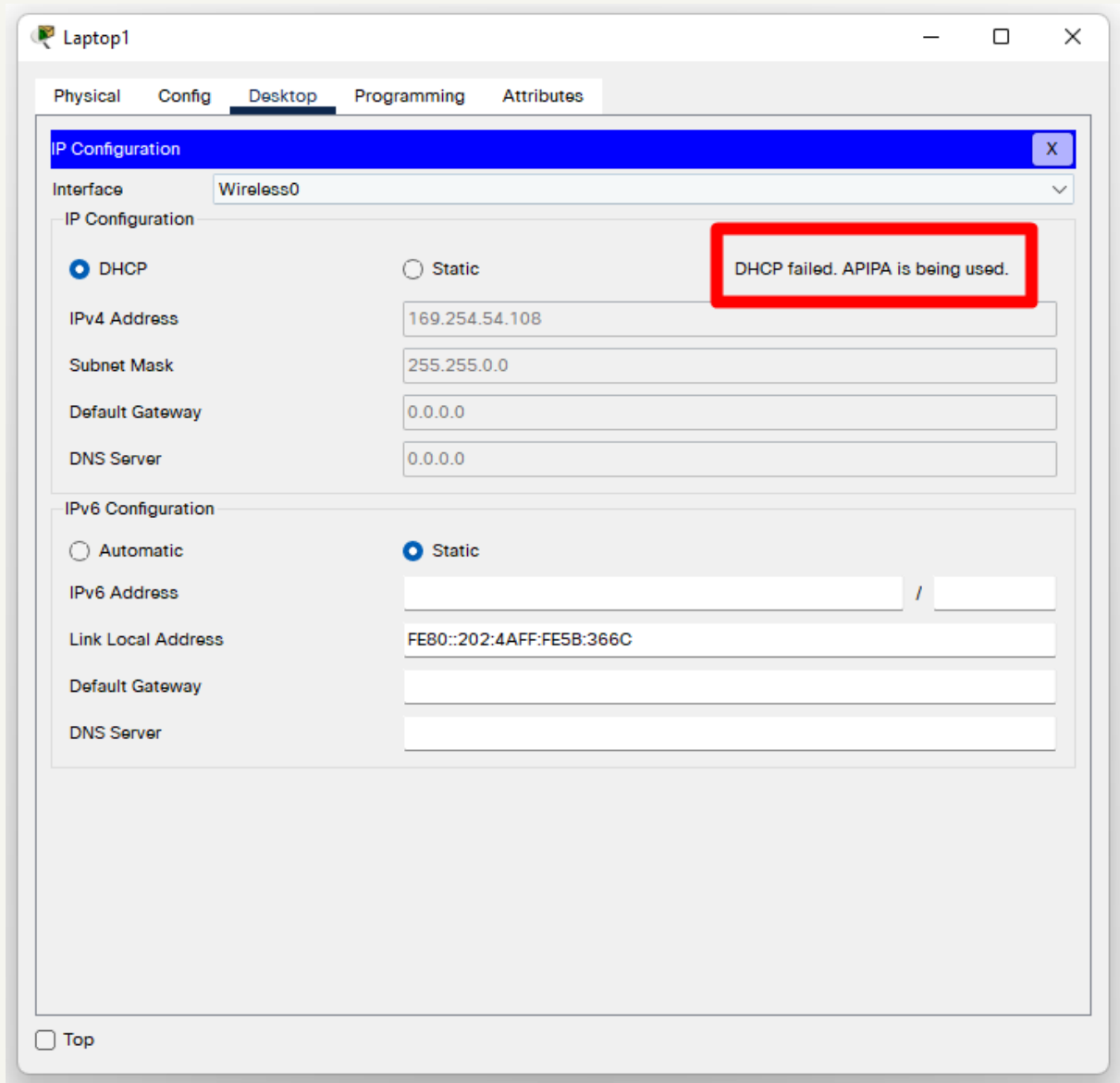


Figure 3.5: DHCP failed on node devices.

4. DHCP Server Configuration

In this step, we will configure our DHCP Server in the WLAN. This server will give IP addresses to our devices who are connected to the Access Point.

In the Services tab of Server, we will go through the DHCP at the left hand. Besides, we will configure the Default Gateway, DNS Server IP addresses. After that we will configure the starting IP and Subnet Mask. DHCP server will start IP assignation with this IP. And for this example,

we have created 254 IP for our IP Pool. We also assign this value on this screen.

After this configuration, we should not forget to “on” our DHCP Service at the top and then, we add our DHCP Pool to the configuration with the “add” button.

Server0

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 172.16.0.1

DNS Server: 172.16.0.1

Start IP Address: 172.16.0.0

Subnet Mask: 255.255.0.0

Maximum Number of Users: 254

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	172.16....	172.16....	172.16....	255.255...	254	0.0.0.0	0.0.0.0

☐ Top

Figure 3.6: configuring DHCP Server.

After DHCP Services configuration on DHCP Server, we will configure one more thing on this DHCP Server. This is the IP address and subnet mask of the Server. Here, our Server IP address will be 172.16.0.1 and the mask will be 255.255.255.0

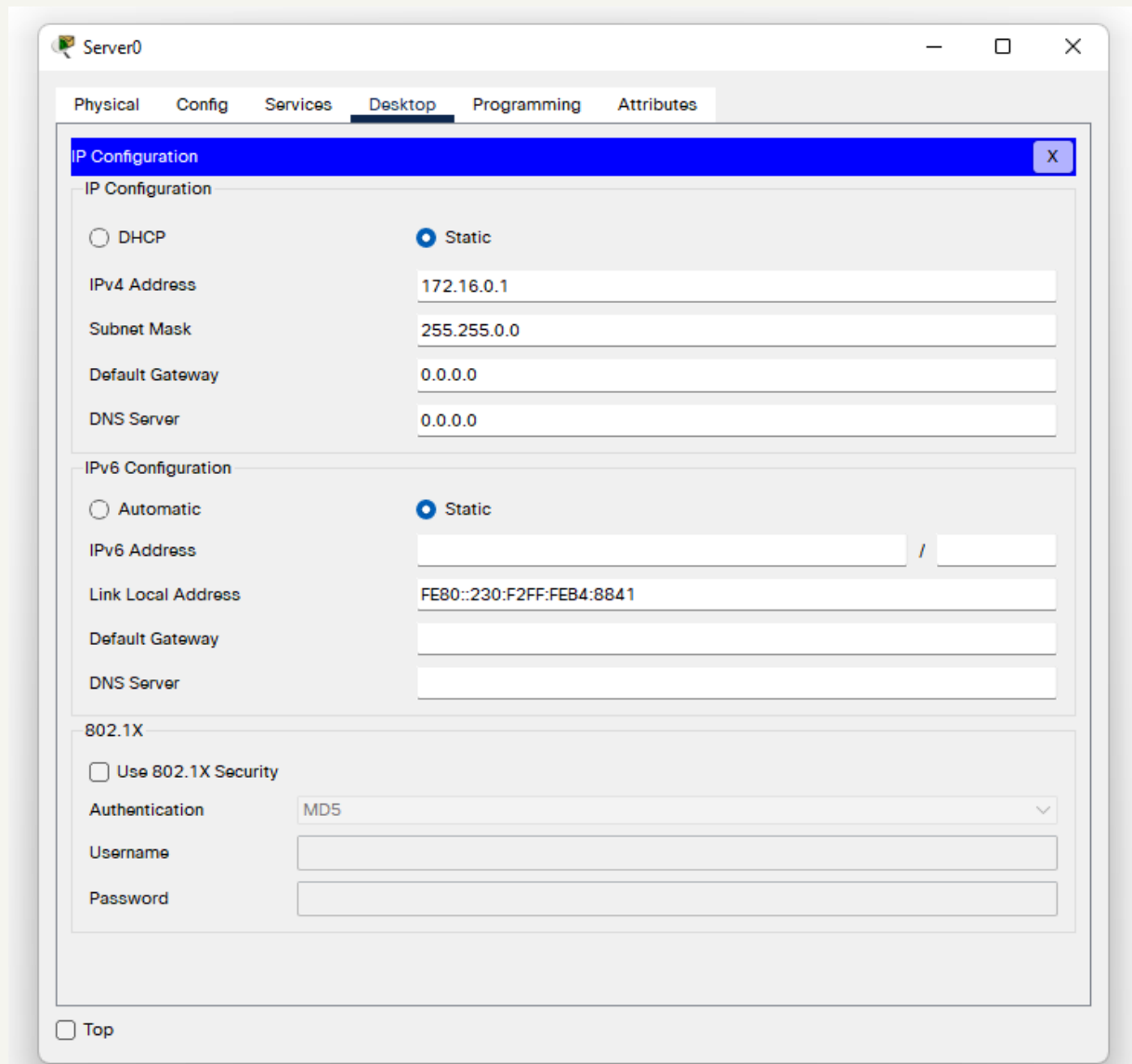


Figure 3.5: assigning DHCP Server's IP Address.

5. IP Check on WLAN Devices again

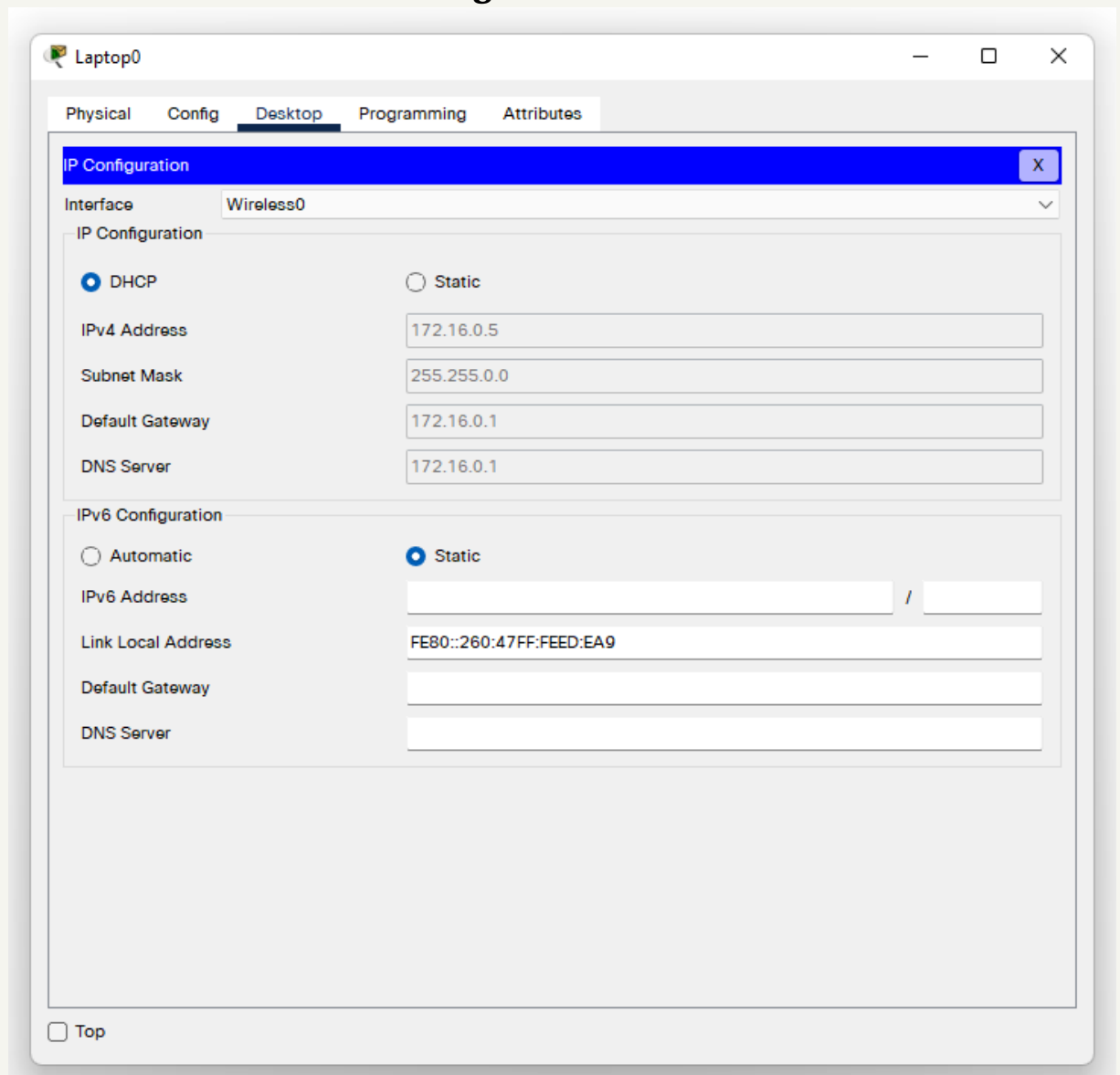


Figure 3.6: DHCP server is working now in node devices.

6. Connection test using simulation:

We have sent a message from Laptop0 to Smartphone0. and the message was sent successfully.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Laptop0	Smartphone0	ICMP		0.000	N	0	(edit)	

Figure 3.7: Connection test using simulation
Laptop0 to Smartphone0

Conclusion:

This network represents the Wireless LAN configuration using Cisco Packet Tracer.

Here we have also compared the Check the connection from Laptop0 to Smartphone0 by sending a simple message which was successfully sent & received.

Report No: 04

Report Title: Basic IOT Devices Simulation using Cisco Packet Tracer.

Objectives:

The main objectives behind Basic IOT Devices Simulation using Cisco packet tracer are:

- Allows to design complex networks
- Allows students to explore concepts IOE
- to explore IoT concepts
- Allows users to build, design, configure smart city, and smart home by providing a different intelligent object that uses them.
- Provides realistic visualization and simulation of IoT devices

Discussion:

IoT means "Internet of Things" that defines things and their connections to the Internet. The Internet of Things enables control of local and remote objects by consuming the integration of network technology. IoT connects devices around us as well as over the Internet and automates communications.

Groups of scientists and organizations have attempted to clarify the Internet of Things and define their proposed definition as "a world where material things are seamlessly integrated into the information network and where material things can become an active participant in the business process." With the emergence of life changing

On the Internet, the Internet of Things is expected to have an enormous impact on life.

Cisco packet tracer is a Cisco multi-platform simulation tool to allow learners to simulate networks. It also helps generate IoT reformatations. In our research work we used the latest version of cisco packet tracer. Fig 1 shows its interface.

Methodology of my project:

To implement smart home Used new released cisco packet tracer, which included different smart object used for home automation such as smart fan, smart window, smart door, smart light, smart garbage door, fire sprinkler, lawn sprinkler and different sensor included control this smart object and sensor, microcontroller (MCU-PT) and Home Gateway Used, since it provides programming environment for controlling smart object connected to it and provide controlling mechanisms by registering smart device to Home Gateway, respectively.

Working Procedure:

To implement a smart home using Cisco packet tracer I used different sensors, smart devices, and detectors to make it smarter. The following figure represents the home architecture that connected each other using wireless and wired medium.

1. Build the Smart home.

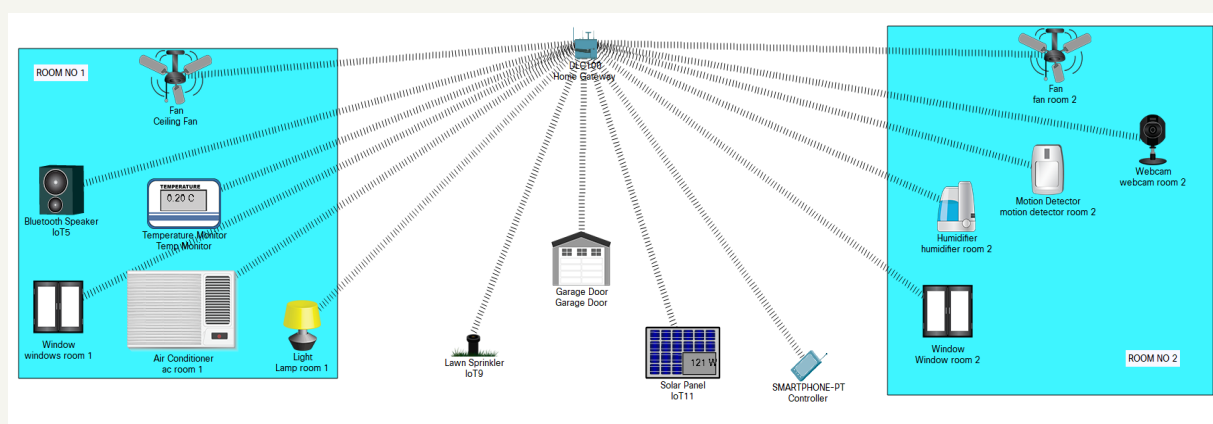


Figure 4.1: Smart Home Architecture.

2. Let's establish a wireless connection.

Go to Wireless devices and choose Home Gateway

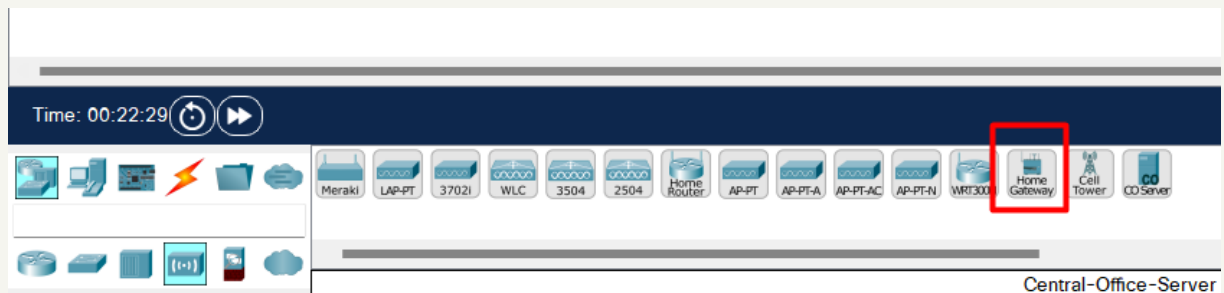


Figure 4.2: Home gateway selection.

3. Now copy the SSID of Home Gateway by clicking on the home gateway.

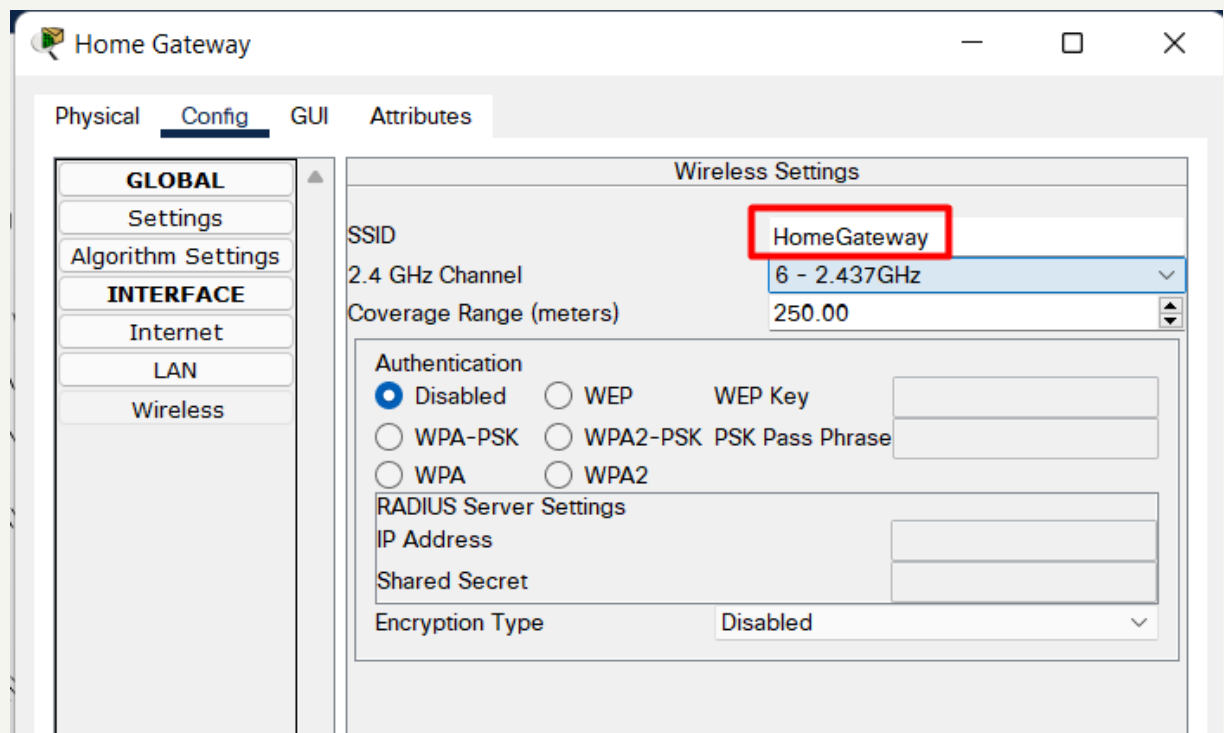


Figure 4.3: Copying the SSID of Home Gateway.

4. Therefore, It's necessary to configure all devices to connect wirelessly to Home Gateway.

Hence we can achieve this by right-clicking a **device-> Advanced->I/O config->select PT-IOT-NW-1W**. Similarly, repeat the steps for other devices as well.

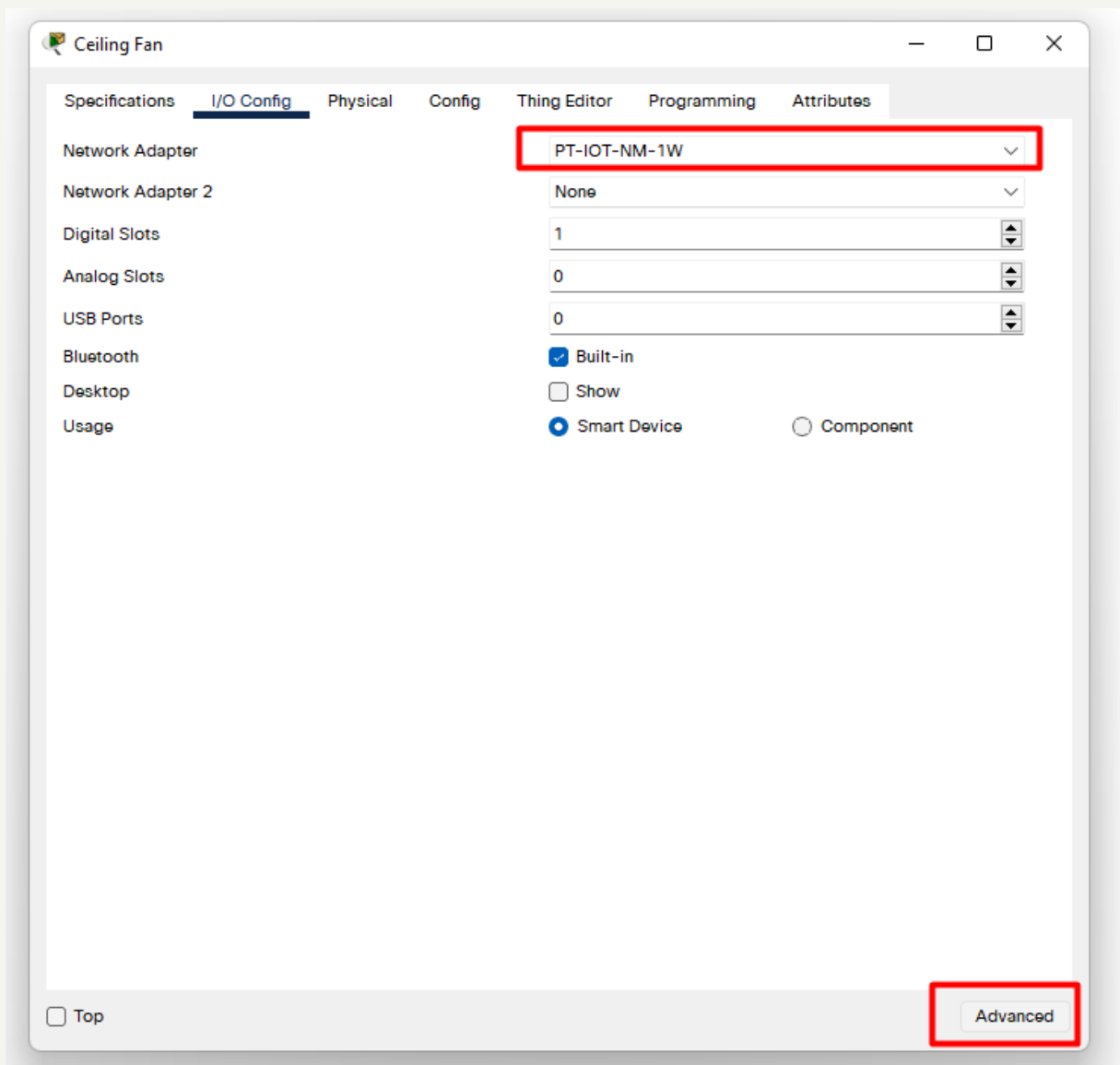


Figure 4.4: Connecting all devices wirelessly to Home Gateway.

5. Then paste the SSID In each appliance by clicking on the config option.

Similarly repeat the steps for other devices as well.

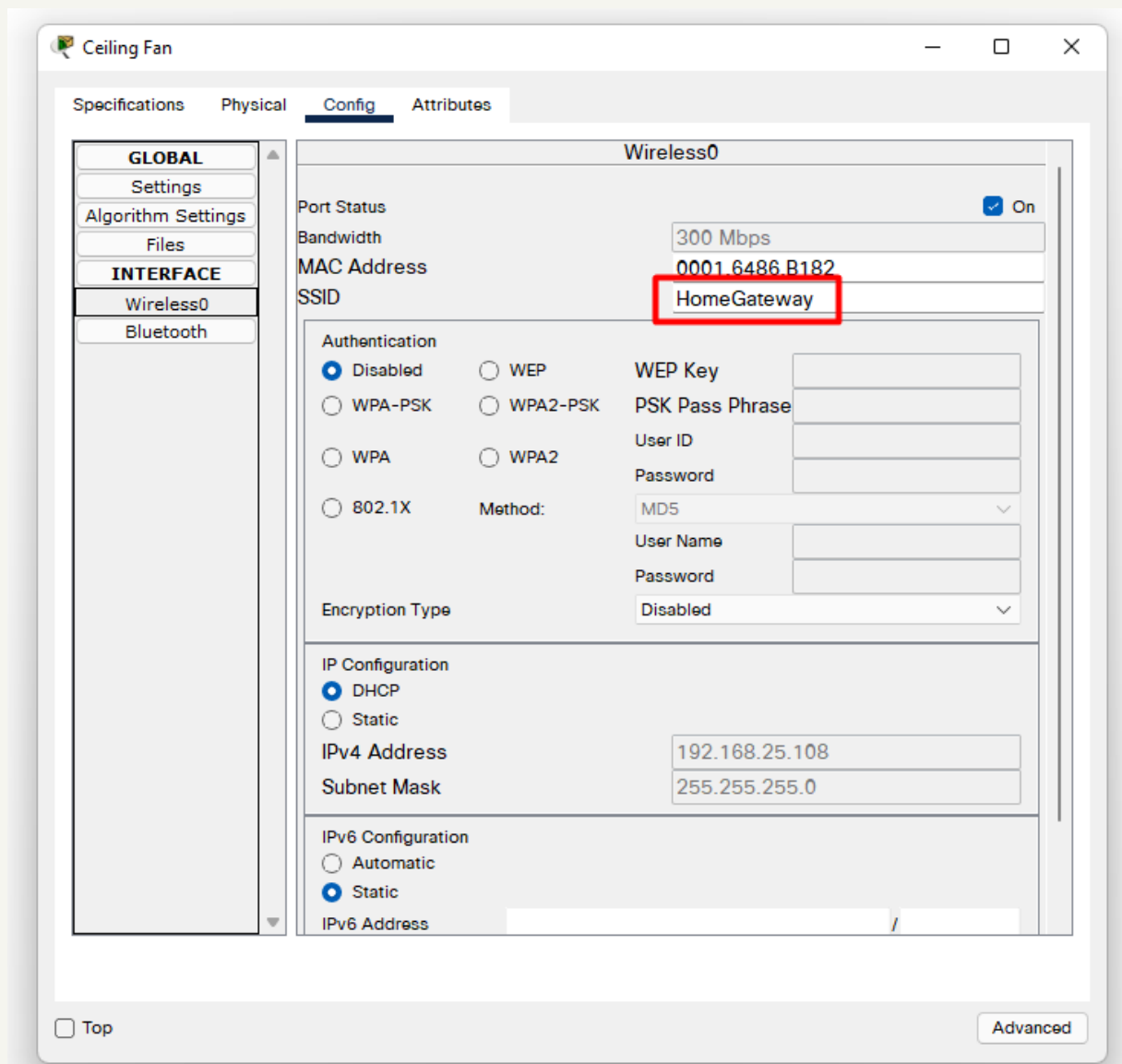


Figure 4.5: Connecting all devices wirelessly to Home Gateway.

6. Now let's select the IOT server as the home gateway to all appliances.

Click on **Appliances->select Advanced->config->choose Home Gateway**. Similarly repeat the steps for other devices as well.

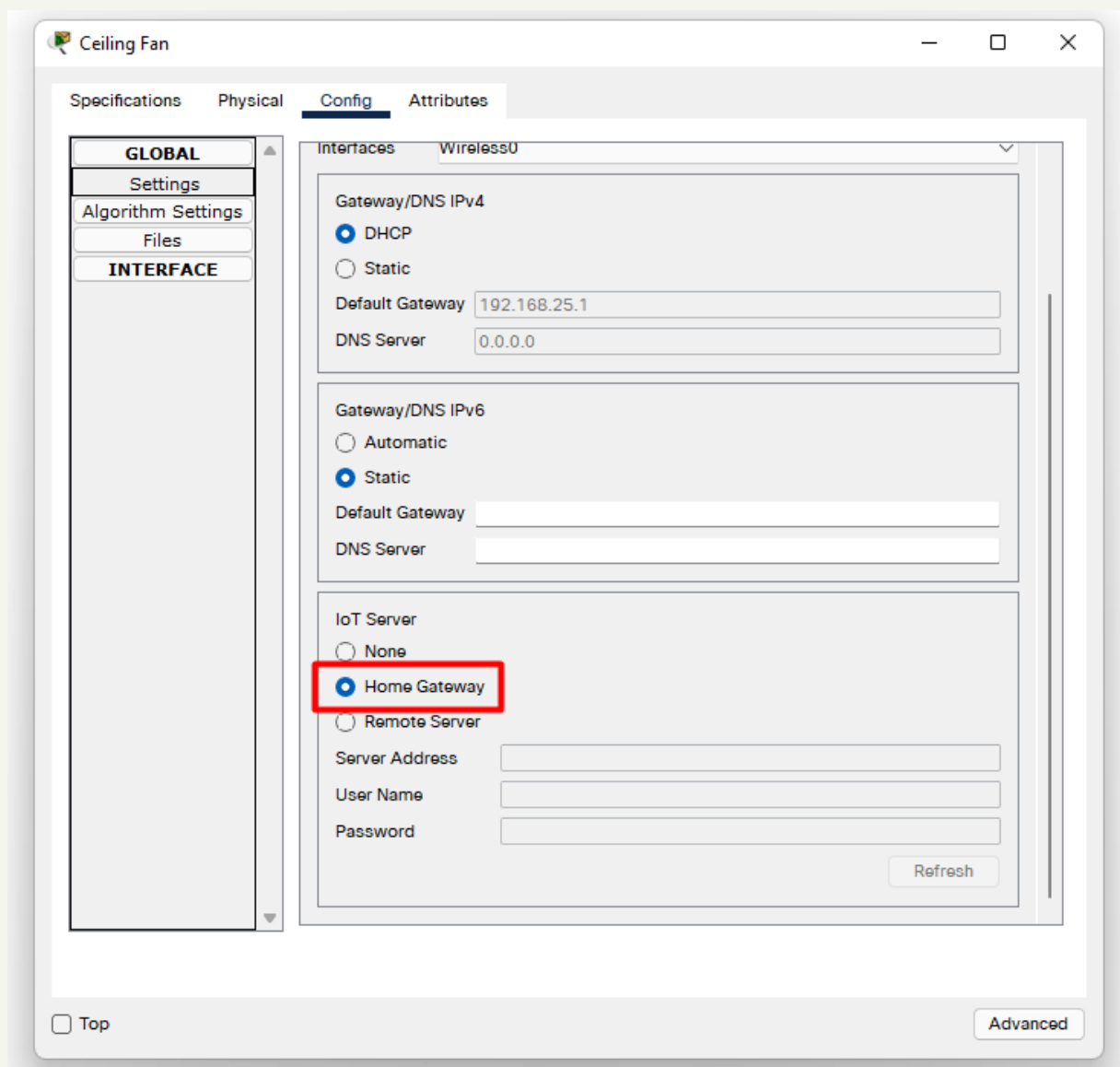


Figure 4.6: Selecting IOT server as home gateway to all appliances.

7. Thus, we can notice that all devices are connected to the Home Gateway

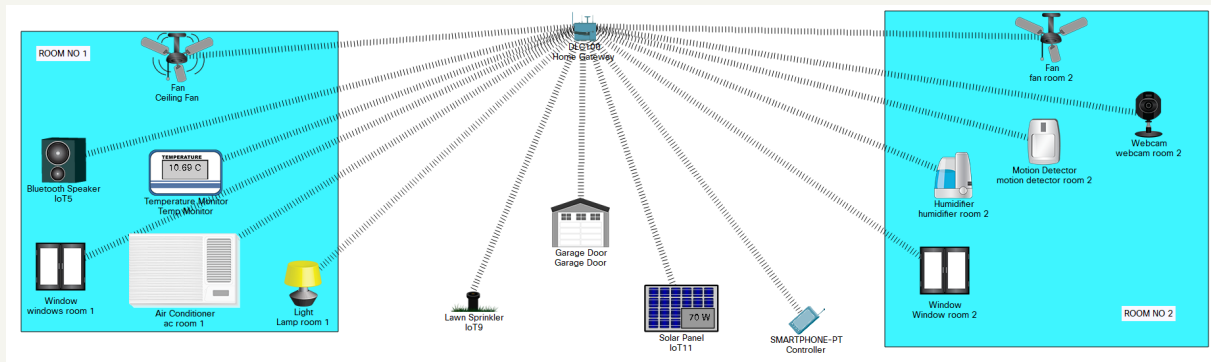


Figure 4.7: Establishment of collection with home gateway to all appliances.

8. Now select a smart device to Control and Monitor Appliances.



Figure 4.8: Selecting a smart device to Control and Monitor Appliances.

9. Now connect our smart device also to our home gateway

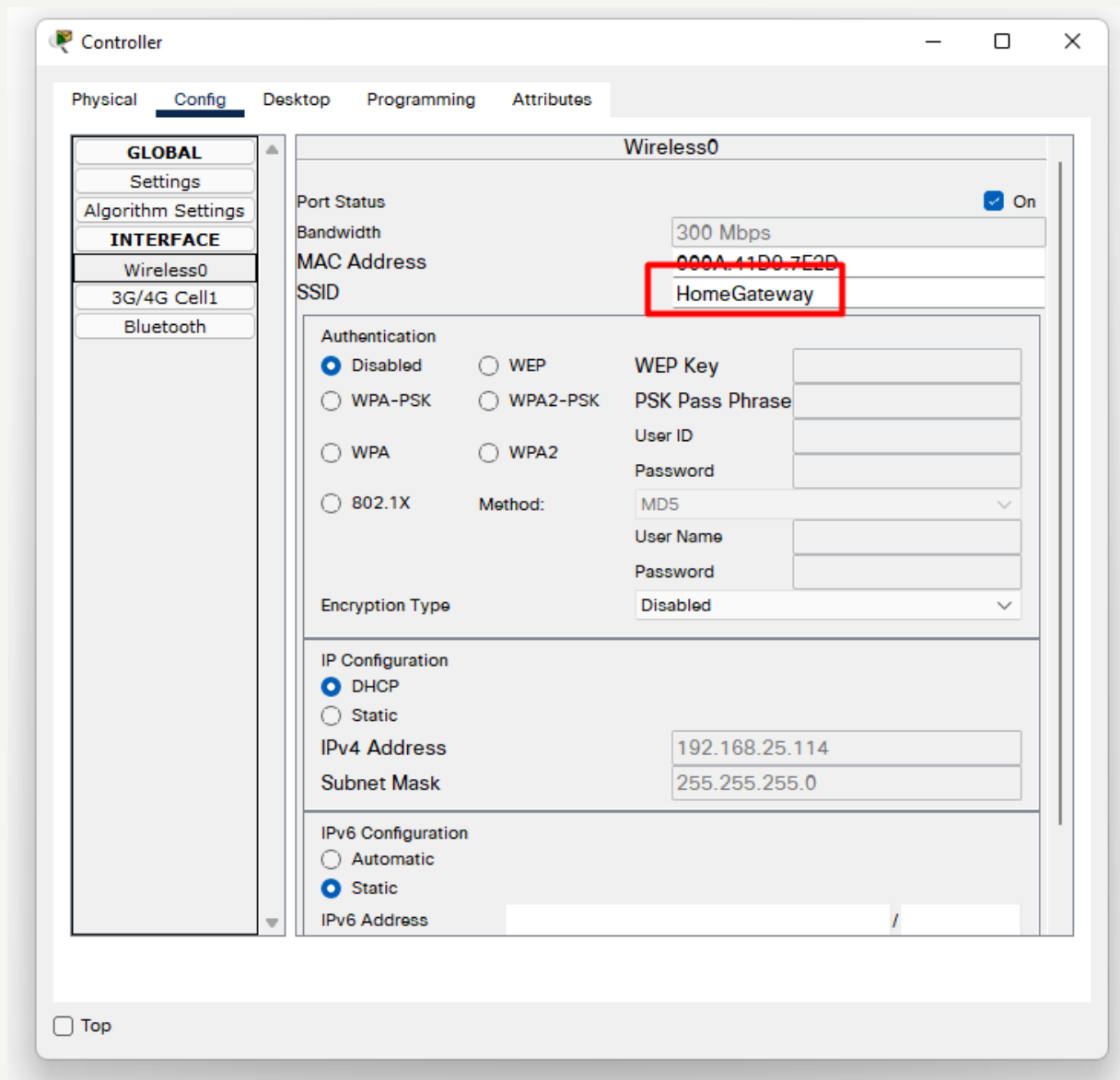


Figure 4.9: Connecting the smart device also to home gateway.

10. Thus, our smart device is connected to our Home Gateway.

Click on the smart device and choose Desktop. We can now login

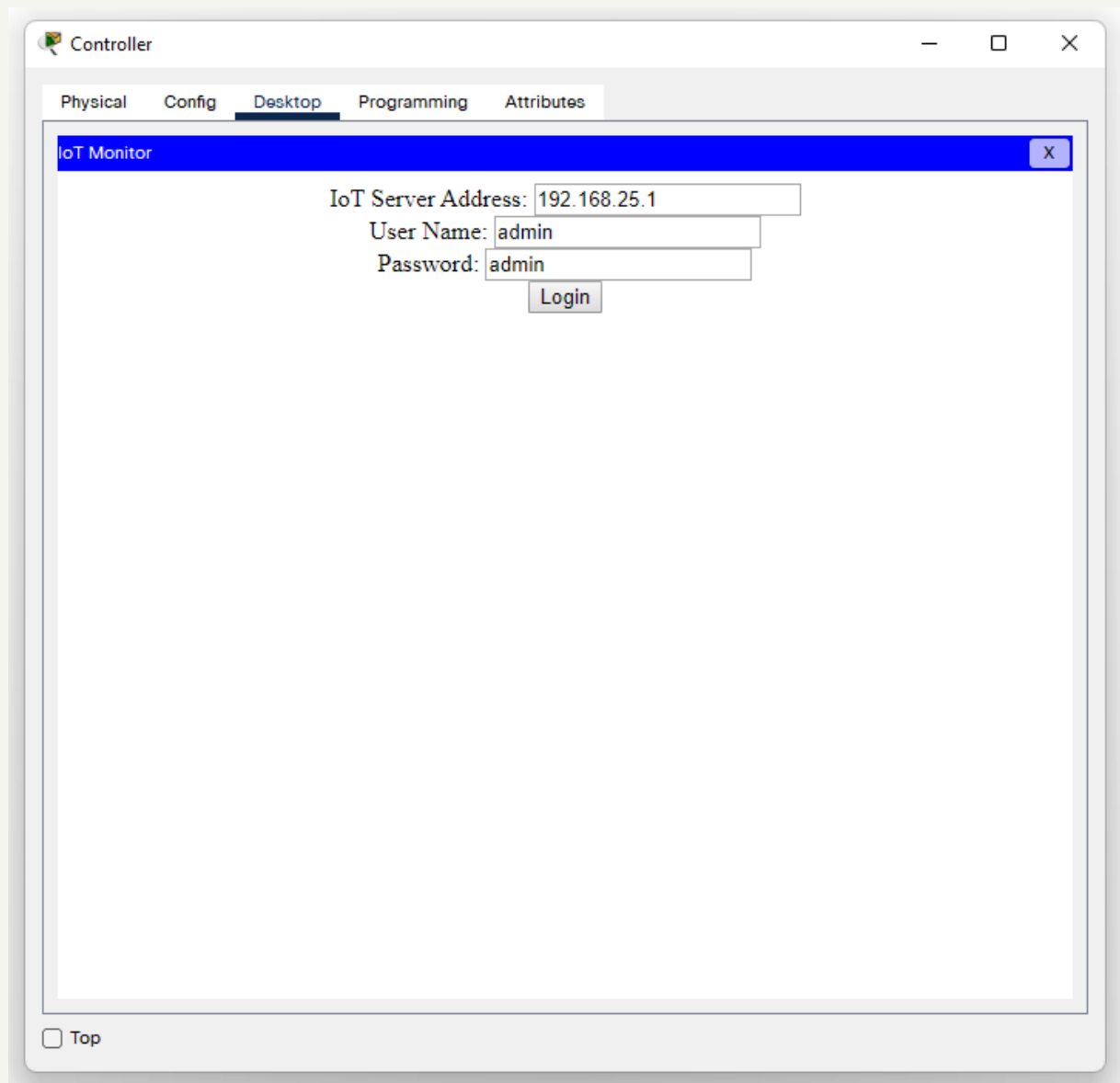


Figure 4.10: Entering Monitoring Dashboard.

11. Finally, We can control and Monitor in the Dashboard.

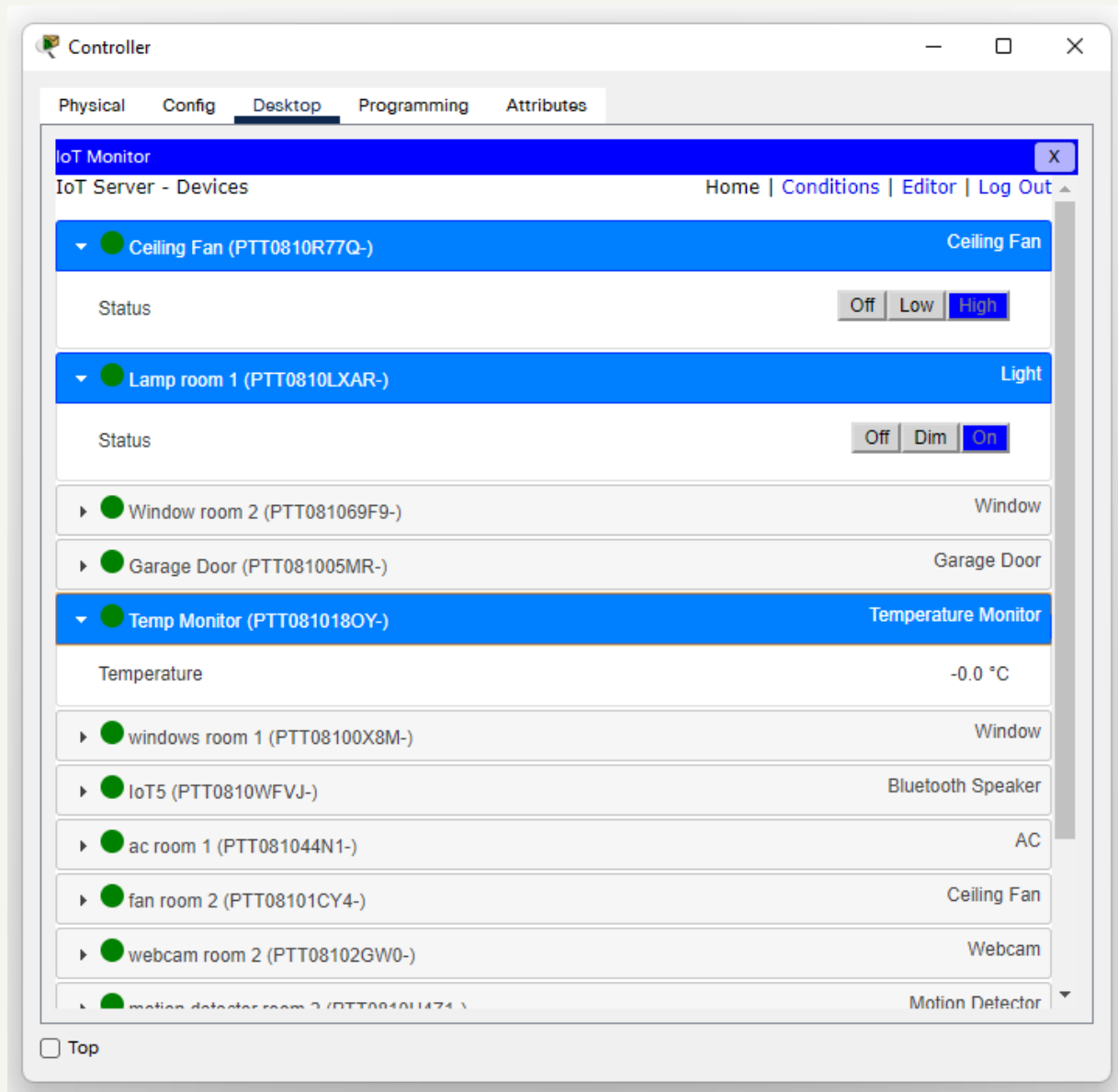


Figure 4.11: Monitoring smart appliances through Dashboard.

Result:

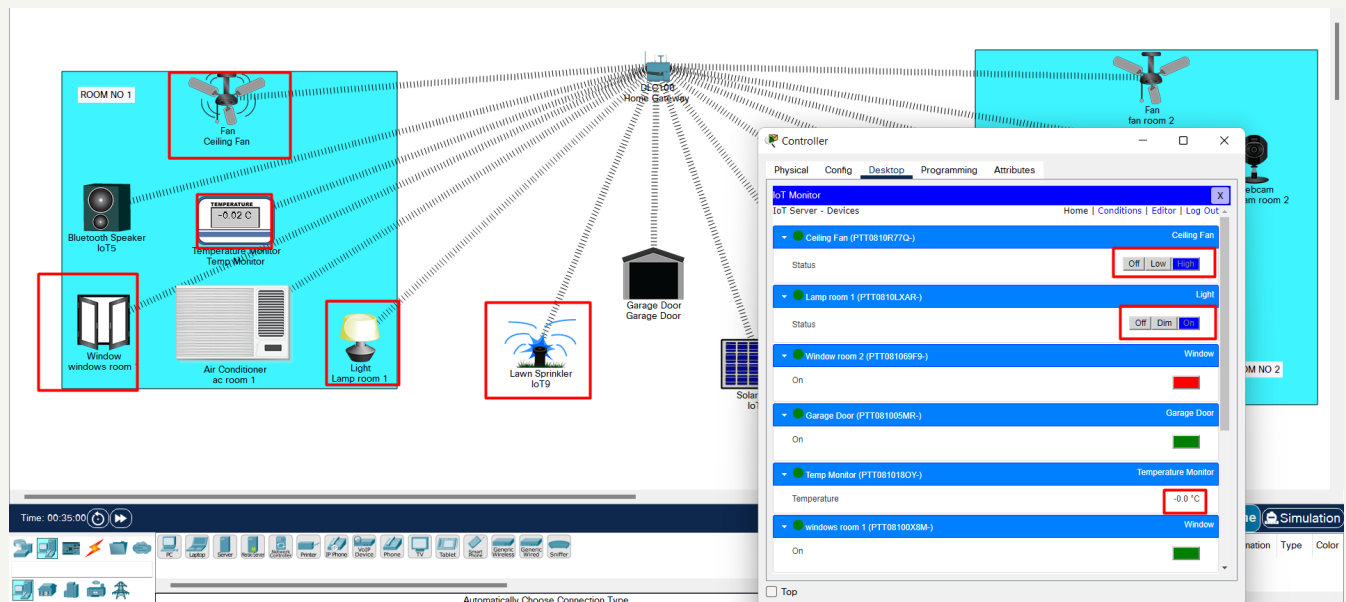


Figure 4.12: Final view of a complete smart home using IOT.

Conclusion:

In this report, I implemented a smart home using the newly released Cisco packet tracer, because this version included different IOE devices used for home automation. I used Home Gateway to register smart devices on it to control them and a Smartphone to interconnect different sensors and IOE devices. Also, Smartphones provide an environment to manage different devices, switch on & off, monitor temperature and so on. The technology innovation and the hike in smartphone usage was the motivation behind this work. The security measures are overly critical and IoT is providing a new and excellent concept to make our surroundings smarter.

Report No: 05

Report Title: Implementation of Basic IP phone configuration using Cisco Packet Tracer.

Objectives:

The main objectives behind Basic IP phone configuration using Cisco Packet Tracer are:

- To acquire knowledge about basic IP phone configuration.
- To learn about Cisco Packet Tracer.
- To implement the basic IP phone configuration using Cisco Packet Tracer.

Discussion:

Cisco IP Phones as full-featured telephones can plug directly into our IP network. We can use the Cisco Call Manager Administration phone configuration windows to configure the following Cisco IP Phones and devices such as Cisco IP Phone 7900 family (models 7960, 7940, 7935, 7910, and 7905), Cisco IP Phone model 30 VIP and H.323 clients etc.

Methodology of my project:

- Create a New Project.
- Create the basic IP phone configuration.
- Configuration of the Network Nodes.
- Choose the Statistics.
- Run the Simulation.
- Analysis of the Results.

Working Procedure:

Network diagram

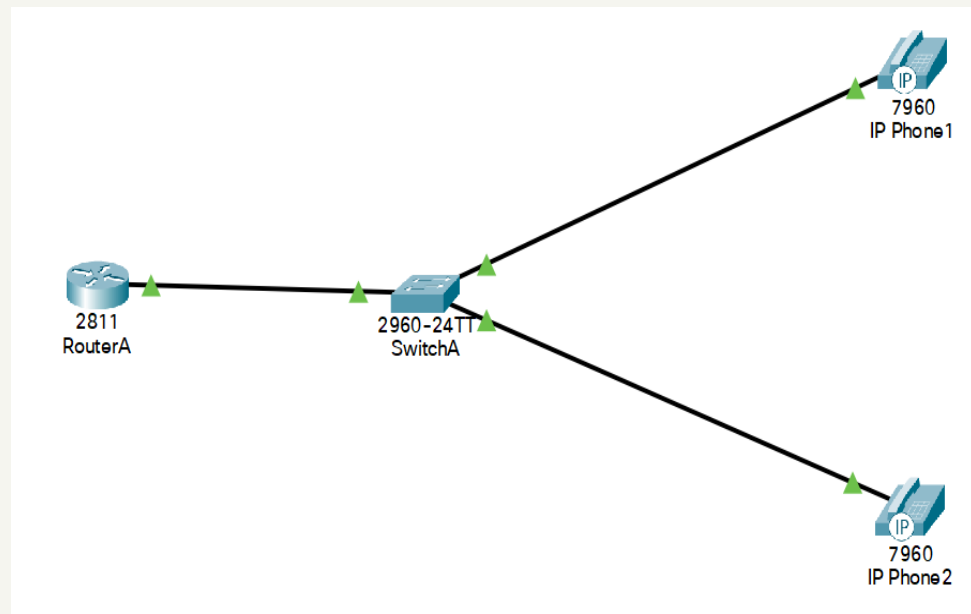


Figure 5.1: Architectural design of the basic IP phone configuration.

Tasks 1: Configuring RouterA (2811 router)

Configure the FastEthernet 0/0 interface with 192.168.10.1/24 ip address. Don't forget to enable the interface with the no shutdown command!

Command Line Interface (CLI) to configure Router:

```
Router>en
Router>enable
Router#configure terminal
Router(config)#interface f0/0
Router(config-if)#no shutdown
```

```
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#exit
Router(config)#ip dhcp pool PHONE
Router(dhcp-config)#network
Router(dhcp-config)#network 10.0.0.0 255.0.0.0
Router(dhcp-config)#default-router 10.0.0.1
Router(dhcp-config)#option 150 ip 10.0.0.1
Router(dhcp-config)#exit
```

Tasks 2 : Configure the Call Manager Express telephony service on RouterA

We must now configure the Call Manager Express telephony service on RouterA to enable VoIP on our network.

```
Router(config)#telephony-service
Router(config-telephony)#max-ephones 5
Router(config-telephony)#max-dn 5
Router(config-telephony)#ip source-address 10.0.0.1 port 2000
Router(config-telephony)#auto assign 4 to 6
Router(config-telephony)#auto assign 1 to 5
Router(config-telephony)#exit
```

Task 3: Configure the phone directory for IP Phone 1

Although 'IP Phone 1' is already connected to SwitchA, it needs additional configuration before being able to communicate. we need to configure RouterA to assign a phone number to this IP phone.

```
Router(config)#ephone-dn 1
Router(config-ephone-dn)#ephone-dn 1
Router(config-ephone-dn)#number 0002
Router(config-ephone-dn)#exit
```

Task 4: Configure the phone directory for IP Phone 2

Connect IP Phone 2 to SwitchA and power the phone ON using the power adapter (Physical tab).

```
Router(config)#ephone-dn 2
Router(config-ephone-dn)#ephone-dn 2
Router(config-ephone-dn)#number 0003
Router(config-ephone-dn)#exit
```

Task 5: Configure a voice vlan on SwitchA

Apply the following configuration on SwitchA interfaces. This configuration will separate voice and data traffic in different vlans on SwitchA. data packets will be carried on the access vlan.

Command Line Interface (CLI) to configure Switch:

```
Switch>enable
Switch#configure terminal
Switch(config)#interface range f0/1 - 24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport voice vlan 1
```

Task 5: Verify the configuration

Ensure that the IP Phone receives an IP Address and the phone number 54001 from RouterA (this can take a short while).

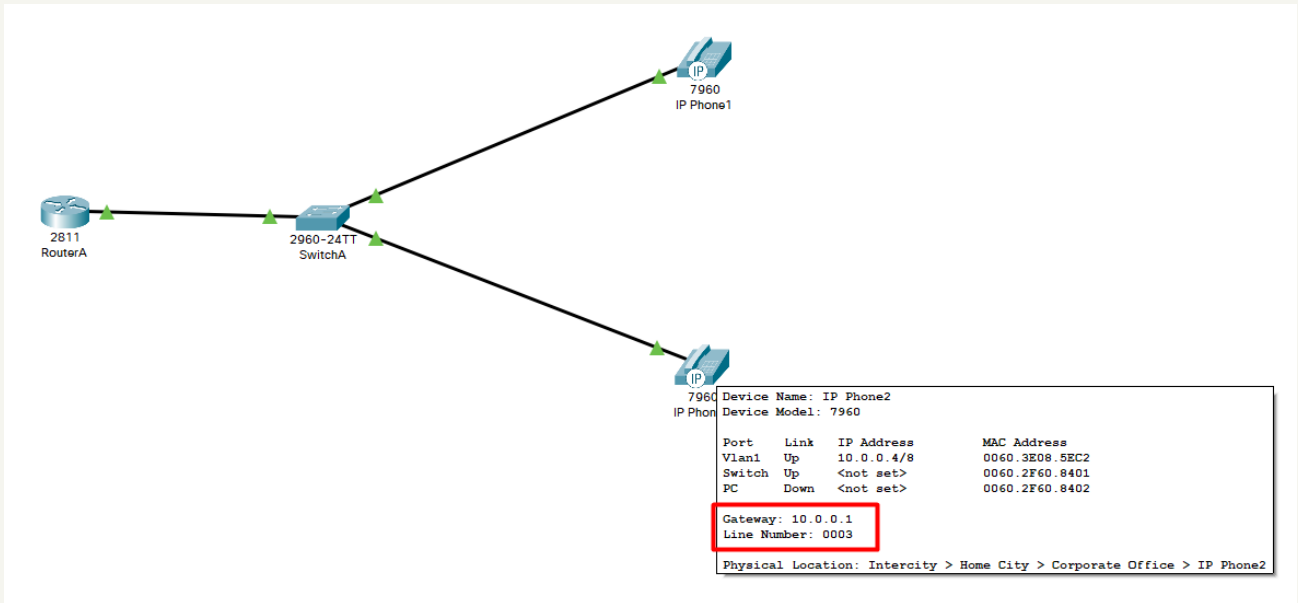


Figure 5.2: Verification of the configuration.

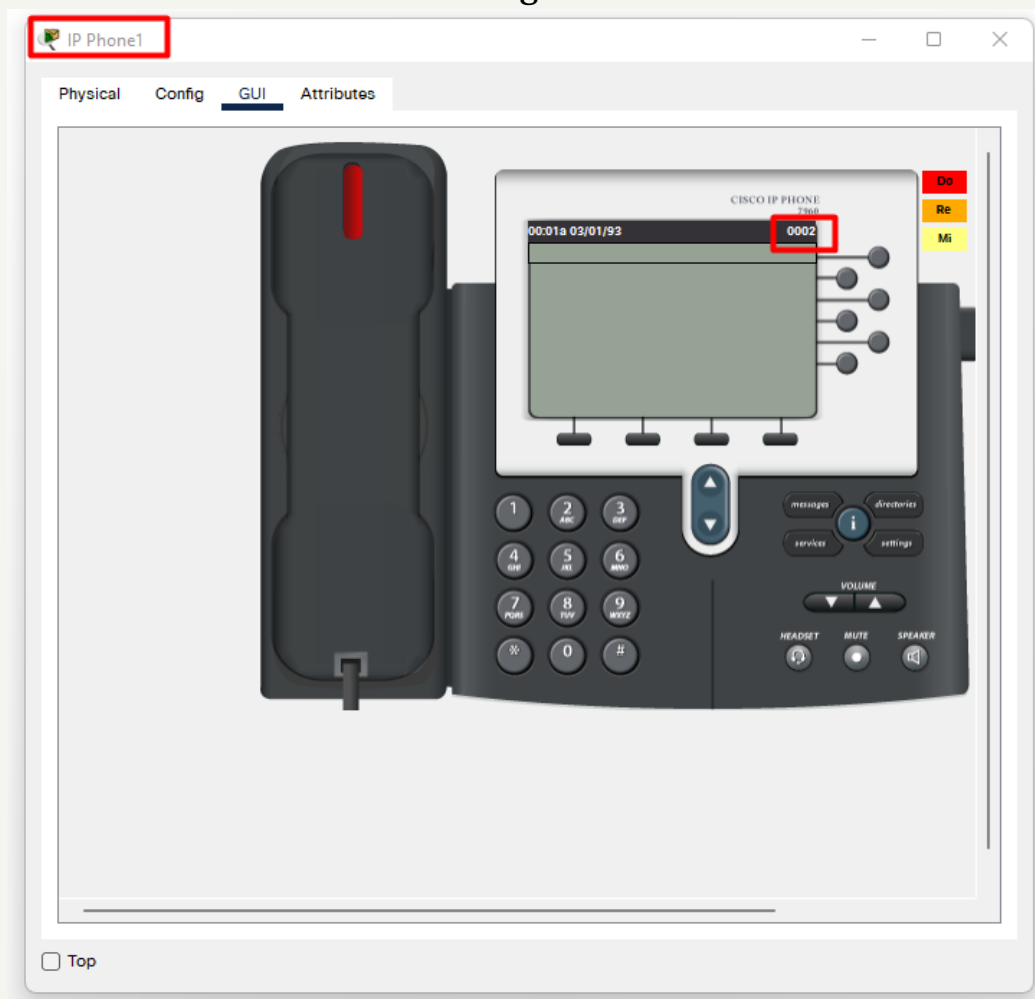


Figure 5.3: IP Phone 1: establishment of connection.

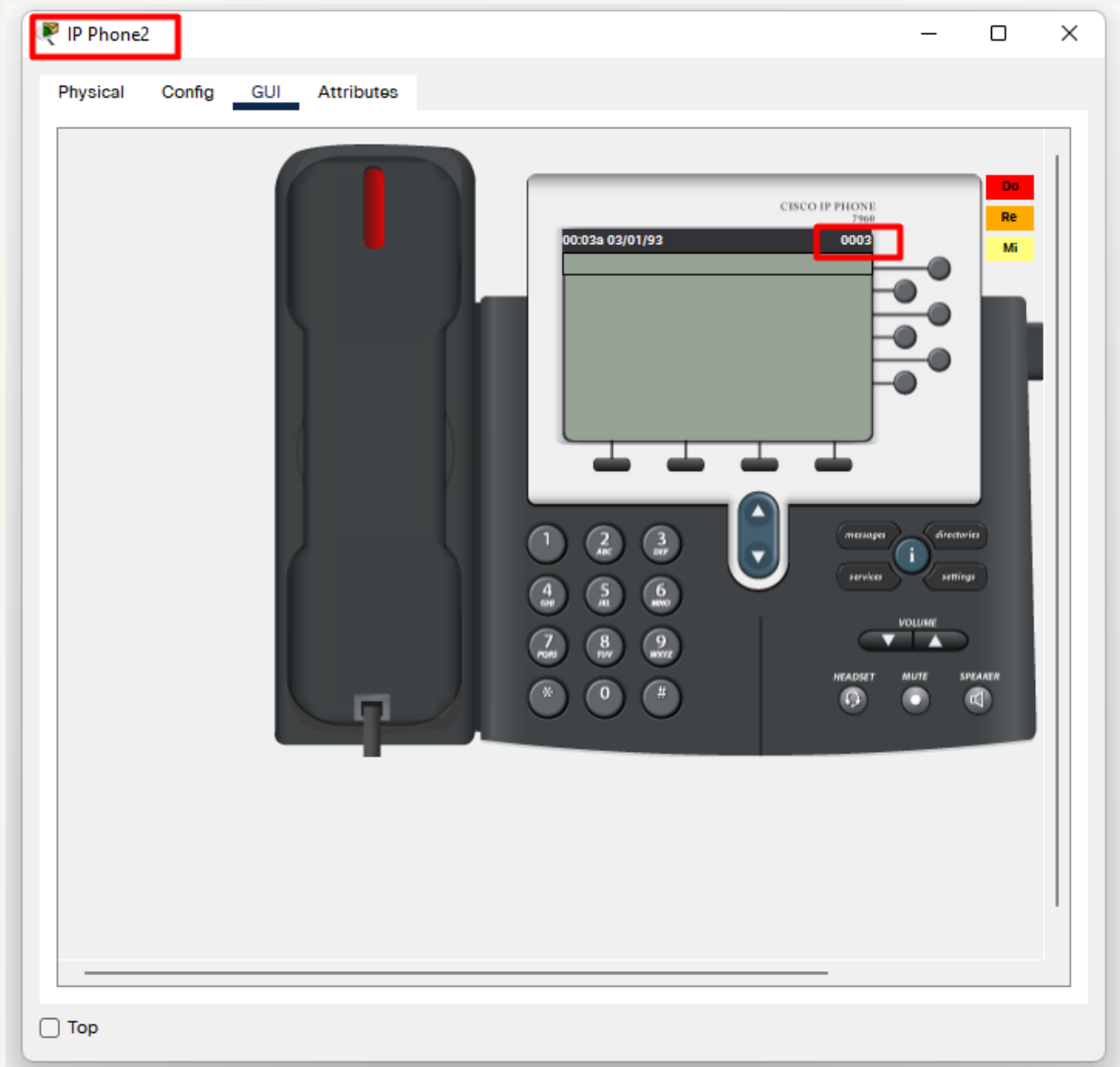


Figure 5.4: IP Phone 2: establishment of connection.

Task 7: Verify the configuration

From IP phone 2 Dial 002 and check if IP phone 1 correctly receives the call.

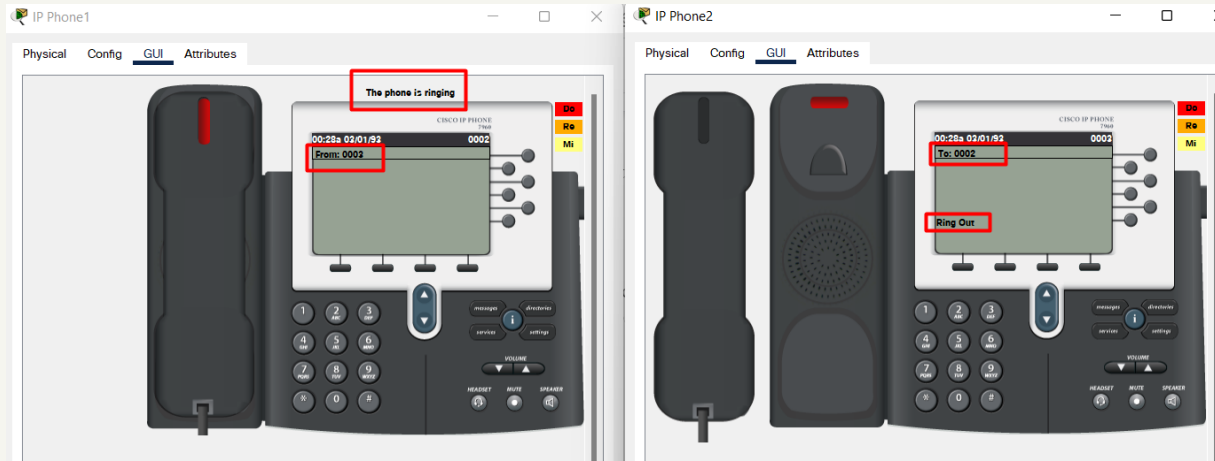


Figure 5.5: IP Phone 1 receives a call from IP Phone 2.

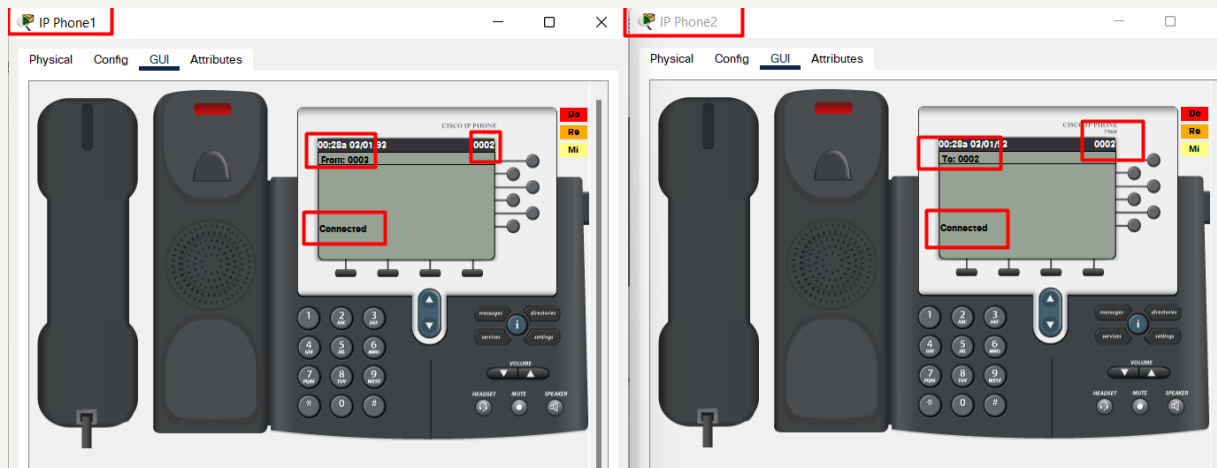


Figure 5.5: IP Phone 1 is now connected with IP Phone 2.

Conclusion:

This network analyzes the performance of the basic IP phone configuration. Here we have also compared the pretending result to gain the best performance of the basic IP phone configuration.

Report No: 06

Report Title: Configuration of TELNET using Cisco packet Tracer

Objectives:

The main objectives behind TELNET implementation using Cisco packet tracer are:

- To acquire knowledge about TELNET.
- To learn about Cisco Packet Tracer.
- To implement the TELNET using Cisco Packet Tracer.

Discussion:

Telnet is an application layer protocol that allows a network administrator to access and manage remote devices. A user on a client machine can use a software (also known as a Telnet client) to access a command-line interface of another, remote machine that is running a Telnet server program.

A network administrator can access the device by telnetting to the IP address or hostname of a remote device. The network administrator will then be presented with a virtual terminal that can interact with the remote host.

Methodology of my project:

- Create a New Project.
- Configuring Telnet.
- Configuration of the Network Nodes.
- Choose the Statistics.
- Run the Simulation.
- Analysis of the Results.

Working Procedure:

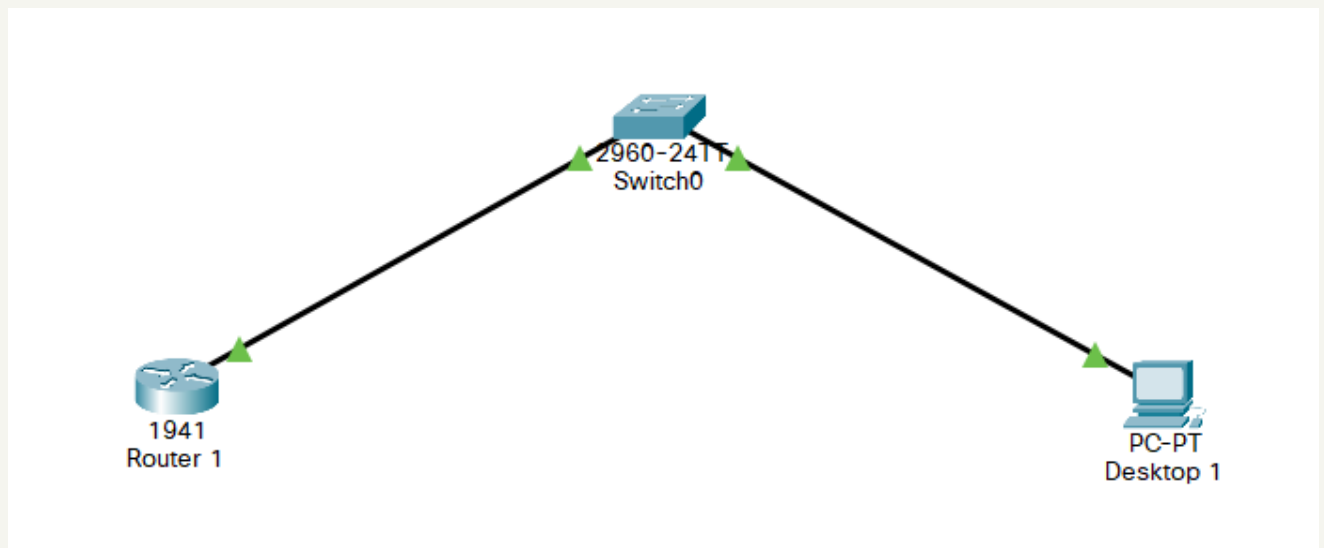


Figure 6.1: Architectural design of the Telnet.

1. Basic IP Setting for connectivity

Admin Desktop

IP address 192.168.1.2 **Subnet mask** 255.255.255.0 **Default gateway** 192.168.1.1

The next step is to assign the suitable IP setting to these devices. For keeping it simple and making basic connectivity we will assign just two IP addresses to these devices. We will assign the IP address to the PC. For this will open the PC setting and then IP configuration.

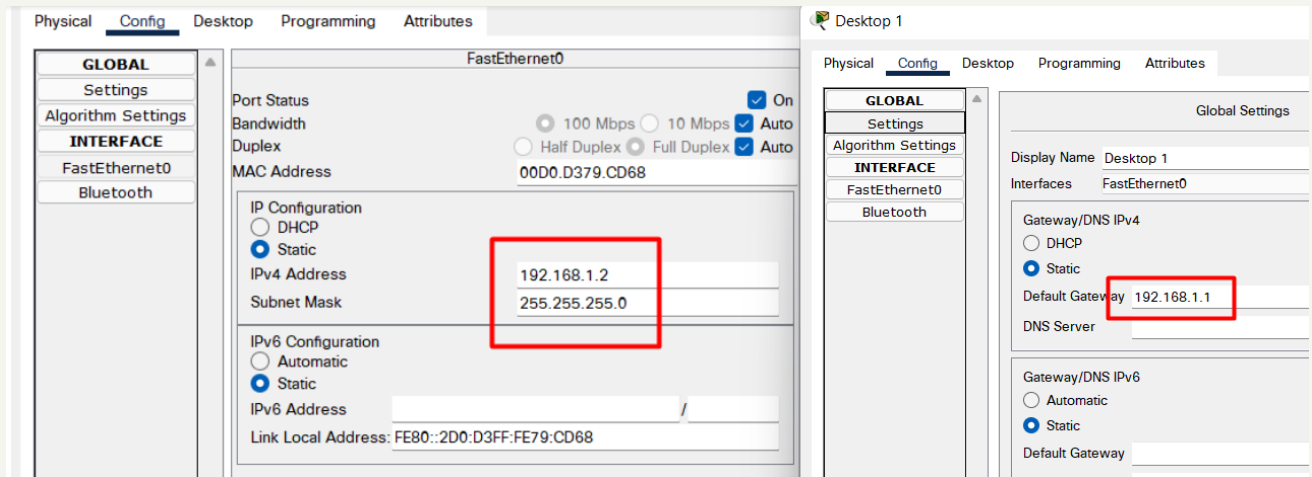


Figure 6.2: IP Setting for Desktop.

Here we will assign an IP address to the host, in our case we are going to assign it 192.168.1.1 with the default gateway. For the default gateway we will assign the IP address 192.168.1.2. We assign the second IP address to our Vlan1 interface on switch. And its IP address will be the gateway of the host that is 192.168.1.2. For this we will use the basic commands.

Double-click Cisco Router1 to open the CLI prompt and type No to skip the initial configuration and press Enter.

To enable Telnet on the Router, execute the following commands in order.

2. Configure IP addresses on the admin PC and interface fa0/0 of the router

Command Line Interface (CLI) to configure Router 1:

```
Router>enable
Router#
Router#config terminal
Router(config)#interface gigabitethernet 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

3.Configure Telnet password on VTY lines and configure remote login.

```
Router(config)#line vty 0 14
Router(config-line)#login local
Router(config-line)#password bdu123
Router(config-line)#privilege level 15
Router(config-line)#exit
Router(config)#user bdu privilege 15 password bdu123
Router(config)#end
Router#wr
```

```
Router(config-if)#no sh

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed
state to up

Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#
Router(config)#line vty 0 14
Router(config-line)#login local
Router(config-line)#
Router(config-line)#password bdu123
Router(config-line)#
Router(config-line)#privilege level 15
Router(config-line)#exit
Router(config)#user bdu privilege 15 password bdu123
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#wr
Building configuration...
[OK]
Router#
Router#
Router#
```

Figure 6.3: Configuring Telnet for remote login

4. Testing Telnet connectivity.

We can now telnet the router using the IP address of fa0/0 interface. So, in the command prompt of the admin PC type telnet 192.168.1.1 then hit enter key.

5. Provide Telnet Password (that we set in step 4), then hit enter. Correct password allows access to the CLI of the router.

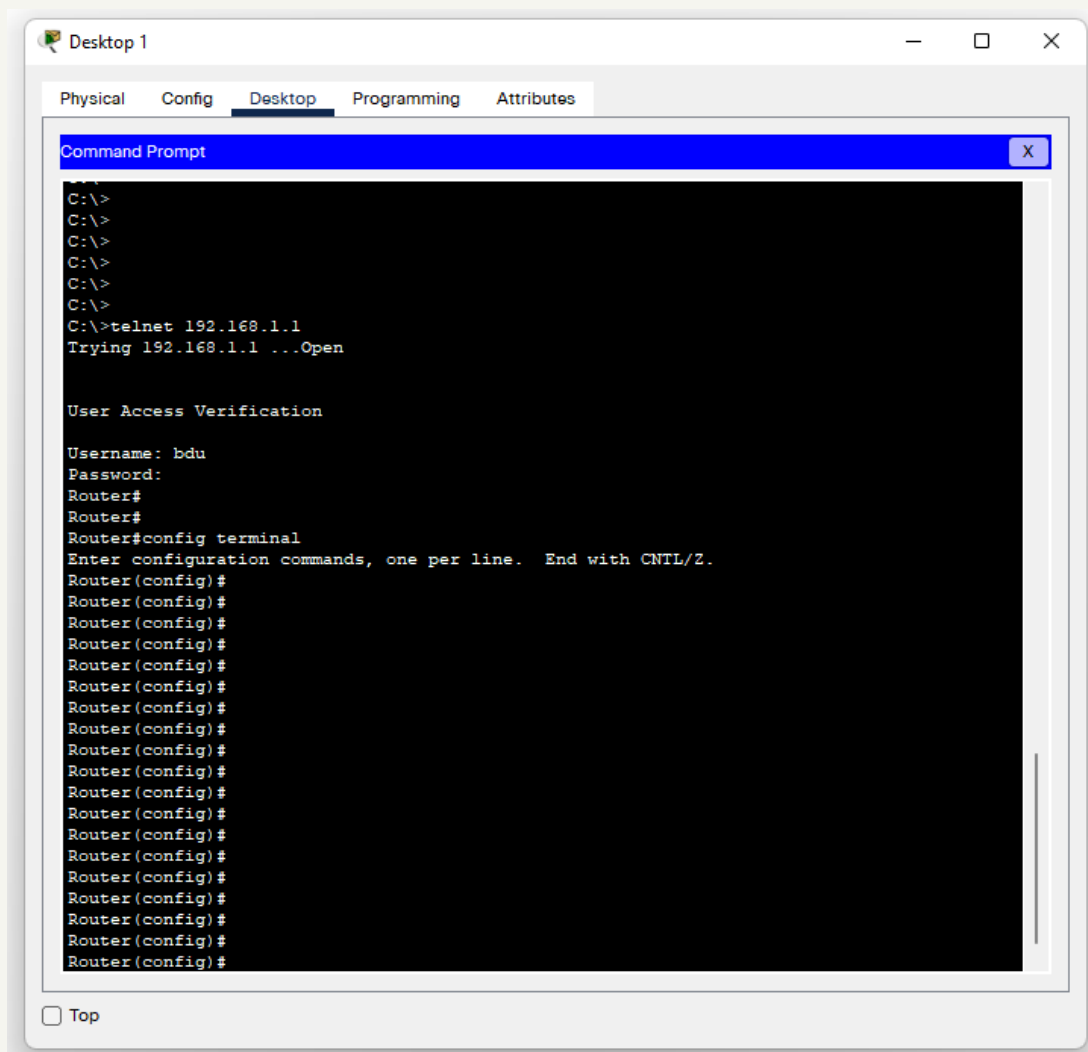


Figure 6.4: Provide Telnet Password for remote login

6. Now provide the enable password (that we set in step 2) to be allowed into privileged executive mode of the router.

7. Once connected to the Cisco Router, we can now manage our device by accessing it through LAN or WAN.

To view the connections to the device, simply run the **show line** command

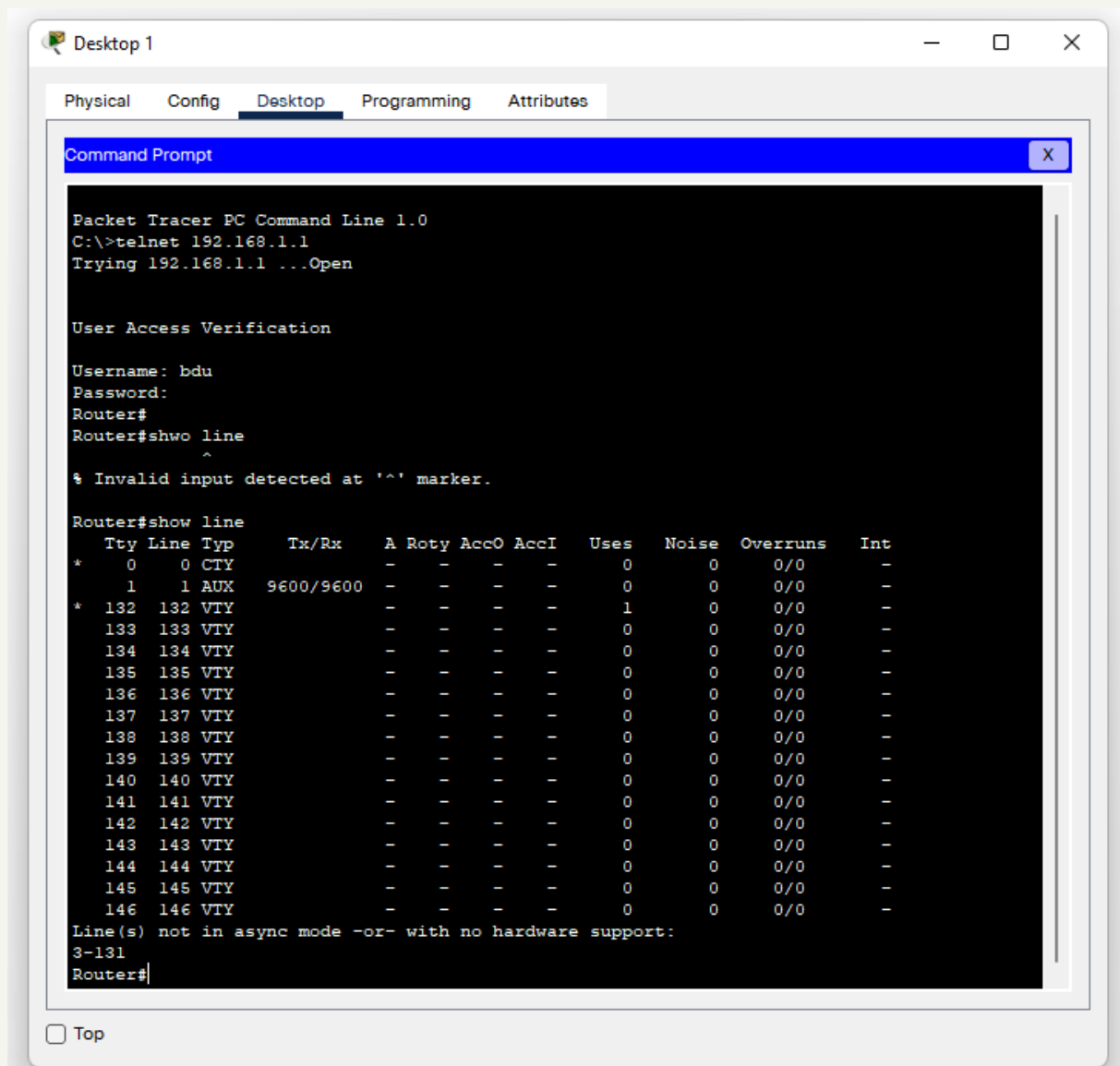


Figure 6.5: Accessing router from Admin desktop using telnet.

8. we can review open sessions on the Cisco Router

Router#show running-config

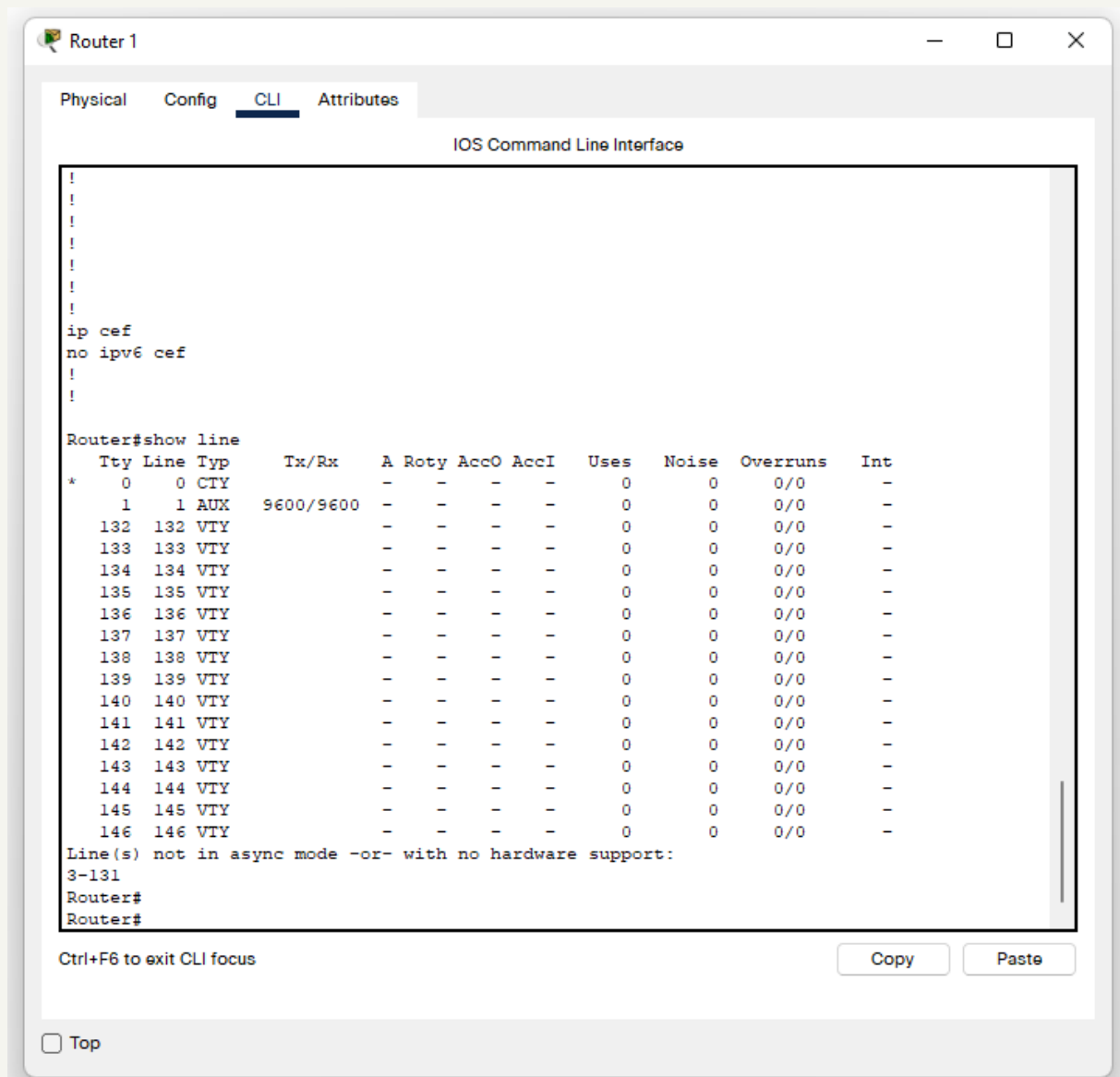


Figure 6.6: Displaying running-config from direct router router

Result:

We can now access open sessions of router 1 from the Admin Desktop using telnet which is 100% the same as open sessions shown from the router itself.

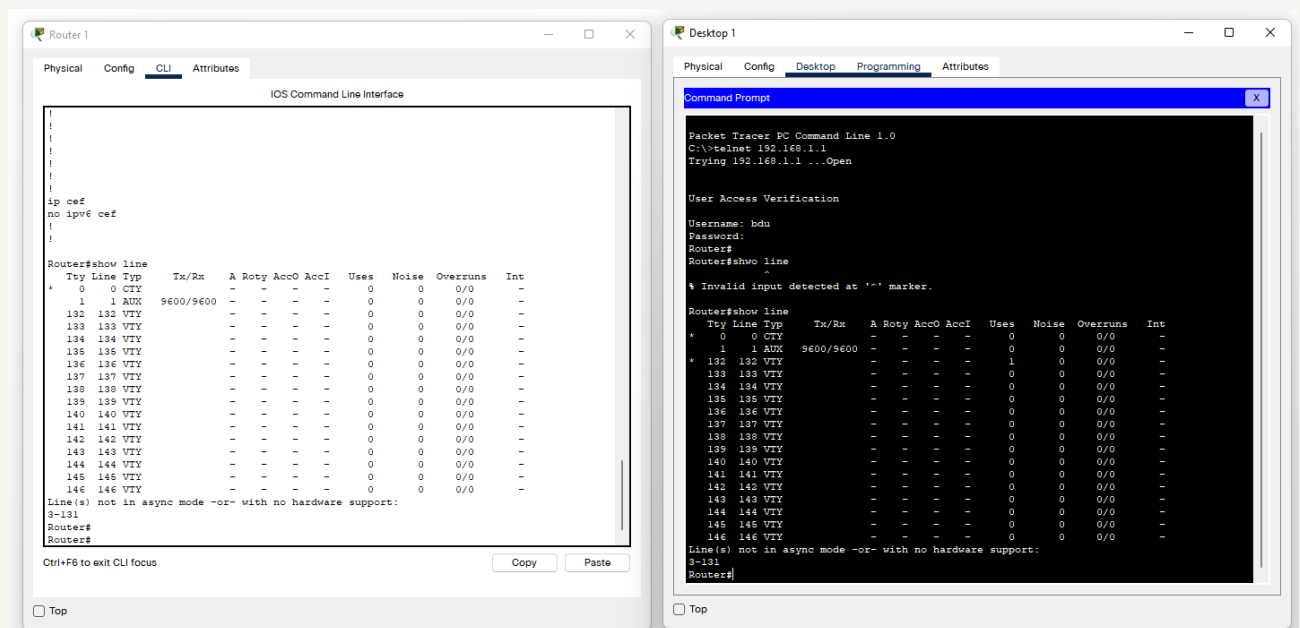


Figure 6.7: Accessing open sessions from Admin Desktop using telnet.

Conclusion:

My achievement is to get access to the router from the admin desktop by implementing the Telnet. Here I could also perform router configurations from the admin desktop.

Report No: 07

Report Title: Configuration of Secure Shell (SSH) using Cisco Packet Tracer.

Objectives:

The main objectives behind SSH implementation using Cisco packet tracer are:

- To acquire knowledge about Secure Shell (SSH).
- To learn about Cisco Packet Tracer.
- To implement the Secure Shell (SSH) using Cisco Packet Tracer.

Discussion:

SSH, also known as Secure Socket Shell (SSH), is a network protocol that provides administrators with a secure way to access a remote computer. SSH also refers to the suite of utilities that implement the protocol. SSH (Secure Shell) is one of the most used protocols in network World. As a secured alternative to Telnet, SSH is always in the life of a network engineer. It helps us to connect our routers, switches, and any other network equipment. Especially because SSH is more secure, it is always preferred more than Telnet.

Methodology of my project:

- Create a New Project.
- Create the Secure Shell (SSH).
- Configuration of the Network Nodes.
- Choose the Statistics.
- Run the Simulation.
- Analysis of the Results.

Working Procedure:

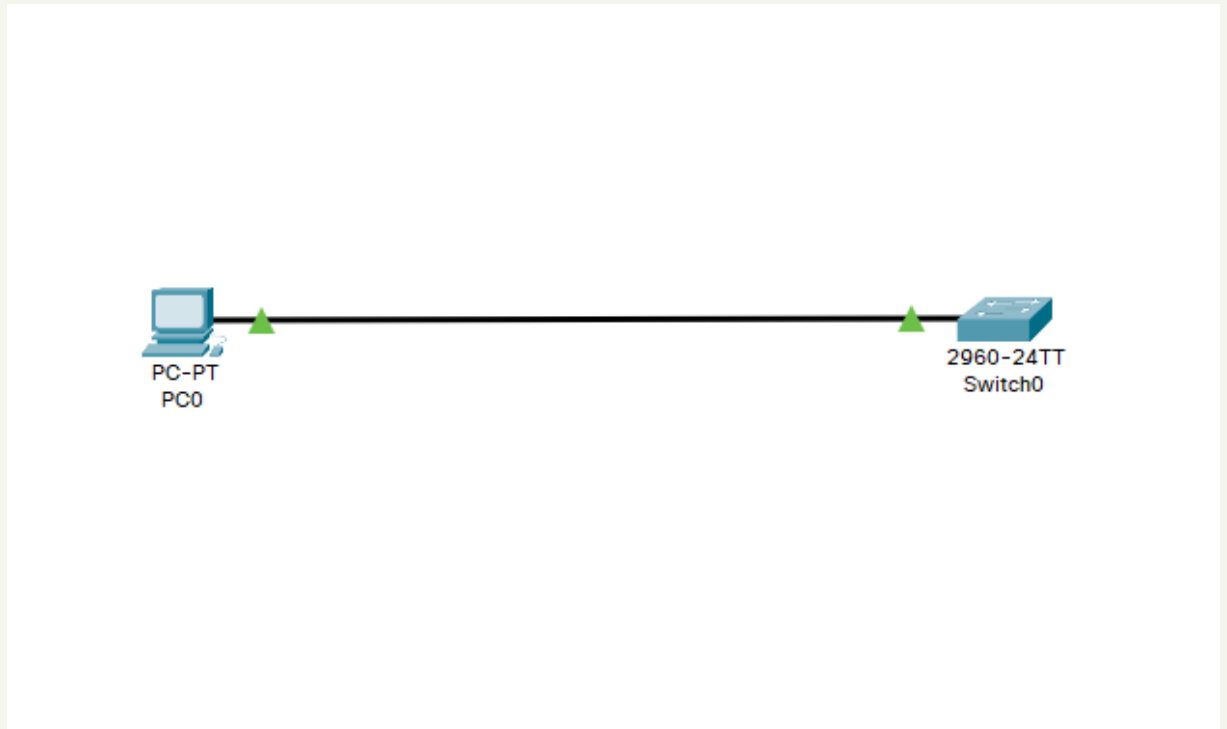


Figure 7.1: Architectural design of the Secure Shell (SSH).

1. Basic IP Setting for connectivity

The next step is to assign the suitable IP setting to these devices. For keeping it simple and making basic connectivity we will assign just two IP addresses to these devices. We will assign the IP address to the PC. For this will open the PC setting and then IP configuration.

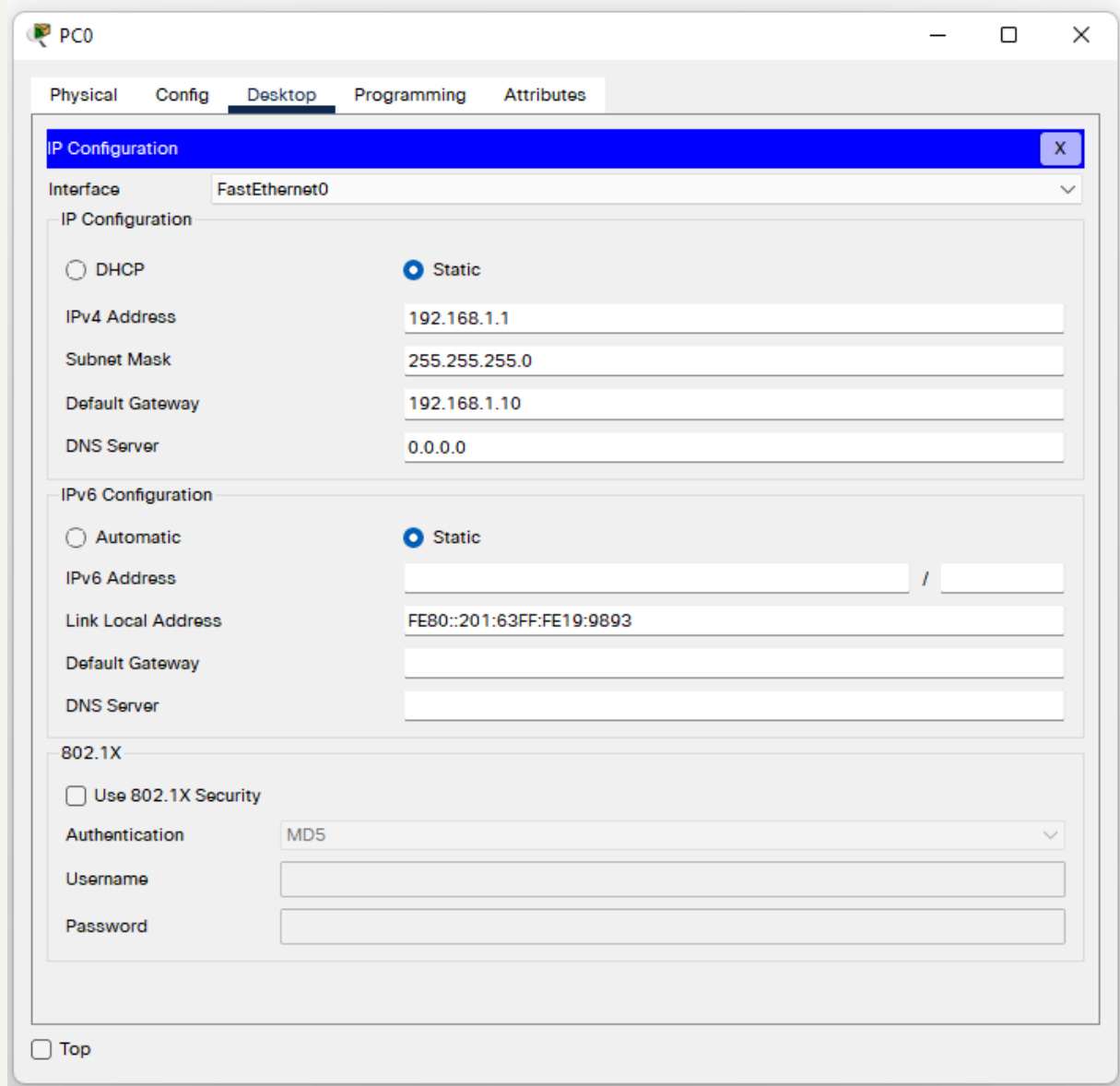


Figure 7.2: IP Setting for PC0.

Here we will assign an IP address to the host, in our case we are going to assign it 192.168.1.1 with the default gateway. For the default gateway we will assign the IP address 192.168.1.10. We assign the second IP address to our Vlan1 interface on switch. And its IP address will be the gateway of the host that is 192.168.1.10. For this we will use the basic commands.

2. Command Line Interface (CLI) to configure Switch:

```
Switch> enable
Switch# config t
Switch(config)#interface vlan 1
Switch (config-if)# ip address 192.168.1.10 255.255.255.0
Switch (config-if)#no shut
```

3. Set host-name and domain-name on Switch

For SSH configurations we need to configure a hostname and domain-name for our switch. We can do this with these simple commands.

```
Switch# config t
Switch (config)#hostname SW1
SW1 ( config)#ip domain-name bdu.com
```

4. Set console and enable password for SSH login

For SSH access it is required that we must configure the console and enable password on our cisco switch. We can set these two passwords with the following commands.

```
SW1 ( config)#line console 0
SW1(config-line)#password cisco
SW1(config -line)#logging synchronous
SW1(config- line)#login local
SW1 (config- line)#exit
SW1 # enable secret cisco
```

5. Generate the RSA Keys

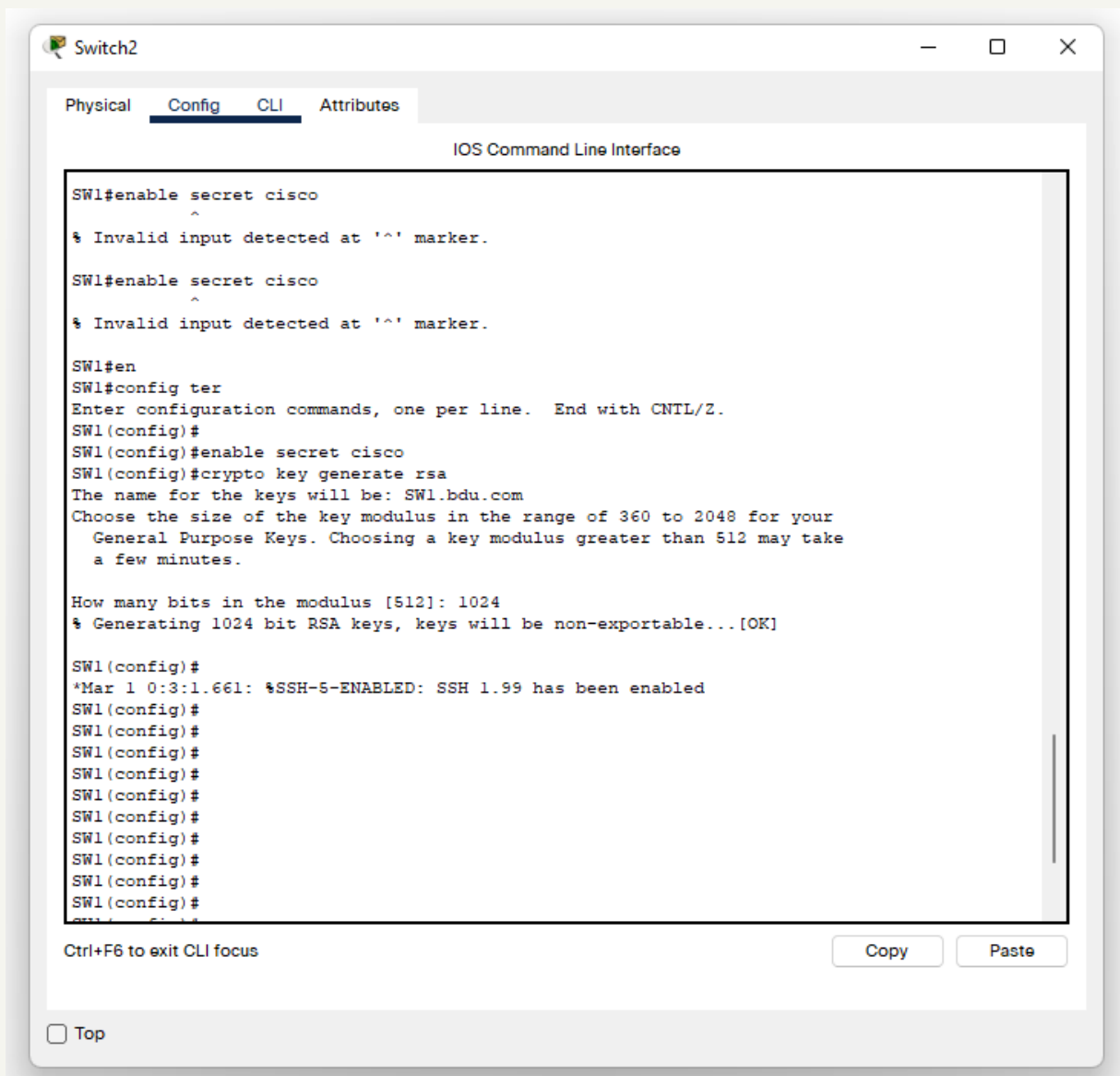


Figure 7.3: Generate RSA Keys.

Our Cisco switch must have RSA keys for the SSH process. we can generate the RSA keys with following command:


```
SW1 ( config)# crypto key generate rsa
```

```
How many bits in the modulus [512]: 1024
```

```
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Set the size of the key to 1024 bits.

If our Cisco Switch is running an older version of Cisco IOS image, then it is extremely recommended that we upgrade to the latest Cisco IOS.

6. Setup the Line VTY configurations

For the configuration of SSH on cisco switch we need the following line vty configurations, and input transport is required to set to SSH. Set the login-to-local, & password to 7.

```
sw1 ( config)#line vty 0 4
sw1 ( config-line)#transport input ssh
sw1( config -line)#login local
sw1(config- line)#password 7
sw1(config- line ) #exit
```

7. Create the username password for SSH access from PC

If we do not have a username for SSH access we need to create a username. we can do it with this simple command:

```
sw1# config t
sw1 (config ) # username bdu password cisco
```

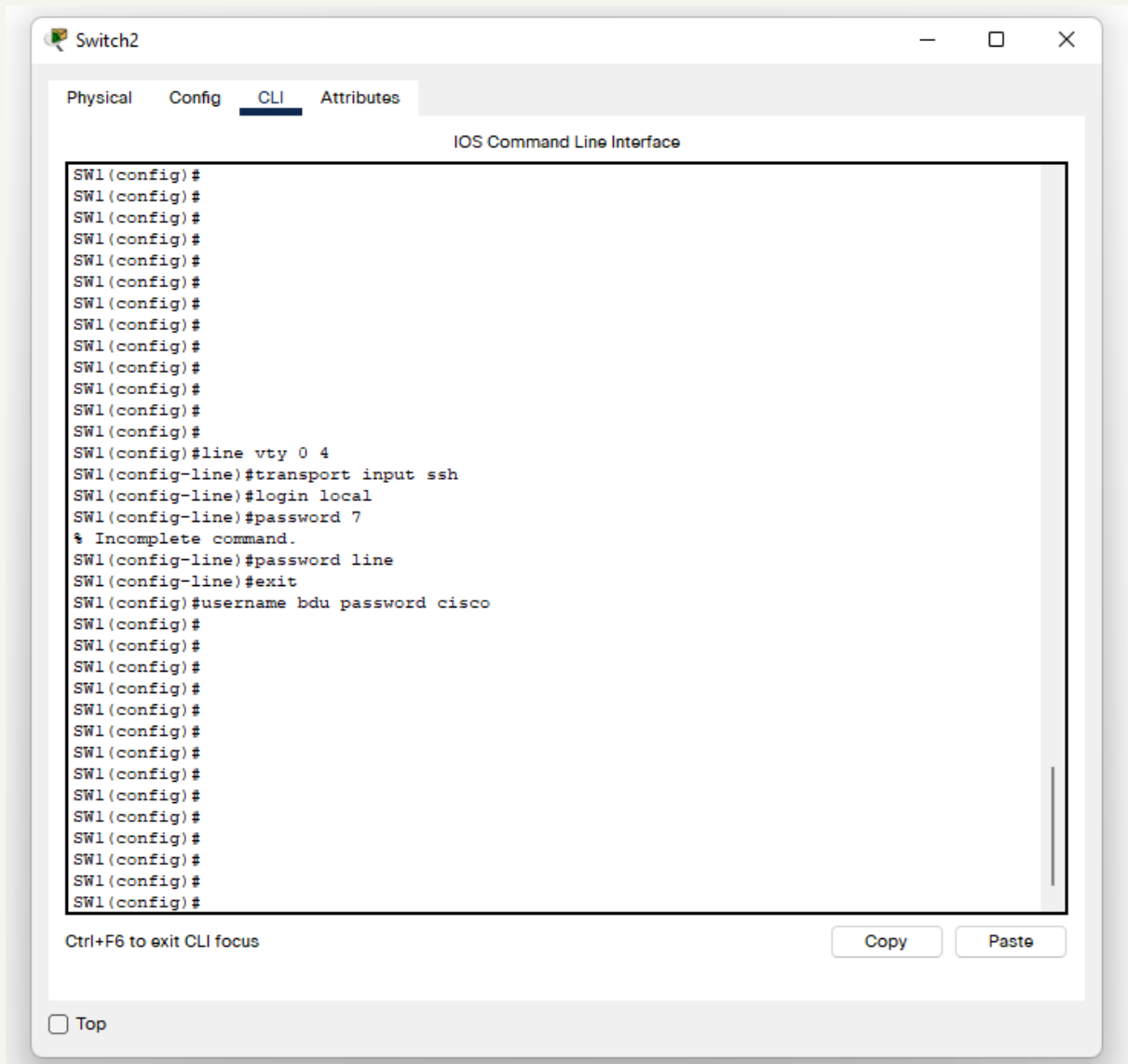


Figure 7.4: Creation of username & password for SSH.

Make sure the password encryption service is enabled on our switch, this service will encrypt our password, & when we do “sh run”, we’ll see only the encrypted password, not clear text password.

SW1# service password-encryption

8. Verify SSH access from Host

Once we are done with the above configurations, we can test all these configurations by creating a SSH connection from Host. We do it with the command `ssh -l <username> <IP address>`. Open the host command prompt and use the command

```
C:\>ssh -l bdu 192.168.1.10
```

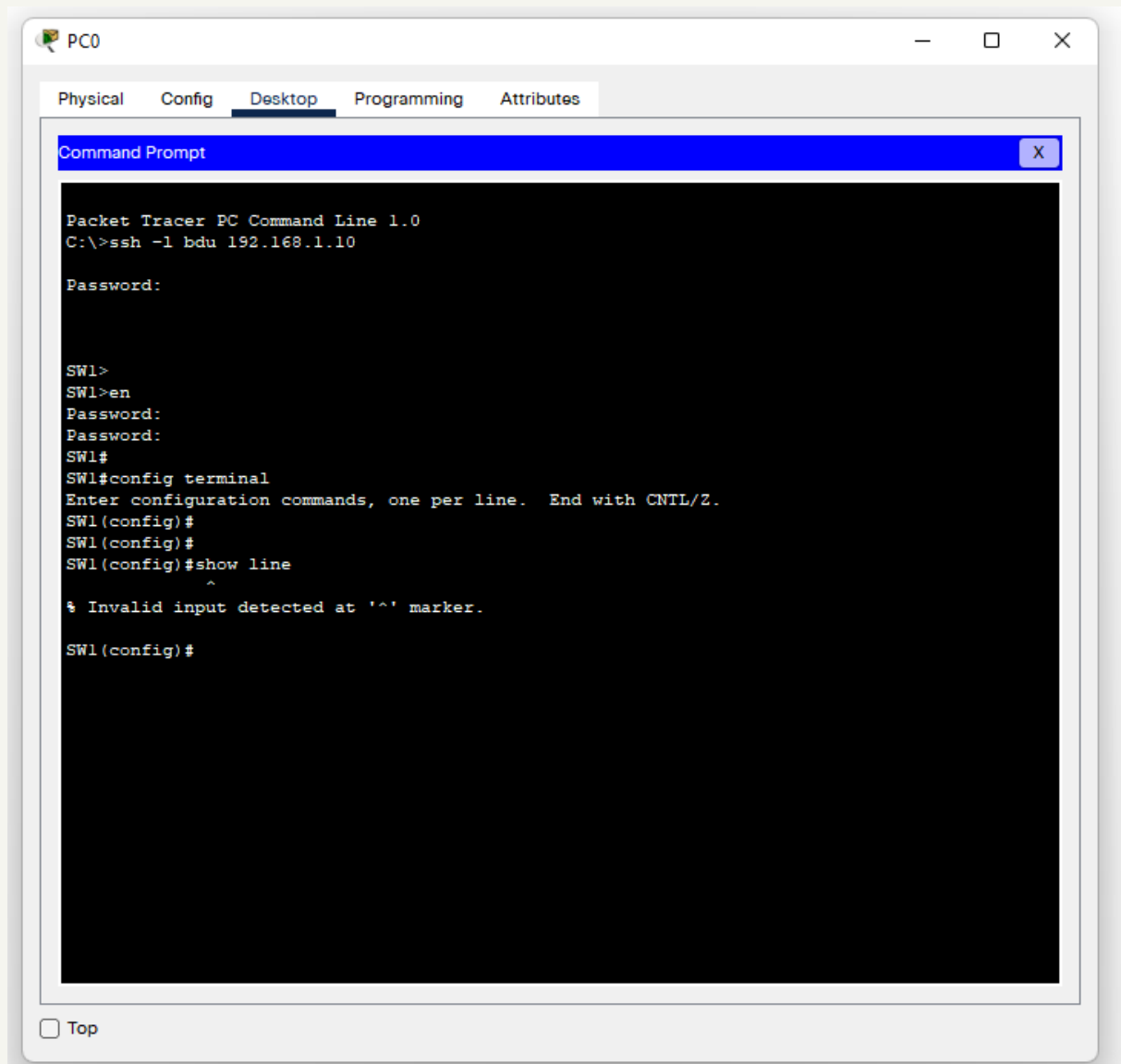
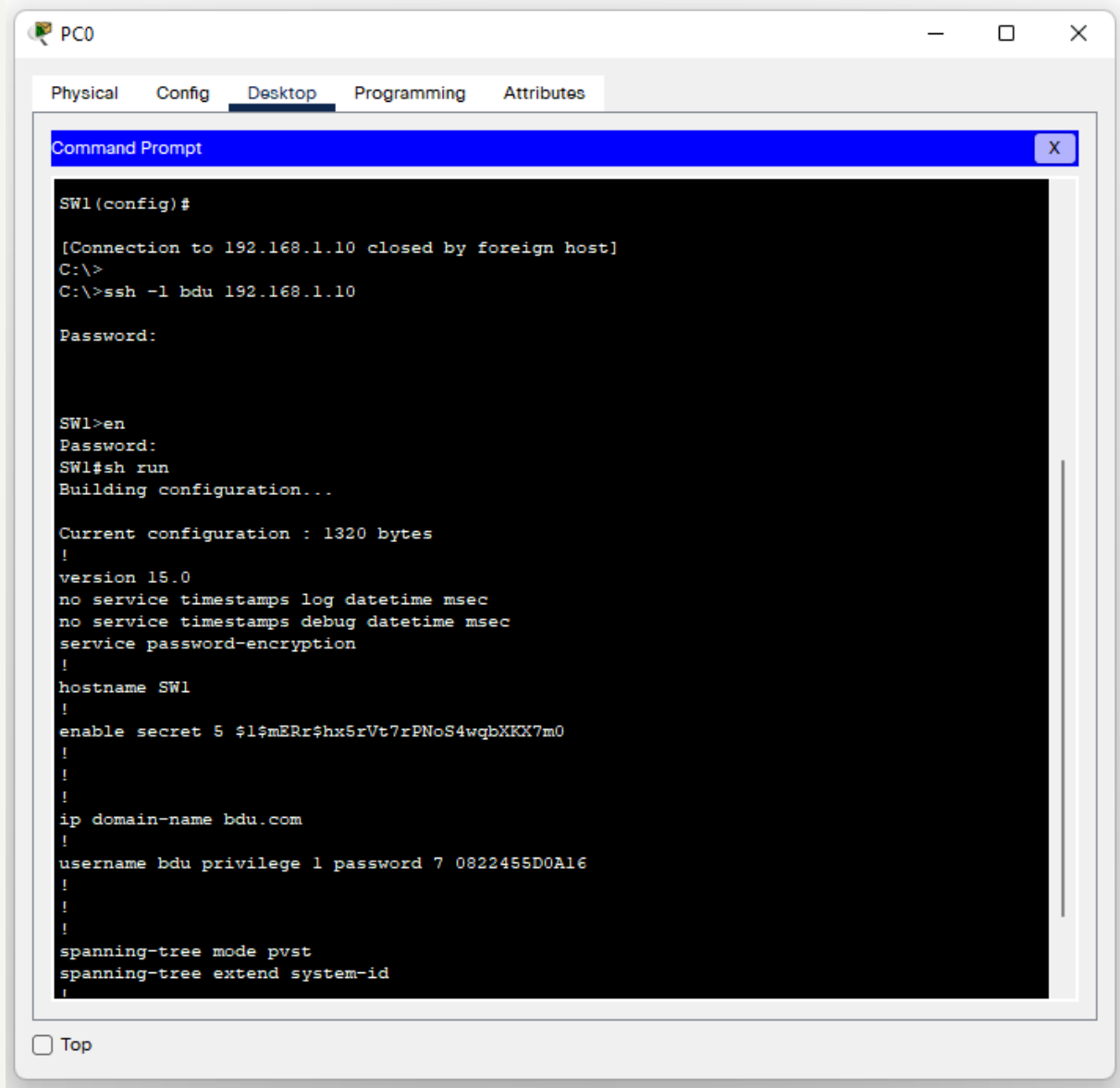


Figure 7.5: Verify SSH access from Host.

It will ask for password, provide the password that we created with this username in previous steps. Then it asks for the console password and then we need to provide the enabled password. Now we are in our Cisco switch. we can perform switch configurations from our host.

From the switch, if we use the command 'sh ip ssh', it will also confirm that SSH is enabled on this Cisco switch.

Result:



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
SW1(config)#
[Connection to 192.168.1.10 closed by foreign host]
C:\>
C:\>ssh -l bdu 192.168.1.10
Password:
SW1>en
Password:
SW1#sh run
Building configuration...

Current configuration : 1320 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname SW1
!
enable secret 5 $l$mERr$hx5rVt7rPNoS4wqbXKK7m0
!
!
!
ip domain-name bdu.com
!
username bdu privilege 1 password 7 0822455D0A16
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
```

Figure 7.6: Output of the Secure Shell (SSH).

Conclusion:

My achievement is to get access to the switch from the host PC by implementing the Secure Shell (SSH). Here I could also perform switch configurations from the host.