Mini Project Report Cover Sheet

SRM Institute of Science and Technology

College of Engineering and Technology

Department of Electronics and Communication Engineering

18ECC303J COMPUTER COMMUNICATION NETWORKS

Sixth Semester, 2020-21 (Even Semester)

Name **:** YAJNISH.M

Register No. **:** RA1811004010291

Title of the project **: WIFI Establishment Using Cisco Packet Tracer**

Project team members **:** Pradiksha.M (280); Yajnish.M (291); Ribhu.B (298)

Lab Supervisor **:** Vasanthi.M Ma'am, Priyalakshmi.B Ma'am

Reg. No →		RA1811004010280	RA1811004010291	RA1811004010298
Mark split up ↓	Maximum Marks	Marks obtained	Marks obtained	Marks obtained
Novelty in the project work / Abstract	**5**			
Level of understanding of the design / Configuration	**10**			
Individual Contribution to the project	**5**			
Report writing	**5**			
Total	**25**			

REPORT VERIFICATION

Lab supervisor Signature with date **:**

WIFI Establishment Using Cisco Packet Tracer

Abstract-

Wireless networks have seen unprecedented rise in their size and number of users in recent years. This unprecedented rise is attributed to the rise in the number of mobile computing devices. Moreover, the amount of data that is handled by these wireless networks has increased in recent years. The project is to study and understand the WLAN WPA2 PSK concept and the advantages of using Wireless Local Area Network, how the devices are controlled in this network. We understand the configuration that we use in Cisco packet tracer to build a WLAN WPA2 PSK network using router, switches and access points.

This circuit increases the security level of LAN and hence disallows unidentified devices to connect in this network.

Motivation/Challenge-

Motive of this project is to design a simple network with WLAN networking.

Objective-

The primary objective of this project is to design a simple network with WLAN WPA2 PSK protected access networking and connect the devices using Wi-Fi under one network.

Software/Hardware Requirements-

Cisco Packet Tracer

Engineering Standards-

WLAN- is a network that allows devices to connect and communicate wirelessly. Unlike a traditional wired LAN, in which devices communicate over Ethernet cables, devices on a WLAN communicate via Wi-Fi. New devices are typically added and configured using DHCP. They can communicate with other devices on the network the same way they would on a wired network. The primary difference is how the data is transmitted. In a LAN, data is transmitted over physical cables in a series of Ethernet packets. In a WLAN, packets are transmitted over the air.

WPA2 PSK- This standard specifies security mechanisms for wireless networks, replacing the short Authentication and privacy clause of the original standard with a detailed Security clause. In the process, the amendment deprecated broken Wired Equivalent Privacy (WEP), while it was later incorporated into the published IEEE 802.11-2007 standard. 802.11i supersedes the previous security specification, Wired Equivalent Privacy (WEP), which was shown to have security vulnerabilities. Wi-Fi Protected Access (WPA) had previously been introduced by the Wi-Fi Alliance as an intermediate solution to WEP insecurities. WPA implemented a subset of a draft of 802.11i. The Wi-Fi Alliance refers to their approved, interoperable implementation of the full 802.11i as WPA2, also called RSN (Robust Security). 802.11i makes use of the Advanced Encryption Standard (AES) block cipher, whereas WEP and WPA use the RC4 stream cipher.

Realistic Constrains-

When an actual network is being designed, they might be some loss of signal and hence the efficiency of the network will be lesser than theoretical efficiency. But here since it is a simulation of a network, Outcomes will be very accurate.

Deliverables-

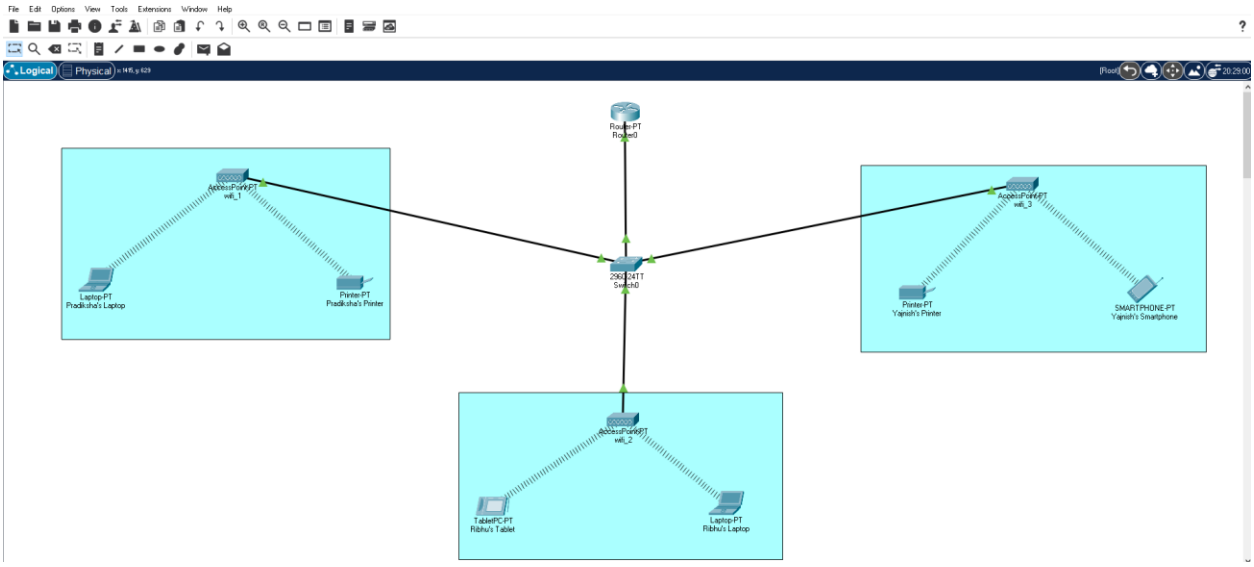
1. WPA2-PSK

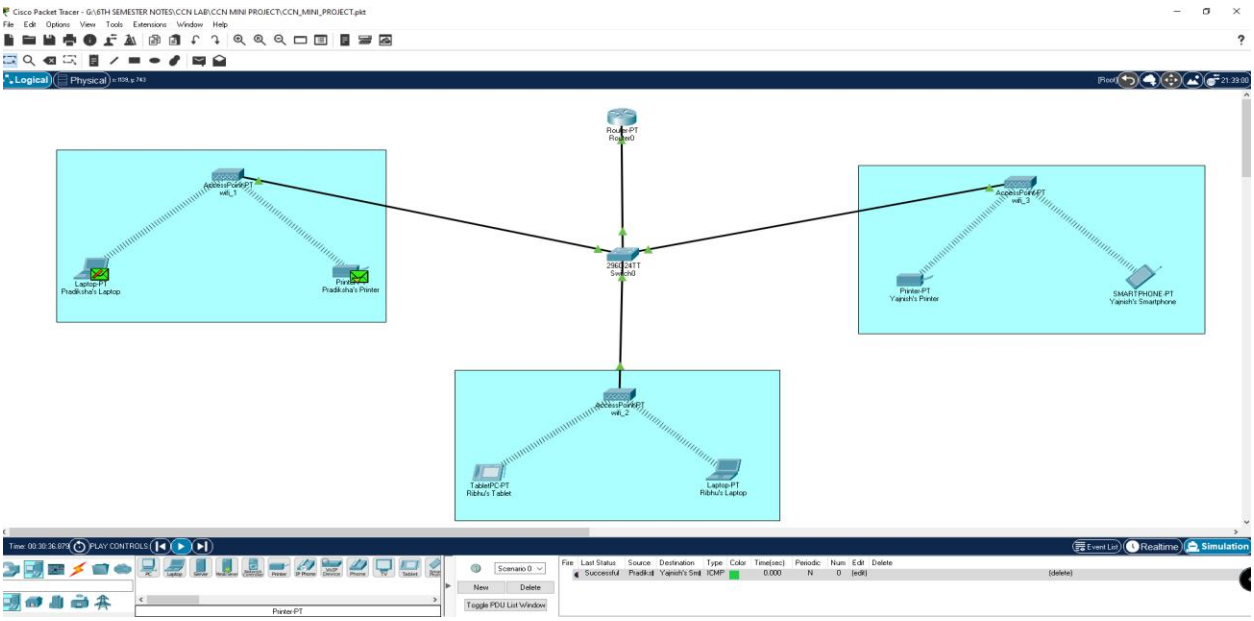
1. In addition to the encryption benefits, WPA2 also adds two enhancements to support fast roaming of wireless clients moving between wireless AP's.
2. PMK caching support – allows for reconnections to AP's that the client has recently been connected without the need to re-authenticate.
3. Pre-authentication support – allows a client to pre-authenticate with an AP towards which it is moving while still maintaining a connection to the AP it's moving away from.
4. PMK caching support and Pre-authentication support enable WPA2 to reduce the roaming time from over a second to less than 1/10th of a second. The ultimate benefit of the fast roaming is that WPA2 can now support timing-sensitive applications like Citrix, video, or VoIP (Voice over IP) which would break without it.

2. WLAN

1. It's a reliable sort of communication.
2. As WLAN reduces physical wires so it's a versatile way of communication.
3. It provides high rate thanks to small area coverage.

Methodology-





Network Design of a Simple network

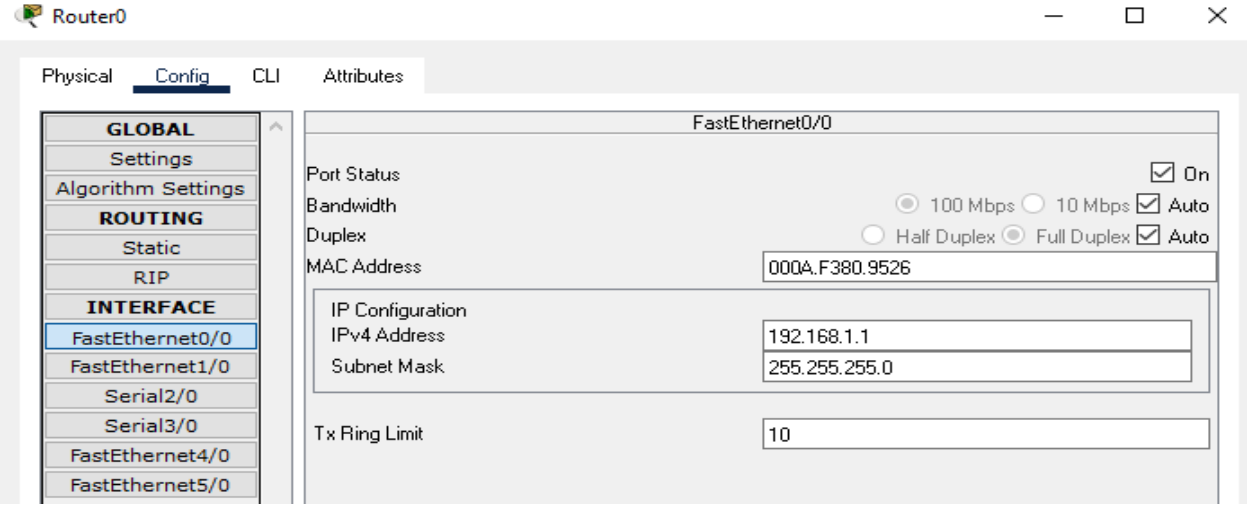
A WLAN, or wireless LAN, is a network that allows devices to connect and communicate wirelessly. Unlike a traditional wired LAN, in which devices communicate over Ethernet cables, devices on a WLAN communicate via Wi-Fi. While a WLAN may look different than a traditional LAN, it functions the same way. New devices are typically added and configured using DHCP. They can communicate with other devices on the network the same way they would on a wired network. The primary difference is how the data is transmitted. In a LAN, data is transmitted over physical cables in a series of Ethernet packets. In a WLAN, packets are transmitted over the air.

WPA stands for "Wi-Fi Protected Access", and PSK is short for "Pre-Shared Key."
WPA2-PSK [AES] is the recommended secure method of making sure no one can actually listen to your wireless data while it's being transmitted back and forth between your router and other devices on your network. We use WPA2-PSK protection.
Each device is given its own IP address and configured in such a way to connect it wireless.

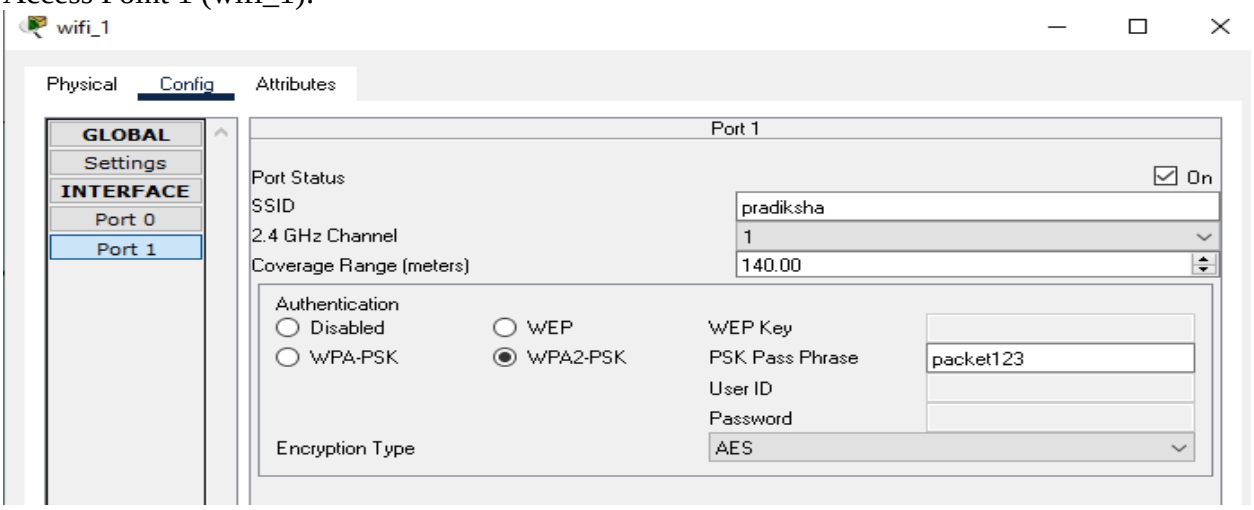
WMP300N module is a wireless adapter module, used in P.C, laptops, printers and servers in order to establish a wireless communication. We have to power of the device first, remove the wired default module and then replace it with this WMP300N wireless module and then power on the device and configure.

The default IP address that the router is configured with is 192.168.1.1 under fast Ethernet 0/0 static IP address. The access points here are named as wifi_1, wifi_2 and wifi_3. Those are the SSID's given to those access points.
The mode of security of access points is WPA2 PSK which is encrypted under AES Encryption.
The data type of password generated is Hexadecimal and the size of password is 8 characters. Coming to the devices, their IP configurations will start from 192.168.1.2 and it goes on. All devices have static IP. In order to check the working of the network, we can send a message packet from any device to any other device and the status will turn into successful. . During simulation, message packets will be assigned to different colours.
For example let's set the source as pradiksha's Laptop and the destination as Yajnish's printer. During the simulation the packet first goes to access point and then transmits to other access points, and checks where does this packet belong to. Once when the packet reaches the destination and comes back to original device, it shows the tick mark. We can check the ping and trace route as well.

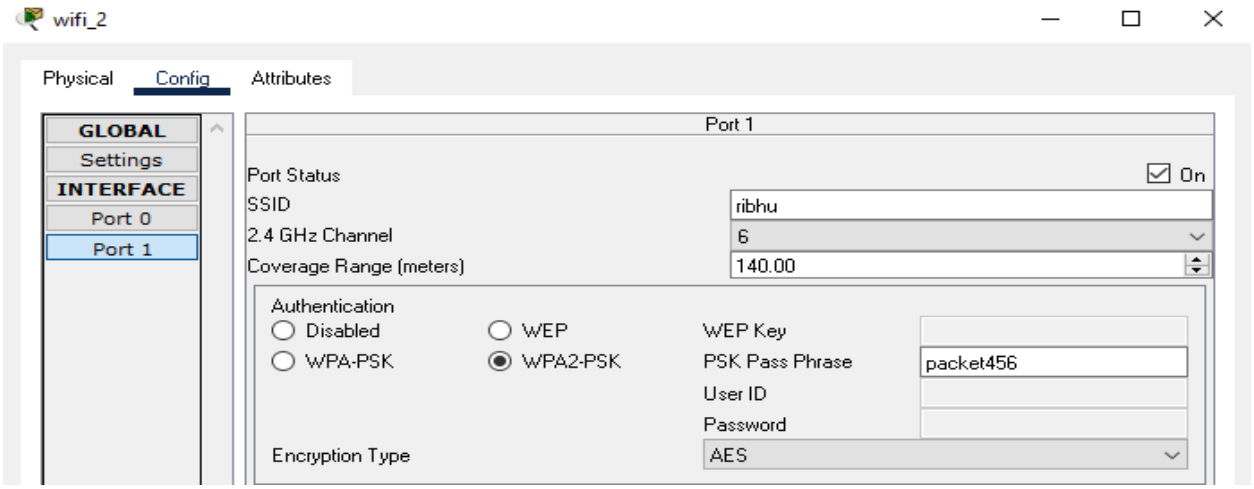
Router 0:



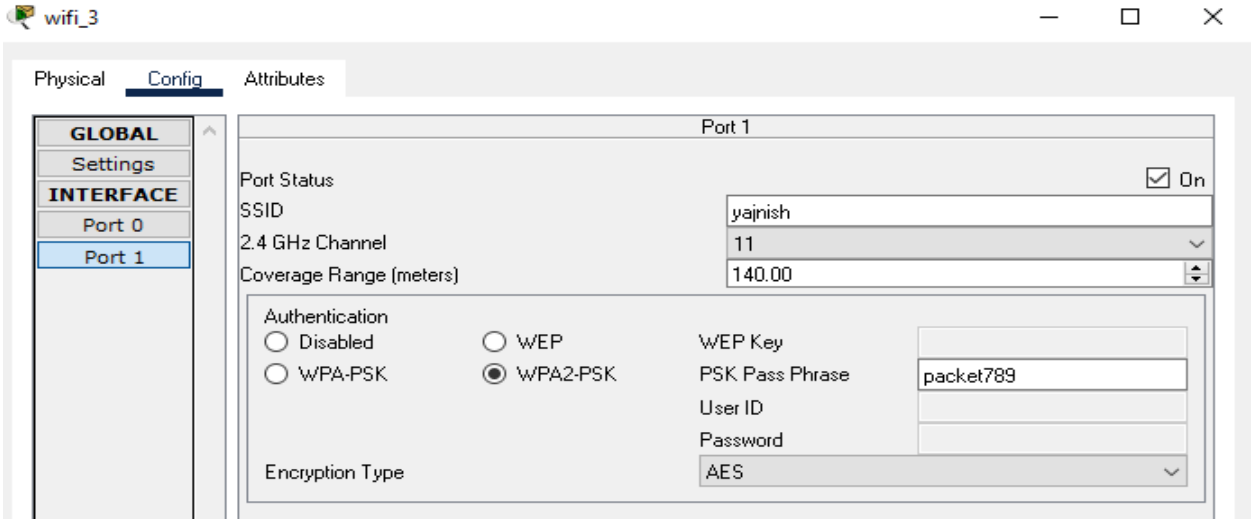
Access Point 1 (wifi_1):



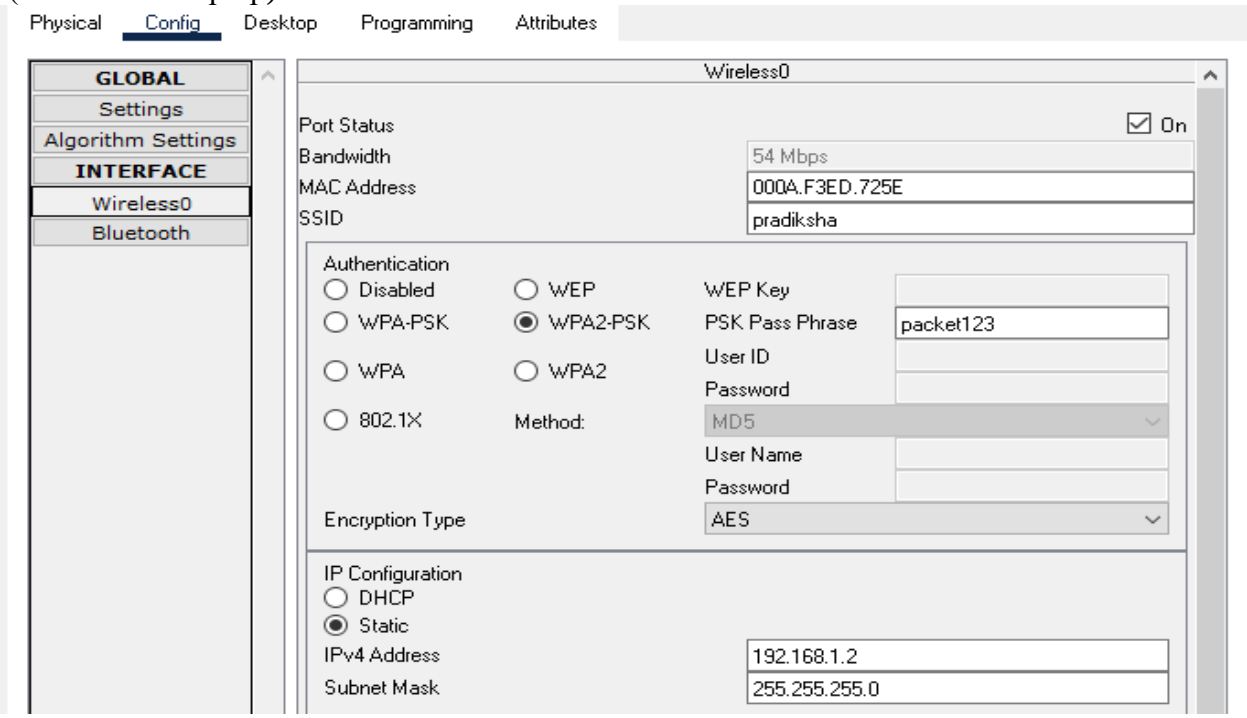
Access Point 2 (wifi_2):



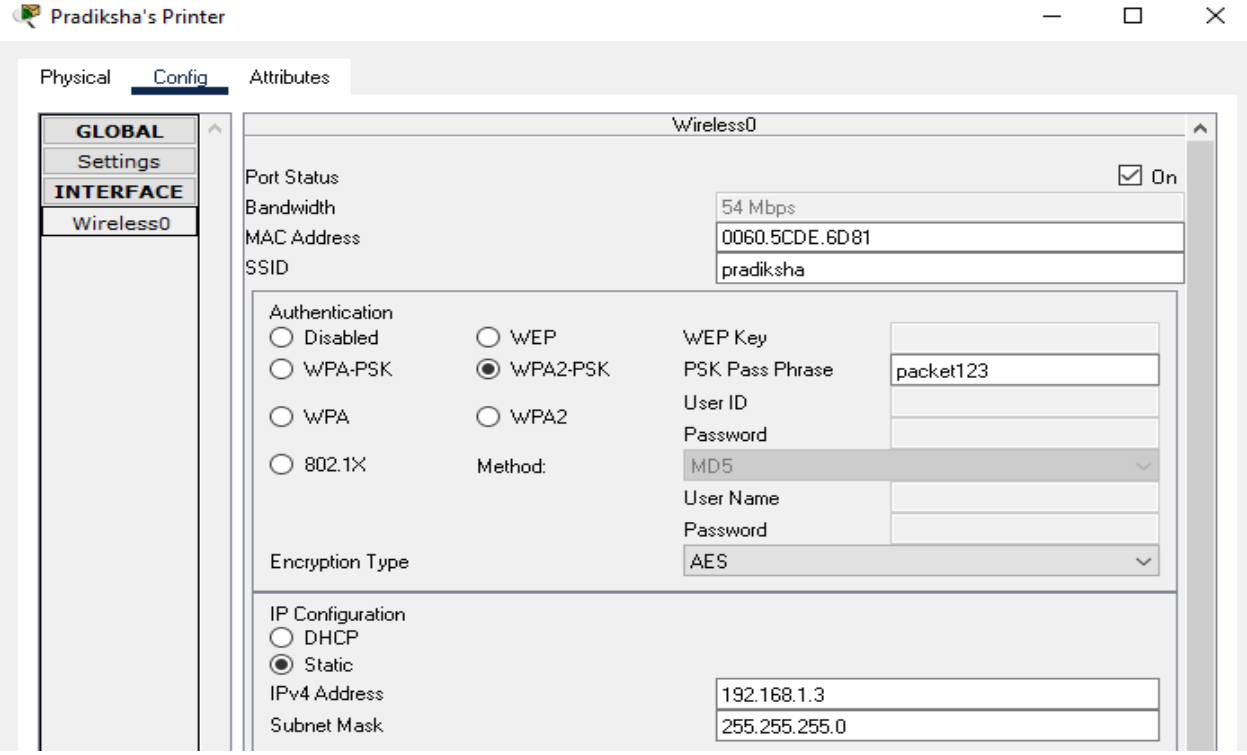
Access Point 3(wifi_3):



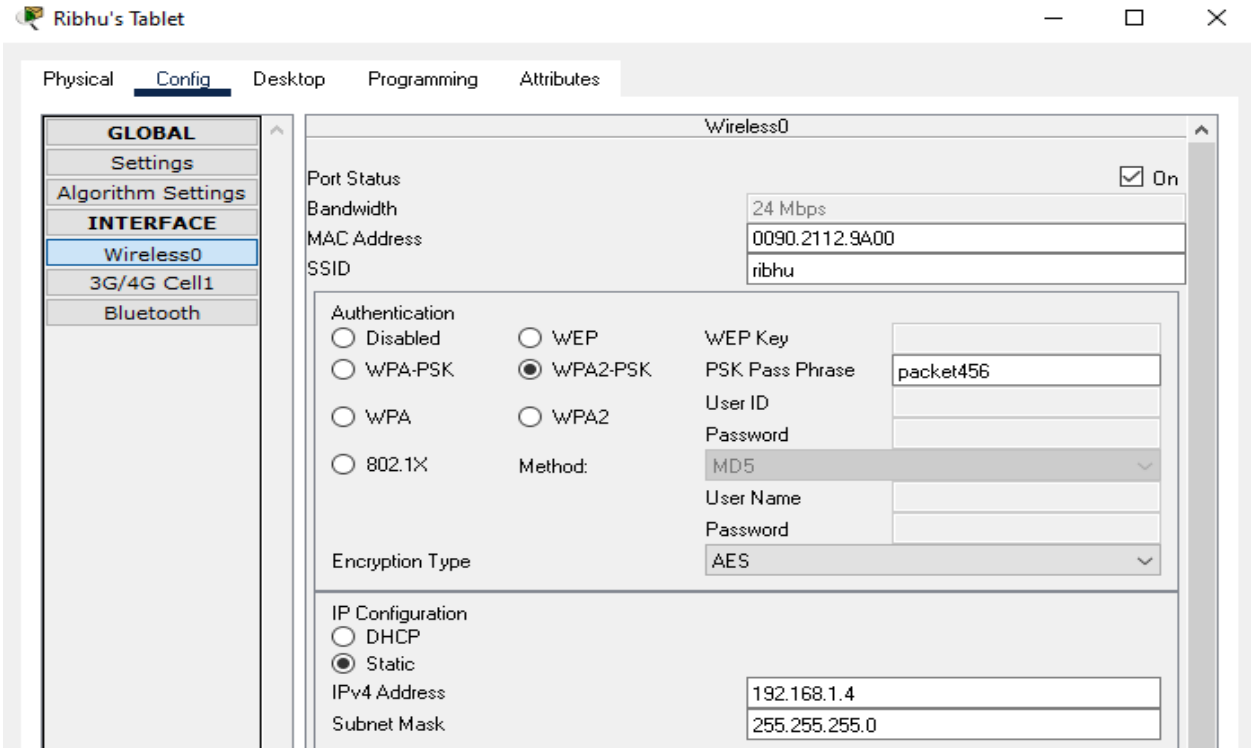
(Pradiksha's Laptop):



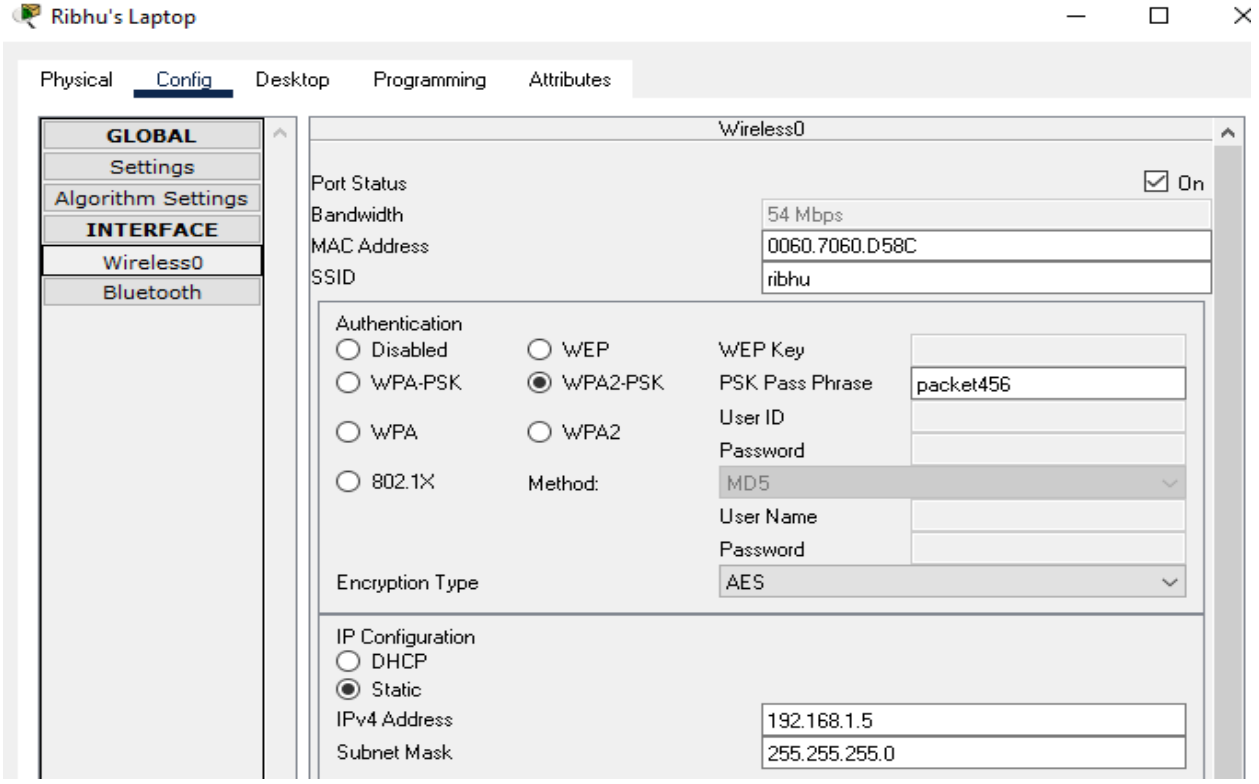
(Pradiksha's Printer):



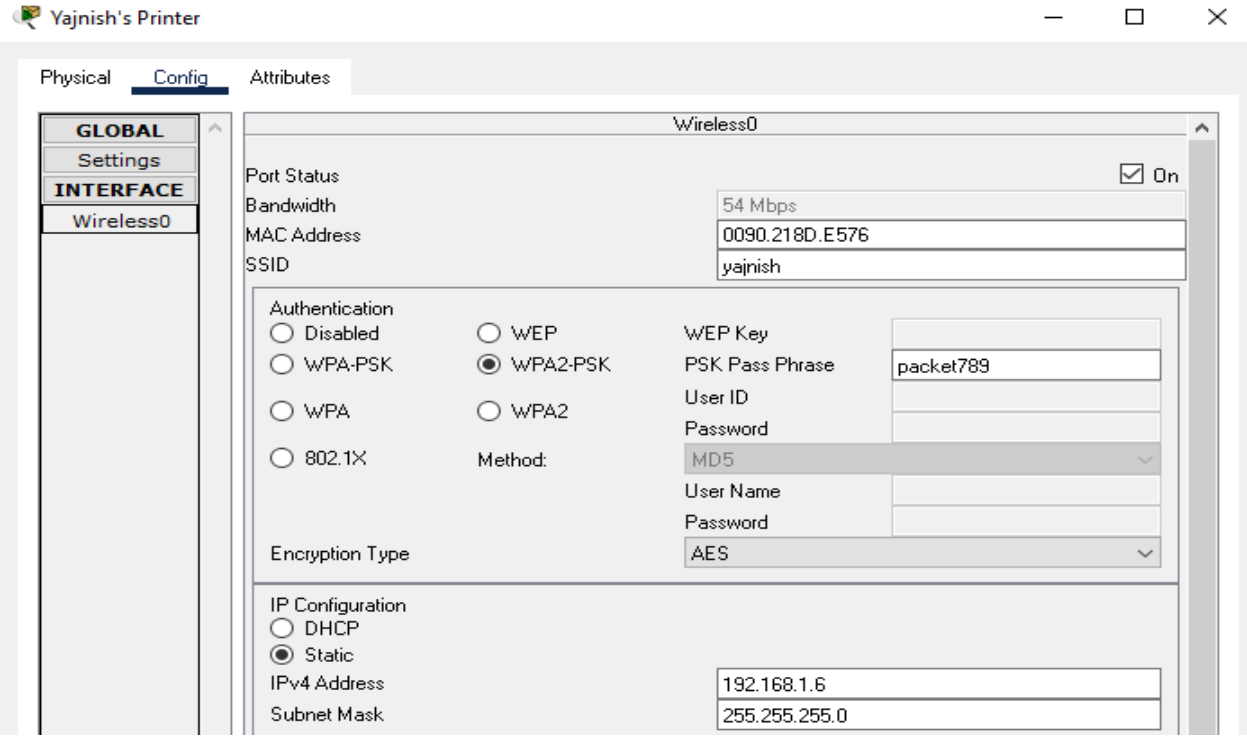
(Ribhu's Tablet):



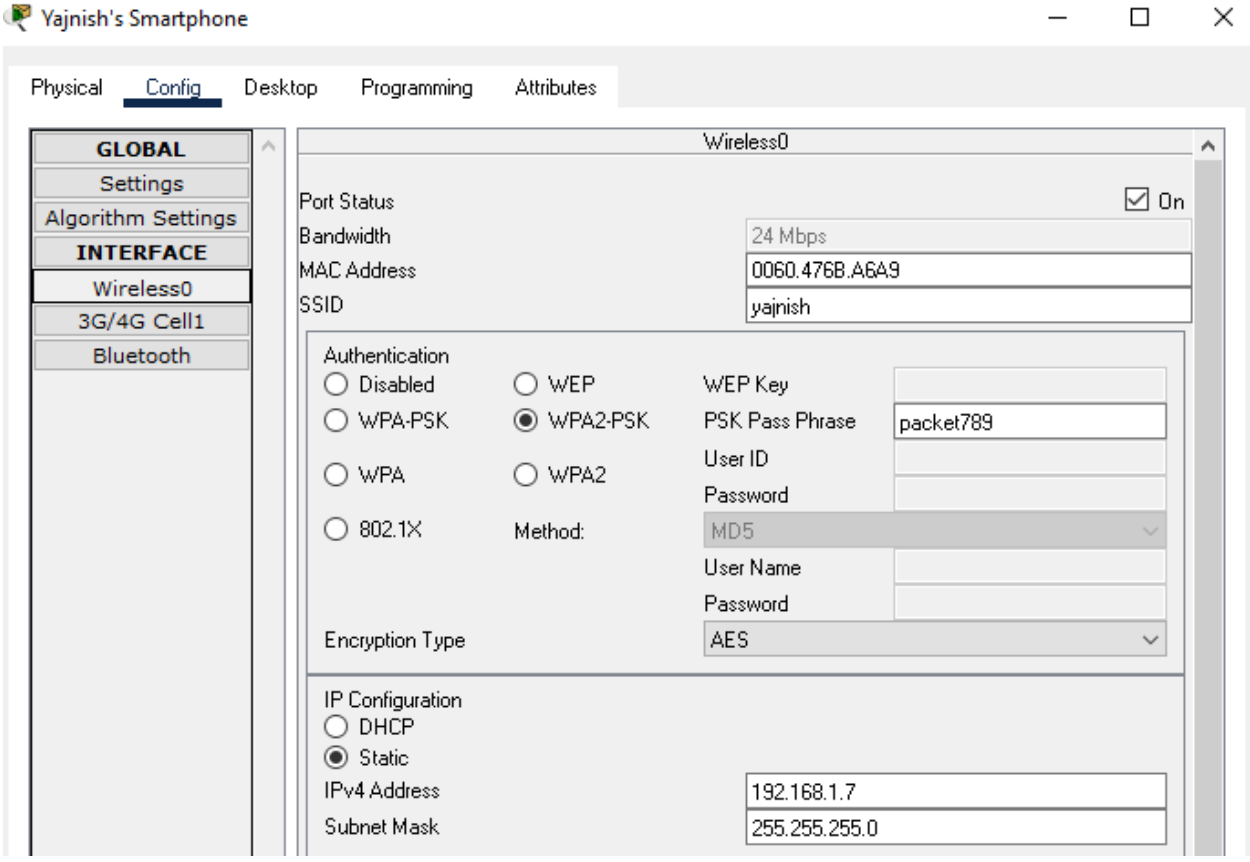
(Ribhu's Laptop):



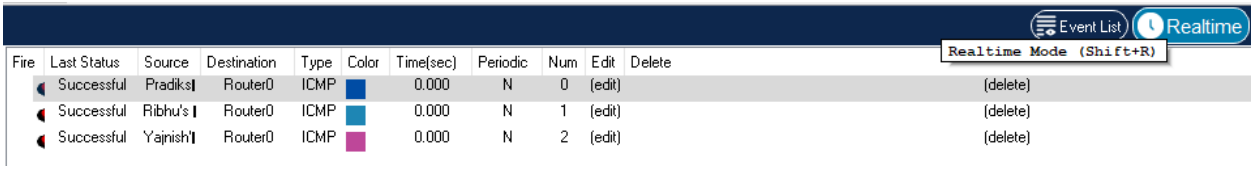
(Yajnish’s Printer):

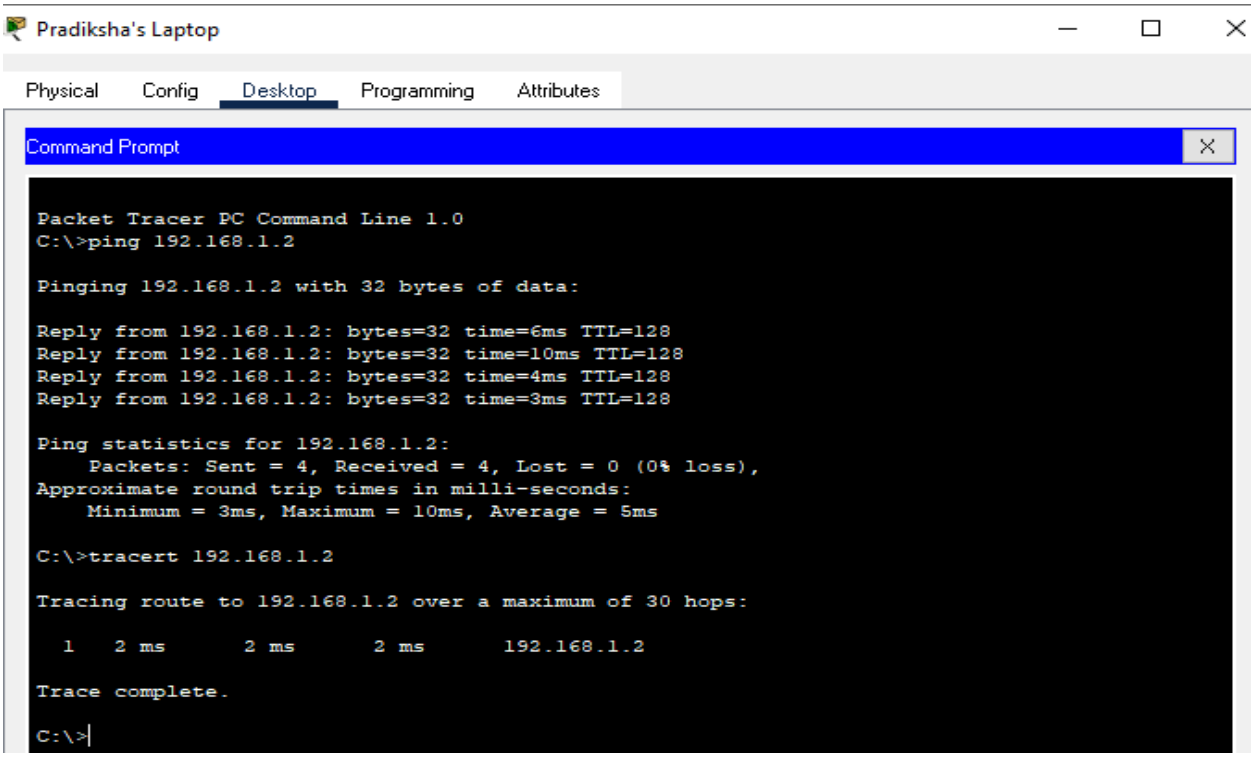


(Yajnish’s Smartphone):



Result/Illustration-





Ribhu's Tablet

Physical | Config | Desktop | Programming | Attributes

Command Prompt

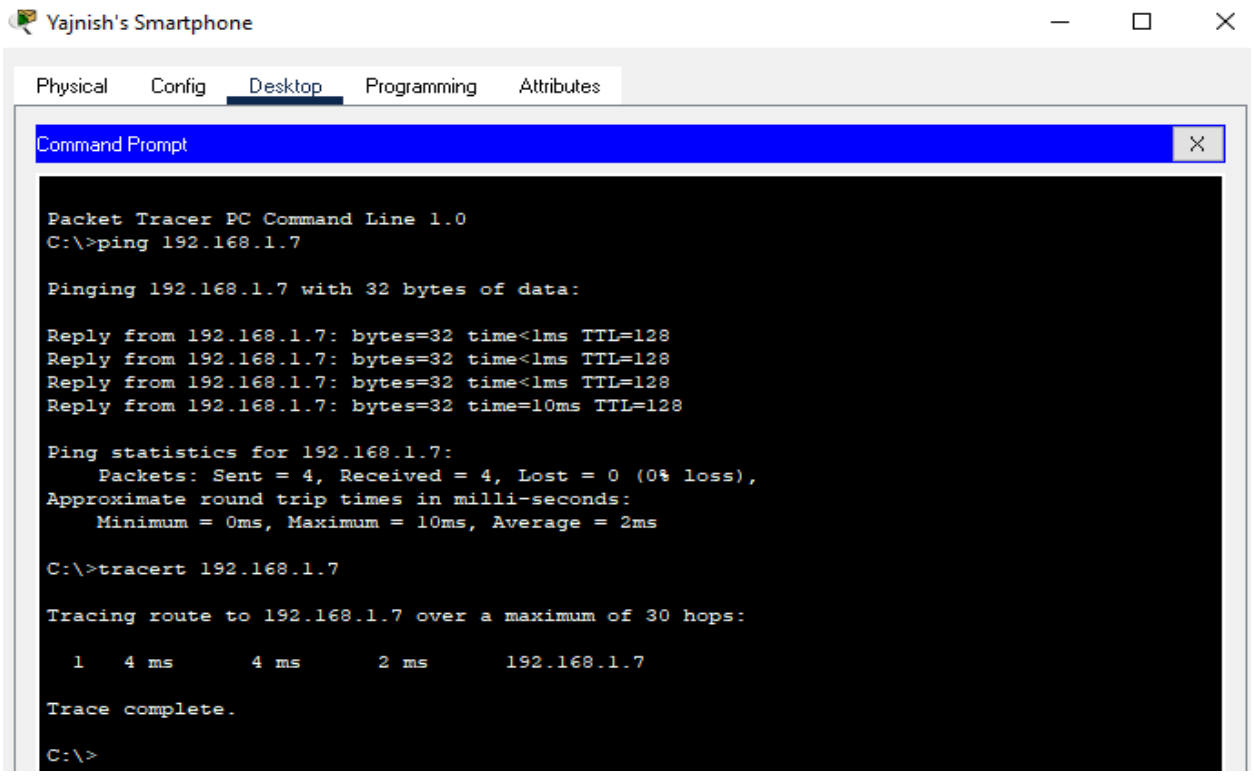
```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time=4ms TTL=128
Reply from 192.168.1.4: bytes=32 time=10ms TTL=128
Reply from 192.168.1.4: bytes=32 time=3ms TTL=128
Reply from 192.168.1.4: bytes=32 time=18ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 18ms, Average = 8ms

C:\> tracert 192.168.1.4

Tracing route to 192.168.1.4 over a maximum of 30 hops:

  1    2 ms      0 ms      2 ms      192.168.1.4

Trace complete.

C:\>
```

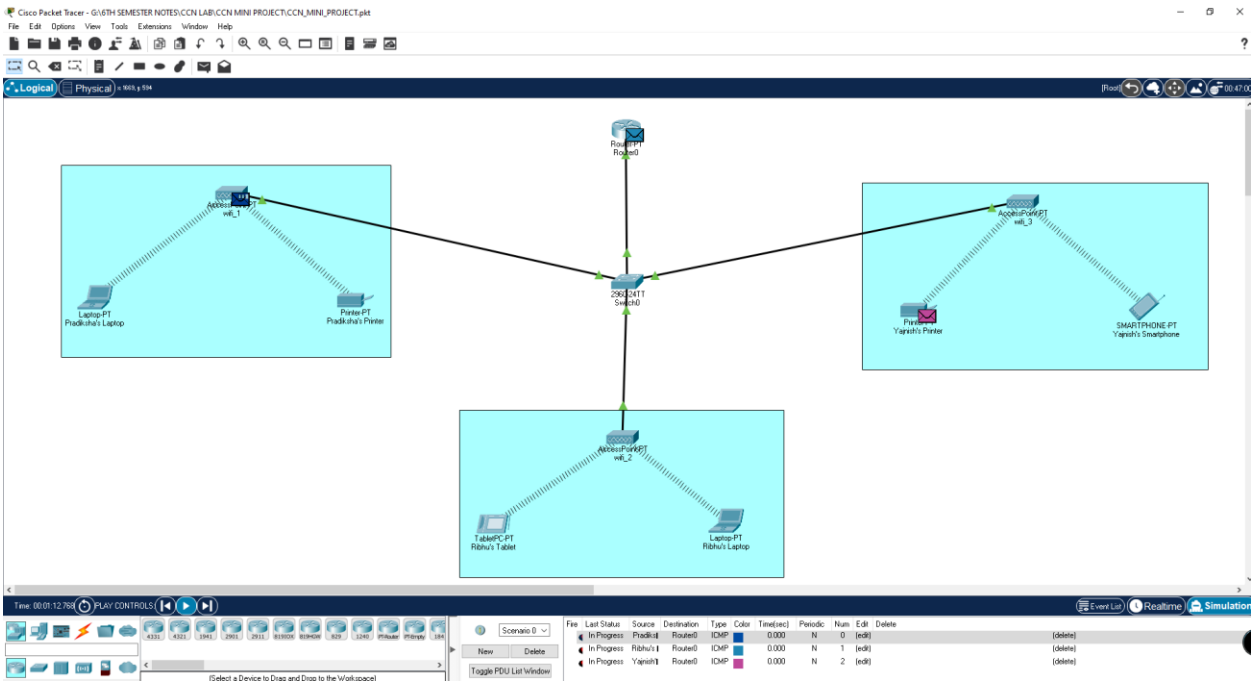
Ribhu's Laptop

Physical | Config | Desktop | Programming | Attributes

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time=7ms TTL=128
Reply from 192.168.1.5: bytes=32 time=11ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 5ms

C:\>tracert 192.168.1.5

Tracing route to 192.168.1.5 over a maximum of 30 hops:

  1    2 ms      4 ms      2 ms      192.168.1.5

Trace complete.

C:\>
```


Yajnish's Smartphone
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.7
Pinging 192.168.1.7 with 32 bytes of data:
Reply from 192.168.1.7: bytes=32 time<1ms TTL=128
Reply from 192.168.1.7: bytes=32 time<1ms TTL=128
Reply from 192.168.1.7: bytes=32 time<1ms TTL=128
Reply from 192.168.1.7: bytes=32 time=10ms TTL=128
Ping statistics for 192.168.1.7:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 10ms, Average = 2ms
C:\>tracert 192.168.1.7
Tracing route to 192.168.1.7 over a maximum of 30 hops:
1 4 ms 4 ms 2 ms 192.168.1.7
Trace complete.
C:\>


Logical
Physical
Laptop-PT
Pradiksha's Laptop
Printer-PT
Pradiksha's Printer
Printer-PT
Yajnish's Printer
SMARTPHONE-PT
Yajnish's Smartphone
TabletPC-PT
Ribhu's Tablet
Laptop-PT
Ribhu's Laptop

Conclusion-

Thus, a simple network of WLAN WPA2 PSK is successfully designed and executed using Cisco packet Tracer.

References-

[1] WLAN definition <https://techterms.com/definition/wlan>

[2] AES Encryption https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

[3] WEP, WPA. WPA2 https://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/

[4] PSK < https://www.juniper.net/documentation/en_US/junos-space-apps/network-director3.0/topics/concept/wireless-wpa-psk-authentication.html>

[5] Engineering Standards <http://en.wikipedia.org/w/index.php?title=IEEE_802.1>

[6] Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2) Paul Arana INFS 612 – Fall 2006 <https://cs.gmu.edu/~yhwang1/INFS612/Sample_Projects/Fall_06_GPN_6_Final_Report.pdf>

[7] Reference to design a WLAN WPA2 PSK network <https://youtu.be/vAr9XsAo0iM>

[8] Wireless Router configuration in Cisco Packet Tracer <https://computernetworking747640215.wordpress.com/2018/06/22/wireless-router-configuration-in-cisco-packet-tracer/>