PASSWORD PROTECTION IN WIRELESS COMMUNICATION USING CISCO PACKET TRACER

A PROJECT REPORT

Submitted by

BIDYASAGAR BEHERA (230720100128)
SUBRAT NAYAK (230720100134)
SONAL SANJIT ROUT (230720100142)
JIBAN JAGANNATH JENA (230720100147)

in partial fulfillment for award of the degree of

MASTER OF COMPUTER APPLICATION
IN
COMPUTER SCIENCE & ENGINEERING

Centurion
UNIVERSITY
Shaping Lives...
Empowering Communities...

SCHOOL OF ENGINEERING AND TECHNOLOGY

BHUBANESWAR CAMPUS

CENTURION UNIVERSITY OF TECHNOLOGY AND MANAGEMENT

ODISHA

FEBRUARY 2024 / MAY 2024

PASSWORD PROTECTION IN WIRELESS COMMUNICATION USING CISCO PACKET TRACER

A PROJECT REPORT

Submitted by

BIDYASAGAR BEHERA (230720100128)

in partial fulfillment for award of the degree of

MASTER OF COMPUTER APPLICATION
IN
COMPUTER SCIENCE & ENGINEERING

Centurion
UNIVERSITY
Shaping Lives...
Empowering Communities...

SCHOOL OF ENGINEERING AND TECHNOLOGY

BHUBANESWAR CAMPUS

CENTURION UNIVERSITY OF TECHNOLOGY AND MANAGEMENT

ODISHA

FEBRUARY 2024 / MAY 2024

BONAFIDE CERTIFICATE

Certified that this project report **PASSWORD PROTECTION IN WIRELESS COMMUNICATION USING CISCO PACKET TRACER** is the bonafide work of **"BIDYASAGAR BEHERA"** who carried out the project work under my supervision. This is to further certify to the best of my knowledge, that this project has not been carried out earlier in this institute and the university.

SIGNATURE
(Asst. Prof. Nibedita Sahoo)
(Asst. Prof. Dept. of MCA)

Certified that the above mentioned project has been duly carried out as per the norms of the college and statutes of the university.

SIGNATURE
(Prof. Rakesh Kumar Ray)
HEAD OF THE DEPARTMENT
HOD Of Master Of Computer Application

DEPARTMENT SEAL

DECLARATION

I hereby declare that the project entitled "**PASSWORD PROTECTION IN WIRELESS COMMUNICATION USING CISCO PACKET TRACER**" submitted for the "Minor Project" of 2 nd Semester in Master of Computer Application is my original work and the project has not formed the basis for the award of any Degree / Diploma or any other similar titles in any other University / Institute.

Name Of The Student : Bidyasagar Behera

Signature Of The Student :

Registration No. : 230720100128

Place : Bhubaneswar

Date :

ACKNOWLEDGEMENTS

I wish to express our profound and sincere gratitude to Asst. Prof. Nibedita Sahoo, Department of Master of Computer Application, SoET, Bhubaneswar Campus,who guided me into the intricacies of this project nonchalantly with matchless magnanimity.

I thank Prof. Mr. Rakesh Kumar Ray, Head of the Dept. of Master of Computer Application, SoET, Bhubaneswar Campus and Dr. Sujata Chakravarty, Dean,School of Engineering and Technology, Bhubaneswar Campus for extending their support during Course of this investigation.

I would be failing in my duty if I don't acknowledge the cooperationrendered during various stages of image interpretation by Mrs. Nibedita Sahoo .

I am highly grateful to Asst. Prof. Nibedita Sahoo who evinced keen interest and invaluable support in the progress and successful completion of my project work.

I am indebted to Asst.Prof. Nibedita Sahoo for their constant encouragement, co- operation and help. Words of gratitude are not enough to describe the accommodation and fortitude which they have shown throughout my endeavor.

Name Of The Student : Bidyasagar Behera
Signature Of The Student :
Registration No. : 230720100128
Place : Bhubaneswar
Date :

ABSTRACT

In today's interconnected world, security of wireless communication is paramount. This study focuses on implementing password protection in wireless communication using Cisco Packet Tracer, a simulation tool widely used for network modeling. The primary objective is to enhance the security of wireless networks by implementing robust password authentication mechanisms.

The study explores various authentication protocols supported by Cisco Packet Tracer, including WPA2 (Wi-Fi Protected Access 2) and WPA3, and their effectiveness in securing wireless communication. Through practical simulations and analysis, the study evaluates the strengths and weaknesses of different password protection methods, considering factors such as encryption strength, ease of implementation, and compatibility with existing network infrastructure.

The findings of this study provide valuable insights into enhancing the security of wireless communication using password protection mechanisms in Cisco Packet Tracer, thereby contributing to the broader discourse on network security in the digital age.

This paper delves into the implementation of password protection within wireless communication systems, employing Cisco Packet Tracer as a simulation platform. The primary focus is to fortify the security posture of wireless networks through the deployment of robust password authentication protocols.

The investigation encompasses a thorough exploration of authentication methodologies supported by Cisco Packet Tracer, including but not limited to WPA2 and WPA3, with an emphasis on their efficacy in thwarting unauthorized access attempts. Through a series of practical simulations and meticulous analysis, the study scrutinizes the strengths and vulnerabilities inherent in various password protection mechanisms.

Factors such as encryption robustness, implementation feasibility, and compatibility with existing network infrastructures are meticulously evaluated. The insights gleaned from this study serve to enrich the discourse surrounding wireless network security, offering practical guidance for bolstering the resilience of communication channels against potential threats in the digital landscape.

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	CERTIFICATE	I
	DECLARATION	ii
	ACKNOWLEDGEMENT	iii
	ABSTRACT	iv
CHAPTER – 1	INTRODUCTION	01
CHAPTER – 2	PROJECT OVERVIEW	02
CHAPTER – 3	ENVIRONMENTAL CHARACTERISTICS	03
CHAPTER – 4	OBJECTIVES & METHODOLOGY	04
CHAPTER – 5	NETWORK ARCHITECTURE	05 - 14
CHAPTER – 6	CONCLUSION	15
CHAPTER – 7	FUTURE SCOPE	16
	REFERENCE	

CHAPTER – 1 : INTRODUCTION

The introduction of password protection in wireless communication marked a significant milestone in ensuring the security and integrity of data transmitted over wireless networks. Before password protection, wireless communication was vulnerable to unauthorized access, data interception, and other security threats .

With the advent of password protection mechanisms, such as WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), and WPA2, users gained the ability to secure their wireless networks and devices effectively.

These password-based security measures introduced several key features like Authentication , Encryption and Access control.

The proliferation of wireless communication technologies has revolutionized the way we connect and interact with each other and the world around us. From smartphones to smart homes, wireless networks form the backbone of our modern digital ecosystem. However, this increased connectivity also brings forth significant security challenges, as wireless networks are inherently vulnerable to unauthorized access and data breaches.

In light of these challenges, the implementation of robust security measures is imperative to safeguard sensitive information and ensure the integrity of wireless communication. Password protection stands as one of the fundamental mechanisms in fortifying the security of wireless networks, serving as the first line of defense against unauthorized intrusion.

This paper aims to explore the implementation of password protection in wireless communication using Cisco Packet Tracer, a versatile simulation tool widely utilized for network modeling and analysis. By leveraging the capabilities of Cisco Packet Tracer, we seek to evaluate the efficacy of various password authentication protocols in enhancing the security posture of wireless networks.

Furthermore, we aim to elucidate the practical considerations involved in deploying password protection mechanisms, such as key management, configuration best practices, and compatibility with existing network infrastructure.

CHAPTER -2 : PROJECT OVERVIEW

Introduction:
Brief overview of the project's objectives and significance.Introduction to the challenges and vulnerabilities in wireless communication security.Importance of password protection as a security measure.Overview of Cisco Packet Tracer as the simulation tool of choice.

Literature Review:
Exploration of existing literature on wireless communication security and password protection mechanisms.Review of authentication protocols and encryption standards commonly used in wireless networks.Examination of previous studies and projects related to password protection using Cisco Packet Tracer.

Theoretical Framework:
Explanation of the theoretical principles underlying password protection in wireless communication.Discussion on encryption techniques, authentication methods, and access control mechanisms.Overview of password-based authentication protocols such as WPA2 and WPA3.

Methodology:
Description of the experimental setup using Cisco Packet Tracer.Explanation of the simulation scenarios designed to implement password protection in wireless networks.Overview of the parameters and variables considered in the experiments.

Implementation:
Step-by-step guide to implementing password protection mechanisms in Cisco Packet Tracer.Configuration of wireless access points, client devices, and authentication parameters.Demonstration of different password authentication protocols and their configurations.

Analysis:
Evaluation of the effectiveness of password protection mechanisms in securing wireless communication.Assessment of the strengths and weaknesses of various authentication protocols.Analysis of simulation results, including security metrics, performance indicators, and practical considerations.

Results and Discussion:
Presentation of the findings from the experiments conducted in Cisco Packet Tracer.Discussion on the implications of the results and their relevance to real-world wireless network security.Comparison of different password protection mechanisms and their suitability for specific use cases.

CHAPTER- 3 : ENVIRONMENTAL CHARACTERISTICS

Cisco Packet Tracer - Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface.

Switch PT- A network switch is a piece of hardware that facilitates computer networking. It accepts physical connectors from computers and other devices on a network and then receives and forwards data using packet switching. Connecting various devices to the ports on a network switch allows them to interact with each other through data transfer within the switch. Most networking devices also connect to the internet, allowing the devices to obtain internet access through the switch ports.

Router PT - The router is a physical or virtual internetworking device that is designed to receive and forward data packets between computer networks. A router examines a destination IP address of a given data packet, and it uses the headers and forwarding tables to decide the best way to transfer the packets.

Static Routing:- Static routing is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from dynamic routing traffic. Static Routing is also known as non-adaptive routing which doesn't change routing table unless the network administrator changes or modify them manually. It exploits the paths between the two ways, and they can't automatically be updated. Thus you must manually reconfigure static routes when the network changes. It uses low bandwidth as compared to the dynamic maps. It can be used in those areas where the network traffic is predictable & designed. It can't be used in the vast and continuously changing network because they can't react to the network change.

Dynamic Routing - Dynamic routing, also called adaptive routing, is a process where a router can forward data via a different route for a given destination based on the current conditions of the communication circuits within a system. Dynamic routing is also known as adaptive routing which change routing table according to the change in topology. Dynamic routing uses complex routing algorithms and it does not provide high security like static routing. When the network change(topology) occurs, it sends the message to router to ensure that changes then the routes are recalculated for sending updated routing information. Dynamic routing uses multiple algorithms and protocols. The most popular are Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).

Fast Ethernet Modules - The Gigabit Ethernet port adapter offers an additional choice of high-speed LAN connection to the Cisco 7200VXR basically it is used to connect router with switch. 7 | Page Fast Ethernet network module with TX connector, Cisco product number NM-1FE-TX. This module provides an RJ-45 connector for direct connection to 100BASE-T Ethernet networks. Fast Ethernet network module with FX connector, Cisco product number NM-1FE-FX. This module provides a duplex SC-type fibre-optic port for direct connection to 100BASE-FX Ethernet networks.

CHAPTER-4 : OBJECTIVES & METHODOLOGY

OBJECTIVES

The primary objective of password protection in wireless communication is to secure the communication channel and prevent unauthorized access to sensitive information or resources. Here are some key objectives:

Authentication: Password protection ensures that only authorized users can access the wireless network or device. By requiring a password, the system verifies the identity of the user before granting access.

Integrity: Password protection helps ensure that data transmitted over the wireless network remains unchanged and unaltered during transmission. It helps detect any unauthorized modifications or tampering attempts.

Access Control: Passwords enable administrators to control who can access the network or specific resources within the network. By setting up unique passwords for different users or devices, administrators can enforce access policies effectively.

Prevention of Unauthorized Access: Password protection acts as a barrier against unauthorized access attempts by malicious users or entities. It reduces the risk of data breaches, unauthorized use of network resources, and other security threats.

METHODOLOGY

Requirement Analysis: When designing a Password Protection in Wireless Communication using Cisco technologies, several requirements need to be considered to ensure the system meets the specific needs and standards of the Wireless Communication

.

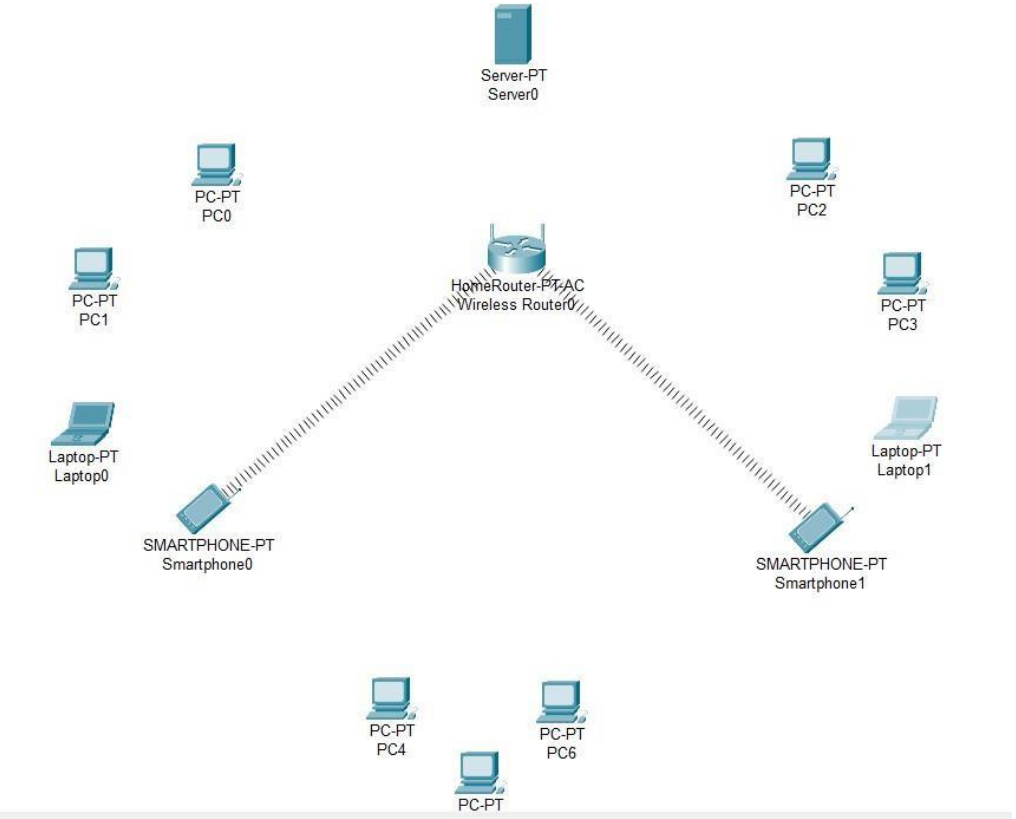
Network Design: Designing the network topology using Cisco Packet Tracer involves creating a blueprint of how different network devices are interconnected to form a functional network.

Subnetting:Subnetting is a crucial aspect of network design that involves dividing a larger network into smaller subnetworks or subnets.

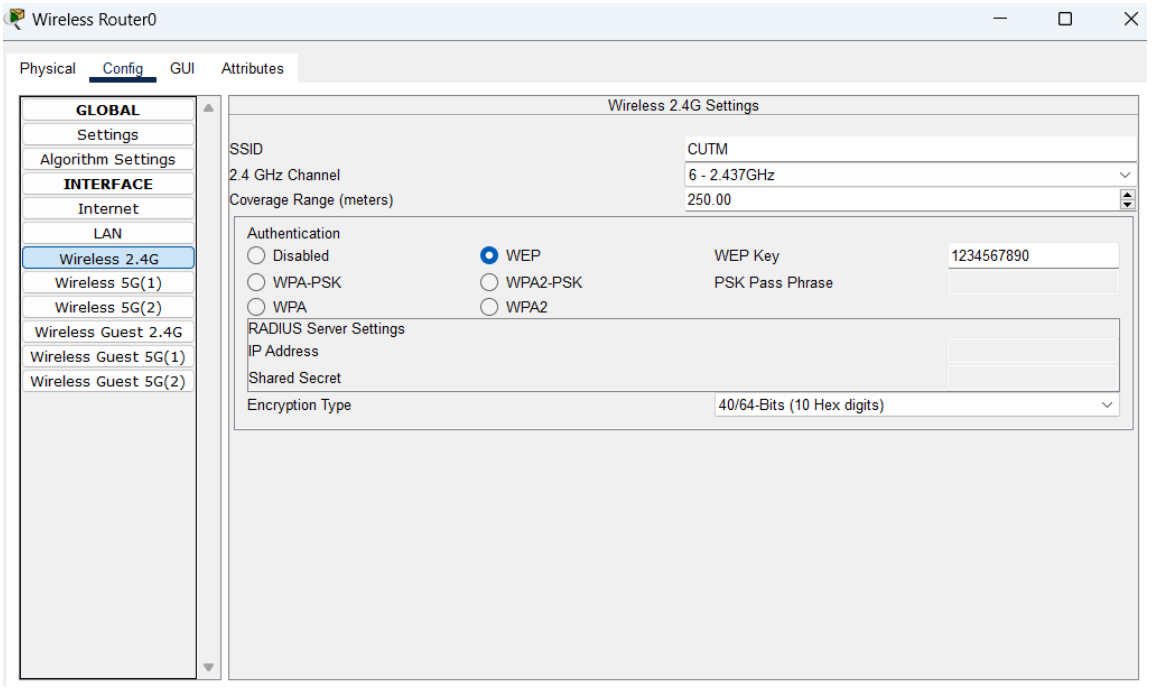
Implementation: During the implementation phase of the Password Protection in Wireless Communication design, we focused on configuring routers, servers, PC, Laptop and other network devices based on the designed topology. The goal was to ensure seamless integration and functionality across all network components.

Chapter – 5 : NETWORK ARCHITECTURE

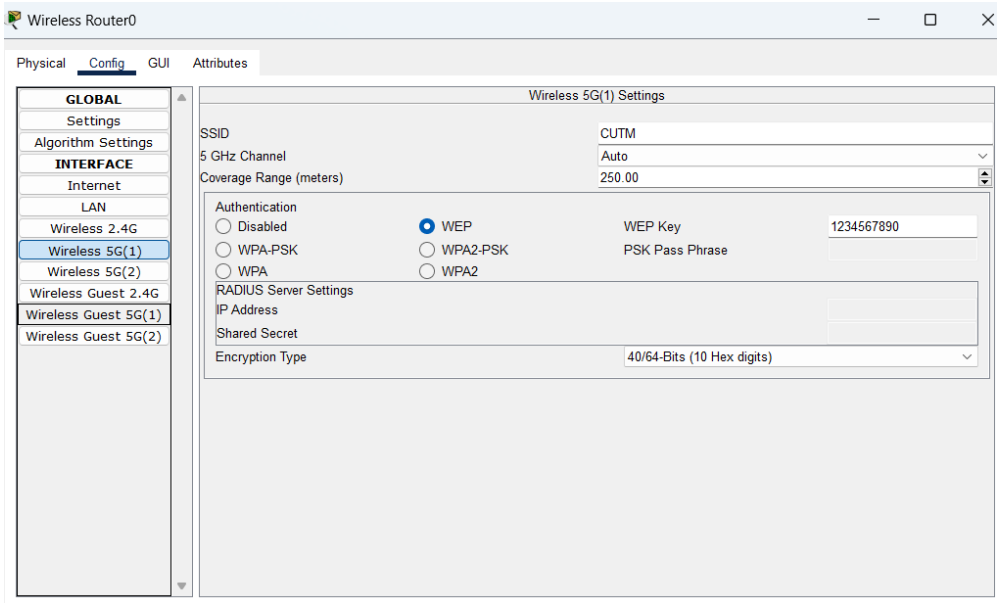
1. Open Cisco Packet Tracer.
2. Drag and Drop 7 PCs , 2 Laptop , 2 Smart Phone , 1 Server and 1 Home Router.

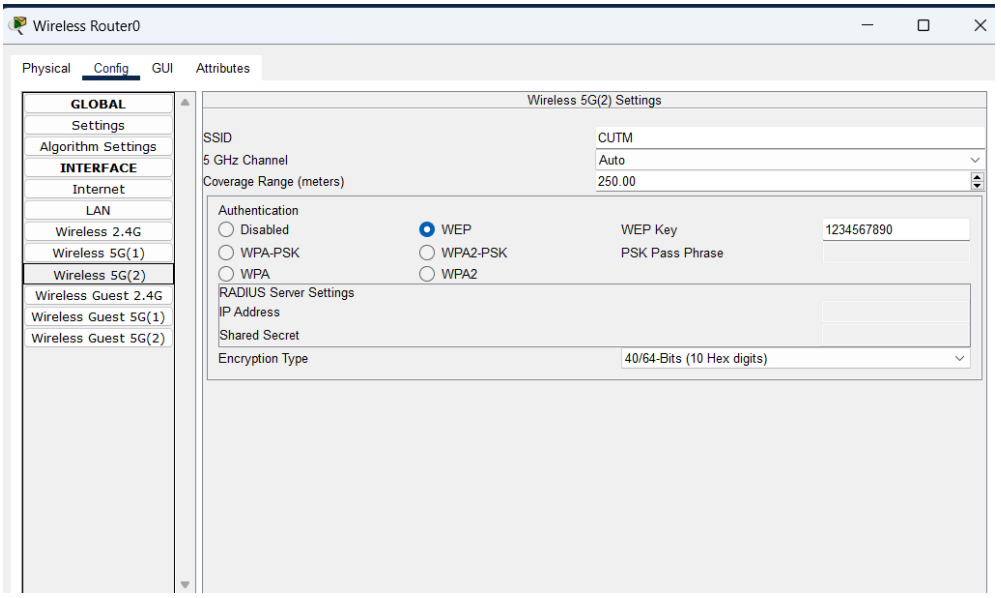


3. Click on Home Router and go to config section.
4. Now go to the Wireless 2.4G and change the SSID .
5. Then change the Authentication to WEP and put the WEP key.

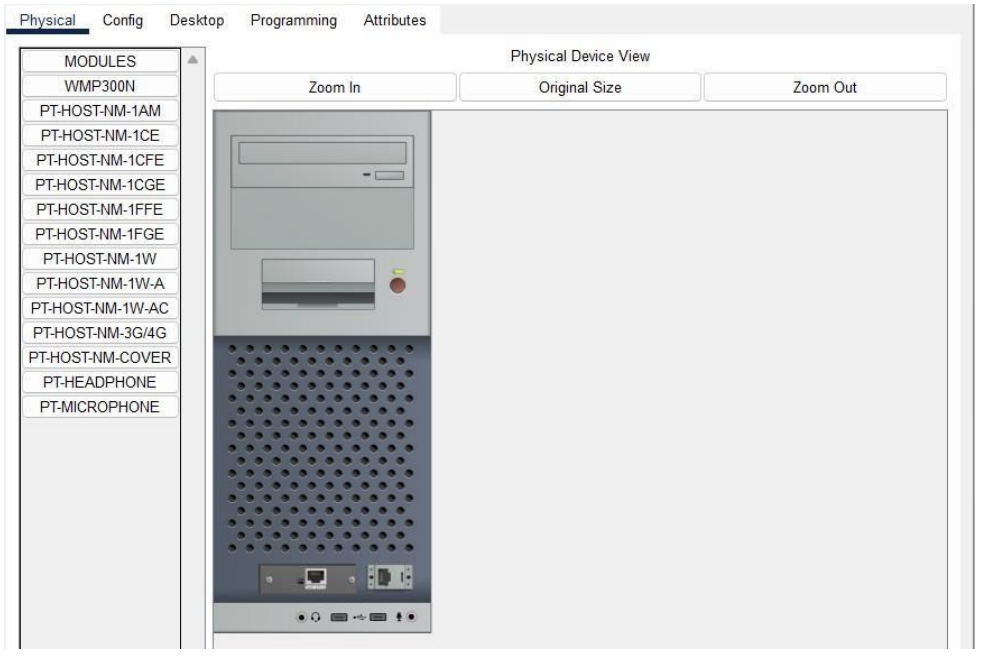


6. Continue the Same Process for Wireless 5G (1) & Wireless 5G (2).

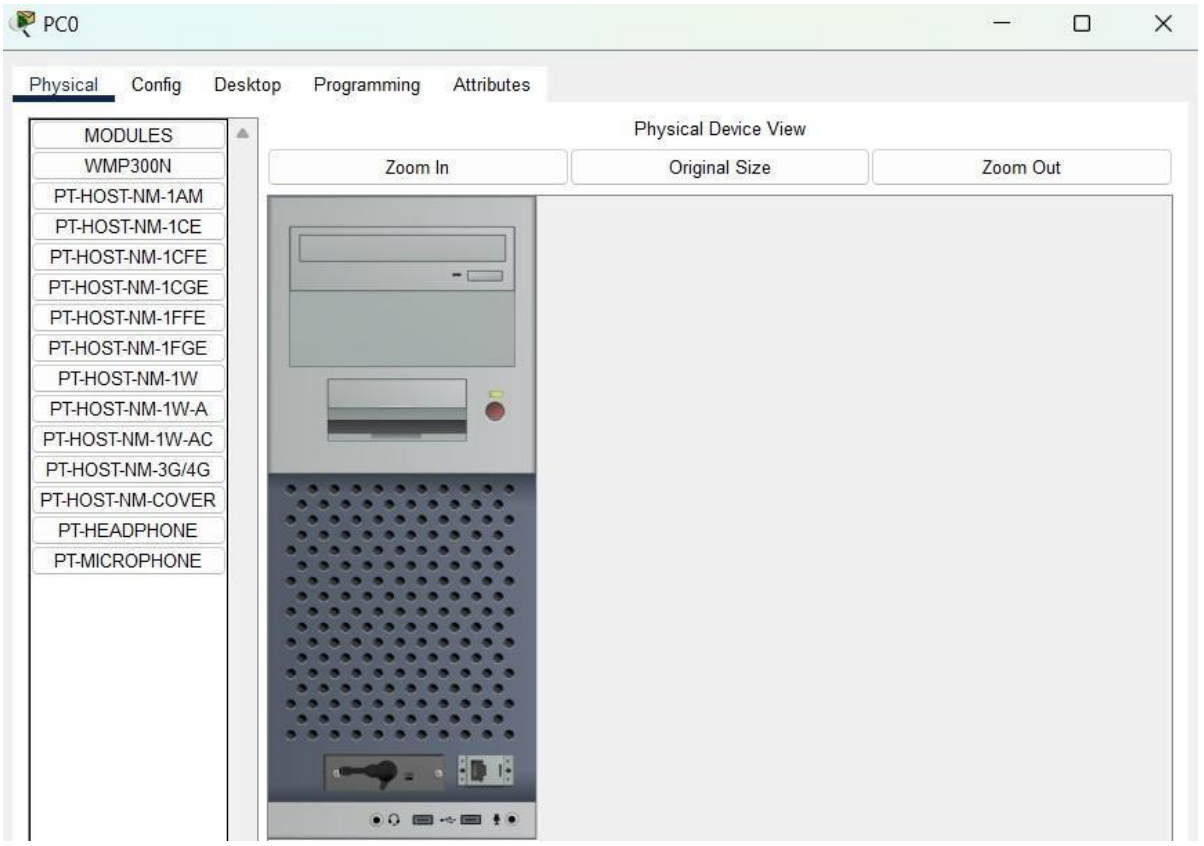




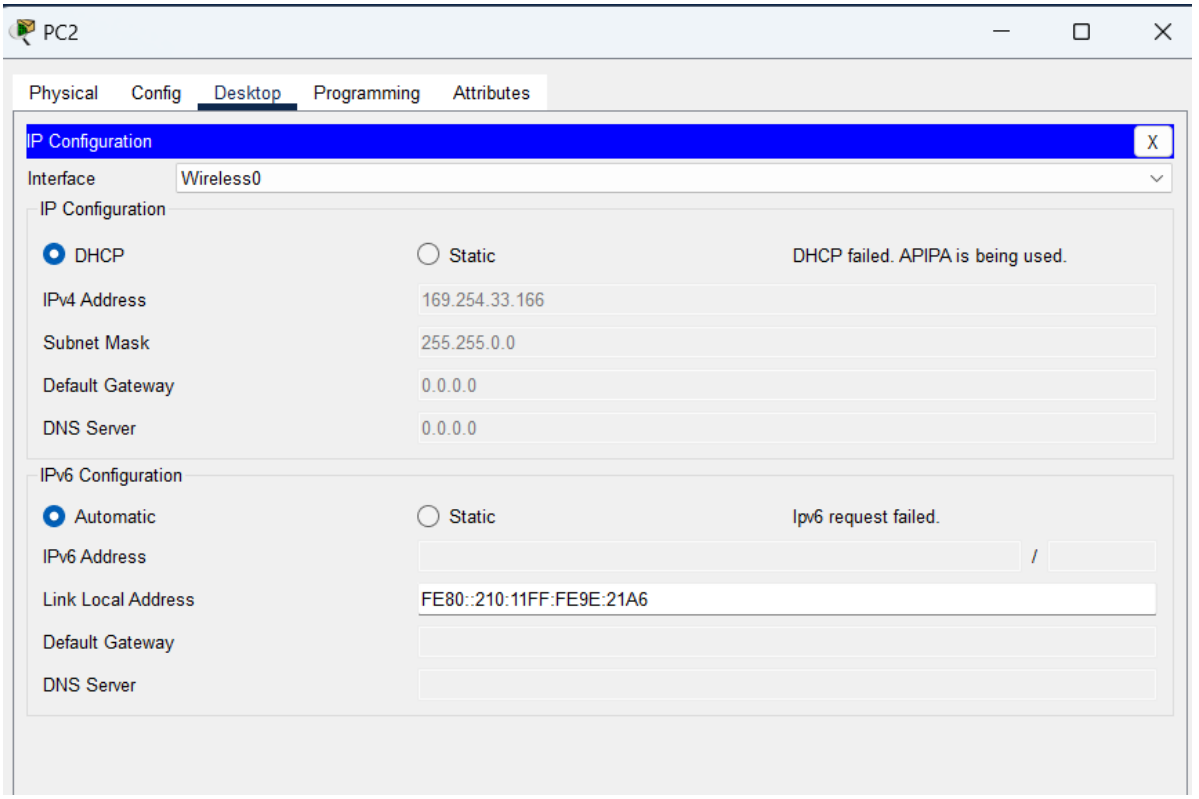
7. Now Click on the PC.



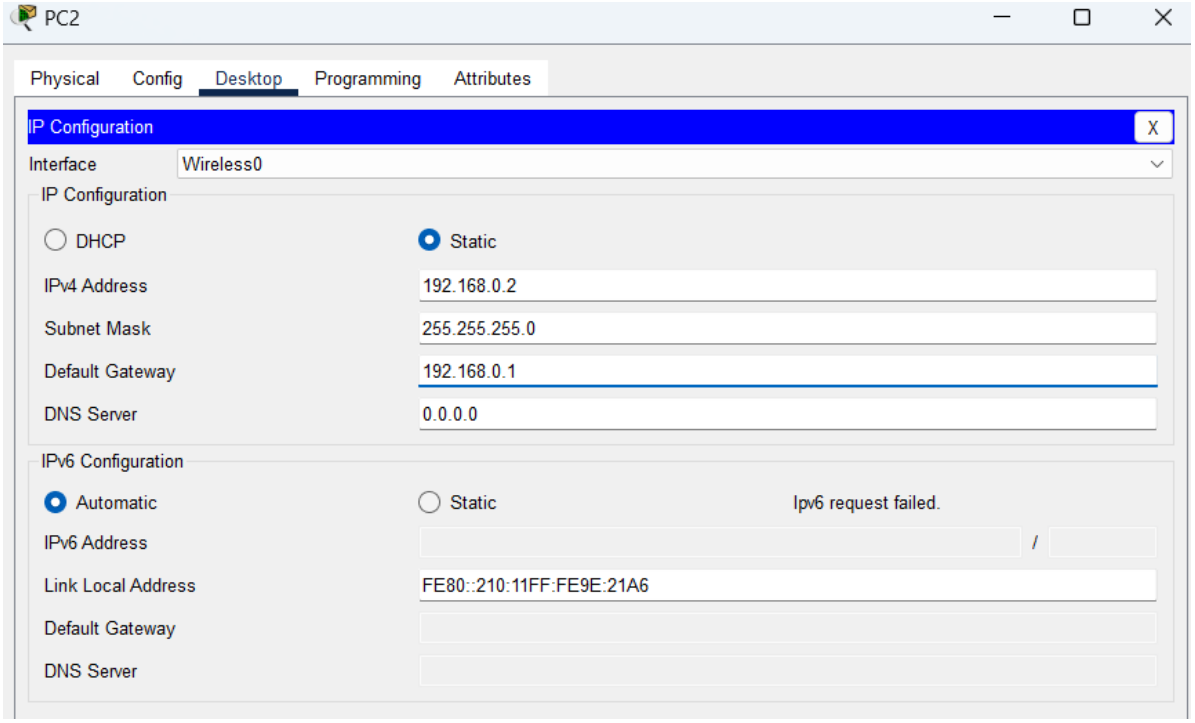
8. Here we See that PC has RJ 45 Port . It can't transmit wireless signal.
9. So, In the place of RJ 45 put the WMP300N port. First Power off the PC the do all the changes.



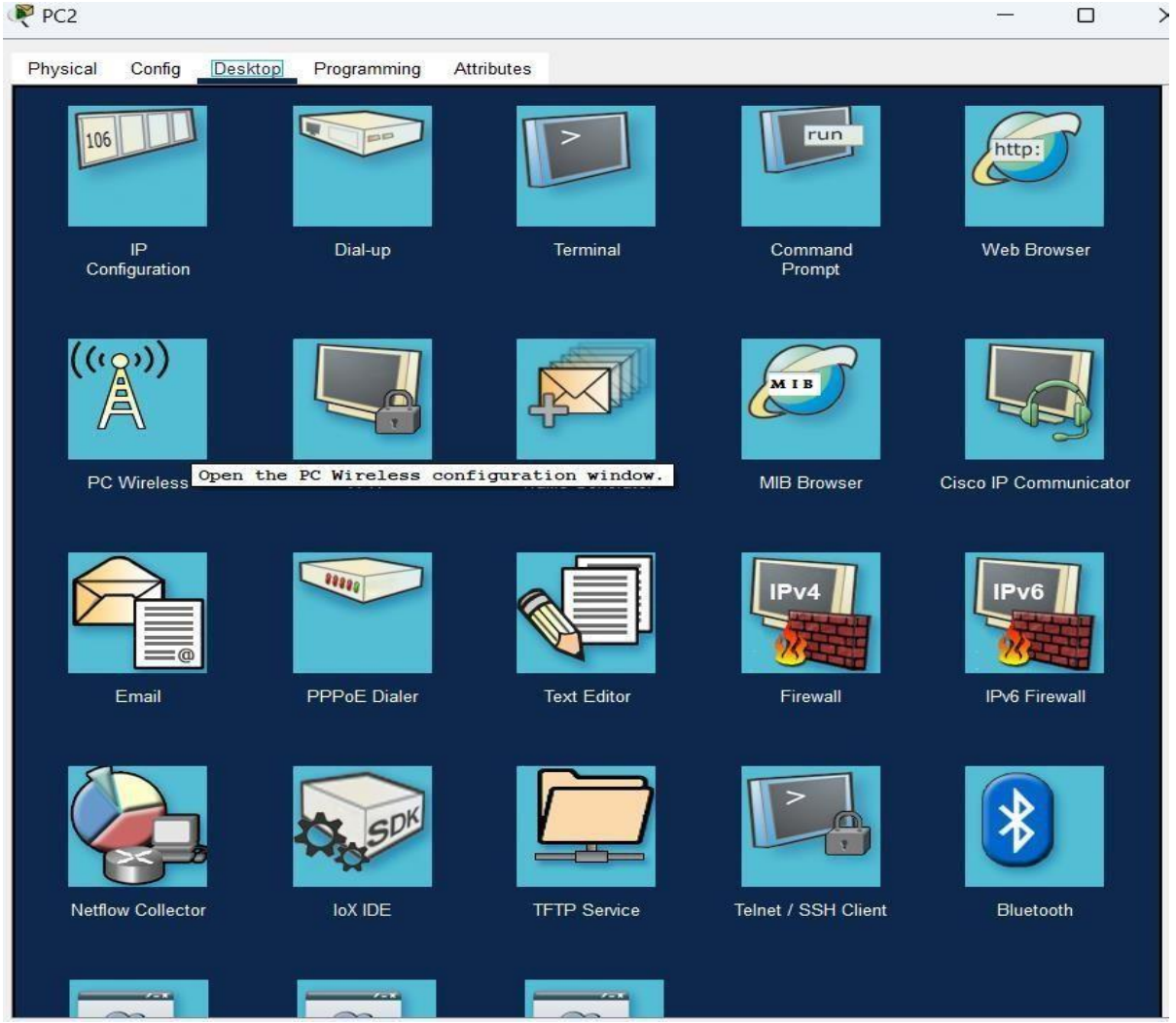
10. After Replacing the port now we have to assign the IP Address , Subnet Mask and Default Gateway of that System. By default Our Home Router provide the IP Address using DHCP .



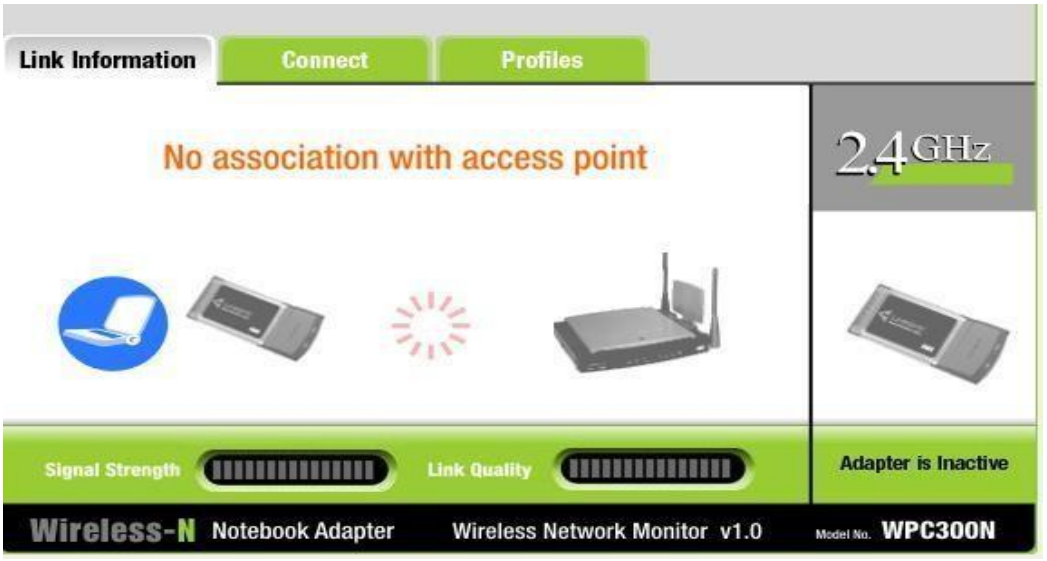
11. So we have to change DHCP to Static . After that provide all the things.



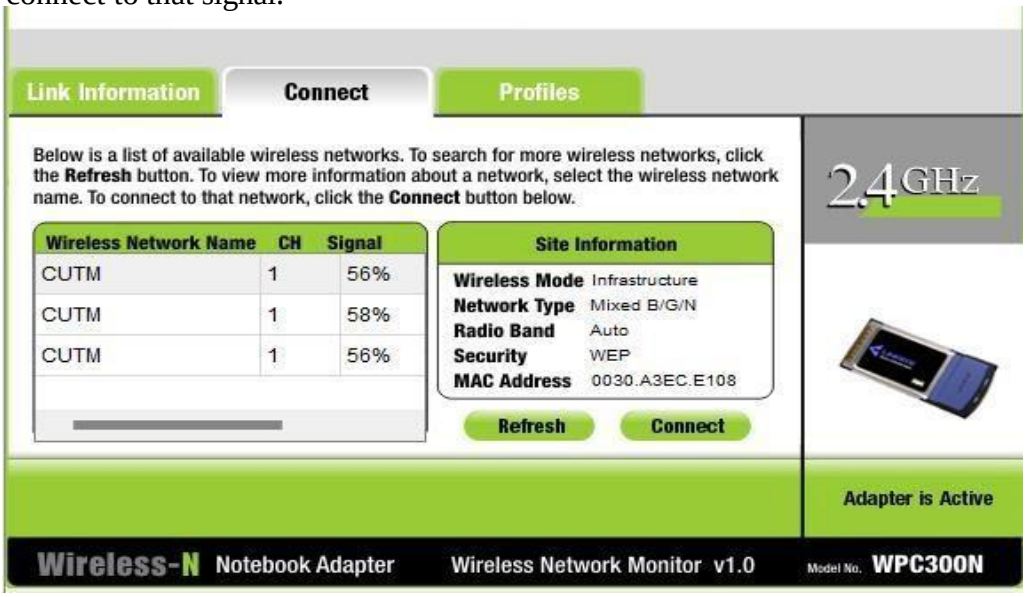
12. After Providing the IP Address now go to the Desktop option Then select the PC Wireless .



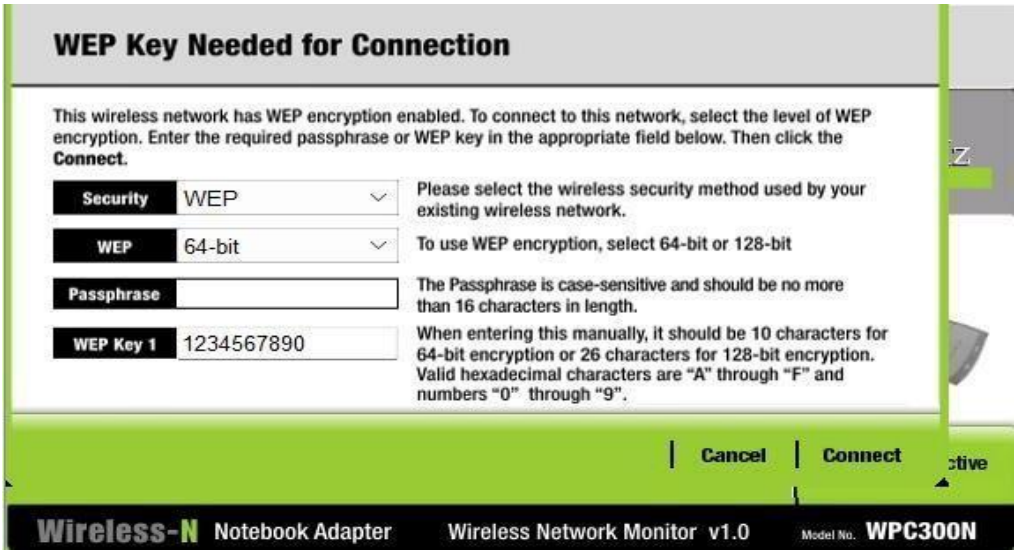
13. Here we See that No Association with Access point is written



14. Then we go to the Connect option to Establish the Between PC and Router . First we to Refresh the Site Information so that we can see all the Available signal then select the Signal and connect to that signal.

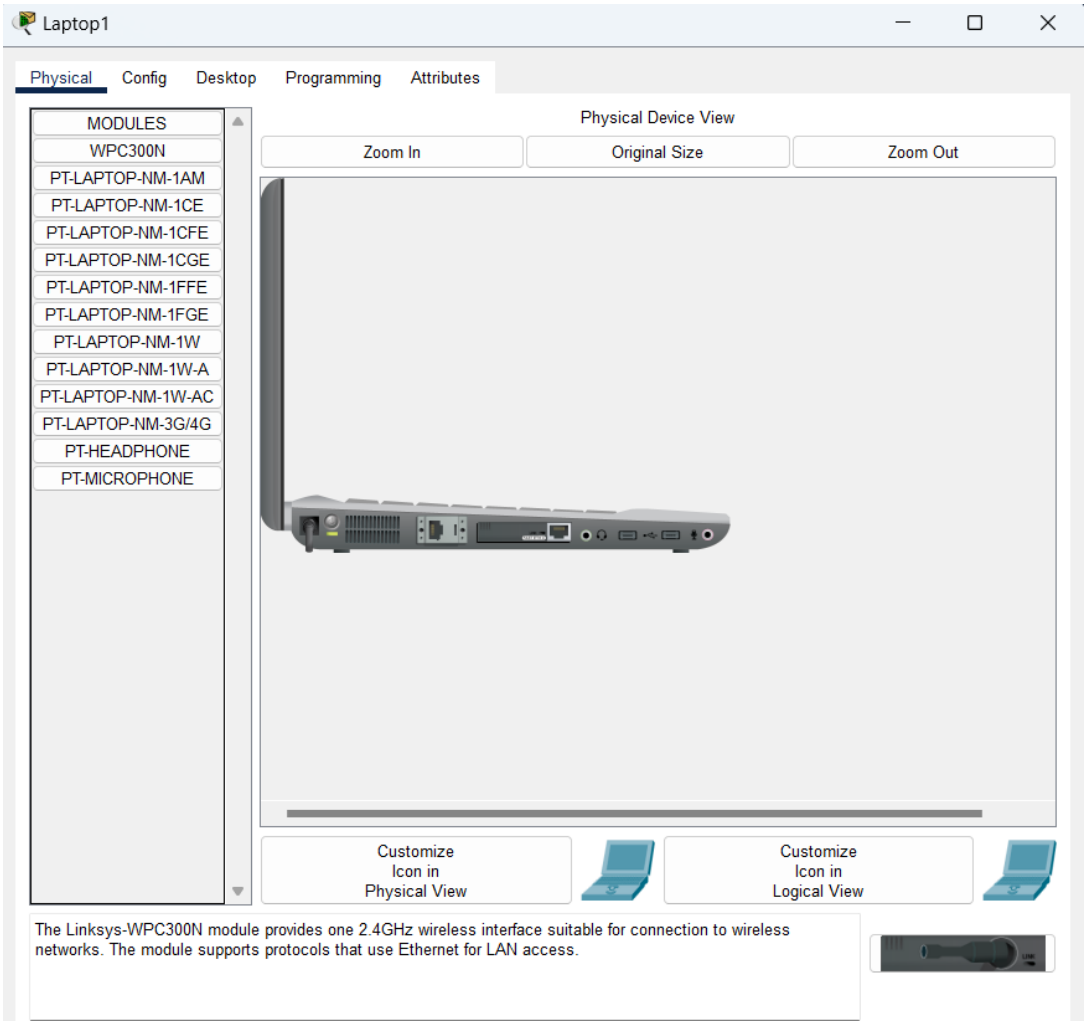


15. Then Type the Correct Password to connect to that signal.

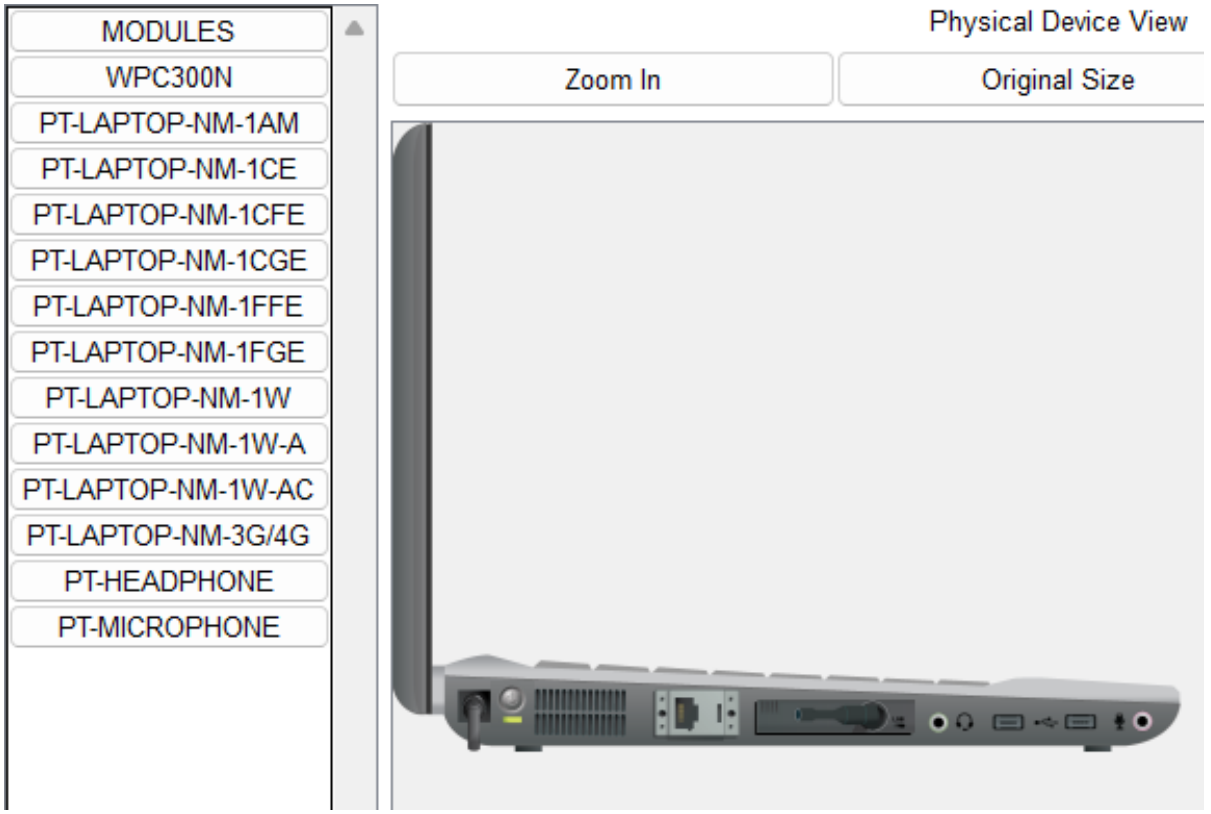


16. After Type the Correct password it show that You have successfully connected to the Access point.

17. Now we set up the connection for the Laptop.
18. Here we See that Laptop has the Ethernet port . So we replace the Ethernet port with WPC300N port for wireless communication.

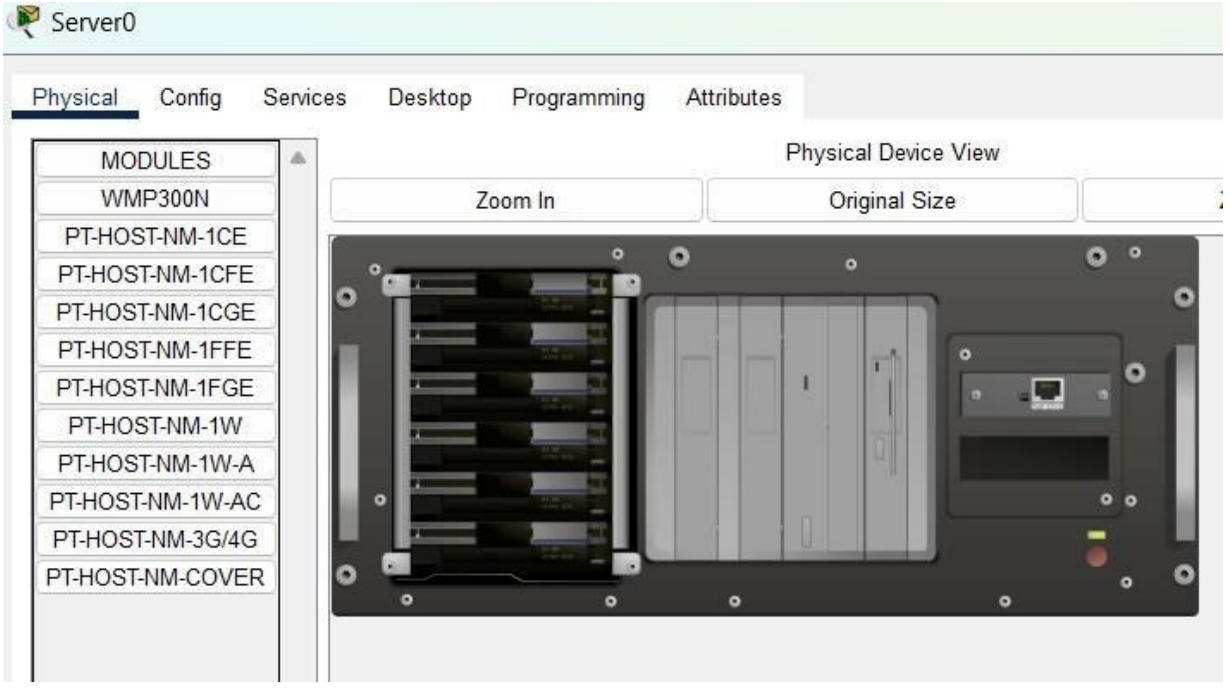


19. The process is same for as Pc , First we Power off the Laptop after that remove the Ethernet port , in that place the WPC300N is placed . Then Power On the Laptop.

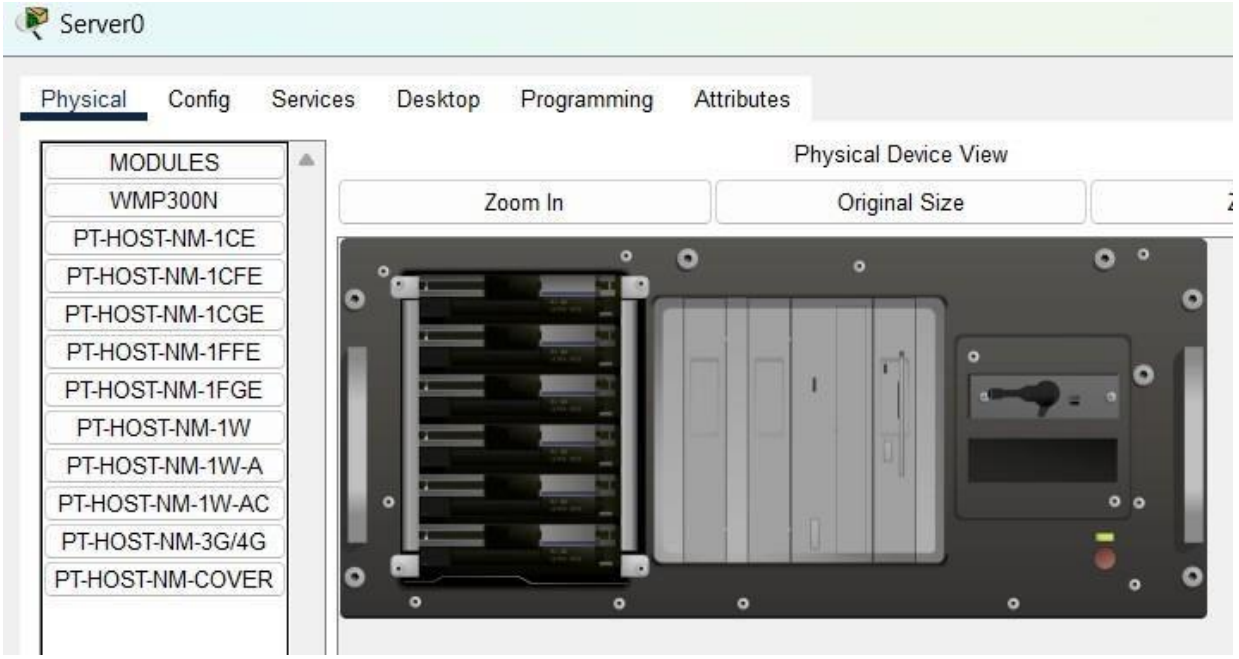


20. After that we provide the IP Address , Subnet Mask and Default Gateway. Then we able to connect to the Router. The Process is same as PC.

21. Now set up the Server. Here we that Server is also not able to communicate Wirelessly. So our first task is remove the Ethernet port in place we put the WPC300N port for wireless transmission

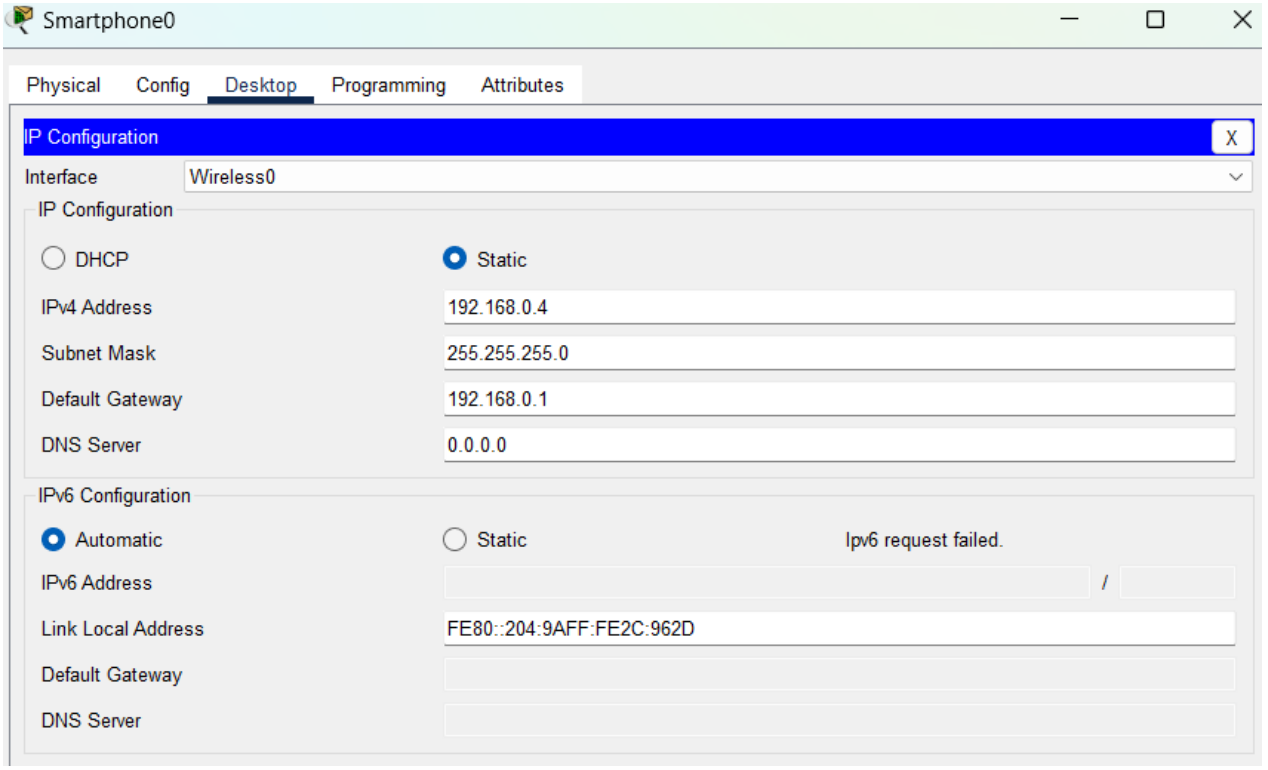


22. Here First we Power off the Server. After that Remove the Ethernet port , in place of Ethernet port put the WPC300N port.

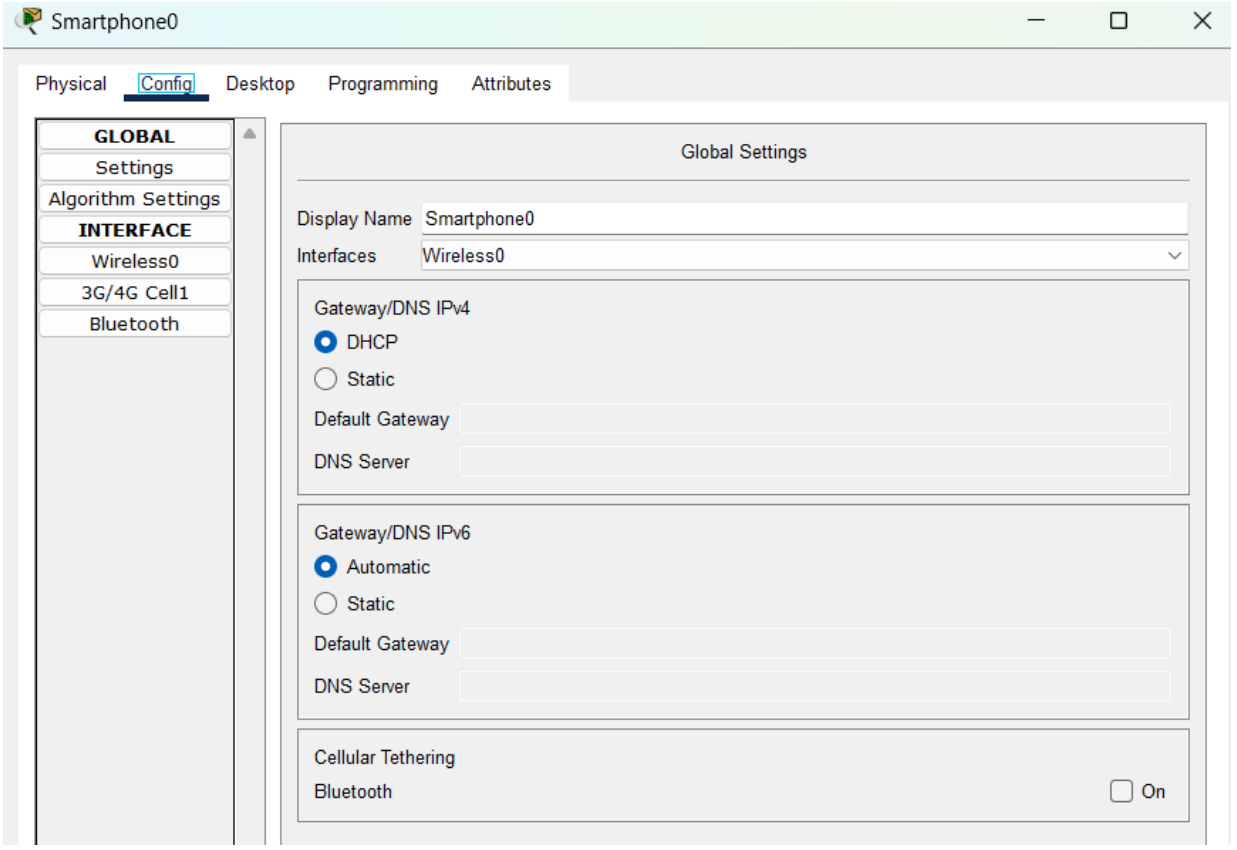


23. Then assign the IP Address , Subnet Mask and Default Gateway for the Server . Then Connect the Server to the Router.

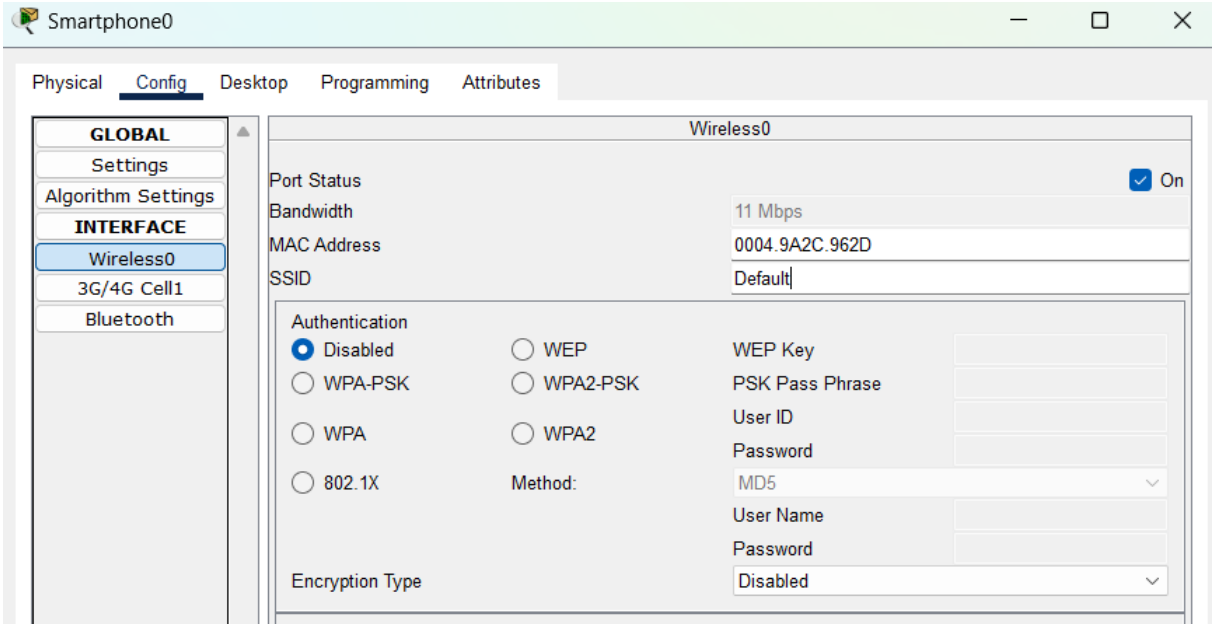
24. Now set up the Smart Phone . First we assign the IP Address , Subnet Mask and Default Gateway for the Smart Phone.



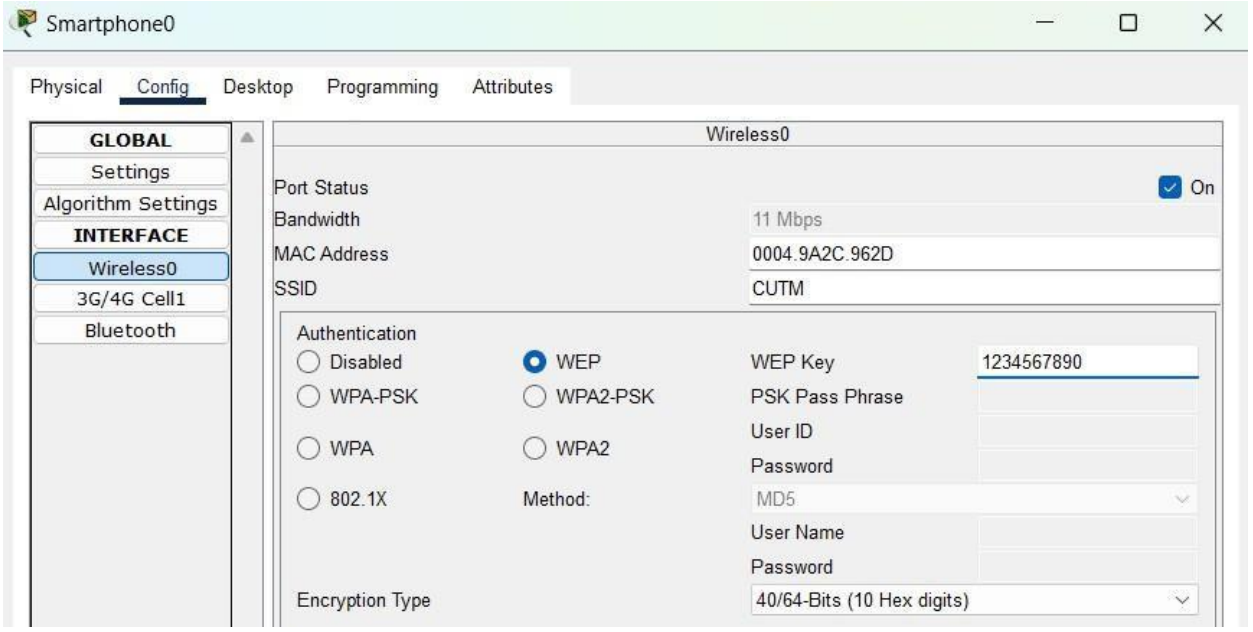
25. For Connecting to the Router , First go to the config option.



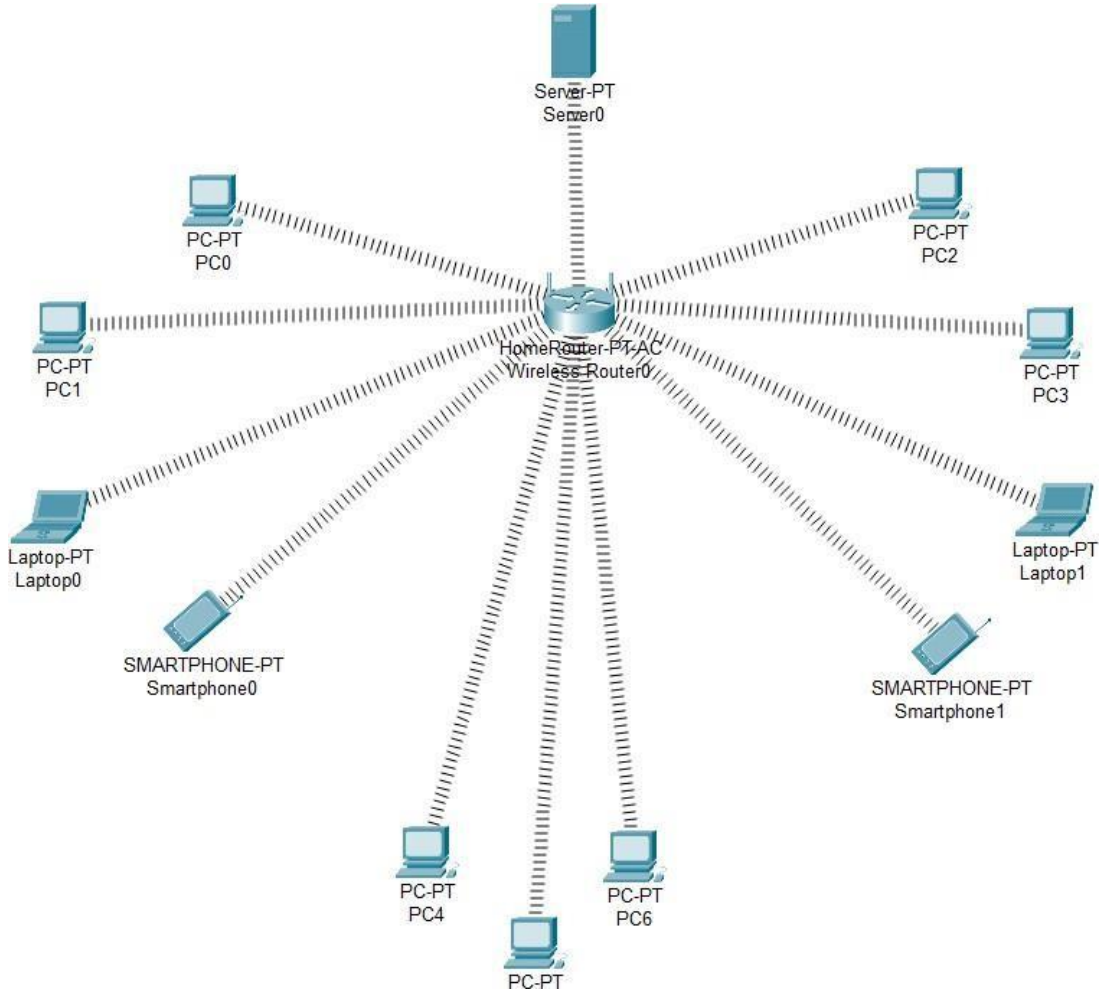
26. Then Go to the Wireless0 option , Here we see the name of the SSID is Default . So first we change the name of the SSID Default to our SSID then go to Authentication Section and choose the WEP.



27. Here we change the SSID default to the CUTM and also put the WEP Key . After the we can see our Devices are connected wirelessly to the Router.



28. Here our all Devices are Successfully connected to the Router. And the can also successfully transmit the data over the Network.



Chapter – 6 : CONCLUSION

In conclusion, password protection is an essential component of securing wireless communication networks. It serves as the first line of defense against unauthorized access, ensuring the confidentiality and integrity of transmitted data. By following best practices, such as using strong, unique passwords, regularly updating passwords, and employing additional security measures like two-factor authentication, the risk of unauthorized access can be significantly reduced. However, it is crucial to remain vigilant, as cyber threats continually evolve.

Therefore, ongoing monitoring, regular security audits, and staying informed about the latest security protocols are essential to maintaining the integrity and security of wireless communication networks. By adhering to these principles, users and organizations can effectively safeguard their wireless networks from potential security breaches.

Furthermore, Cisco Packet Tracer enables the simulation of various attack scenarios, allowing administrators to test the resilience of their password protection measures. By conducting penetration tests and vulnerability assessments within the simulated environment, administrators can identify potential weaknesses and refine their security configurations accordingly.

In essence, the implementation of password protection in wireless communication using Cisco Packet Tracer is not merely a procedural task but a strategic imperative for safeguarding network integrity and preserving data confidentiality. It empowers network administrators to proactively defend against evolving cyber threats and uphold the trust and reliability of their wireless infrastructure.

Chapter – 7 : FUTURE SCOPE

The future scope of password protection in wireless communication using Cisco Packet Tracer is poised for significant advancements in several key areas:.

Advanced Encryption Standards: With the continuous evolution of encryption standards, future versions of Cisco Packet Tracer may incorporate support for emerging encryption algorithms and protocols. This includes advancements in encryption strength, key management, and resistance to cryptographic attacks, ensuring robust protection for wireless communications.

Multi-factor Authentication (MFA): As cyber threats become more sophisticated, the adoption of multi-factor authentication (MFA) is likely to increase. Future iterations of Cisco Packet Tracer may include functionalities for implementing MFA mechanisms, such as combining passwords with biometric authentication, smart cards, or token-based authentication, to enhance the security of wireless networks.

REFERENCE

Website Referred :

- https://youtu.be/Jp0hhYpNSYY?si=gU-R9ZFLy59Y1_Tt
- https://youtu.be/fWVieSvBaM?si=kZPfdrQaYqrUZcI3
- https://www.youtube.com/watch?v=5RenxY9RyuY&list=PLraEtET93taeFgGWxCkDz7qgbToXZ7PCx

Books Referred :

Computer Networks – Andrew S Tanenbaum , 4th Edition , ELSEVIER

ASSESSMENT

Internal:

SL NO	RUBRICS	FULL MARK	MARKS OBTAINED	REMARKS
1	Understanding the relevance, scope and dimension of the project	10		
2	Methodology	10		
3	Quality of Analysis and Results	10		
4	Interpretations and Conclusions	10		
5	Report	10		
	Total	**50**		

Date: **Signature of the Faculty**

COURSE OUTCOME (COs) ATTAINMENT

➢ **Expected Course Outcomes (COs):**

(Refer to COs Statement in the Syllabus)

_____

_____

_____

_____

➢ **Course Outcome Attained:**

How would you rate your learning of the subject based on the specified COs?

☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

1 2 3 4 5 6 7 8 9 10

LOW HIGH

➢ **Learning Gap (if any):**

_____

_____

_____

_____

➢ **Books / Manuals Referred:**

_____

_____

_____

_____

Date: **Signature of the Student**

➢ **Suggestions / Recommendations:**

(By the Course Faculty)

_____

_____

_____

_____

Date: **Signature of the Faculty**