**HOME WIRELESS NETWORK SYSTEM**

**18CSS202J - COMPUTER COMMUNICATIONS**

**Mini Project**

**Submitted by**

**Pranav Vangavety (RA2011003010105)**

**Mohnaa Ghosh (RA2011003010108)**

**Krishitaa Balamurali (RA2011003010115)**

**Putta Sri Naga Sanjana (RA2011003010123)**

**Aaryan G Sharma(RA2011003010134)**

Under the guidance of

**Mr. Bibin Christopher**

(Assistant Professor, Department of Computer Science and Engineering)

**BACHELOR OF TECHNOLOGY**

**in**

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**of**

**FACULTY OF ENGINEERING AND TECHNOLOGY**

****

**SRM INSTITUTE OF SCIENCE AND TECHNOLOGY KATTANKULATHUR- 603 203**

****

***SRM INSTITUTE OF SCIENCE AND TECHNOLOGY***

S.R.M. NAGAR, KATTANKULATHUR -603 203

# BONAFIDE CERTIFICATE

**Register No.**

*Certified to be the bonafide record of work done by*

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*, B. Tech Degree course in the Practical* **18CSS202J-Computer Communications** *in SRM Institute of Science and Technology, Kattankulathur during the academic year2021-2022***.**

## Date: Lab Incharge

Submitted for University Examination held in \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ SRM Institute of Science and Technology, Kattankulathur.

## **Examiner-1 Examiner-2**

**CERTIFICATE**

This is to certify that the project entitled “**Home wireless Network System**” carried out by

**“Pranav Vangavety (RA2011003010105) , Mohnaa Ghosh (RA2011003010108), Krishitaa Balamurali(RA2011003010115) ,**

**Putta Sri Naga Sanjana (RA2011003010123) , Aaryan G Sharma**

**(RA2011003010134)”**

under my supervision at Department of Computing and Technology, SRM Institute of Science and Technology, Kattankulathur, Chennai.

The work is original, as it has not been submitted earlier either in part or full for any purpose before.

**Mr.Bibin Christopher**

**(Asst. Professor)**

**DECLARATION**

I, hereby declare that the work presented in this dissertation entitled “**Home wireless Network System**” has been done by me and my team, and this dissertation embodies my own work.

**Approved By:**

**Mr.Bibin Christopher**

**ACKNOWLEDGEMENT**

We would like to thank **Mr. Bibin Christopher** (Asst.Professor) who has been a great inspiration and who have provided sufficient background knowledge and understanding of this subject.

Our humble prostration goes to him, for providing all the necessary resources and environment, which have aided us to complete this project successfully.

**Home wireless Network System**

**CC Mini Project**

**Literature Survey**

● To complete the project I have gone through some youtube videos and a few articles where I came to know about how to set up a wireless network system.

● This is the link for a youtube video (https://youtu.be/uJnveEz8sFI).

● This the website I have referred to make

(https://www.geeksforgeeks.org/setting-up-a-basic-home-network using-packet-tracer/)

**Introduction**

● We are working on home wireless network design.

● Our aim is to access home appliances such as door lock, garage gate,ac and bulb etc.

● All appliances can be accessible from laptop.

● Access to appliances can be done after entering user id and password for particular device.

**Benefits of Wireless Home Network System**

● Increased efficiency. Improved data communications lead to faster transfer of information within businesses and between partners and customers.

● Access and availability.

● Flexibility.

● Cost savings.

● New opportunities.

● Security.

● Installation problems.

● Coverage.

**Implementation of Wpa &Wpa2 in Network System**

WPA2 introduces the use of AES (Advanced Encryption Standard) algorithms and CCMP (Counter Cipher Mode with Block-Chaining Message Authentication Code Protocol) to tighten the security of both home networks and business enterprises. Dynamic encryption keys are distributed securely after a user logs in or provides a valid digital certificate. WPA2 can be implemented in one of two modes:

● **Pre-Shared Key (PSK) Mode –** For home Wi-Fi networks, the owner defines the encryption passphrase on the wireless router and other APs. That passphrase must then be entered by users when connecting to the network.

● **Enterprise Mode –** Organisations that want government-grade wireless security should use Wi-Fi Protected Access 2 Enterprise (WPA2-Enterprise). To improve the resiliency of mission-critical networks, WPA2-Enterprise was recently enhanced with Protected Management Frames, which further steal WPA2 against eavesdropping and packet forging. All Wi-Fi Certified devices support WPA2 for added protection.

● When WPA2 is enabled with its strongest encryption option,

anyone else within range of the network might be able to see the traffic, but it is scrambled with the most up-to-date encryption standards.

WPA with TKIP (WPA-TKIP): This is the default choice for old routers that don't support WPA2.

● WPA with AES (WPA-AES): AES was first introduced before the WPA2 standard was completed, although few clients supported this mode.

● WPA2 with AES (WPA2-AES): This is the default choice for newer routers and the recommended option for networks where all clients support AES.

● WPA2 with AES and TKIP (WPA2-AES/TKIP): Routers need to enable both modes if any clients do not support AES. All WPA2 capable clients support AES, but most WPA clients do not.

Limitations

● Most routers support both WPA2 and a separate feature called Wi-Fi Protected Setup. While WPS is designed to simplify the process of setting up home network security, flaws in how it was implemented limit its usefulness.

● With WPA2 and WPS disabled, an attacker needs to determine the WPA2 PSK that the clients use, which is a time-consuming process. With both features enabled, an attacker only needs to find the WPS PIN to the clients to reveal the WPA2 key. This is a simpler process. Security

advocates recommend keeping WPS disabled for this reason.

● WPA and WPA2 sometimes interfere with each other if both are enabled on a router at the same time, and can cause client connection failures.

**Modules**

***Server PT***

Switch port Security is a network security feature that associates specific MAC addresses of devices(such as PCs) with specific interfaces on a switch. This will enable you to restrict access to a given switch interface so that only the authorised devices can use it.



***Switch***

Switch allows us to set IP addresses on interface level. The IP address assigned on the interface is used to manage that particular interface. To manage the entire switch we have to assign an IP address to VLAN1( Default VLAN of switch). We also have to set the default gateway IP address from global configuration mode.

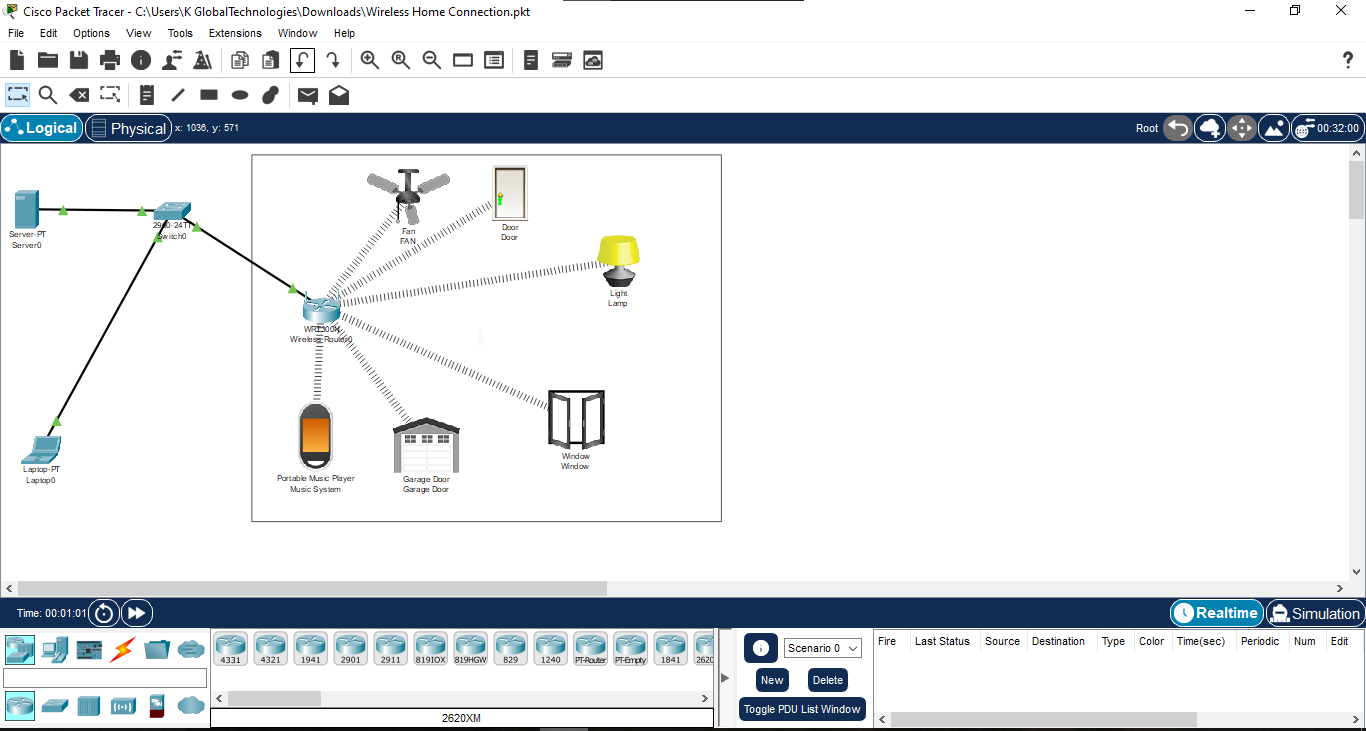


***Wireless Router***

● In this activity, you will configure a Linksys wireless router, allowing for remote access from PCs as well as wireless connectivity with WPA2 security. You will manually configure PC wireless connectivity by entering the Linksys router SSID and password.



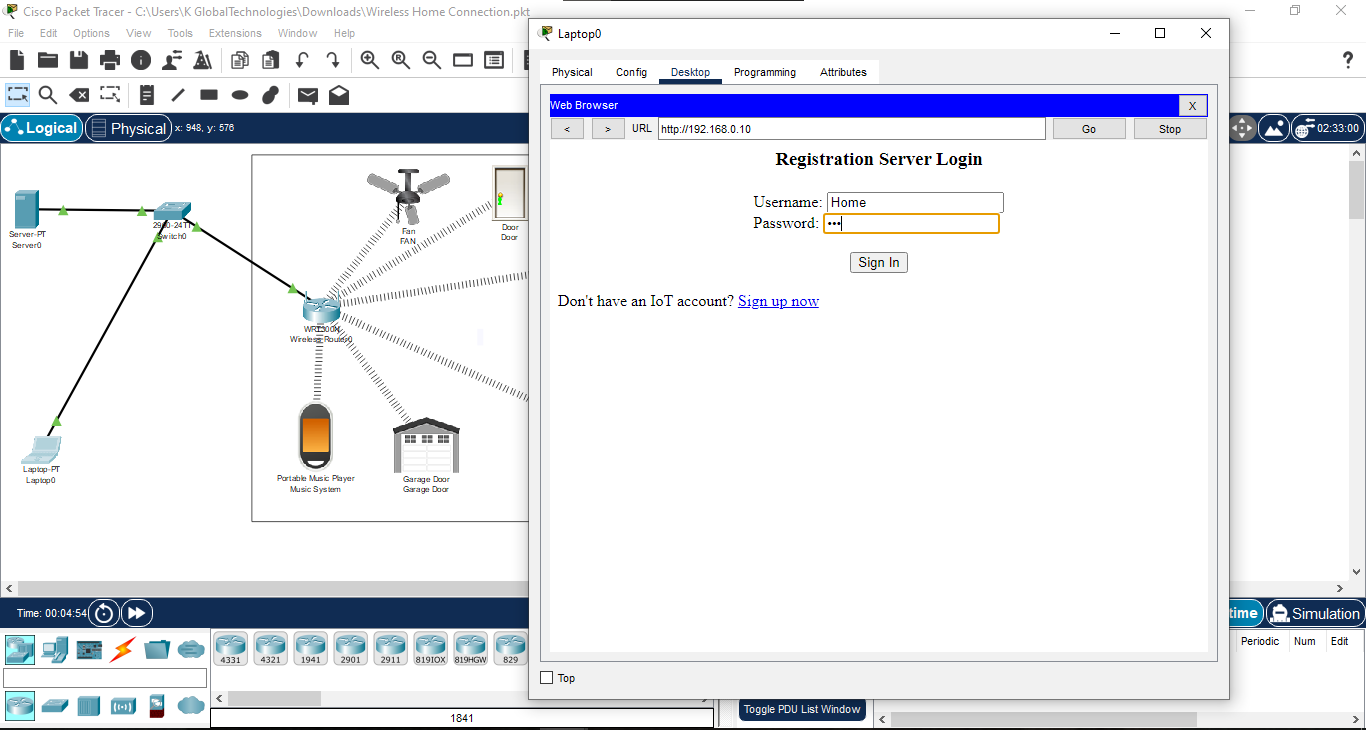
***Topology***

****

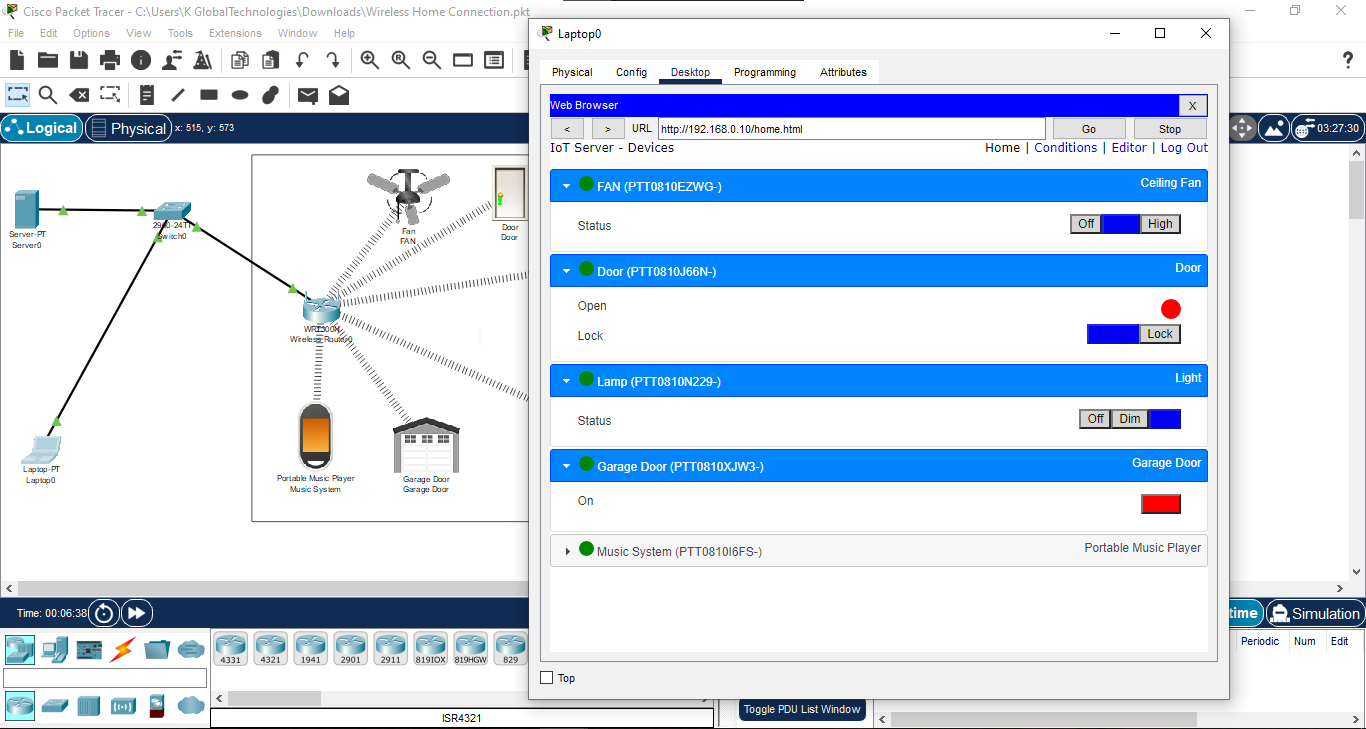
**Result**

● We can access appliances from the laptop in which we have to enter the ip address of the server.

● And enter Username(Home) and password (123) to get access to the door,garage,fan and window.



●

****

**Conclusion**

Wireless communications globally is something that people can expect as technology advances. Wireless communications have a lot of benefits and can make the world a lot more efficient. It does have concerns though as with every other new advancement that is made in today's world.

**Reference**

● We have referred to a youtube video to learn wpa configuration (https://youtu.be/uJnveEz8sFI).

● This the website we have referred to make

(https://www.geeksforgeeks.org/setting-up-a-basic-home-network using-packet-tracer/)