

CS 361

Computer

Networks Lab

Assignment 9

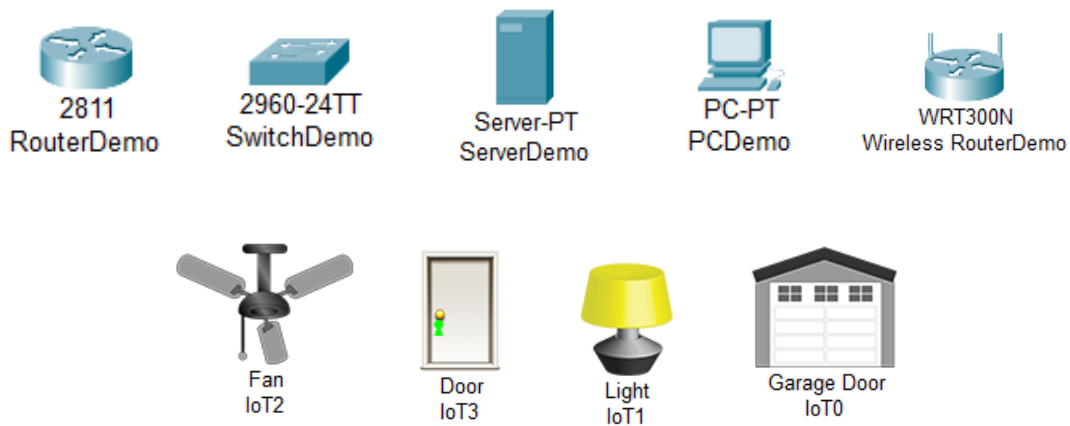
Samanway Maji
Student ID – 202151136
Date – 24/11/2023

Questions:

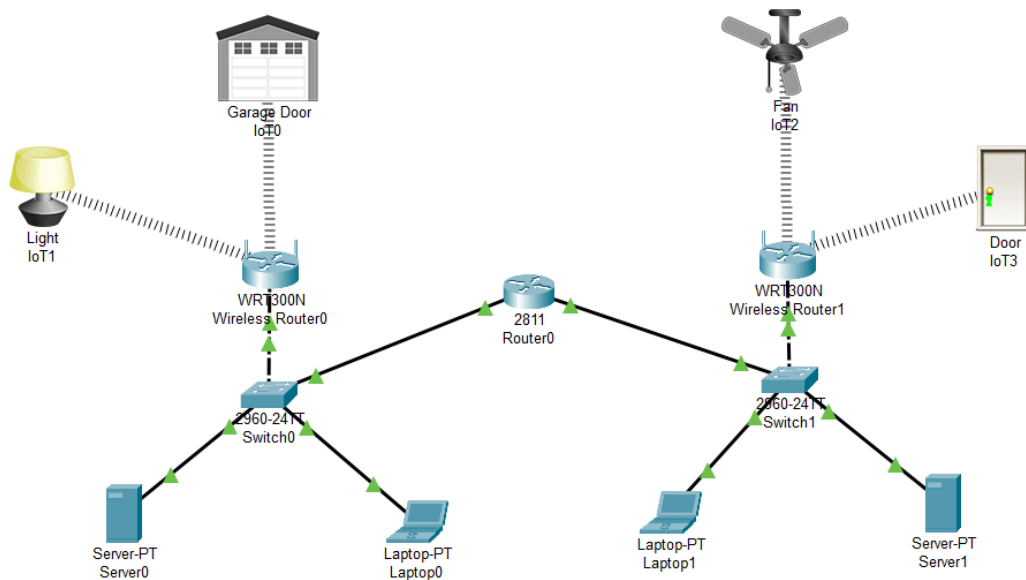
1. Consider that you have two different houses with multiple IoT devices. The two houses are in different subnets and have different IoT servers. Demonstrate the following:

(1) IoT devices of one house can be controlled from the Laptop/PC of another house.

Components used:



Network Diagram:



Steps followed:

The first step is setting up the individual networks. This is done by connecting the wired components to the switch. The **Wireless-Router is connected to the switch using a copper cross-over wire.**

The next step is setting the IPV4, subnet and SSID of the wireless router.

Wireless Router0

Physical Config **GUI** Attributes

Wireless-N Broadband Router

Setup Setup **Wireless** Security Access Restrictions Applications & Gaming Admin

Basic Setup DDNS MAC Address Clone

Internet Setup

Internet Connection type: Automatic Configuration - DHCP

Optional Settings (required by some internet service providers):

Host Name:

Domain Name:

MTU: Size: 1500

Network Setup

Router IP: IP Address: 192 . 168 . 0 . 1

Subnet Mask: 255.255.255.0

Wireless Router0

Physical Config **GUI** Attributes

Wireless-N Broadband Router

Wireless Setup Wireless Security Access Restrictions Applications & Gaming Admin

Basic Wireless Settings Wireless Security Guest Network Wireless MAC Filter

Basic Wireless Settings

Network Mode: Mixed

Network Name (SSID): Home1

Radio Band: Auto

Wide Channel: Auto

Standard Channel: 1 - 2.412GHz

SSID Broadcast: ☒ Enabled ☐ Disabled

The same has been done in the image.

Next steps include, enabling the AAA (Authentication, Authorization, and Accounting) service of the server, and adding the wireless router's SSID along with a password which is to be added in the security portion of the same as well.

The screenshot shows the 'Server0' configuration window with the 'Services' tab selected. On the left, a list of services includes HTTP, DHCP, DHCPv6, TFTP, DNS, SYSLOG, AAA (highlighted), NTP, EMAIL, FTP, IoT, VM Management, and Radius EAP. The main area is titled 'AAA' and shows the service is 'On'. The 'Radius Port' is set to '1645'. Under 'Network Configuration', there is a table with one entry:

	Client Name	Client IP	Server Type	Key
1	Home1	192.168.0.1	Radius	pass123

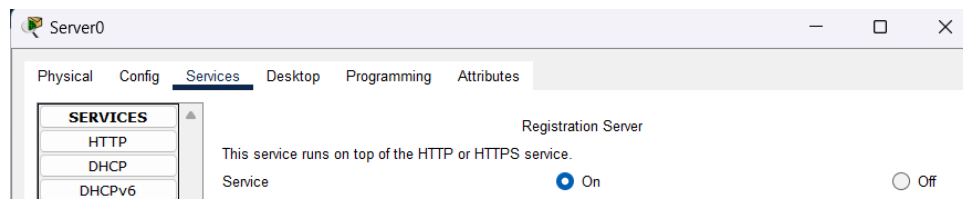
Buttons for 'Add', 'Save', and 'Remove' are visible on the right side of the table.

The router's SSID, IP and a passkey have been added to AAA service.

The screenshot shows the 'Wireless Security' configuration page. The 'Security Mode' is set to 'WPA2 Enterprise' and 'Encryption' is set to 'AES'. The 'RADIUS Server' is configured with IP address '192.168.0.10'. The 'RADIUS Port' is '1645' and the 'Shared Secret' is 'pass123'. The 'Key Renewal' is set to '3600 seconds'.

The passkey, and the server's IP are added to the wireless router to recognize the server it needs to connect to.

Next steps include switching on the IoT services of the server and adding the IoT devices that are to be connected to the wireless router.

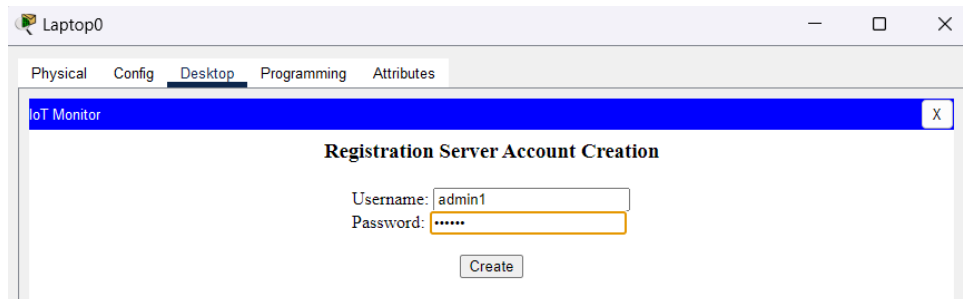


The IoT service is enabled.

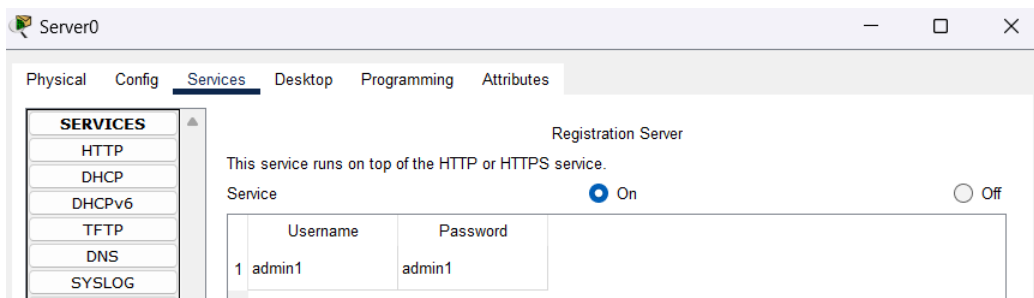


Considering, I am currently setting up the left side of the network diagram, so I have added, **two devices, as shown, i.e., a light and Garage door**, both of which are IoT devices.

The next step is setting the IPV4 of the laptop, and then creating an account to control the IoT devices. This can be done by using the **IoT monitor** application of the laptop.

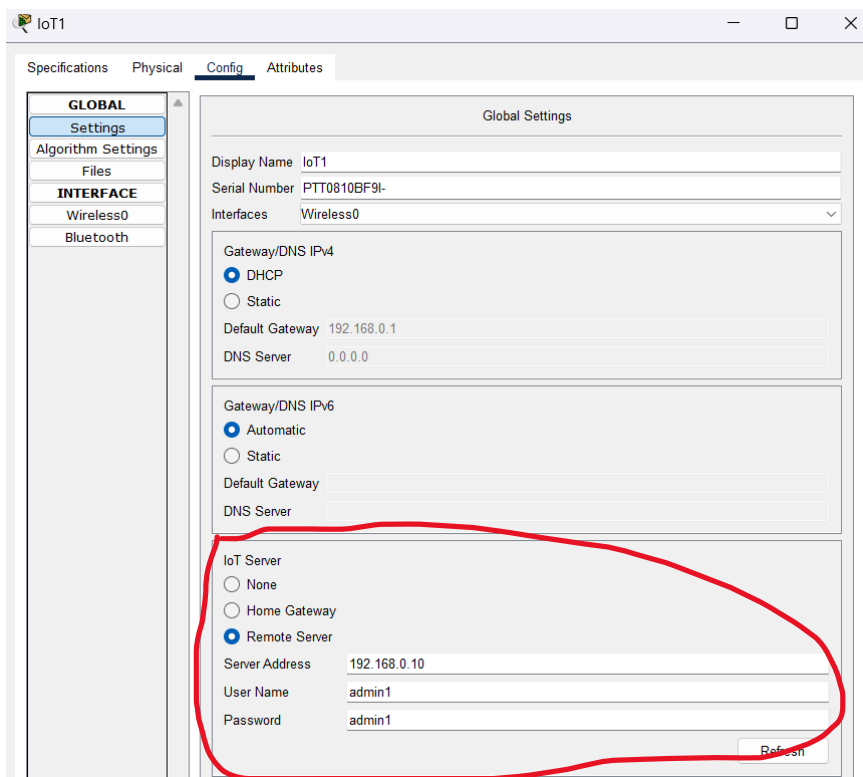
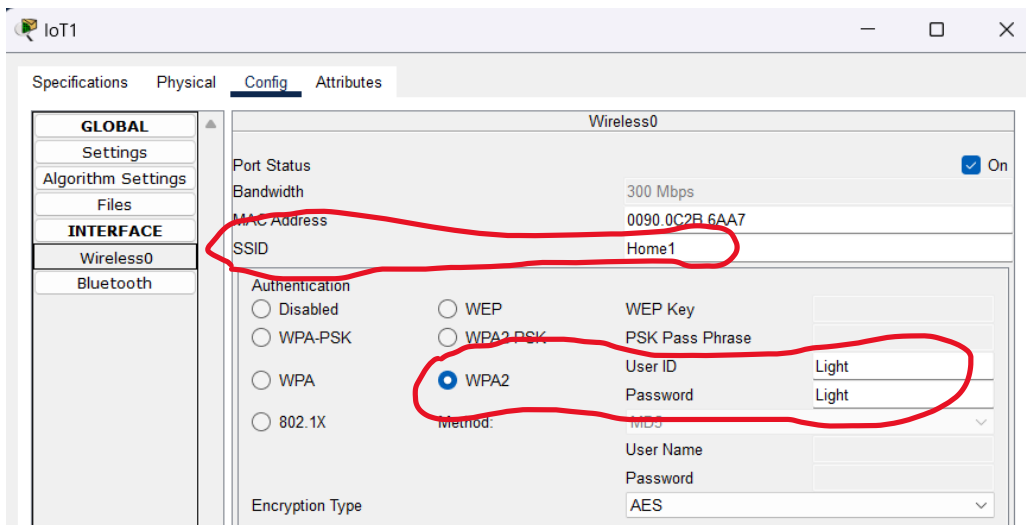


On clicking create, an account gets created, which is also shown in the IoT service of the server.

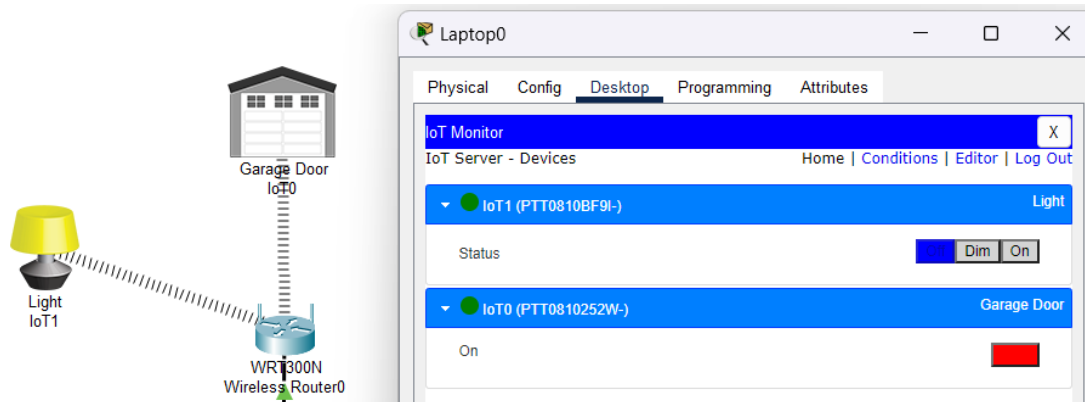


The next step is to configure the IoT devices, by providing the SSID of the router to connect to and the username and password accordingly. Also, since it's a remote server, we also need to provide the necessary credentials.

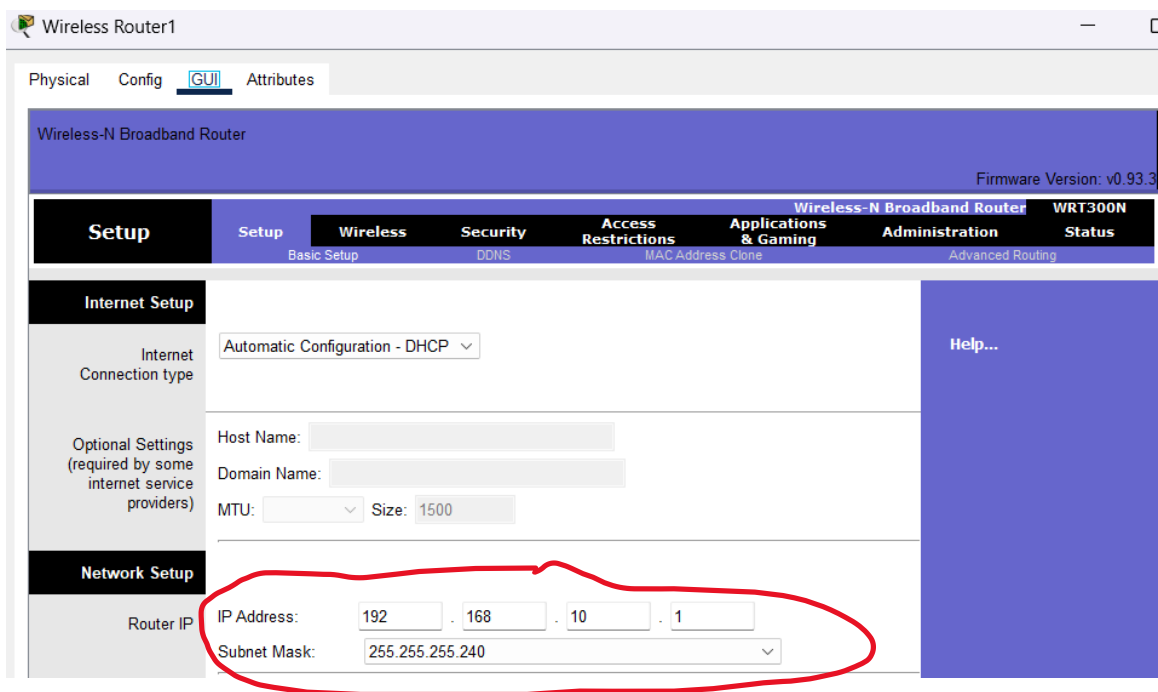
An example for configuring the Light has been shown below.



Now we can login with the username and password in the IoT Monitor application, and find that devices are visible there, and can be controlled as well.



Similarly, the right side of the network diagram is done as well. Few configurations have been shown.



A different subnet mask has been used in this wireless network, as asked in the question. The subnet of the other one was 255.255.255.0.

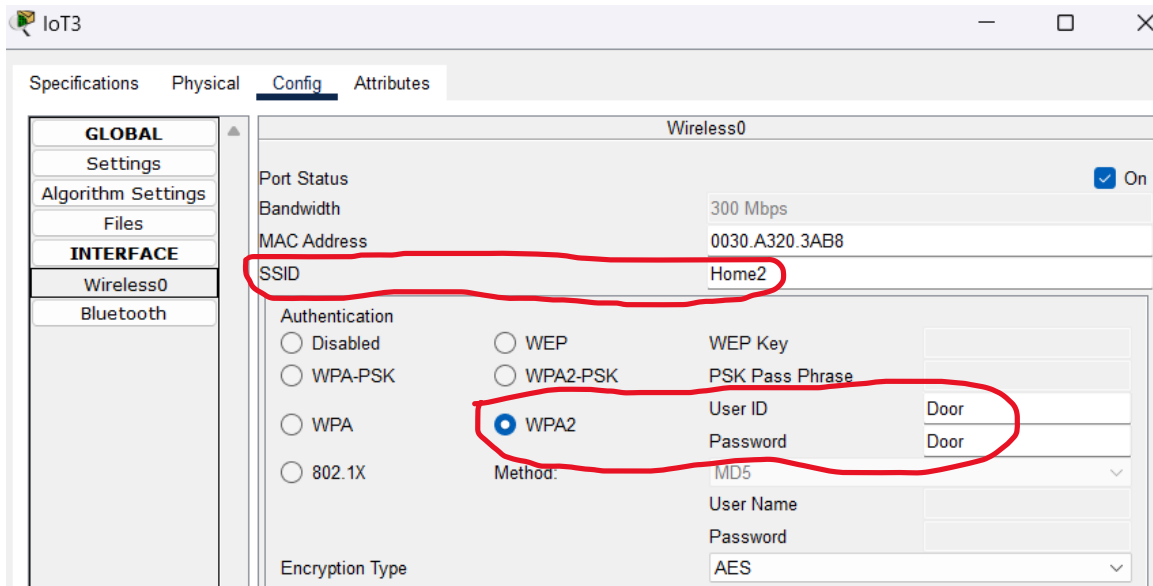
Network Mode:	Mixed
Network Name (SSID):	Home2
Radio Band:	Auto
Wide Channel:	Auto
Standard Channel:	1 - 2.412GHz
SSID Broadcast:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

A different SSID has been assigned. Also, the server IP is different as well, as can be seen in the next diagram. (Previous: 192.168.0.10)

Security Mode:	WPA2 Enterprise
Encryption:	AES
RADIUS Server:	192 . 168 . 10 . 10
RADIUS Port:	1643
Shared Secret:	pass123
Key Renewal:	3600 seconds

And configuration of an IoT device as well:

Specifications Physical Config Attributes	
GLOBAL Settings Algorithm Settings Files INTERFACE Wireless0 Bluetooth	Global Settings Display Name IoT3 Serial Number PTT08107738- Interfaces Wireless0 Gateway/DNS IPv4 <input checked="" type="radio"/> DHCP <input type="radio"/> Static Default Gateway 192.168.10.1 DNS Server 0.0.0.0 Gateway/DNS IPv6 <input checked="" type="radio"/> Automatic <input type="radio"/> Static Default Gateway DNS Server IoT Server <input type="radio"/> None <input type="radio"/> Home Gateway <input checked="" type="radio"/> Remote Server Server Address 192.168.10.10 User Name admin2 Password admin2 Refresh

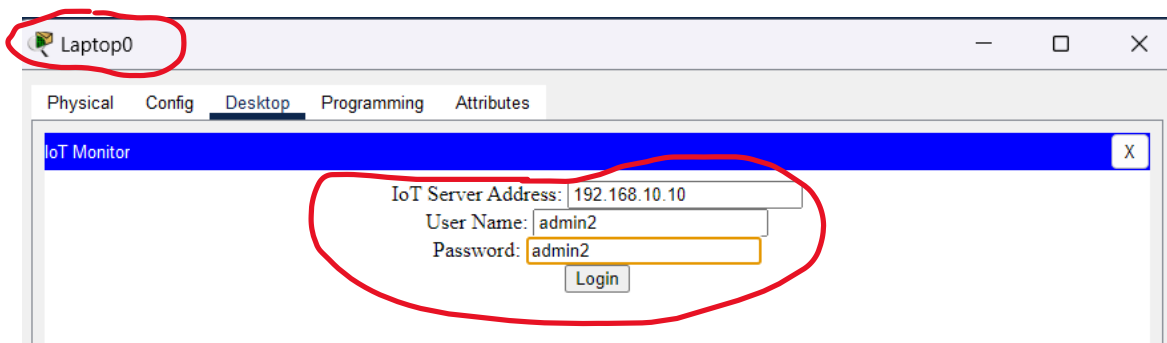


The two networks relate to the router, the steps of which have been covered in previous labs.

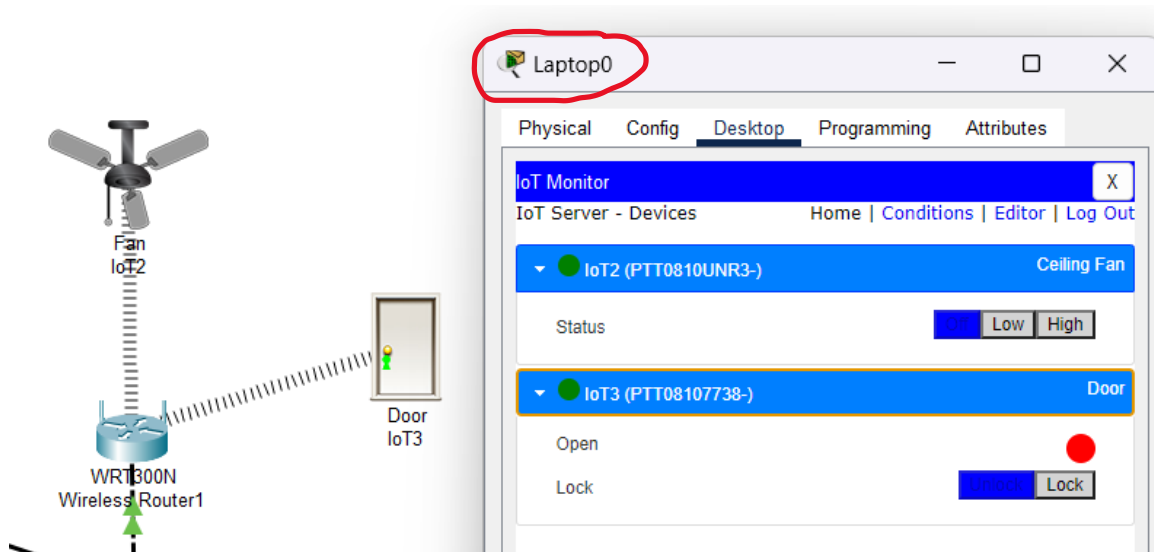
Observation:

I will try to access the Door and Fan (present on the other network, right hand side) from Laptop 0 (present on left hand side).

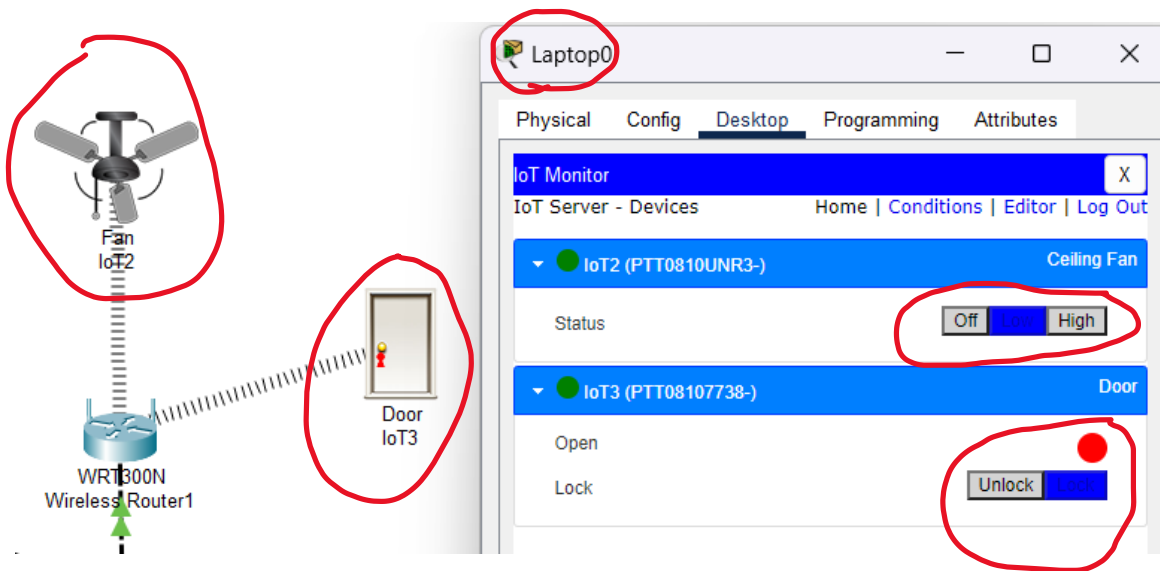
For that, inside IoT Monitor, the username and password of the account associated with the right-hand side, needs to be put.



The devices associated with that side shows up:



Controlling the device:



So, the devices of other networks can be controlled from a device of different network from the former.

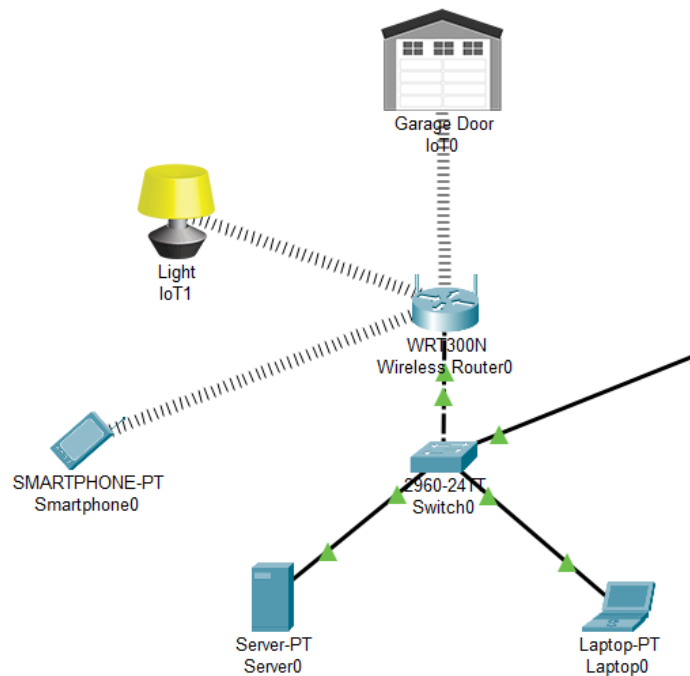
2. Connect at least 10 wireless devices (wireless desktop, laptop, printers, wireless mobile, tabs & etc..) to each access point. Consider that you have two different houses with multiple IoT devices. The two houses are in different subnets and have different IoT servers. Demonstrate the following:

(2) Use a mobile phone to communicate with IoT devices.

Components used:

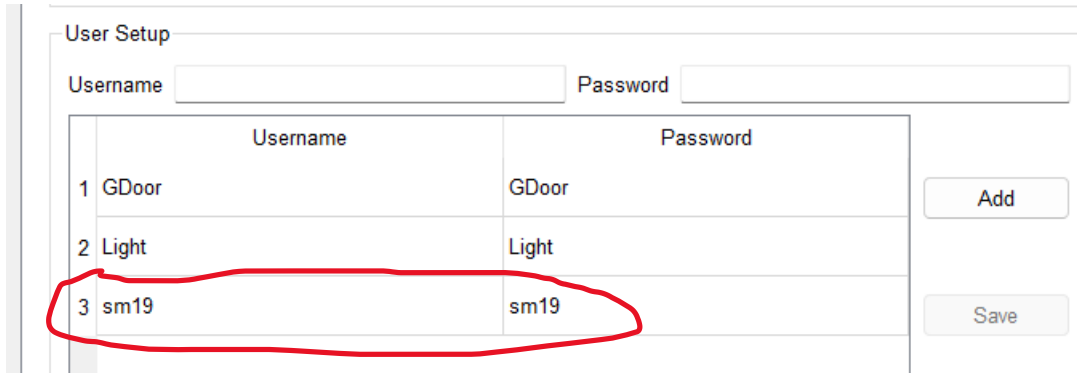

SMARTPHONE-PT
SmartphoneDemo

Network Diagram:



Steps followed:

The way we added the IoT devices, in the same way smartphone needs to be added as well.



User Setup

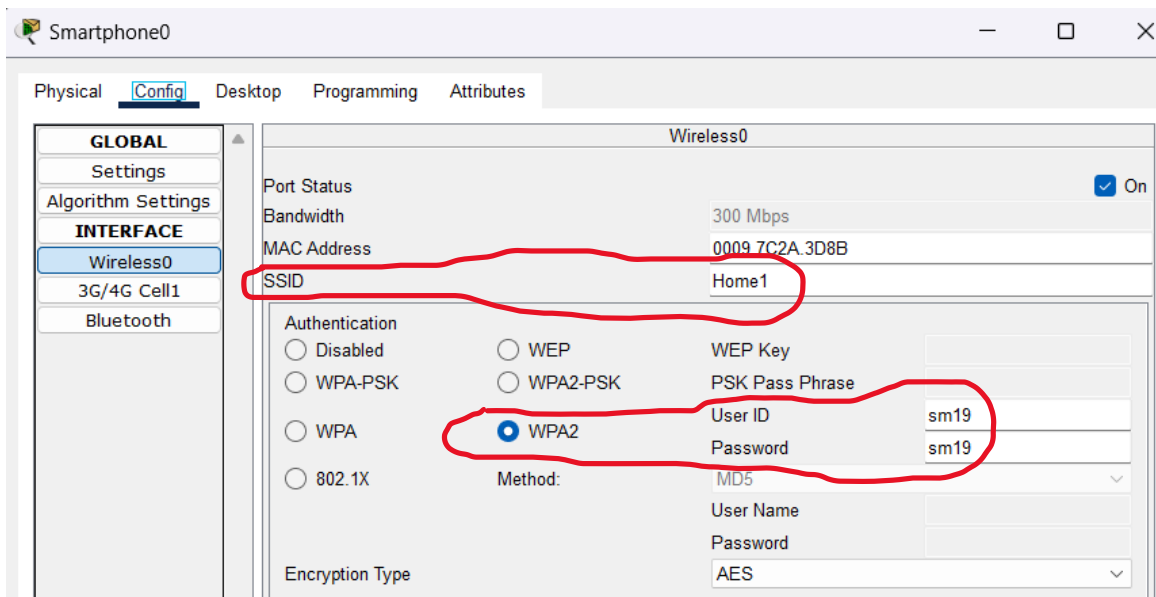
Username Password

	Username	Password
1	GDoor	GDoor
2	Light	Light
3	sm19	sm19

Add

Save

Then the smartphone is configured accordingly:



Smartphone0

Physical **Config** Desktop Programming Attributes

GLOBAL

- Settings
- Algorithm Settings

INTERFACE

- Wireless0**
- 3G/4G Cell1
- Bluetooth

Wireless0

Port Status ☒ On

Bandwidth 300 Mbps

MAC Address 0009 7C2A 3D8B

SSID Home1

Authentication

☐ Disabled ☐ WEP ☐ WPA2-PSK ☒ WPA2

WEP Key

PSK Pass Phrase

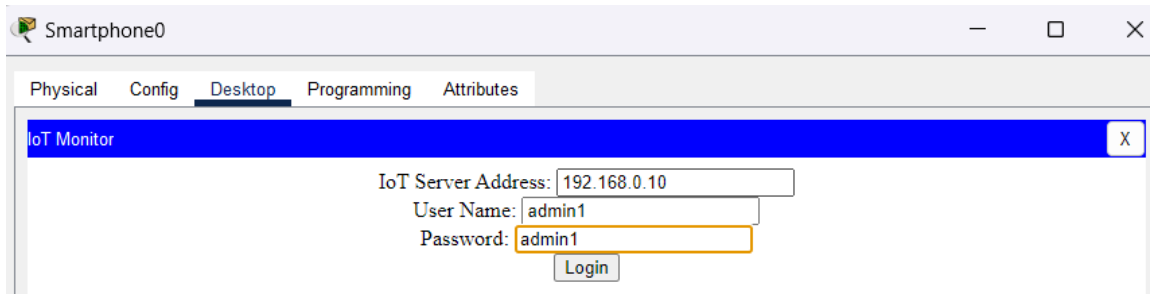
User ID sm19

Password sm19

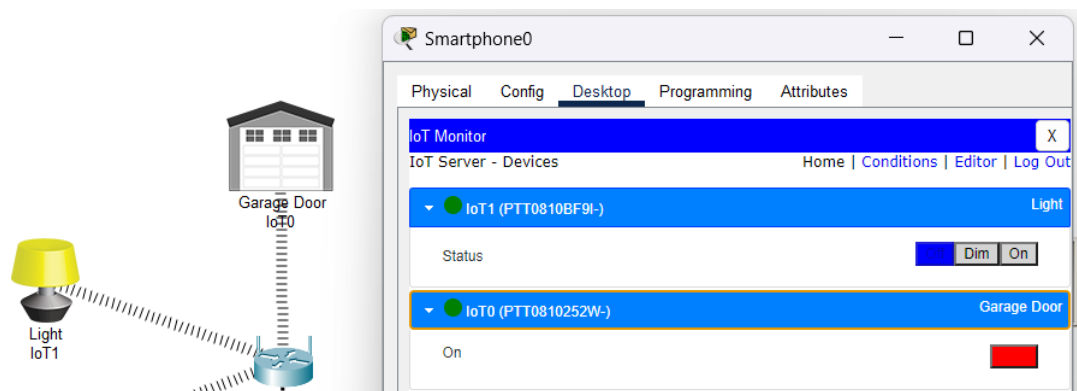
Method: MD5

Encryption Type AES

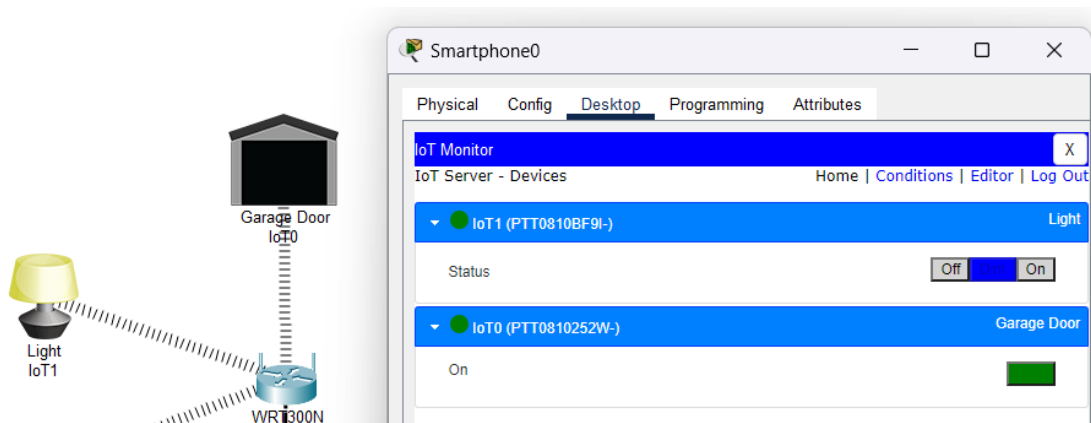
Next, we open IoT Monitor, and login with the credentials:



The devices are shown:



They are also controlled by the smartphone:



Hence, the IoT devices can be controlled by smartphones.