جامعة عجمان

AJMAN UNIVERSITY

College of Engineering & Information Technology

Department of IT Network and Security

FINAL LAB PROJECT REPORT

Submitted by:

Anas Ahmed Hamood

Student ID:

202110589

Course Name:

Wireless Networks – INT433

Supervisor:

Nabia Khalid

Date of Submission:

April 23, 2025

Table of Contents

Table of Figures

Table of Tables

Introduction: Network Overview

Introduction

So, this project is about creating a combined wireless and wired network – a hybrid if you like – for this multi-story building at Ajman University.Specifically, it's the J2 Building.We have three floors here with each floor having three different blocks, A, B and C.Although the intention was to implement reasonably comprehensive wireless coverage.And that meant granting access to students, staff, the IT folks and naturally, the administrators.The critical services that keep things going – think DHCP, RADIUS authentication and web services – those are all based up on the roof, Block B.Where the main switch and the wireless LAN controller, or WLC, are as well. Access points or APs, were strategically placed to give that full coverage.Sounds reasonable huh? Gotta ensure everyone can access their tablets and laptops all around the building.Furthermore, they included an RFID-based system for the admin and IT office doors, which provides an additional layer of security. We segmented the network by VLANs That makes it a big assistance in management, but also in security.It pretty much establishes controlled access, so that people get the access they are supposed to have and it's also authorized.The whole idea here was to create a network that is scalable and highly available.We wanted to be able to keep wireless communication secure and be able to manage it effectively and all through centralized control.It's definitely a good system for the building.

First Draft of the Topology

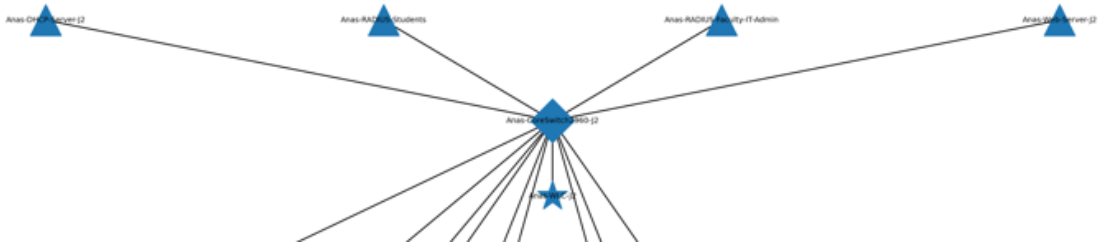

Figure 1 Roof Section Devices

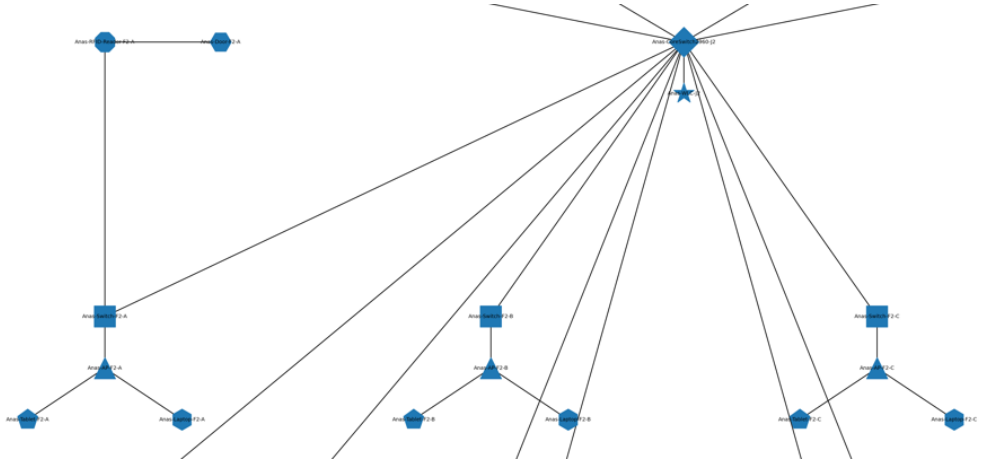

Figure 2 Second Floor with Block (A,B, and C)

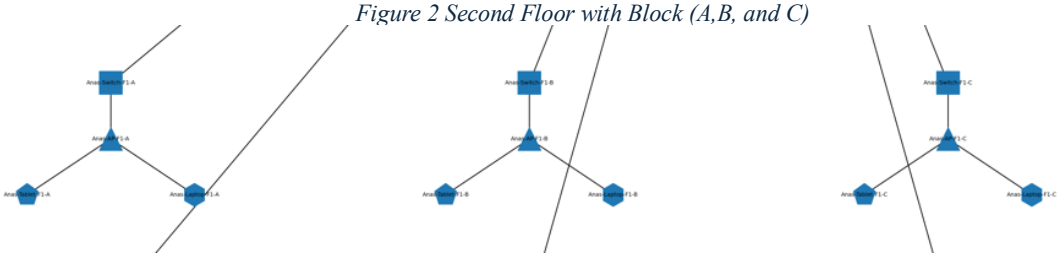

Figure 3 First Floor with Block (A,B, and C)

Figure 4 Ground Floor with Block (A,B, and C)

Figure 5 All Shapes with their Devices Names

Final Draft of the Topology

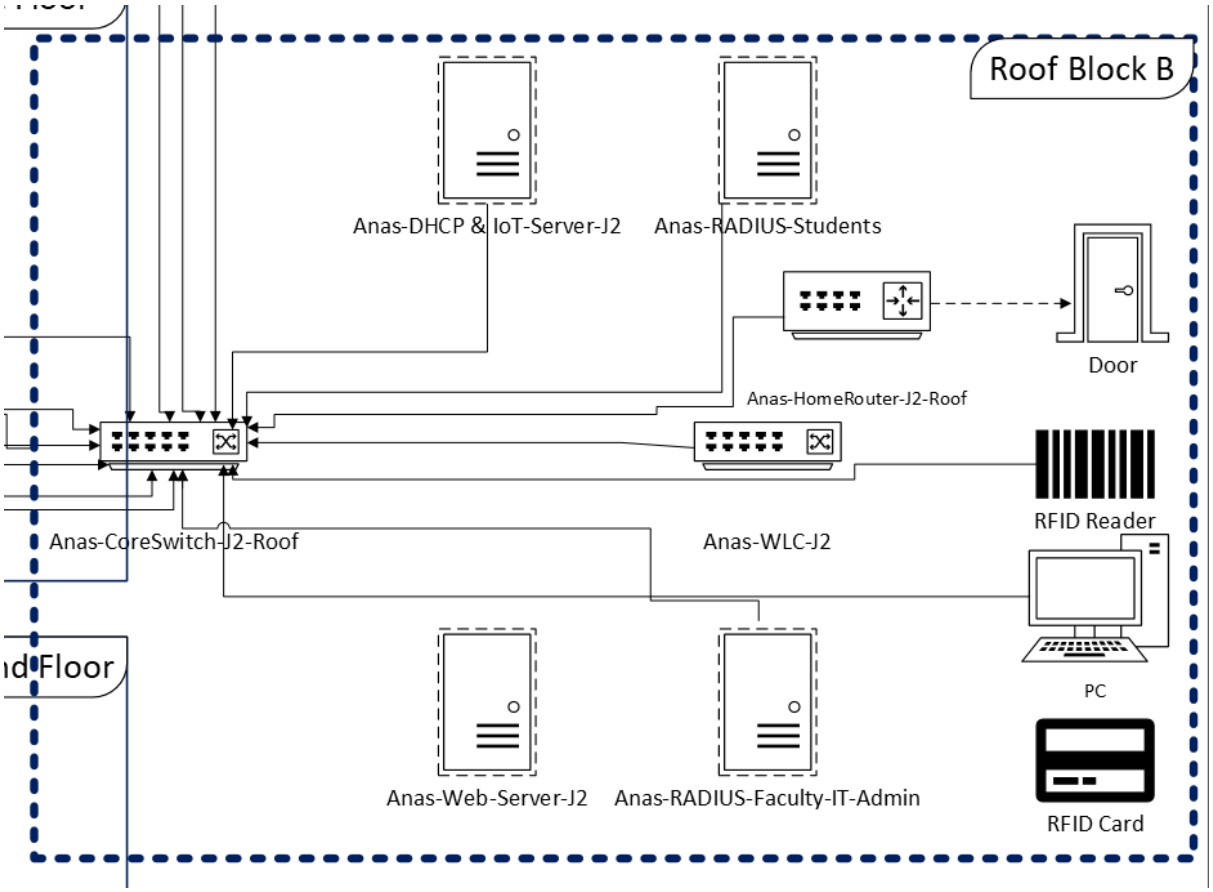

Figure 6 Roof Section with the Devices

Here is the roof of the building J2 where is centre in the Block B, were all the server room are and only the Faculty, IT Support, and Administrator enter there.

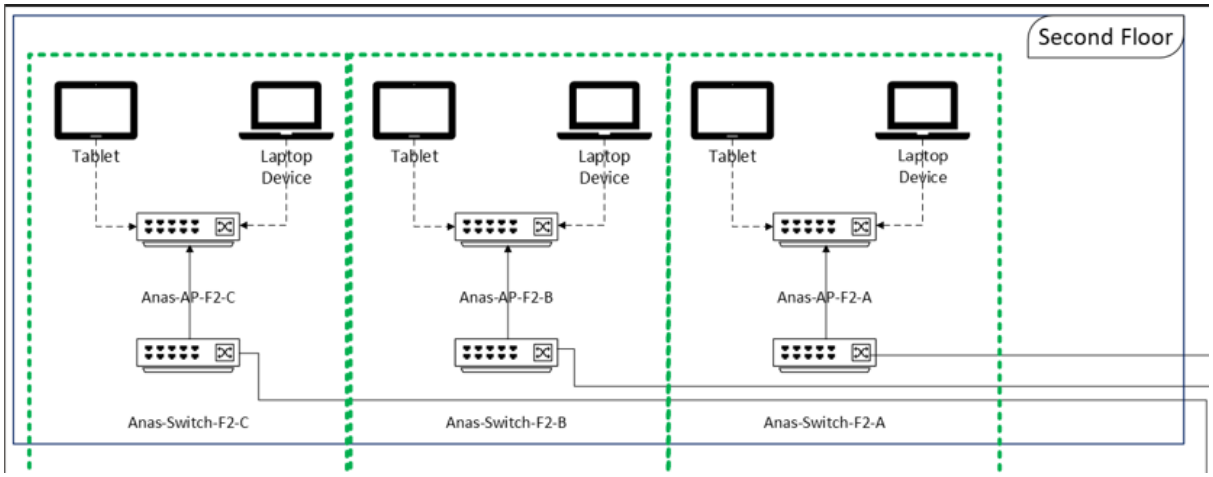

Figure 7 Second Floor which contains Block (A,B, and C)

Here is the second floor where it going to contain of the three block A, B, and C where every block has their own access point and so students can access using their tablet or laptops.

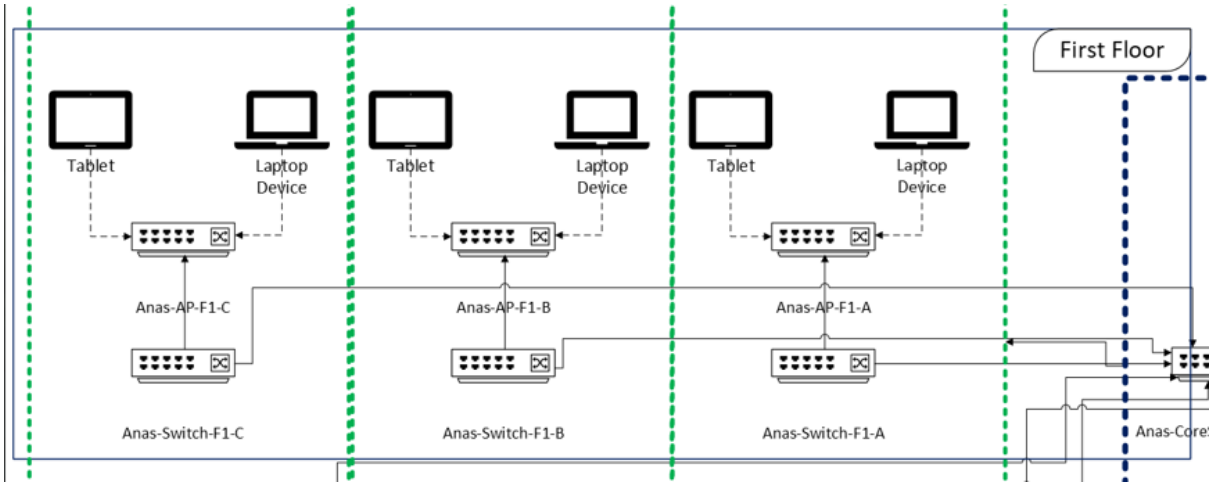

Figure 8 First Floor which contains Block (A,B, and C)

Here is the First floor where it going to contain of the three block A, B, and C where every block has their own access point and so students can access using their tablet or laptops exactly same as second floor.

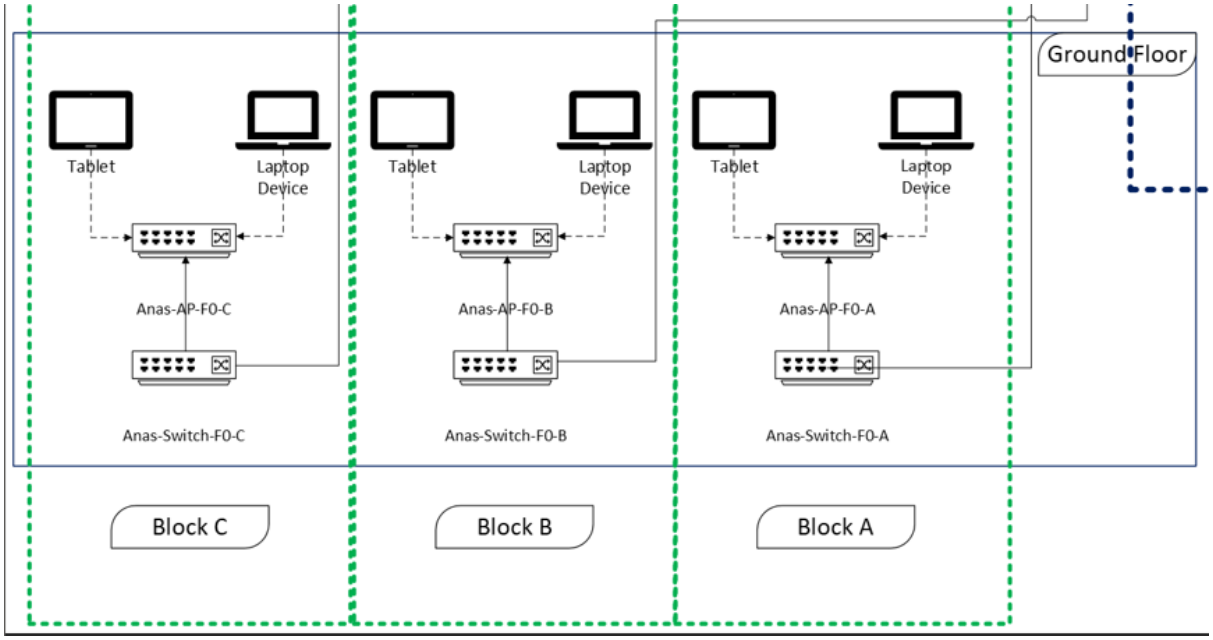

Figure 9 Ground Floor which contains Block (A,B, and C)

Here is the second floor where it going to contain of the three block A, B, and C where every block has their own access point and so students can access using their tablet or laptops exactly same as the second and first floor and here in the topology design it mention the blocks clearly.

Design Justification

Design Justification

This project's design was actually initiated by a requirement of scalability and of course security efficiency.To manage the core of our network traffic, we chose a Cisco 2960 switch.It handles the aggregating of all that and the inter-VLAN routing, which provides us with a nice solid wired backbone.Also, we chose Wireless LAN Controller (WLC) technology.That provides us with the capability to centrally manage all those access points.It makes things a lot easier for consistent SSID broadcasts and makes roaming from one location to another lots smoother.It even makes wireless network maintenance a lot less of a headache VLANs are in place obviously to separate the different groups – students, staff and IT.This eliminates those broadcast domains and adds a layer of security For our critical wireless links, we're using WPA2-Enterprise security, you know the good stuff.It relies on RADIUS authentication servers, so only the right people get to see everything the university has to offer.Also, we've got an RFID system on the roof It handles access control for those sensitive office areas, which should be pretty secure and automated.DHCP dynamically assigns IP addresses, which makes a lot of things easier, while, on the other hand, the critical network devices are statically configured for stability.In the end, the entire design was actually done with the university's needs in mind.We wanted to provide scalable, secure and easily managed network and but also we wanted reliable wireless coverage over all the floors.I think that we have reached that.

IP Addressing Table & WLC SSID & Configuration Table

Device Name	IP Address	Connection Type
Anas-CoreSwitch-J2-Roof-B	N/A	Ethernet
Anas-Switch-F2-A	DHCP	Ethernet
Anas-Switch-F2-B	DHCP	Ethernet
Anas-Switch-F2-C	DHCP	Ethernet
Anas-Switch-F1-A	DHCP	Ethernet
Anas-Switch-F1-B	DHCP	Ethernet
Anas-Switch-F1-C	DHCP	Ethernet
Anas-Switch-F0-A	DHCP	Ethernet
Anas-Switch-F0-B	DHCP	Ethernet
Anas-Switch-F0-C	DHCP	Ethernet
Anas-DHCP-Server-J2-Roof-B	192.168.0.2	Ethernet
Anas-RADIUS-IT-Staff/Students-J2-Roof-B	192.168.0.3	Ethernet
Anas-IoT-J2-Roof-B	192.168.0.4	Ethernet
Anas-WLC-J2	192.168.0.5	Ethernet
Anas-Admin-J2-Roof-B	192.168.0.6	Ethernet

Table 1IP Addressing Table

The subnet mask for all the devices is 255.255.255.0

WLC IP Address	SSID Name	VLAN ID	RADIUS Server IP	Authentication Type	Encryption Type
192.168.0.5	IT Staff/Students	N/A	192.168.0.3	WPA2 (802.1X)	AES

Table 2 WLC SSID & Configuration Table

Packet Tracer Configuration

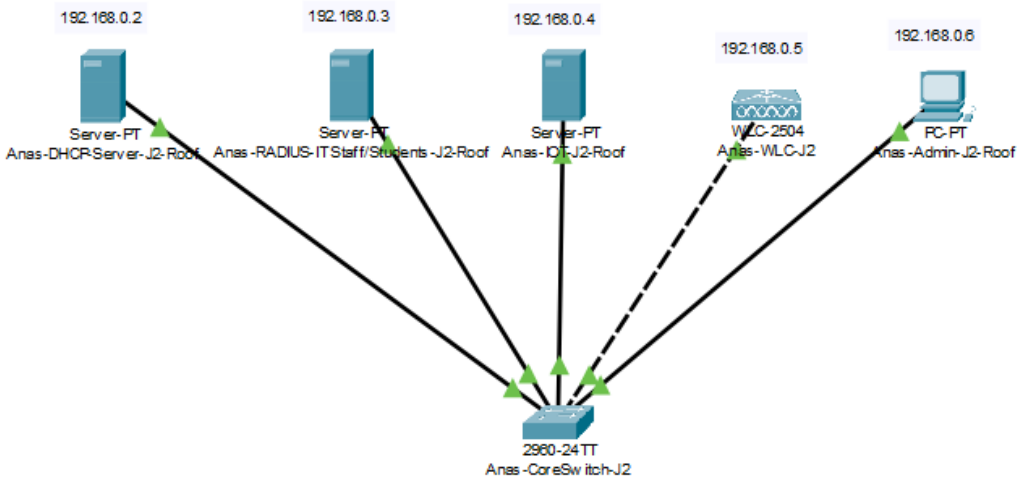

Figure 10 Roof Devices Topology

Here is the Roof Devices which will be only where it will have the sensitive devices

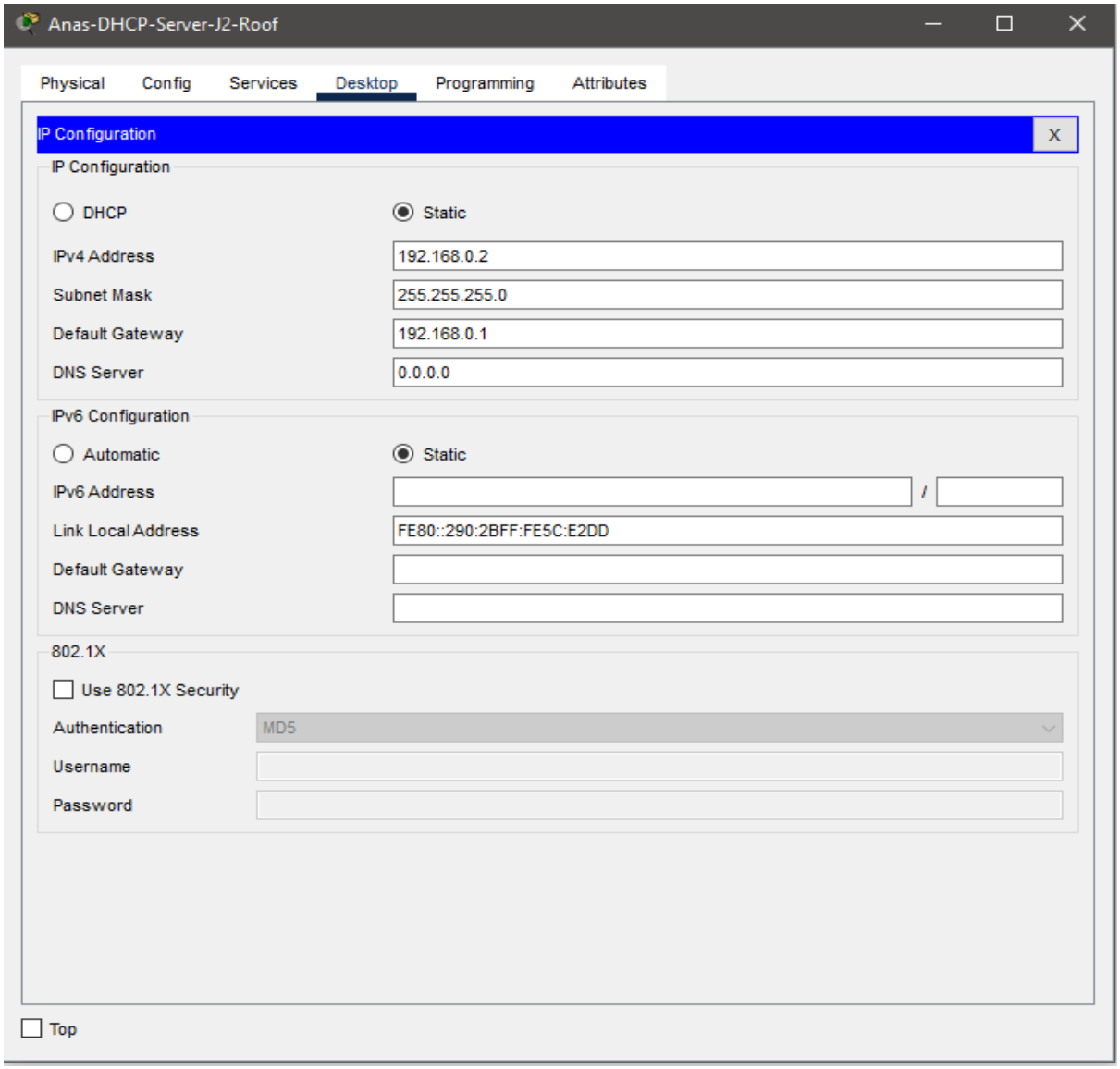

Figure 11 DHCP IP Address

Assigning IP address, Subnet Mask, and Default Gateway for the DHCP Serve

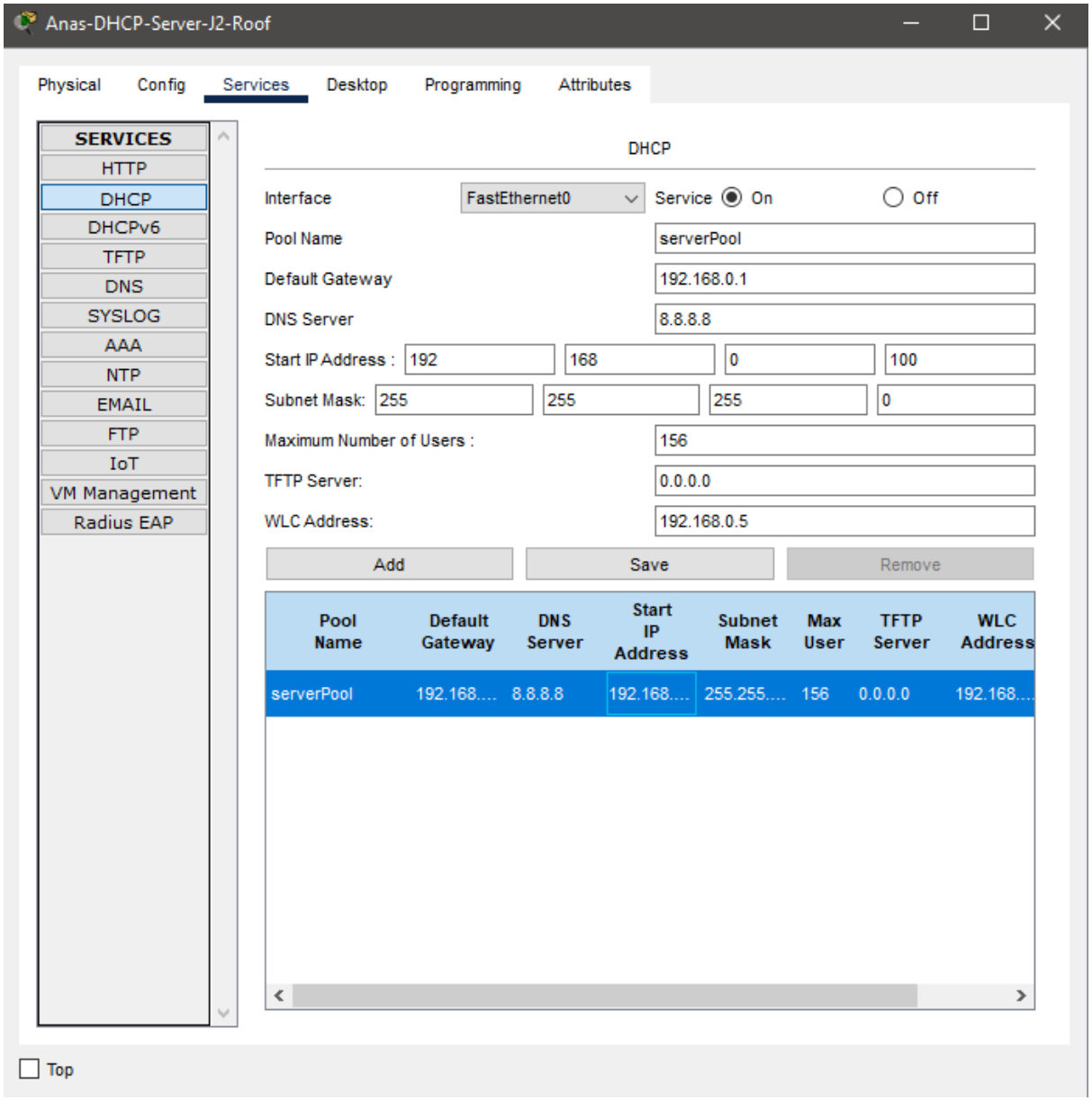

Figure 12 DHCP Server Configuration

Assigning the Default Gateway, DNS, Starting IP Address, Subnet Mask, the Maximum number of the Users, and lastly the WLC IP Address.

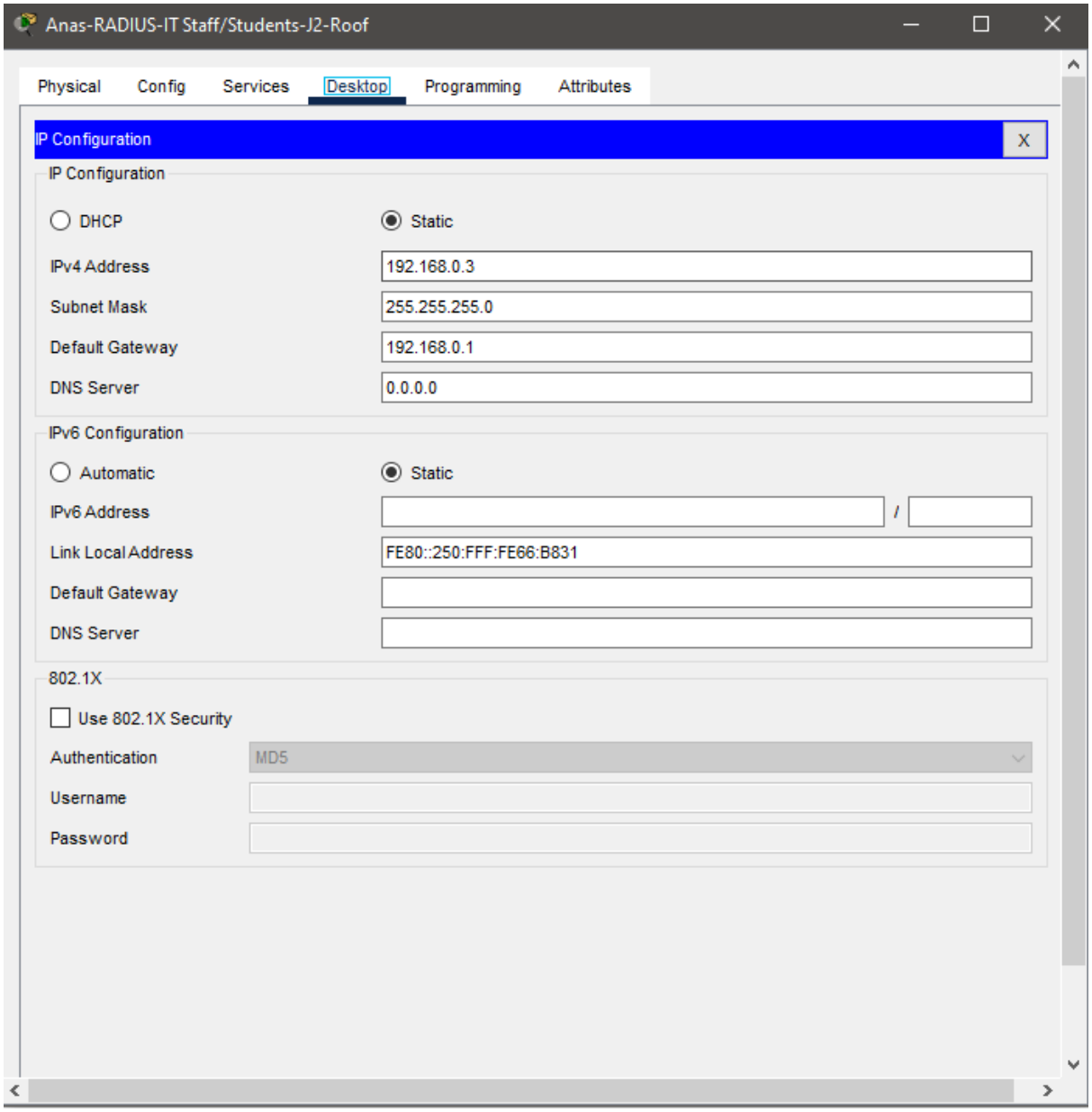

Figure 13 RADIUS IP Adress

Assigning IP address for the RADIUS IT Staff and Student Server

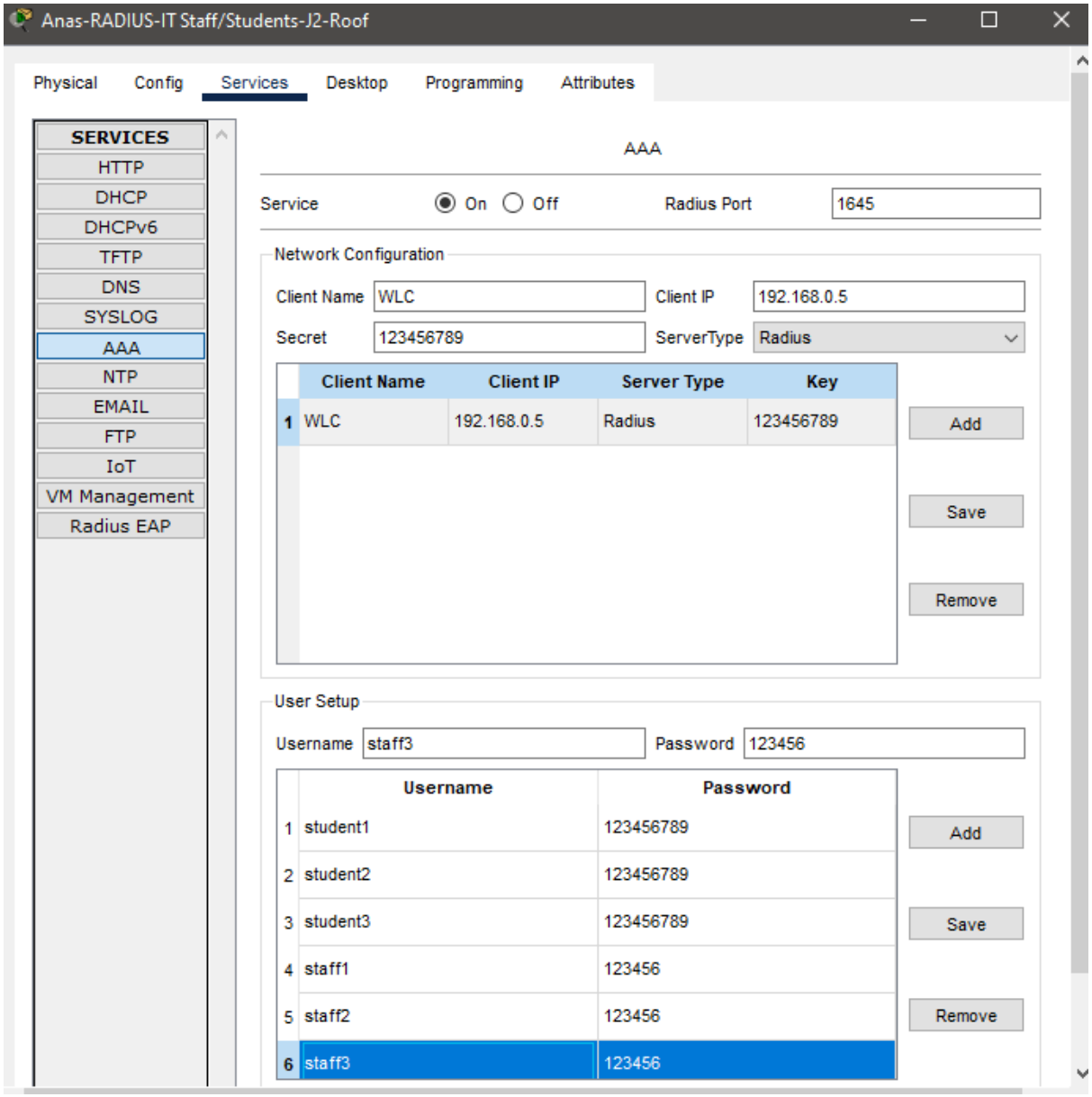

Figure 14 RADIUS Configuration

Here in the Network configuration, we make the client is the WLC

And we add some users to the RADIUS, and it shown below in the table: -

Username	Password
student1	123456789
student2	123456789
student3	123456789

Table 3 Students Usernames & Passwords

Username	Password
staff1	123456
Staff2	123456
Staff3	123456

Table 4 Staff Usernames & Passwords

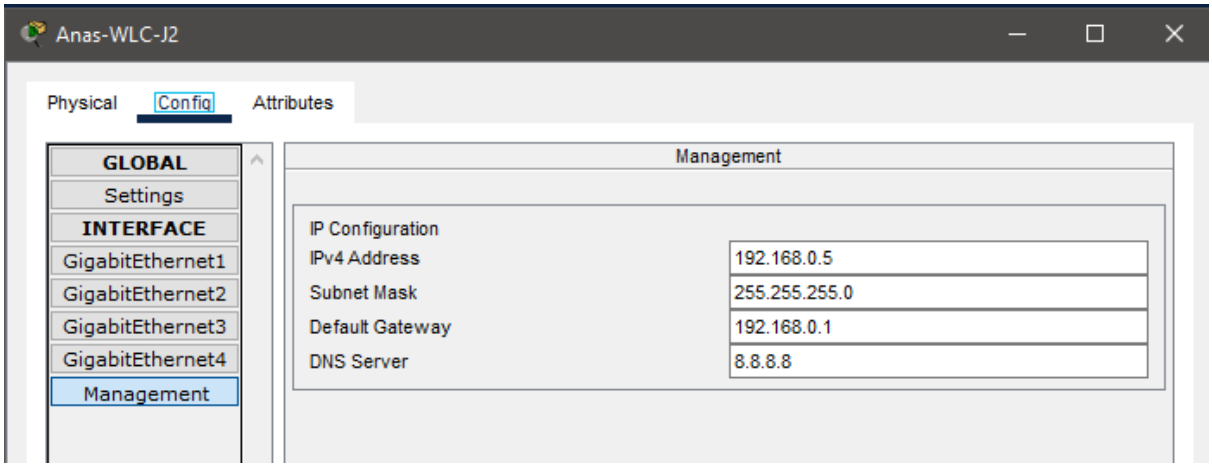

Figure 15 WLC IP Address

Assigning IP Address, Subnet Mask, Default Gateway, and DNS to the WLC

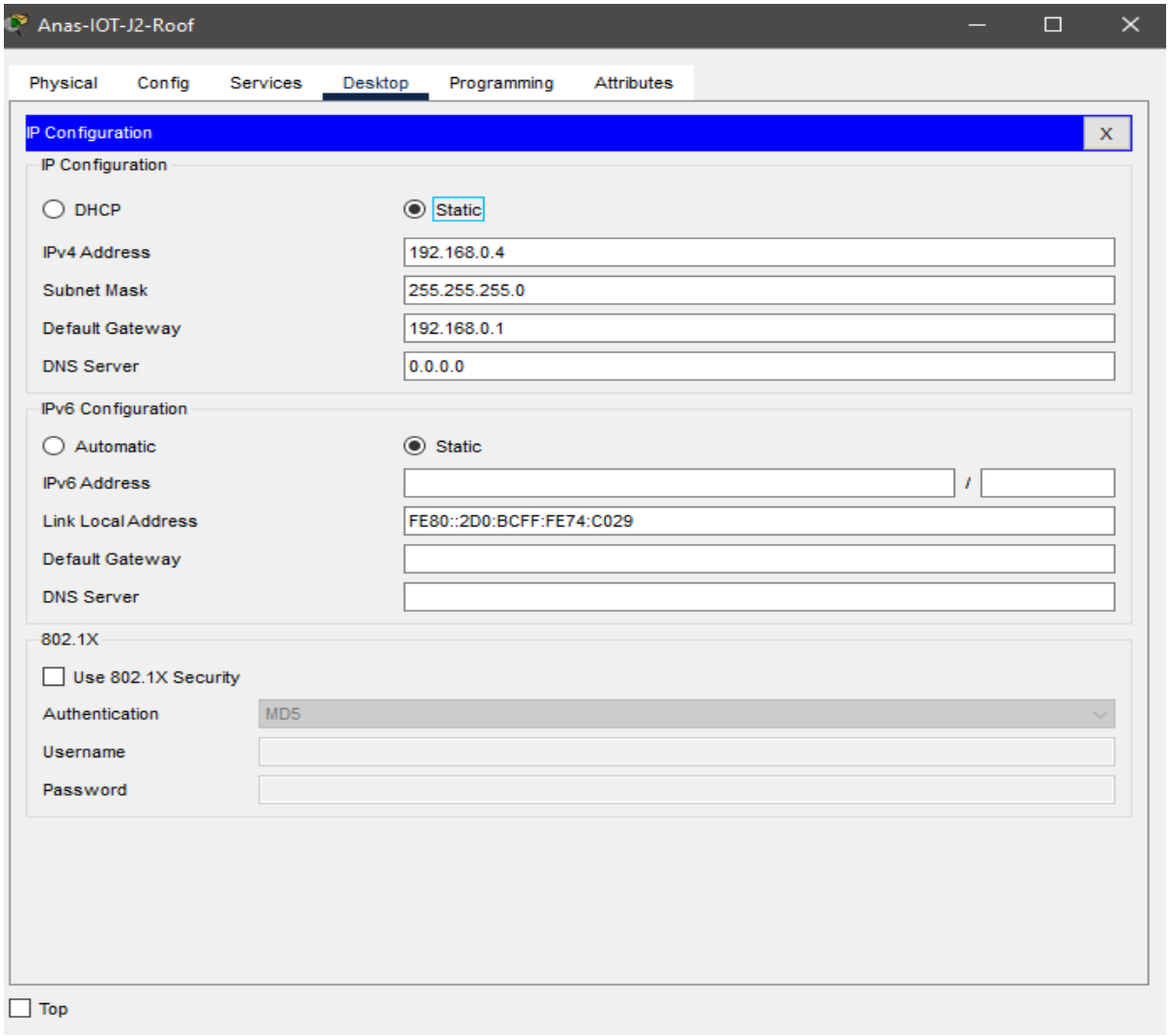

Figure 16 IoT IP Address

Assigning IP Address, Subnet Mask, and Default Gateway to the server

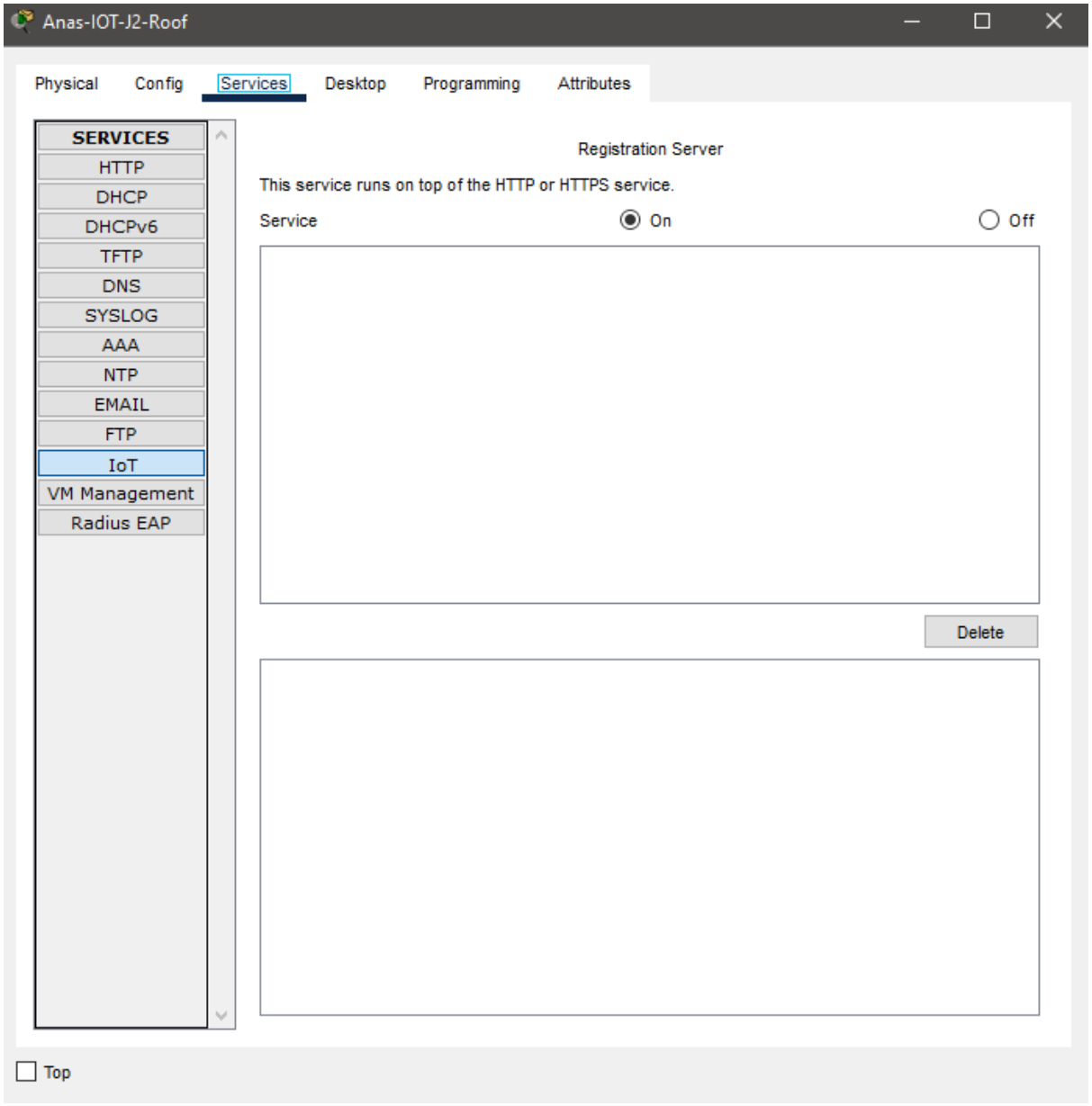

Figure 17 Enable the IoT

Here we click on to enable the IoT server

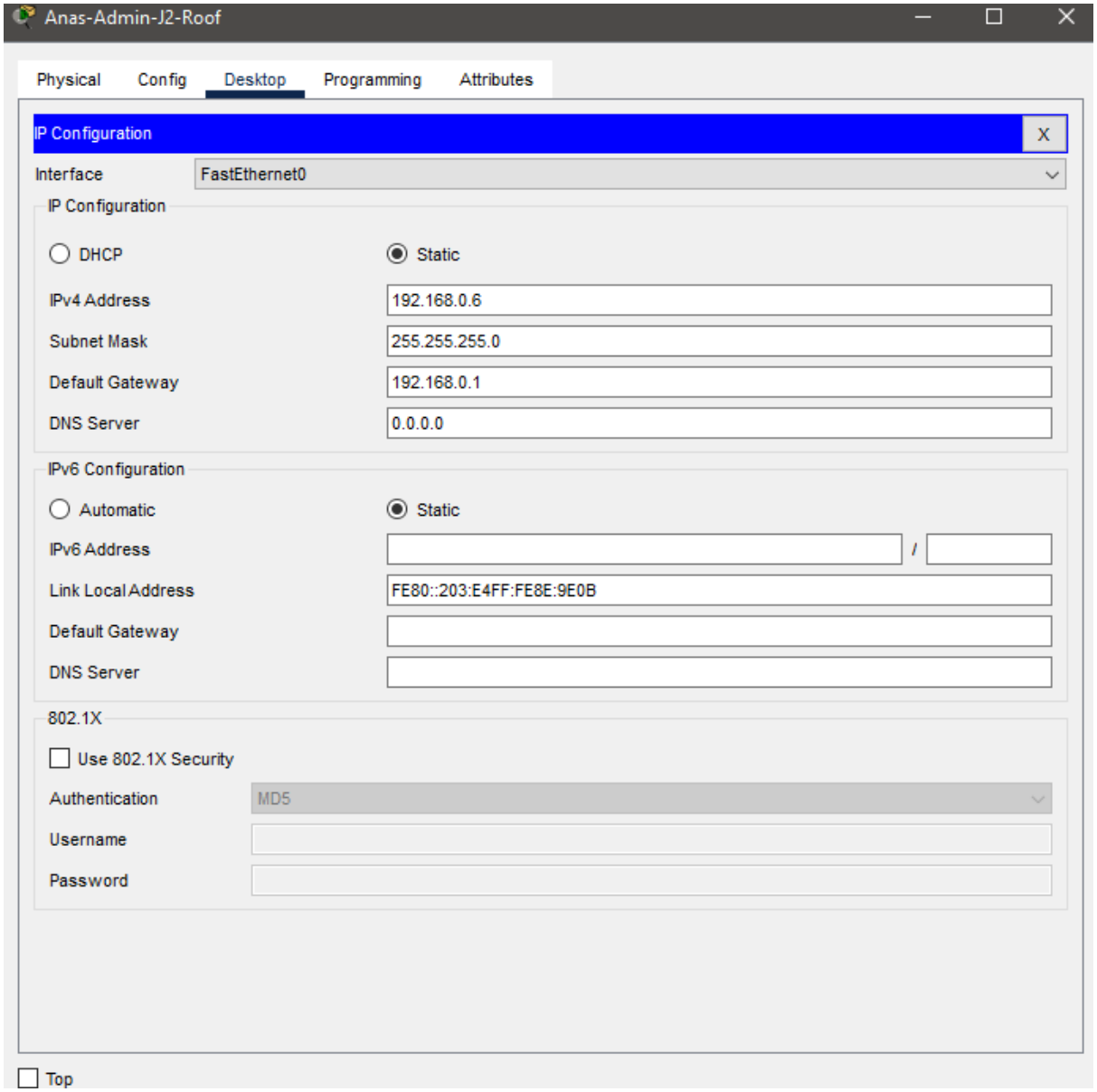

Figure 18 PC Main IP Address

Assigning IP Address, Subnet Mask, Default Gateway to the PC that is on the Roof usually its for the admin to use because it controls the IoT devices and WLC.

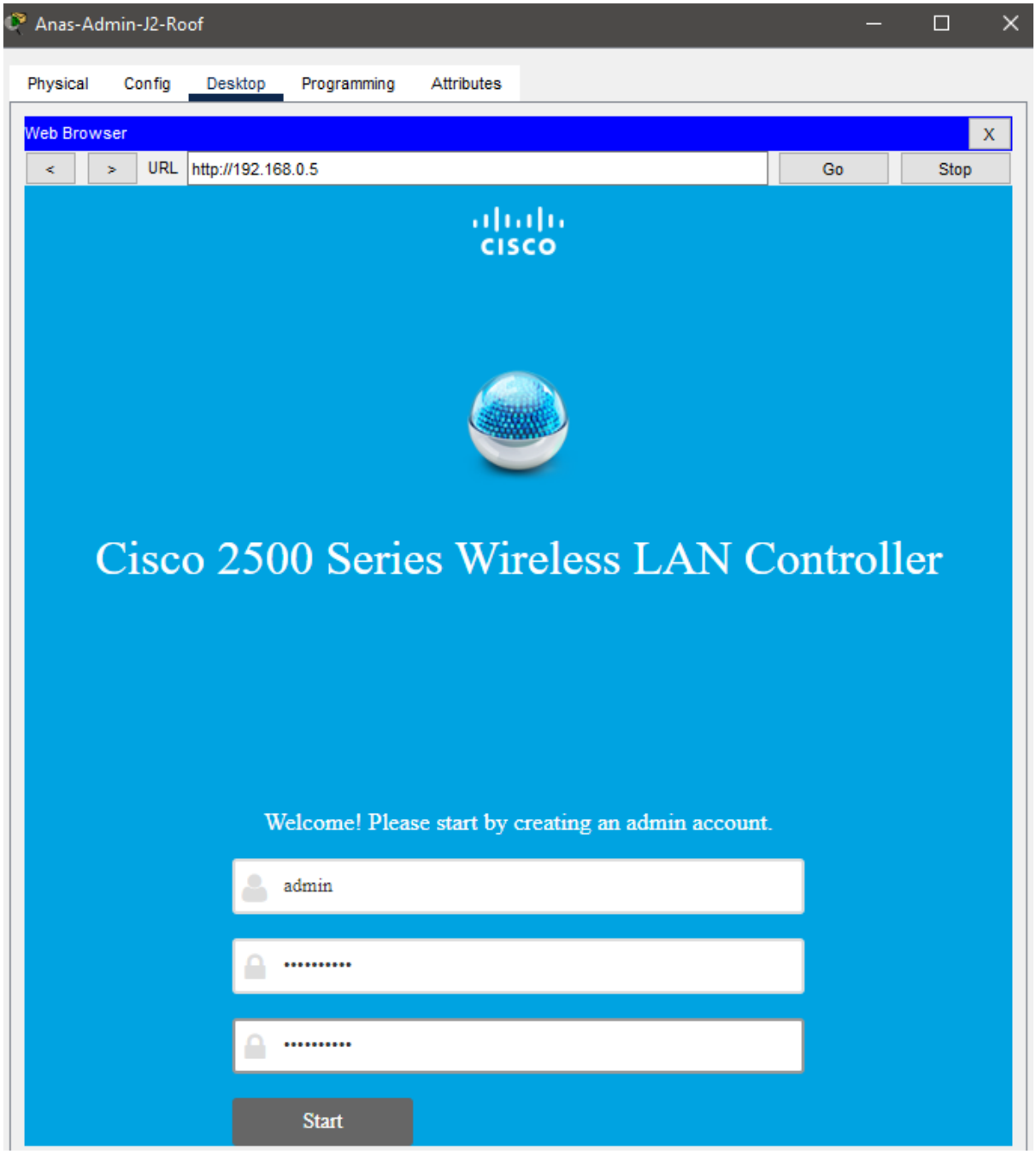

Figure 19 WLC Controller Sign-up

Here we create account to have access to the WLC and can control it

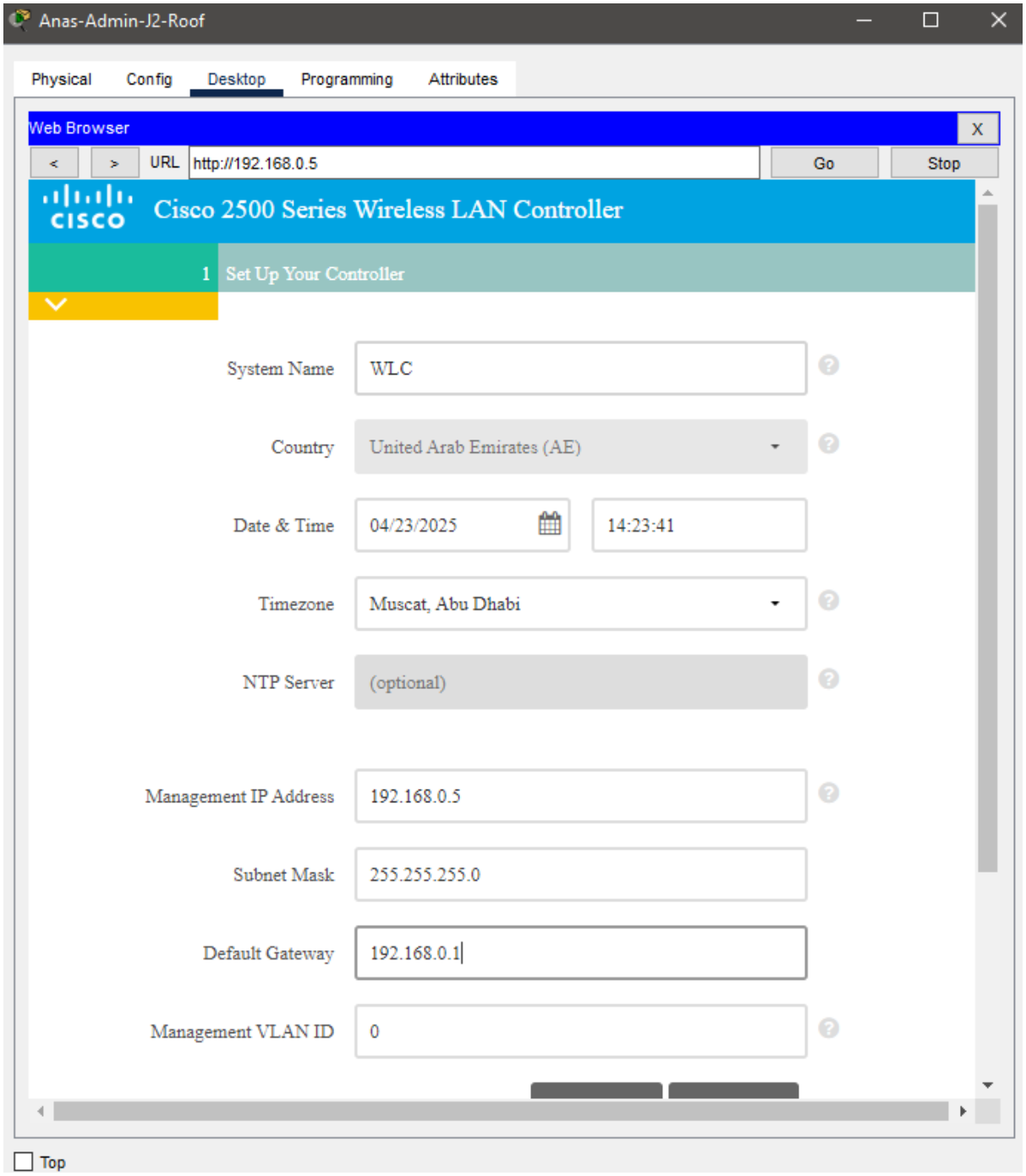

Figure 20 Setting Up the Controller

Here we gave the system name, IP Address, Subnet Mask, and Default Gateway

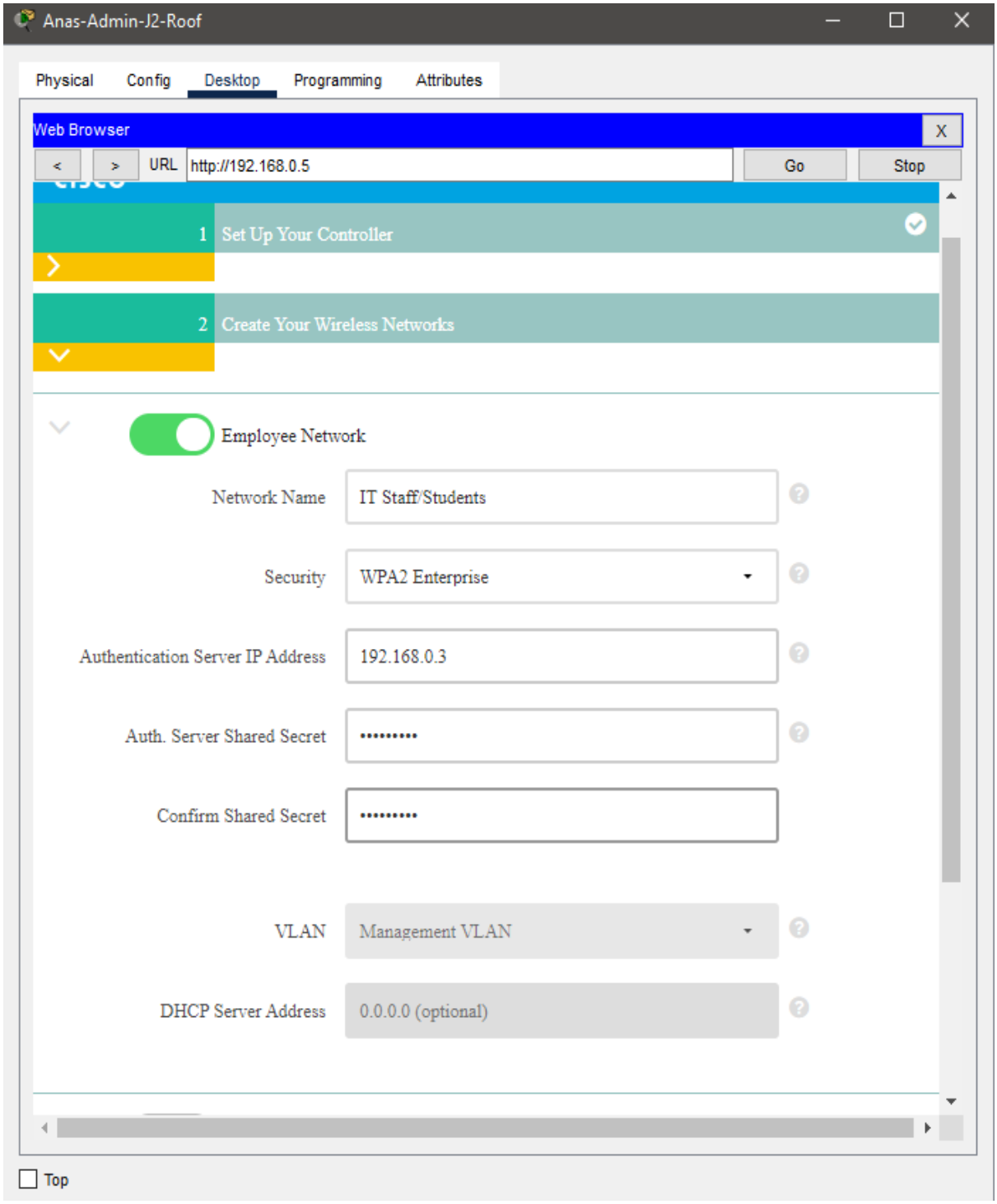

Figure 21 Creating the Wireless Network

Giving name to the network, security policy, and the RADIUS server IP Address with a shared secret which is from 1 to 9 (123456789)

Network Name	Security	Auth. Server IP Address	Auth. Server Shared Secret
IT Staff/Students	WPA2 Enterprise	192.168.0.3	123456789

Table 5 Network Information

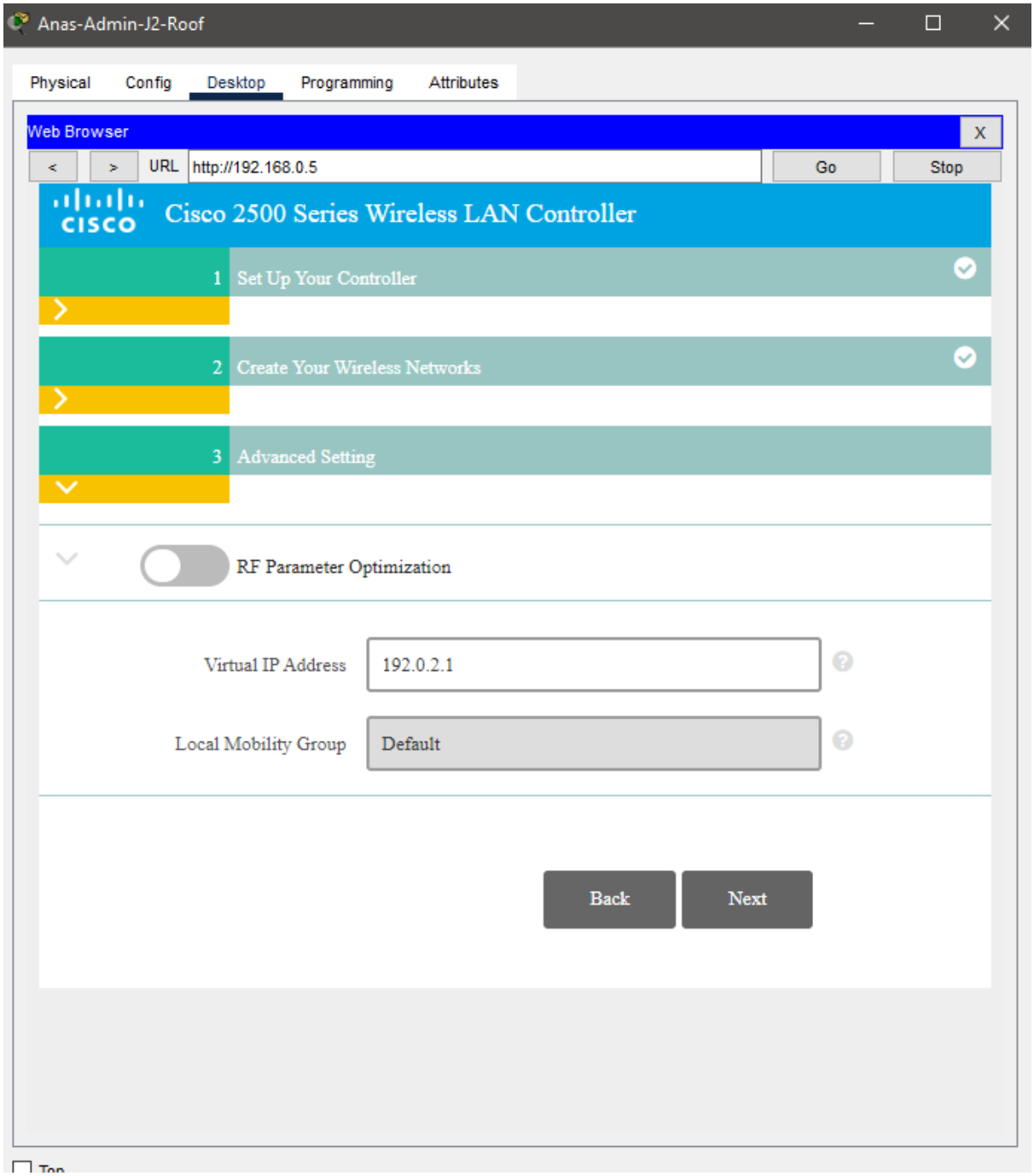

Figure 22 Advance Setting for WLC Configuration

Here we Just Click on Next

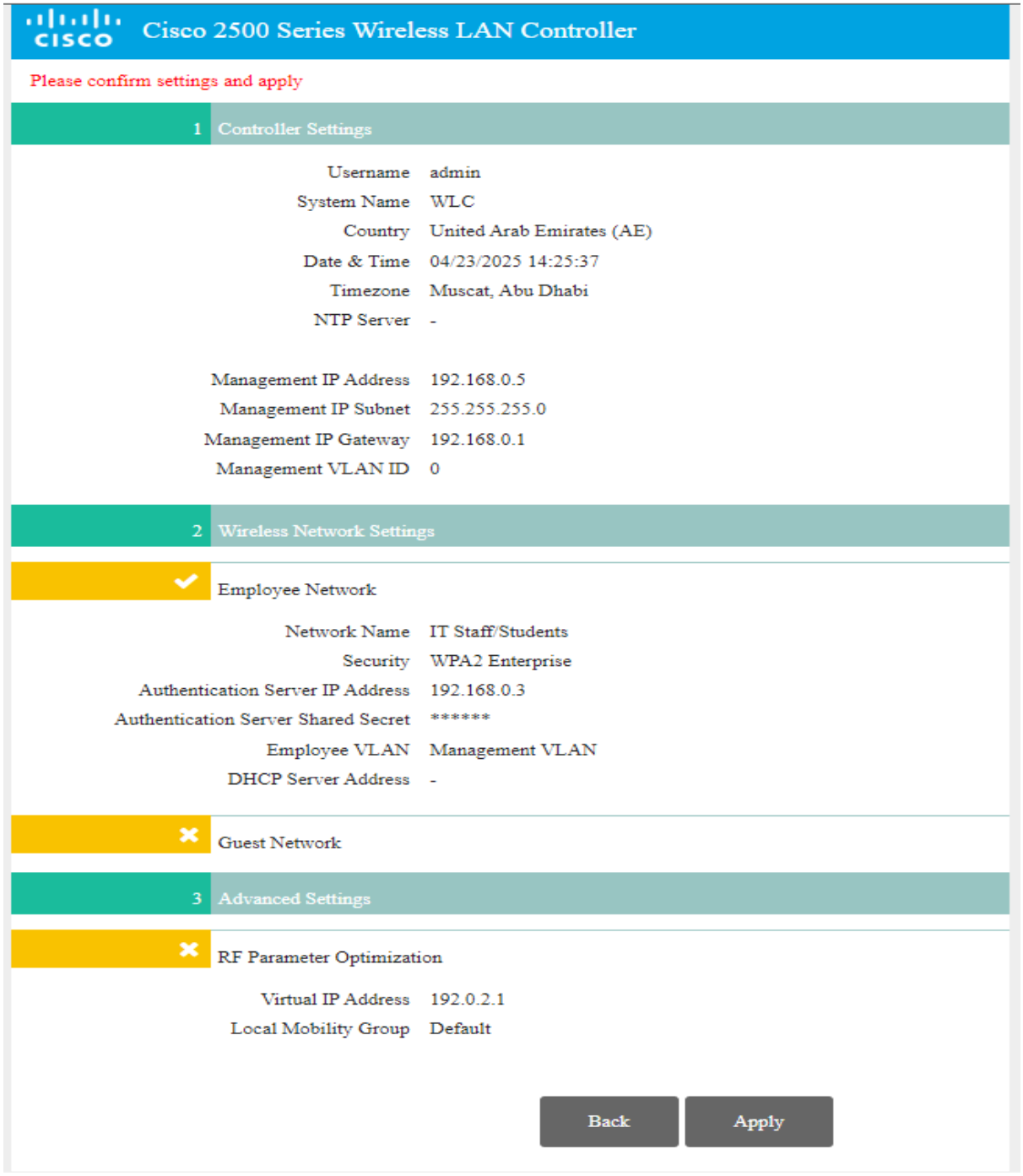

Figure 23 All the Information for the WLC

Here we can check everything before clicking on apply

Figure 24 Login to the WLC with the HTTPS

We sing-in to the WLC controller using the username and the password:

Username	Admin
Password	Admin@1020

Table 6 Username & Password for the WLC Sign-in Page

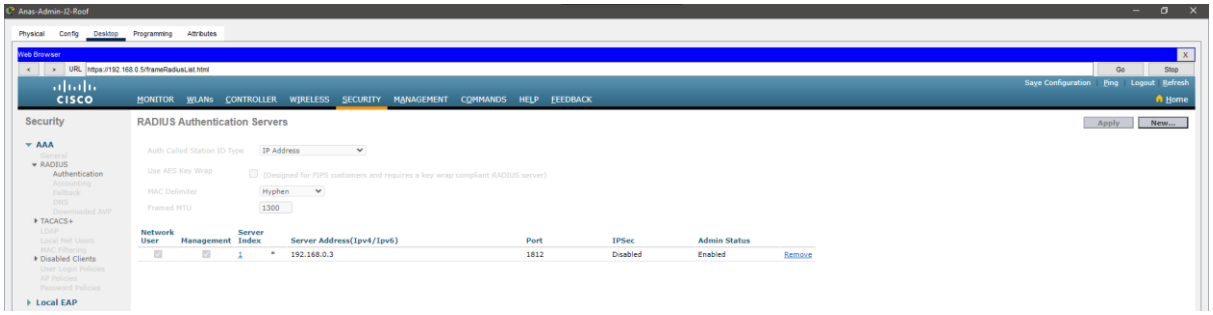

Figure 25 RADIUS Authentication Server Security

Here we can check the part number so we can apply it to the RADIUS server

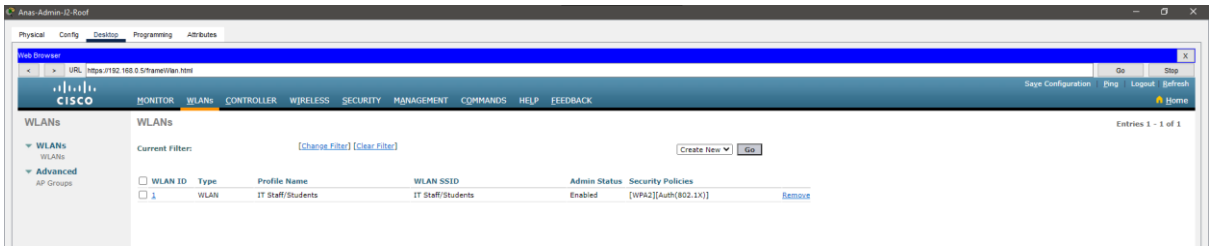

Figure 26 WLANs

Here we can check all network that we have been created

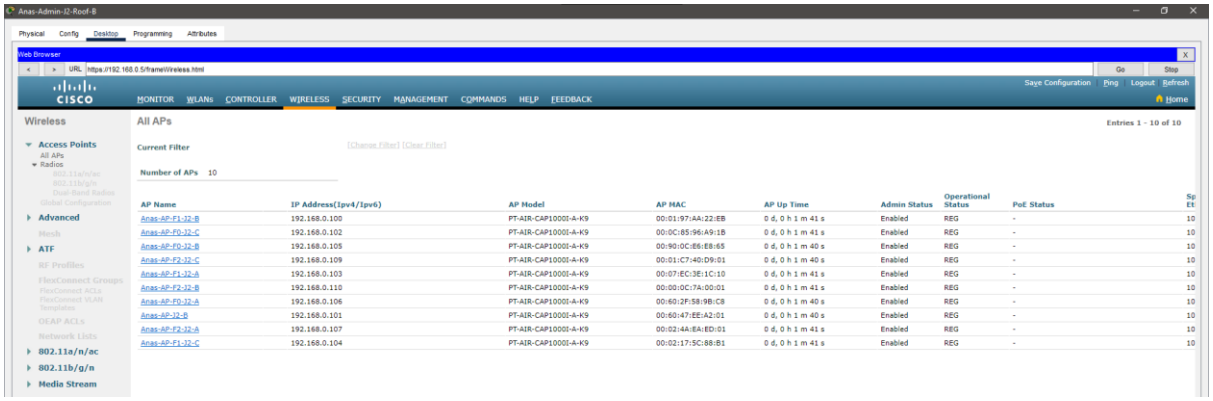

Figure 27 All the Access Points

Here we can see all the access points that's is connected to the WLC

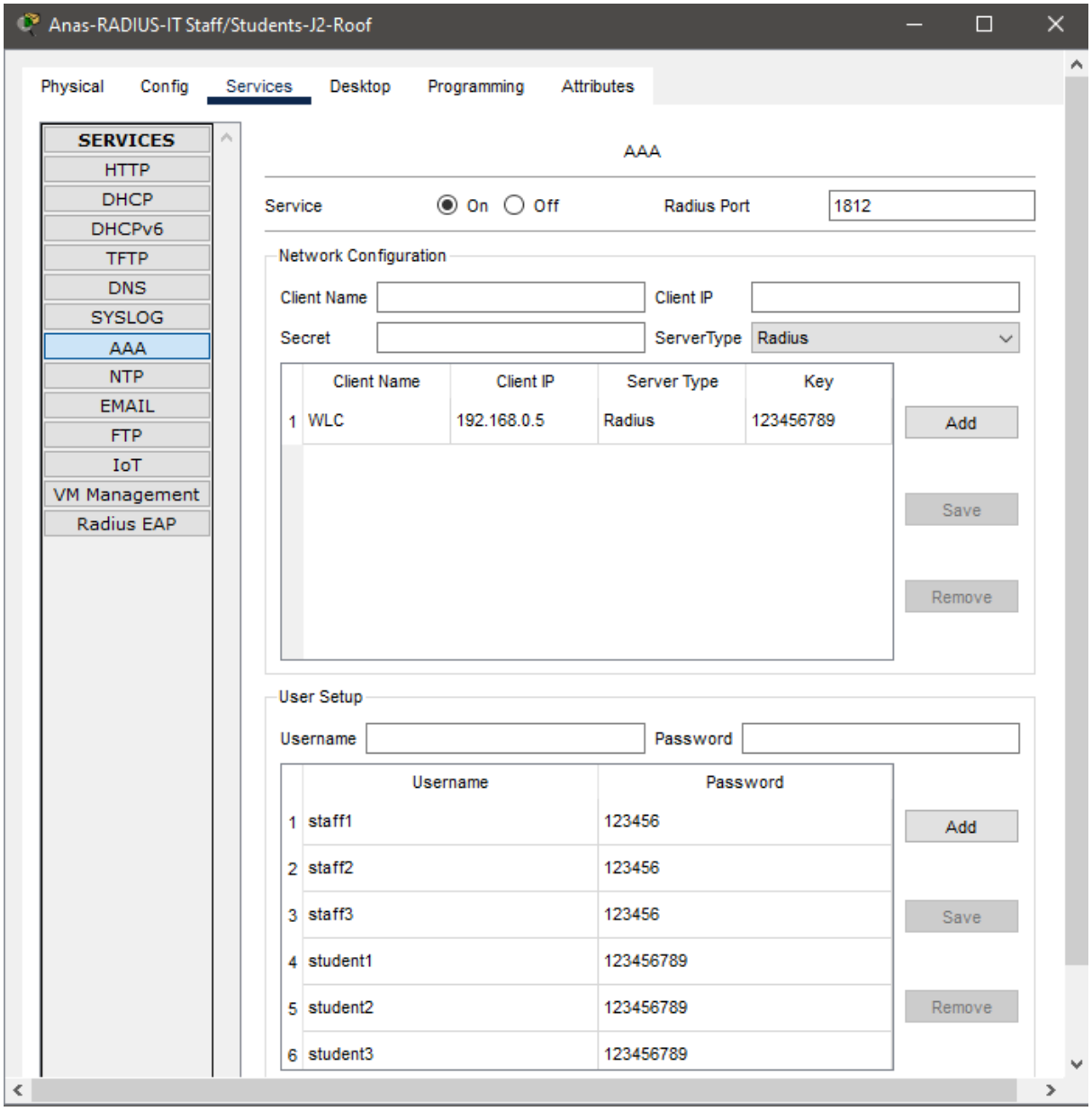

Figure 28 Changing the Port Number

We change the port number from 1645 to 1812

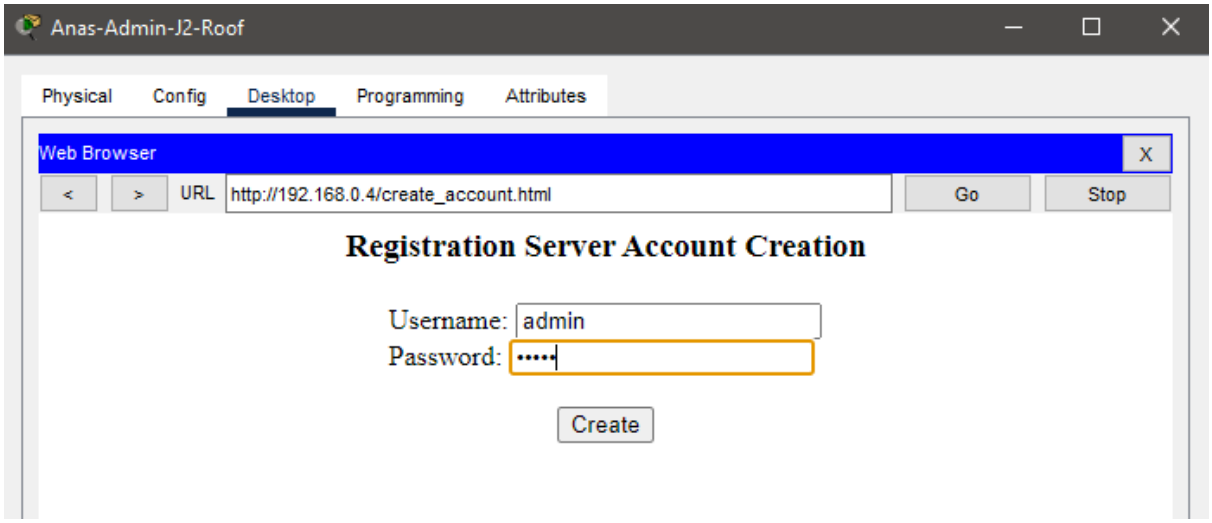

Figure 29 Creating IoT Account

Creating the IoT account so we can have a control to them

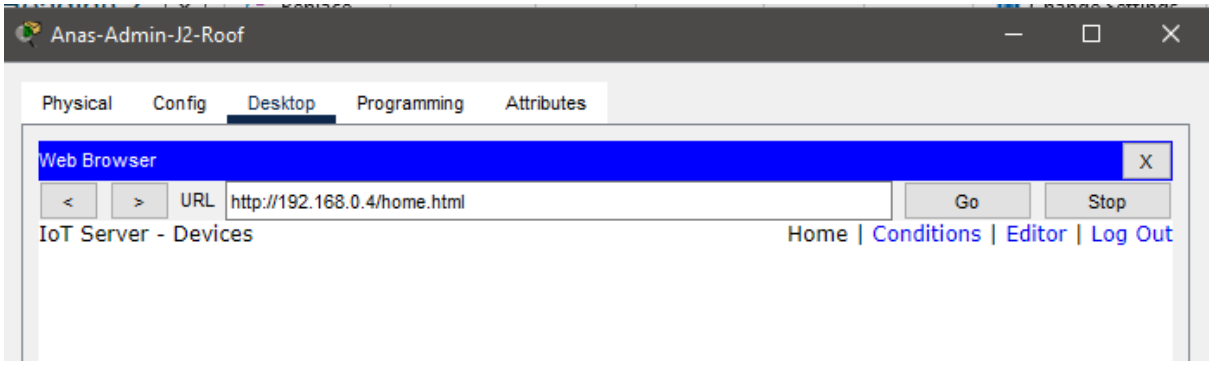

Figure 30 Home Page for IoT Controller

Here we have the home page, right now we didn't connect any device to it yet

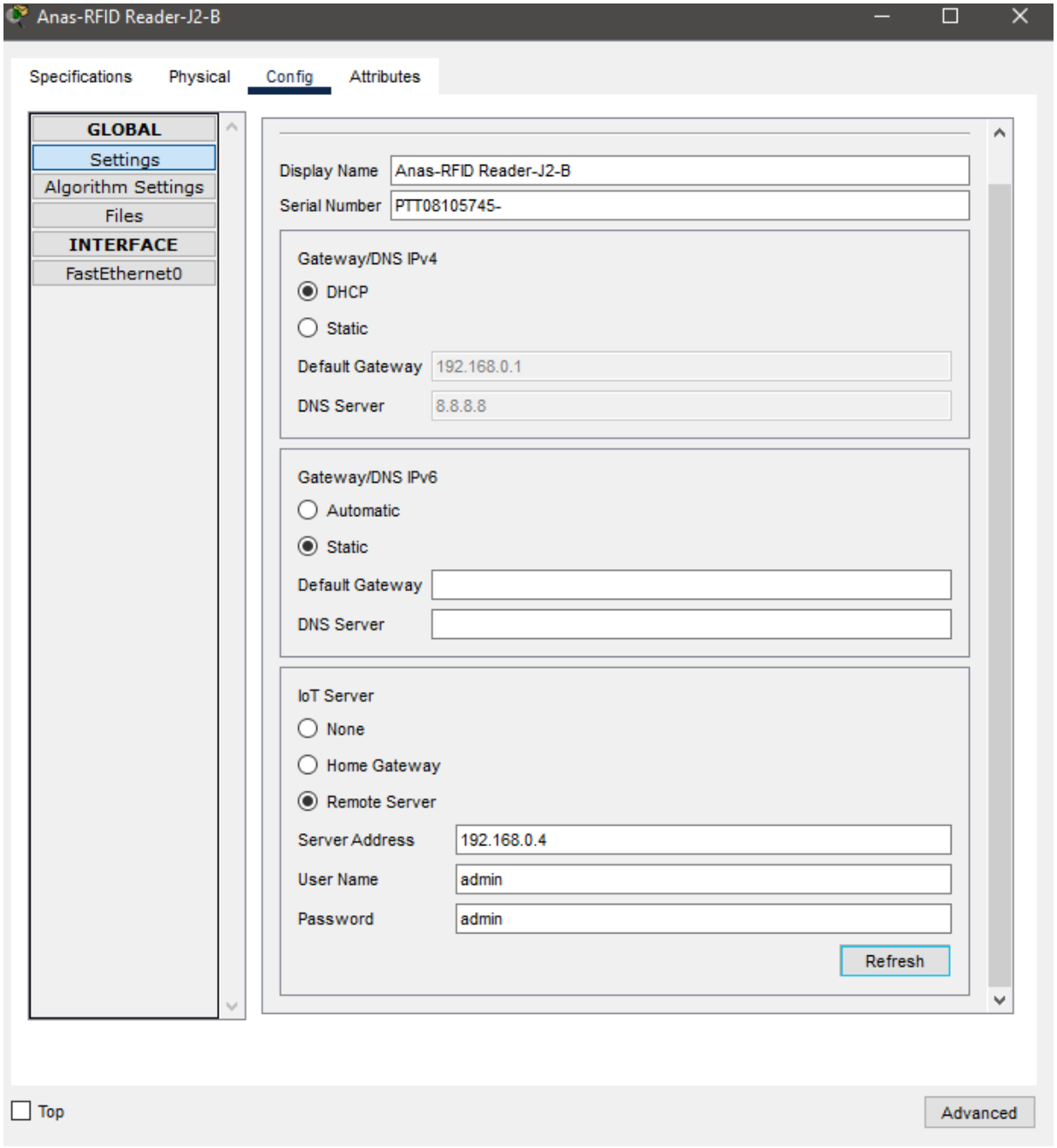

Figure 31 RFID Reader Connection

Connecting the RFID Reader to the IoT controller

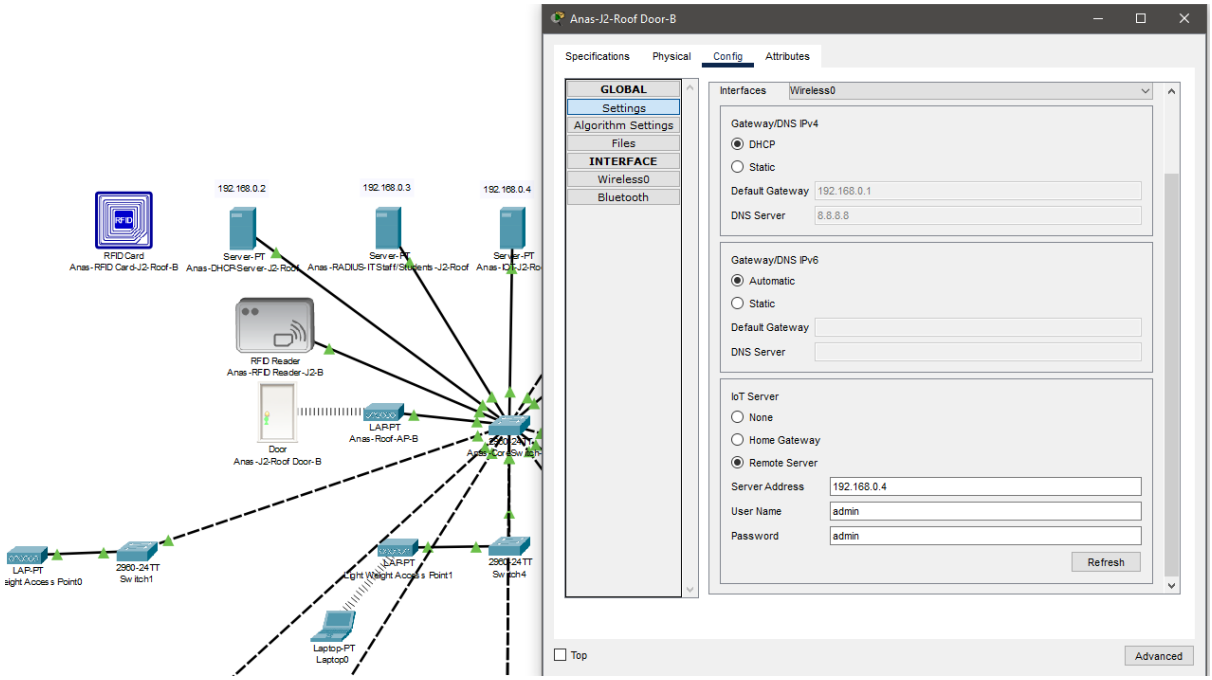

Figure 32 Connecting the IoT Door

Connecting the door to the server so we be able to give it conditions

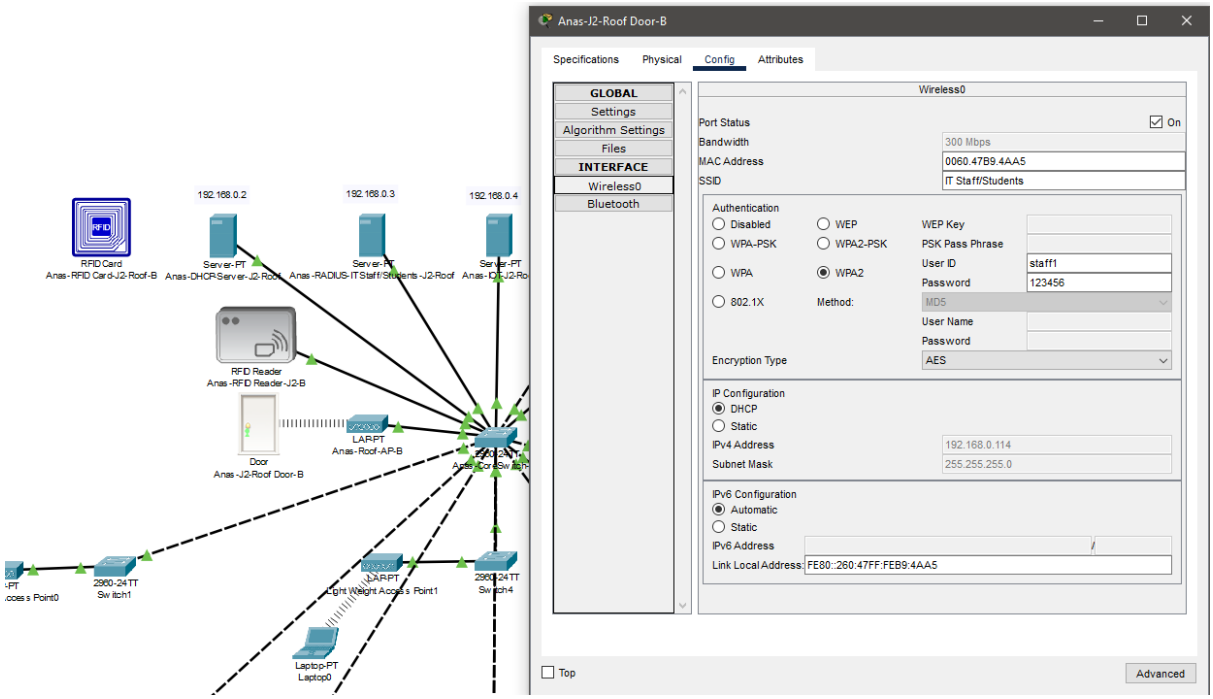

Figure 33 Connecting the Door to the AP

We connected the door the AP so it can be connected to the network by Assigning SSID and user ID and Pass for the Door

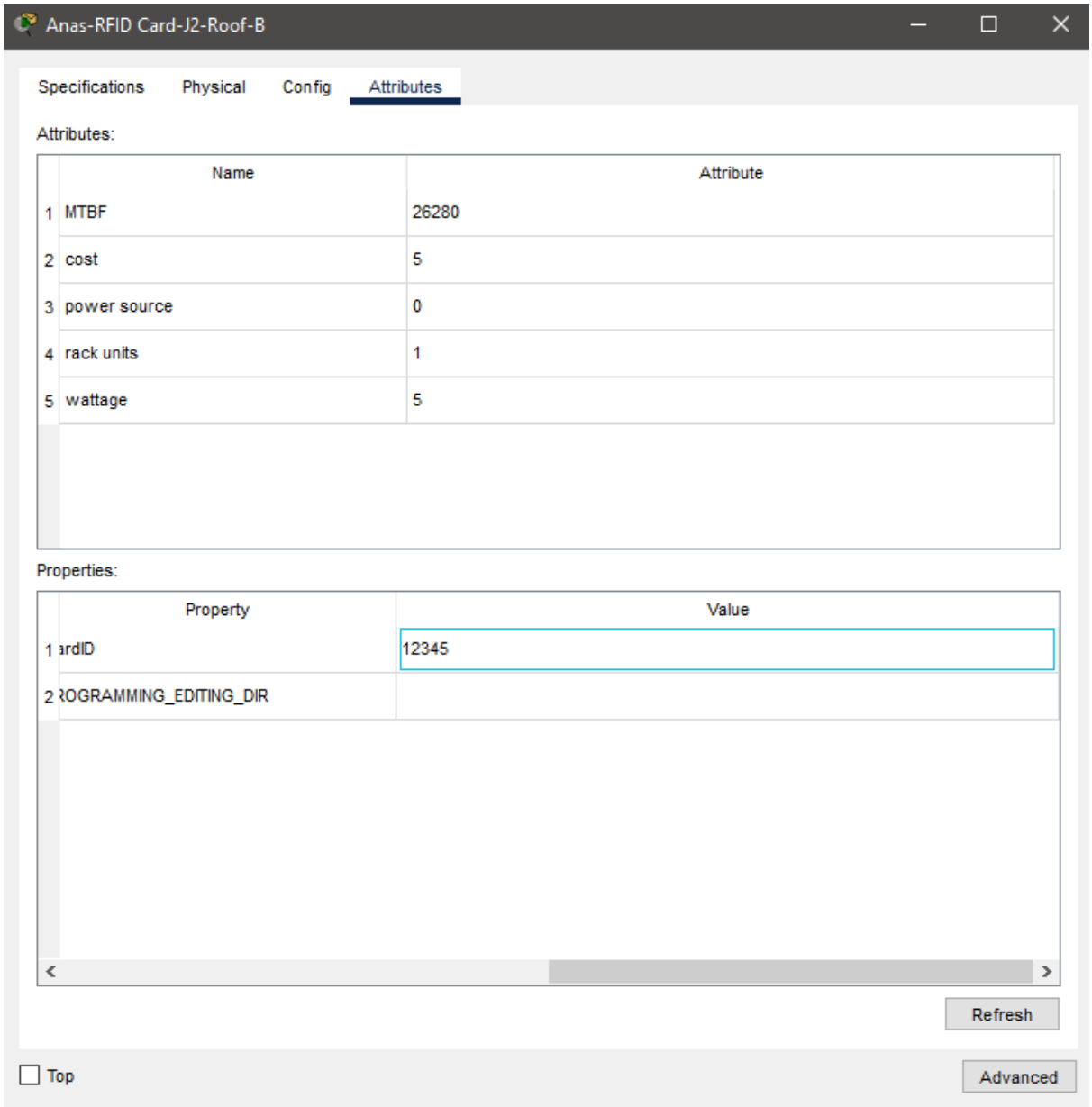

Figure 34 Card Value

Changing the value for the Card so they can access using the card which is 12345

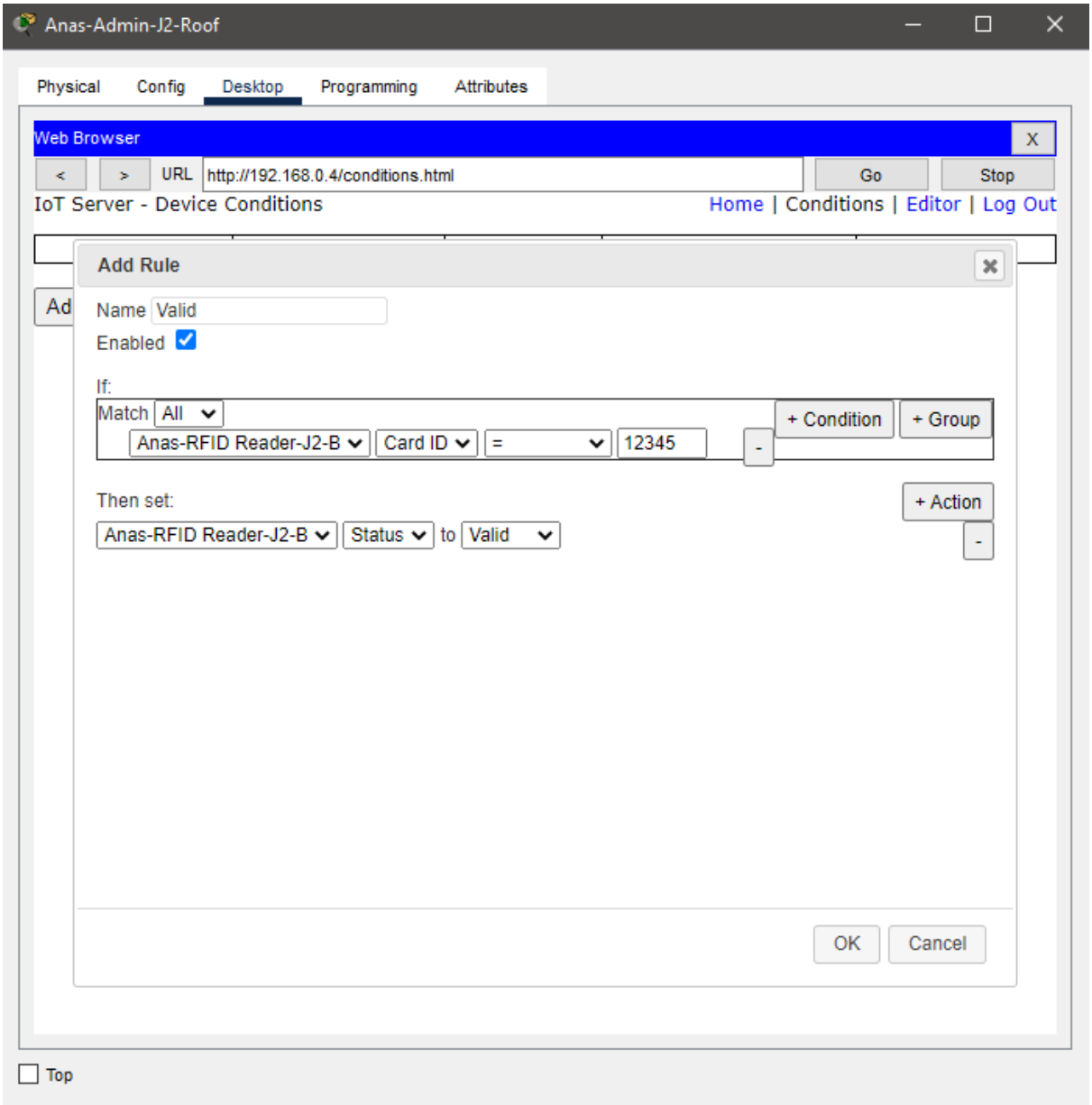

Figure 35 Valid Condition

Applying the Valid condition, so Here we set conditions for the door to be able to open for the staff only

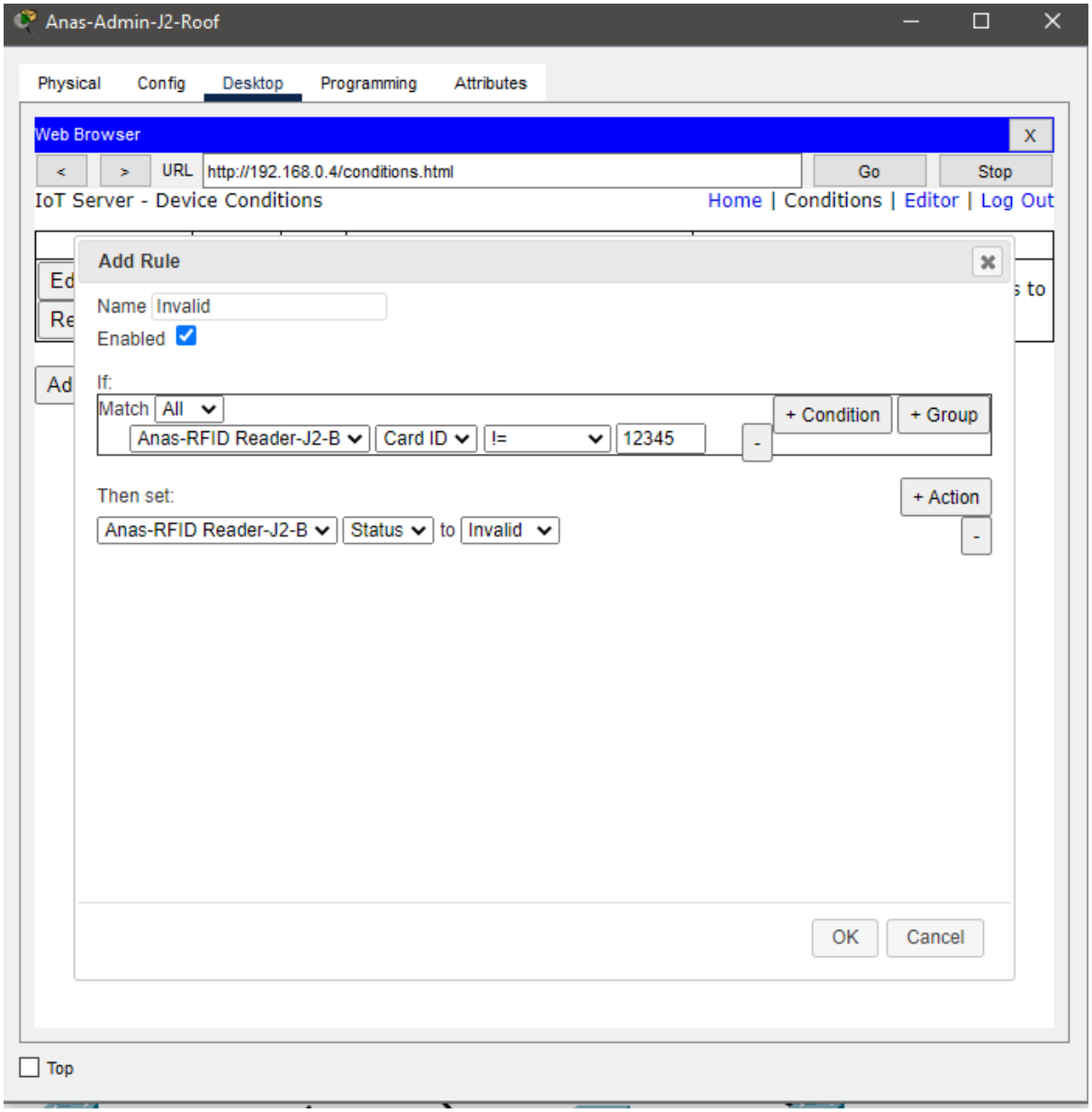

Figure 36 Invalid Condition

This is for the Invalid condition

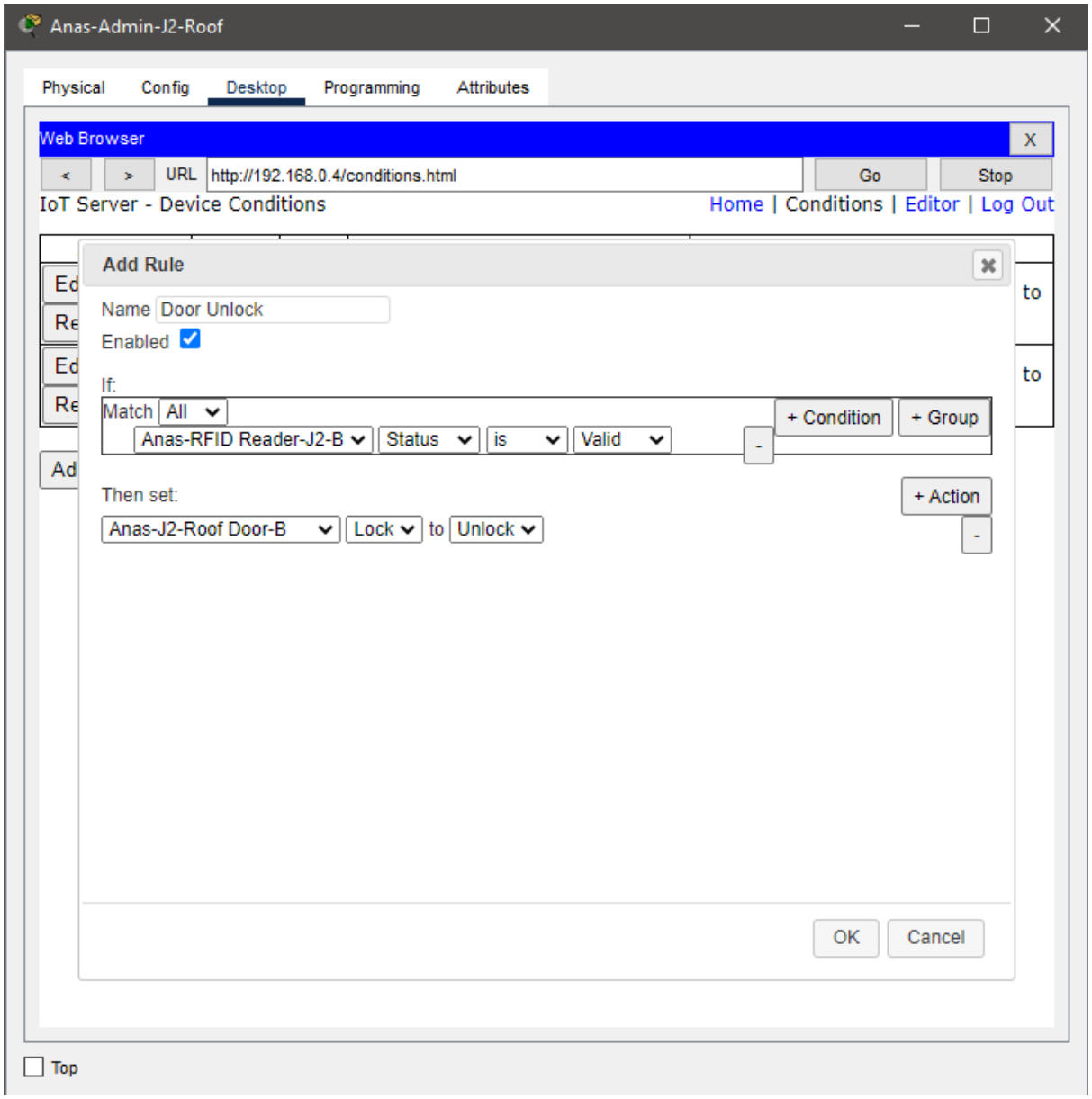

Figure 37 Door Unlock

Door Unlock Condition

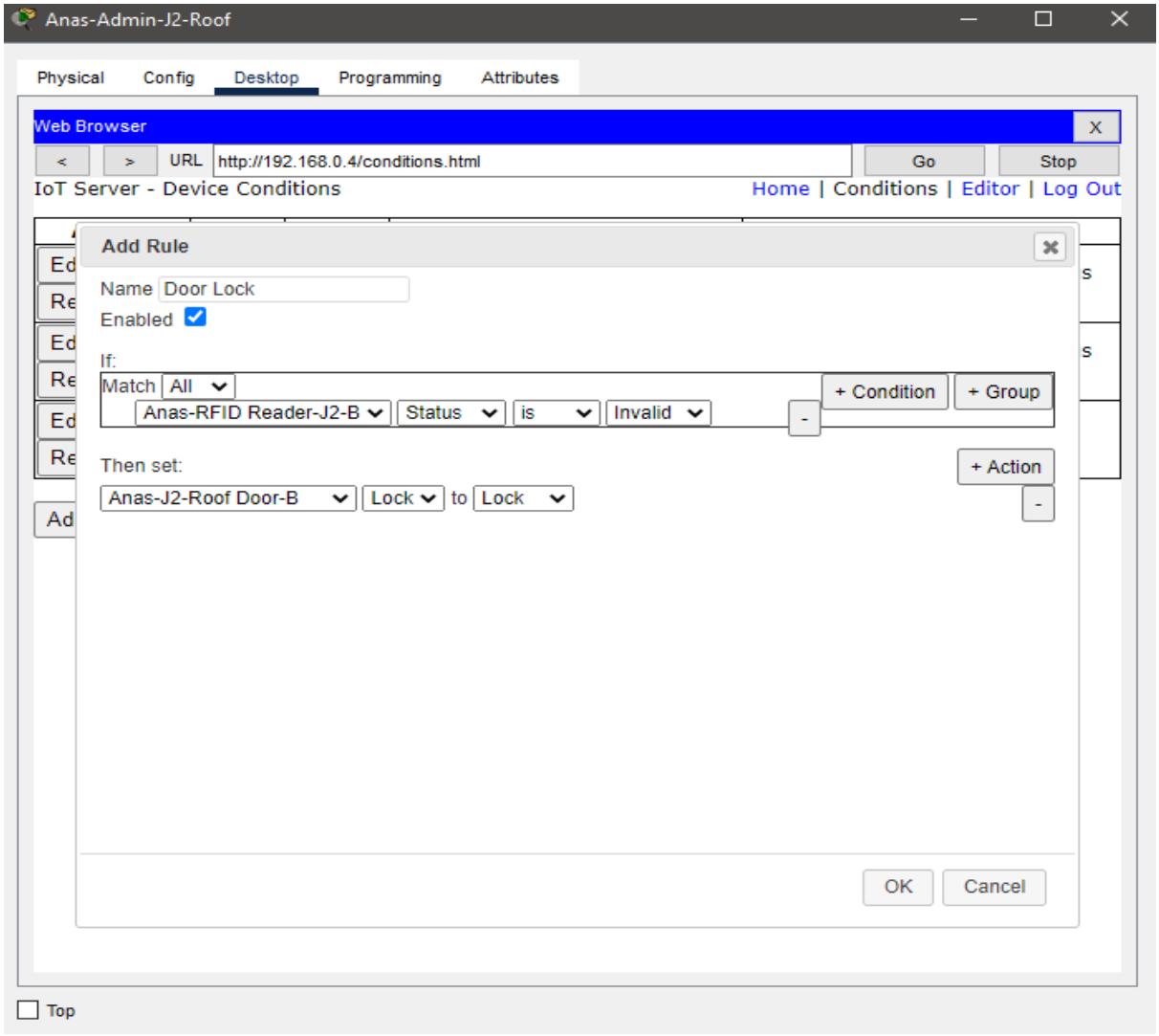

Figure 38 Door Lock

This condition is for the Door Lock

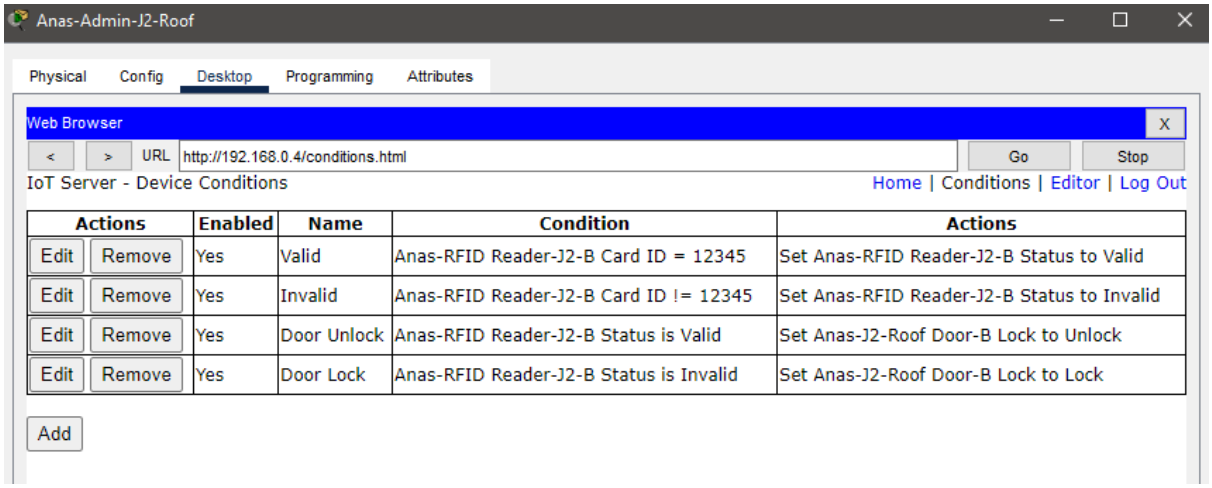

Figure 39 All Conditions

these are all the conditions for the Door

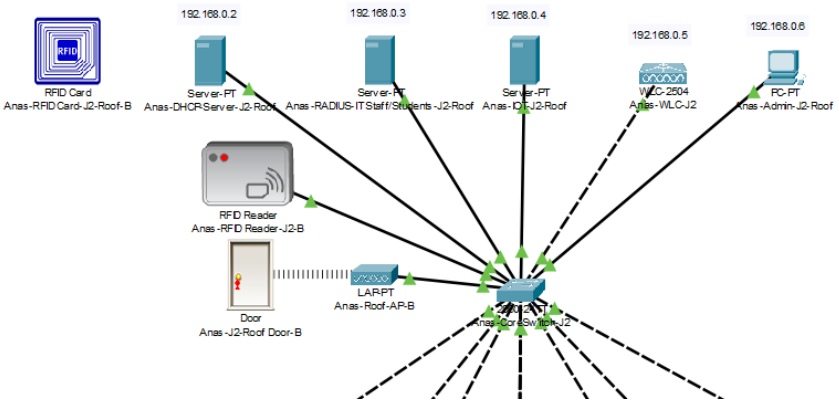

Figure 40 Door Locked

as we can see the Door is lock so the students or the unauthorized people can't access it

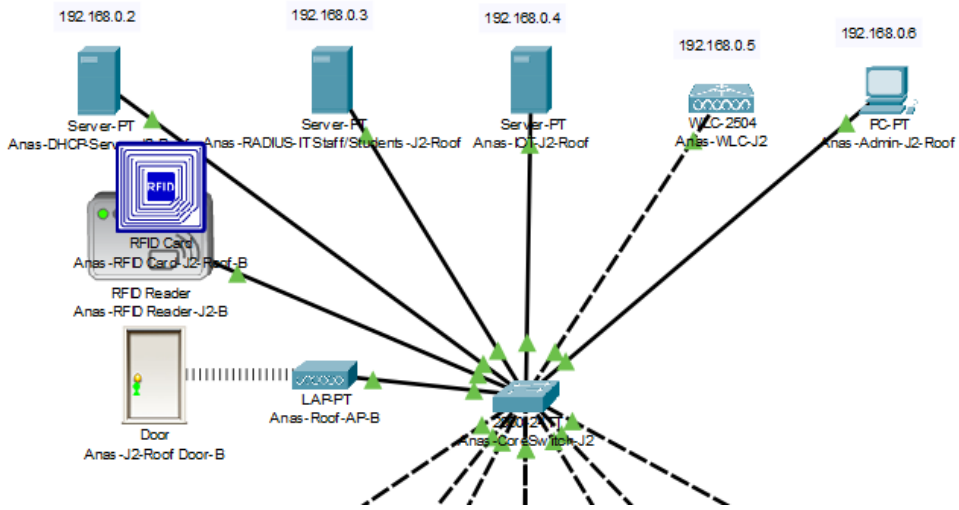

Figure 41 Door Unlock

But the Card that only the Authorized people will have it open

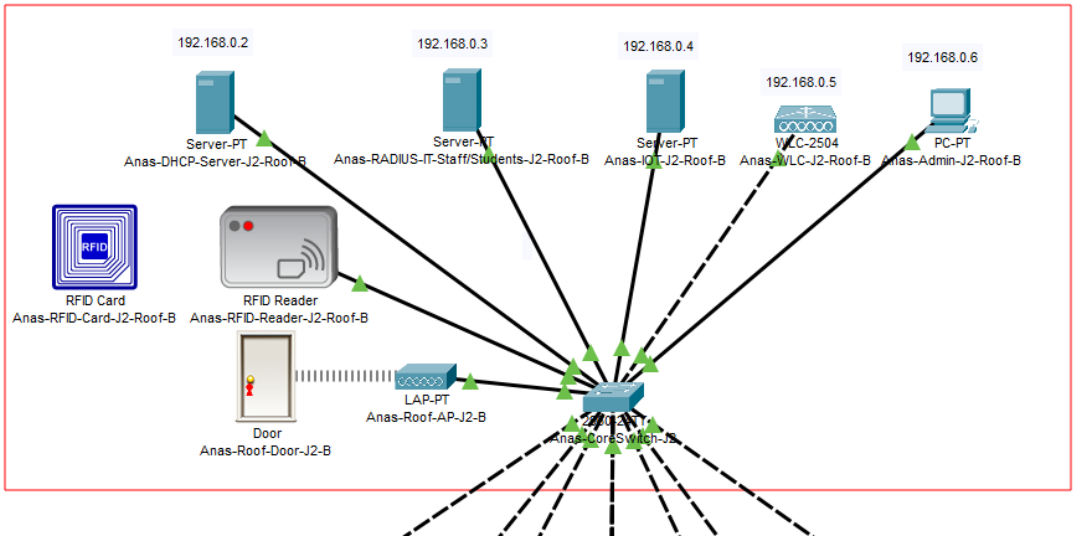

Figure 42 Roof Final Setup

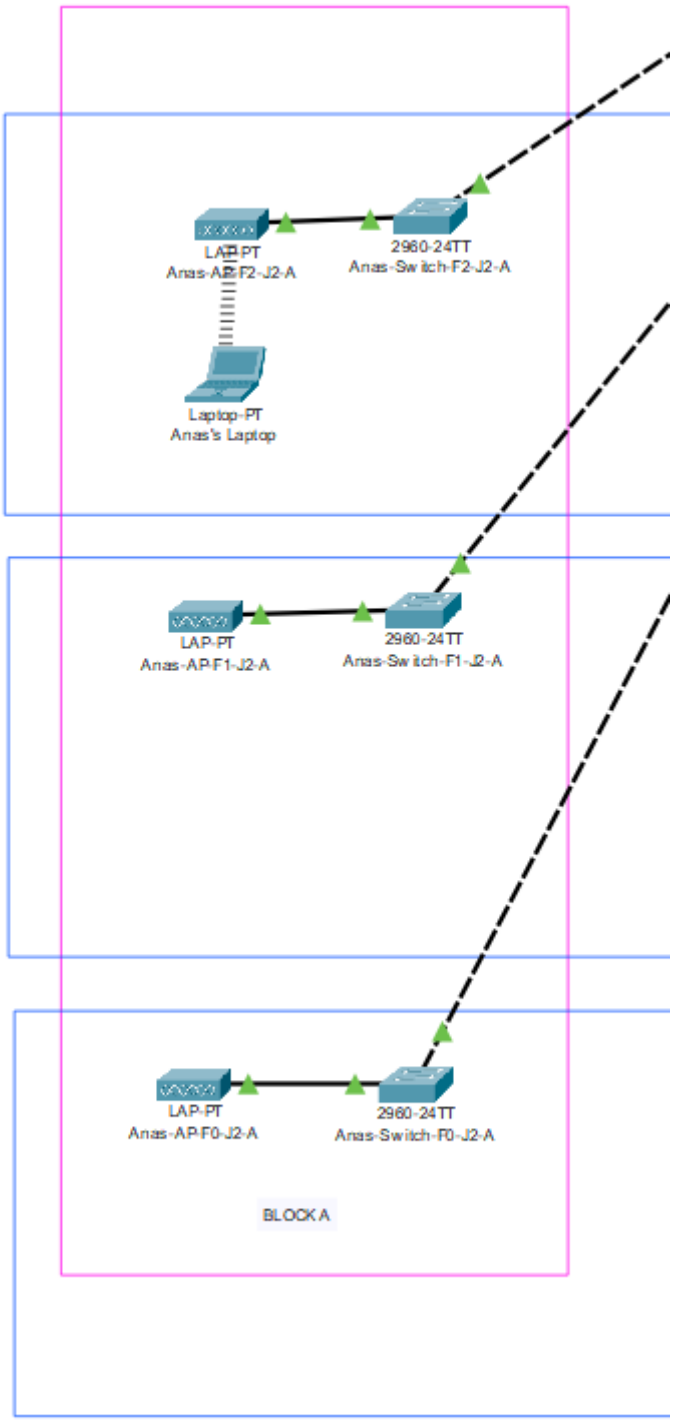

Figure 43 Block A Final setup

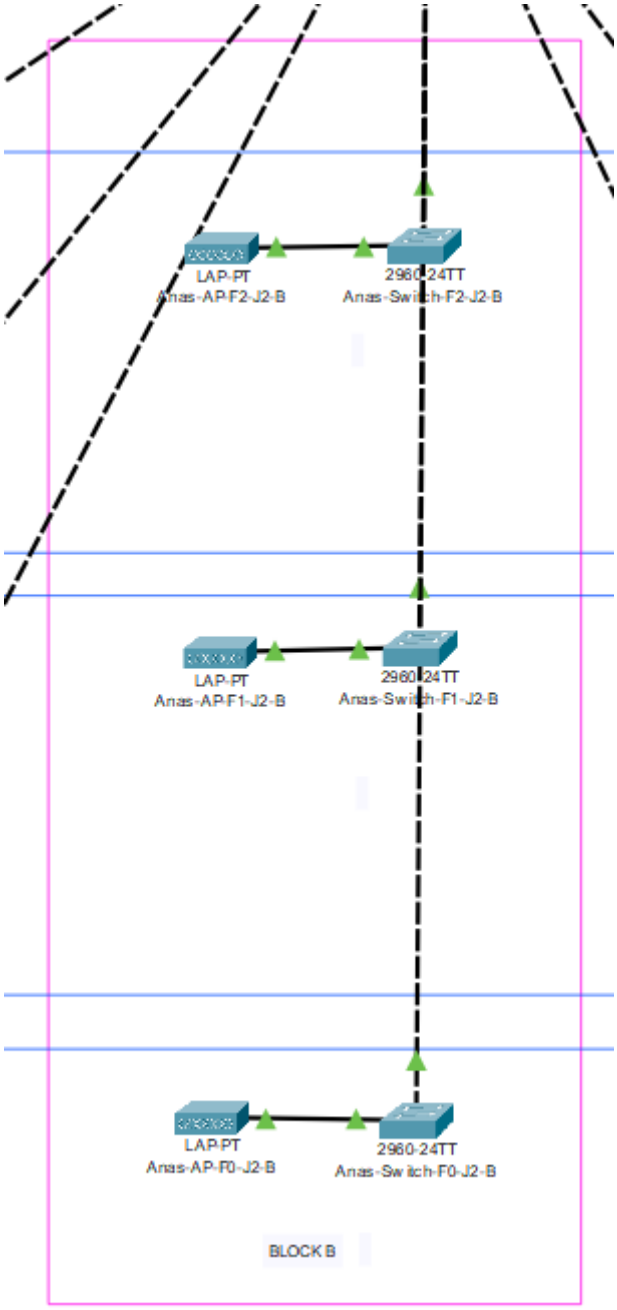

Figure 44 Block B final setup

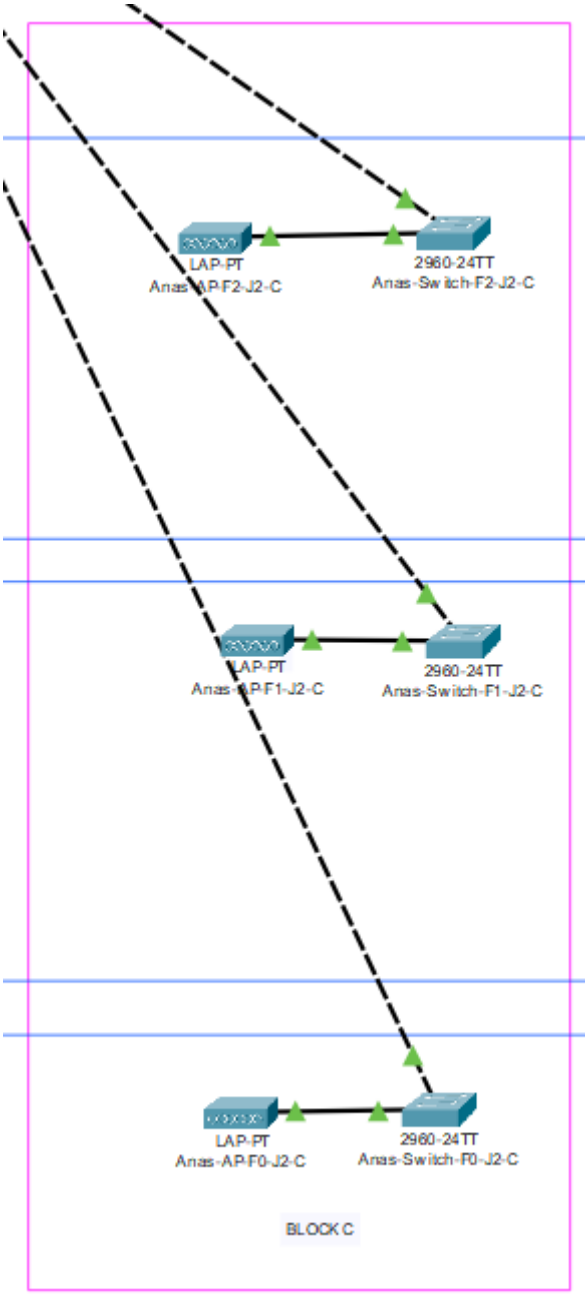

Figure 45 Block C final setup

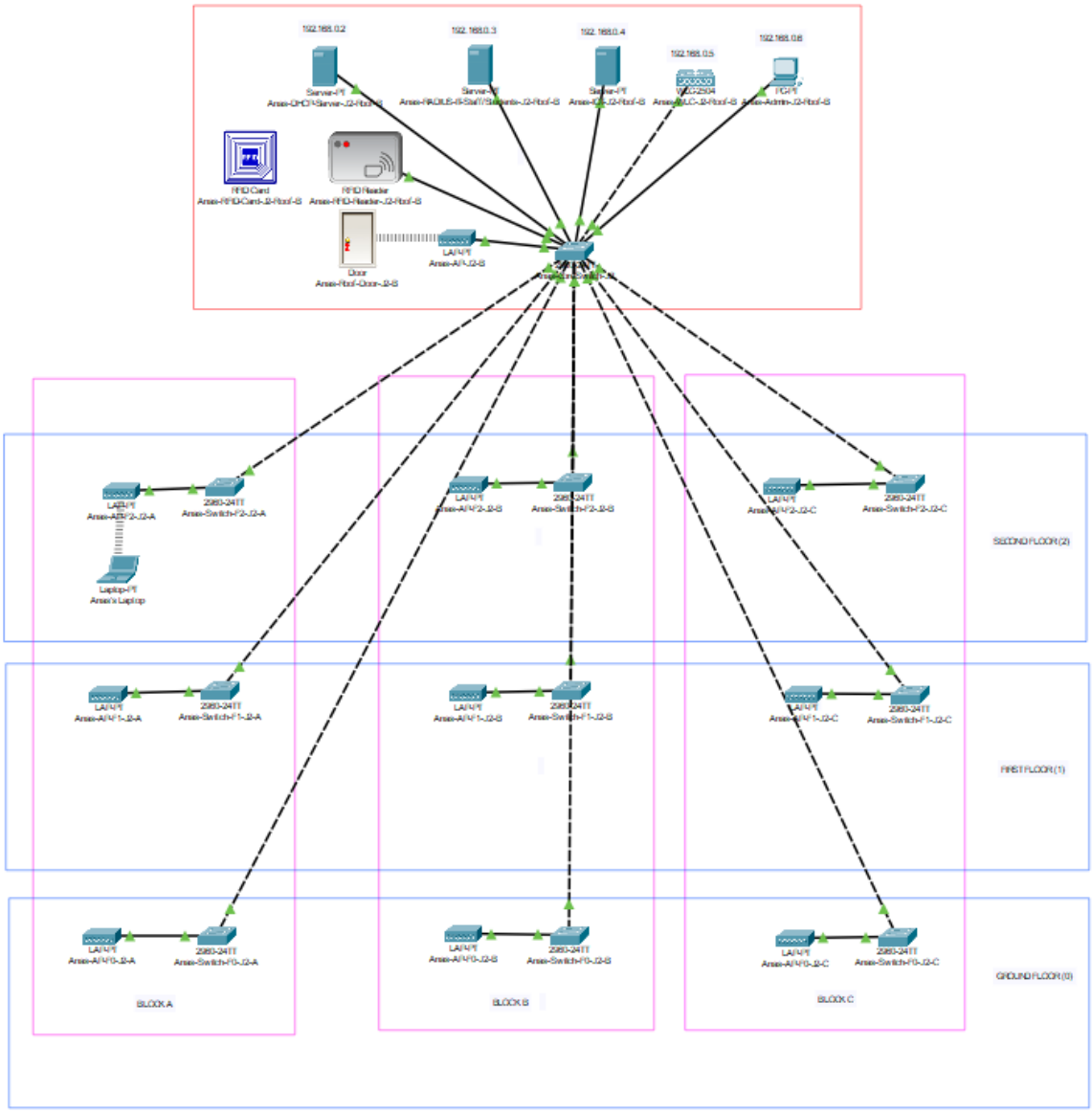

Figure 46 Final setup Topology

Security Analysis and Evaluation (Answering the Questions)

2.a Security Requirements and Implementation

The secure network authentication system enables only authorized users with valid username and passwords to connect Wi-Fi through WPA2 protocol 802.1X. The authentication process results from connection to the RADIUS server at IP 192.168.0.3 that verifies permission status of connecting users.

Both staff and students use the single "IT Staff/Students" SSID as their wireless network access point and the network lacks virtual LAN configuration. Students and staff use the same network, but genuine administrator-access requirements continue to apply. The WLC administers wireless functions by requiring staff members to authenticate with port 1812 of their respective RADIUS server at IP address 192.168.0.5.

The network provides access exclusively to those users that administrators add to the RADIUS server authentication system. The students who pick and choose will be refused network access despite their ability to view the network name.

2.b Evaluation of the Selected Security Scheme

The Wi-Fi network remains protected because it enables access to account holders exclusively, which excludes unauthorized users.

The radius server serves us by achieving student and staff access authorization, which was our primary objective. Each person accesses the network using their username together with their password and the university has an easy method to revoke access for departed staff and students.

References

- Lucidchart. (2025). *Network topology design tool*. Retrieved from https://lucid.app/
- Ajman University. (2025). *Network Final Project Topology*. Retrieved from Ajman4-my.sharepoint.com