VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Nikolaos Karampelias

# EXTENDED SERVICE SET WLAN CONFIGURATION USING NETGEAR WAX610 ACCESS POINTS

School of Technology
2023

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Information Technology

## ABSTRACT

| | |
|---|---|
| Author | Nikolaos Karampelias |
| Title | Extended Service Set WLAN Configuration Using Netgear WAX610 Access Points |
| Year | 2023 |
| Language | English |
| Pages | 34 |
| Name of Supervisor | Chao Gao |

Wireless Local Area Networks have become an essential part of contemporary network structure meaning that the demand for such a high-performance WLAN, especially in organizational environments, is decisive.

This thesis aims to configure and deploy an Extended Service Set WLAN by using two NETGEAR WAX610 Access Points, which will allow the wireless clients to roam within the network seamlessly and without connection interruptions.

The study of the 2.4 GHz and 5 GHz bands was conducted to select the best channel allocation, deal with interference and coverage area and achieve optimal and user-friendly performance.

The security of the network was also considered. A RADIUS server was employed to authenticate the wireless clients and it will allow only those with stored credentials to connect to the wireless network.

Additionally, the Wi-Fi radio settings provided by the APs were studied; it remains to be seen how they affect the clients as well as the entire network.

Finally, the results showed that the configuration of the equipment and the entire network was successful, and the fundamental goal of an extended service set was accomplished.

Keywords Extended Service Set, Roaming, Wireless LAN

## CONTENTS

**LIST OF FIGURES**

# 1 INTRODUCTION

Nowadays, a Wireless Local Area Network (WLAN) is a necessary facility for any organization. A home WLAN is configured by deploying a so-called Wi-Fi router that connects all wireless devices such as laptops, smartphones, and home appliances to the Internet. Such a network is called a Basic Service Set (BSS) and the coverage area is restricted by the wireless signal range, which usually is around ten to thirty meters in an indoor environment.

However, an organizational WLAN usually needs to cover a much larger area such as a campus, an office building, a factory, or a shopping mall. Therefore, the WLAN must be deployed as an Extended Service Set (ESS). An ESS WLAN will use multiple connecting devices, called Access Points (AP) to increase the coverage range. In such a configuration, many things are different from a single Wi-Fi router home configuration.

This thesis aims to inspect the features of an Extended Service Set WLAN and deploy such a network using multiple APs.

## 2 THESIS OBJECTIVES

The main goal of this project is the formation and successful operation of an Extended Service Set WLAN. This will be conducted by the deployment of two NETGEAR WAX610 Access Points which will be using different Basic Service Set Identifiers (BSSIDs), that is their Media Access Control (MAC) addresses and the same Extended Service Set Identifier (ESSID), which is the network name. Furthermore, a Raspberry Pi (RPi) 3 Model B will operate as a Dynamic Host Configuration Protocol (DHCP) server as well as a Remote Authentication Dial-In User Service (RADIUS) server. All the above components will be connected to a Cisco SG110D-05 switch, which in turn will connect to a TP-Link Archer C50 default gateway router for Internet access. Figure 1 shows the network structure.

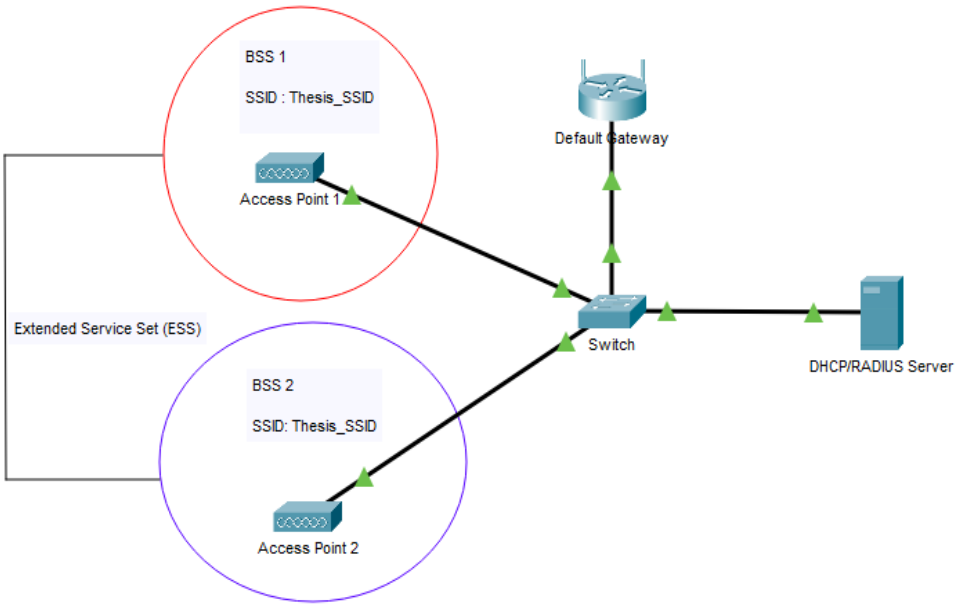


**Figure 1.** The network structure of the project.

After the successful operation of the ESS WLAN, the final goal of the project is to document a four-hour laboratory exercise for the Wireless Networks course.

# 3 THEORETICAL BACKGROUND

Before proceeding with the equipment configuration and the project deployment, it is required to provide the necessary theoretical information regarding the WLAN spectrum at both 2.4GHz and 5GHz radios which are offered by the NETGEAR WAX610 Access Points, as well as how the RADIUS protocol works.

## 3.1 WLAN Spectrum

Figure 2 shows that there are fourteen channels available in the 2.4 GHz band, with channel 14 available only in Japan. This means that there are only three non-overlapping channels, which are 1, 6, and 11 each with a 22 MHz channel width. So, to avoid interference and poor performance when the 2.4 GHz band is used, one of the abovementioned channels should be used. It is easily understood that with only three non-overlapping channels, network congestion, and interference would occur. /1/

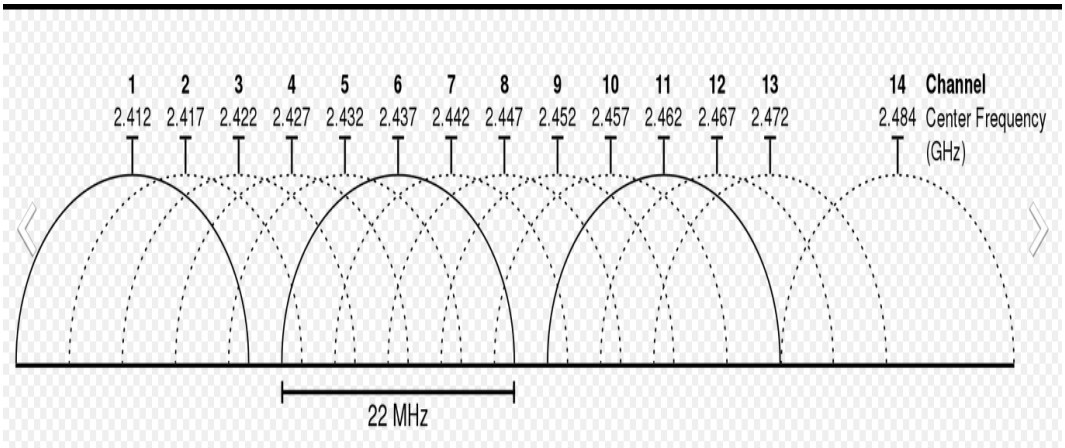


**Figure 2.** IEEE 802.11 WLAN spectrum at 2.4GHz. /1/

This problem could be solved by using the 5 GHz band which provides more channels and channel widths, as shown in Figure 3.

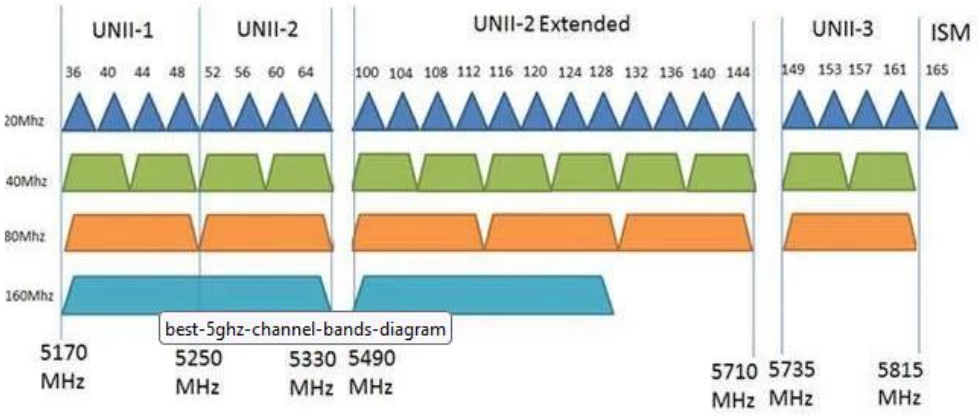


**Figure 3.** 5 GHz band spectrum. /2/

We can also see that the number of non-overlapping channels varies, depending on the channel width. It is noticeable that with the 5 GHz band, interference, and network congestion are highly decreased. /2/

At this point, it should be mentioned that both 2.4 GHz and 5 GHz can be deployed for different purposes and uses. The 2.4 GHz band will cover a greater area and transmit through walls and other solid objects, while the 5 GHz will provide greater speed and less interference due to the more non-overlapping channels. /3/

### 3.2 RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides authentication, authorization, and accounting for users who connect to a network service. The authentication methods that are used by a RADIUS server are Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), and Extensible Authentication Protocol (EAP)./4/

The 802.1X standard is used by the Access Points when a RADIUS user tries to connect to the WLAN. It is comprised of three parties which are the supplicant or the client device which is roaming in the WLAN, the authenticator or the AP, and the authentication server which is the RADIUS server. In Figure 4, we can see the communication of these parties. /5/

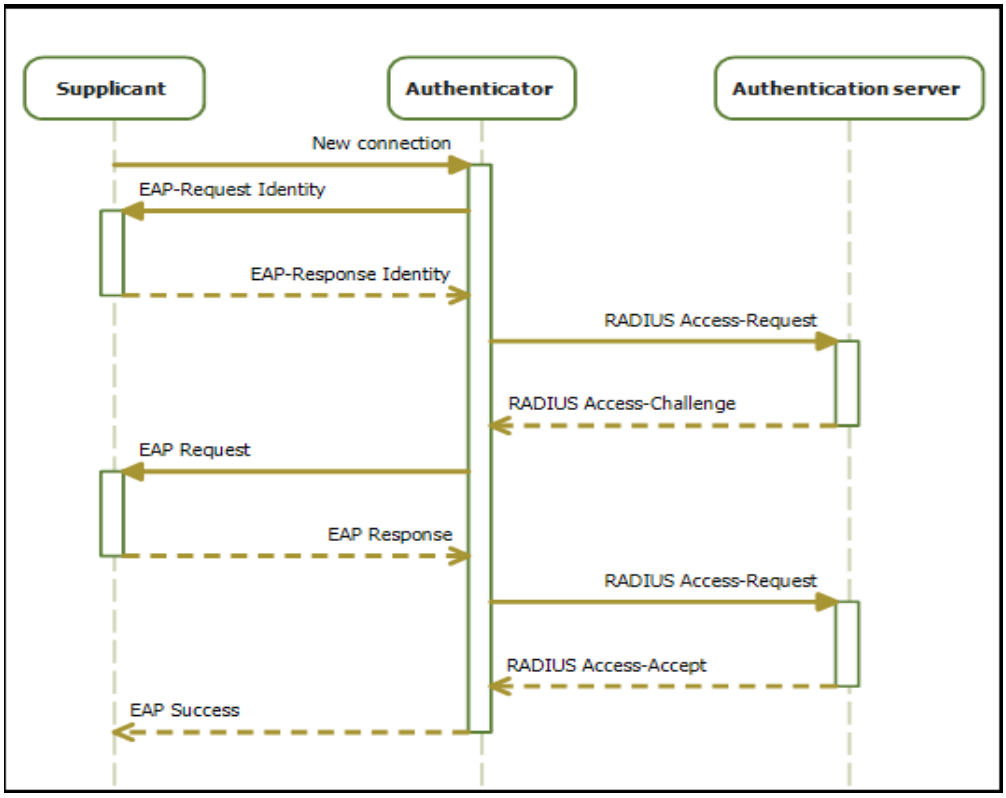


**Figure 4.** The 802.1X progression.

The EAP is used by the 802.1X AP to provide a secure authentication function and generate a Pair-wise Master Key (PMK) between the supplicant and the authenticator which is used for a wireless session using TKIP or CCMP encryption. /6/

# 4 EQUIPMENT CONFIGURATION

At this stage of the project, the devices that comprise the network were the switch, the default gateway router with an IP address of 192.168.0.1/24, and the RPi. The router, apart from the default gateway, also functions as a DHCP server. After the installation and configuration of the DHCP server on the RPi, it was disabled. When the RPi was first connected to the network, it was allocated an IP address by the router which has a DHCP range of 192.168.0.100/24 – 192.168.0.199/24, as shown in Figure 5. By navigating to the router's DHCP Clients List as seen in Figure 6, we can see the IP address that was assigned to the RPi and it was entered into the program Putty to connect to it through SSH.


**Figure 5.** DHCP range of the router.

| | | | | |
|---|---|---|---|---|
| 2 | mypi | B8:27:EB:7F:AB:A1 | 192.168.0.103 | 01:58:07 |

**Figure 6.** RPi's dynamically allocated IP.

## 4.1 Static IP address on Raspberry Pi.

It is a good option to set a static IP address on the RPi because a server must be running on a fixed IP address so that its clients can always find it. To set a static IP address, the *dhcpcd.conf* file should be configured and to do that, the command

*sudo nano /etc/dhcpcd.conf* is issued. Figure 7 shows the commands that must be typed.

```
interface eth0
static ip_address=192.168.0.2/24
static routers=192.168.0.1
static domain_name_servers=192.168.0.1
```

**Figure 7.** Static IP configuration in "/etc/dhcpcd.conf" file on RPi.

Since the RPi is connected through an Ethernet cable the command *interface eth0* should be issued, followed by the setting of the static IP address and the subnet mask. The *static routers* command was used for determining the default gateway as well as the Domain Name System (DNS) server, which in this case is the one of the default gateway. Then, the RPi was restarted with the command *sudo reboot* and this time in Putty, the static IP address was typed./7/

### 4.2 DHCP on Raspberry Pi

The Dynamic Host Configuration Protocol (DHCP) is a network protocol used for automatically assigning IP addresses and other communication parameters to devices connected to the network using a client–server architecture. /8/

For this project, the ISC DHCP server was installed. The installation began with the command *sudo apt-get install isc-dhcp-server*. After the installation an error occurred, while the system was trying to start the DHCP service, as seen in Figure 8.

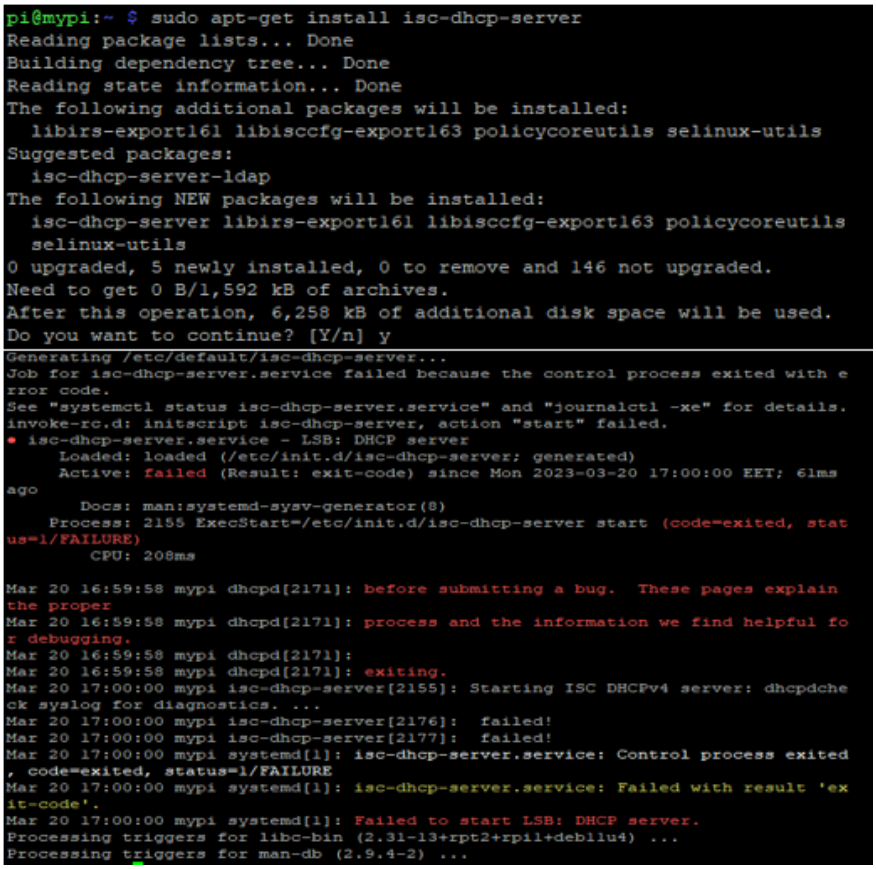


**Figure 8.** Error after the installation of ISC DHCP server.

First, the network interface which the ISC DHCP server will work for, was defined. To access this, we the command *sudo nano /etc/default/isc-dhcp-server* and apply *eth0* were entered, as depicted in Figure 9.

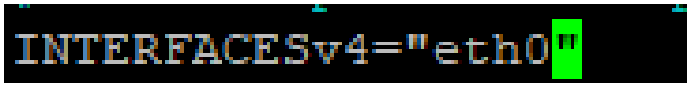


**Figure 9.** Interface for which the ISC DHCP server will work.

After this, the file */etc/dhcp/dhcpd.conf* was configured according to Figure 10.

```
authoritative;
default-lease-time 7200;
max-lease-time 7200;

subnet 192.168.0.0 netmask 255.255.255.0 {
 range 192.168.0.10 192.168.0.100;
 option routers 192.168.0.1;
 option domain-name-servers 192.168.0.1;
}
```

**Figure 10.** DHCP server configuration.

The *authoritative* directive means that this DHCP server is responsible for the network distribution. The *default-lease-time* is the duration of the validity of the IP and is set in seconds, that is two hours, and the *max-lease-time* is the maximum time that an IP is valid, also set in seconds. Next, the subnet and netmask for which an address range, a default gateway, and a DNS server were configured. When the configuration was saved, the server could start by using *sudo systemctl start isc-dhcp-server*. /9/

### 4.2.1 Testing the DHCP Server

After installing and configuring the DHCP server on RPi, it was time to disable the DHCP server on the default gateway router and test the functionality of the newly configured server. A Windows laptop and an Android phone were connected wirelessly to the network and as shown in Figure 11 and Figure 12, the DHCP server was functioning properly and assigned IP addresses within the range specified above, as well as a default gateway, a subnet mask, and a lease of two hours.

```
IPv4 Address. . . . . . . . . . . : 192.168.0.10(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Lease Obtained. . . . . . . . . . : Tuesday, 31 January 2023 12:47:05
Lease Expires . . . . . . . . . . : Tuesday, 31 January 2023 14:47:05
Default Gateway . . . . . . . . . : 192.168.0.1
DHCP Server . . . . . . . . . . . : 192.168.0.2
DNS Servers . . . . . . . . . . . : 192.168.0.1
```

**Figure 11.** Correct functionality of DHCP server on Windows 10 laptop.

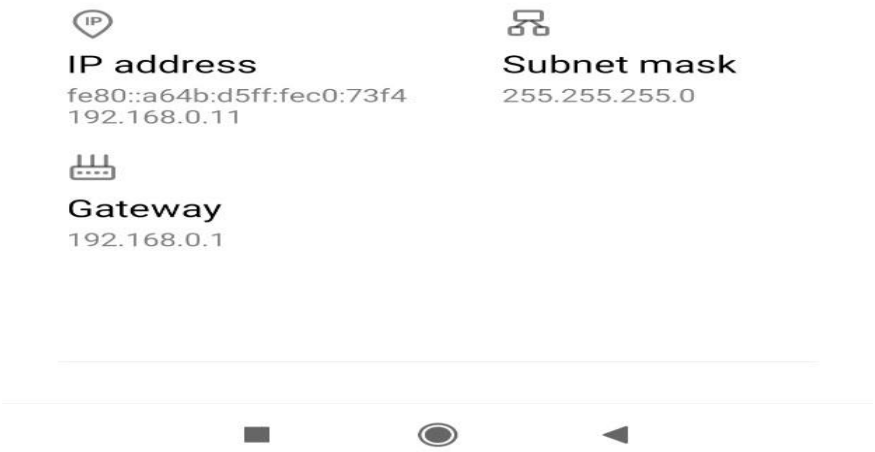


**Figure 12.** Correct functionality of DHCP server Android phone.

### 4.3 First Access Point

Next, the first of the two APs was connected to the network. This AP has a Media Access Control (MAC) address of 80:cc:9c:d0:de:df and an IP address of 192.168.0.13 that was assigned by the RPi, as depicted in Figure 13. During the configuration, a static IP address was set.

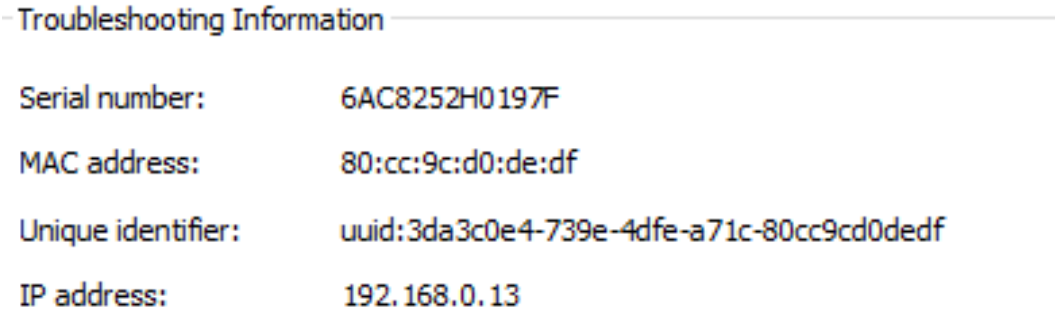


**Figure 13.** MAC and IP address of first Access Point.

This AP was configured via the local browser over the LAN. This local browser runs on a Windows laptop which is connected to the same network as the AP, with an IP address of 192.168.0.10. By entering the IP address 192.168.0.13 that was assigned to the AP by the RPi in the address bar, at first, we were presented with a security warning because of the self-assigned certificate, and we could proceed

normally. At the sign-in page, the default username and password must be entered which are *admin* and *password* respectively. When the Day Zero Easy Setup displays, the Web-browser button should be selected, as in Figure 14 and settings can be made.

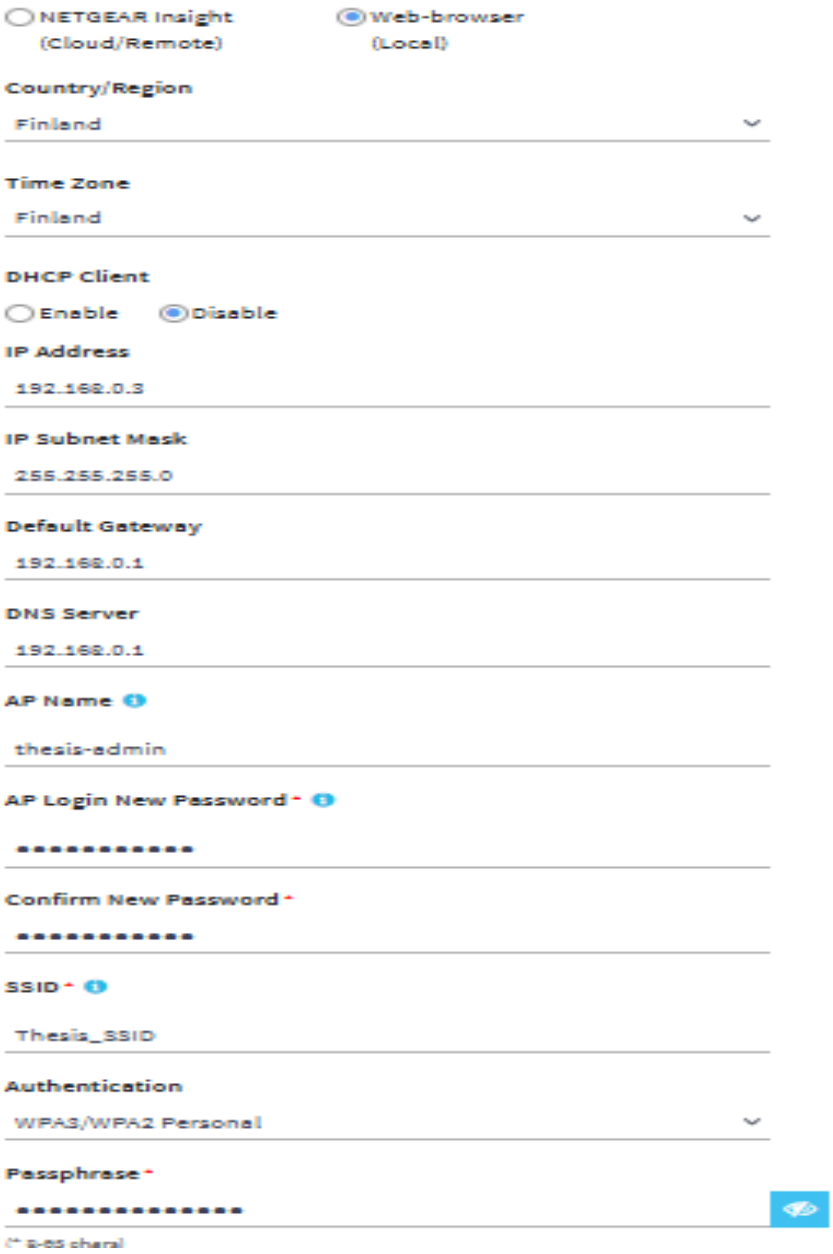


**Figure 14.** Web-browser configuration of Access Point.

A static IP address 192.168.0.3 was assigned because we did not want it to change every time, along with the subnet mask, default gateway, and DNS server. Next,

we assigned the AP's name, password, and the SSID, which was also the same as the second AP. As for the Authentication, we chose WPA3/WPA2 Personal and a Passphrase, which was changed into WPA2 Enterprise after the setup process was completed and the RADIUS server was configured. After the restart, the AP could be accessed by entering the static IP address in the address bar. The username was *admin* as before, but the password was the "password" that we set in the *AP Login New Password* field in Figure 14. Finally, the Dashboard page was presented, as shown in Figure 15.

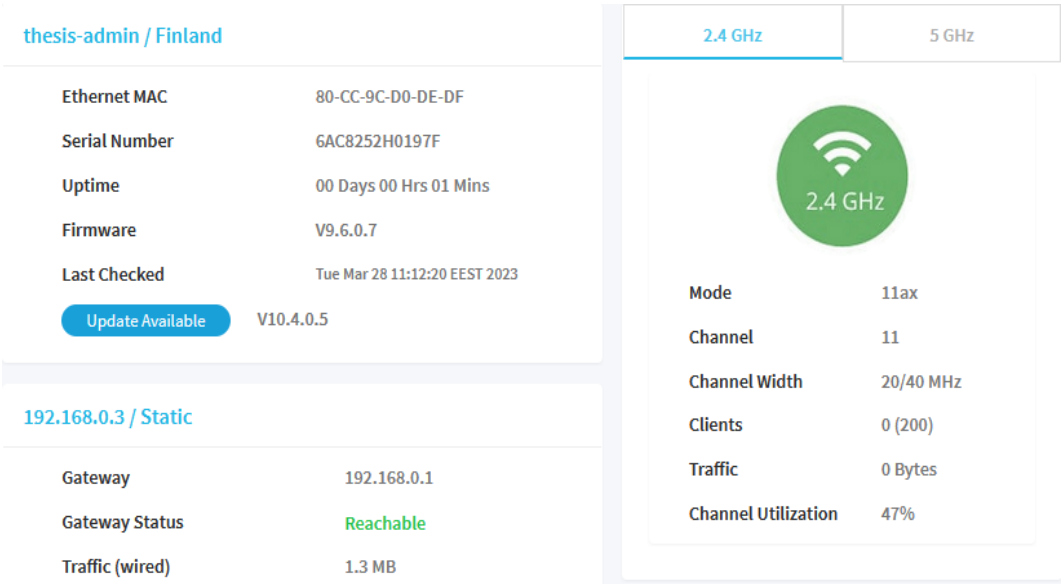


**Figure 15.** Access Point Dashboard after initial setup.

### 4.4 Second Access Point

After the connection and initial setup via the local browser of the first AP, it was time for the second AP to enter the network. This AP was configured via the NETGEAR Insight application which can be downloaded from Google Play on an Android mobile phone. After the download, we could connect wirelessly to the AP, that in its current state has an SSID *NETGEARCF421F-SETUP* and a default password of *sharedsecret.* The application was started on an Android phone. Figure 16 shows the "Create NETGEAR Account" page and the setup of the network location, in which the AP was added.

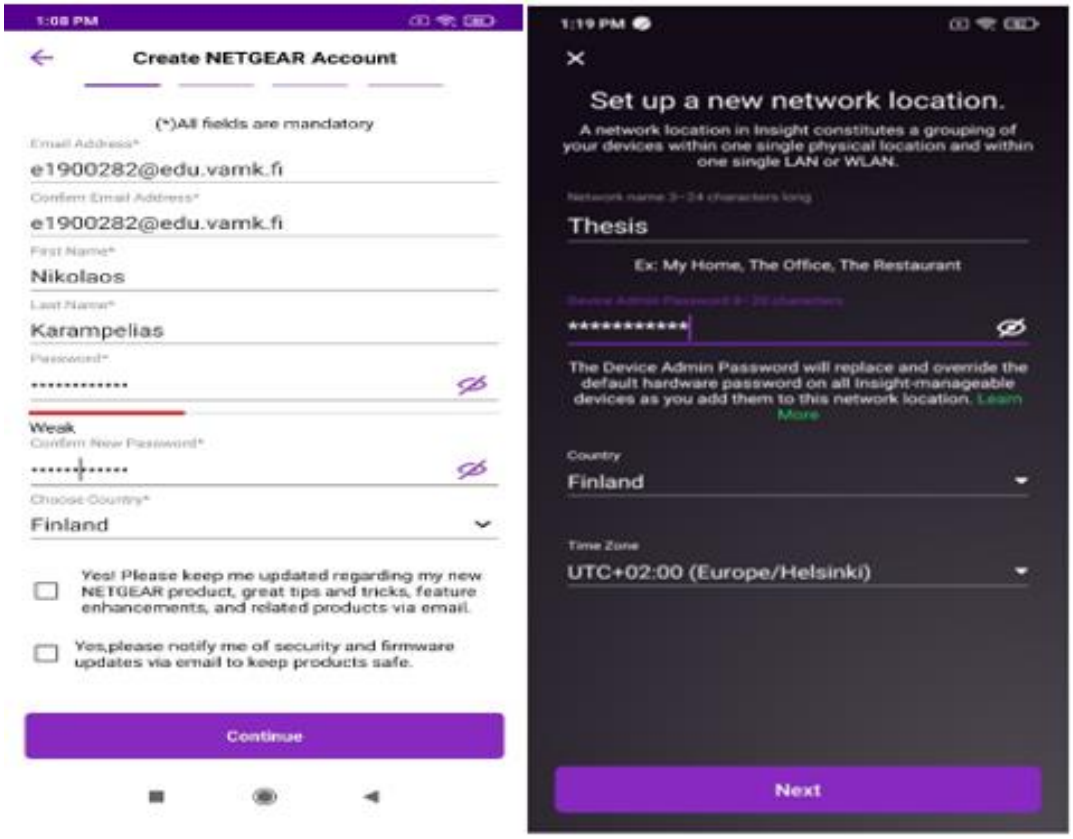


**Figure 16.** NETGEAR account and network location creation using the NETGEAR Insight application.

After the addition of the AP to the network location, the name *thesis-admin* was given to the AP and a restart commenced. We were finally presented with the environment which can be seen from Figure 17. /10/

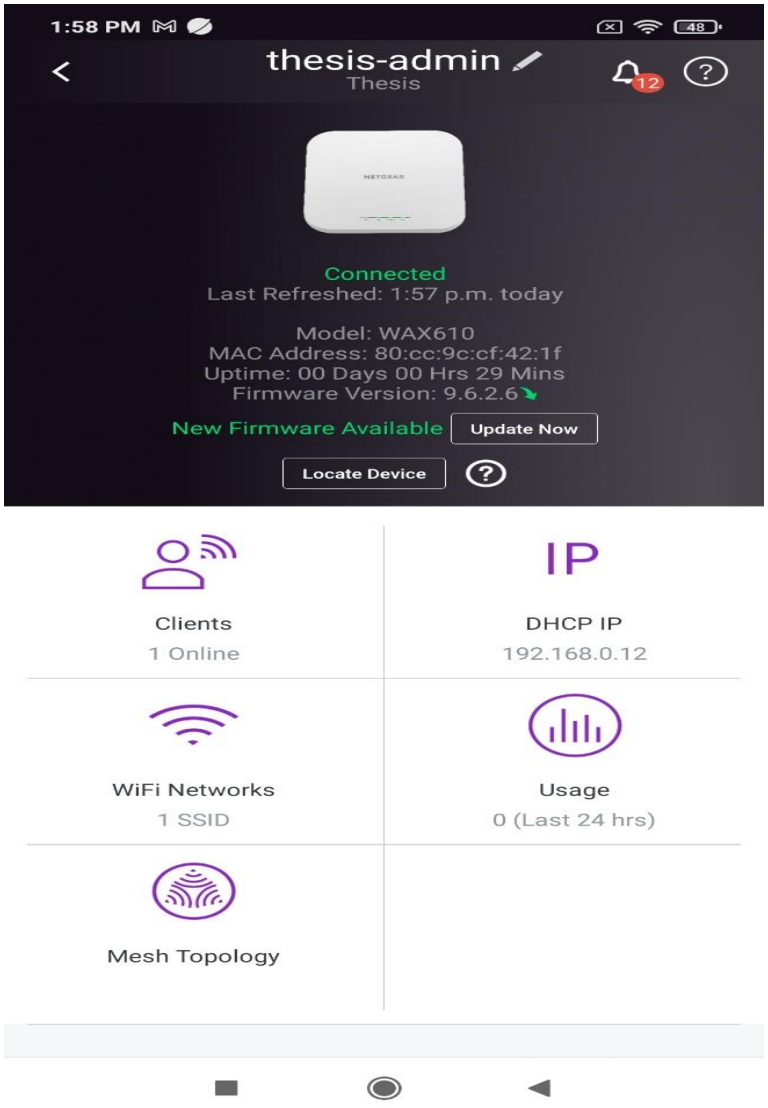


**Figure 17.** Insight application environment.

From Figure 17, it can be seen that the AP has been assigned an IP address from the RPi. As with the first AP, we set a fixed IP for this one also. To do that, we went to the "IP DHCP IP" section, and we set an IP of 192.168.0.4. Furthermore, an SSID named *Thesis_SSID* was given, the same as with the first AP. This was achieved by entering the "WiFi Networks" section and selecting *Add New WiFi (SSID).* The final configuration of the environment can be seen in Figure 18.

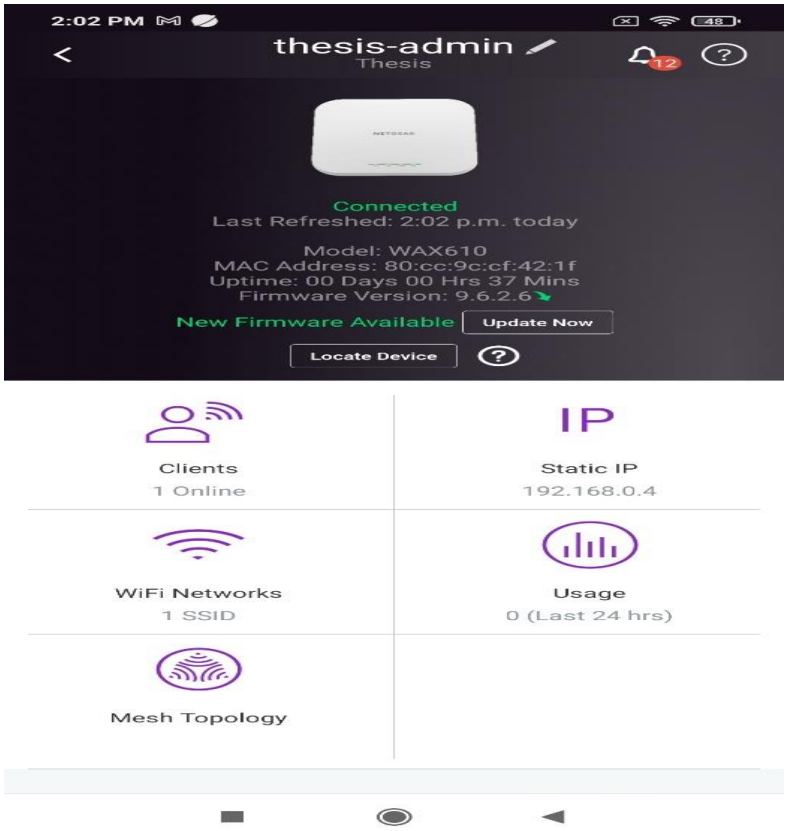


**Figure 18.** Final environment configuration.

### 4.5 Radius server on Raspberry Pi

First, the RADIUS server should be configured on the RPi. For this project, the modular FreeRADIUS was installed. The command *sudo apt-get install freeradius* was issued. After the installation, the configuration started and the first step was to add supplicants, that is users to be roaming in the WLAN. This can be done by editing the */etc/freeradius/3.0/users* file and adding the usernames and passwords, as seen in Figure 19.

```
thesis_user1 Cleartext-Password :="password1"
thesis_user2 Cleartext-Password :="password2"
```

**Figure 19.** Users to be authenticated by the RADIUS server.

The next step was to add the clients, that is the Access Points, by editing the file */etc/freeradius/3.0/clients.conf*. The fixed IP addresses that were set above for the APs were the only addresses that are able to access and communicate with the RADIUS server, as shown in Figure 20. /11/

```
client 192.168.0.3 {
 secret = radius_secret
 shortname = Thesis_SSID
}

client 192.168.0.4 {
 secret = radius_secret
 shortname = Thesis_SSID
}
```

**Figure 20.** Allowed IP addresses to communicate with the RADIUS server.

### 4.5.1 Access Points RADIUS Server

After the installation and configuration of the RADIUS server on the RPi, it was configured also on the APs. The first access point was configured by using the local browser and the second by the NETGEAR Insight application. In the first case, the static IP address of the access point was typed in the address bar, which is 192.168.0.3. Once in the AP's GUI, we navigated to RADIUS settings through Management -> Configuration -> Security. As Figure 21 shows, we added the IP address of the RPi, the default port to access the RADIUS server, which is 1812, and the password which must match the secret from Figure 20.

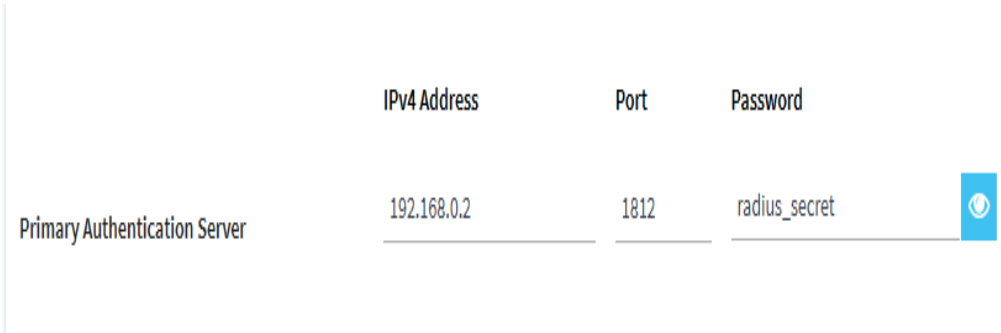


**Figure 21.** RADIUS configuration using the local browser.

For the second AP, we accessed the NETGEAR Insight application on the Android phone, we went to Wi-Fi networks -> SSID -> MAC Access Control -> RADIUS ACL and applied the same settings as depicted in Figure 22. /10/

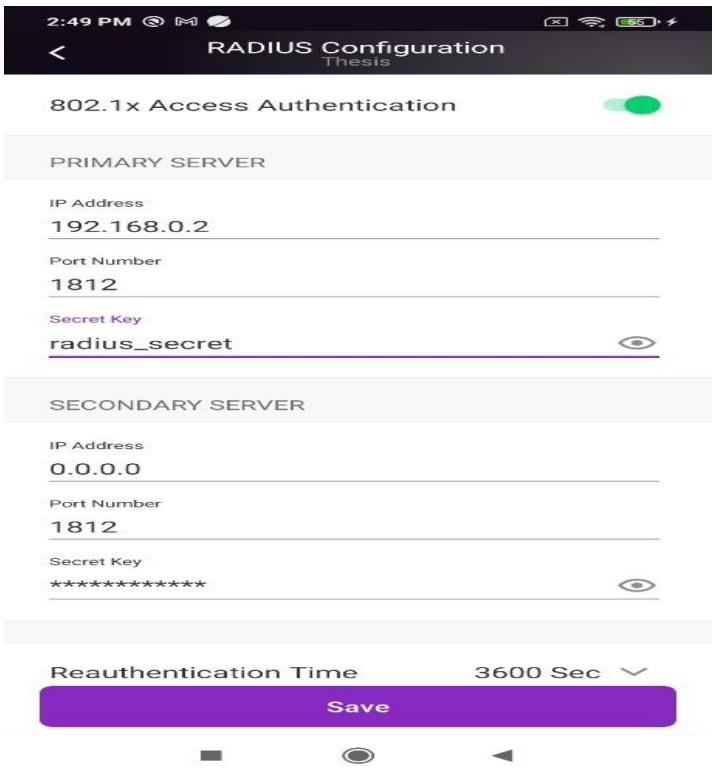


**Figure 22.** RADIUS configuration using the NETGEAR Insight application.

### 4.5.2 Testing the RADIUS Server

For the testing, two Android clients were used. The first client used the credentials *thesis_user1* and *password1* and the second client used the credentials *thesis_user2* and *password2*. Both clients, while trying to connect, were prompted with the fields of username and password, as shown in Figure 23.

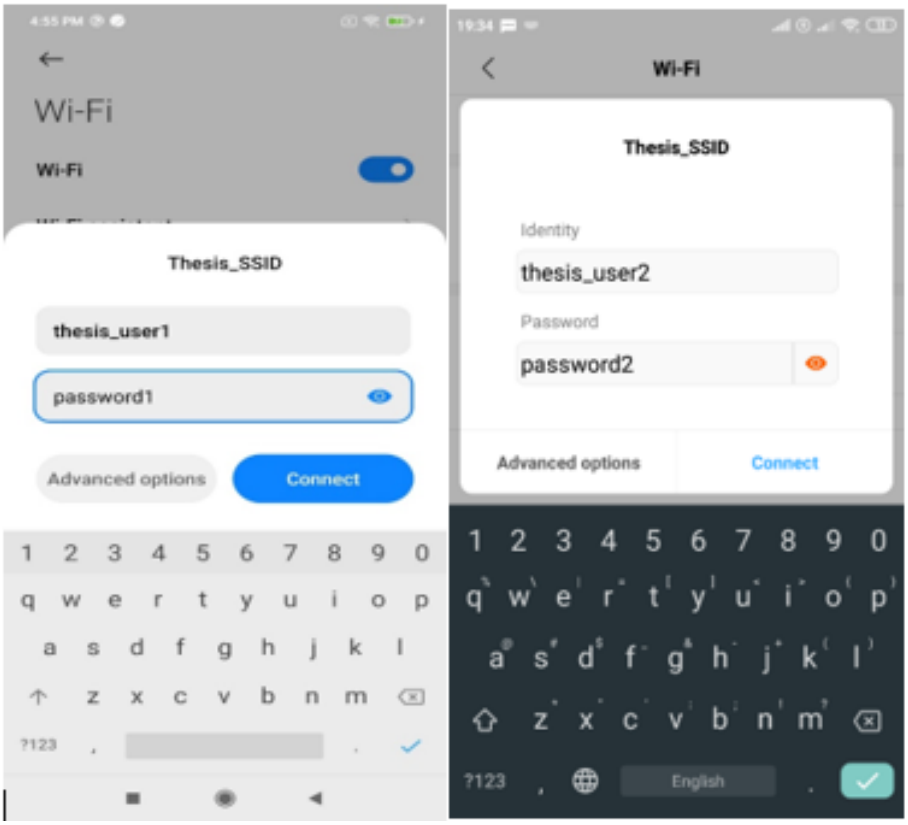


**Figure 23.** Asking for username and password for client authentication.

In Figure 24 we can notice that the connection and authentication were successful for both clients in the browser-configured AP. After this, we tapped on the *Forget network* option and we entered the coverage area of the application-configured AP. We started the connection and once again we were prompted for a username and a password. The connection to the second AP was successful as well, as depicted in Figure 25.

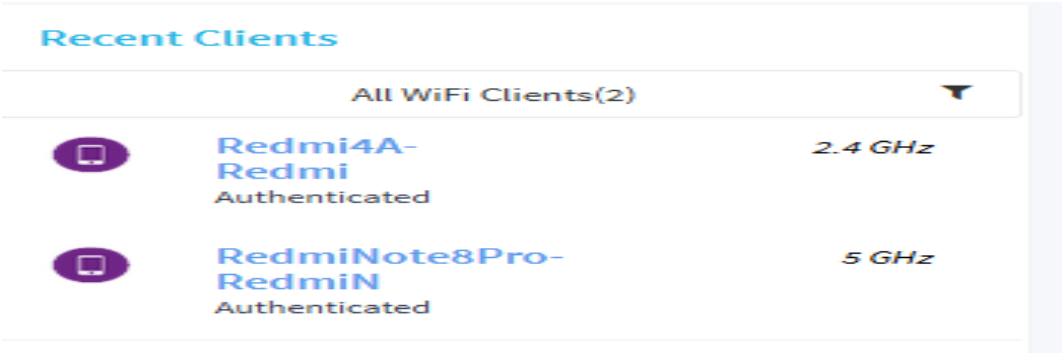


**Figure 24.** Successful authentication and connection of the two clients in the first AP.

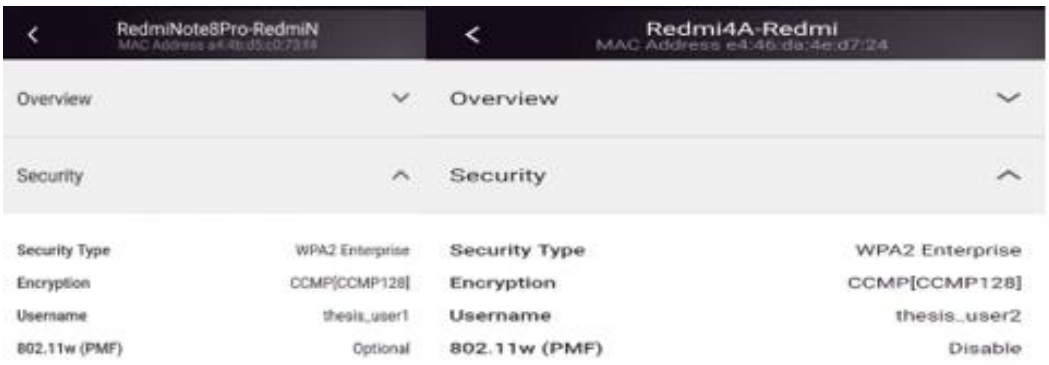


**Figure 25.** Successful authentication and connection of the two clients in the second AP.

# 5 RESULTS

The entire ESS WLAN was successfully configured. The two APs formed their own Basic Service Set (BSS), BSS1 and BSS2, they had the same SSID and used the same RADIUS server for user authentication and they formed an Extended Service Set (ESS), as shown in Figure 1. Since roaming is the fundamental goal of an ESS WLAN, an Android phone was used to test it. The phone was first connected to the AP configured via the Insight application and it was moved out of this AP's coverage area and brought to the second AP's area which was configured via the local browser. In Figure 26, we see that the phone successfully roamed between the two APs and kept its IP address.

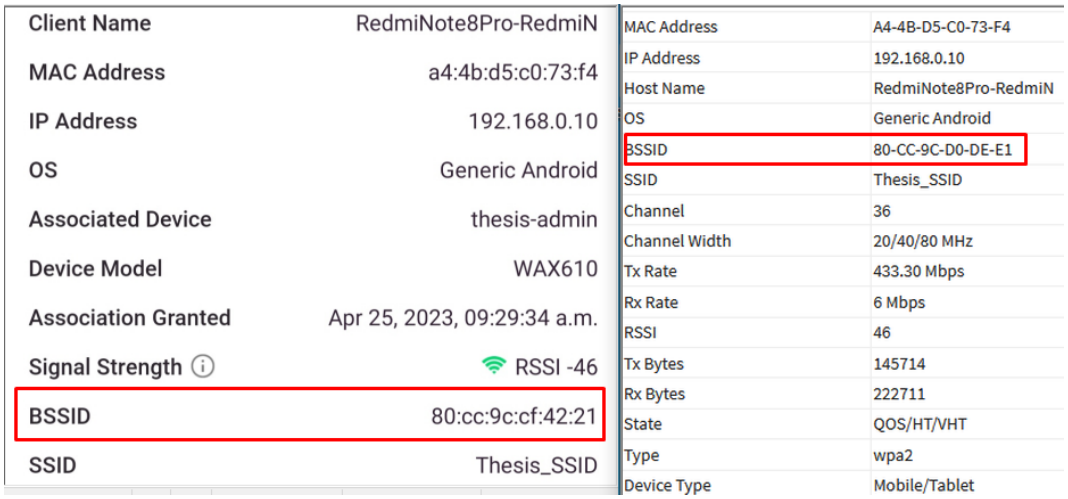


**Figure 26.** Successful roaming of Android phone between the two Access Points.

## 5.1 Band Steering with 802.11k RRM and 802.11v Wi-Fi Network Management

Band steering allows an access point to identify which devices are dual-band capable and steers them to the 2.4 GHz or 5GHz band of the Wi-Fi network. The 5GHz band in general allows more channels and bandwidth, with less interference and a better experience for the user. Two features were included in the band steering of the APs, one is 802.11k radio resource management (RRM), and the other is 802.11v Wi-Fi network management. Before explaining what these two features are used for, let us see how to choose a channel manually for both bands

in the APs environment. For the browser-configured AP we navigate to Management -> Configuration -> Wireless -> Basic -> Wireless Settings, and in Figure 27 we can see the channels available for both the 2.4 GHz and the 5GHz.

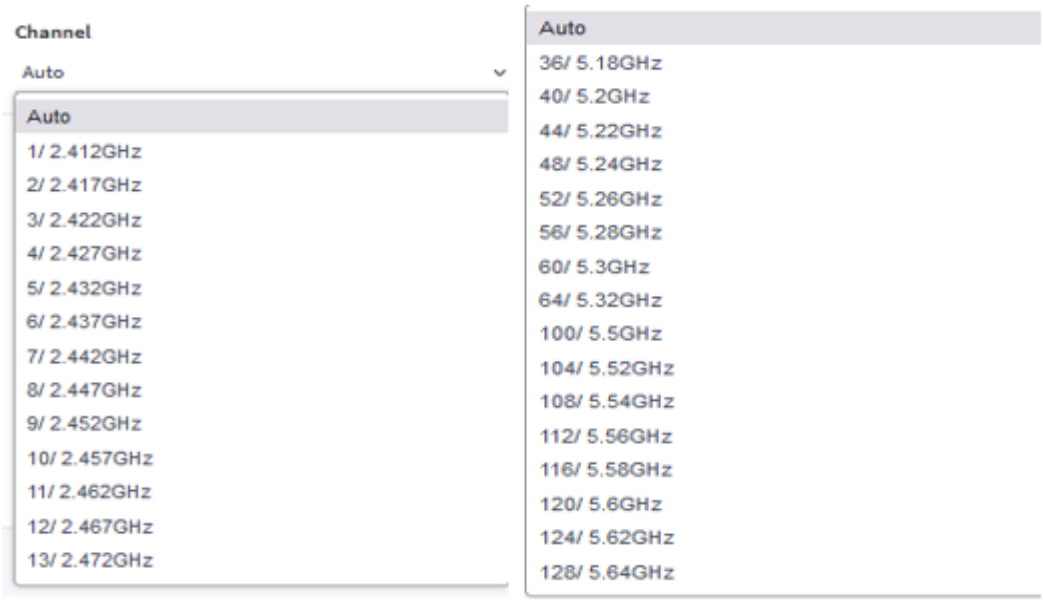


**Figure 27.** Manual channel selection for the 2.4 GHz and 5 GHz bands using the local browser.

It is also possible to select different channels from the Insight application, by selecting the option *Radio and Channels,* as depicted in Figure 28.

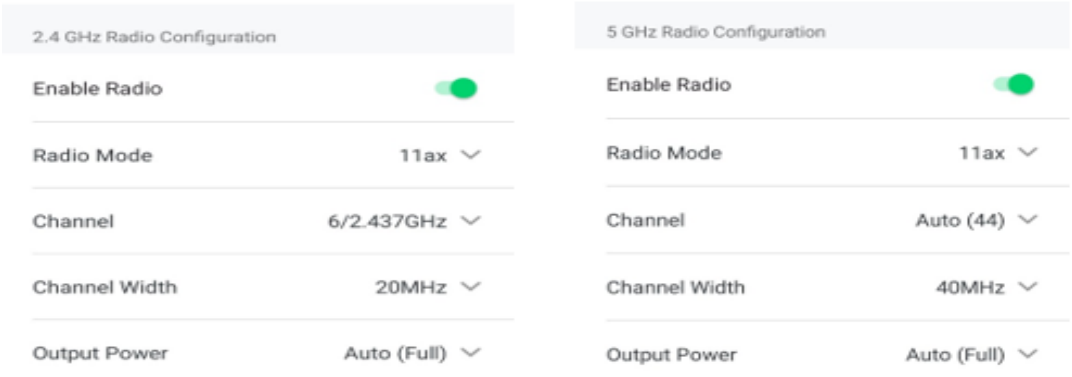


**Figure 28.** Manual channel selection for the 2.4 GHz and 5 GHz using the app.

In Figure 2 and Figure 3, it can be seen which the non-overlapping channels are and how a manual channel configuration should be performed for the best

network benefits. Once enabling band steering though, one of the two features mentioned above is 802.11k RRM. This feature allows the access points and 802.11k-aware clients to dynamically measure the radio resources by exchanging information such as neighbor, beacon, and link measurement reports and allowing the clients to select the best access point for initial connection or roaming. In this way, there is improved performance and reduced congestion and interference since the APs can make decisions automatically about which channels to use and how to allocate resources to clients. The second feature included when enabling band steering in the NETGEAR WAX610 APs is 802.11v Wi-Fi network management. It lets the AP steer the clients to 2.4 GHz or 5 GHz, depending on the channel load. This feature assists the clients to select the best AP among multiple/10/.

In Figure 29, we can see a channel graph of the 2.4 GHz and 5 GHz bands in the thesis development area, captured by the Wi-Fi Analyzer application.

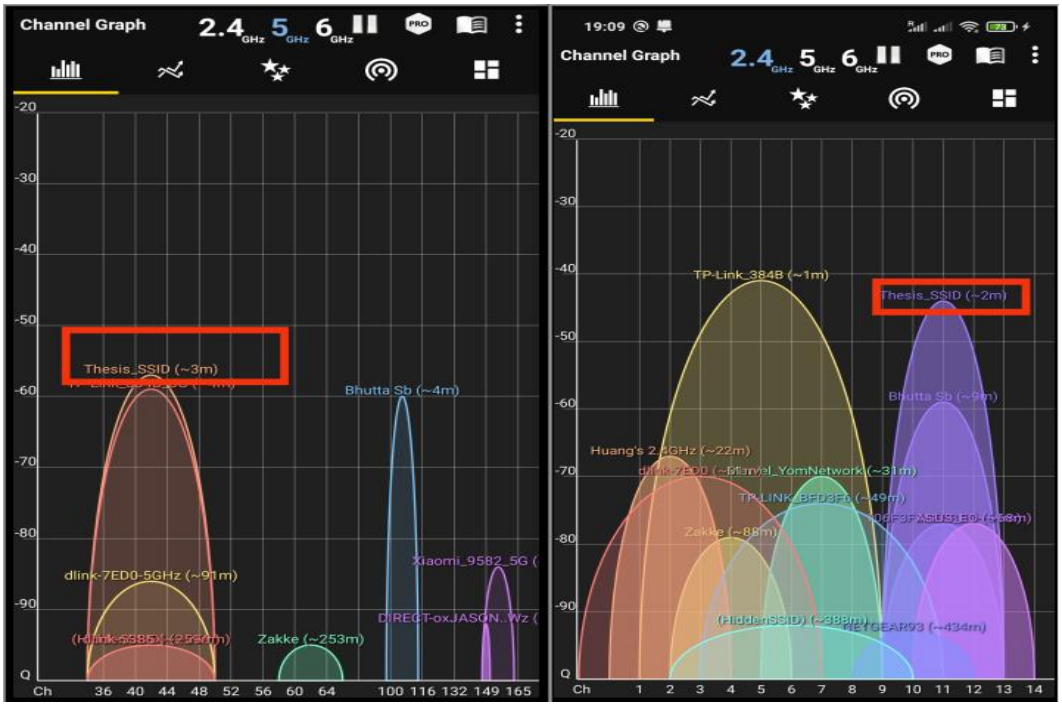


**Figure 29.** 5GHz and 2.4 GHz channel graph from Wi-Fi Analyzer.

One can notice the highly congested 2.4 GHz environment with the possible interference and lower performance than the 5 GHz environment, which has to offer more channels, less density, and higher performance. It is clear why band steering with 802.11k RRM and 802.11v is important for a better and improved user experience.

To enable band steering since it was disabled by default, we accessed the AP GUI in the browser and navigate to Management -> Configuration -> Wireless -> Basic, expanded the SSID tab, and enabled Band Steering / 802.11k/v. Band steering can also be enabled or disabled via the NETGEAR Insight application. Figure 30 shows both ways./10/

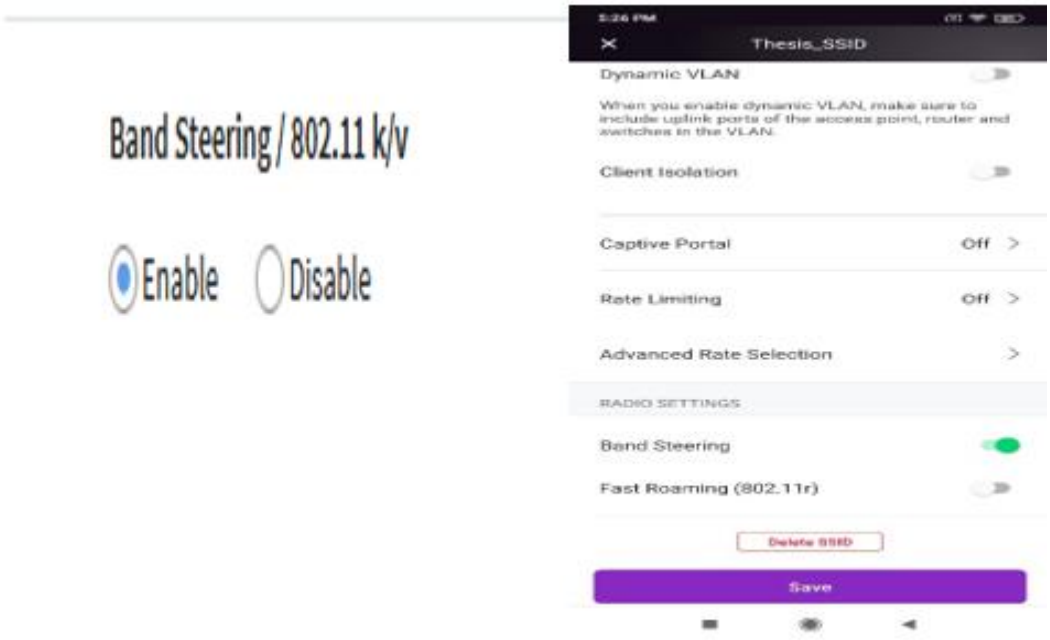


**Figure 30.** Enabling band steering via the local browser and the Insight application.

## 5.2 Testing Band Steering

One way to test band steering is to move a dual-band capable client away from the AP. In this way, from 5GHz it will steer to 2.4 GHz, as it is better for a larger range. An Android phone was connected to the 5GHz band. When the client was

moved away from the AP so that the signal is low, Figure 31 shows that band steering was in effect and the client changed to the 2.4 GHz band.

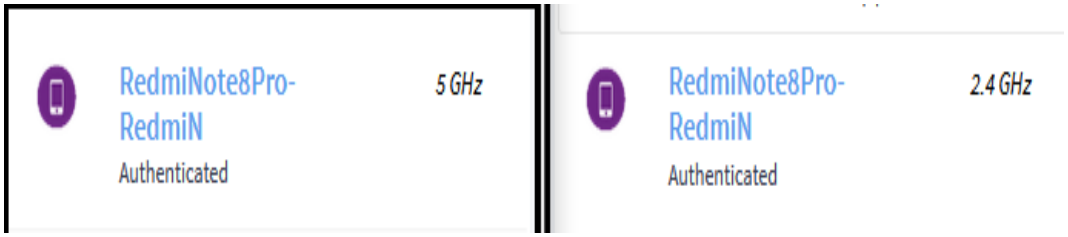


**Figure 31.** Band steering in effect.

Another test that was conducted while band steering was enabled in the APs, was roaming, that is the capability of the mobile device to connect to the "best" AP while moving in the ESS and keep its IP address. By navigating to Management -> Monitoring -> Connected Clients, we can see the mobile device's IP address among others, as shown in Figure 32.

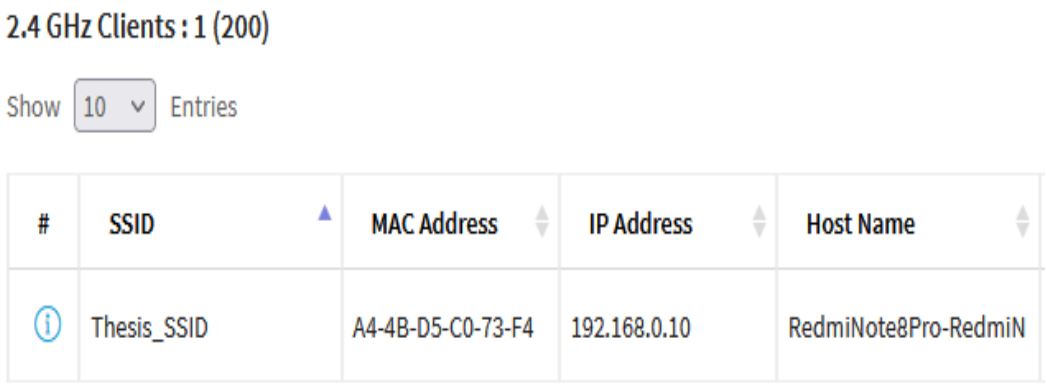


**Figure 32.** The mobile device on 2.4GHz with an IP address of 192.168.0.10.

Let us manually select a channel that is not non-overlapping, for example, channel 5. The device is now at a longer distance from the first AP and a closer one to the second AP with a stronger signal. Figure 33 shows the steering of the device to the second AP's 5GHz band while keeping its IP address.

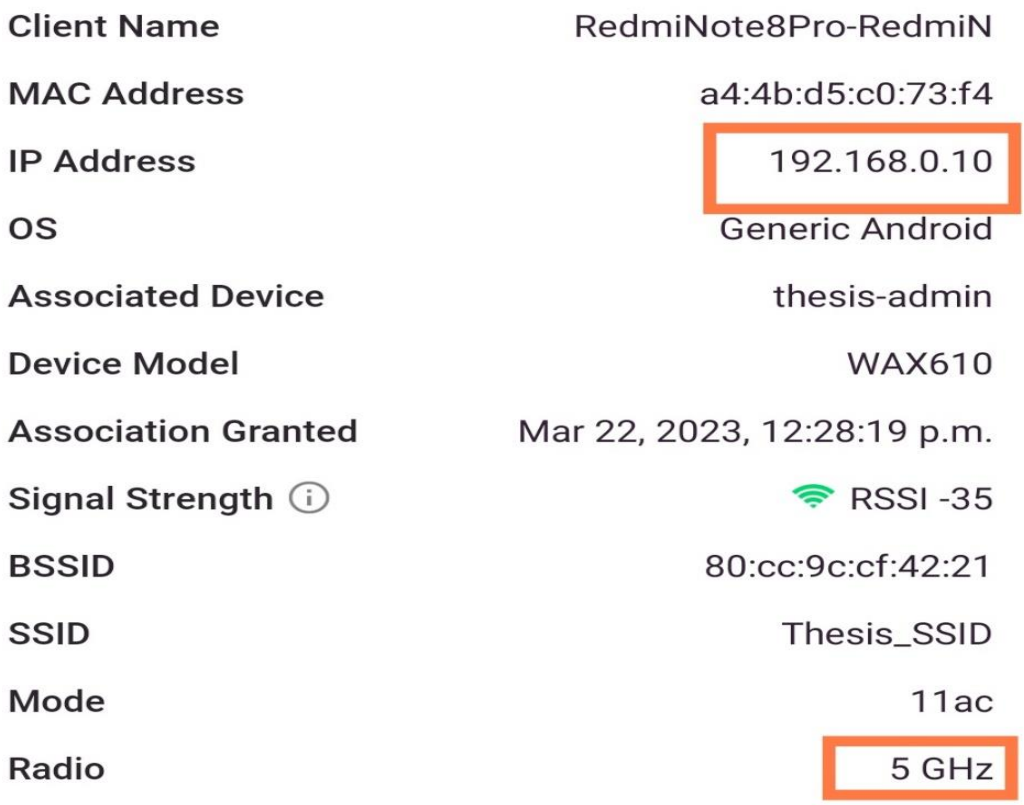


**Figure 33.** The client roamed between the “best” AP while having kept its IP address.

# 6 WIFI RADIO SETTINGS

The NETGEAR WAX610 Access Point has two categories of radio settings for the Wi-Fi, one is the Basic Settings and the other is the Advanced Settings/10/. First, the Basic Settings were examined.

## 6.1 Basic Settings

The basic settings for both 2.4GHz and 5GHz Wi-Fi radios can be accessed by navigating to Management -> Configuration -> Wireless -> Basic -> Wireless Settings and we were prompted with them, as shown in Figure 34.

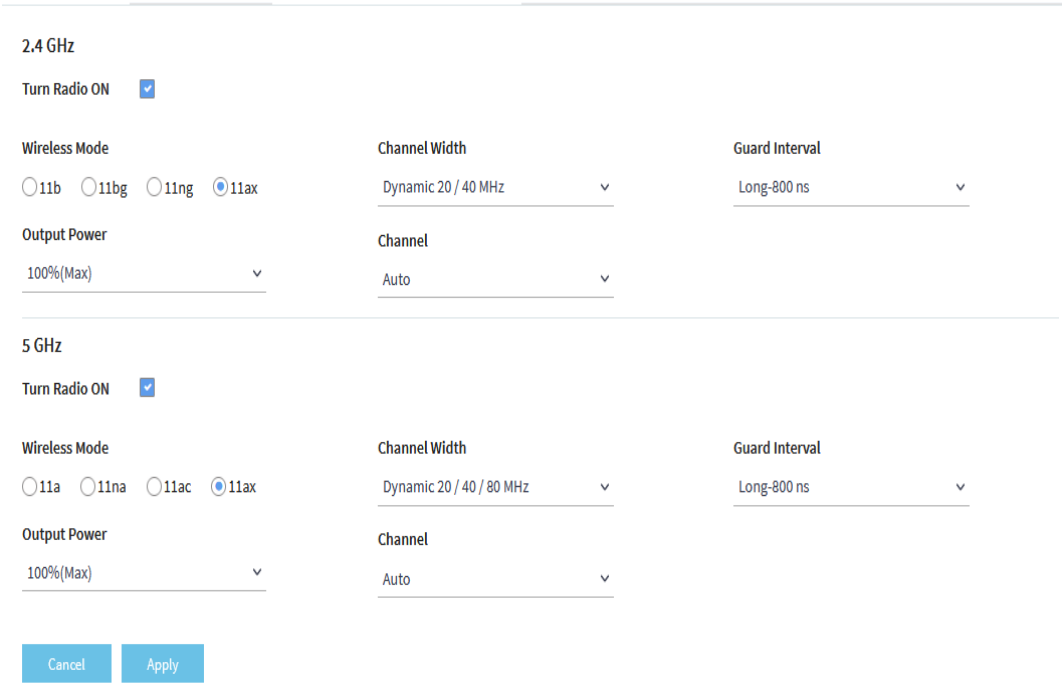


**Figure 34.** Basic settings for 2.4 GHz and 5 GHz radios.

One can notice that there are five different sections which include Wireless Mode, Channel Width, Guard Interval, Output Power, and Channel. First, let us focus on the sections for the 2.4GHz radio. The Wireless Mode section comprises 11b, 11bg, 11ng, and 11ax. These are the 802.11 standards or Wi-Fi generations, that depending on which mode is selected for the AP, the speed of the client is affected. From left to right, the order is going from the oldest and slowest to the newest

and fastest. All different devices, which might be 802.11ax, 802.11ng, 802.11bg, and 802.11b clients, can connect to every mode of the AP, but their speed will be adjusted to that of the mode. 11b mode can offer a speed of about 11 Mbps, 11bg which is a combination of b and g can offer a speed of 54 Mbps, 11ng, a combination of n and g can offer a speed from 72 to 400 Mbps, and finally 11ax mode offers a speed from 574 to 9608Mbps./12/

An Android phone which only supports the standards b, g, and n and is only capable of 2.4GHz was used to inspect the link speed when the AP operated on these different modes. Figure 35 shows the different link speeds that the client can get when connected to the above-mentioned modes.

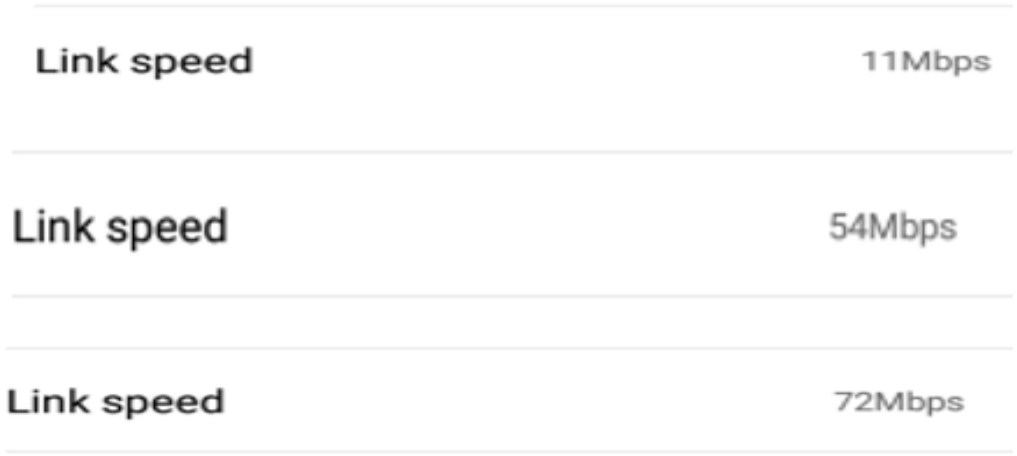


**Figure 35.** Different link speeds in 2.4 GHz radio under different 802.11 modes.

The next section is Channel Width, which is only available for the 11ng and 11ax modes. In general, for the 2.4GHz radio it would be more beneficial to set the channel width to 20MHz, because as it was explained in Chapter 3.1, there are only three non-overlapping channels, which are 1, 6, and 11, so a wider channel would cause interference.

The next setting is Guard Interval, which is also only available for the 11ng and 11ax modes. A guard interval is used for preventing transmissions from interfering with one another/13/. For the 11ng mode, there is only the option of Long at

800ns, whereas, for the 11ax mode, there is the Long, Double Long, and Quadruple Long at 800, 1600, and 3200 ns respectively. A shorter guard interval can provide more throughput where the devices operate at a short distance from the AP, while a longer one is more beneficial in an environment with multiple SSIDs and devices that operate at a longer distance from the AP.

The next setting is Output Power, which is set to maximum by default. In a situation in which multiple APs operate in the same area and on the same channel, it would be a good choice to decrease the output power of the AP to decrease the chance of interference in return. /10/

The last 2.4GHz setting for the WAX610 AP is the selection of the Channel. As mentioned above, for the 2.4GHz radio the only three non-overlapping channels are 1, 6 and 11, so unless the Auto-configuration is selected, the choice of the channel should be among these three.

For the 5GHz radio, we had the same basic settings apart from the fact that the Wireless Mode section is comprised of different modes with the only common being 11ax. As with the 2.4 GHz, all clients could connect to the AP, but again the speed was affected. The 11a mode can offer a total speed of 54 Mbps, the 11na which is a combination of 11n and 11a modes, can offer a speed of 72 to 600 Mbps and finally 11ac which is a combination of 11a and 11c modes a speed of 433 to 6933 Mbps./12/

Another Android phone which is 5GHz was used to examine the functionality of the different modes. In Figure 36 we can see the results.

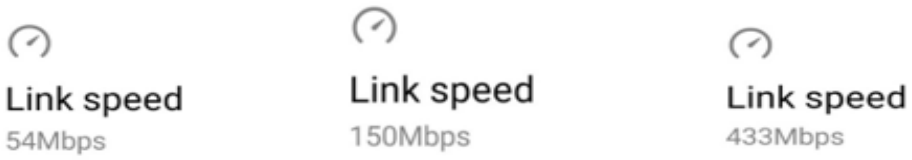


**Figure 36.** Different link speeds in 5 GHz radio under different 802.11 modes.

The next section is Channel Width, and 11a is the only mode for which the channel width is not available. In 5GHz radio, we had an additional 80 MHz. As it is mentioned in Chapter 3.1, we were no longer limited to the 20 MHz because of interference.

The Guard interval, same as channel width was not available for the 11a mode and there was only the option of Long-800 ns for the 11na and 11ac modes, whereas for the 802.11ax we have the Long, Double Long, and Quadruple Long same with the 2.4 GHz radio. The Output Power section had the same values as described in the 2.4 GHz band. Finally, the channels that were offered by the NETGEAR WAX610 AP can be seen in Figure 37.

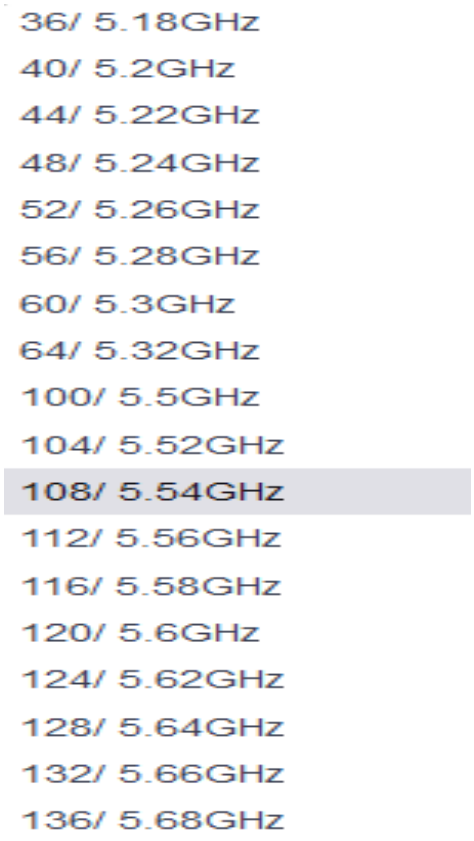


**Figure 37.** Available 5GHz radio channels on WAX610 AP.

## 6.2 Advanced Settings

The advanced settings for the radios can be accessed by navigating to Management -> Configuration -> Wireless -> Advanced -> Wireless Settings. Figure 38 shows the available settings for the two radios.

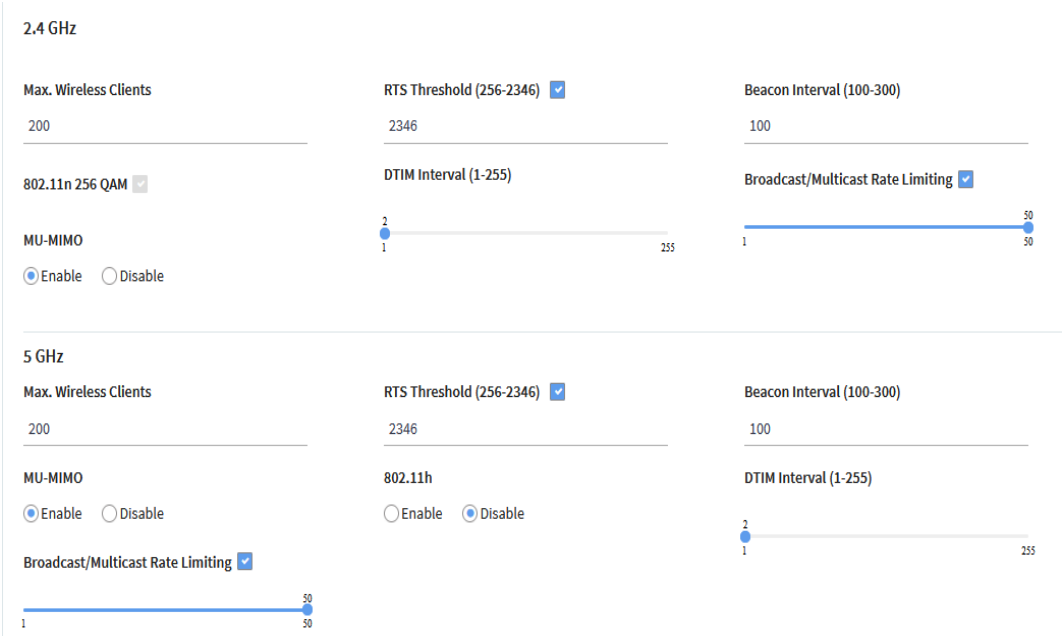


**Figure 38.** Advanced settings for the 2.4 GHz and 5GHz radios.

The first setting is Maximum Wireless Clients which corresponds to the maximum number of clients that can associate with the band, with a range of 1 to 200.

The next setting is the Request to Send (RTS) Threshold and it is noticeable that the range is from 256 to 2346 bytes, with 2346 being the default value. This feature helps in reducing collisions and increasing performance. When the packet size transmitted by the client device to the AP is equal to or less than the RTS threshold, then the radio will use the Carrier Sense Multiple Access with Collision Detection (CSMA/CD), and the data will be transmitted immediately. If the packet size is greater than the threshold, the CSMA with Collision Avoidance (CSMA/CA) mechanism will be used and the client will first send an RTS message and wait for a Clear to Send (CTS) message before sending the actual data./10/

The Beacon Interval setting comes next. A beacon is a frame that contains all the information about the network, transmitted periodically by the AP and announces the presence of a WLAN, and lets the members synchronize. The beacon interval is the time interval between the transmissions of these beacons. Increasing the beacon interval will result in beacons being sent less frequently, and this in return will increase throughput but will delay association and roaming as a beacon could be missed. On the other hand, if we decrease the interval, the beacons will be sent more frequently, resulting in decreasing throughput but faster roaming/14/. From Figure 38 we can see that the range is between 100 and 300 Time Unit (TU), with 100 being the default value.

The next setting is 802.11n 256 QAM, which can be enabled or disabled for the 2.4 GHz radio when the wireless mode is set to 802.11n. The feature is by default enabled in the 5 GHz radio and cannot be disabled. When it is enabled for the 2.4 GHz radio, it can increase the throughput for these clients that can support it/10/.

Another common setting for both radios is the Delivery Traffic Indication Message (DTIM). A DTIM is used to inform the client devices of the availability of multicast and broadcast frames on the AP. The DTIM interval specifies how often a beacon includes a DTIM and it is a multiplier of the beacon interval. The higher the interval the longer a device may sleep, resulting in saving more power/15/. The value of the DTIM interval as depicted in Figure 38, is between 1 and 255 with a default of 2.

One more common feature for both radios is Broadcast/Multicast Rate Limiting. As its name suggests this feature is used to limit the amount of broadcast and multicast traffic sent over the network, improve performance, and decrease congestion. There is a span between 1 and 50 packets per second and the default value is the maximum rate limit of 50.

The next setting which is enabled by default in both the 2.4 GHz and 5 GHz is MU-MIMO. Multi-User Multiple Input Multiple Output is a feature that allows multiple

devices on the same channel to communicate with the AP simultaneously, by increasing the antennas of the AP. Since the nature of traditional Wi-Fi is that one AP serves one device at a time, it is easy to understand that congestion and low network performance would occur, so such a technology is very important, especially in highly crowded environments where clients 'battle' for connection. At this point, it should also be mentioned that this feature is only available from the 802.11ac standard and after, meaning that previous wireless modes that were inspected earlier, such as 802.11b,g,n are not compatible./16/

Finally, there is the 802.11h feature which is only available for the 5 GHz radio. This feature is an amendment to the 802.11 standards and is used to cope with interference with radars and satellites using the same band./17/

When enabled on the WAX610 AP, the clients can automatically switch to another channel without disconnecting and without losing data when the AP changes the channel./10/

# 7 CONCLUSIONS

The thesis dealt with the configuration and implementation of an Extended Service Set (ESS) WLAN and how different and more challenging this procedure is compared to a Basic Service Set (BSS) or a home network. Various technologies have been studied and investigated thoroughly to achieve the desirable result and create a feasible and effective wireless network. The results of the project show that the NETGEAR WAX610 Access Points are capable of delivering all the services needed for a high-performance ESS and that they would be extremely effective and operable in any environment. Additionally, the security configuration must be highlighted as it must be implemented properly. In general, the project was successful, and the main objective of a functional and operational ESS WLAN was achieved. It is expected that it will help, even slightly, in the improvement of wireless networking.

# 8 REFERENCES

/1/Wikipedia. 2.4 GHz radio use. Accessed 27.03.2023. https://en.wikipedia.org/wiki/2.4_GHz_radio_use

/2/ Crowder, C. 2021. How to Find the Best Wi-Fi Channel for 5Ghz Frequency. Accessed 27.03.2023. https://www.maketecheasier.com/best-wifi-channel-for-5ghz-frequency/

/3/ ScreenBeam. 2.4 GHz vs 5 GHz WiFi: What's the difference and how do I use them? Accessed 27.03.2023. https://www.screenbeam.com/wifihelp/wifi-networking/2-4ghz-vs-5ghz-wifi/

/4/Wikipedia. RADIUS. Accessed 27.02.2023. https://en.wikipedia.org/wiki/RADIUS

/5/Wikipedia. IEEE 802.1X. Accessed 27.02.2023. https://en.wikipedia.org/wiki/IEEE_802.1X

/6/ Wikipedia. Extensible Authentication Protocol. Accessed 27.03.2023. https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol

/7/ King, P. 2022. How Do I Set a Static IP Address on Raspberry Pi? Accessed 29.01.2023. https://www.makeuseof.com/raspberry-pi-set-static-ip/

/8/ Wikipedia. Dynamic Host Configuration Protocol. Accessed 29.01.2023. https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

/9/Kalitut. 2020. Setup ISC DHCP server. Accessed 29.01.2023. https://kalitut.com/setup-isc-dhcp-server/

/10/ NETGEAR, Inc. 2022. Insight Managed Wi-Fi 6 AX1800 Dual Band Access Point. Accessed 01.02.2023. https://www.downloads.netgear.com/files/GDC/WAX610/WAX610_WAX610Y_UM_EN.pdf

/11/ Bhatnagar, D. 2020. Setup of FreeRADIUS Server Using Raspberry Pi3. Accessed 27.02.2023. https://www.talentica.com/blogs/setup-of-freeradius-server-using-raspberry-pi3/

/12/Wikipedia. IEEE 802.11. Accessed 30.03.2023. https://en.wikipedia.org/wiki/IEEE_802.11

/13/Wikipedia. Guard Interval. Accessed 30.03.2023. https://en.wikipedia.org/wiki/Guard_interval

/14/Wikipedia. Beacon frame. Accessed 31.03.2023. https://en.wikipedia.org/wiki/Beacon_frame

/15/Wikipedia. Traffic indication map. Accessed 31.03.2023. https://en.wikipedia.org/wiki/Traffic_indication_map

/16/ Shaw, K. 2022. What is MU-MIMO, and why is it essential for Wi-Fi 6 and 6E? Accessed 01.04.2023. https://www.networkworld.com/article/3250268/what-is-mu-mimo-and-why-is-it-essential-for-wi-fi-6-and-6e.html

/17/Wikipedia. IEEE 802.11h-2003. Accessed 01.04.2023. https://en.wikipedia.org/wiki/IEEE_802.11h-2003