

**Wi-Fi Networking Solution Technology and
Practical Offering Solutions**

Mohammad Junaid



**UNIVERSITY
OF ALBERTA**

Table of Contents

Project Objective	5
Abstract.....	5
Introduction	6
Evolution of Wi-Fi Technology	8
Era before the standardization of WLAN	8
Wi-Fi technology became IEEE Standard.	11
Evolution of WLAN technologies and standards	14
Challenges faced in deploying Wi-Fi	32
Solutions to the challenges in deploying Wi-Fi.....	40
On-Premise Enterprise Wi-Fi Solution.....	66
Public Cloud Based Enterprise Wi-Fi Solution.....	74
Configuration Lines	117
Conclusion	139
Works Cited.....	140

Table of Figures

Figure 1 Growth of Internet users [1]	6
Figure 2 Bandwidth usage of various applications [1]	7
Figure 3 Diffuse optical channels connecting terminal clusters in an in-house environment, S = Satellite and T = Terminals [2]	8
Figure 4 ALOHA System [7]	9
Figure 5 Full-size NCR ISA WaveLAN 915MHz card [10]	12
Figure 6 Half-size AT&T WaveLAN 915MHz card [10]	12
Figure 7 Half-size AT&T WaveLAN 2.4 GHz card [10]	13
Figure 8 IEEE 802 Standards family and its relationship with OSI [11]	14
Figure 9 802.11b features [14]	16
Figure 10 Cisco Aironet AP350 802.11B Access Point [16]	17
Figure 11 802.11a features [14]	18
Figure 12 SMC 802.11a Access Point [17]	19
Figure 13 D-Link DWL-700AP 802.11g Access Point [18]	21
Figure 14 802.11n features [14]	22
Figure 15 Cisco AIR-3602e 802.11n Access Point with Multiple Antennas [19]	23
Figure 16 802.11ac features [14]	24
Figure 17 802.11 ac wave 1 vs. wave 2 [21]	25
Figure 18 Scenario 1 - 4 Multiple Spatial Streams [21]	26
Figure 19 Scenario 2 – 4 Multiple Spatial Steams [21]	27
Figure 20 802.11ad features [14]	28
Figure 21 TP-Link Talon AD7200 Wireless Router [22]	29
Figure 22 Aruba AP-505 802.11ax Access Point [23]	31
Figure 23 Students in a University Auditorium [24]	32
Figure 24 Wireless Access Point placed outside in the rain [25]	36
Figure 25 Interference caused by home appliances [27]	38
Figure 26 2.4 GHz RF Spectrum Analysis [29]	42
Figure 27 The goal accomplished is to install the AP in a low-profile ceiling mount while still using the original tile. [30]	43
Figure 28 Example of an AP deployment within an intelligent building ceiling designed for aesthetics. The goal accomplished is to hide the AP. [20]	44
Figure 29 Outdoor Access Point mounted on a pole [48]	45
Figure 30 Easily accessible access point in hotel room [31]	47
Figure 31 Different types of copper cables [33]	49
Figure 32 Cisco 3850x with Wireless LAN controller inbuilt [34]	50
Figure 33 Ekahau Pro software [35]	51
Figure 34 Corporate Training Room [36]	62
Figure 35 AP on a Stick survey [37]	63
Figure 36 Cisco 2504 WLC [38]	67
Figure 37 Cisco 2500 Series Wireless Controller Features and Benefits [38]	67
Figure 38 Cisco Aironet 1700 Series Access Point [39]	70
Figure 39 On-Premises versus Public Cloud service models [42]	74
Figure 40 Basic Cisco Meraki Topology [43]	75
Figure 41 Typical Cloud Wireless solution	77

Figure 42 VPN between AWS and Corporate Network [44] 79
Figure 43 Routing between AWS -VPC and On-premises Network. [44]..... 80

Project Objective

The main objective of this project is to study various wireless networking technology and their practical solutions based on different scenarios, primarily following the latest industry trends.

Abstract

With the advent and ever-growing concept of the Internet of Things, traditional wired Local Area Network (LAN) has a lot of challenges with people bringing devices like smartphones and tablets into the workplace. A Wi-Fi network can solve this, but implementing a solution with central management, rapid deployment, security, high availability, and cost-effectiveness can be challenging. Every business has different needs; hence a Wi-Fi solution must be deployed which fits their requirements. This project will delve into those other practical solutions available to carefully plan and implement those solutions.

Introduction

A mobile with Wi-Fi capability was such a big deal only a decade ago. Fast forward to 2021, almost every smartphone is equipped with Wi-Fi. We as humans cannot imagine our lives without the Internet, and I believe the main reason for this is wireless technologies such as 3G,4G, and Wi-Fi. Wi-Fi has a crucial role in the future of networking and other small cell technologies such as 5G.

There has been an enormous growth in the total number of Internet users all-round the globe. In terms of population, 66 percent of the global population by 2023 (Figure 1). [1]

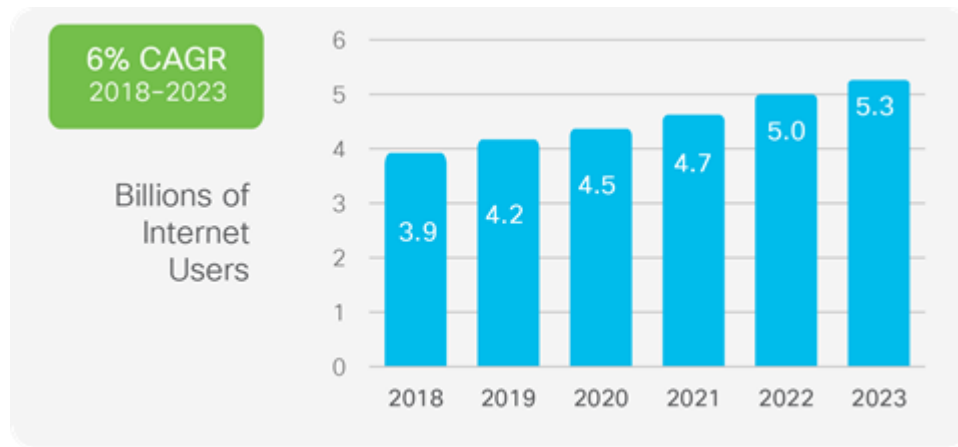


Figure 1 Growth of Internet users [1]

Applications are leading us into being more and more developed. Everywhere we go, we have Wi-Fi around us. It doesn't matter if we connect to it, but it exists everywhere. The rise in computing resources such as processing speed, memory, and storage capabilities has helped us develop several applications; Due to this, there has been enormous demand for high-speed communication, especially wireless technologies. [1]

Currently, in 2021, we have two wireless technologies at our disposal. One is IEEE 802.11 wireless local area network – Wi-Fi, and another is cellular technologies. Wi-Fi is the first choice due to the high bandwidth rate and lower cost. Whereas on the other hand, cellular technologies are always a second choice due to their higher cost and lesser bandwidth rate. [1]

Currently, the 5G data rate is equivalent to a Wi-Fi connection. But being so expensive, people usually prefer Wi-Fi, especially in those countries where 5G is not yet implemented. [1]

It's not only laptops or smartphones which connect to Wi-Fi; with the advent of the Internet of things, but almost every device in the house also connects to Wi-Fi, such as security systems, entertainment systems, home appliances, etc. This proves the importance of Wi-Fi in our lives. Video and other applications continue to be in major demand in today's homes. [1]

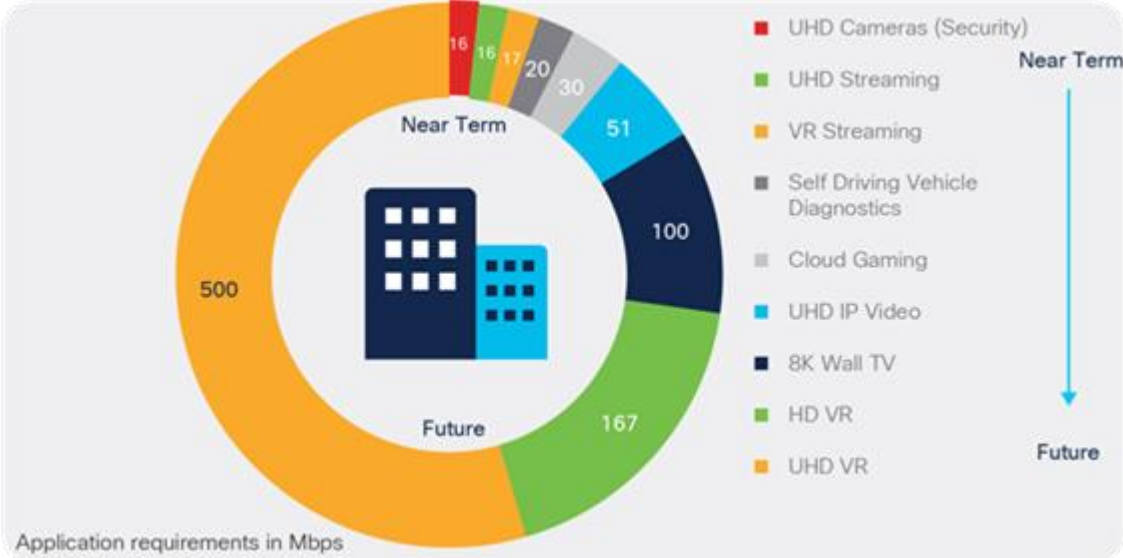


Figure 2 Bandwidth usage of various applications [1]

Evolution of Wi-Fi Technology

Here we will discuss the evolution of Wi-Fi technologies, mainly divided into three parts. Firstly, the era before the standardization of WLAN by IEEE. Secondly, when IEEE 802.11 and Wi-Fi technology became an IEEE standard and finally the current period of Wi-Fi technologies.

Era before the standardization of WLAN

In the year 1979, Fritz R. Gfeller and Urs Baps, employed by IBM in their Rueschlikon Laboratory, were working on a wireless communication network employing infrared radiation. The idea was to connect the group of data terminals inside a single room. For wireless range up to 50 meters, it used infrared of 950nm wavelength. Theoretically, temporal dispersion restricts the system's transmission bandwidth to 260 Mbit per second, but in practice, noise generated by ambient sunshine drops the transmission speed below 1 Mbit per second. [2]

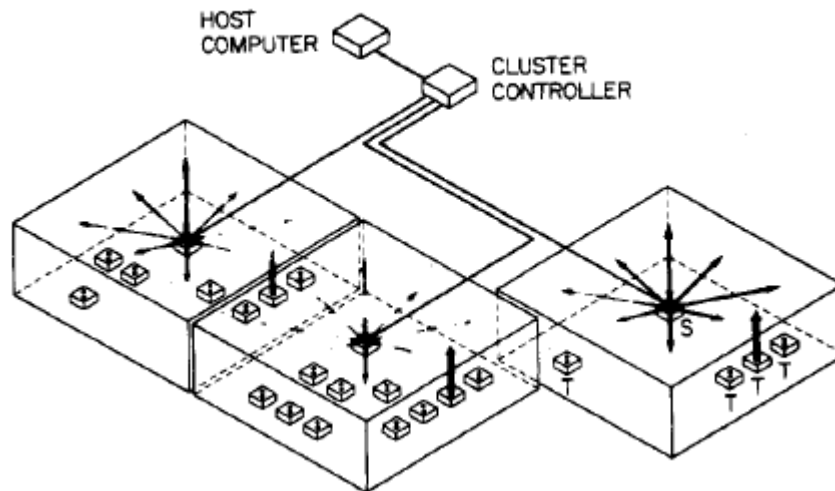


Figure 3 Diffuse optical channels connecting terminal clusters in an in-house environment, S = Satellite and T = Terminals [2]

During those days, wired communication was crucial and used everywhere, especially in offices and large manufacturing warehouses. General Motors thought of using wired connectivity for their floor manufacturing using computers. But the major problem was the cabling because in offices it's easy usually the cable will be inside of the walls and low ceiling height. But when we are talking about large manufacturing floors, there is a lot of limitation, mainly due to the high ceilings and no partition walls. Hence Wireless LAN was thought of as an alternative. [3]

Hewlett-Packard was working during the late 1970s, and in 1980, they came up with a prototype of wireless LAN using direct sequence spread spectrum – DSSS. In this prototype, we can access using the telephone system. Here, base stations will be connected to the telephone network directly or indirectly. Hence, they will make or receive the phone calls on the telephone network. Mobile user stations with a spread-spectrum transmitter or receiver will have the ability to dynamically connect to specified base stations. [4]

Hewlett-Packard had offices with open spaces without partition walls, which brought immense challenges for cabling. If you drop wires from the ceilings to the workstations or desks, it might not look pleasing or aesthetically beautiful. Hence combining optical wireless and DSSS was suitable as it could support a bigger capacity for interconnecting several desktops and printers in an office within a LAN. [5] [6] [3]

A long time ago, before HP and IBM brought the WLAN solutions, the University of Hawaii was already working on radio communications between computers during the late 1960s. The result was the ALOHA system. During those days, the only way of communications was wired communications such as leased copper lines or ISDN dial-up connections. These were enough to fit the needs of inter-computer communication but then restricted to a physical area and hence no remote computing. [7]

THE ALOHA SYSTEM was created to provide system designers with another option and identify scenarios when radio communications are better than traditional cable connections. [7]

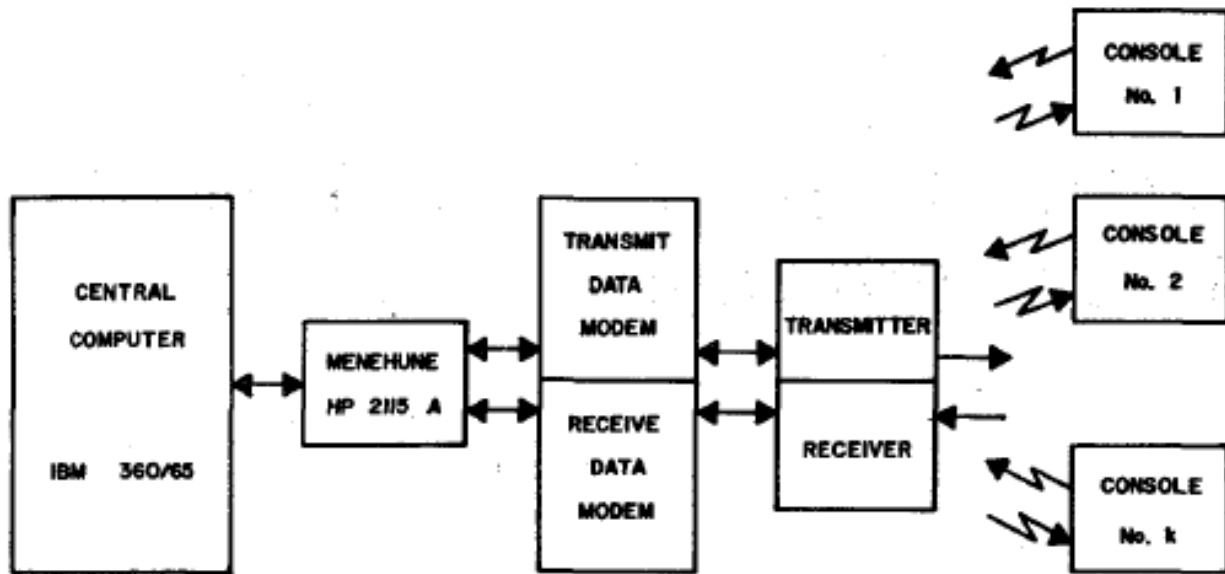


Figure 4 ALOHA System [7]

The distinction between IBM's or HP's method and this technique is that the ALOHA system was an academic experiment with wireless packet data networks using outdoor antennas and rather low data rate modems at roughly 9600 bits per second. [3]

The major problem with all the technologies listed so far was the inability to penetrate walls or other obstacles, which made use of the technologies only in areas that are open spaces without any walls or obstacles.

A much-needed solution was required and came up in 1985, discussed next.

Wi-Fi technology became IEEE Standard.

The life-changing moment in the history of Wi-Fi came in 1985 when M.J. Marcus, employed in Federal Communications Commission – FCC, permitted the use of unlicensed Industrial, Scientific, and Medical (ISM) bands but with restrictions and can use the spreading spectrum for management of interference. [8]

High bandwidths (considering the bandwidths at that time) and technology that could overcome the constraints of indoor Radio Frequency propagation to generate data speeds of more than 1 Megabits per second were mandatory to be deemed a LAN by the IEEE 802 committee and finally for the WLANs to establish itself as a commercial product. Both difficulties were addressed using ISM bands and spread spectrum technologies. [3]

This was terrific news for aspiring wireless communications technology developers since it meant they could now develop without having to pay license costs. Regrettably, this resulted in many developments that did not lead to a successful journey and result.

The IEEE, on the other hand, recognized in the early 1990s that a wireless LAN standard was required to fill a clearly defined market need. The IEEE 802 standard for Local and Metropolitan Area Networks decided that an executive committee must be formed to define a wireless LAN standard. [9] Using the unlicensed ISM band from 2.4 to 2.5 GHz, the 802.11 group focused on developing a stable, high bandwidth, affordable, and resilient wireless technology that might evolve into a standard with universal support. [10]

In Nieuwegein, Netherlands, NCR Corporation/AT&T (now Nokia Labs and LSI Corporation) devised a forerunner to 802.11 in 1991. The technology was created with the intention of being used in Point of Sale – Cashier machines. WaveLAN was the brand name for the earliest wireless devices, which had raw data speeds of 1 Mbit/s and 2 Mbit/s. [10]

The Worcester Polytechnic Institute hosted the inaugural (IEEE) - Institute of Electrical and Electronics Engineers meeting on Wireless LANs in 1991. It was conducted in Worcester in conjunction with a discussion of the IEEE 802.11 Wireless Access Methods and Physical Layer Standardization Committee for Wireless LAN. This was hosted to address the challenges we are or might be facing in the implementation of wireless LANs. The significant idea was to raise knowledge of current advancements in the WLAN sector and stimulate contact between researchers, spectrum regulators, standardization committees, vendors, manufacturers, and customers. [10]



Figure 5 Full-size NCR ISA WaveLAN 915MHz card [10]

The first WaveLAN operated in 900 MHz or the ISM band of 2.4GHz. Since it was not certified as an IEEE 802.11 standard, the interoperability with the 802.11 standards was out of the question. But later, in November 1997, the WaveLAN was already certified under the IEEE 802.11 standard. [10]



Figure 6 Half-size AT&T WaveLAN 915MHz card [10]



Figure 7 Half-size AT&T WaveLAN 2.4 GHz card [10]

Hence, we understand that from 1985 to 1997, we were trying our best to understand wireless technologies and find the best solution. In this process, many technologies were tried and tested, such as spread spectrum, infrared, licensed bands at 18 GHz with antennas, DFE, M-ary orthogonal coding, and OFDM. But eventually, only spread spectrum, OFDM, M-ary orthogonal coding, and infrared got successful industry recognition and usage in the future. In Bluetooth, we used FHSS, M-ary orthogonal coding, and OFDM are currently used in the latest Wi-Fi standards.

The first panel talks on the future of the WLAN sector were held in collaboration with the IEEE 802.11 standardization organization at the inaugural **IEEE workshop on WLAN (1991)** and the **IEEE International Symposium on Personal, Indoor, and Mobile Communications (1992)**. The first scientific publication, the International Journal of Wireless Information Networks, was published in 1994, as was the first scientific magazine devoted to this field, IEEE Personal Communications, subsequently renamed as **IEEE Wireless Communications**. [3]

Evolution of WLAN technologies and standards

Before we discuss the IEEE wireless standards and technologies, it is pretty crucial to understand the function of the IEEE 802 family and its specifications.

IEEE 802

IEEE 802 is a set of networking standards that corresponds to the physical and data link layer of the OSI Network Model. These operate at Layer 0, Layer 1, and Layer 2, respectively. The purpose of these standards is to have a similar language for intercommunicating between different vendors so that they understand one another.

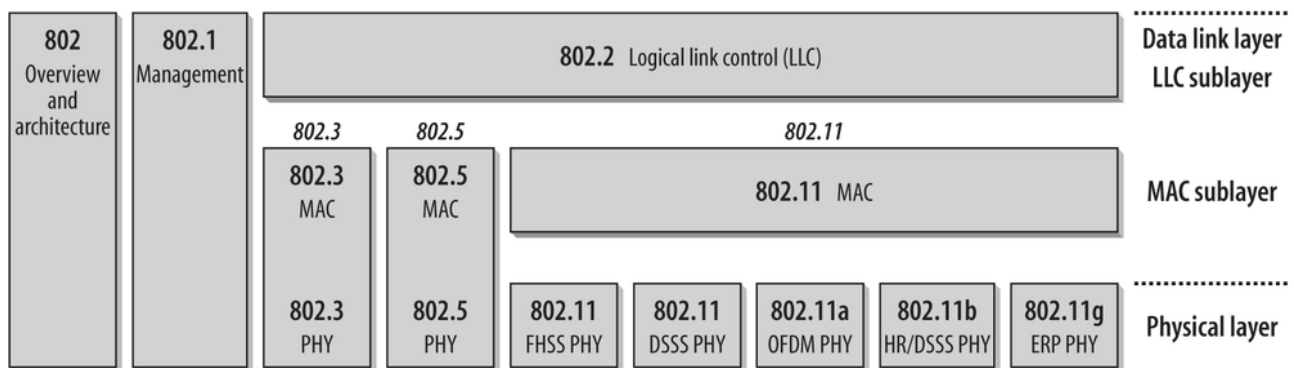


Figure 8 IEEE 802 Standards family and its relationship with OSI [11]

IEEE 802 is subdivided into Layer 1 and Layer 2. Layer 2 is subdivided into MAC Sublayer and LLC – Logical Link Control sublayer. The MAC layer is a collection of rules for accessing the medium and sending data, whereas the PHY Layer is in charge of transmission and reception. [11]

Now there are many specifications under the IEEE 802 family; we can see those below-

- i. IEEE 802.3 - Carrier Sense Multiple Access networks with Collision Detection (CSMA/CD)
- ii. IEEE 802.5 – Token Ring
- iii. IEEE 802.2 – Common Logical Link Control LLC
- iv. IEEE 802.1 – Management features such as 802.1D for spanning tree protocol and 802.1Q for VLAN Tagging.
- v. IEEE 802.11 – Wireless LAN, also known as Wi-Fi, uses the 802.2 LLC layer and two physical layers: FHSS and DSSS. [11]

Legacy IEEE 802.11

The initial IEEE 802.11 standard was introduced in 1997, and it is now referred to as Legacy 802.11 since it is no longer in use in the industry and has been supplanted by newer standards that we shall explore later.

The handling of mobile and portable stations, which is primarily a station capable of moving from one site to another, was a key advantage of IEEE 802.11. Because mobile stations are frequently battery-powered, power management was carefully studied in the development of this standard. [3]

The data rates which were achieved are between 1 and 2 Mbps using infrared signals operating in the industrial, scientific medical – ISM bands around 2.4 GHz. But it was always a theory because the practical implementation of this standard was never achieved. [12]

The carrier sense multiple access with collision avoidance (CSMA/CA) media access mechanism is also used in the original standard. A considerable portion of the bandwidth capacity was sacrificed because of the CSMA/CA method. [12]

The major drawback of the original specification of the 802.11 standards was the variety of options it offered which made the intercommunication and interoperability between different vendors next to impossible. Keeping it simple was the thing which they should have done to let manufacturers adapt to this new technology. Hence, later it was replaced by the IEEE 802.11b. [13]

802.11b

In the year 1999, IEEE brought 802.11b to the market.

Direct Sequence Spread Spectrum (DSSS) is employed at the physical layer, and it was operating in the same ISM band as the original IEEE 802.11, which is the 2.4 GHz. The channel width was only 20MHz. Advanced antenna options were not supported since it was a simple standard easy for adapting to the various industry manufacturers. Only one single transmission and single receiving antenna were supported. Q-PSK was the modulation order. All of these elements together resulted in a maximum throughput of 11 Mbps. [14]

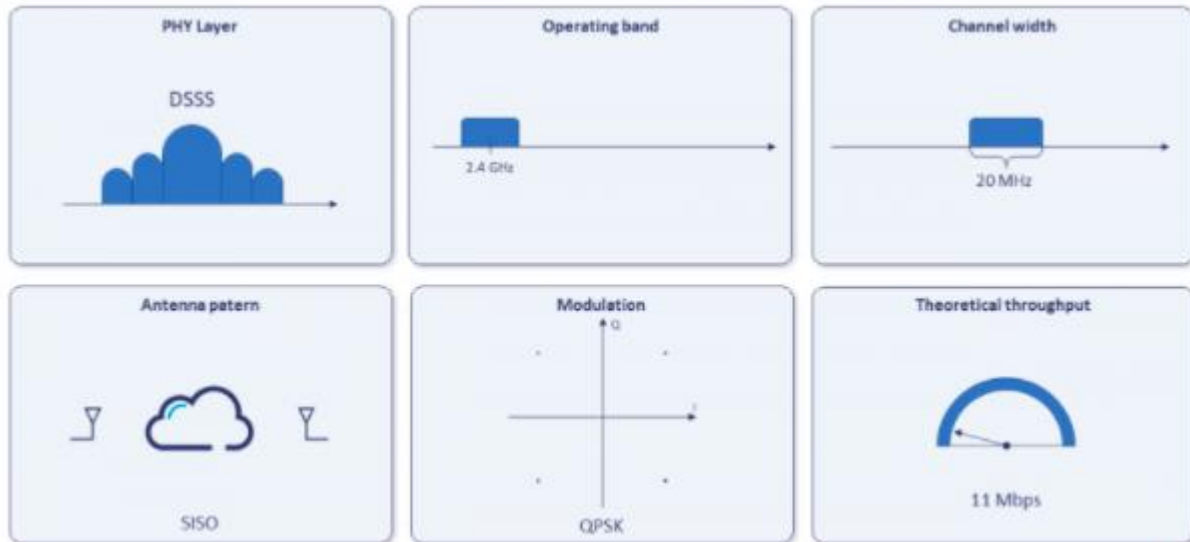


Figure 9 802.11b features [14]

Because 802.11b used the same unlicensed ISM radio frequency band, there is a possibility that a massive amount of interference would be there from home appliances such as cordless phones, Bluetooth devices, microwave ovens, or any other devices which also run on 2.4 GHz.

When you look at the raw data rates of 802.11b, it seems very appealing to the end-users. But in reality, the actual data rates will differ from the theoretical data rates; in fact, they will be quite smaller. This is due to a number of factors such as interference, environment, noise, etc. The maximum actual data rate will be around 5.9 Mbps using TCP. Another reason for low data rates is the use of CSMA/CA, where the device has to wait for the medium to be free and take its permission to send and receive data. In the case of UDP, the data rates will be somewhere around 7.1 Mbps. [15]

But even though the actual data rates were lower than theoretical data rates, the IEEE 802.11b is still considered a success due to its wide adoption by manufacturers, vendors, and users. This was truly a steppingstone of the Wi-Fi we know now and enabled several future standards to learn from its success. [15]



Figure 10 Cisco Aironet AP350 802.11B Access Point [16]

802.11a

802.11a came after 802.11b. this is due to the fact that it uses a 5GHz frequency band, which caused significant delays in its testing, release, and production. Since it was the first time, we had a standard using the 5GHz. But by the time it came out, 802.11b was so popular and adopted that 802.11a became a little less known. In fact, the data speeds offered by 802.11a were higher than 802.11b, which is 54Mbps. [14]

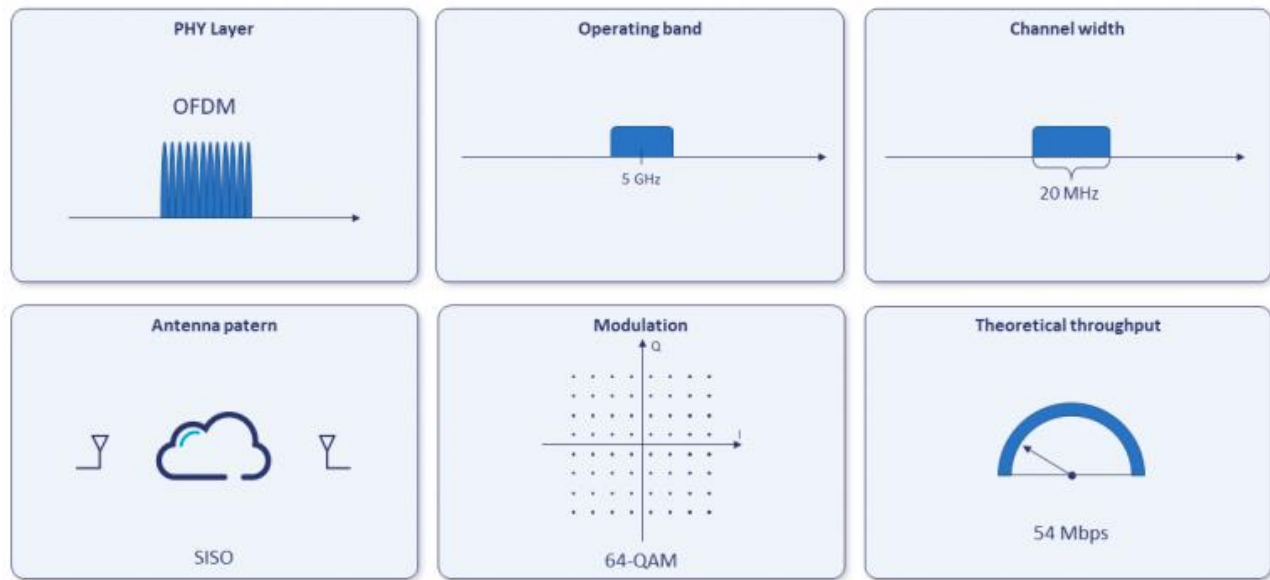


Figure 11 802.11a features [14]

The 802.11a uses the 5GHz band, but the overall channel width will be 20MHz, which is similar to the 802.11b. At the PHY layer, we will find that 52 sub-carrier orthogonal frequency-division multiplexing (OFDM) is being used, which can give us theoretical bandwidth of 54 Megabits per second. But again, remember that this is just a theoretical rate; when implemented practically comes down to around 20Mbps. There were initially 12-13 non-overlapping channels; the good thing is that 12 of them can be used indoors, and 4-5 can be used in an outdoor setting such as wireless mesh topologies. [14]

Many governments across the world have recently allowed secondary users to operate in the 5GHz band using a sharing technique adapted from 802.11h. 802.11a and 802.11b are not compatible and interoperable together since they operate on totally different bands unless you use dual-band wireless access points. In today's market, dual-band access points are widely available and used. [14]

There are pros and cons of using 802.11a versus 802.11b; the major advantage is the lack of much interference. Since 2.4GHz is overcrowded due to several other devices also being used in that frequency band range. Which causes frequency connection drops and low quality of experience. Whereas in the case of 802.11a, the 5GHz band is less crowded. Hence increased quality of

experience. But the disadvantage is the range of 802.11a, which cannot penetrate the walls and other thick objects like the 802.11b. Hence the range of 802.11a will be less as compared to 802.11b. [14]

In an area like interior office, however, OFDM offers inherent propagation benefits, and the higher frequencies allow for the construction of shorter antennas with better radiofrequency system gain, which offsets the drawback of an upper band of performance. [14]



Figure 12 SMC 802.11a Access Point [17]

802.11g

The next is 802.11g, which had become quite widespread when cell phones first became available. This one was introduced in 2003 as an upgrade to the earlier 802.11b standard, which operated in the 2.4 GHz frequency band but provided better bandwidth and less interference. [18]

It's the first IEEE standard to be pushed across the world under the moniker 'Wi-Fi.' The highest network throughput supported by 802.11g Wi-Fi is 54 Megabits per second, which is much better than the 11 Mbps bandwidth of 802.11b but significantly lower than that of the 150 Mbps data speeds of 802.11n. [18]

As we have seen earlier, it is not possible to achieve the theoretical data rates by any standard; it is the same case with 802.11g. Practically, in reality, the data rates will be between 24Mbps and 31Mbps, with the remaining throughput will be used up by overhead. [18]

Orthogonal Frequency Division Multiplex (OFDM), which was seen with 802.11a, has been adopted into this standard as well. This is the major reason that 802.11g could achieve higher throughputs. [18]

But the radio frequency band on which 802.11g operates is similar to the 802.11b, which is a 2.4 GHz range. Hence as compared to 802.11a, this standard could reach higher coverage and penetrate walls. [18]

The major advantage of 802.11g is the cross-compatibility, which means even if the wireless LAN access point is running 802.11g standard, it could connect clients running 802.11b. Even to this day, all the standards support connections from 802.11g clients because they operate in the same frequency band. [18]

Wi-Fi radios offering 802.11g were found in a variety of manufacturers and types of pc, laptops, and certain other Wi-Fi gadgets. 802.11g had become the presiding Wi-Fi standard which coincided when the Internet of Things device's use was exploding because it integrated several of the greatest characteristics of 802.11a and 802.11 b. [18]

Even today, we can see that the 54Mbps bandwidth offered by 802.11g is enough for a lot of home user and their devices. This can provide adequate video streaming as well as basic web surfing.



Figure 13 D-Link DWL-700AP 802.11g Access Point [18]

802.11n

One of the most popular implementations of the IEEE 802.11 family is 802.11n which came in the year 2009.

The major feature was the support of dual bands – 2.4GHz and 5GHz along with using a channel width of 40MHz. The PHY layer will still be using OFDM as 802.11a and 802.11g. Another mind-blowing feature that was the first time to be implemented was using multiple antennas, which is up to 4 antennas. As a result, bandwidth and stability have increased. Using all of the capabilities listed above, 802.11n may produce a throughput of 600Mbps, which is ten times faster than earlier standards. [14]

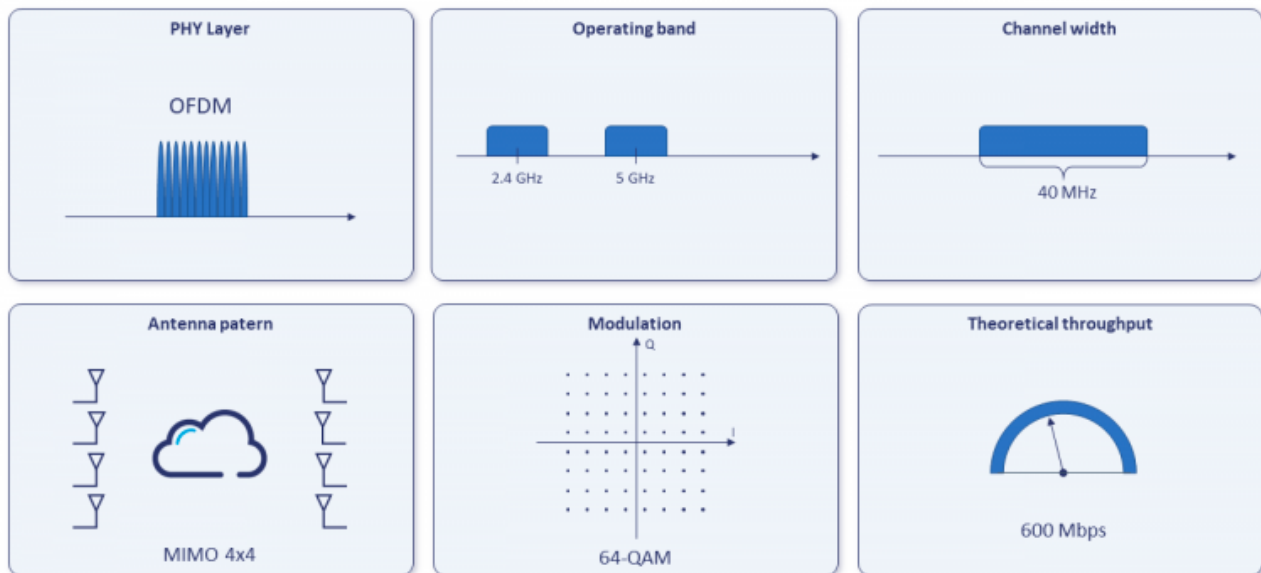


Figure 14 802.11n features [14]

To broadcast and receive data, 802.11n employs numerous wireless antennas. The capacity of 802.11n and comparable technologies to synchronize numerous concurrent radio communications is referred to as MIMO (multiple input, multiple outputs). 802.11n can handle up to four streams at once. Hence with the help of MIMO, there is a massive increment in the wireless network's coverage and performance. [18]



Figure 15 Cisco AIR-3602e 802.11n Access Point with Multiple Antennas [19]

802.11ac

802.11ac was made to accomplish equivalent to Gigabit Ethernet in order to stay competitive in the market and serve progressively widespread applications like video on demand that demand high-performance connectivity. Actually, theoretically, bandwidth up to 1 Gbps are possible with 802.11ac.

The 802.11ac standard has a wider channel of 160MHz which is way bigger than its predecessors. Also, the number of MIMO streams is higher for more concurrent communications. [20]

It utilizes the 5GHz radio frequency band, which helps avoid interference. Interference is quite common in the 2.4 GHz frequency band, as we have discussed earlier. Also, in 5GHz, the channel width can be higher. [20]

802.11ac wireless access points will continue to provide backward compatibility with the 802.11n standard. [20]

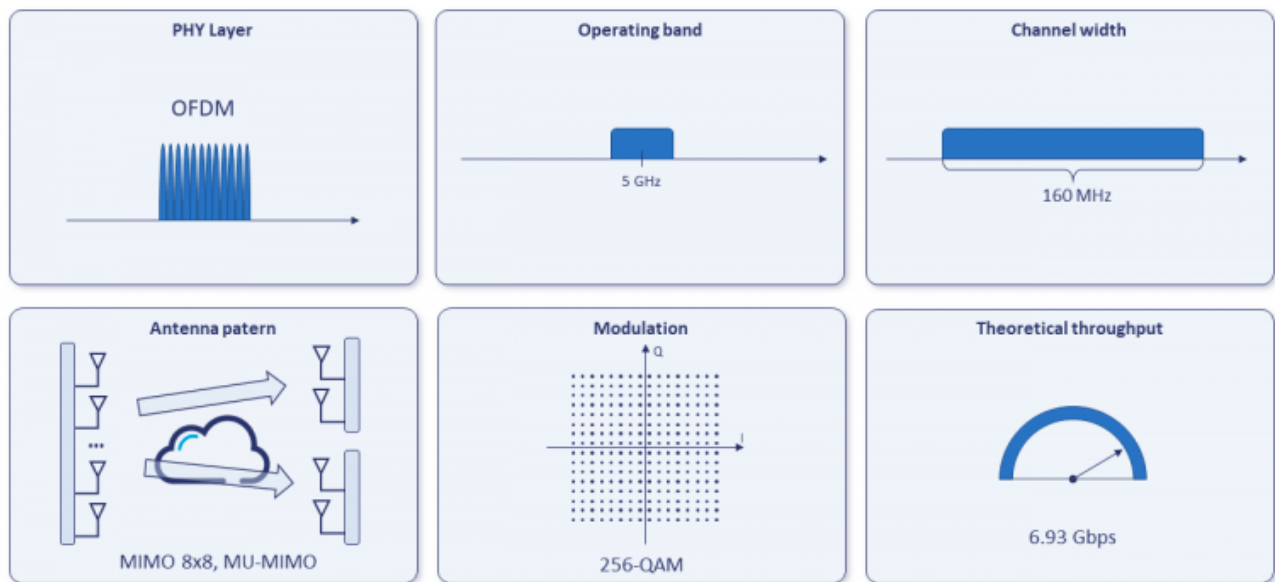


Figure 16 802.11ac features [14]

With recent advancements, 802.11ac evolved into two types, the first is 802.11ac wave 1, and another is 802.11ac wave 2. Using 802.11ac wave 2, we can achieve up to 3.5Gbps bandwidth, whereas with 802.11ac wave 1, the raw data rate was around 1.3 Gbps. [21]

Below is a comparison image to specific the technicalities of the 802.11ac wave 1 versus 802.11ac wave 2-

Feature	802.11ac Wave 1		802.11ac Wave 2		
PHY Rate	1.3 Gbps	1.3 Gbps	1.73 Gbps	2.6 Gbps	3.5 Gbps
# of Spatial Streams	3	3	4	3	4
Modulation	256 QAM	256 QAM	256 QAM	256 QAM	256 QAM
Channel Width	20, 40, 80 MHz	20, 40, 80 MHz	20, 40, 80 MHz	20, 40, 80, 80+80, 160 MHz	20, 40, 80, 80+80, 160 MHz
MIMO	Single User	Single User Multi User	Single User Multi User	Single User Multi User	Single User Multi User
802.11 protocol support	a, n, ac	a, n, ac	a, n, ac	a, n, ac	a, n, ac

Figure 17 802.11 ac wave 1 vs. wave 2 [21]

As discussed earlier, MIMO gives us immense throughput as compared to previous versions. In the above comparison, you can see the number of spatial streams; with the case of 802.11ac wave 1, it is three spatial streams. Whereas if you look at 802.11ac wave 2, it ranges from 3-4 spatial streams.

But the thing which remains constant is the modulation, which is at 256 QAM and backward compatibility to support older 802.11 standards such as 802.11a, 802.11n, and 802.11ac. This is due to those standards operating on the 5GHz radio frequency band.

Let us consider two scenarios on how an 802.11ac client will connect to an access point with multiple streams, which is four spatial streams in this case.

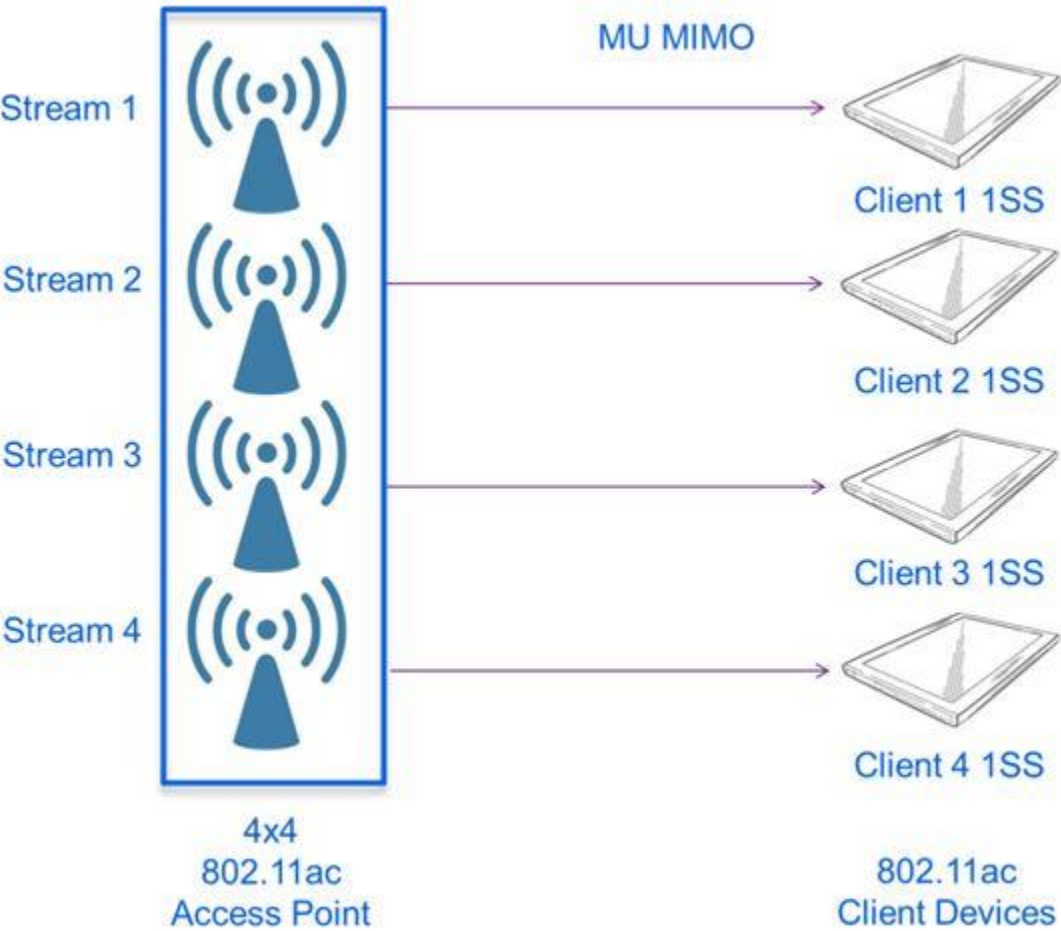


Figure 18 Scenario 1 - 4 Multiple Spatial Streams [21]

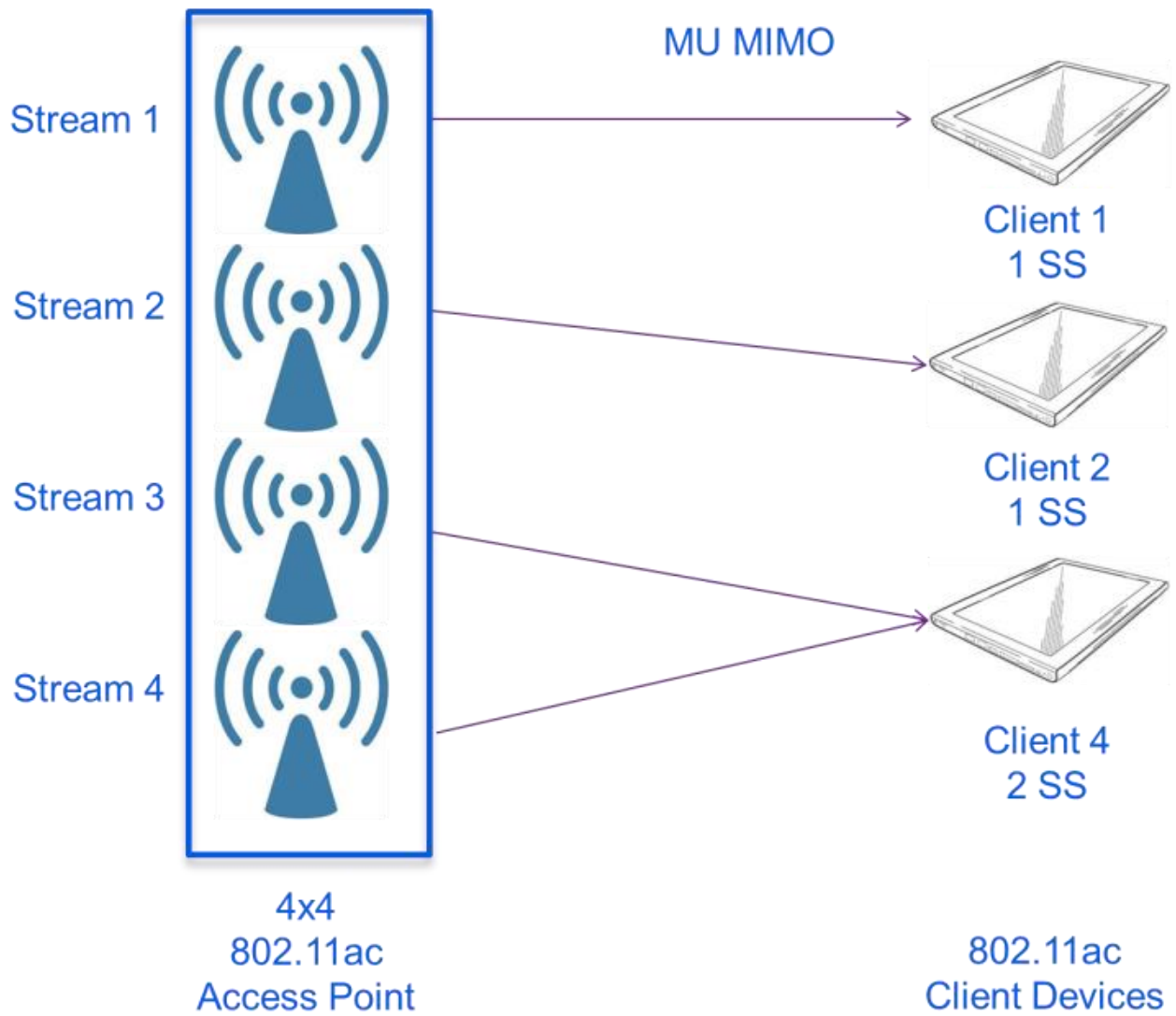


Figure 19 Scenario 2 – 4 Multiple Spatial Steams [21]

802.11ad

The next standard which we will discuss is the 802.11ad. This standard did not get as popular as its predecessors due to some reasons which will discuss later. It defined a new PHY layer that will be working in the 60GHz band, and the channel width will be larger, i.e., 2160 MHz

You must have realized now that 802.11ad is totally different than its predecessors. This standard was introduced to the industry as the WiGig brand name. [22]

The maximum raw data throughput was reported around 7Gbits per second. The major drawback is that it needs the access point and user device to be very close in a range which is around 1-10 meters.

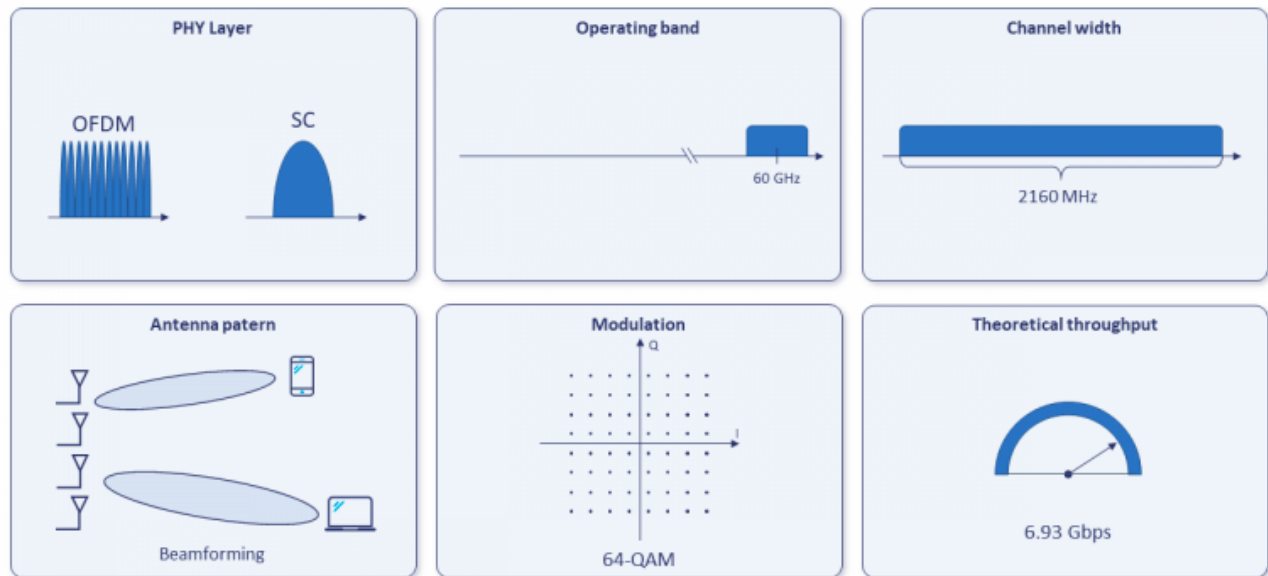


Figure 20 802.11ad features [14]

Despite its advertised unrivaled bandwidth, some Wi-Fi device makers potentially refused to embrace the 802.11ad standard as they believed it offers little value to the customers since we end-users don't need a huge amount of bandwidth for wireless LAN communication.

TP-Link announced the world's first 802.11ad router in January 2016. [22]



Figure 21 TP-Link Talon AD7200 Wireless Router [22]

802.11 ax

The next Wi-Fi standard we will cover is 802.11ax; it is one of the current 802.11 standards, which is commonly known as Wi-Fi 6. Since change and evolution is inevitable in the world of wireless LAN communication standards, 802.11ax also brings faster and more reliable communication. [23]

The features of Wi-Fi 6 are as follows- [23]

- Higher Bandwidth rates
- Avoiding congestion with stability in connection
- Long-lasting battery life
- Enhanced security

If you compare 802.11ax with the previous version, such as Wi-Fi 5, the bandwidth is three times higher, and the latency is 75% lower. The raw data rate of 802.11ax is around 10Gbps, which is enormous as compared to Wi-Fi 5. This will enable multiple users to simultaneously download and upload high-definition video streams. In today's world, where Netflix, YouTube, and Prime are major applications in every household, a faster wireless connection is a must. [23]

As we discussed in earlier standards, the theoretical raw data rate is around 10Gbps, but it doesn't mean that every router or access point will give us that amount of bandwidth. There are multiple factors involved, such as interference and Internet data rate provided by the Internet service provider.

Target wake time (TWT) is a Wi-Fi 6 innovation that minimizes end users' equipment energy consumption. It essentially allows the end-user and access point to agree on when data will be communicated through, enabling the end-user device such as a mobile phone to conserve energy when there is no wireless communication between the two. [23]

Let's consider a scenario where TWT comes into play. Usually, what happens is the device will always stay online throughout, as long as it's connected to the Wi-Fi. But TWT allows the end-user device's radio to shut down when it's not required. [23]



Figure 22 Aruba AP-505 802.11ax Access Point [23]

Challenges faced in deploying Wi-Fi



Figure 23 Students in a University Auditorium [24]

We cannot imagine a world without Wi-Fi, let alone the universities or schools. Quick and stable Internet is not a luxury anymore; it has become a necessity that needs to be there in place. [24]

Every person today carries averaging three connected devices such as a laptop, cellphone, and tablet. Proper planning and careful consideration of wireless networks are of utmost importance. [24]

Let's say, for example, in hotels, maximum customer reviews mention "Wi-Fi" either good or bad reviews. This implies the importance of stable and better wireless connectivity in our modern world. [24]

Any network that hasn't been updated in the past five or so years can be considered outdated, especially if they're not up to the IEEE 802.11ac standard. [24]

These are the common challenges faced in deploying large scale Wi-Fi networks-

1. Cost

The cost will always be a more significant factor in any IT solution. I have seen that companies majorly spend a big chunk of their budget procuring and maintaining IT solutions.

Any Wi-Fi network of more than 4-5 years is considered outdated. As discussed in the previous sections, the IEEE 802.11 standards are developing rapidly, and people purchase mobiles or laptops at a quicker rate than it was ten years ago.

Newer models support newer standards; hence the demand to adapt to the recent user device is always required. However, the standards are made in such a way that they have legacy support.

Also, with the pace at which the data and security threats are evolving and increasing, the need to adapt to the recent technology standards is a must. But with, the need to upgrade comes with a massive hole in the wallet of an enterprise. [24]

It's costly, and finding out how to pay for everything is a difficult and tough issue. Understanding what you need in terms of IT is one thing; having a budget allocated to fund it is quite another.

During unprecedented times like recession or recently like COVID-19 pandemic, it becomes more and more difficult to survive for businesses. Hence many IT vendors are offering payment options like paying in installments or subscription-based models.

It's not only the device cost but also the cost of replacing and installing. Imagine a business with multiple sites across the country; it's a daunting task to replace more than 5000+ access points in diverse locations. Sometimes the cost of replacement and installation would exceed the cost of access points.

2. Coverage and Density needs

This is another challenge when planning for Wi-Fi networks. Sometimes, we have concrete information on this, but most of the time, it's assumptions only. Coverage and density are like a must-win area for wireless network planning.

The important thing is that both should work; it's not successful deployment if you succeed in achieving only one of those. The first question which comes up while planning for the Wi-Fi is – Where is the wireless access needed?

The answer to this question usually comes from the customer/enterprise who owns the Wi-Fi. But it's often the planning engineer who must guide the enterprise because sometimes even the owner doesn't know that they will need the wireless in certain areas like washrooms, laundry room, outdoor, etc.

If the wireless isn't covered in these areas, the blame will always come onto the planning engineer even though the Wi-Fi owner didn't mention those areas. Hence careful planning is of utmost critical.

Coverage is still manageable using the solutions we will discuss in the next section, but managing density is another ballgame. Density refers to the number of concurrent users that are expected to have connected to a single access point at a given time.

Usually, our home wireless access points give excellent coverage but are not meant to support 100+ users concurrently. Because it's practically not possible to make a cheap wireless access point that can support so many users concurrently, failure to address the density requirement properly will result in a poor Wi-Fi network and drops in the connection.

Another factor is the future expansion; coverage and density requirements must always consider at least 20 percent capacity for future expansion. This will help the infrastructure to sustain for a minimum period of 3 – 4 years down the line.

3. Network infrastructure

Often people don't realize that Wi-Fi infrastructure needs a wired infrastructure backbone to run. This is the biggest misconception surrounding the Wi-Fi industry.

Wireless connectivity is just the access layer network connectivity to the end devices such as computers or mobile devices.

If you are planning for the Wi-Fi network, you must give the same importance to the wired backbone network. Different types of challenges occur, such as the type of connectivity required to connect the wireless access points.

Most of the current wireless access points support only copper connectivity which is RJ-45 Jack. This can be connected to a twisted pair cable, which can be CAT5 or CAT6 or even the latest CAT7. The point to consider here is the maximum cable length which is approx. One hundred meters, but practically, it is only like 80 meters.

If we have a wireless access point at a location of 100+ meters from the switch, it might be a problem. The thing here to consider is whether the cable will be run along with electric cables because it will cause interference and impact connectivity.

Aggregation switch working at the core or distribution layer of the network backbone must support the bandwidth required to connect several access points. The misconception around a network switch is its throughput calculation. People often misinterpret the throughput as the number of ports multiplied by twice the maximum port speed. Still, in reality, it depends on the manufacturer on how much throughput the switch is capable of.

Another thing to consider is the power for wireless access points. Access points work on DC power, and arranging for a power source near the access point can be pretty troublesome, especially when the access point is mounted on a ceiling.

4. Physical Conditions

Placement of the wireless access point is crucial due to the environmental conditions. There might be challenges in the placement location, such as water leakage, moisture, or even the ceiling height in places like warehouses. Sometimes the placement becomes difficult due to heat in areas like the kitchen.

In the modern world, we expect Wi-Fi to be present in almost every place we visit, such as parks or beaches. The challenge to deploy in these places is an environmental challenge: rain, dust, snow, and heat.

Also, some home or company owners do not want their interior look to be tarnished due to the presence of access points. This creates a challenge for the planning engineer to accomplish deployment without spoiling the aesthetics of the building.



Figure 24 Wireless Access Point placed outside in the rain [25]

5. Interference

Radiofrequency (RF) interference in Wi-Fi may be devastating. Several businesses apparently managed to get through it by avoiding it completely, but unfortunately, others aren't that lucky; hence they are facing a huge number of problems leading to loss of quality of experience. The main reason is interference from others. Hence, it's critical to understand the effects of Radio Frequency interference and how to avoid it. [26]

Before we dig deep into the world of Radiofrequency interference, let us understand how exactly the end-users communicate and send packets to the wireless access point over the medium. Whenever the user device wants to send data, it will check if the medium is free. In the case of wireless, the medium is air. But due to radio frequency interference, sometimes the packet is not reached by the access point. This mechanism is called CSMA/CA.

Due to the unwanted signals in a particular area, it becomes quite difficult to send and receive packets. Sometimes the access point is busy attending to other devices' signals, and the real 802.11 stations keep waiting.

The exact problem is that these interference RF signals are not following the 802.11 protocol standard; hence they appear randomly out of nowhere, which creates huge problems for the real 802.11 users who are following and obeying the standards. Due to this, the wireless access point is busy and causing delays and latency to the users and degraded quality of experience. In some cases, 802.11 protocols will try to keep running in the face of RF interference by turning to a reduced bit rate, which limits the usage of wireless systems. In an extreme scenario, which really is rare, the end-user devices will wait until the interference has fully disappeared, which might take hours. [26]

Another question is, where on earth does this radio frequency interference emerge? As per our previous sections, we have mentioned again and again that 2.4 GHz operates in the ISM frequency band. This band is unlicensed and has also been used by other home appliances.

The common sources of interference are-

- i. Nearby wireless LAN networks
- ii. Microwave Oven
- iii. Home Landline cordless phones
- iv. Bluetooth headphones
- v. Walkie Talkie
- vi. Infant monitoring system

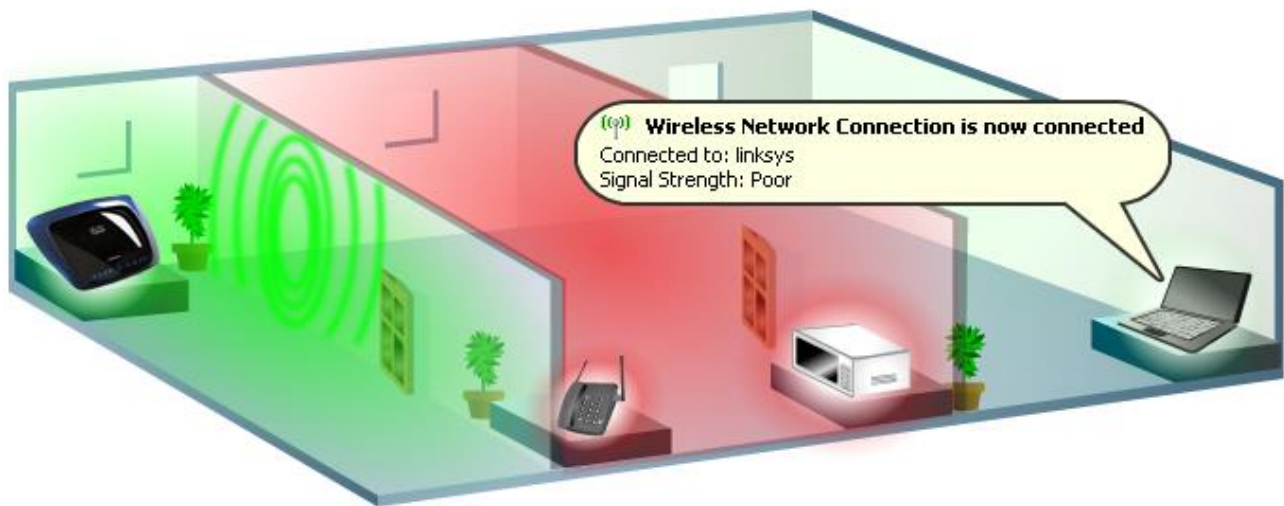


Figure 25 Interference caused by home appliances [27]

6. IT Staff

I am considering a complex wireless LAN network with 1000+ access points and several locations around the globe. This poses a severe challenge for the enterprise due to staff requirements.

To manage and operate such a huge wireless network, you will need competent IT professionals who have the knowledge to manage, configure and troubleshoot a wireless LAN infrastructure. In today's world, it will be pretty challenging to hire many such staff in the IT department. Hence, we need a proper solution to address this challenge.

Is it said that IT professionals keep track of the number of help desk calls they receive might give a fair indicator of whether they're successfully managing their wireless LAN infrastructure. You can't just set it and forget it; that will only lead to more Wi-Fi problems. [28]

Solutions to the challenges in deploying Wi-Fi

1. Cost

The solution to expensive Wi-Fi access points and controllers lies within the next solutions, which we will discuss later. Because of careful planning, the Wi-Fi solution will become relatively cost-effective.

But market analysis is of utmost importance, such as comparing the top wireless vendors offering the latest 802.11 standard solutions. Some of them are offering easy pay-to-go payment schemes such as subscription-based services or paying in installments.

Installing the wireless access point in an easily accessible location will enable anyone to replace the access point in case of an upgrade. In this way, we will not require expert personnel to replace it.

Another possibility these days is transferring from the CAPEX model to the OPEX model. Instead of paying all the equipment costs and licenses payment, you can opt for the subscription-based payment model that Cisco Meraki offers.

Many IT Procurement managers or someone responsible for purchasing into IT infrastructure may ignore the OPEX model and use the upfront model instead. But sometimes, when you look at the inflation and future expenses, this might fire back.

2. Interference

We can take the following methods to avoid or reduce potential Radio frequency interference issues-

- i. One of the first things we can do before deploying a Wi-Fi network is to analyze the existing radio frequency in that area. Monitoring one time won't help me; monitoring several times at different times will definitely help us to know what to expect and how to deploy the access points properly in order to reduce the Radio Frequency interference. [26]
- ii. After identifying the causes of radio frequency interference, we can take the next action to avoid those by shutting them down. This is 100 percent effective, but we cannot use it all the time. Let's say, for example; we have a microwave oven in the neighboring apartment; we can't simply tell them not to use it. All we can do is avoid using Bluetooth headsets or microwave ovens in our Wi-Fi area.
- iii. Another solution to these interferences is proper planning of Wi-Fi access points; we need to deploy and install access points in such a way that the signal strength remains quite high. Because the point to note is that when the signal becomes extremely low or poor, that's it when the interference becomes the maximum. We will cover more on this in the Coverage and Density section.
- iv. With the help of artificial intelligence, some vendors like Cisco have used technology like Cisco CleanAir, wherein they automatically sense the medium and avoid using channels that are already overcrowded hence increasing the quality of experience. Let's say microwave ovens usually operate in the upper band of the 2.4 GHz range; hence if we were used to using channel 6 or 11, it might be possible to avoid the interference. [26]
- v. Focusing on deploying Wi-Fi operating on 5GHz, it is a no-brainer that we need to deploy the maximum of our wireless LAN networks focusing more on the 5GHz band instead of the 2.4 GHz band. Dual-band, wireless access points will be pretty helpful in this case.

Below we can see how the Ekahau Spectrum Analyzer works and gives us output after an RF Spectrum analysis-

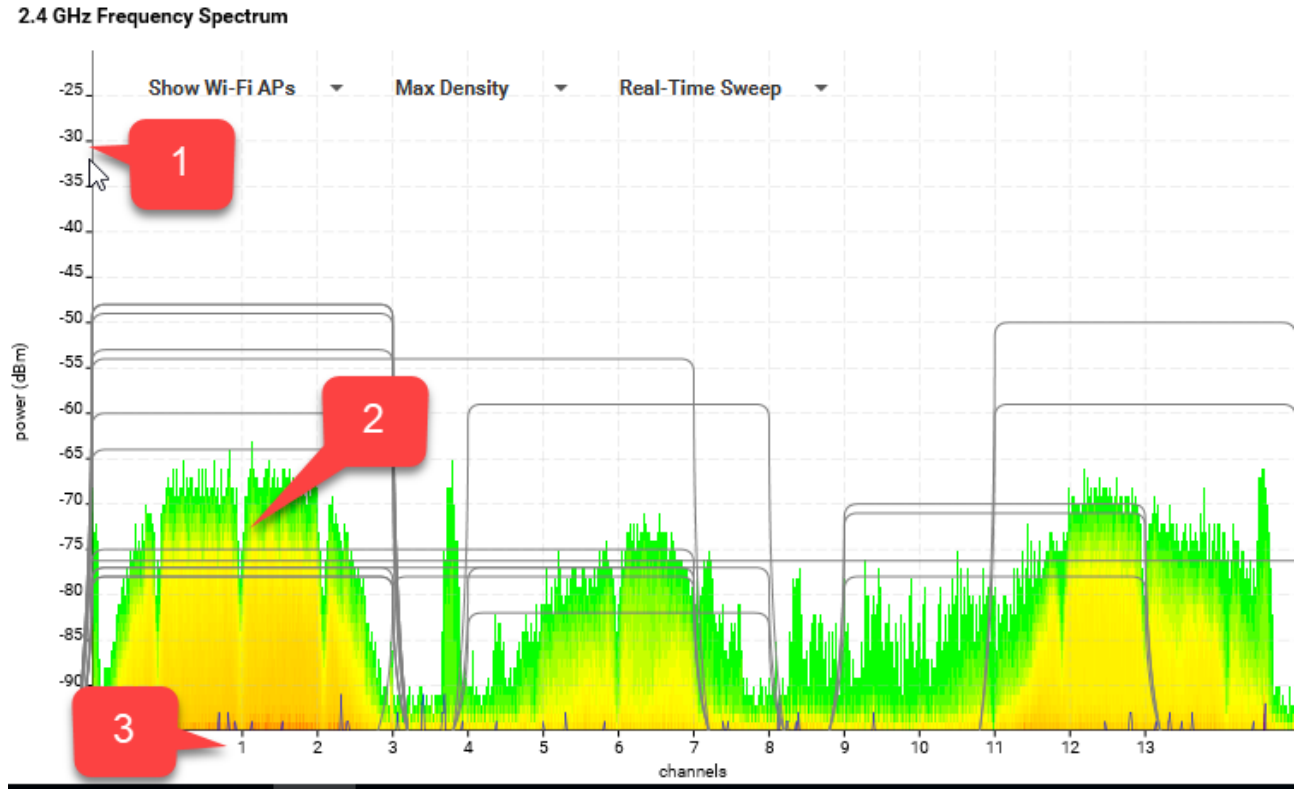


Figure 26 2.4 GHz RF Spectrum Analysis [29]

1. Intensity of the Interference in dBm
2. Spectrum activity on Wi-Fi channels 1-3
3. Wi-Fi channels

The fundamental concept is to be proactive and constantly check for radio frequency interference. There is no lasting fix to RF interference difficulties; for instance, your neighbor may install a new strong access point in his home, causing problems in your own wireless LAN network. As a result, RF interference may increase or decrease over a period. Hence, we must keep a close eye on the use of Wi-Fi gadgets in your immediate environment.

3. Physical Conditions

The placement and location of the wireless access point within a room is extremely crucial, first of all, because of the coverage it provides, and secondly, it must fit in the existing building and environment conditions.

The planning engineer will have to sit with the client, building owner, interior designer, or architect to understand how the interior of the room will be. This is important so that they blend and do not spoil the aesthetics of the building.

As we can see in the below figures, the access point has been installed in such a way that it works perfectly, blends with the room, and doesn't ever compromise on the aesthetics of the room. In the second figure, the access point is hidden carefully, which is again the art of the planning engineer.



Figure 27 The goal accomplished is to install the AP in a low-profile ceiling mount while still using the original tile. [30]



Figure 28 Example of an AP deployment within an intelligent building ceiling designed for aesthetics. The goal accomplished is to hide the AP. [20]

The weather would be one more important factor to think about. Because you'll be outside, the environment will vary, and the seasons will change. Throughout the summer, it may rain, snow, or be extremely hot. The functionality, efficiency, or performance of the wireless LAN will be affected by differences in seasons.



Figure 29 Outdoor Access Point mounted on a pole [48]

Fortunately, today IT vendors have different outdoor access points offered, which can offer robust protection against the weather. But another challenge with outdoor access points is the materials used to mount the access point and its surroundings, such as building materials. This can hurt the performance of our outdoor Wi-Fi network.

While most Wi-Fi APs with integrated antennas should be installed in the horizontal configuration, that's not always possible when working with solid vertical walls. Furthermore, choosing a location to mount and rack the cabling and component is an issue. [30]

In addition, some solutions, such as navigation, demand that the access points be pointed in specific directions. The whole aim is to provide the consumer with a mounting system that will make wireless access point placement simple and rapid while also offering security and looking perfect aesthetically. [30]

4. IT Staff

Training your IT staff is not the only solution for a large-scale Wi-Fi network; there are other things that can be focused on improving the manageability of a large-scale Wi-Fi network spanning several locations.

The goal is to create a cost-effective migration path for Wireless APs updates or changes. As technology progresses, wireless access points will be technically upgraded every two to four years. Providing an appropriate mounting option to allow for a rapid and cost-effective update would aid in cost reduction and consistency. [30]

For servicing and administration, it is critical that the staff or location has rapid and straightforward access to the Wireless access point and the wiring elements. Providing a wireless access point mounting solution that protects the access point and modules while allowing for quick servicing access will save the client time & expense. [30]

Another solution would be to go with the latest Wi-Fi solutions on the Cloud, such as Cisco Meraki Wireless LAN solutions. We will discuss this in the upcoming sections.



Figure 30 Easily accessible access point in hotel room [31]

For training, the best resources would be to train on the following certifications-

i. CWT® - Certified Wireless Technician

This is for the entry-level technicians who are responsible for installing and configuring the wireless access points. [32]

ii. CWNA® - Certified Wireless Network Administrator

This certification is an advancement to the certificate as mentioned above, where the staff will learn about the RF behavior, site survey, etc. [32]

iii. CWDP® - Certified Wireless Design Professional

This is a professional-level certification which folks who already have CWNA and need a thorough understanding of RF technologies and their application. This will guide on how to design a network carefully and correctly. [32]

There are many certificates offered by the CWNP - Certified wireless network professionals corporation, which are usually vendor-neutral.

5. Infrastructure Backbone

Since the access point needs copper connectivity from the switch, personally for me, the rule of thumb was placing an IDF every three floors in case of a multistorey tower, which would allow sufficient length not exceeding 90 meters between the network switch and wireless access point.

But sometimes, only the cable length factor is not the only one that counts. Another is the existing infrastructure such as AC ducts, power cables, and water pipes. Suppose any close contact between the copper cable and such infrastructure may cause interference. In these scenarios, Shielded Twisted Pair – STP comes to the rescue.

Shielded twisted pair (STP) is a kind of copper cable which is used primarily for telephone and local area networks (LAN) in some commercial installations. Two separate copper wires but with insulation are coupled around each other to prevent interference or electromagnetic resonance between the pairs of copper wires. Both copper wires are required for each signal on twisted pair. [33]

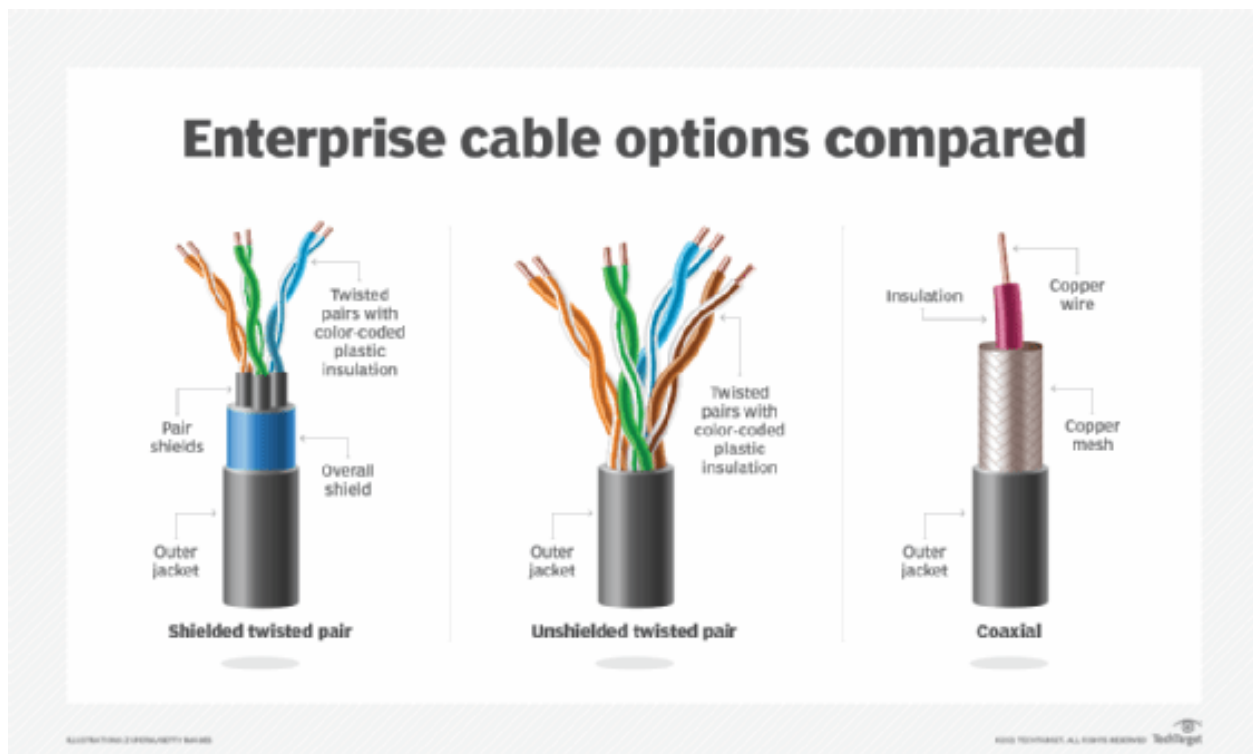


Figure 31 Different types of copper cables [33]

Around a decade ago, the access points were usually powered using a power adapter. It was pretty troublesome to arrange for a power source near the access points, especially when the access point was mounted on a ceiling.

With the advent of IEEE 802.3af and later IEEE 802.3at, we could actually provide 15.4 W or 30 W power, respectively, using existing UTP or STP cables. This was a game-changer in implementing wireless access points and enabling widespread use. The power source here will be the network switch which is Power Over Ethernet - PoE enabled.



Figure 32 Cisco 3850x with Wireless LAN controller inbuilt [34]

6. Coverage and Density needs

This will be an extensive section about solutions to the challenges we face about coverage and density needs in a Wi-Fi network.

The first challenge is how do you evaluate or predict the Wi-Fi coverage of a building which is non-existent. There is no place for you to go physically and see. Here comes the RF predictive software. In our report, I have used the most famous one, which is Ekahau software.

Ekahau Pro guarantees great performance by including capacity, planning, and analysis. All Wi-Fi access points, hundreds of antennas, and historical and current Wi-Fi technologies, including 802.11ax, are all supported (Wi-Fi 6). If you don't already have a Wi-Fi system, Ekahau Pro will figure out how many wireless access points you'll really need and which location they should go to. For optimal performance, Ekahau Pro would also suggest a wireless LAN network setup. Ekahau Pro enables fast and simple site surveys, range and density analysis, bandwidth optimization, and diagnostics for existing wireless LAN networks. [35]

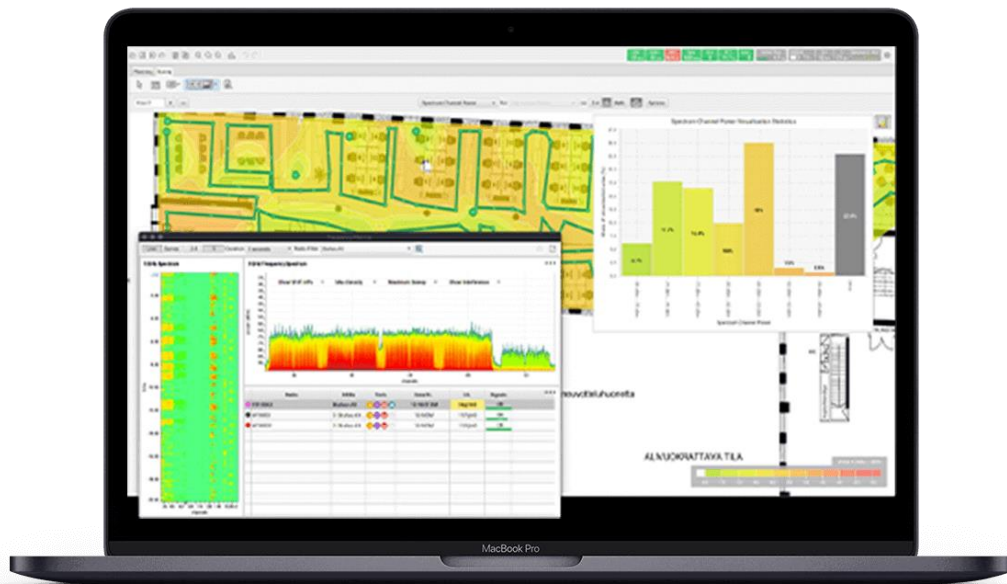


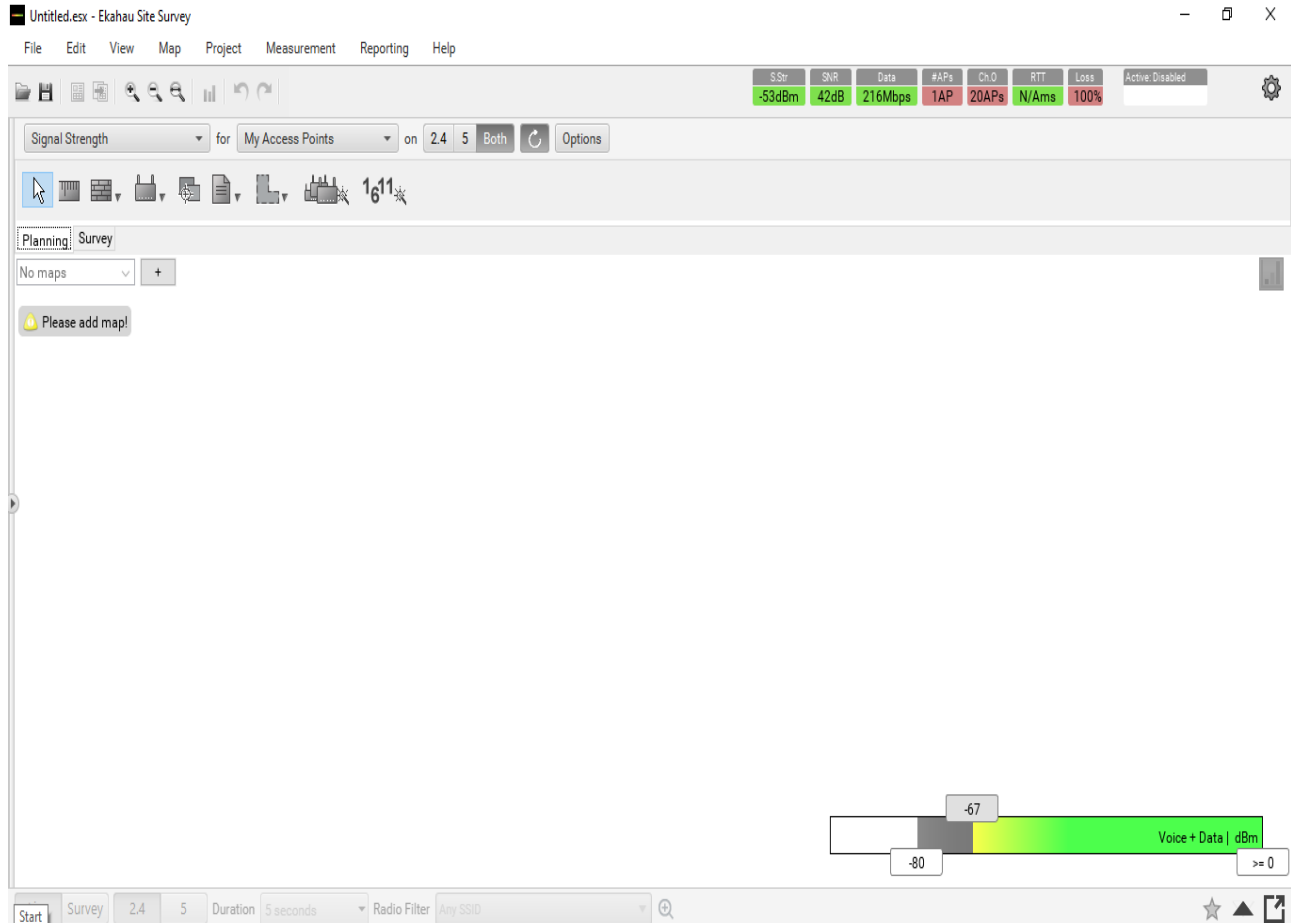
Figure 33 Ekahau Pro software [35]

I have downloaded the trial version of the Ekahau Pro software, wherein it gives me full features of the paid version; the only downside is I cannot save any changes made to the map or save the project itself.

But for our demonstration, it will serve the purpose.

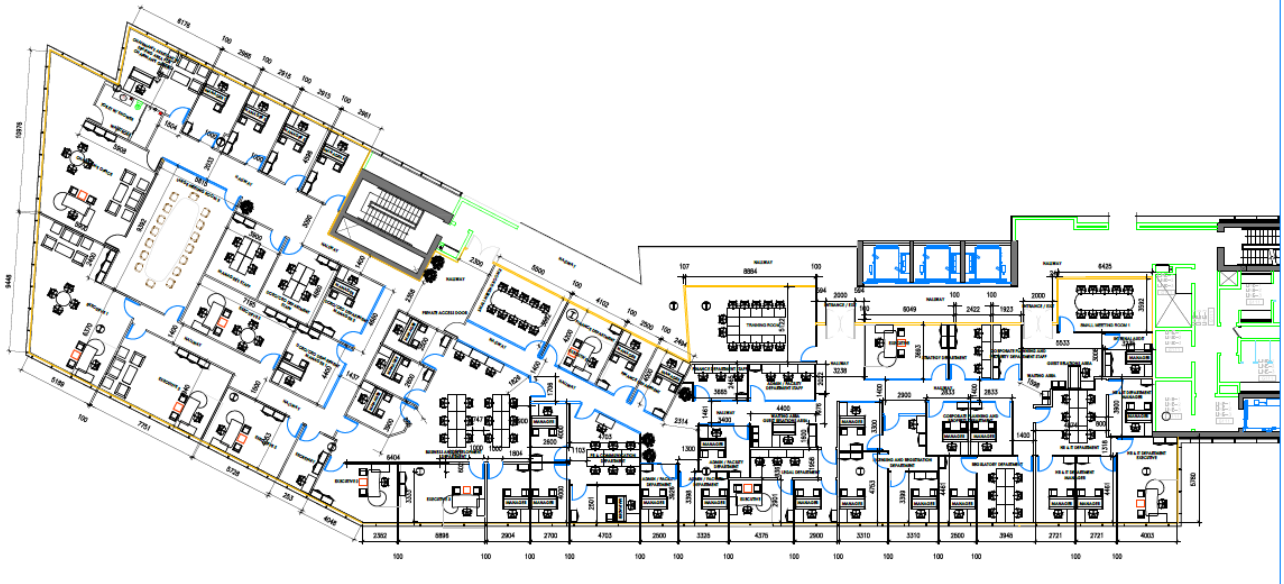
We will go step by step and perform a predictive survey-

i. Open Ekahau Pro Site Survey software



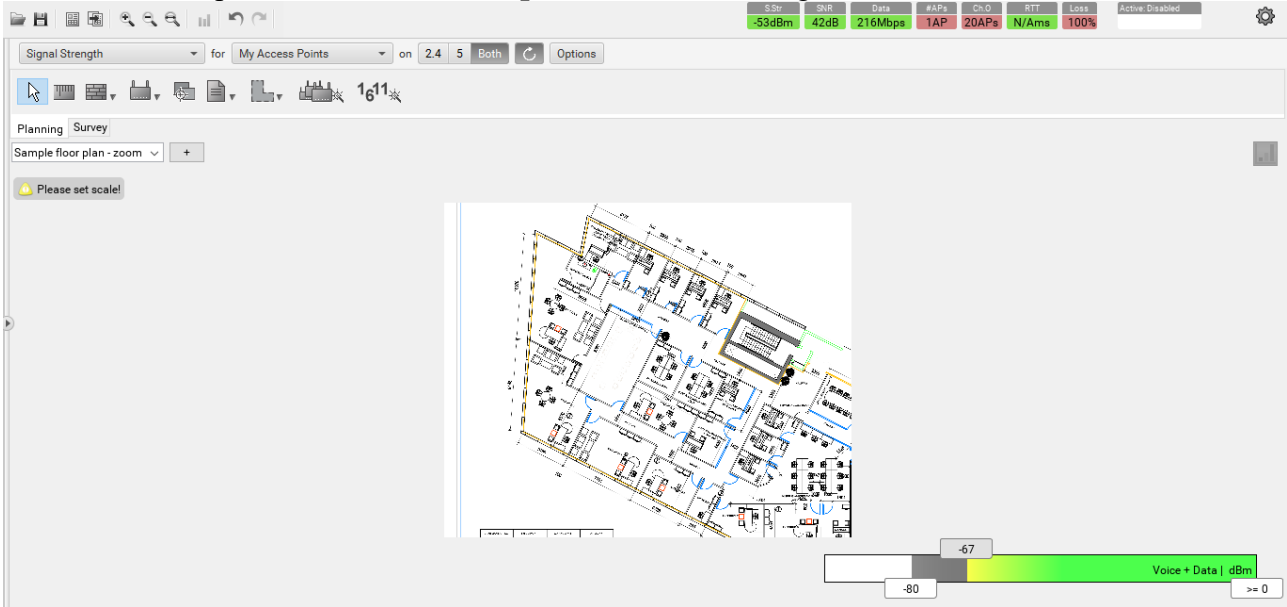
ii. At this moment, we need to import/add a map, which is an image file of a CAD drawing. Most people import a .dwg file, but the Ekahau software does not support it.

iii. I have a sample floor plan of a building; the file is converted from .dwg into .jpg format.



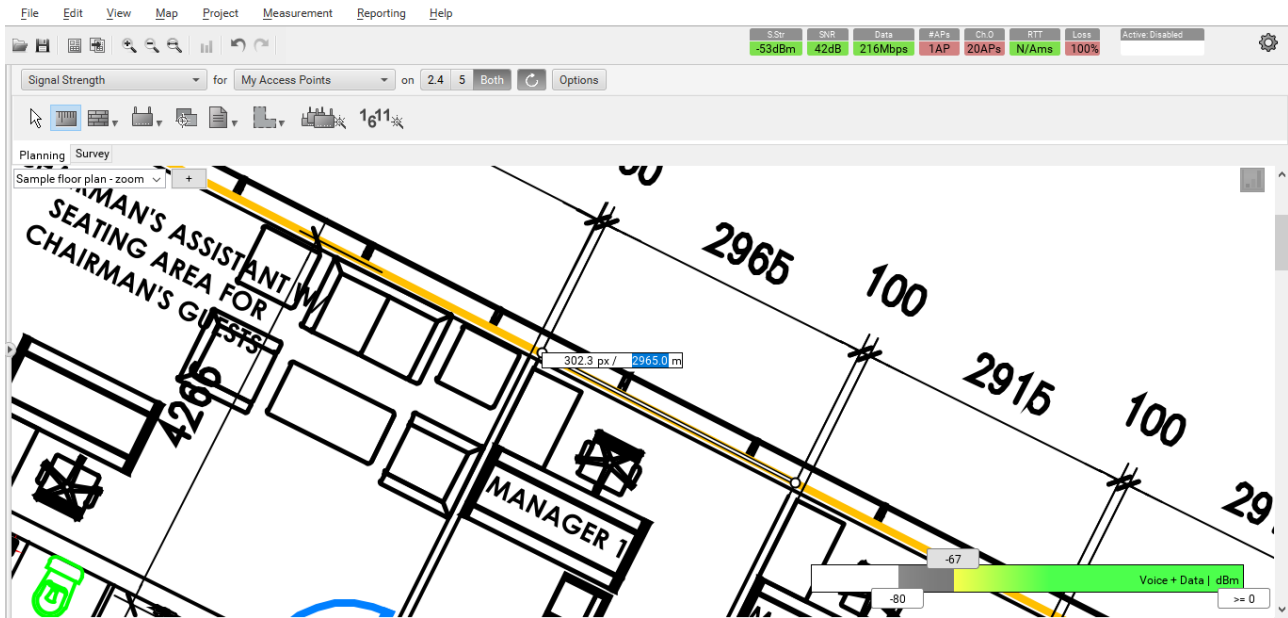
iv. Out of the whole area, our focus will be on the left part of the floor map.

v. Click on the option **‘Please add a map!’** and select the image.

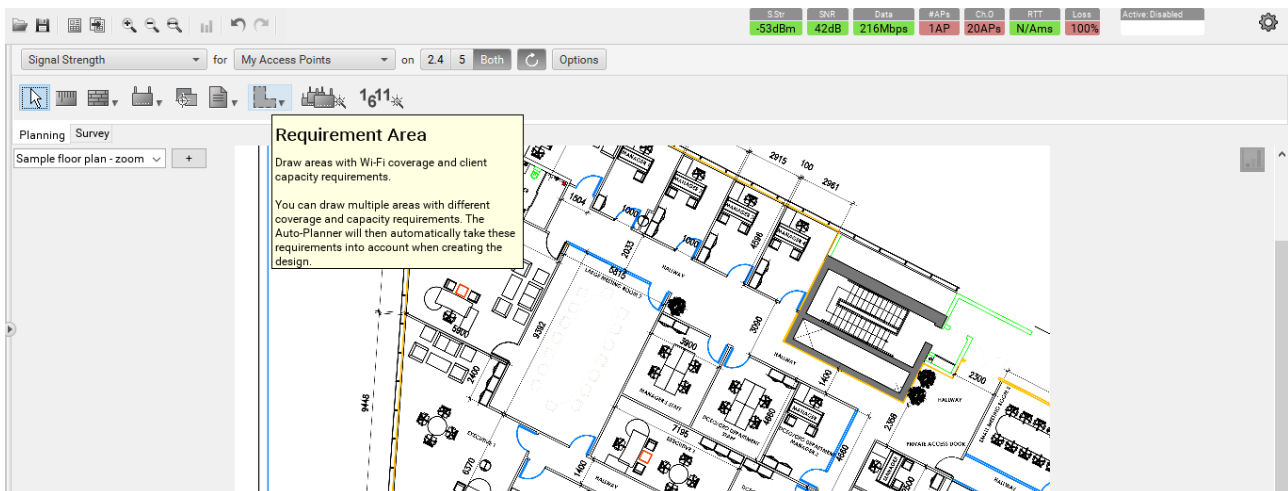


vi. Now, we need to define a scale in order for Ekahau software to understand the scaling of the floor map.

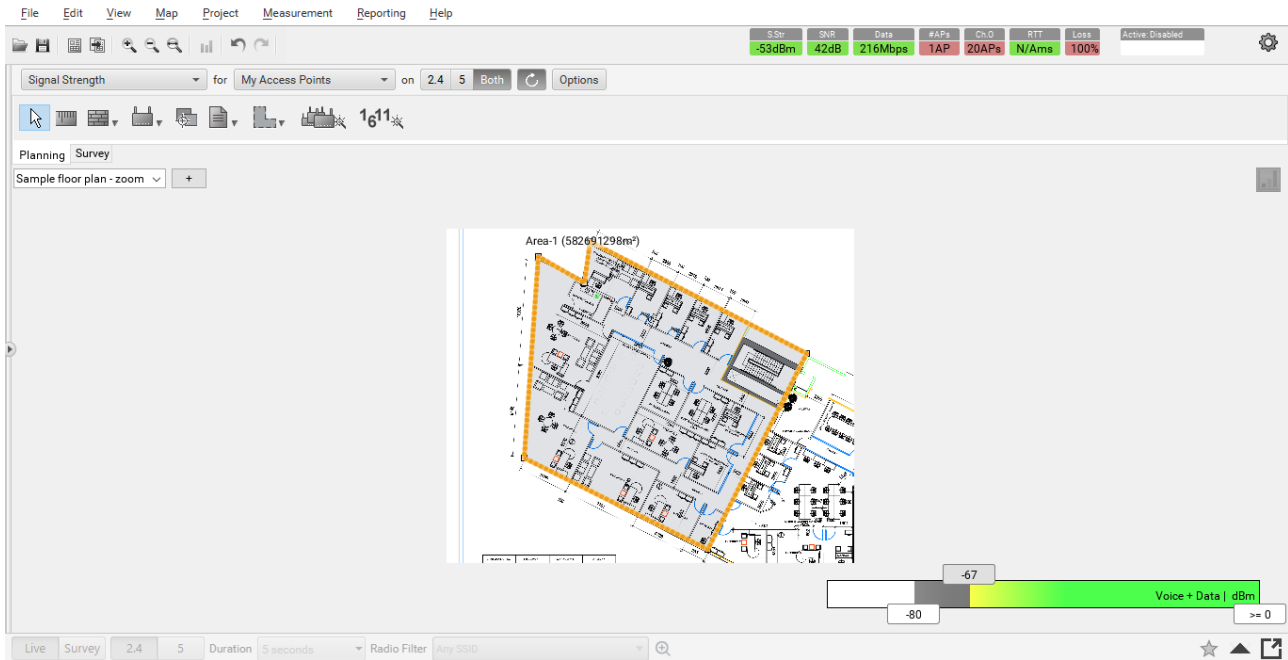
vii. Click on **‘Please set scale’** and, with the help of scale provided on the map, draw a line and mention the length in meters.



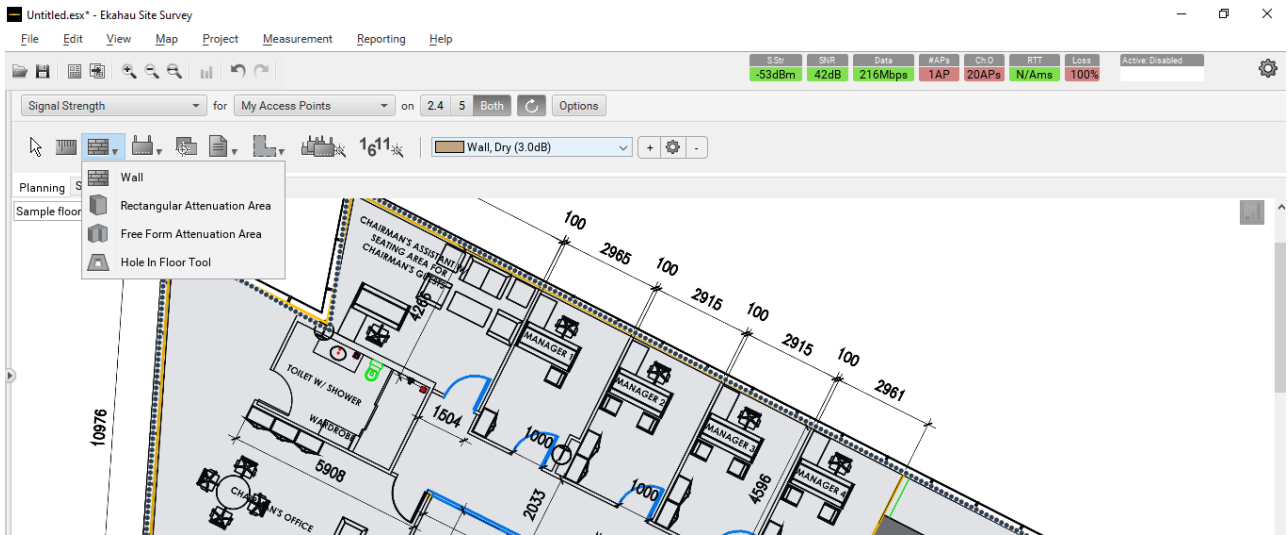
vii. Next step is to set a **requirement area**.



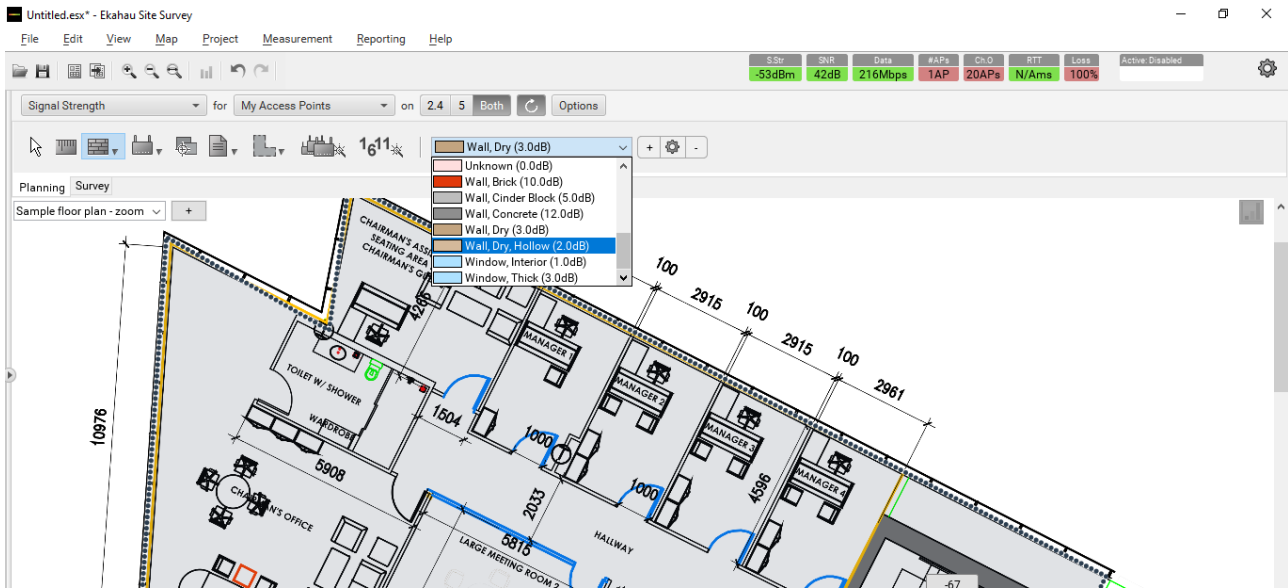
viii. Requirement Area means the area where our focus is, such as excluding any outdoor area where the RF will reach.



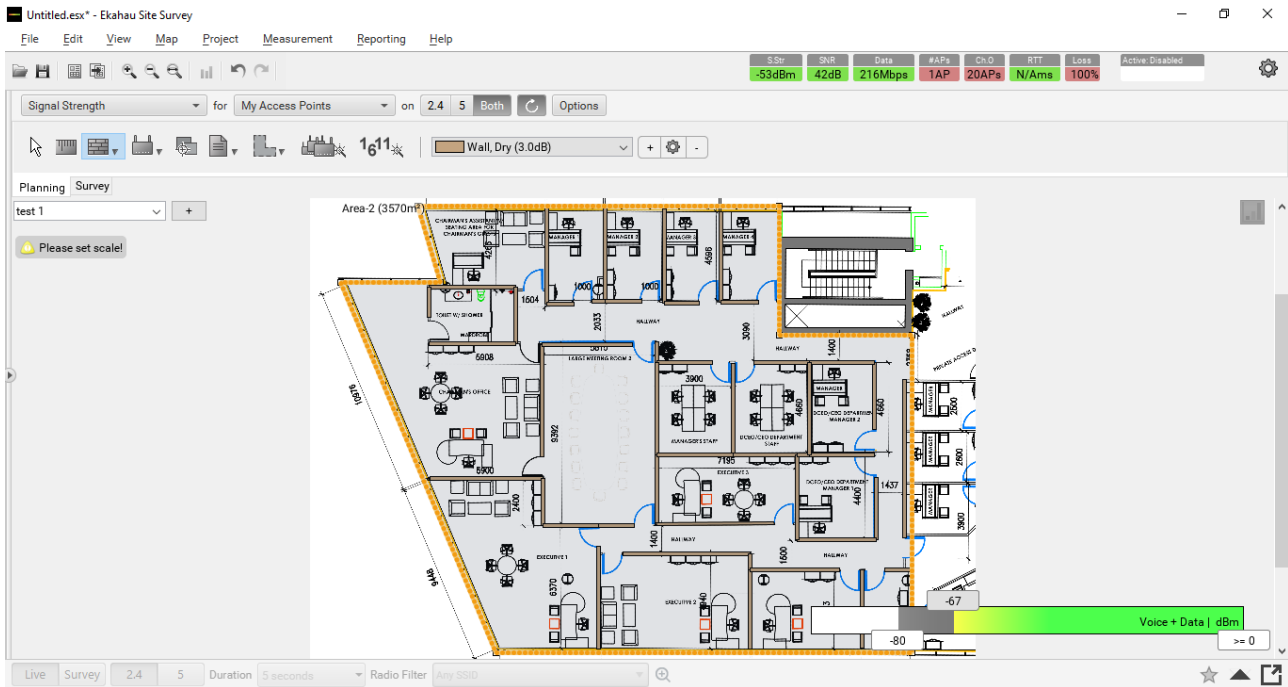
ix. Next step will be defining the structure inside the area, such as walls or elevators, which will cause an interruption in the path of wireless RF. We have several options as shown below-



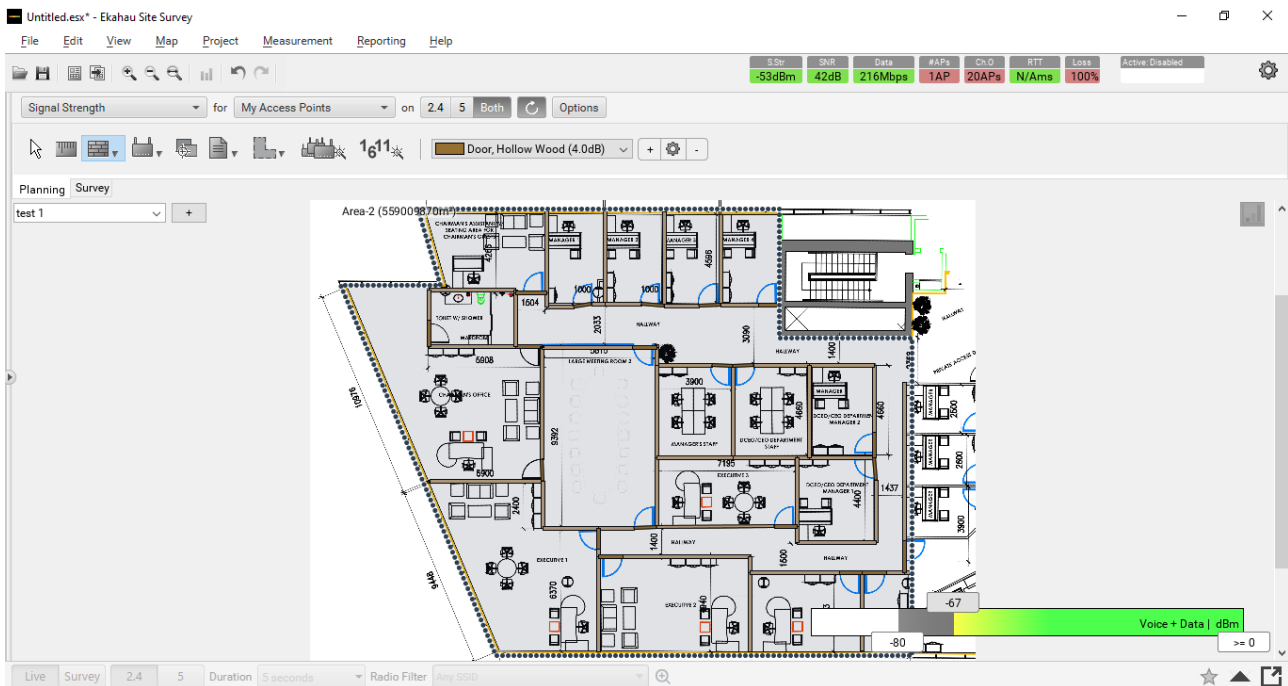
x. In case we choose the **wall** option, we have even more opportunities to decide which kind of wall or window or door we have in place, such as shown below –



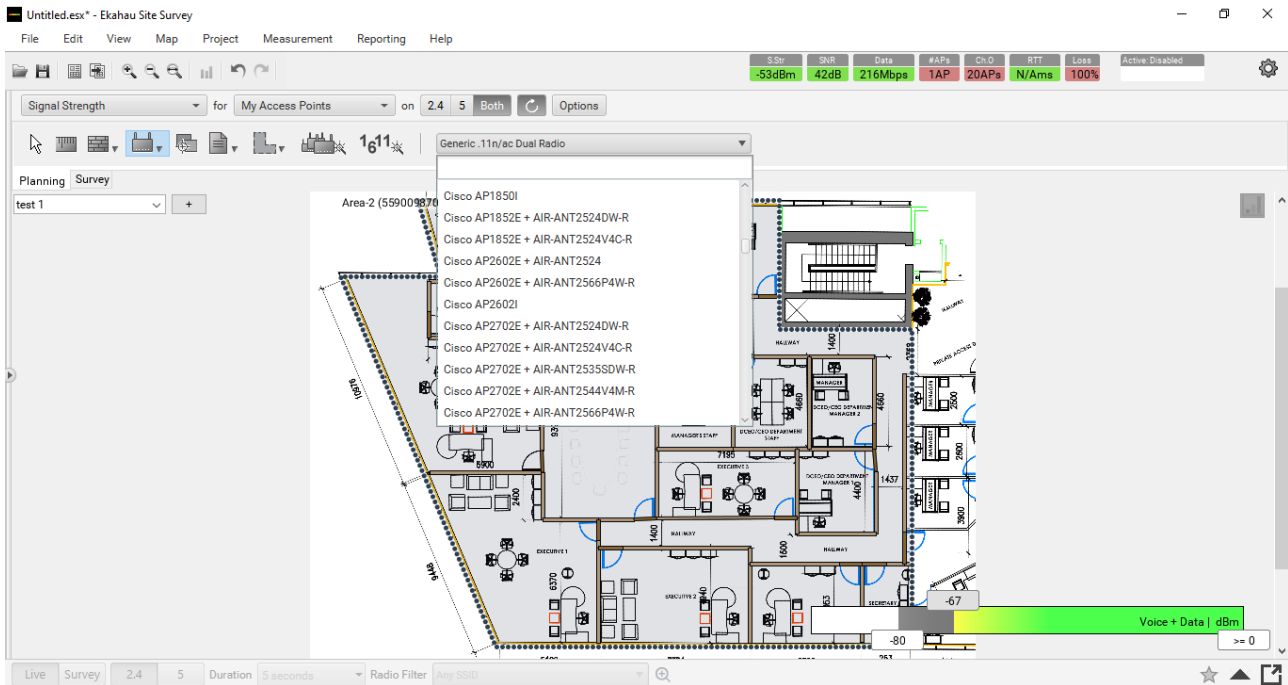
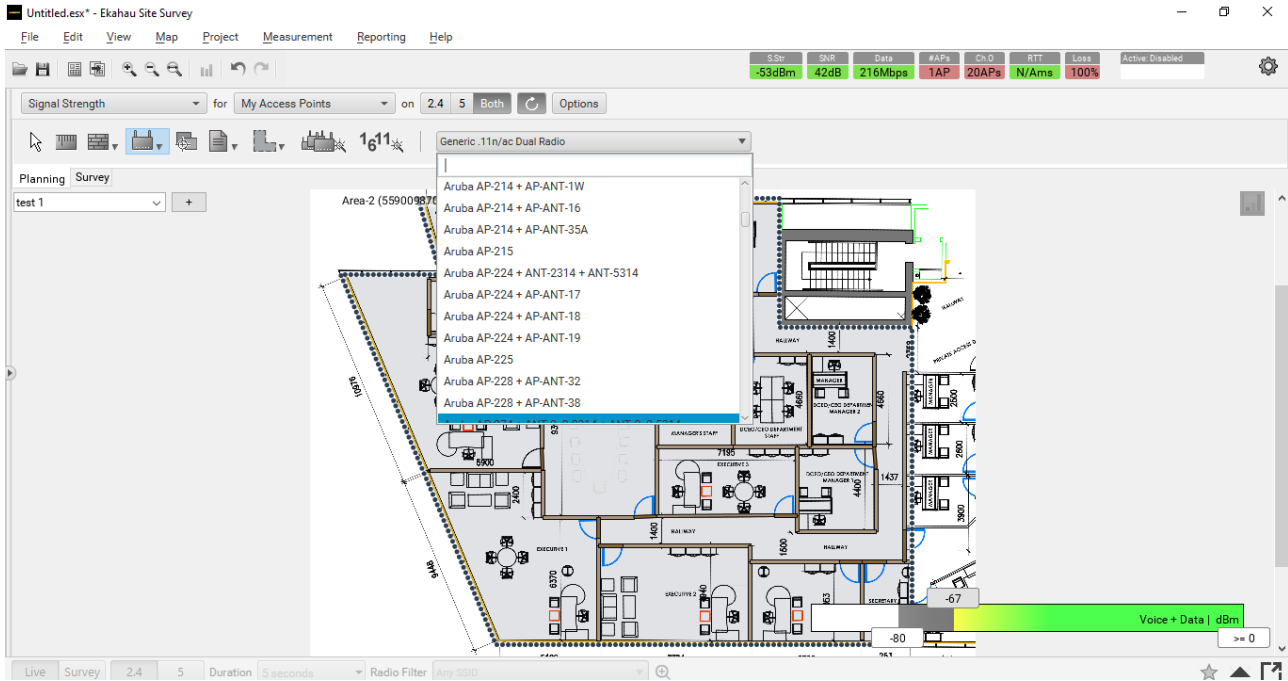
xi. Now, I have rotated the image and drew the walls according to the floor map, and used some assumptions.



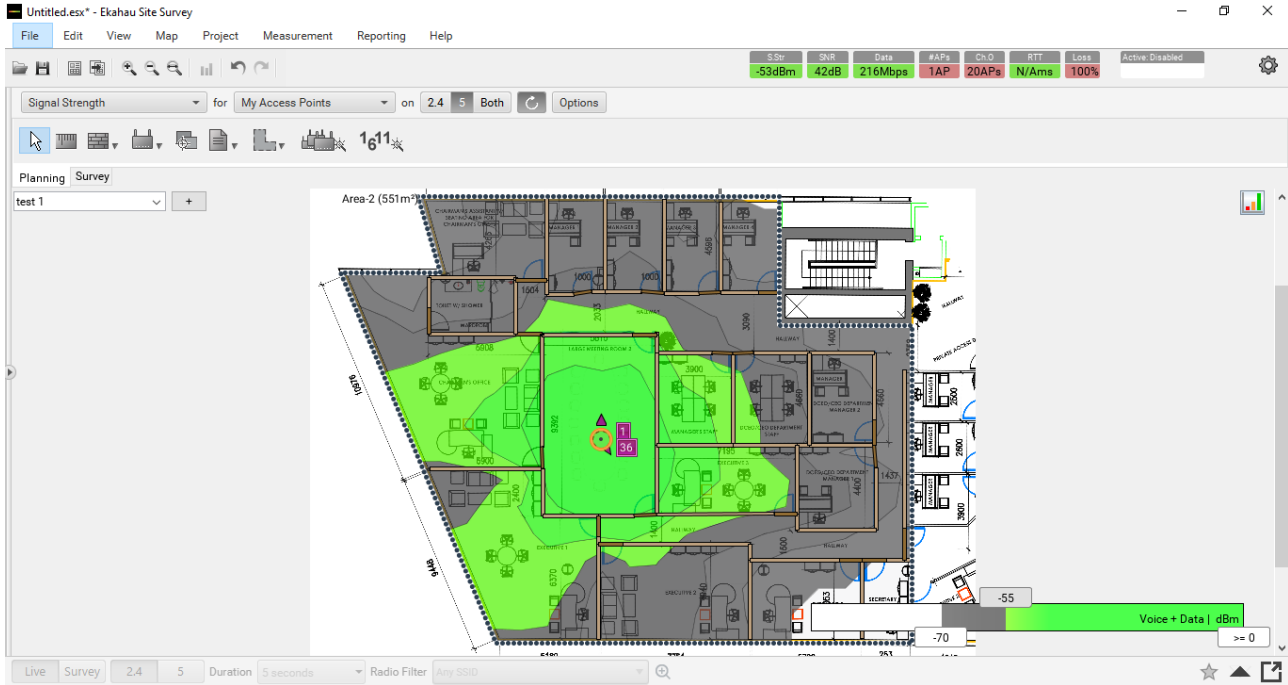
xii. Remaining will be doors and windows



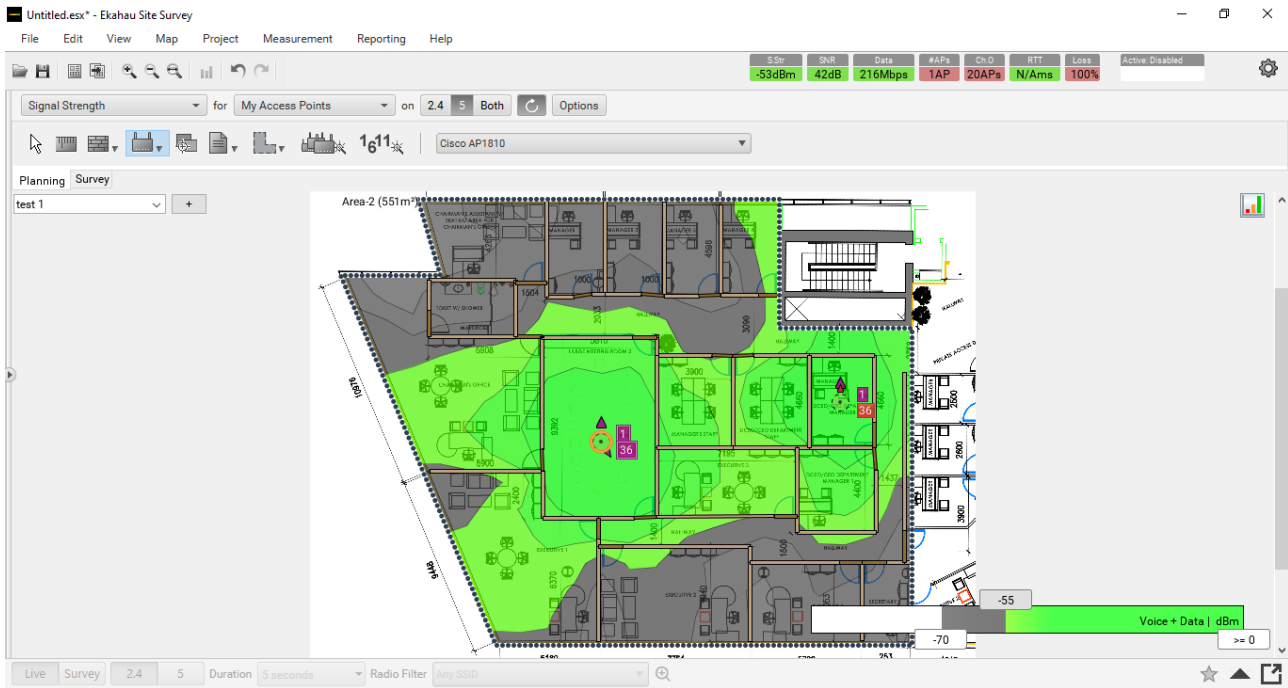
xiii. Now, it's time to place your access points strategically, but before that, you have to decide on the model of the wireless access point. Ekahau has a massive list of the latest and old models of APs.



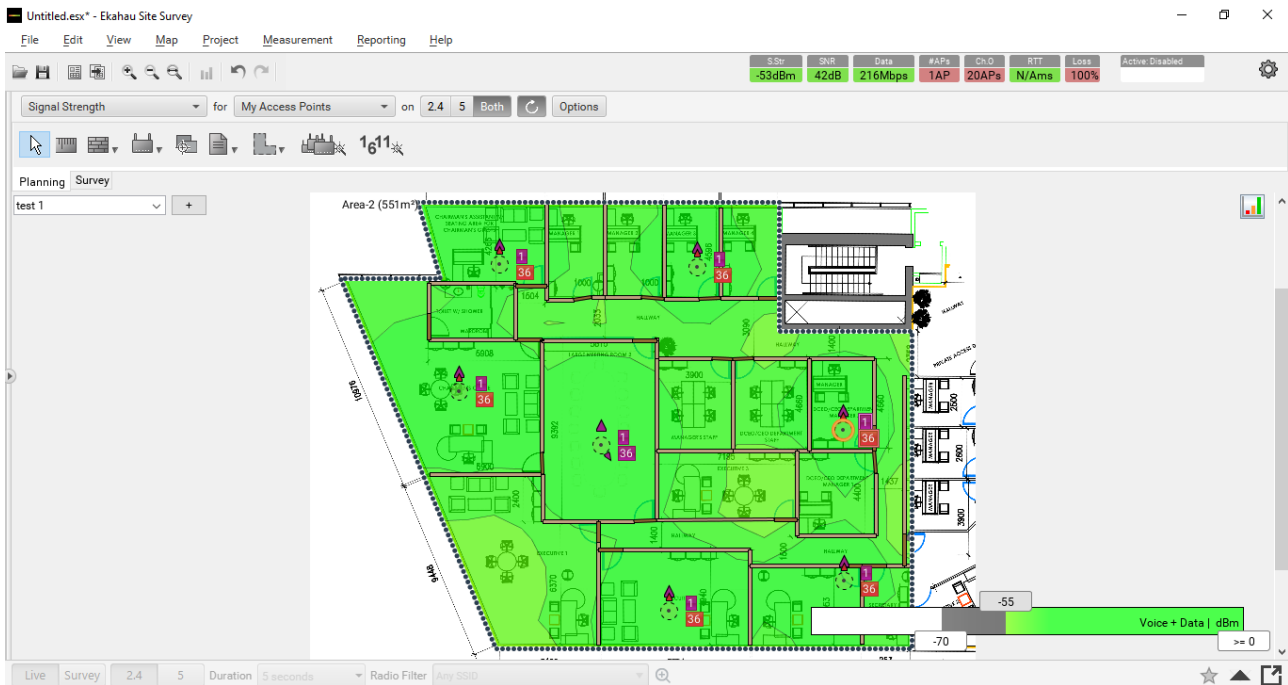
xiv. I have kept the green signal strength until **-55 dBm** and grey strength only beyond **-70 dBm**. I placed one **Cisco 2602i Aironet Access Point** in the middle, and here's what the RF spectrum looks like.



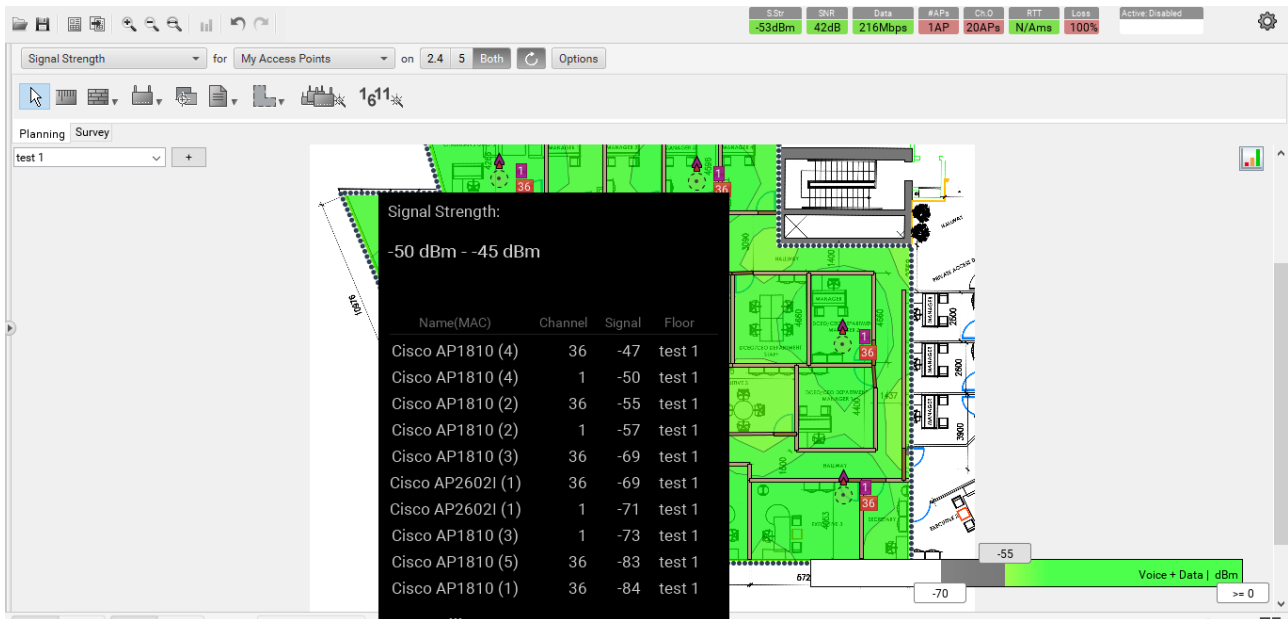
xv. Placed another access point – **Cisco Aironet 1810W** and below is the result-

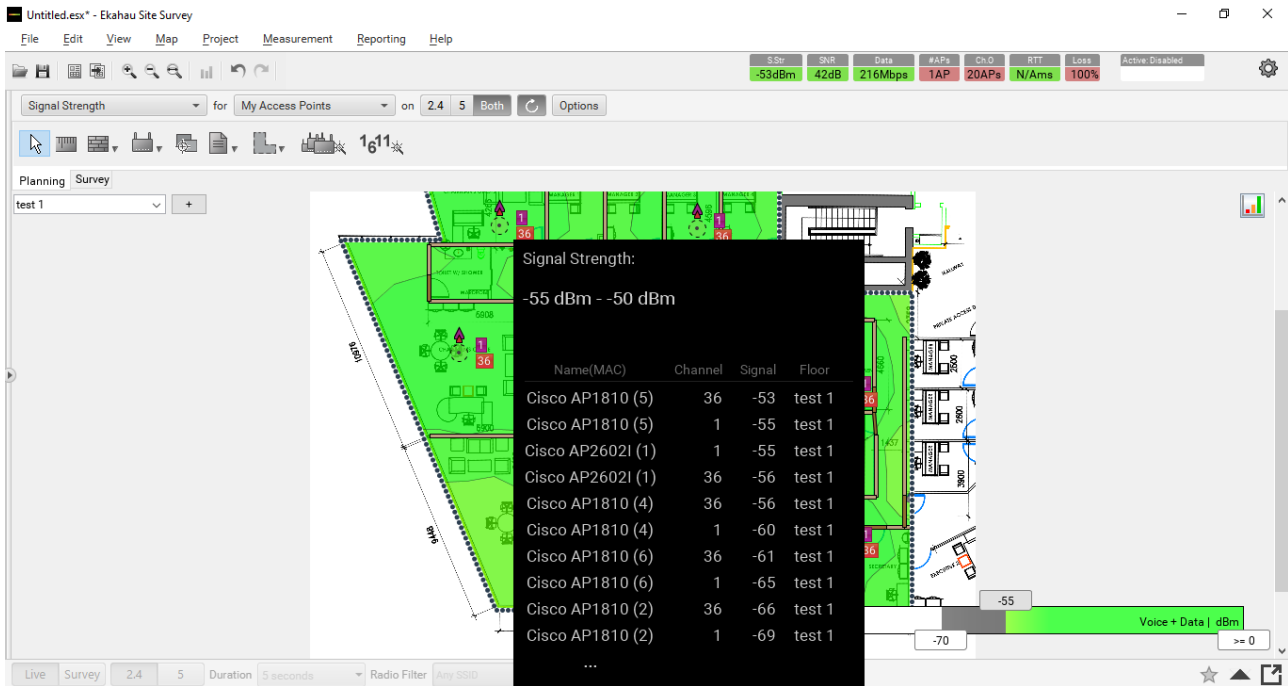
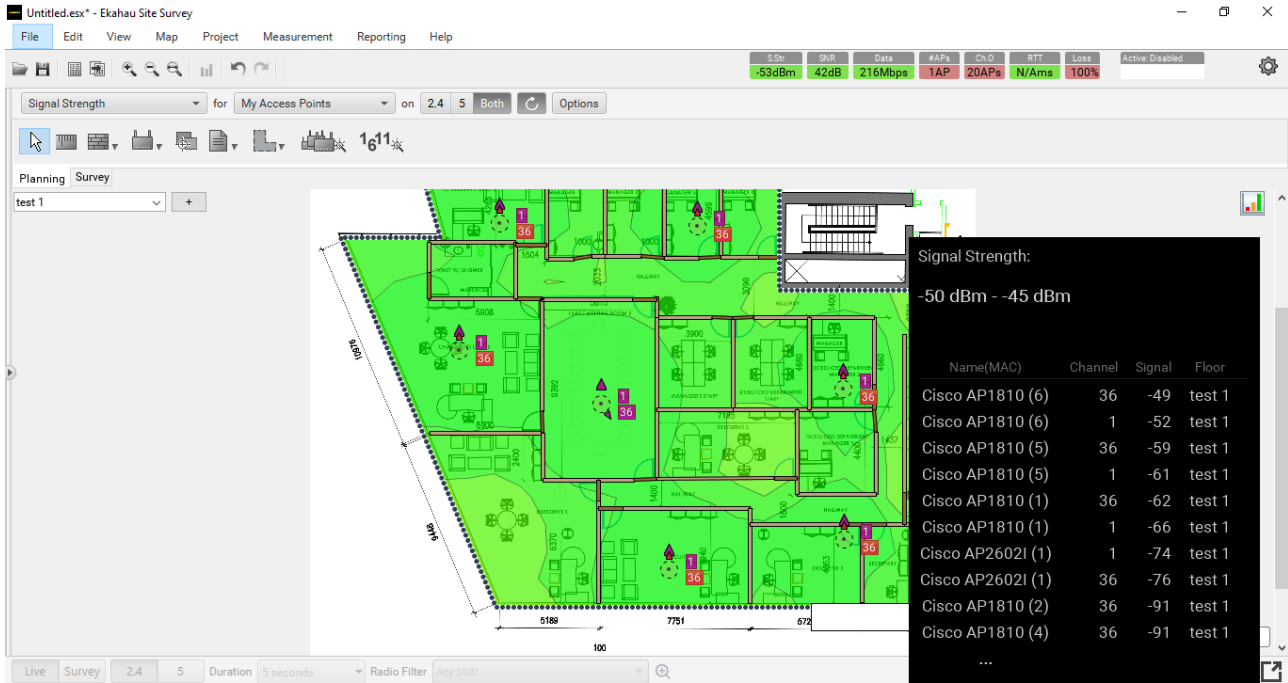


xvi. Strategically placing several access points, we must cover the whole area in green.



Of course, this survey won't give us accurate results when converted in reality, but Ekahau software is 80 to 90 percent accurate, and in some cases, it is better than the prediction. If we right-click on the corner, it will display the information of RF Spectrum.





Regarding the density, let's consider a use case of an auditorium or Amphitheatre or a corporate training room where we have around 400 people.

With a floor area of 6500 square feet (600 square meters) and 400 chairs, the client density in this space is one person per 1.5 square meters. Nevertheless, a single wireless access point will not support 400 customers without lowering the quality of the experience. So, at the very least, you'll need a few extra wireless access points. [36]

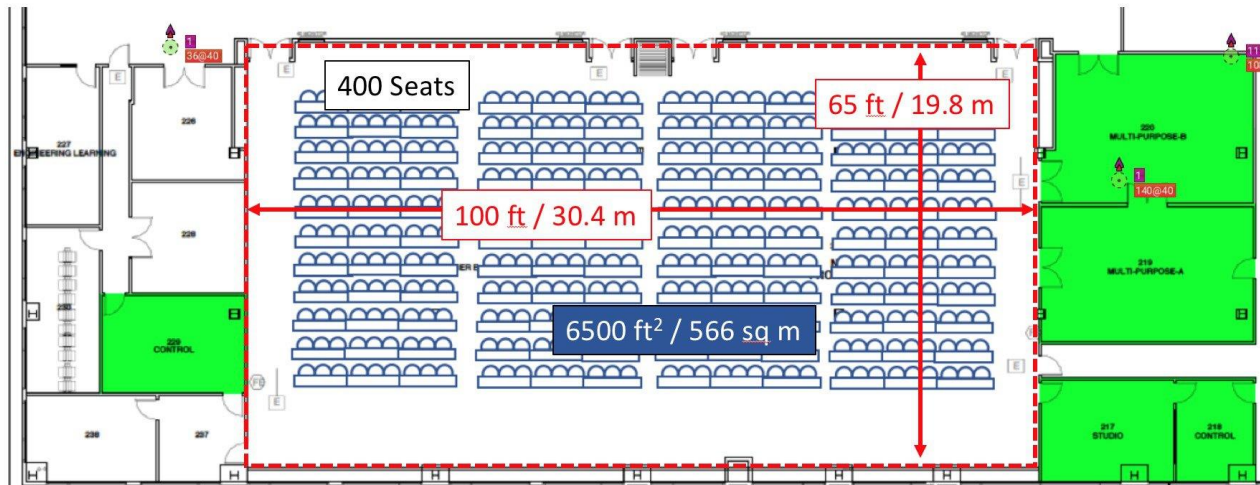


Figure 34 Corporate Training Room [36]

You could also question why we consider one seat as one customer instead of the more common 1.5-3 gadgets per client. An individual person is 1.5 to 3 devices for the sake of generic capacity planning. For the sake of this discussion, we will only discuss active bandwidth and the worst (probable) possible case. If a client has two or more devices (or three or four, as most of us, might), they will only use one of them at a time. The total device population is still essential since it goes straight into the resources category for the core network and other non-airtime/throughput-related items. We're more worried about simultaneous transmissions in the air when it comes to speed reaching the client device. [36]

The max associated clients which Cisco supports on an access point is 200 per interface - 400 per wireless access point; if we try to make it more, the quality of experience won't be good enough. [36]

Another way of addressing the challenge of wireless coverage we will discuss here is the **AP on a Stick survey**.

An AP on a Stick (APoS) survey is a means of mounting an access point at installation height using a tripod or other mounting alternatives to evaluate your predicted designs just before you perform a complete wireless LAN deployment. APoS scans determine the environment's Radio Frequency signals, giving you more confidence that your design concept will perform as expected, eliminating any need for expensive AP placement adjustments, and ensuring we possess the correct quantity of wireless access points in our design. [37]



Figure 35 AP on a Stick survey [37]

With Ekahau software working so accurately, sometimes the question is whether we need anything like the APoS. The answer is it's better to be safe than sorry.

Sometimes there are some things that are not considered during the predictive surveys, such as noise, interference, and thickness of walls, some random objects. These will affect the actual deployment.

The sort of equipment required for an AP on a Stick survey varies depending on the location (for instance, a tripod may well not offer sufficient height for a location like a warehouse with more than 40 feet reaching the ceiling). [37]

1. Wireless access point which you have chosen
2. If you have used any external antennas
3. Tripod or any other mounting system
4. Power source like POE switch
5. Ekahau Site Survey

Some points to consider for APoS-

i. Planning

Planning will be our best friend during the survey; hence we need at least one hour to survey for one access point location. [37]

ii. Two different models of Access Points

Always have two different models of access points at the minimum while doing the survey; this will help to analyze and make a better decision between the two.

iii. Second Pair of Hands

A second person may help you work faster and more efficiently. One individual should set up the next access point, whereas the other evaluates the current access point. [37]

iv. External Battery Pack

You will save a lot of time by powering the access point with additional batteries. To guarantee that the Access point is appropriately energized throughout the survey, ensure the power supply is fully charged. [37]

Every vertical is unique and has its own set of requirements. When conducting an AP on a Stick Survey, here are a few suggested practices for various verticals:

Industrial, Manufacturing, and Warehouse Environments

These locations bring a distinct set of issues. There seem to be safety concerns (machinery and long aisles of shelves), as well as high ceilings and installation choices that could go further than an ordinary tripod APoS. This is vital to just get the access point in the right spot so that radiofrequency will reach the end-user. Furthermore, knowing which product the facility is storing (if appropriate) and the amount or level of products the store is storing may have a significant influence on Radiofrequency absorption and layout. [37]

Enterprise and Office Environments

Because of BYOD needs, privacy, open, collaborative areas, and aesthetic considerations, corporate and workplace settings have increasing challenges. Interferers like cordless webcams, cordless landlines, and other handheld technologies may also create disruption in the wireless LAN. You may use AP on a Stick to find out who could be interfering within the office. [37]

Healthcare

Whenever it comes to life-critical handheld types of equipment, the word "life-critical" takes on a whole new difference. Identifying your infrastructure needs is crucial while developing the wireless LAN since healthcare is a volatile and complex world. Make sure you've arranged with maintenance and personnel for accessibility to the places where you'll be conducting the APoS. [37]

Large Public Venues (LPV)

As we saw earlier, in the case of an auditorium, the large number of clients can be disastrous if we have only one access point. Hence the solution is to deploy multiple access points to increase the quality of experience. But this scenario is when you know there will be so many client or end-user devices. What if you do not know that there will be so many clients. Conducting a survey during a live production environment is apt. This is required to see in-depth analysis. [37]

Government

Old government buildings provide another set of problems. Attempting to develop a "common" wireless LAN for a range of situations is sometimes a difficulty. Furthermore, ancient structures provide special issues. Copper windows refurbished things, and the difficulty in changing the appearance of old structures may all need considerable architectural changes. In certain ancient structures, APoS is used to identify at which location the Access point may be installed. [37]

Education

We need to design for different contexts in Academic settings such as schools and colleges; not only that, we also need to plan for high-density density needs for numerous devices for every pupil. Furthermore, aesthetic considerations are a crucial part of developing educational wireless LAN infrastructure. [37]

AP-on-a-stick surveys help in a lot of ways to expect what will happen in reality. Sometimes we cannot rely on the predictive design model. But in some cases, we will have no other choice, only to rely on a predictive design model in cases like where the building is not yet built.

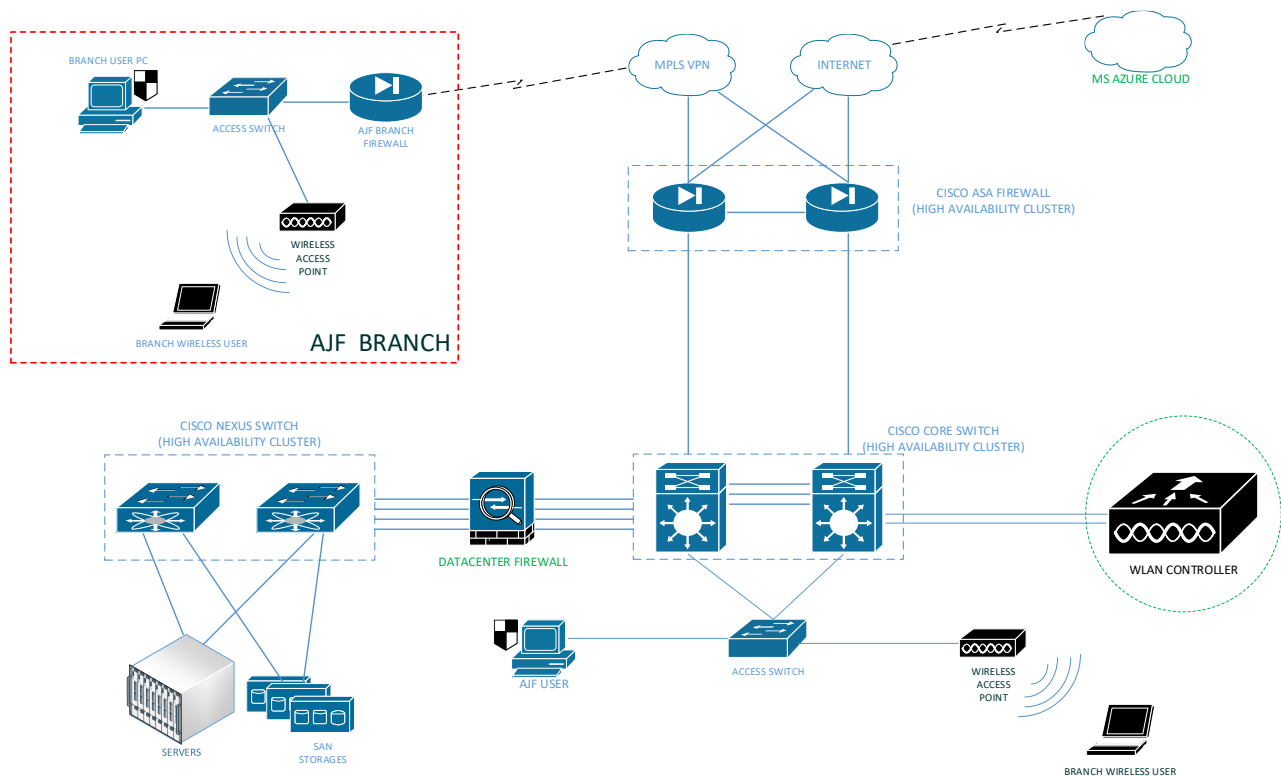
On-Premise Enterprise Wi-Fi Solution

Here in this section, we will discuss the most popular wireless LAN solution used in the campus/enterprise networks. The architecture is based on a master/slave relationship, where the master will be a WLAN controller, and the slave will be the Wireless Access Point.

A WLAN Controller will be a centralized device that will manage all the access points in your campus network infrastructure, either the data plane or control plane, or both, depending upon your setup.

Below is a typical enterprise network consisting of a centralized WLAN controller with several wireless access points placed across different locations.

The model of the WLAN controller used is Cisco WLC 2504, and the wireless access points used are Cisco Aironet 1702 with internal antennas.



Cisco 2504 Wireless LAN Controller



Figure 36 Cisco 2504 WLC [38]

Cisco 2500 Series Wireless Controllers are the first level into the world of Cisco Wireless LAN Controllers, which will offer real-time interactions with Cisco Aironet® wireless access points to ease the setup and management of the Wi-Fi. In medium and small-sized businesses and branch offices, the Cisco® 2500 Series Wireless Controller delivers companywide wireless LAN functionality. It is intended for IEEE 802.11n and 802.11ac standards. [38]

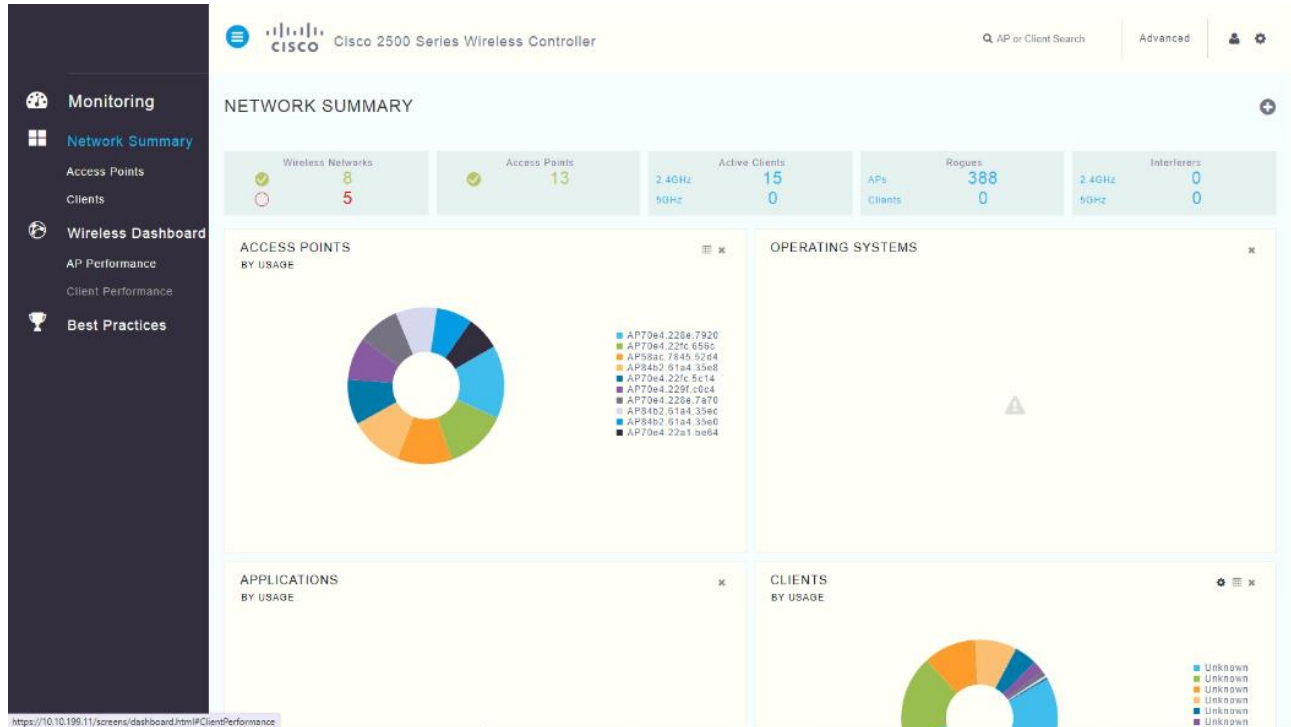
Feature	Benefits
Scalability	<ul style="list-style-type: none"> • Supports up to 75 access points • Supports up to 1000 clients
Ease of Deployment	<ul style="list-style-type: none"> • For quick and easy deployment Access Points can be connected directly to 2504 Wireless LAN Controller via two PoE (Power over Ethernet) ports
High Performance	<ul style="list-style-type: none"> • Wired-network speed and nonblocking performance for 802.11n and 802.11ac networks. Supports up to 1 Gbps throughput
RF Management	<ul style="list-style-type: none"> • Provides both real-time and historical information about RF interference impacting network performance across controllers, via systemwide Cisco CleanAir® technology integration
Comprehensive End-to-End Security	<ul style="list-style-type: none"> • Offers CAPWAP-compliant Datagram Transport Layer Security (DTLS) encryption to help ensure full-line-rate encryption between access points and controllers across remote WAN/LAN links
End-to-end Voice	<ul style="list-style-type: none"> • Supports Unified Communications for improved collaboration through messaging, presence, and conferencing • Supports all Cisco Unified Wireless IP Phones for cost-effective, real-time voice services
High-Performance Video	<ul style="list-style-type: none"> • Integrates Cisco VideoStream technology as part of the Cisco medianet framework to optimize the delivery of video applications across the WLAN
PCI Integration	<ul style="list-style-type: none"> • Part of Payment Card Industry (PCI) certified architecture, and are well-suited for retail customers who deploy transactional data applications such as scanners and kiosks

Figure 37 Cisco 2500 Series Wireless Controller Features and Benefits [38]

2504 WLC, which is part of the Cisco wireless LAN controller suite, provides centralized security policies, wireless intrusion prevention system (WIPS) features, award-winning Radiofrequency

control, and VoIP quality of service (QoS). This WLC offers a low TCO and the potential to extend as the network needs to increase, thanks to its 802.11ac throughput and adaptability. [38]

After successful login into the WLAN controller, we can see the Network Summary with the number of access points, wireless networks, active clients,



With the advanced view, there is detailed information on the same. Also, we can view the frequency band on which the access point is operating.

Controller Summary

Management IP Address	10.10.199.11, ::1/128
Software Version	8.1.102.0
Field Recovery Image Version	7.6.101.1
System Name	HQ-13-WLC-1
Up Time	253 days, 22 hours, 47 minutes
System Time	Wed Feb 16 08:19:52 2022
Redundancy Mode	N/A
Internal Temperature	+31 C
802.11a Network State	Enabled
802.11b/g Network State	Enabled
Local Mobility Group	AJF
CPU(s) Usage	0%
Individual CPU Usage	0%/1%, 0%/1%
Memory Usage	46%
Fan Status	3500 rpm

Access Point Summary

	Total	Up	Down	
802.11a/n/e/r Radios	13	0	13	Detail
802.11b/g/n Radios	13	13	0	Detail
Dual-Band Radios	0	0	0	Detail
All APs	13	13	0	Detail

Client Summary

Current Clients	22	Detail
Excluded Clients	0	Detail
Disabled Clients	0	Detail

Rogue Summary

Active Rogue APs	398	Detail
Active Rogue Clients	0	Detail
Adhoc Rogues	0	Detail
Rogues on Wired Network	0	

Top WLANs

Profile Name	# of Clients	
AJF	22	Detail

Most Recent Traps

- Rogue AP: 5e:a9:50:5a:a0:09 detected on Base Radio MAC: cc:46:d6:08:46:00 Interface no: 0(802.11b/g) Channel: 1 RSSI: -1
- Rogue AP: 5e:a9:50:5a:a0:09 detected on Base Radio MAC: cc:46:d6:08:41:d0 Interface no: 0(802.11b/g) Channel: 1 RSSI: -1
- Rogue AP: 4e:44:6c:24:09:bb removed from Base Radio MAC: cc:46:d6:08:41:d0 Interface no: 0(802.11b/g)
- Rogue AP: 34:79:16:bf:38:9c detected on User Radio MAC: cc:46:d6:08:46:a0 Interface no: 0(802.11n(2.4 GHz)) Channel: 6 F
- Rogue AP: 34:79:16:bf:38:9c detected on User Radio MAC: cc:46:d6:1c:9e:b0 Interface no: 0(802.11n(2.4 GHz)) Channel: 6 F

In the basic view, we can view the list of access points currently associated with the WLAN controller, along with their uptime.

ACCESS POINTS

AP Name	Clients	Usage	Uptime	Chan...	Channels	Cover...	Interfe...	Rogues	MAC Address	IP Address
AP84b2.61e4.34d0	1	589 GB	1980 Days 13 Ho...	80	1	5	52	07	84:b2:61:e4:34:d0	1451.ad9c::11e5.d8...
AP70e4.22a1.be64	1	589 GB	342 Days 1 Hour	59	11	0	53	80	70:e4:22:a1:be:64	1451.ad9c::11e5.d8...
AP84b2.61e4.35e0	1	813 GB	1979 Days 23 Ho...	79	6	0	65	44	84:b2:61:e4:35:e0	1451.ad9c::11e5.d8...
AP58ac.7845.52d4	2	924 GB	1980 Days 8 Hours	70	11	3	65	12	58:ac:78:45:52:d4	1451.ad9c::11e5.d8...
AP70e4.22fc.5cb0	0	183 GB	342 Days 37 Min...	88	1	0	83	17	70:e4:22:fc:5c:b0	1451.ad9c::11e5.d8...
AP70e4.228e.7a70	0	715 GB	1980 Days 7 Hours	81	11	0	75	86	70:e4:22:8e:7a:70	1451.ad9c::11e5.d8...
AP84b2.61e4.35ec	2	790 GB	1980 Days 6 Hours	58	6	1	51	82	84:b2:61:e4:35:ec	1451.ad9c::11e5.d8...
AP70e4.229f.c30c	0	582 GB	1980 Days 7 Hours	88	11	0	62	81	70:e4:22:9f:c3:0c	1451.ad9c::11e5.d8...
AP84b2.61e4.35e8	1	904 GB	1980 Days 14 Ho...	70	1	5	64	84	84:b2:61:e4:35:e8	1451.ad9c::11e5.d8...
AP70e4.22fc.5c14	2	766 GB	342 Days 1 Hour	46	6	44	39	22	70:e4:22:fc:5c:14	1451.ad9c::11e5.d8...
AP70e4.229f.c0c4	1	715 GB	1980 Days 16 Ho...	74	11	0	79	68	70:e4:22:9f:c0:c4	1451.ad9c::11e5.d8...
AP70e4.228e.7920	2	1 TB	1980 Days 19 Ho...	73	6	93	69	80	70:e4:22:8e:79:20	1451.ad9c::11e5.d8...
AP70e4.22fc.655c	3	1 TB	171 Days 16 Hours	87	6	0	81	11	70:e4:22:fc:65:5c	1451.ad9c::11e5.d8...

Stability is one of the most priced features of any network device; as you can see, there are many access points with an uptime of almost 2000 days.

Cisco Aironet 1702 Lightweight Access Point



Figure 38 Cisco Aironet 1700 Series Access Point [39]

The Cisco Aironet 1700 Series Access Points are equipped with the modern IEEE 802.11ac standard. The Aironet 1700 Series Access Point is created to accommodate the rising demands of today's modern medium and small-sized wireless LAN business infrastructure. It provides the proper affordability to enable companies to transition to 802.11ac communication. [39]

In the detailed advanced view, the AP model is shown as well.

AP Name	IP Address (IPv4/IPv6)	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status	PoE Status
AFS4b2.61a4.3d88	10.10.199.89	AIR-CAP17021-E-K9	84:b2:61:a4:3d:b8	1980 d, 13 h 25 m 09 s	Enabled	REG	PoE/Full Power
AFZ0e4.2281.be64	10.10.199.00	AIR-CAP17021-E-K9	70:e4:22:a1:be:64	342 d, 01 h 05 m 27 s	Enabled	REG	PoE/Full Power
AFS4b2.61a4.35e0	10.10.199.01	AIR-CAP17021-E-K9	84:b2:61:a4:35:e0	1979 d, 23 h 10 m 48 s	Enabled	REG	PoE/Full Power
AFS8ac.7845.5284	10.10.199.92	AIR-CAP17021-E-K9	58:ac:78:45:52:84	1980 d, 09 h 00 m 37 s	Enabled	REG	PoE/Full Power
AFZ0e4.228f.5cb0	10.10.199.93	AIR-CAP17021-E-K9	70:e4:22:8f:5c:b0	342 d, 00 h 41 m 04 s	Enabled	REG	PoE/Full Power
AFZ0e4.228e.7a70	10.10.199.94	AIR-CAP17021-E-K9	70:e4:22:8e:7a:70	1980 d, 07 h 06 m 51 s	Enabled	REG	PoE/Full Power
AFS4b2.61a4.35ec	10.10.199.95	AIR-CAP17021-E-K9	84:b2:61:a4:35:ec	1980 d, 06 h 18 m 29 s	Enabled	REG	PoE/Full Power
AFZ0e4.228f.c30c	10.10.199.99	AIR-CAP17021-E-K9	70:e4:22:8f:c3:0c	1980 d, 07 h 57 m 39 s	Enabled	REG	PoE/Full Power
AFS4b2.61a4.35e8	10.10.199.111	AIR-CAP17021-E-K9	84:b2:61:a4:35:e8	1980 d, 14 h 10 m 52 s	Enabled	REG	PoE/Full Power
AFZ0e4.228f.5c14	10.10.199.112	AIR-CAP17021-E-K9	70:e4:22:8f:5c:14	342 d, 01 h 13 m 17 s	Enabled	REG	PoE/Full Power
AFZ0e4.228f.c0c4	10.10.199.07	AIR-CAP17021-E-K9	70:e4:22:8f:c0:c4	1980 d, 16 h 06 m 11 s	Enabled	REG	PoE/Full Power
AFZ0e4.228e.7920	10.10.199.96	AIR-CAP17021-E-K9	70:e4:22:8e:79:20	1980 d, 19 h 08 m 40 s	Enabled	REG	PoE/Full Power
AFZ0e4.228f.630c	10.10.199.99	AIR-CAP17021-E-K9	70:e4:22:8f:63:0c	171 d, 16 h 17 m 00 s	Enabled	REG	PoE/Full Power

Upon checking the WLAN section, we can see the complete list of WLAN networks configured along with their security policy.

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	AJF	AJF	Enabled	[WPA2][Auth(PSK)]
2	WLAN	Data Network	Aljazera	Enabled	[WPA2][Auth(PSK)]
3	WLAN	Mgmt	Mgmt	Disabled	[WPA2][Auth(PSK)]
4	WLAN	Q-MATC	Q-MATC	Enabled	[WPA + WPA2][Auth(PSK)]
5	WLAN	ISE-Test	ISE-Test	Disabled	[WPA][Auth(802.1X)]
6	WLAN	Guest-test	ISE-Guest	Disabled	MAC Filtering
7	WLAN	Collection	Collection	Enabled	[WPA2][Auth(PSK)]
8	WLAN	CCTV	CCTV	Enabled	[WPA2][Auth(PSK)]
9	WLAN	Phones	AVIVA	Enabled	[WPA2][Auth(PSK)]
10	WLAN	AJFQ	AJFQ	Disabled	[WPA + WPA2][Auth(PSK)]
11	WLAN	C-Level	C	Enabled	[WPA2][Auth(PSK)]
12	WLAN	Test	Test	Disabled	None
13	WLAN	Sales	Sales	Enabled	[WPA2][Auth(PSK)]

Wireless Entries 1 - 13 of 13

AP Model	Power Status	No of Clients	Port	AP Mode	Certificate Type	OCAP	Primary SW version	Backup SW version	AP Sub Mode	Download Status	Upgrade Role (Master/Slave)	mDNS Status
Advanced	PoE/Full Power	0	LAG	Local	MDC	No	8.1.102.0	0.0.0.0	None	None		Disabled
Mesh	PoE/Full Power	1	LAG	Local	MDC	No	8.1.102.0	0.0.0.0	None	None		Disabled
RF Profiles	PoE/Full Power	0	LAG	Local	MDC	No	8.1.102.0	0.0.0.0	None	None		Disabled
FlexConnect Groups	PoE/Full Power	0	LAG	Local	MDC	No	8.1.102.0	0.0.0.0	None	None		Disabled
FlexConnect ACLs	PoE/Full Power	0	LAG	Local	MDC	No	8.1.102.0	0.0.0.0	None	None		Disabled
FlexConnect VLANs	PoE/Full Power	0	LAG	Local	MDC	No	8.1.102.0	0.0.0.0	None	None		Disabled
Templates	PoE/Full Power	0	LAG	Local	MDC	No	8.1.102.0	0.0.0.0	None	None		Disabled
OEAP ACLs	PoE/Full Power	0	LAG	Local	MDC	No	8.1.102.0	0.0.0.0	None	None		Disabled
Network Lists	PoE/Full Power	0	LAG	Local	MDC	No	8.1.102.0	0.0.0.0	None	None		Disabled
802.11a/n/ac	PoE/Full Power	0	LAG	Local	MDC	No	8.1.102.0	0.0.0.0	None	None		Disabled
802.11b/g/n	PoE/Full Power	0	LAG	Local	MDC	No	8.1.102.0	0.0.0.0	None	None		Disabled
Media Stream	PoE/Full Power	0	LAG	Local	MDC	No	8.1.102.0	0.0.0.0	None	None		Disabled
Application Visibility And Control	PoE/Full Power	0	LAG	Local	MDC	No	8.1.102.0	0.0.0.0	None	None		Disabled

Wireless All APs > Details for AP70e4.22a1.be64

General Credentials Interfaces High Availability Inventory Advanced

General	Versions
AP Name: AP70e4.22a1.be64	Primary Software Version: 8.1.102.0
Location: default location	Backup Software Version: 0.0.0.0
AP MAC Address: 70:e4:22:a1:be:64	Predownload Status: None
Base Radio MAC: cc:46:d6:3d:0a:e0	Predownloaded Version: None
Admin Status: Enable	Predownloaded Next Retry Time: NA
AP Mode: local	Predownloaded Retry Count: NA
AP Sub Mode: FlexConnect	Boot Version: 15.3.0.0
Operational Status: monitor	IOS Version: 15.3(3)188E
Rogue Detector: Spiller	Mini IOS Version: 8.0.115.0
Port Number: Bridge	IP Config
Venue Group: Flex+Bridge	CAPWAP Preferred Mode: Ipv4 (Global Config)
Venue Type: Unspecified	DHCP Ipv4 Address: 10.10.199.50
Venue Name:	Static IP (Ipv4/Ipv6): <input type="checkbox"/>
Language:	Time Statistics
Network Interface Key: BBD615A70A163D333C883F1CF1A1B513	UP Time: 342 d, 20 h 41 m 17 s
GPS Location:	Controller Associated Time: 254 d, 18 h 22 m 36 s
GPS Present: No	Controller Association Latency: 0 d, 00 h 03 m 09 s

Hardware Reset: Perform a hardware reset on this AP. **Reset AP Now**

Set to Factory Defaults: Clear configuration on this AP and reset it to factory defaults. **Clear All Config**, **Clear Config Except Static IP**

Foot Notes:
 1(a) DNS server IP Address and the Domain name can be set only after a valid static IP is pushed to the AP.
 1(b) Whenever Static IP version gets changed i.e. Ipv4 to Ipv6 or Ipv6 to Ipv4, the DNS server IP Address and the Domain name displayed in configuration page are not valid. Needs to re-configure DNS IP and Domain name after newly assigned static IP pushed to AP.
 1(c) Whenever Static IP version gets changed i.e. Ipv4 to Ipv6 or Ipv6 to Ipv4, the values given for DNS server IP and Domain name won't be set. Needs to configure DNS IP and Domain name after newly assigned static IP pushed to AP.

There are different modes in which the access point operates. We will discuss one by one those-

i. **Local** – This is the default mode for all the wireless access points connected to the WLAN controller. Here the access point creates a CAPWAP tunnel between itself and the WLAN controller. All the traffic goes to the WLC, and from there, it will go to the router.

ii. **FlexConnect** - A wireless Access Point located in a distant site or remote location can be connected to the headquarters' WLC. Functional, but this is not it is not a good concept. The access points wrap all the wireless data in an encrypted tunnel across the WAN channel via the CAPWAP. Secondly, if the WAN connection fails, your remote site's Wi-Fi will also be unavailable. Here comes Flexconnect mode to the rescue that may be used in scenarios like mentioned. Whenever the CAPWAP tunnel to the WLC fails, the AP will locally switch traffic between VLANs and SSIDs. [40]

iii. **Monitor** – In this mode, the access point will simply monitor for IDS events or check for any rogue access points in the surrounding. It also has the ability to detect the exact location of an end-user station.

The only thing which we need to remember is that in this mode, the access point will not broadcast any SSID; hence no one will be able to connect to the access point running in this mode. [40]

iv. **Sniffer** – Imagine you are an IT administrator of an enterprise, and users are complaining about a wireless LAN network issue. This mode will come to your rescue, wherein it will sniff all the packets wirelessly. We can use an application like Wireshark and troubleshoot the problem. A broadcast of SSID will not take place. [40]

v. **Rogue Detector** – In this mode, the access point will only work and detect any rogue access points in the area nearby. How will it know that this is a rogue device? The way is that it will scan nearby SSID and any MAC address it sees in the medium. Whereas it can only switch to entertaining end users if the administrator does it. [40]

vi. **Bridge/Mesh** - The access point transforms into a specialized point-to-point or point-to-multipoint bridge. In this mode, two or more access points may link located at two distant locations but within the range. Multiple access points may also be used to create an indoor or outdoor mesh. Users are unable to access the access points working in this mode.

The only drawback with the on-premise Wi-Fi solution we have is the cost to purchase and maintain the hardware initially, and there is no flexibility in scalability to accommodate future expansion and technology innovation.

Public Cloud Based Enterprise Wi-Fi Solution

Today Cloud computing has become the latest trend in the IT industry, but here we will try to understand whether it is really worth it or it's just that everyone is moving to the Cloud; we must also go?

The flexibility, scalability, and quick offering by Cloud service providers cannot match with the traditional on-premise solutions.

Let us discuss the public Cloud service models. According to the National Institute of Standards and Technology (NIST) Special Publication 800-145; we have three different types of service models [41]

- i. Infrastructure as a Service (IaaS)
- ii. Platform as a Service (PaaS)
- iii. Software as a Service (SaaS)

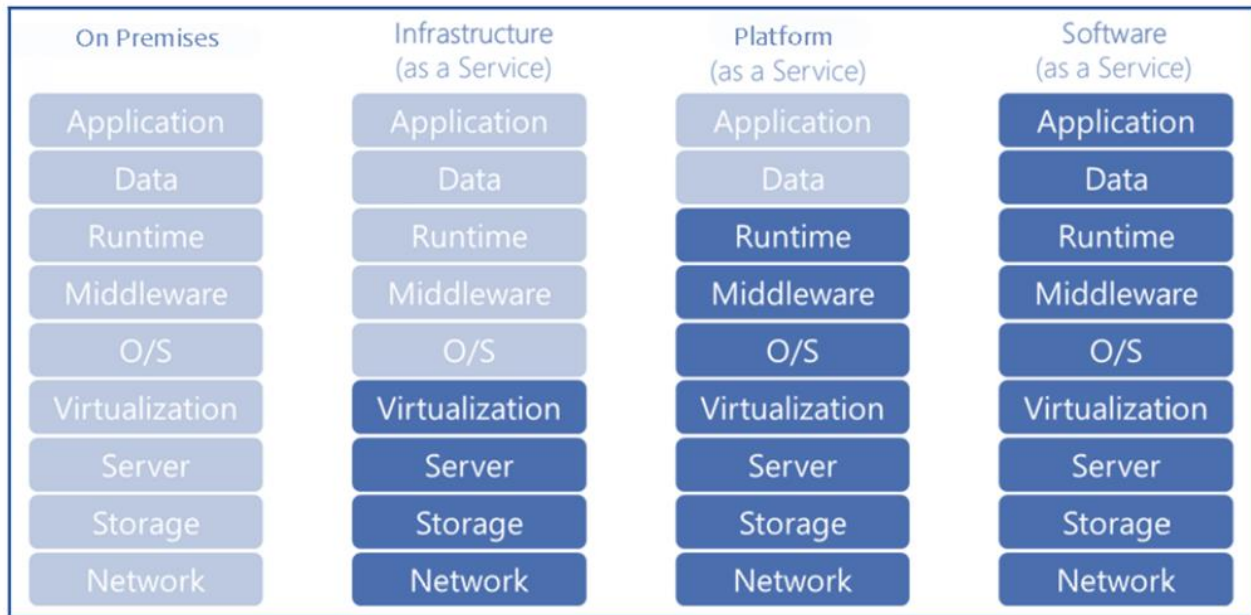


Figure 39 On-Premises versus Public Cloud service models [42]

The first and easiest one to deploy and administer is the SaaS model. Software as a service model is when you are just going to use the service from a client’s point of view. A famous example is using Microsoft Office 365 emails services. You can access the admin portal or the APIs. But do not have access to the underlying hardware. Cisco Meraki leverages this type of Cloud.

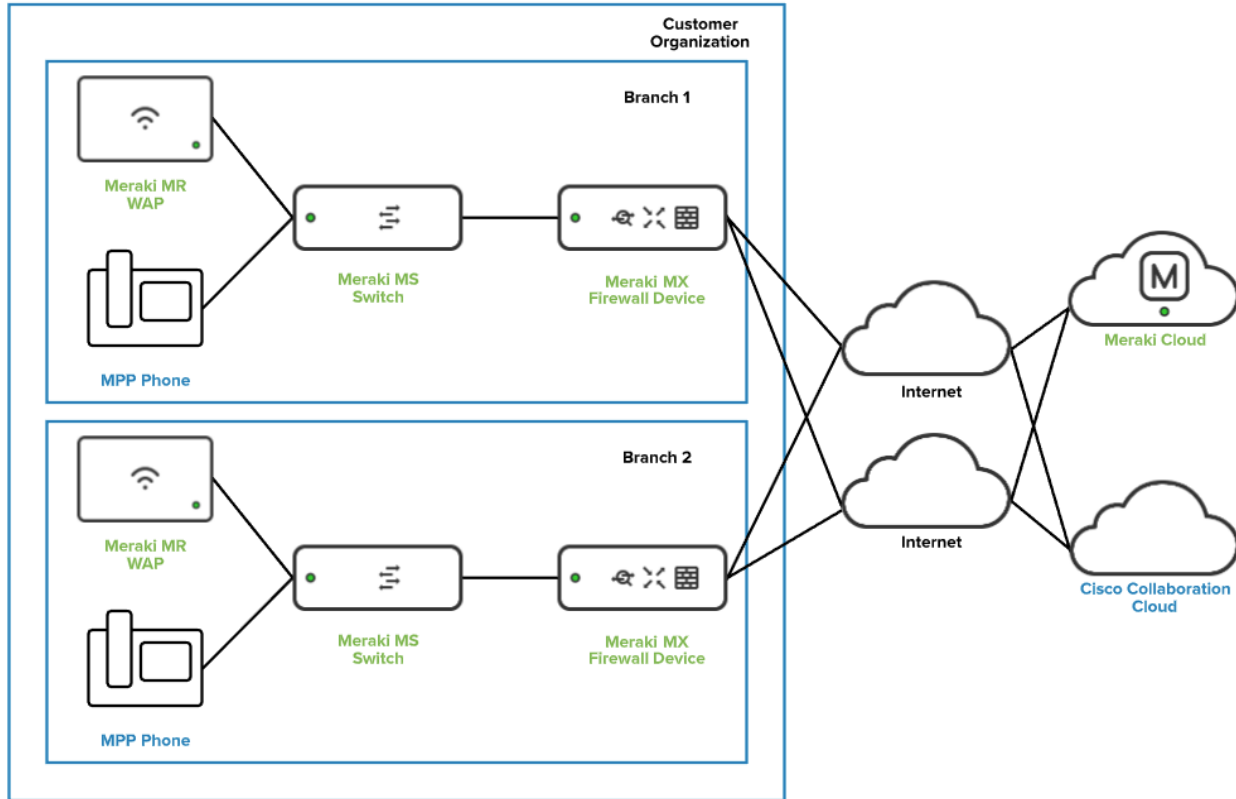


Figure 40 Basic Cisco Meraki Topology [43]

The next model we will cover is the PaaS model of the Cloud. Here, Cloud providers such as Amazon or Microsoft will be responsible for managing the hardware, network, security, and middleware. The client just needs to deploy their application and bring the data that is required to run the application, and we are good to go. Websites usually use this model. [44]

Lastly, we will discuss the IaaS model, which is personally one of my favorite models due to the benefits it offers. Apart from the hardware and hypervisor, everything is managed by the client, which gives us control over everything.

The client will have the highest level of control over any Cloud model. This model is the best one and chosen for our **Catalyst 9800 Wireless Controller** deployment on AWS Cloud. [44]

The public Cloud model for our Cloud wireless solution is the Infrastructure as a Service (IaaS). The customer will depend on the public cloud service provider for computing, networking, and security. But the ability to manage all those things will stay in the hands of the customer.

Below we will discuss the various advantages of public Cloud and deploying C9800-CL WLAN controller on the Cloud [44]:

Agility: It just takes a couple of minutes to launch a C9800 server on AWS Cloud, making it very simple to deploy a wireless LAN controller to try out a new functionality or capability and then kill it. [44]

Scalability: This is the most significant advantage the public Cloud provides; when there will be an expansion to the enterprise, the public Cloud can quickly accommodate that within seconds.

Global footprint: This is significant not just in terms of response time but also in terms of privacy and security rules. Because major Cloud providers have a worldwide presence, you can access a C9800-CL in the Cloud in less than 50 milliseconds from any area where you deploy Access points. Some clients have tight policies that require customer data and traffic to remain inside the area; popular Cloud providers offer Data Centers in every continent. [44]

Cost-effectiveness: You cannot imagine the amount an enterprise spends on a CAPEX model and then on OPEX expenses such as power, cooling, backups, disaster recovery sites, and so on. With the Cloud model, we will be shifting to an OPEX model, which is the pay-as-you-go model. [44]

With these features in mind, we will implement the Wi-Fi solution on the public Cloud. Below is the typical wireless LAN solution with the WLAN controller on the public cloud service provider such as Amazon Web services – AWS.

The access points will connect to the WLC through the secure IPSec VPN using the Internet.

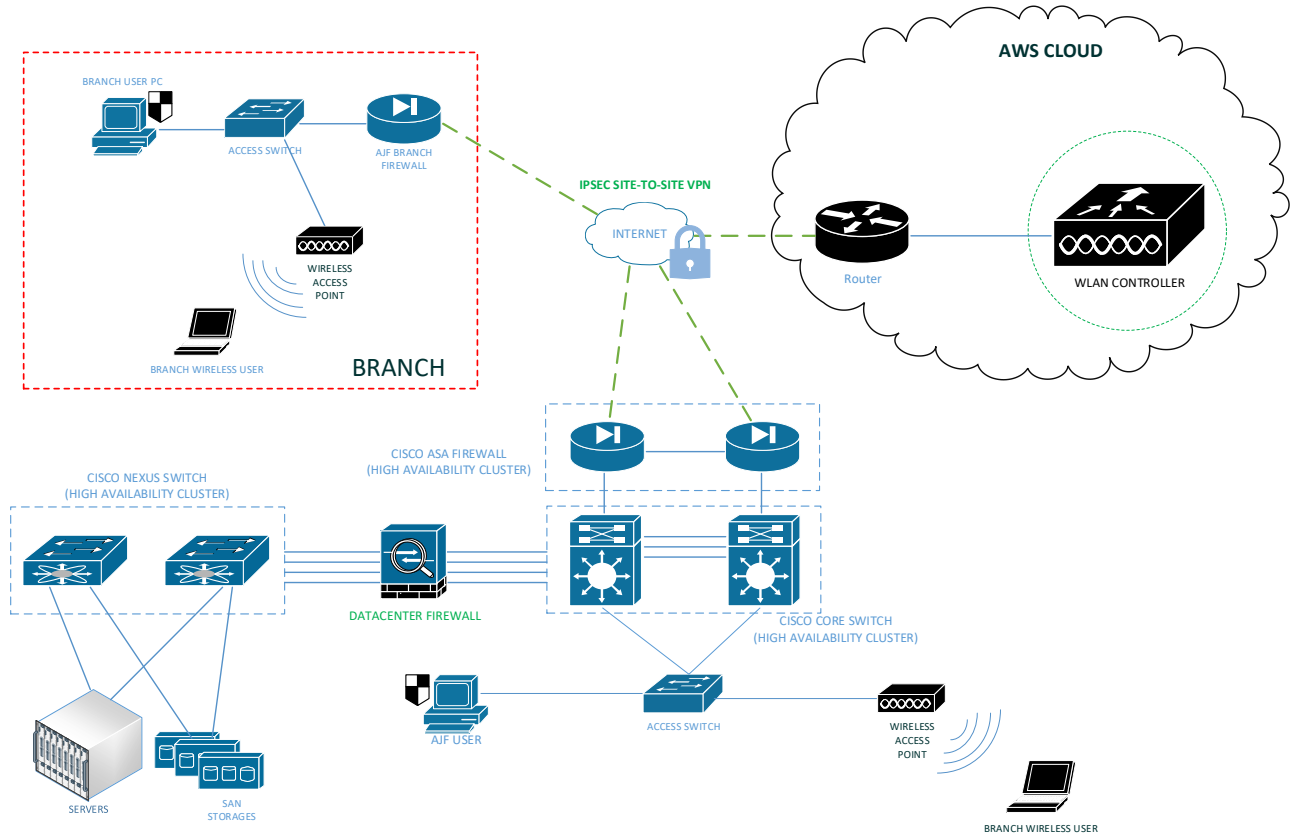
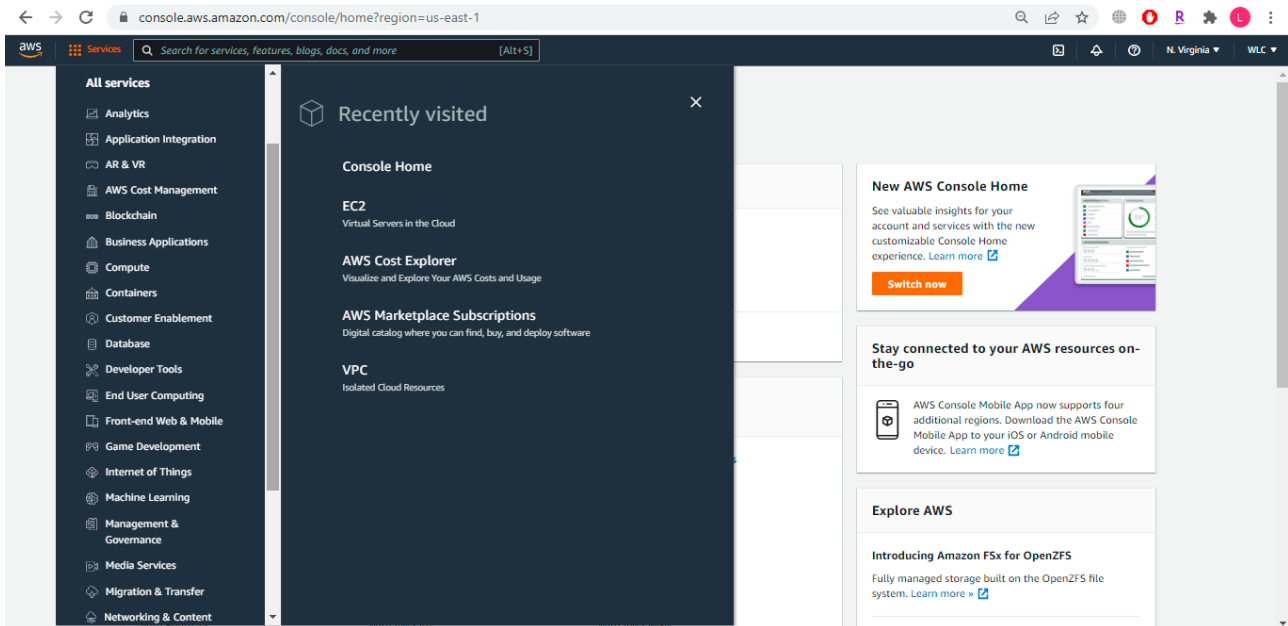
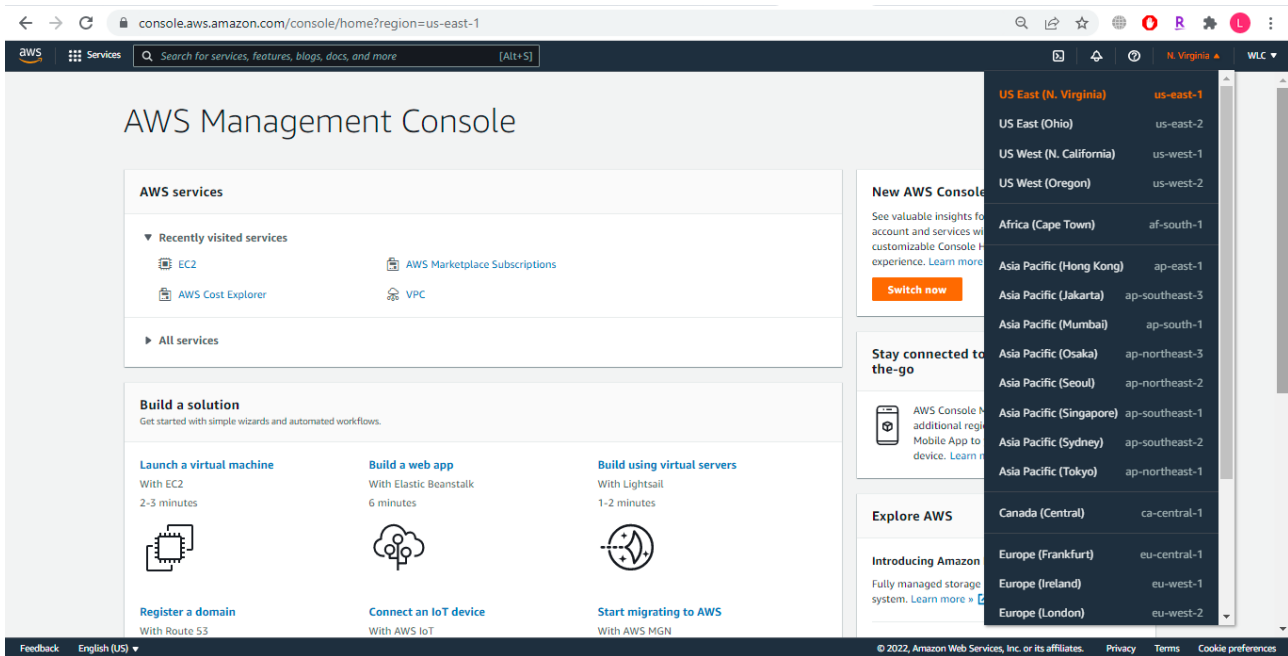


Figure 41 Typical Cloud Wireless solution

In our implementation, we will use the Amazon Web services – AWS public Cloud service. But before we implement the wireless solution, let us understand the AWS infrastructure.

Upon logging into the AWS console – <https://console.aws.amazon.com/>

We are presented with the AWS Management Console; on the right side, we can find the various data centers of Amazon, which we can choose from. The Datacenter which I have chosen is the **US East – North Virginia**.



As you can see in the above picture, AWS offers a huge number of services. But the services which are relevant to us are the VPC for private Cloud resources such as networking and EC2 for computing resources such as Virtual Machines - VM.

First of all, we will configure the VPC and its associated elements such as CIDR, VLANs, default gateway, security access policies, and so on. [45]

Once the VPC is created on AWS, we need to establish a connection between the VPC and the customer's on-premises infrastructure. There are two ways to do that.

- i. Site-to-Site IPsec VPN
- ii. Routing using the public IP address to reach the WLAN controller on Cloud

Connecting the access points using the public IP address is not supported. It is good because of security reasons; you will never want direct access to the public IP address of the wireless LAN controller. But the client can use this public IP address for management purposes, which makes it easy for the remote IT admin to manage and troubleshoot if required. [44]

Hence, the only deployment model that remains to our use is the Site-to-Site VPN through the Internet.

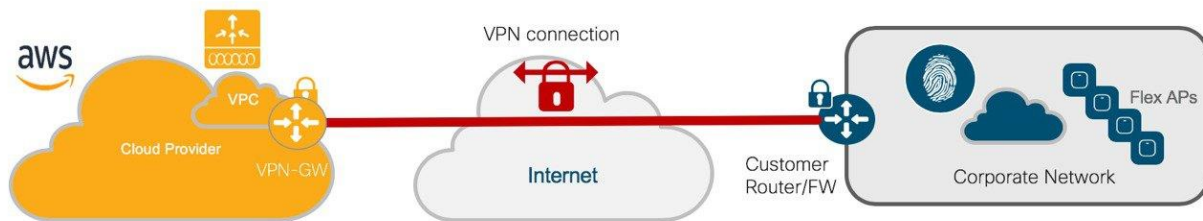


Figure 42 VPN between AWS and Corporate Network [44]

The VPN tunnel will be configured between the on-premises corporate network and the VPC in the AWS Cloud. This connection is secured using encryption, i.e., IPsec encryption.

By default, there is a VPN connectivity option provided by the AWS Cloud itself, but it, of course, has some limitations, like a maximum of 10 VPN connections. We can use the Cisco CSRv Router on the Cloud, which supports more VPN connections and technologies like DMVPN, FlexVPN, or EZVPN.

When the tunnel is UP and running, we need to ensure proper routing is in place for the access points on the corporate network to reach the private IP address of the C9800-CL instance. [44]

Here is a simple example:

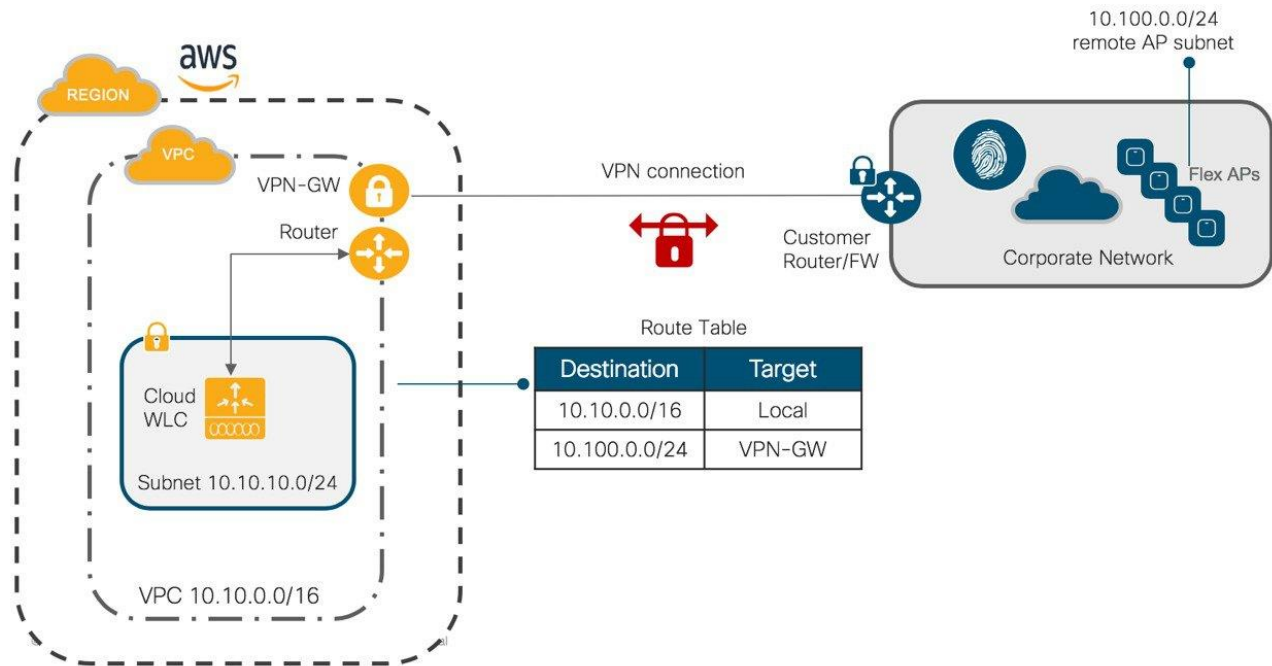
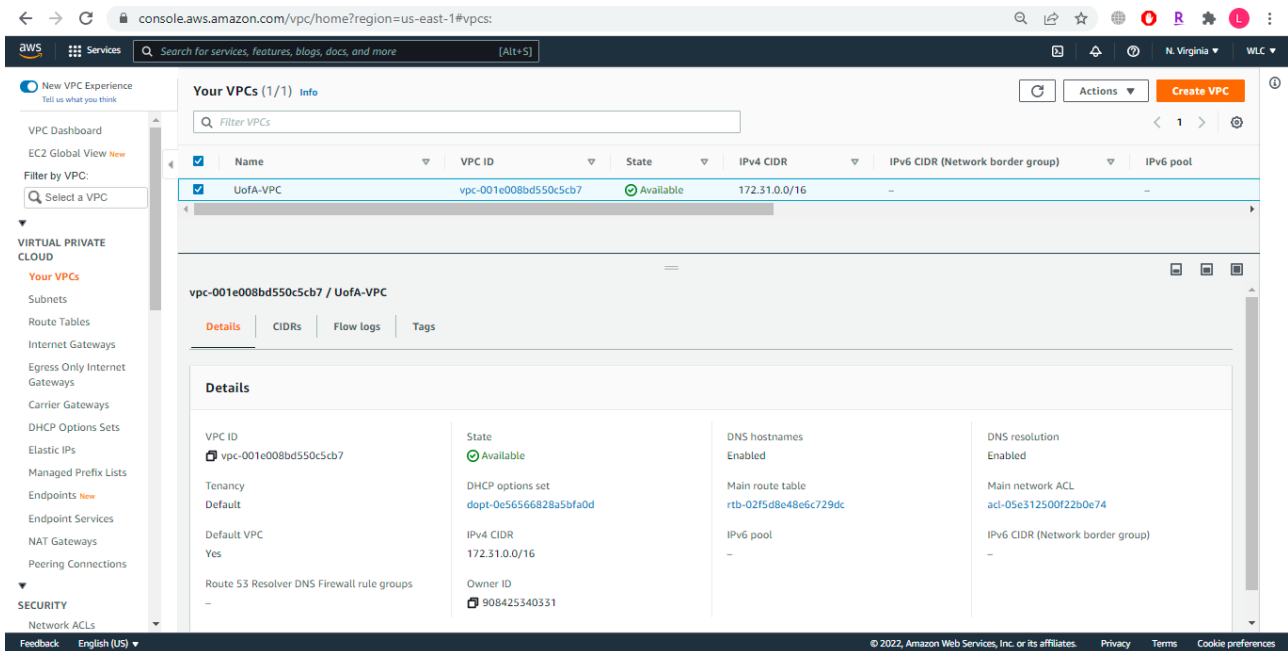


Figure 43 Routing between AWS -VPC and On-premises Network. [44]

To achieve the above scenario, we will need first to set up VPC and define a subnet. By default, there is a VPC available with the 172.31.0.0/16 CIDR and default route 0.0.0.0/0 towards the Internet gateway along with NAT configuration. Here, we will be using the same default VPC with adding a name to it, which is **UofA-VPC**.



As you can see, the CIDR Block of /16 network is already defined along with the information like DHCP options, route table, and network ACL. Below is a screenshot of the various subnets which are created by default under the VPC CIDR.

The screenshot displays the AWS Management Console interface for the 'Subnets (1/6)' page. The top section shows a table of subnets with columns for Name, Subnet ID, State, VPC, IPv4 CIDR, IPv6 CIDR, and Available IPv4. Below this, a detailed view for a selected subnet (subnet-03e8bd88d5527c12b) is shown, detailing its configuration.

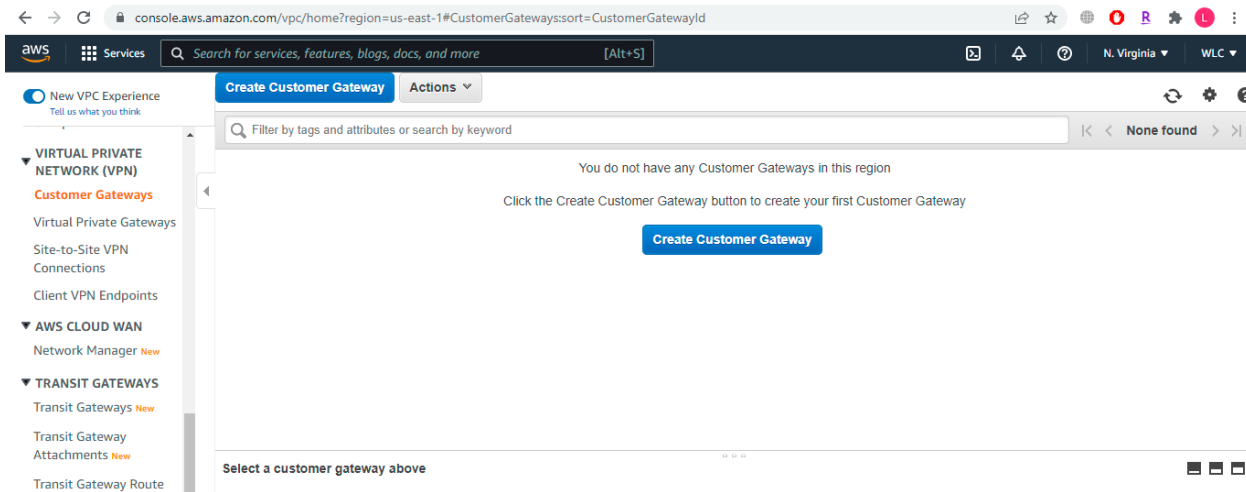
Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4
✓	subnet-03e8bd88d5527c12b	Available	vpc-001e008bd550c5cb7 Uo...	172.31.0.0/20	-	4091
☐	subnet-01bd9b3bb07362a33	Available	vpc-001e008bd550c5cb7 Uo...	172.31.64.0/20	-	4090
☐	subnet-0af373481656d65ce	Available	vpc-001e008bd550c5cb7 Uo...	172.31.80.0/20	-	4090
☐	subnet-05b4dcb3e06c5ec9d	Available	vpc-001e008bd550c5cb7 Uo...	172.31.16.0/20	-	4091
☐	subnet-0d0d4514f1dfc95f8	Available	vpc-001e008bd550c5cb7 Uo...	172.31.32.0/20	-	4091
☐	subnet-029314c41cfbb107a	Available	vpc-001e008bd550c5cb7 Uo...	172.31.48.0/20	-	4091

Subnet ID subnet-03e8bd88d5527c12b	Subnet ARN arn:aws:ec2:us-east-1:908425340331:subnet/subnet-03e8bd88d5527c12b	State Available	IPv4 CIDR 172.31.0.0/20
Available IPv4 addresses 4091	IPv6 CIDR -	Availability Zone us-east-1b	Availability Zone ID use1-az1
Network border group us-east-1	VPC vpc-001e008bd550c5cb7 UoA-VPC	Route table rtb-02f5d8e48e6c729dc	Network ACL acl-05e312500f22b0e74
Default subnet Yes	Auto-assign public IPv4 address Yes	Auto-assign IPv6 address No	Auto-assign customer-owned IPv4 address No
Customer-owned IPv4 pool -	IPv4 CIDR reservations -	IPv6 CIDR reservations -	

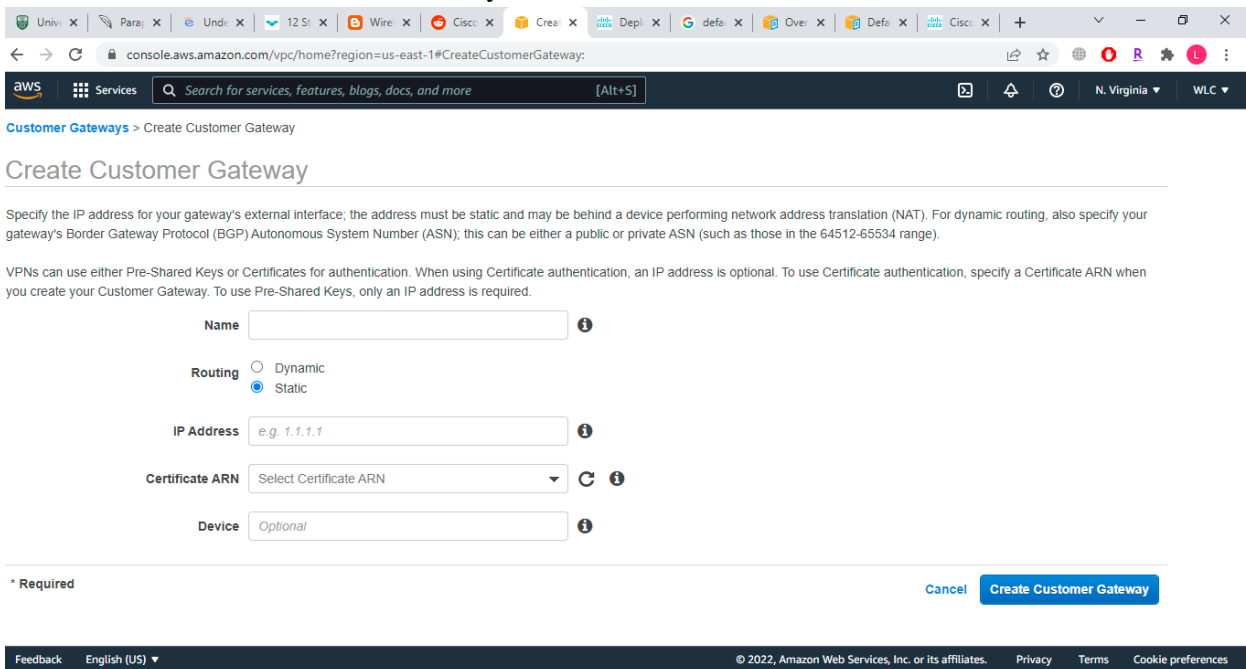
Configuring the Site-to-Site VPN

Since our VPC is ready, the next task is to create a Site-to-Site VPN between the VPC and on-premises corporate network. The first task is to create a **Customer Gateway**, which will act as a VPN gateway for the subnets in VPC to reach the on-premises network.

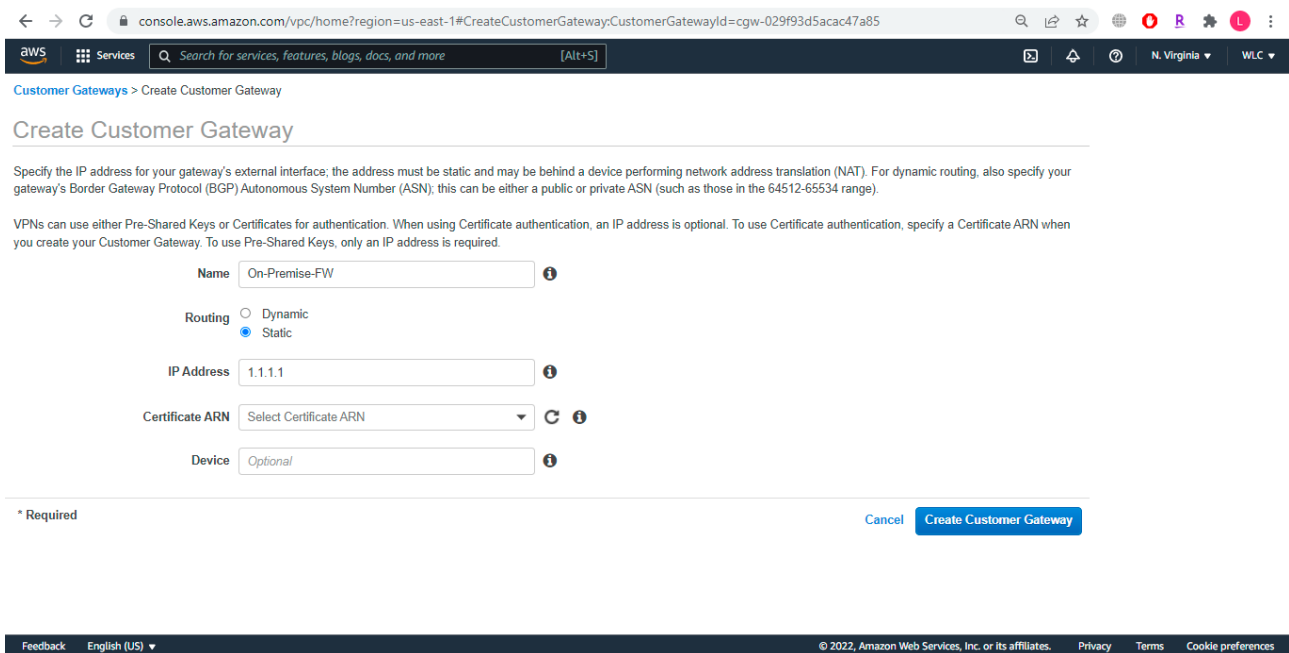
1. Go to the VPC dashboard.
2. Browse the left menu, go to VPN Connections > Customer Gateways



3. Click on 'Create Customer Gateway.'

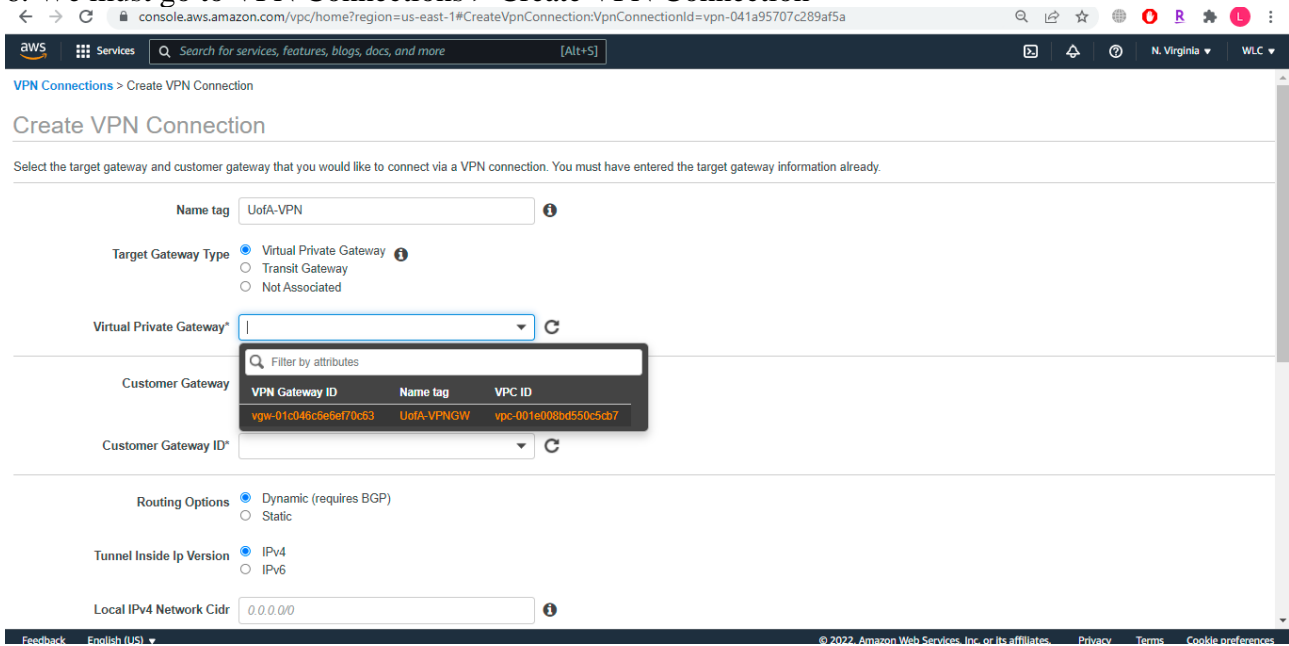


4. Enter the name of Customer Gateway and IP address of the other end of the VPN connection, i.e., corporate network router/firewall.



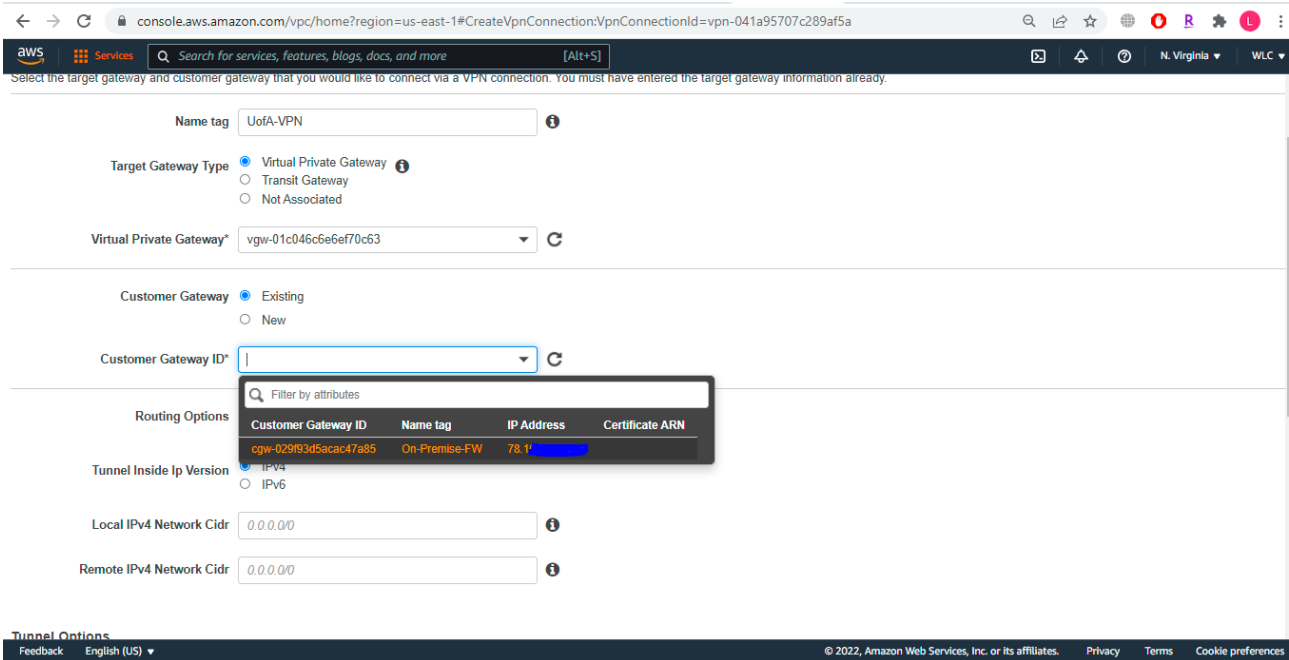
5. Now that the customer gateway is ready, we can go ahead with the actual VPN configuration.

6. We must go to VPN Connections > Create VPN Connection

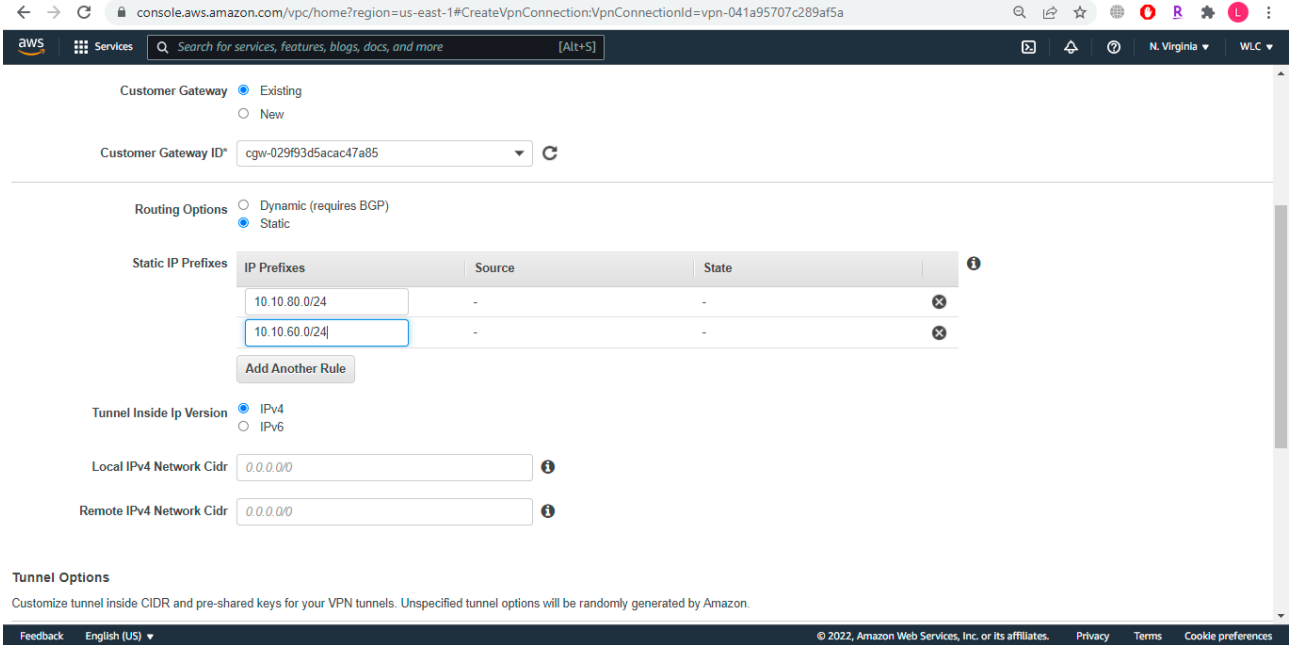


7. Select the VPN Gateway ID

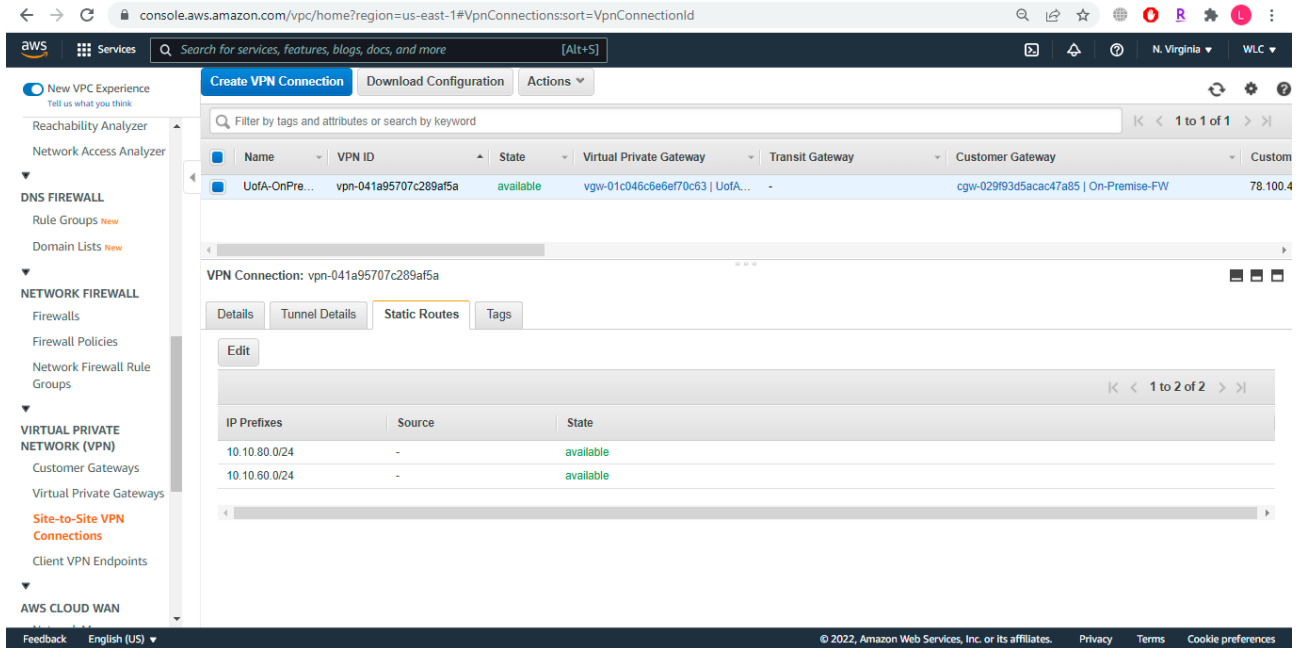
8. Select the existing Customer Gateway. The IP address is hidden due to privacy and security reasons.



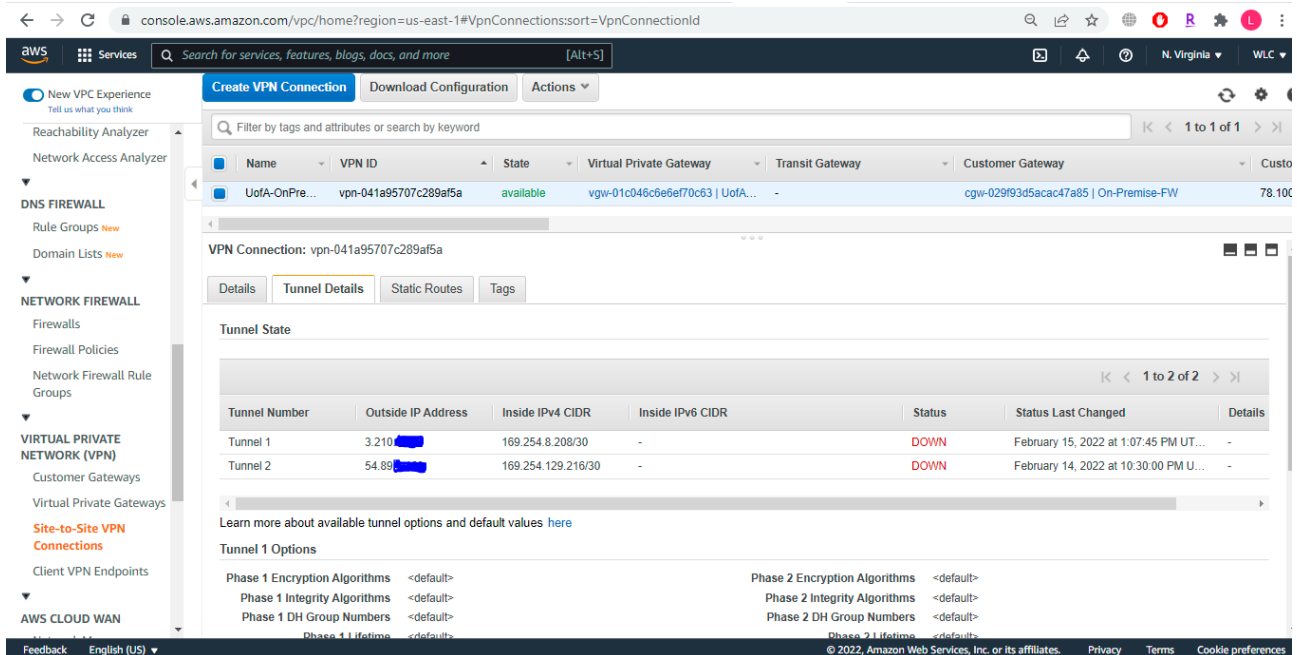
9. Routing Options will be **Static**; hence we must define the **Static IP prefixes**.



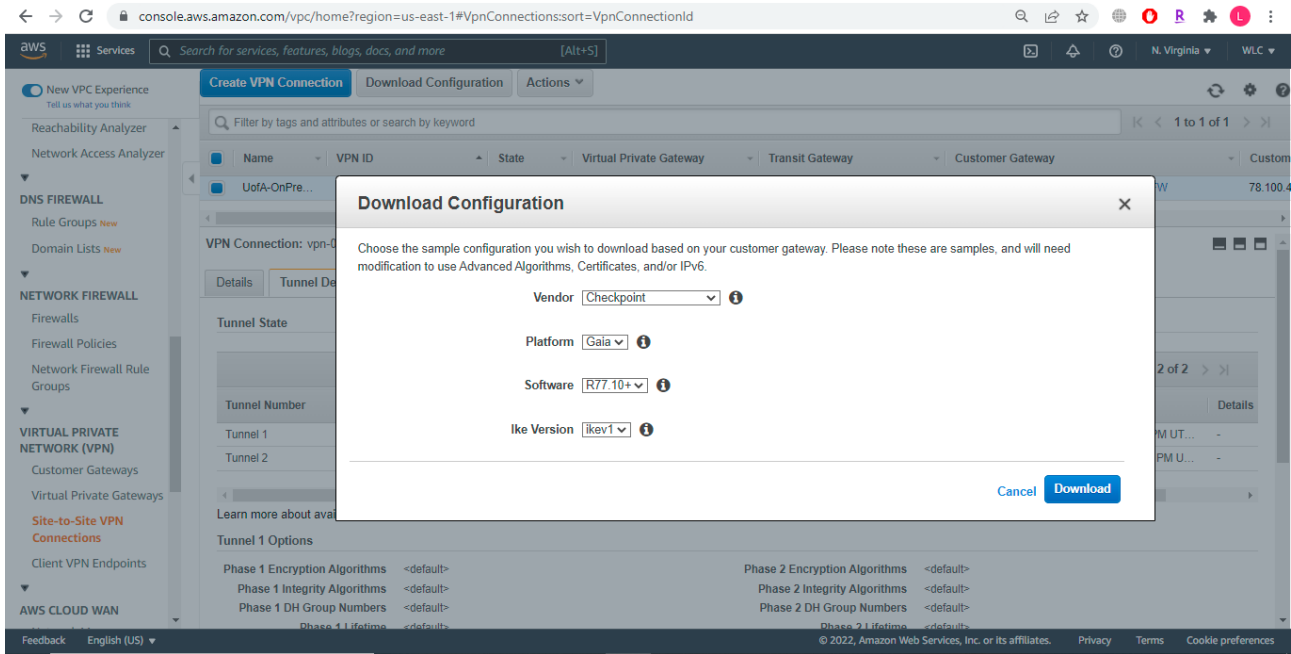
10. Rest options will be left to default, and the VPN connection will be created.



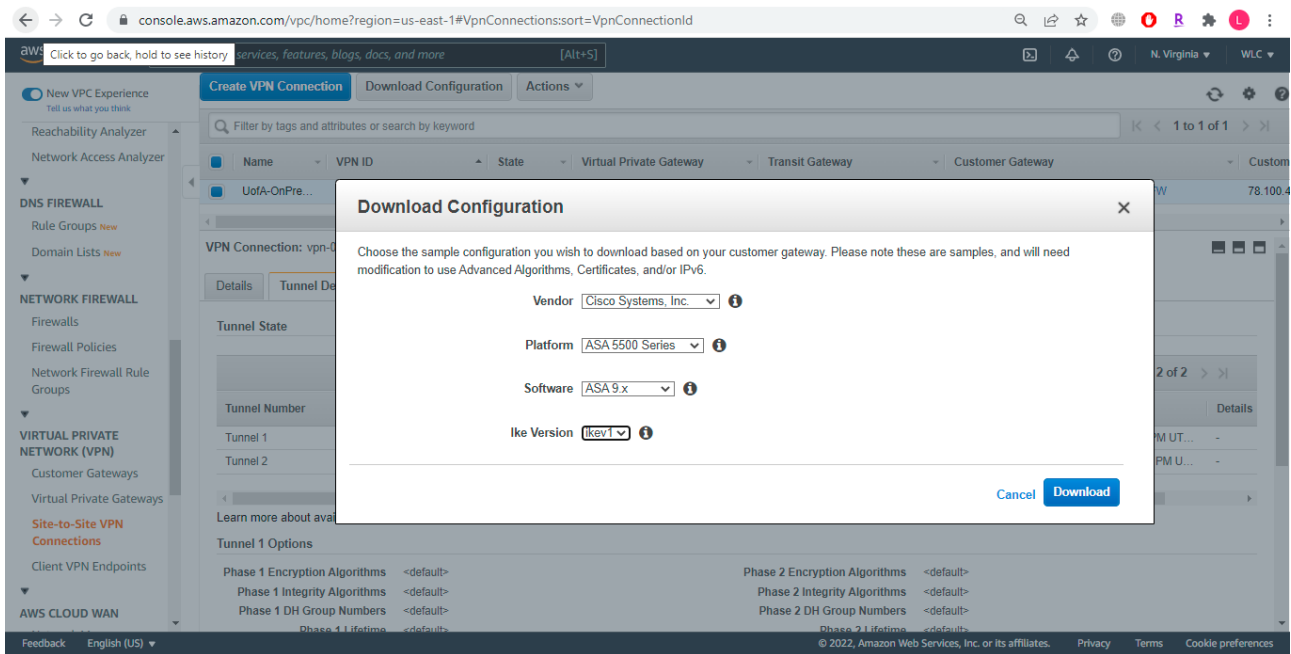
11. As you can see, there are two tunnels created. Rest configuration will be done on the corporate router/firewall.



12. AWS has a pre-built configuration for each VPN connection created with several vendor-specific config files.



13. In our scenario, we have **Cisco ASA 5508-X firewall** on the corporate network edge.



14. A text file containing all the steps to successfully connect to the VPN from the corporate network is downloaded. All we need to do is edit the file based on some values personal to our firewall.

```

vpn-041a95707c289af5a - Notepad
File Edit Format View Help
! Amazon Web Services
! Virtual Private Cloud
!
! AWS utilizes unique identifiers to manipulate the configuration of
! a VPN Connection. Each VPN Connection is assigned an identifier and is
! associated with two other identifiers, namely the
! Customer Gateway Identifier and Virtual Private Gateway Identifier.
!
! Your VPN Connection ID           : vpn-041a95707c289af5a
! Your Virtual Private Gateway ID  : vgw-01c046c6e6ef70c63
! Your Customer Gateway ID        : cgw-029f93d5acac47a85
!
!
! This configuration consists of two tunnels. Both tunnels must be
! configured on your Customer Gateway. Only a single tunnel will be up at a
! time to the VGW.
!
! You may need to populate these values throughout the config based on your setup:
! <outside_interface> - External interface of the ASA
! <outside_access_in> - Inbound ACL on the external interface
! <amzn_vpn_map> - Outside crypto map
! <vpc_subnet> and <vpc_subnet_mask> - VPC address range
! <local_subnet> and <local_subnet_mask> - Local subnet address range
! <sla_monitor_address> - Target address that is part of acl-amzn to run SLA monitoring
!
! -----
! IPsec Tunnels
! -----
! #1: Internet Key Exchange (IKE) Configuration
!
! A policy is established for the supported ISAKMP encryption,
! authentication, Diffie-Hellman, lifetime, and key parameters.
!
! Note that there are a global list of ISAKMP policies, each identified by
! sequence number. This policy is defined as #201, which may conflict with

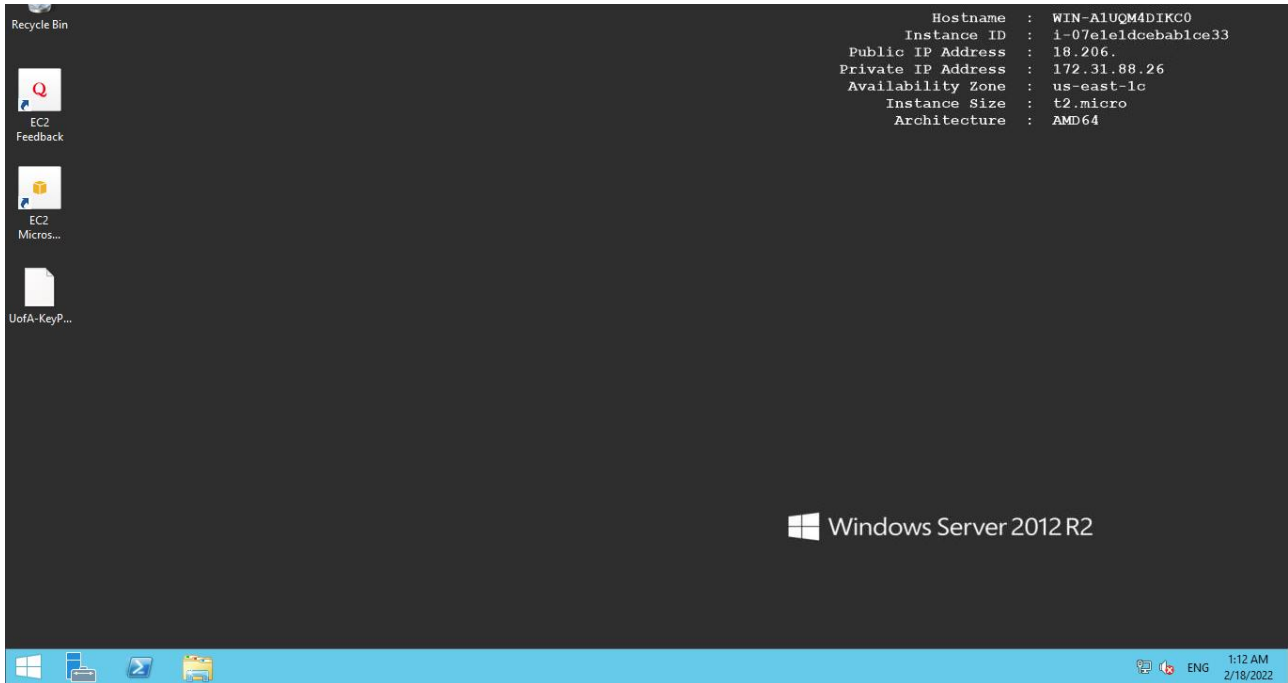
```

15. Make sure that we have a route in your VPC to reach the remote subnet pointing to the VPN gateway.

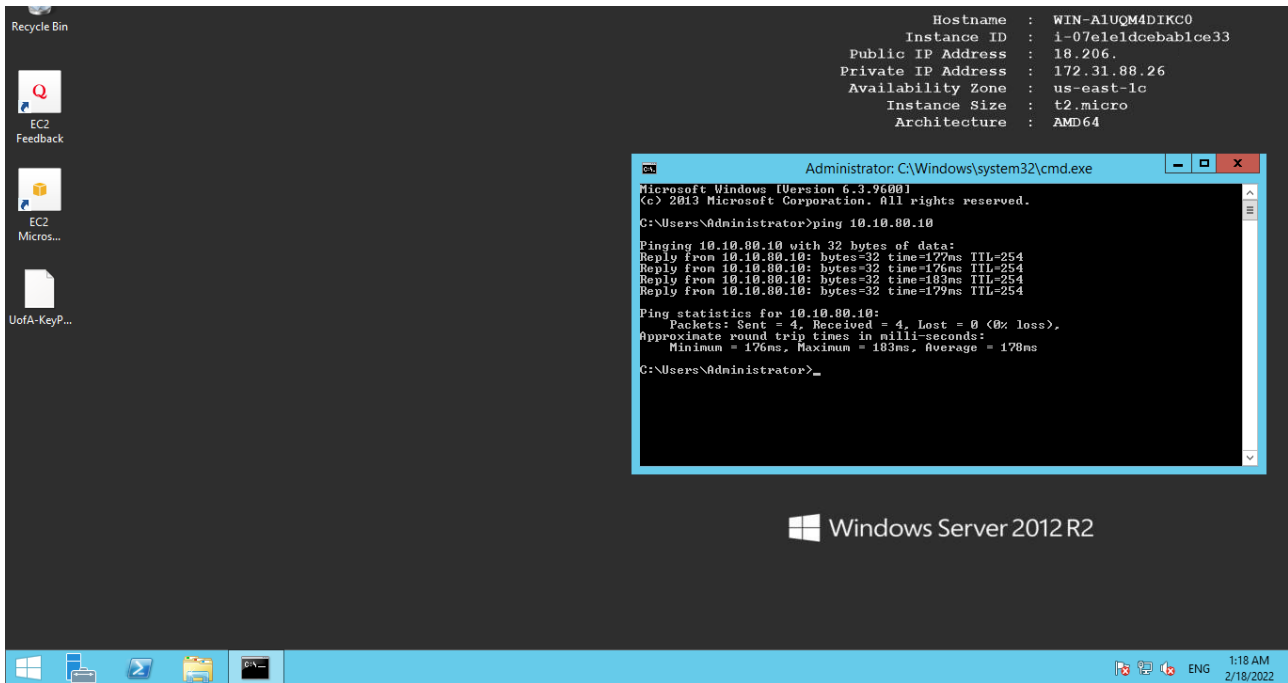
The screenshot shows the AWS Management Console interface for configuring a route table. The main content area displays the 'Routes (4)' section for the 'UofA-RouteTable' (rtb-02f5d8e48e6c729dc). The routes are as follows:

Destination	Target	Status	Propagated
10.10.60.0/24	vgw-01c046c6e6ef70c63	Active	No
10.10.80.0/24	vgw-01c046c6e6ef70c63	Active	No
172.31.0.0/16	local	Active	No
0.0.0.0/0	igw-03b05f56c1d55beb5	Active	No

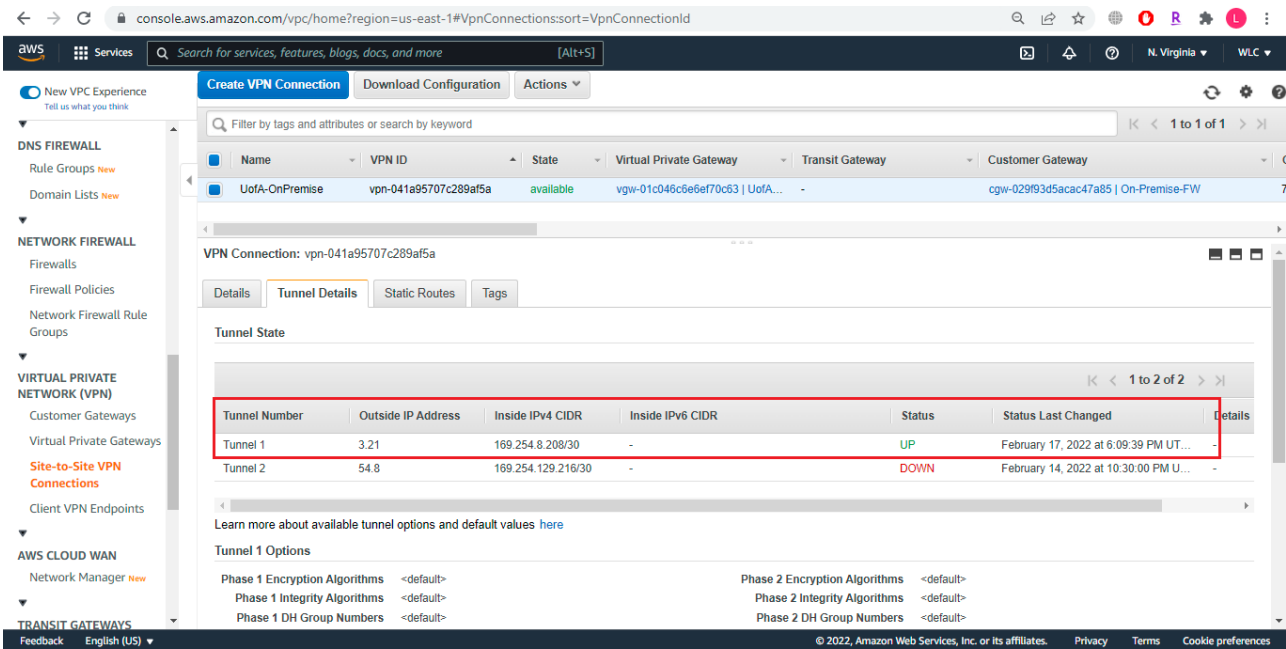
16. After configuring the firewall at the corporate network, I will have to test the VPN connectivity. In order to do that, I have set up a Virtual machine with Windows Server 2012 R2 Operating system.



17. This VM is in the subnet of our default VPC; we will try to ping the subnet at the corporate network, i.e., **10.10.80.0/24**.



18. As we can see, the ping is successful. That means the VPN Tunnel will be **UP**. We can verify this in the VPC dashboard under Site-to-Site VPN Connections.



Now that the VPN connectivity is successfully established, we focus our attention on actually implementing the Cisco 9800 wireless LAN controller.

Configuring the Cisco Wireless 9800 instance in AWS Cloud

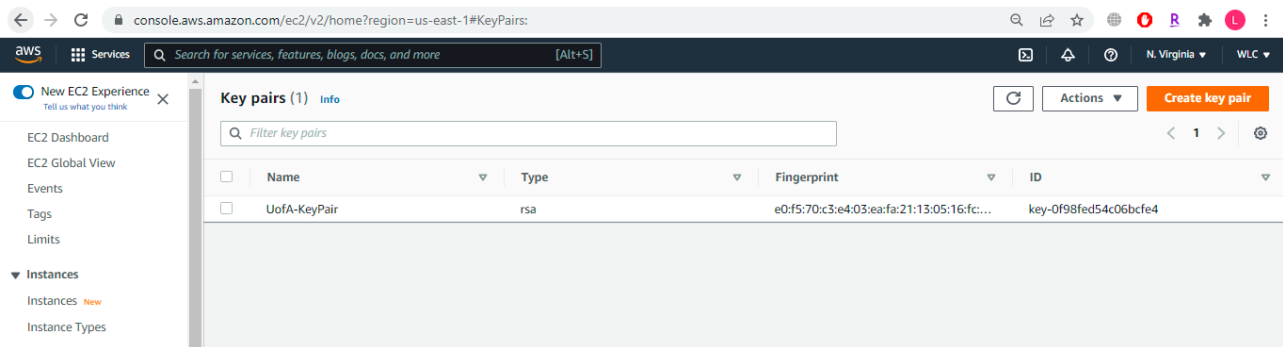
AWS Cloud gives us three ways to establish the C9800-CL on the AWS Cloud.

- i. Using the AWS Marketplace feature – CloudFormation template
- ii. Using the AWS Marketplace feature – AMI
- iii. Launching from the AWS Console

The process ranges from a more manual operation in which the client has complete power over each setup setting (through the AWS interface) to a fully guided tool (using the CloudFormation template), helping clients to select the right and appropriate choice for their needs. [44]

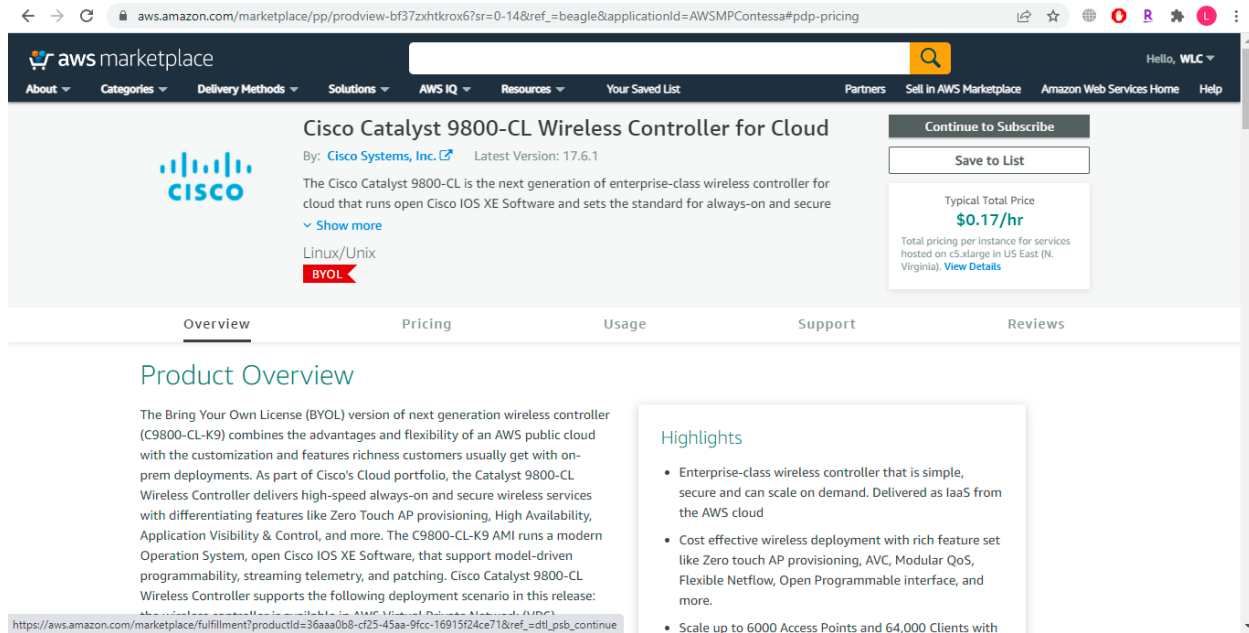
In our case, we will opt for the second option, which is launching the C9800-CL instance from AWS Marketplace using the AMI, wherein we will have more options as compared to the CloudFormation template.

Before we start, we need to make sure that a Key-pair is present. If you don't have one already, create a key pair by going to EC2 dashboard > Network & Security > Key pairs and clicking on "Create Key Pair." [44] but in our case, I have already configured a key-pair as shown below-

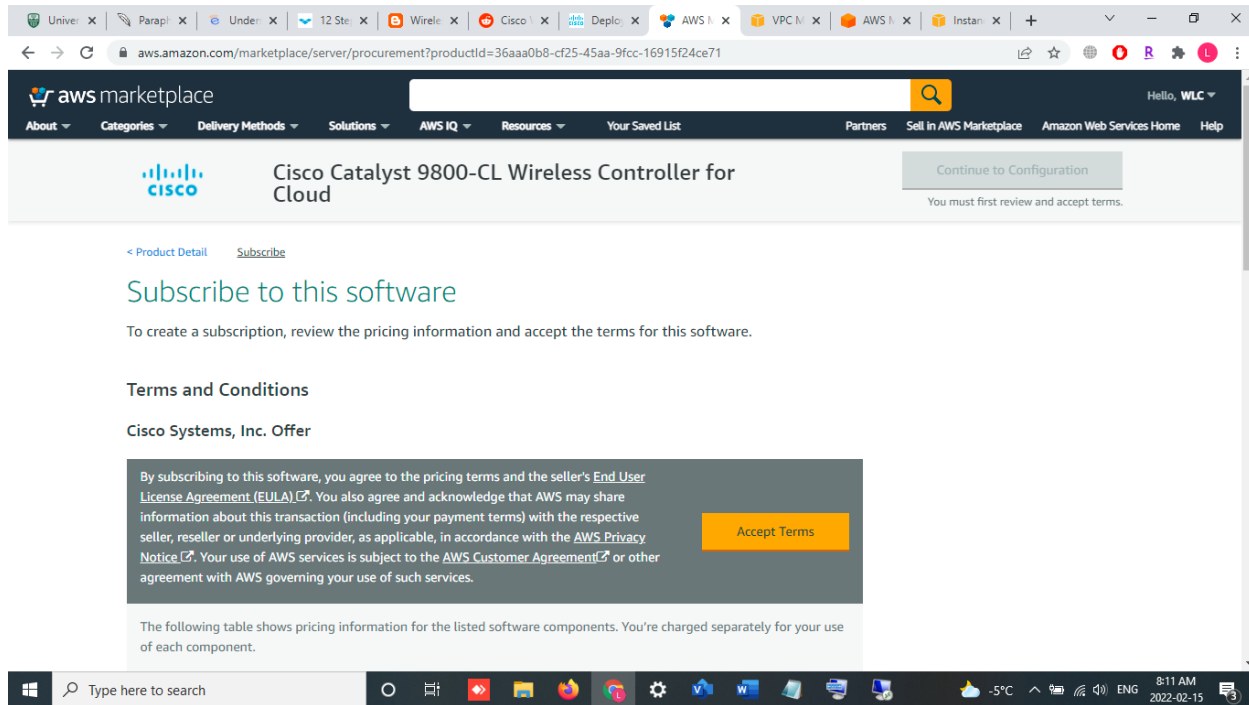


1. First, we need to access the AWS Marketplace-
<https://aws.amazon.com/marketplace/>

2. Locate the Cisco Catalyst 9800-CL in the search box and follow the first result.



3. Click on **Continue to Subscribe**



4. Below is the page; we will find the instance to which we want to subscribe to. In our implementation, we will select **c5.xlarge**.

Information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the [AWS Privacy Notice](#). Your use of AWS services is subject to the [AWS Customer Agreement](#) or other agreement with AWS governing your use of such services.

The following table shows pricing information for the listed software components. You're charged separately for your use of each component.

EC2 Instance Type	Software/hr
c5.xlarge	\$0
c5.2xlarge	\$0
c5.4xlarge	\$0

[End User License Agreement](#)

5. After accepting the terms, our request will be processed. It will take around 2-3 minutes.

Thank you for subscribing to this product! We are processing your request.

[Product Detail](#) [Subscribe](#)

Subscribe to this software

Your subscription to this product is pending and may take a few minutes. You will be notified on this page when the subscription is complete.

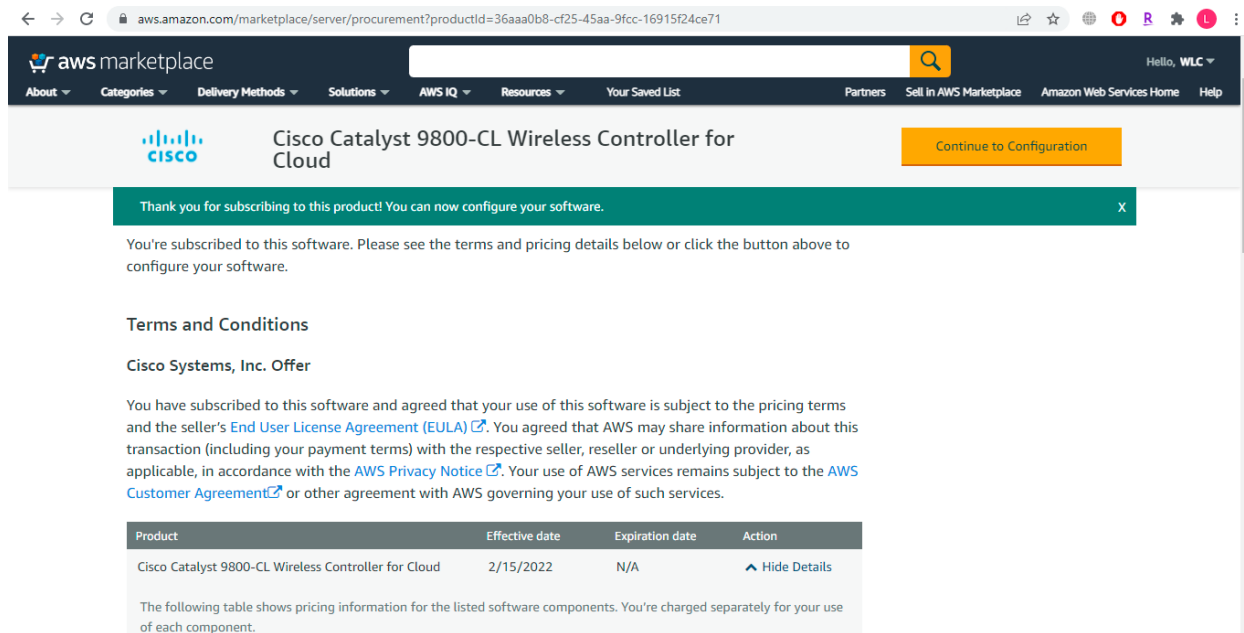
Terms and Conditions

Cisco Systems, Inc. Offer

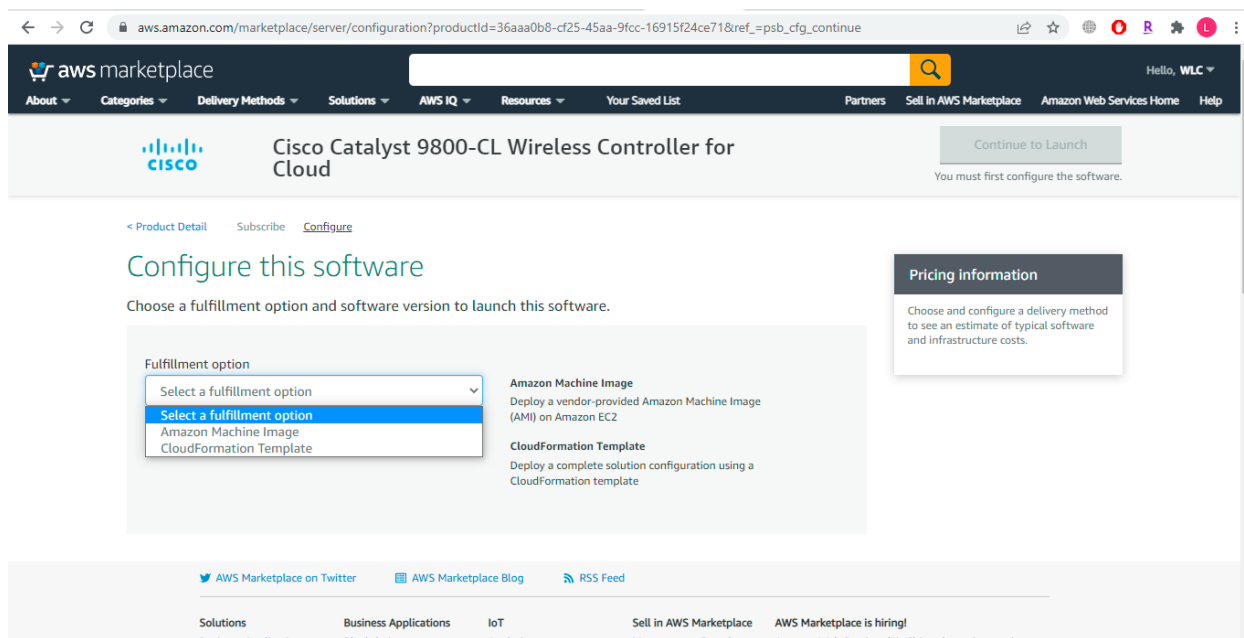
You have subscribed to this software and agreed that your use of this software is subject to the pricing terms and the seller's [End User License Agreement \(EULA\)](#). You agreed that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the [AWS Privacy Notice](#). Your use of AWS services remains subject to the [AWS Customer Agreement](#) or other agreement with AWS governing your use of such services.

Product	Effective date	Expiration date	Action
---------	----------------	-----------------	--------

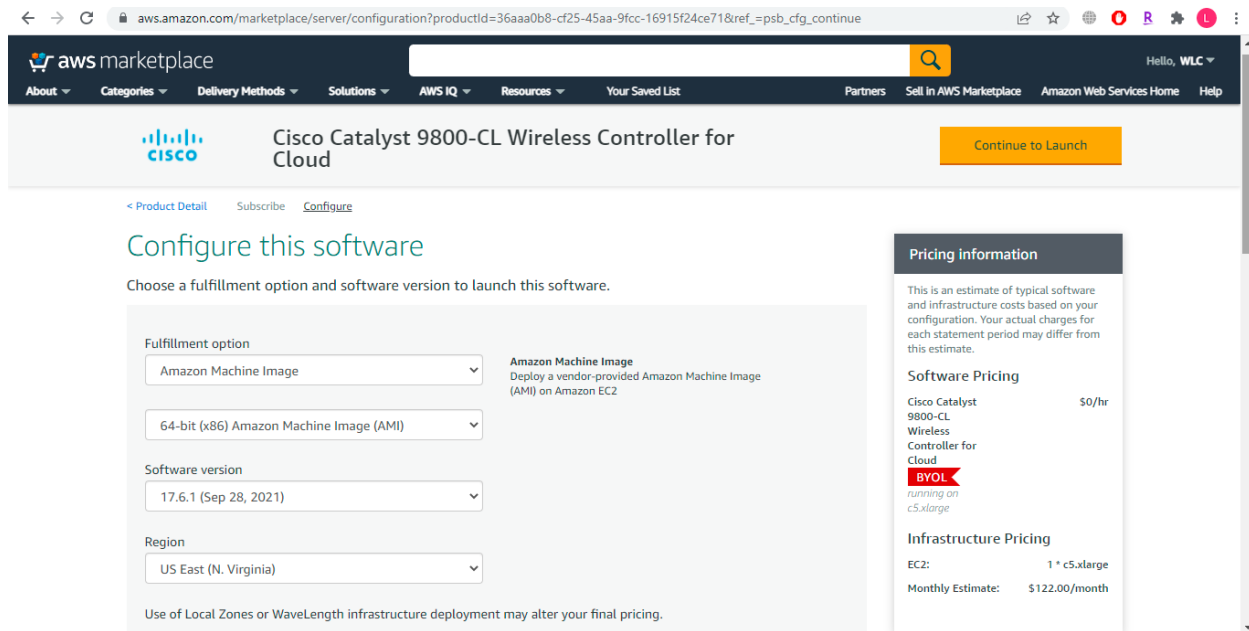
6. Once the request is processed, the option **Continue to Configuration** will be available, and we need to click on that to proceed ahead.



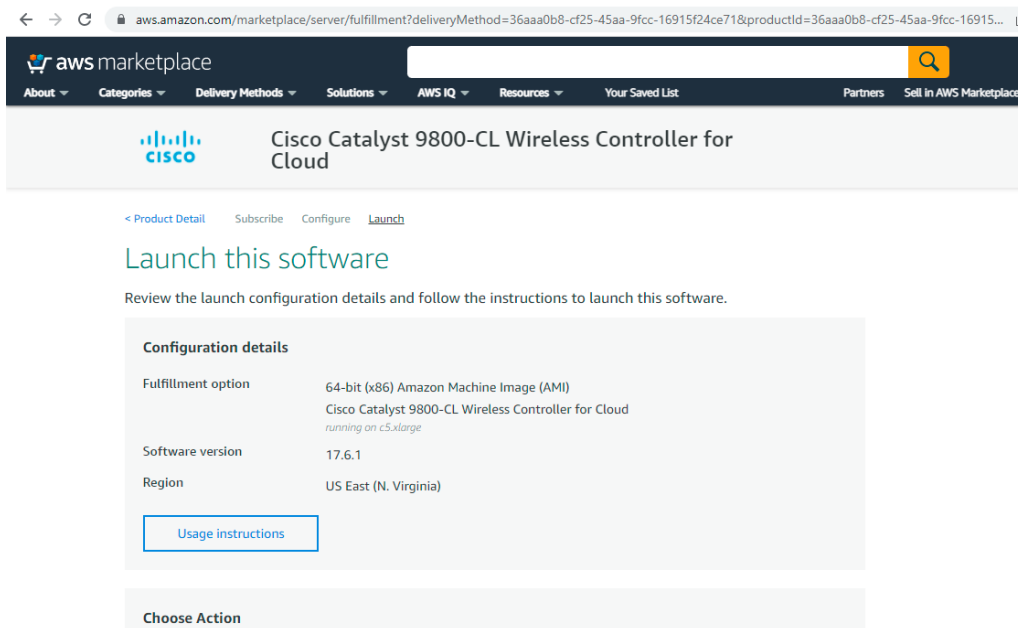
7. For the configuration, we have two options to proceed with. The first one is the CloudFormation template, and another one is the Amazon Machine Image which we will select.



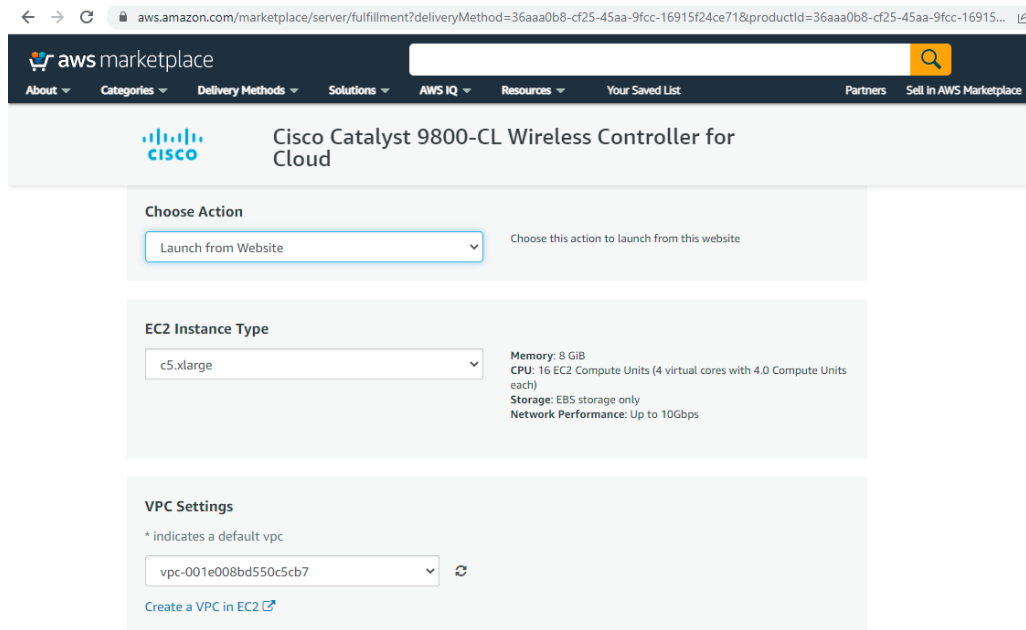
8. The following details input will be the software version and Amazon data center location where the image will be hosted. In our case, we will be hosting in the US East N. Virginia data center, and its monthly pricing for infrastructure will be \$122 per month.



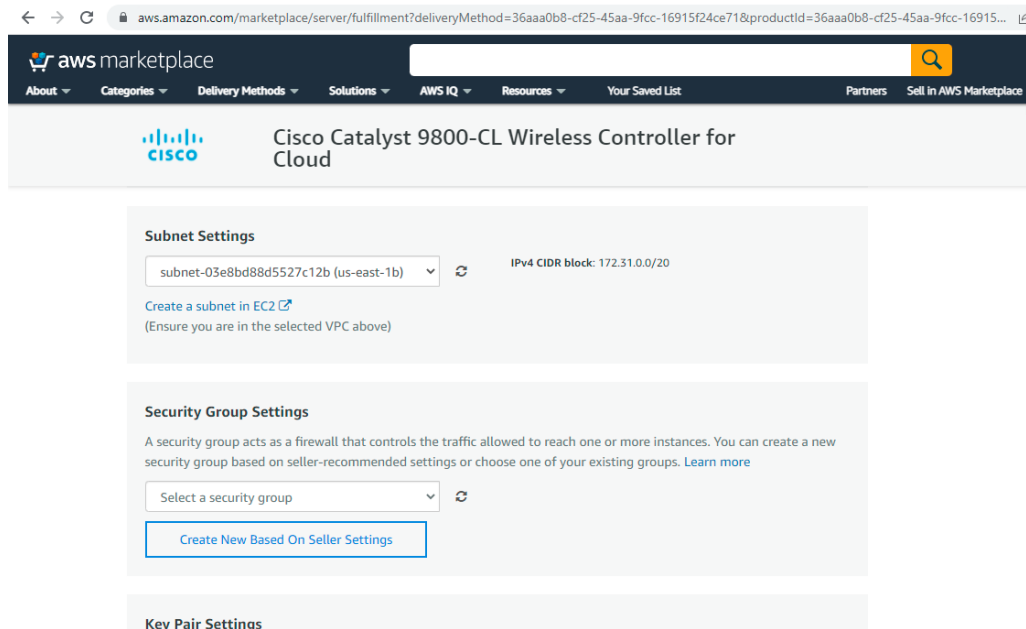
9. After clicking on **Continue to launch**, we will be presented with the configuration details.



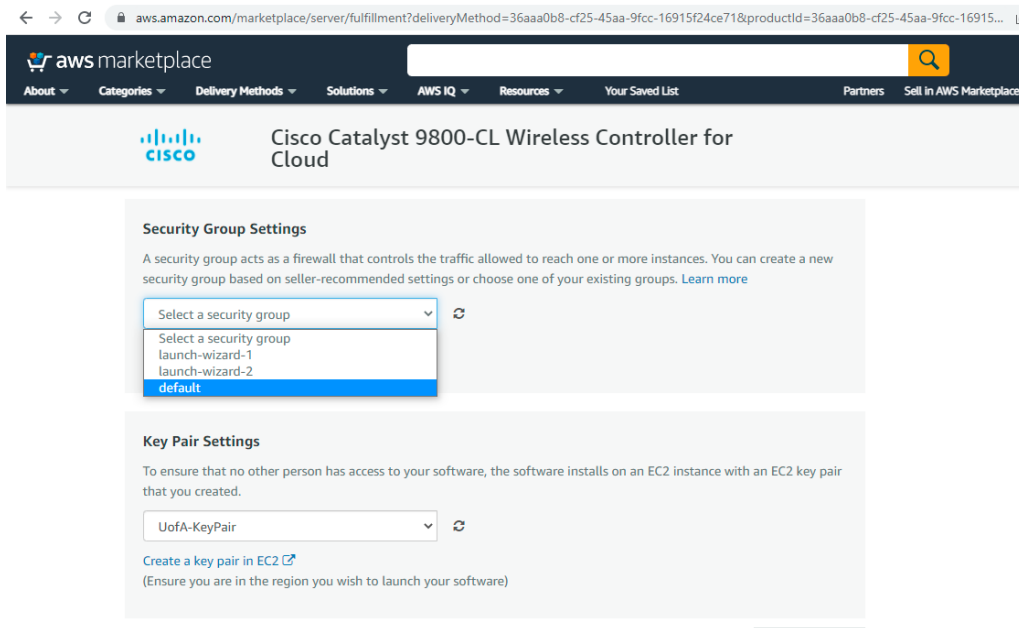
10. Here, we need to select the VPC. I chose the default VPC we had earlier.



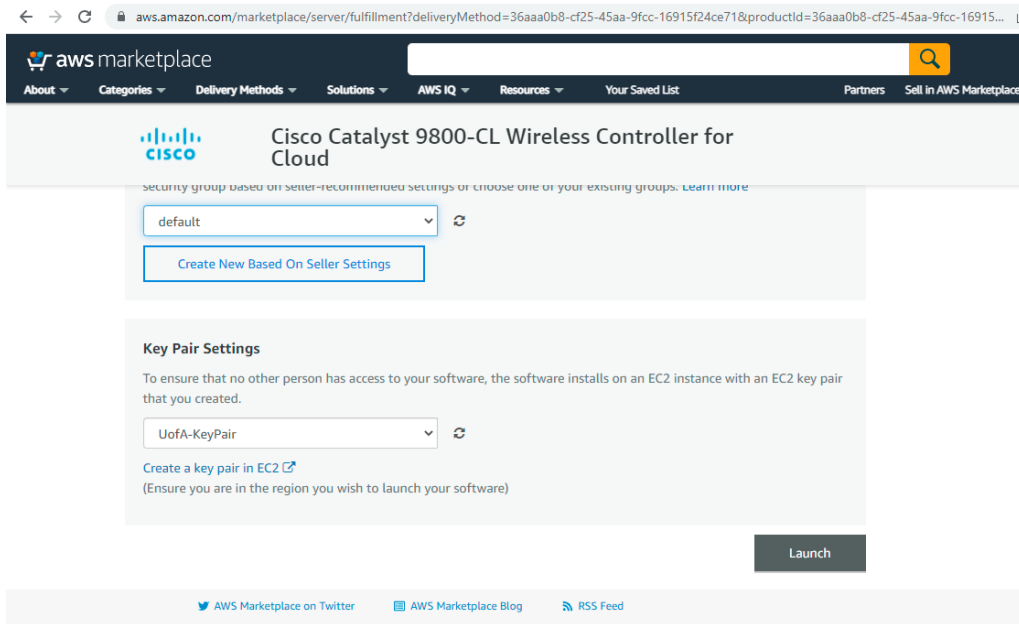
11. Selecting the subnet, in our case, we selected **172.31.0.0/20**



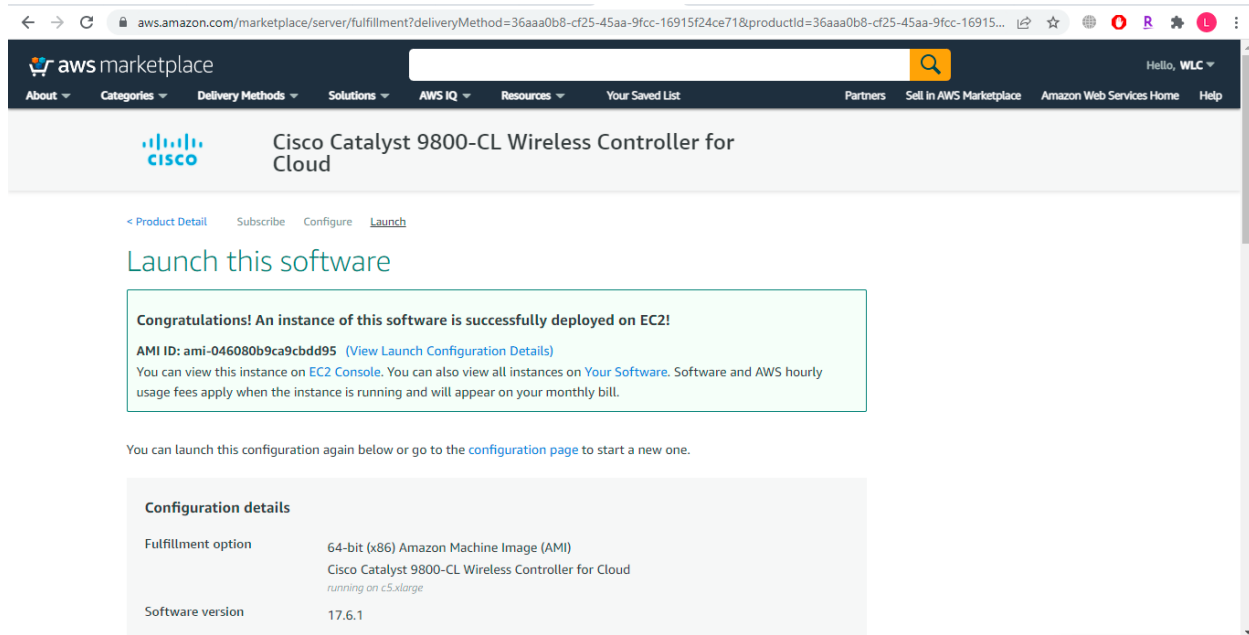
12. Security group must be defined; I selected the default security group in our case.



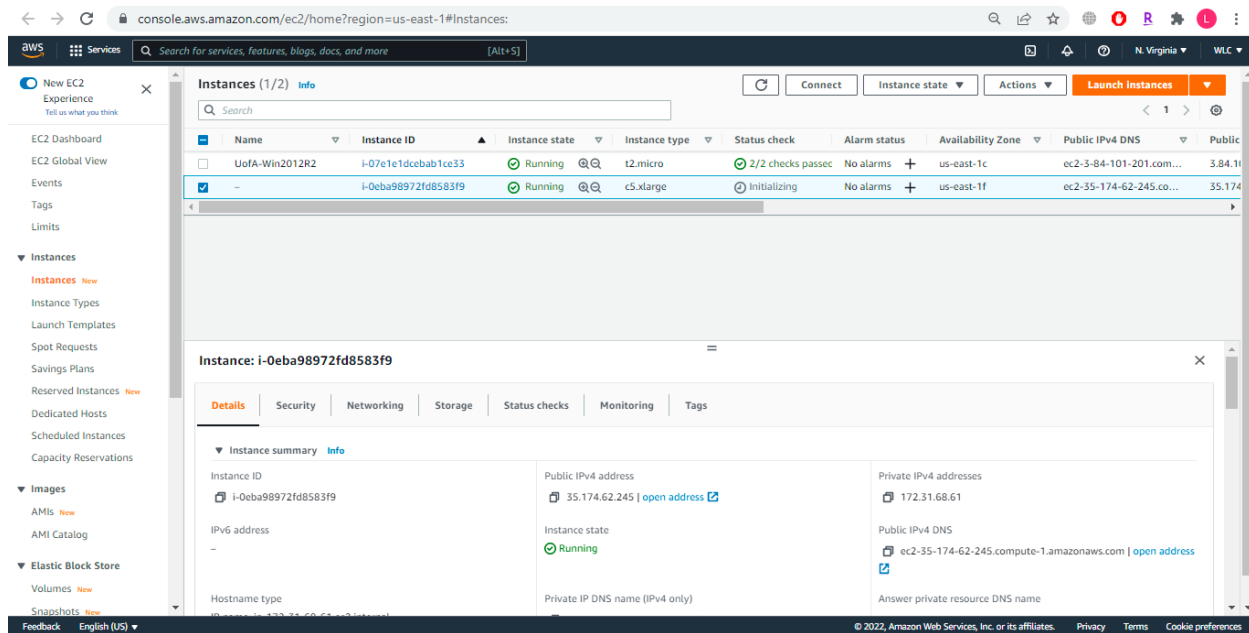
13. Finally, we select the Key-Pair; in our scenario, we had already created a key pair named **UofA-KeyPair**.



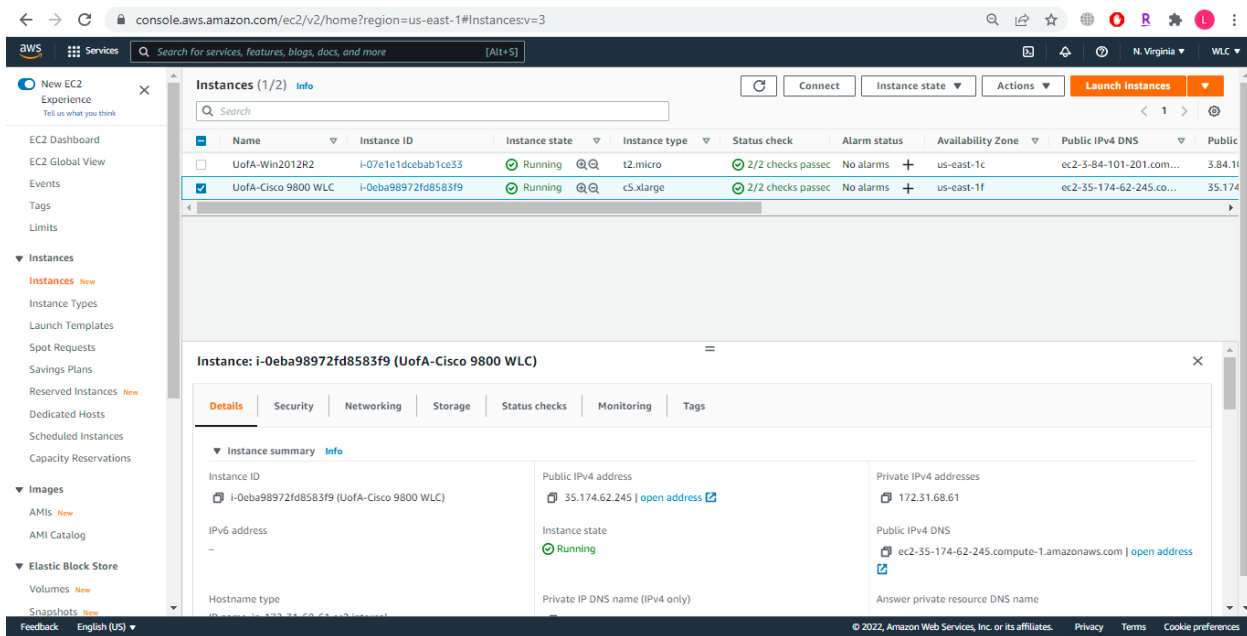
14. Now, the instance will be successfully launched on EC2. A confirmation will be present upon the same as shown below.



15. Reaching the EC2 dashboard, we will see our new Cisco 9800 instance running but still not yet ready as it is initializing.



16. After 5-10 minutes, we will see the instance completed, ready, and initialized.



17. Now, we can access the WLC using the IP address and SSH into it.

18. Access the CLI via ssh as below:

Use the .pem file to authenticate using the certificate.

- `chmod 400 <file>.pem`
- `ssh -i "file name.pem" ec2-user@<c9800-CL IP>`

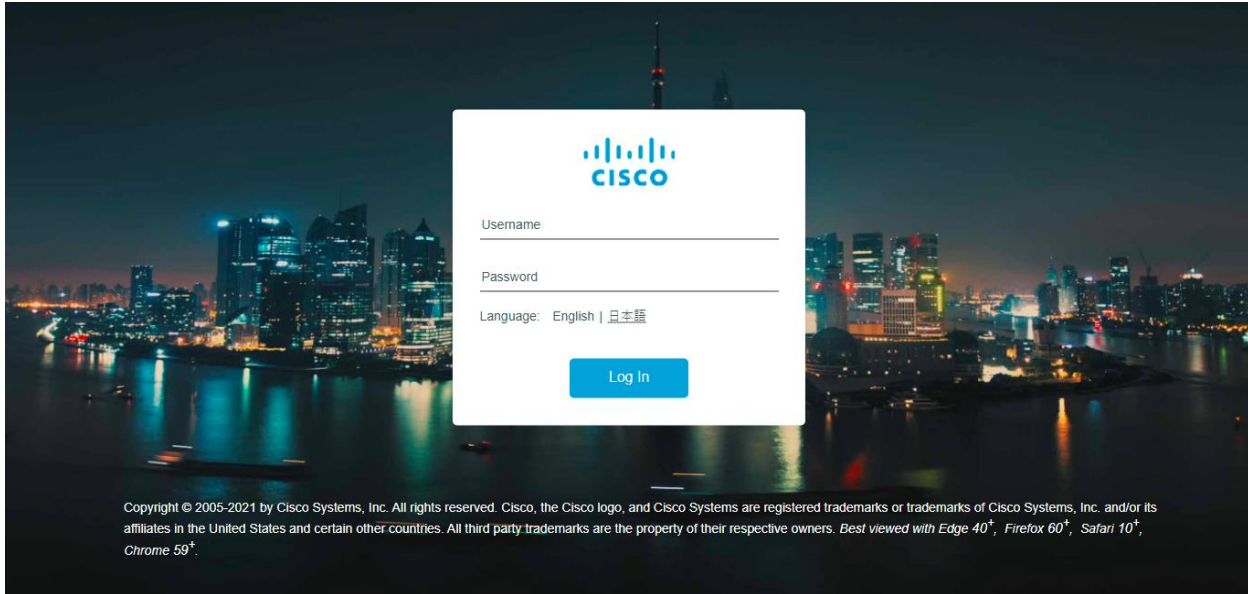
19. Optionally, we can set the hostname-

```
WLC (config) #hostname UofA-C9800
```

20. Enter the config mode and add login credentials using the following command:

```
UofA-C9800 (config) #username <name> password <yourpwd>
```

21. Upon connecting to the webpage using the public IP address of the WLC instance, we can log in using credentials created through the SSH



22. First, we need to define the general settings, such as hostname, country, date, time, time zone, and NTP server.

 Configuration Setup Wizard

1. General Settings

Host Name*

Country +

Date 📅

Time / Timezone ▾

NTP Servers +

Added NTP servers

🗑️

AAA Servers 🔑 +

Added AAA servers

Next

23. Now, we must specify the private IP address of the WLC. This will be the IP address that the access point will reach to associate itself with the WLC. In our case, it is **172.31.68.61**





Configuration Setup Wizard

1. General Settings

AAA Servers

Added NTP servers

Enter Radius Server IP Enter Key  

Added AAA servers

Wireless Management Settings

Port Number: GigabitEthernet1

IP Address: 172.31.68.61

[Next](#)

24. Now, the option to create a new SSID will be presented.



Configuration Setup Wizard

2. Wireless Network Settings

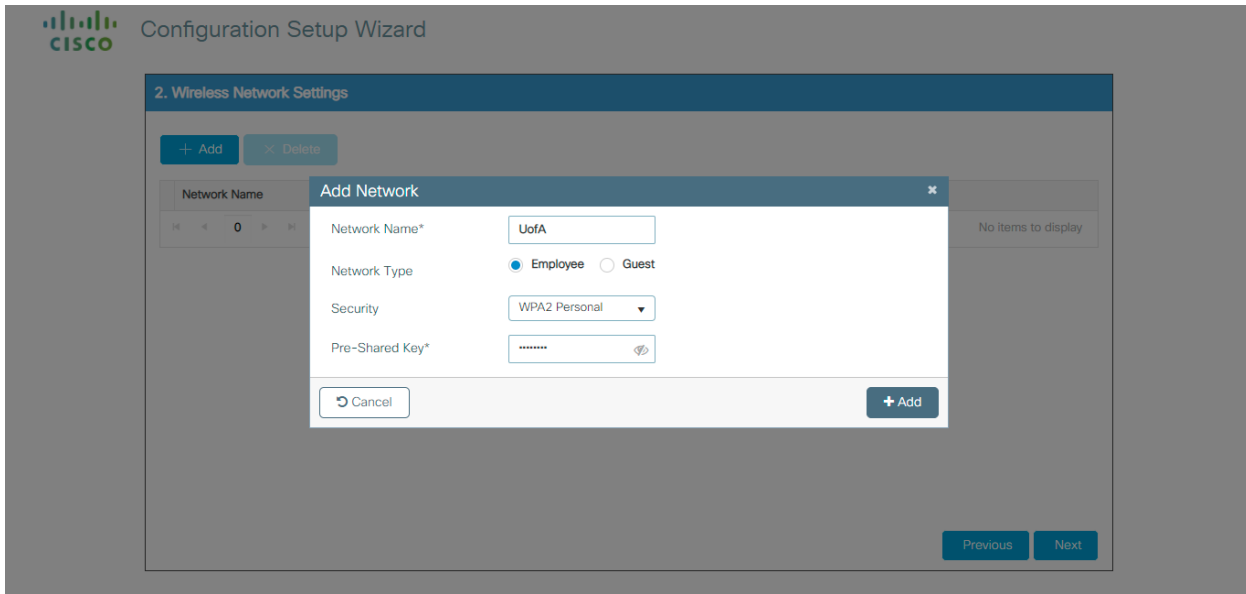
[+ Add](#) [x Delete](#)

Network Name	Network Type	Security
No items to display		

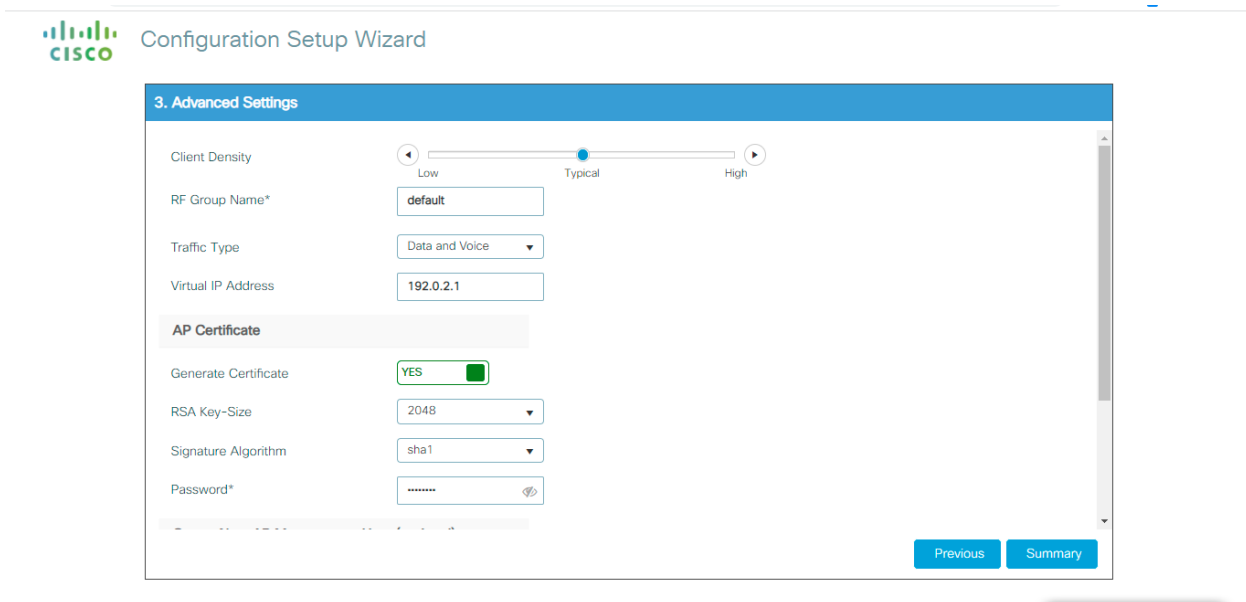
10 items per page

[Previous](#) [Next](#)

25. I will be creating a new network named **UofA** with a WPA2 personal key.



26. The last section is the Advanced Settings, defining the Client density, RF Group, AP Certificate, etc.



27. The WLC will summarize all the settings we mentioned in the summary section.



4. Summary

General Settings

Host Name	UofA-C9800
Country	QA
Date	15 Feb 2022
Time / Timezone	20:59:23 / AST
NTP Servers	10.10.80.10

Wireless Management Settings

Port Number	GigabitEthernet1
-------------	------------------

Wireless Network Settings

Network Name	Network Type	Security
UofA	employee	personal

10 items per page 1 - 1 of 1 items

Previous Finish



4. Summary

Network Name	Network Type	Security
UofA	employee	personal

10 items per page 1 - 1 of 1 items

Advanced Settings

Client Density	Typical
RF Group Name	default
Traffic Type	data and voice
Virtual IPv4 Address	192.0.2.1

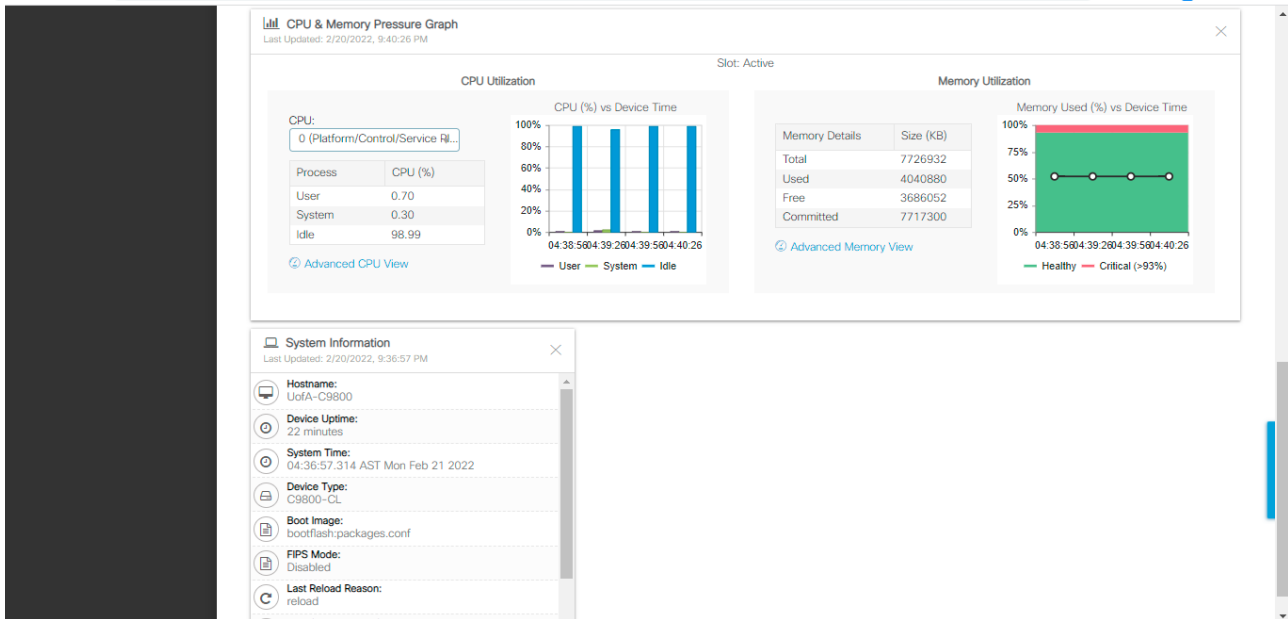
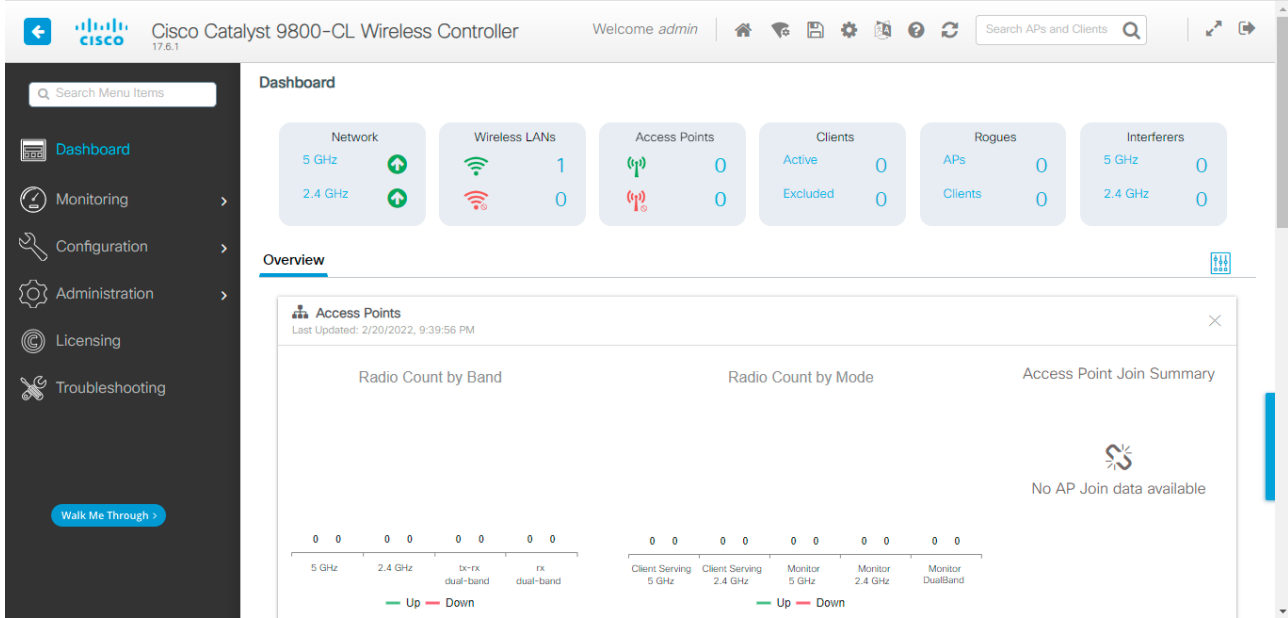
AP Certificate

Generate Certificate	Yes
RSA Key-Size	2048
Signature Algorithm	sha1

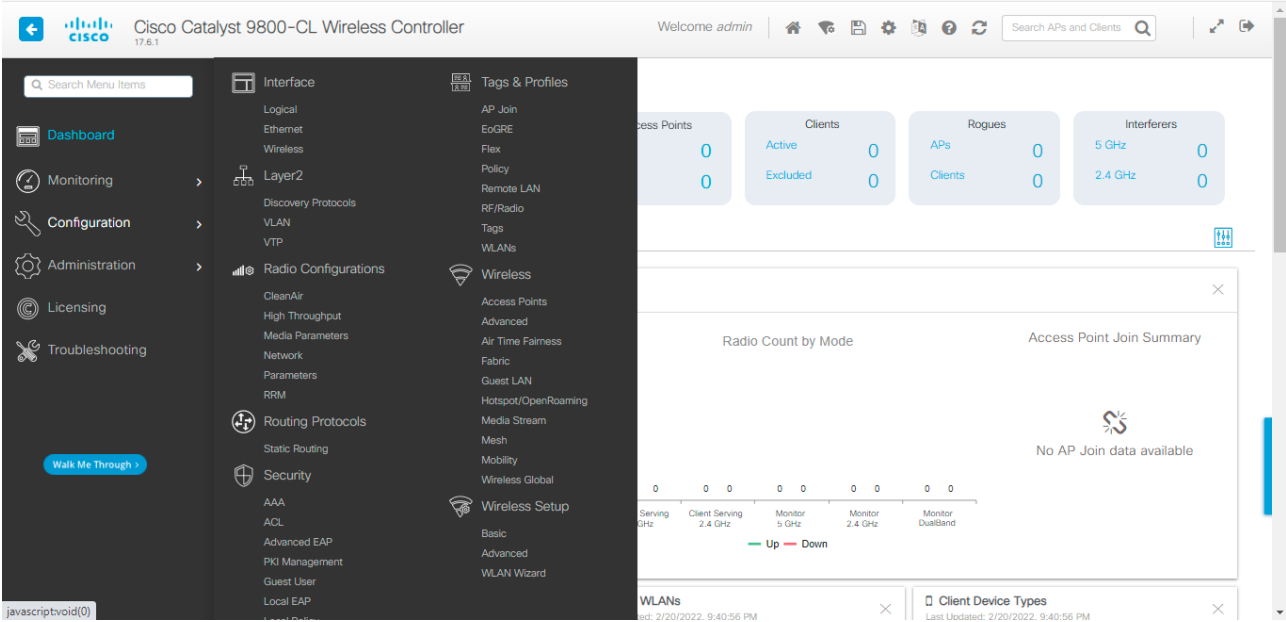
Previous Finish

Upon clicking the finish, the WLC will reload and apply those settings.

The WLC will reload, and the login page will be displayed again. Upon successful login, we will be presented with the C9800 Dashboard.



In the configuration section, we have a massive number of options to configure.



Configuring DHCP server for Lightweight Wireless Access Points

The remaining configuration resides on the corporate on-premises network, where we connect the wireless access points to the PoE switch and assign Layer 3 attributes using DHCP.

We have several options to achieve this; it does not matter what vendor you choose, as long as it serves the purpose.

First, we will look into the **Cisco DHCP server**.

Let's consider we have a Cisco L3 switch/router; DHCP Option 43 will help the wireless access points to identify its WLAN controller. [46]

1. Login into the configuration mode at the Cisco IOS command-line interface.
2. Create a DHCP pool, which includes the necessary parameters such as the default router and server name. [46]

This is how we can configure the DHCP scope:

```
ip dhcp pool <pool name>
network <ip network> <netmask>
default-router <default-router IP address>
dns-server <dns server IP address>
```

3. Add the Option 43 line with this syntax:

```
option 43 hex <hexadecimal string>
```

The confusing thing is the hexadecimal string, which is to be supplied along with option 43, is actually a combination of Type+Length+Value. The type will always be 0xf1. Length value will be the number of wireless LAN controllers. Sometimes, we can have multiple wireless LAN controllers in an enterprise for redundancy and high availability. They will be listed in order of preference. [46]

For instance, we have two wireless LAN Controllers, with IP addresses as 192.168.10.20 and 192.168.10.5.

Hence the values will be as below-

- i. Type - 0xf1
- ii. Length - 2x4 = 0x08
- iii. Value - c0a80a05 (192.168.10.5) and c0a80a14 (192.168.10.20)

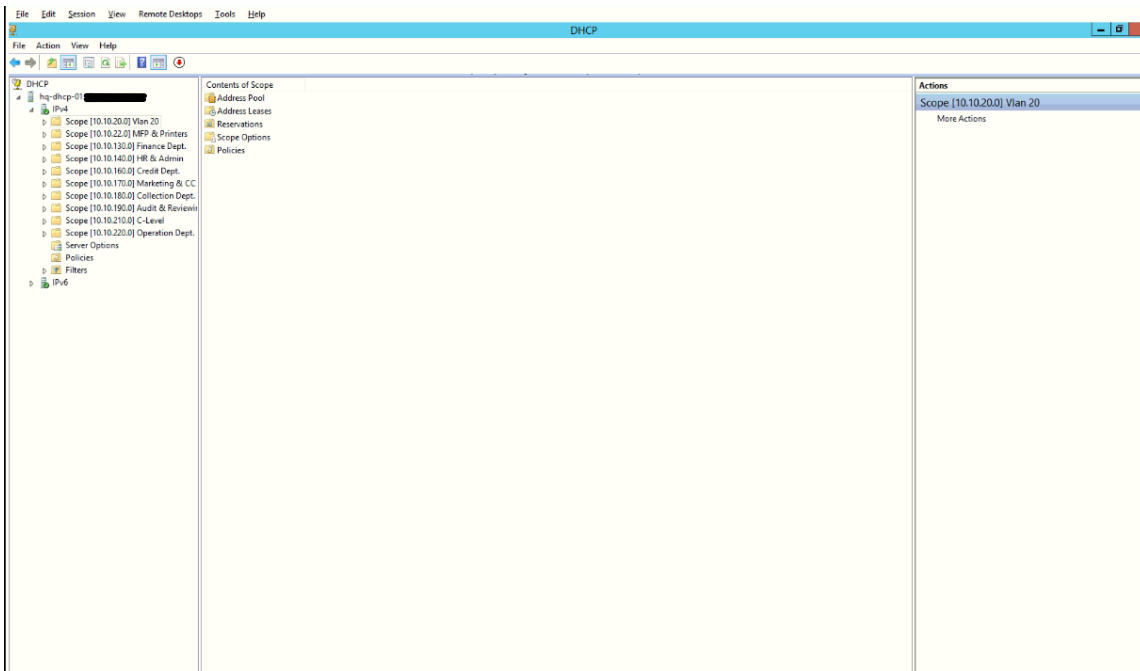
when we combine all the values, the string will f108c0a80a05c0a80a14. [46]

The Cisco IOS command will be as follows [46]:

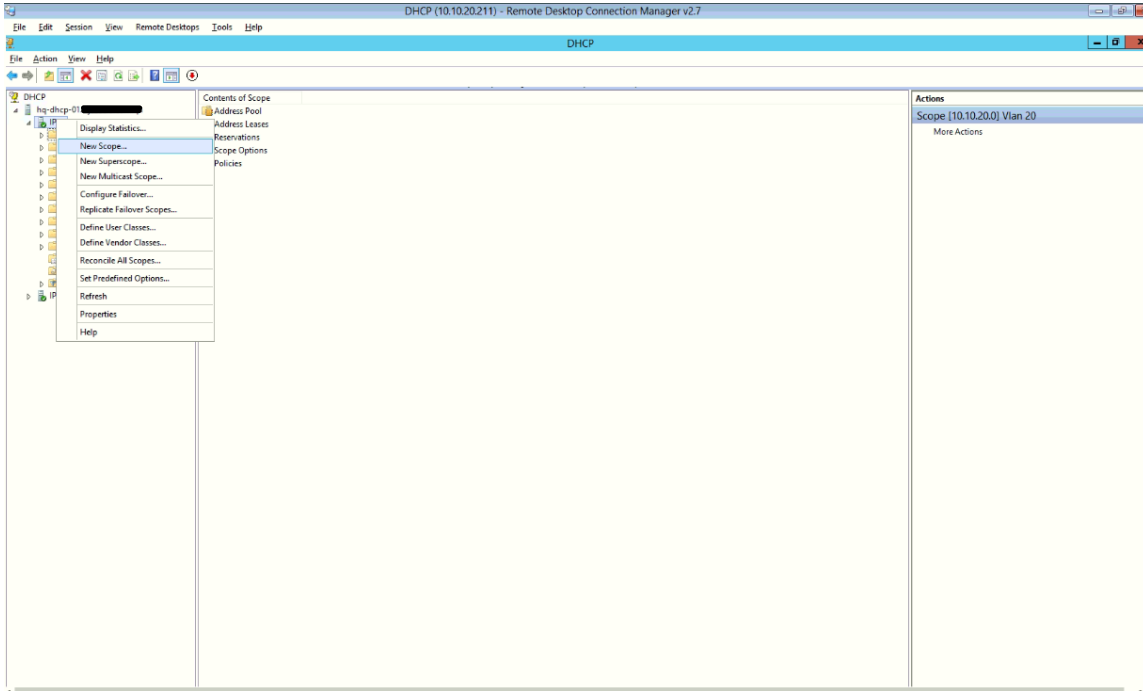
```
option 43 hex f108c0a80a05c0a80a14
```

Our second choice for implementation will be Microsoft Windows Server 2012 R2.

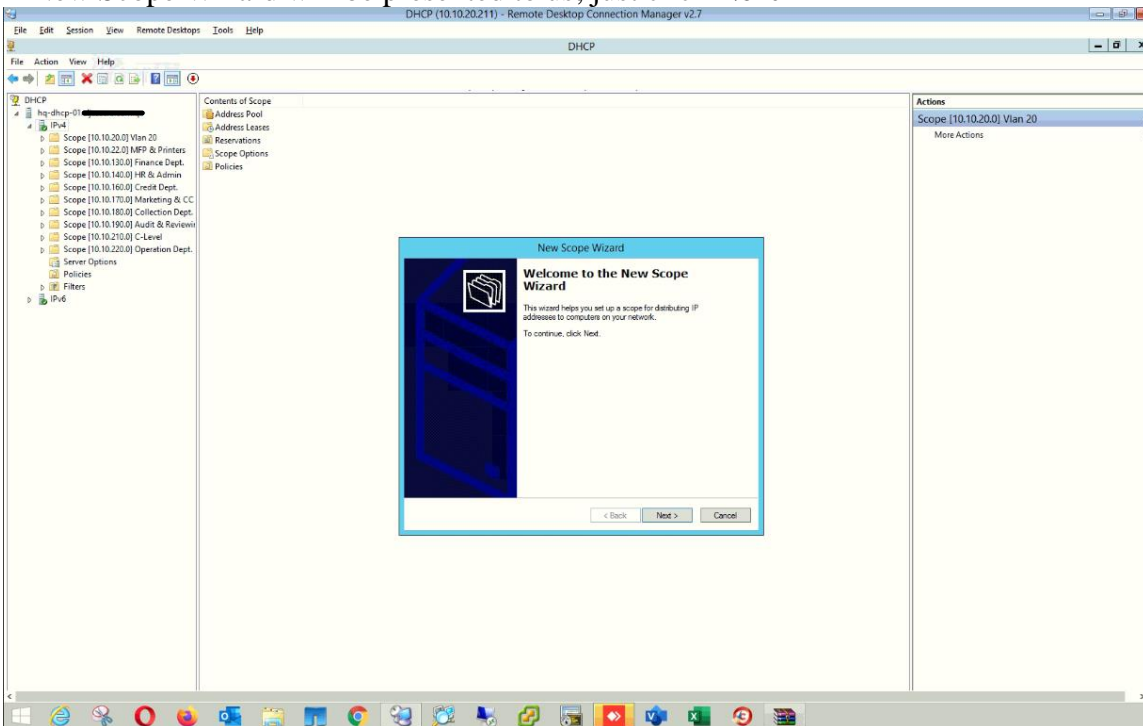
1. Below, I have a production DHCP server already set in place. There are existing IPv4 address scopes defined since this server is catering to several VLANs.



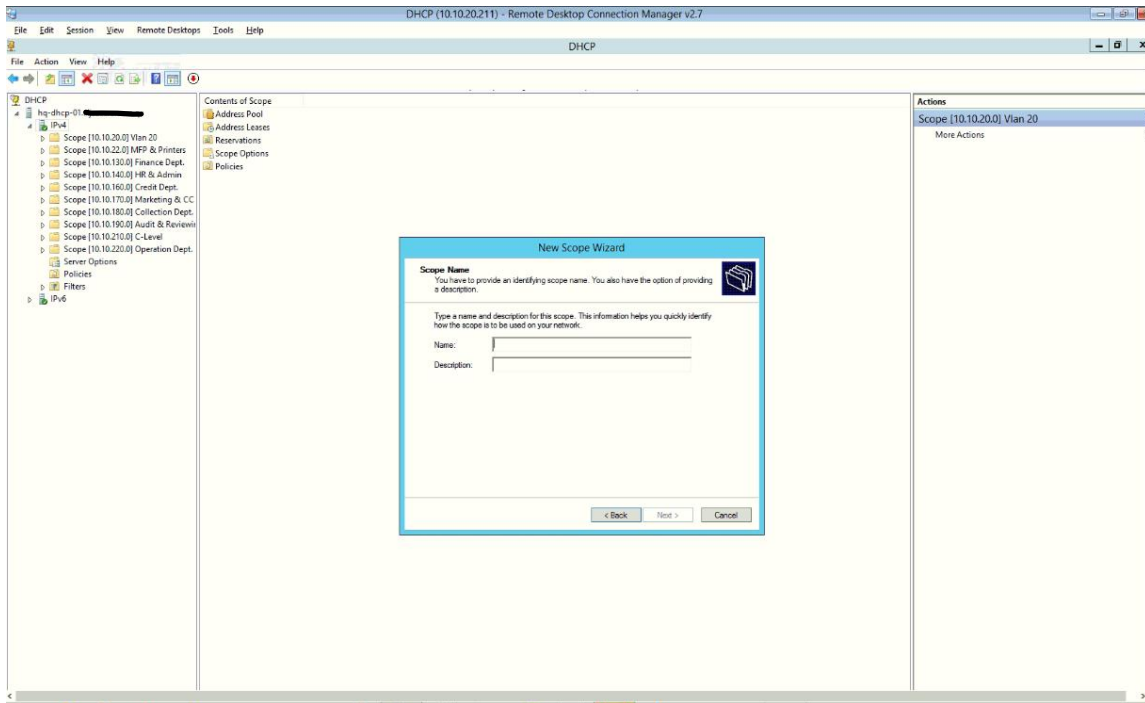
2. Since we will be creating IPv4 Address Scope, Right-click under **IPv4** and Select **New Scope**.



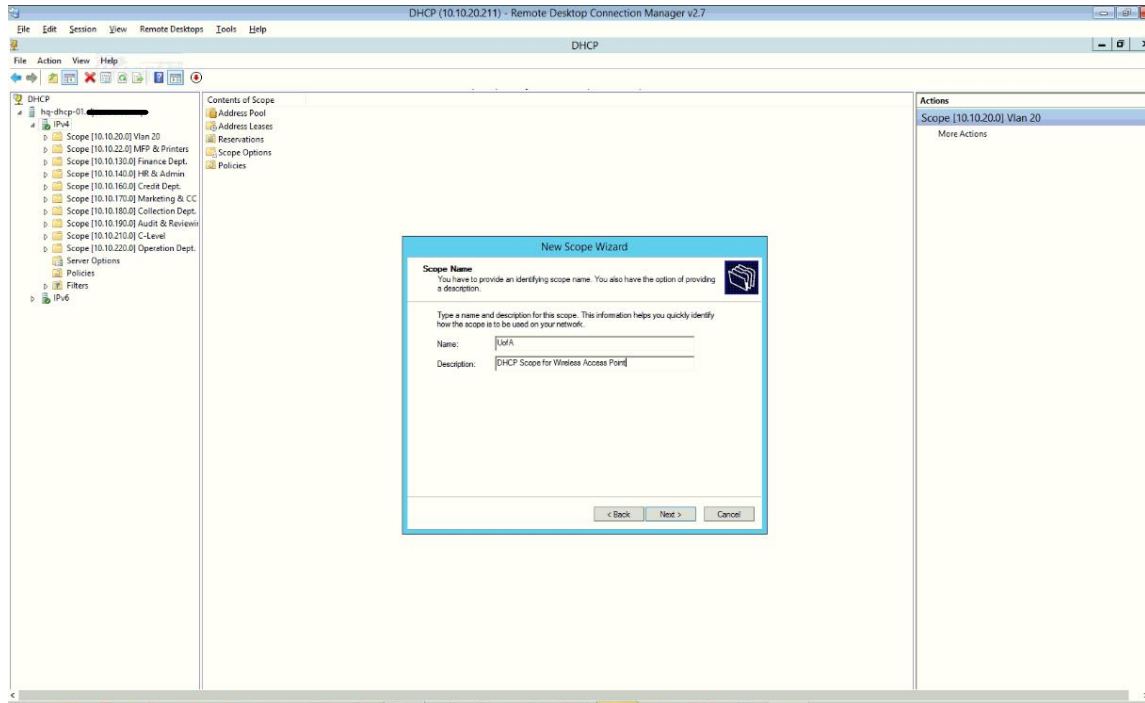
3. New Scope Wizard will be presented to us; just click **Next**



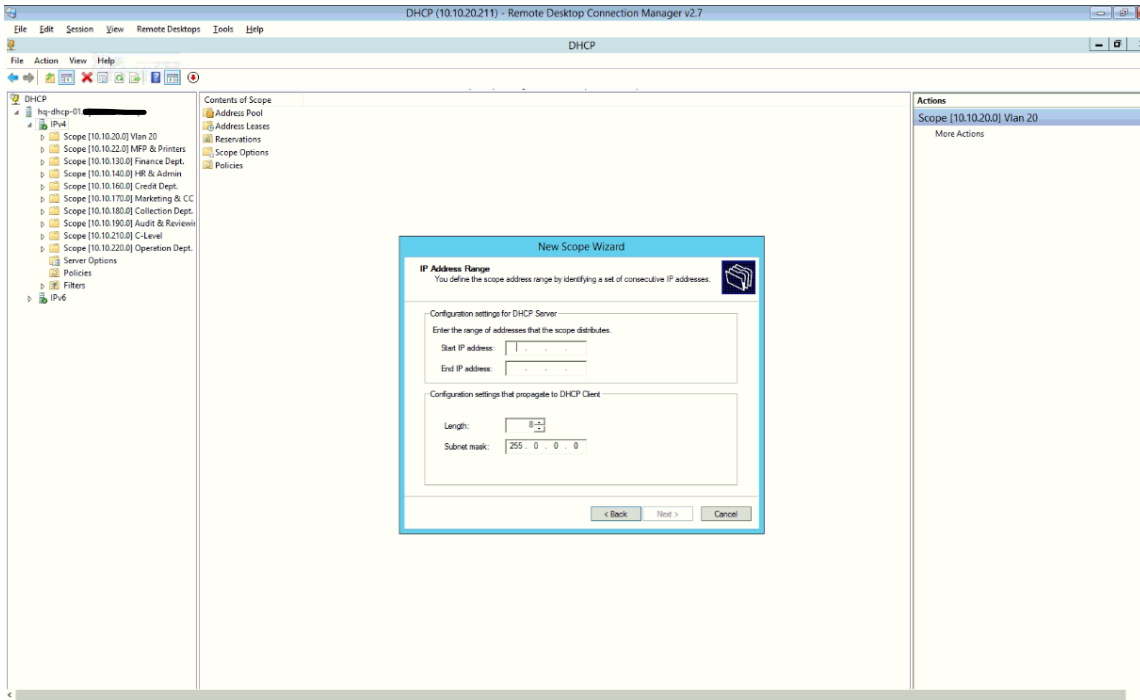
4. We need to define the **Scope Name** and **Description**, which is optional.



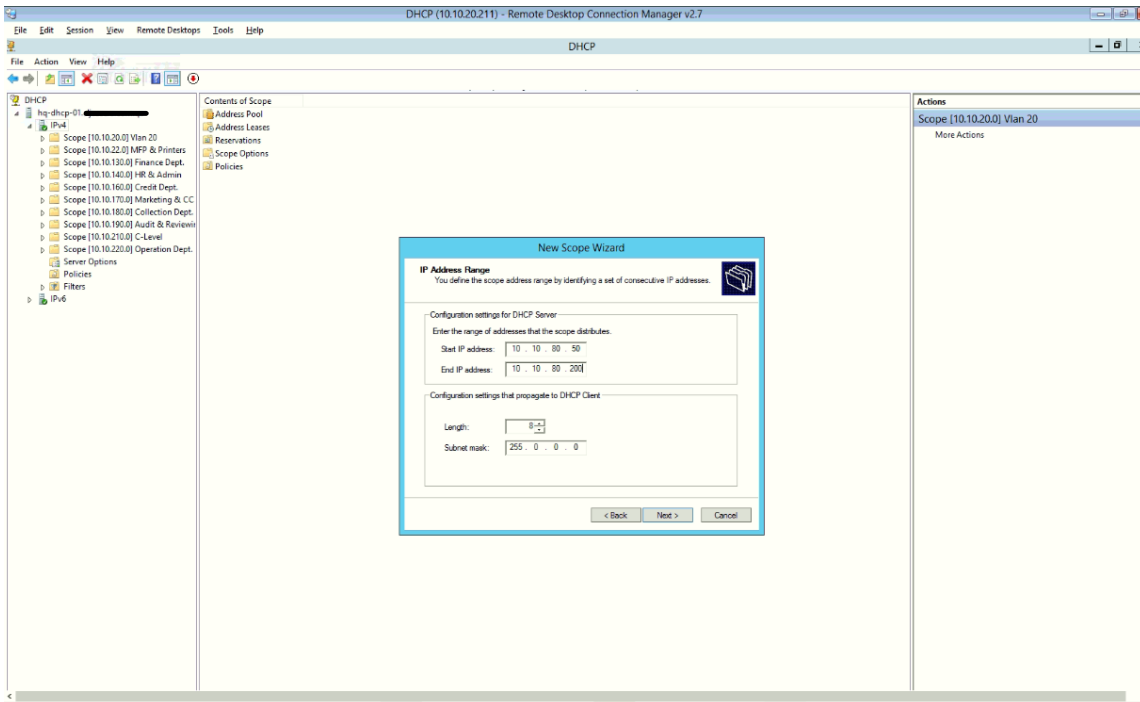
5. I have given the scope name as **UofA** and description as seen below



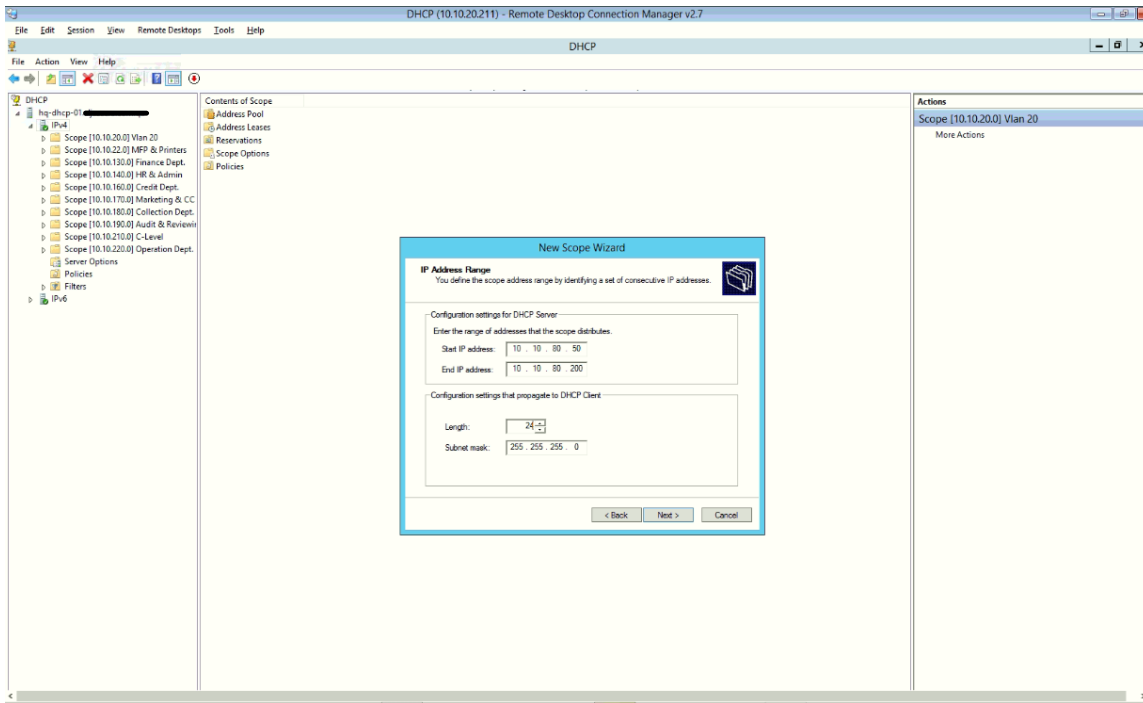
6. The primary information is the **IP Address Range**



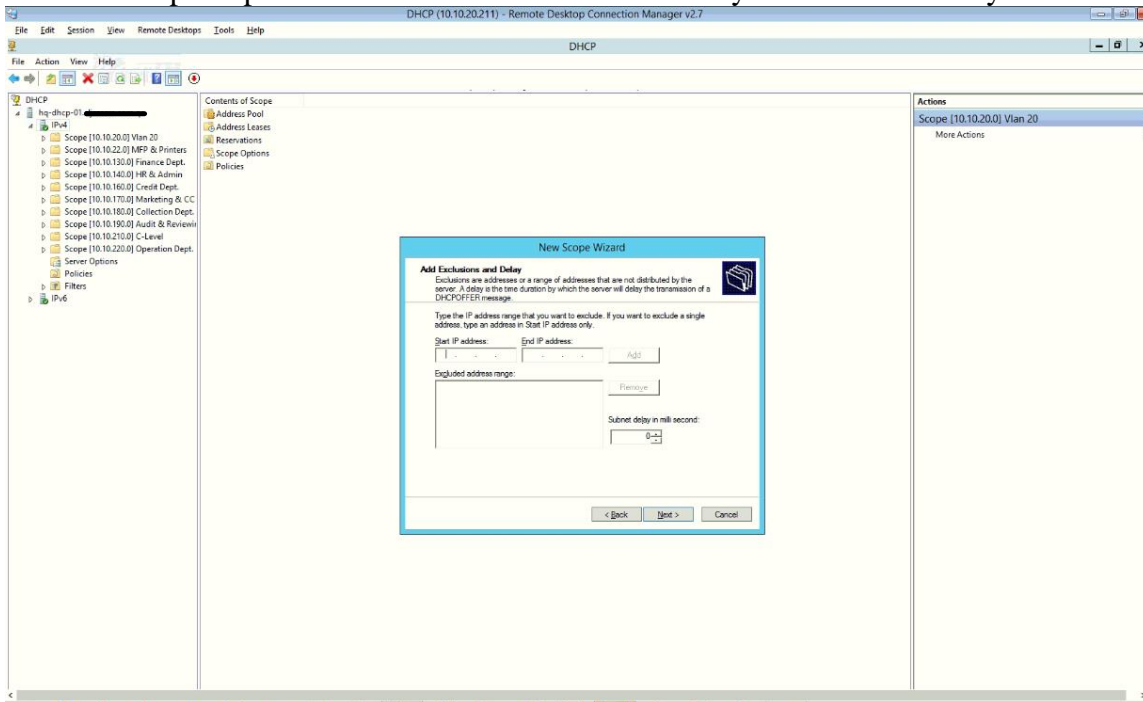
7. Here, I have filled the IP address starting from **10.10.80.50** until **10.10.80.200**



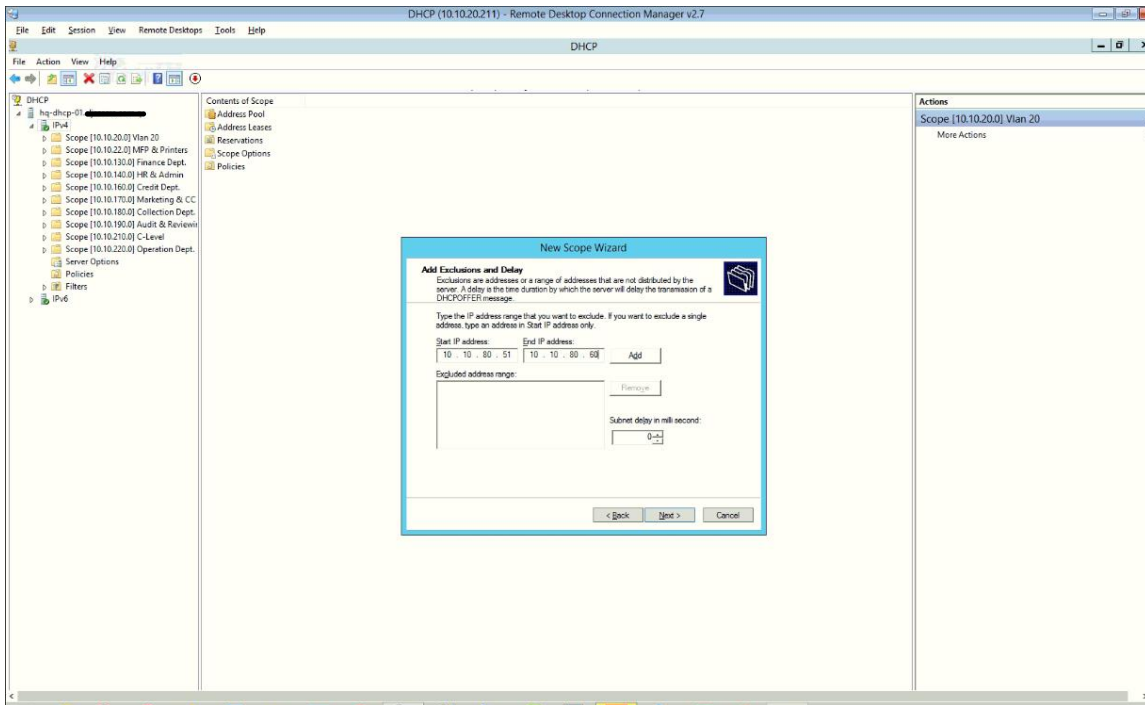
8. We need to define the subnet mask; in our scenario, we will choose /24 – 255.255.255.0



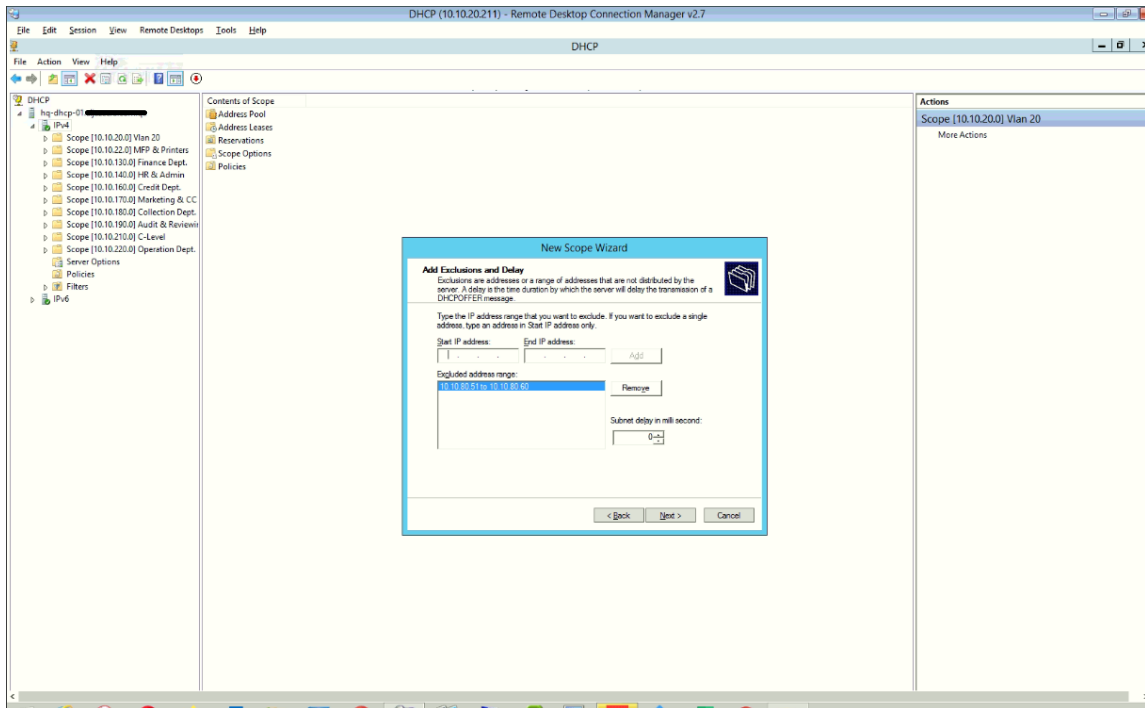
9. The next option presented to us is if we need to add any exclusions or delays.



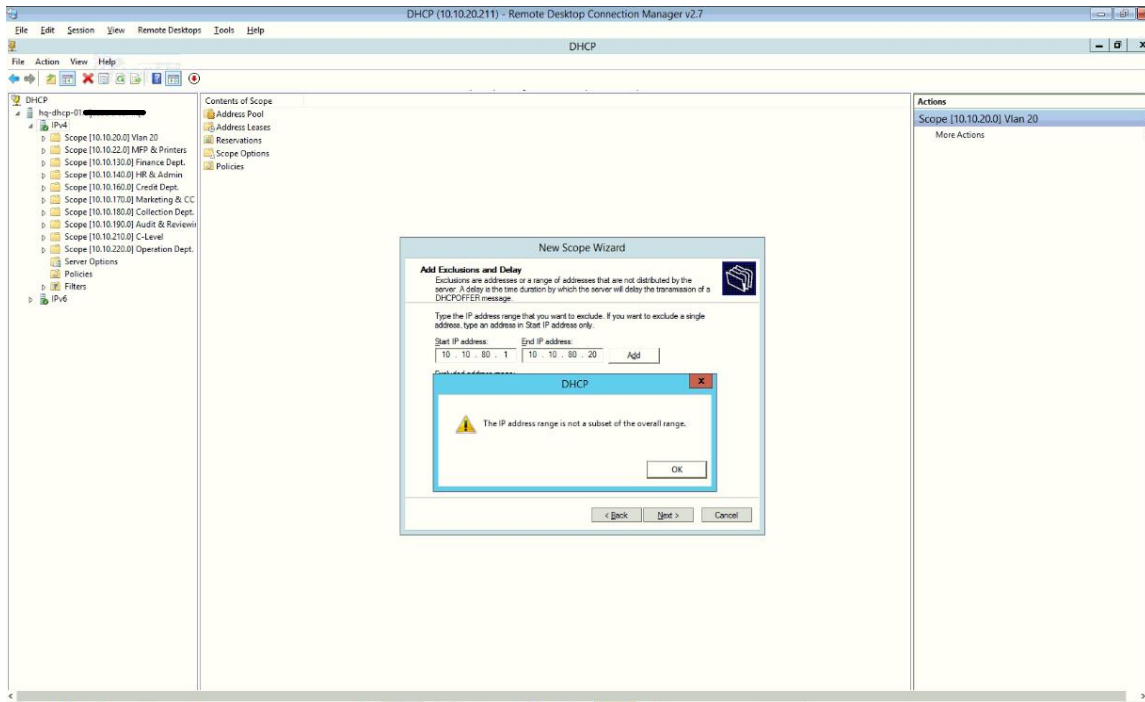
10. I will exclude the IP address from **10.10.80.51** to **10.10.80.60**



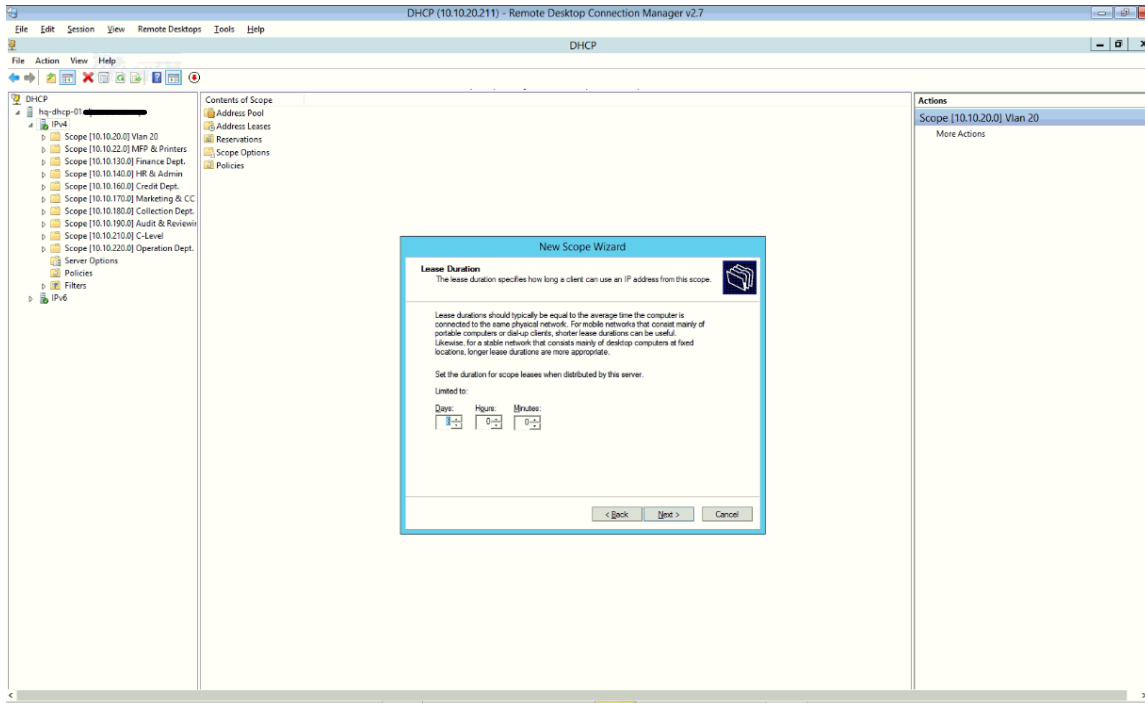
11. Clicking on **Add** will finalize these IP addresses for exclusion.



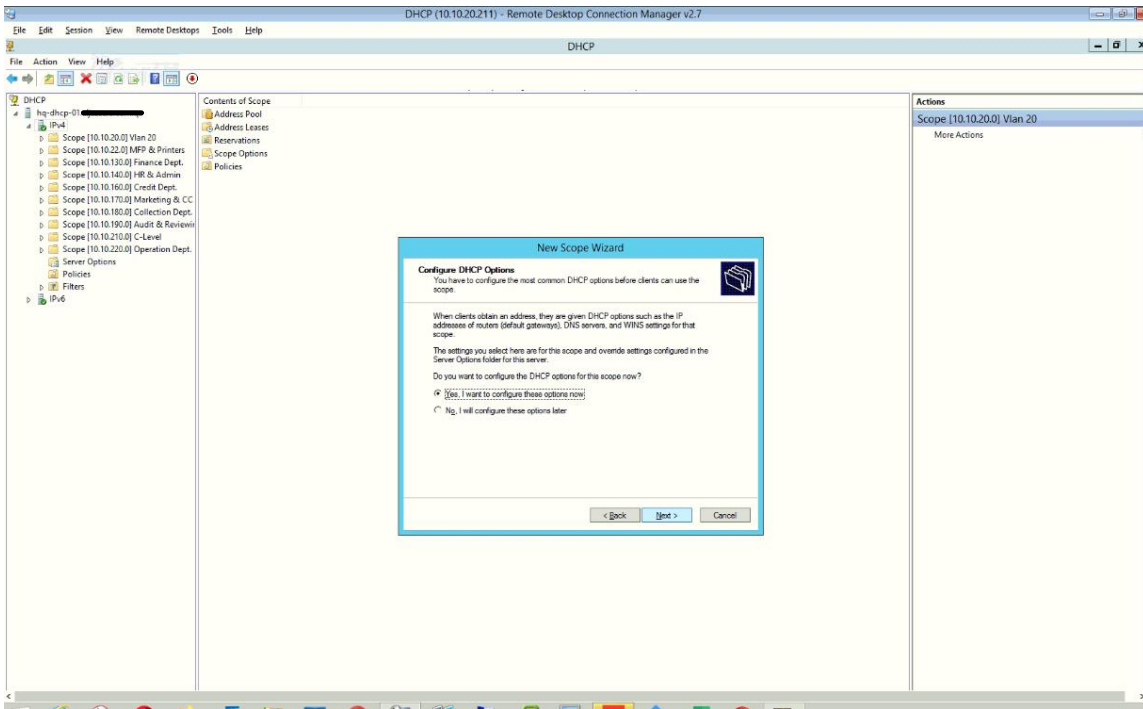
12. If you specify an IP address range for exclusion outside the specific IP address range, it will show an error as below.



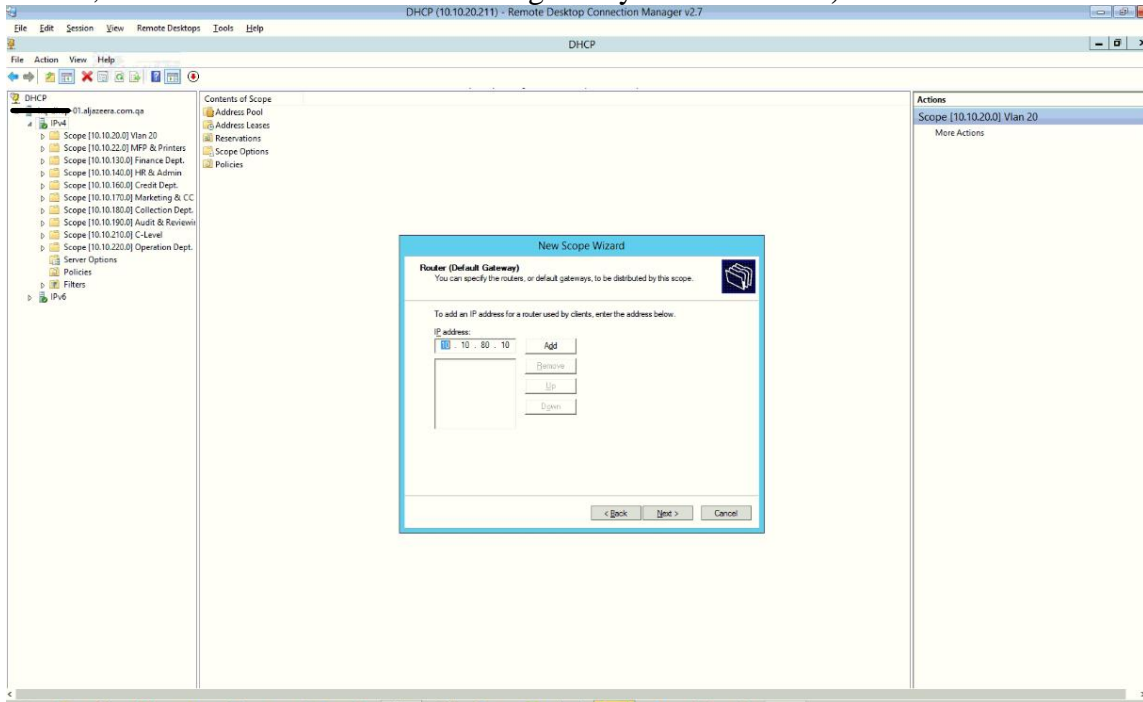
13. The Lease duration will be kept as default, which is **eight days**.



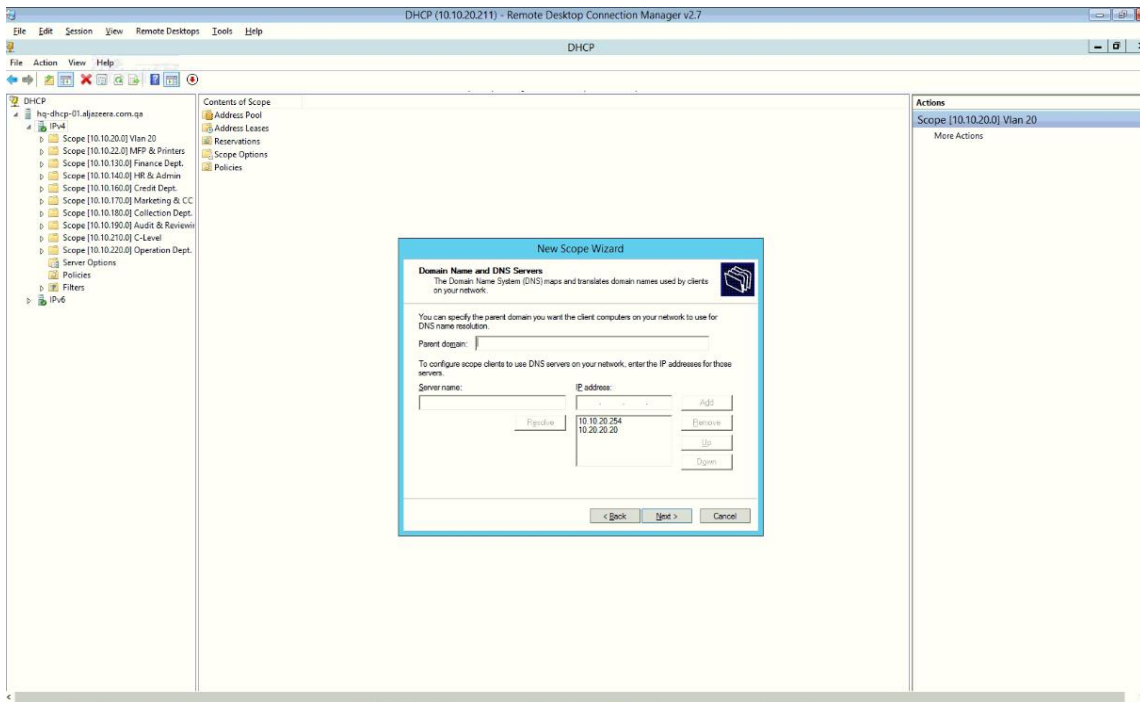
14. We want our lightweight access point to receive additional options such default gateway for reaching the WLAN controller on the Cloud because it is in another subnet. Hence, we will configure the options now.



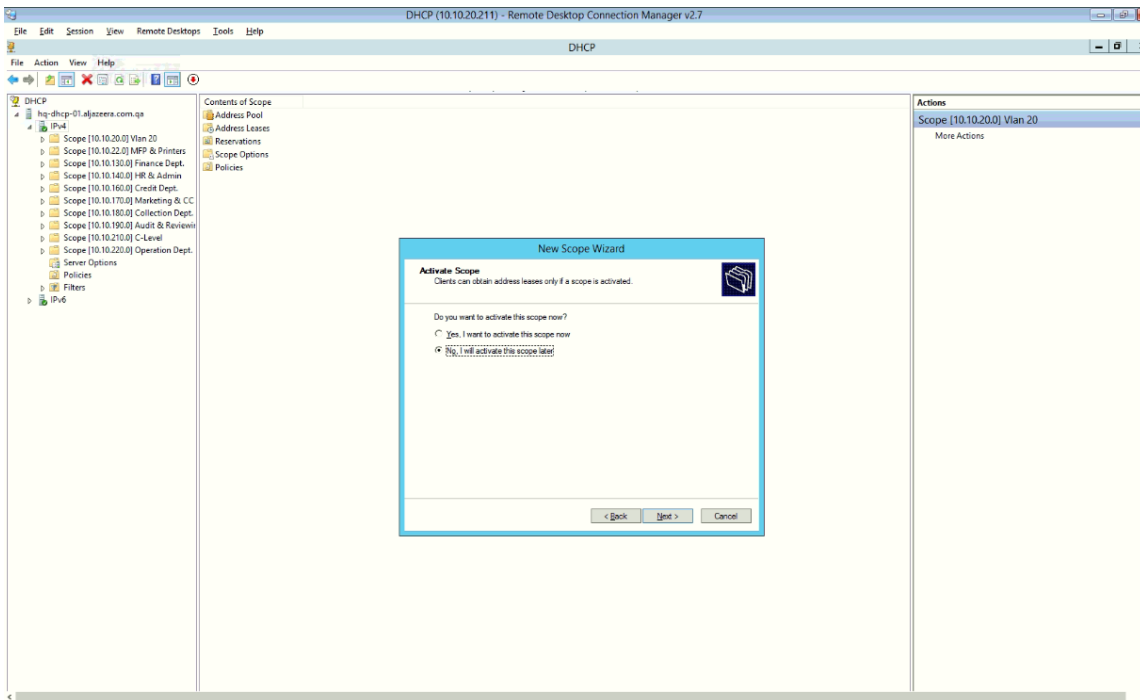
15. Here, we will define the default router/gateway as **10.10.80.10**, which is the core switch.



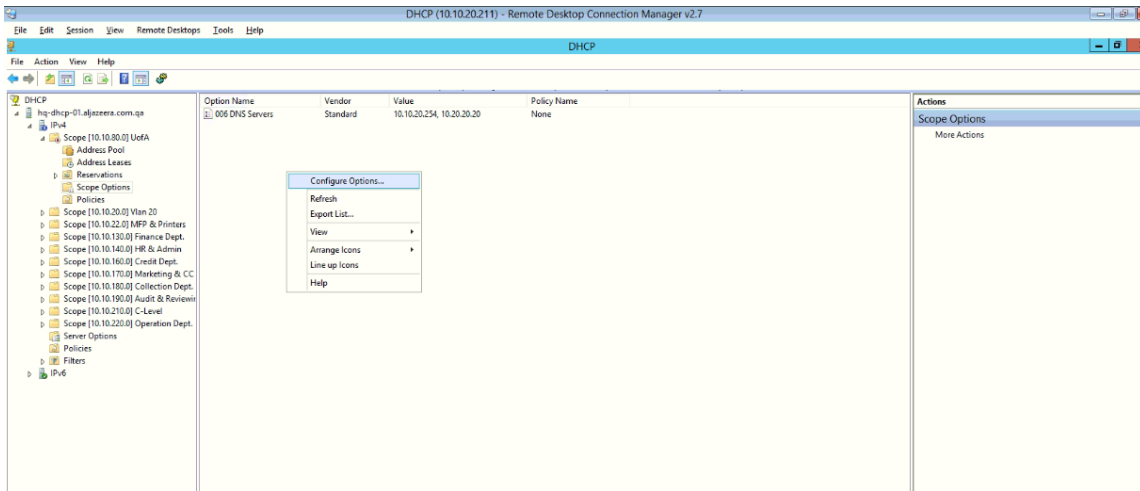
16. We will leave the Option for DNS as default.



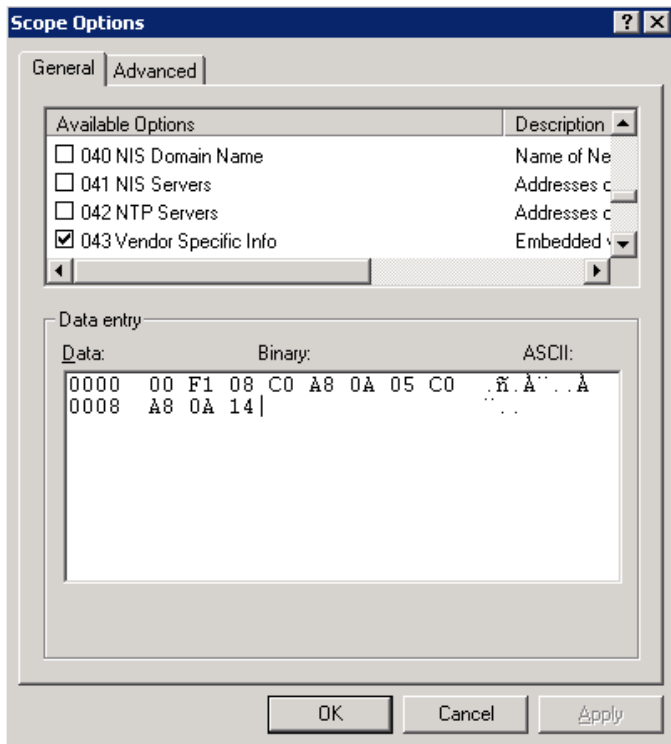
17. We will not activate the scope because we must assign another important option before distributing the IP addresses.



18. After the scope is created, we can navigate to **Scope Options** and right-click to select **Configure Options**

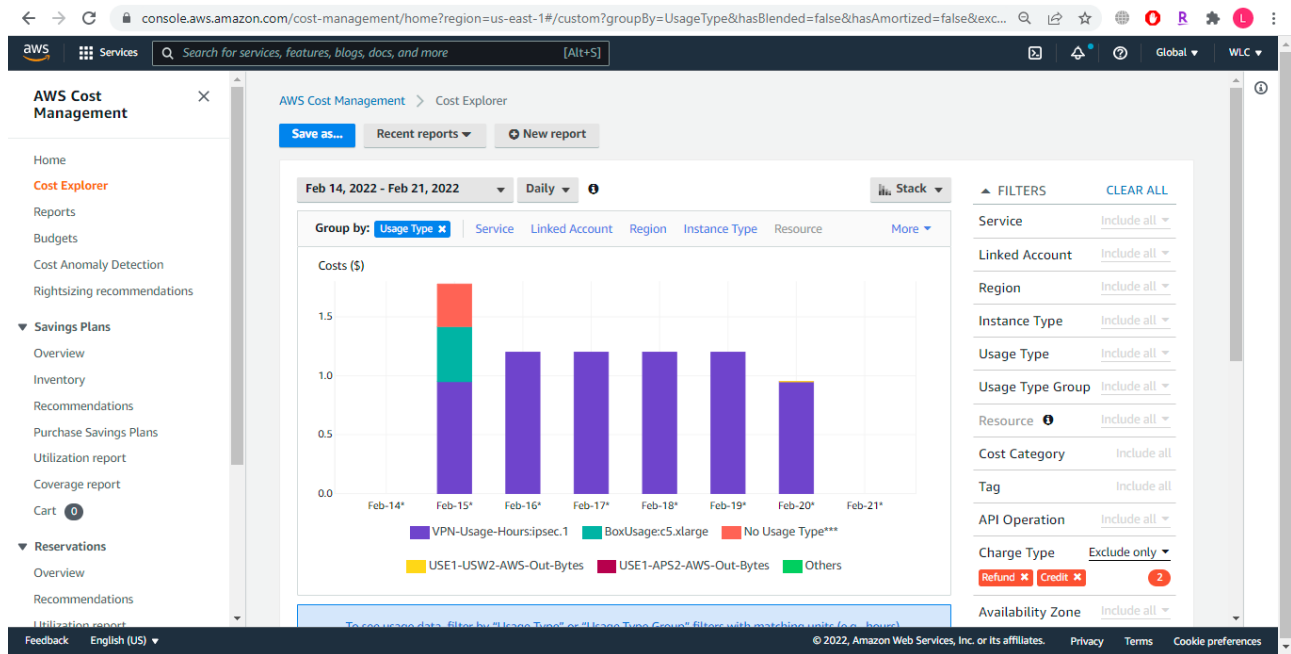


19. Scroll down to option **043 Vendor Specific Info**; here, we will have to enter the Hex value as discussed while configuring the Cisco DHCP server. [46]



The cost associated with AWS Cloud

The primary thing to consider in case of migrating to the Cloud environment is understanding the cost associated with it. In our case, we will see the last one-week cost incurred as shown below-



We can also download the minute information of the cost incurred.

The screenshot shows the AWS Cost Explorer interface with a table of usage data. The table includes columns for Usage Type, Feb-14*, Feb-15*, and Feb-16*. The y-axis represents Costs (\$) from 0.00 to 1.20. The legend includes USE1-USW2-AWS-Out-Bytes, USE1-AP52-AWS-Out-Bytes, and Others.

Usage Type	Feb-14*	Feb-15*	Feb-16*
Total cost (\$)	0.00	1.78	1.20
VPN-Usage-Hours:i...		0.95	1.20
BoxUsage:c5.xlarge (\$)		0.47	
USE1-USW2-AWS-Out... (\$)		0.00	0.00
USE1-AP52-AWS-Out... (\$)		0.00	0.00
USE1-EUC1-AWS-Out... (\$)		0.00	0.00
USE1-EUW3-AWS-Out... (\$)		0.00	0.00

Configuration Lines

Since we worked on a live production environment, the configuration will contain some additional lines which are not relevant to our scenarios. But I have kept it to understand how networking works in an enterprise environment. Sensitive information has been hidden from the configuration for privacy concerns.

On-Premise Core Switch – Cisco 4500X with VSS

```
Current configuration: 18678 bytes
!
version 15.2
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service compress-config
!
hostname HQ-XXX-DIST-SW
!
boot-start-marker
boot system flash bootflash:cat4500e-universalk9.SPA.03.07.02.E.152-3.E2.bin
boot-end-marker
!
vrf definition mgmtVrf
!
  address-family ipv4
  exit-address-family
!
  address-family ipv6
  exit-address-family
!
no aaa new-model
clock timezone QTR 3 0
!
switch virtual domain 100
  switch mode virtual
  mac-address use-virtual
!
no ip gratuitous-arps
!
ip vrf Liin-vrf
!
ip domain-name *****
ip name-server 8.8.8.8
!
power redundancy-mode redundant
!
mac access-list extended VSL-BPDU
  permit any 0180.c200.0000 0000.0000.0003
```

```

mac access-list extended VSL-CDP
  permit any host 0100.0ccc.cccc
mac access-list extended VSL-DOT1x
  permit any any 0x888E
mac access-list extended VSL-GARP
  permit any host 0180.c200.0020
mac access-list extended VSL-LLDP
  permit any host 0180.c200.000e
mac access-list extended VSL-MGMT
  permit any 0022.bdcd.d200 0000.0000.00ff
  permit 0022.bdcd.d200 0000.0000.00ff any
mac access-list extended VSL-SSTP
  permit any host 0100.0ccc.cccc
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1-250 priority 0
!
redundancy
  mode sso
!
vlan internal allocation policy ascending
!
class-map match-any VSL-MGMT-PACKETS
  match access-group name VSL-MGMT
class-map match-any VSL-DATA-PACKETS
  match any
class-map match-any VSL-L2-CONTROL-PACKETS
  match access-group name VSL-DOT1x
  match access-group name VSL-BPDU
  match access-group name VSL-CDP
  match access-group name VSL-LLDP
  match access-group name VSL-SSTP
  match access-group name VSL-GARP
class-map match-any VSL-L3-CONTROL-PACKETS
  match access-group name VSL-IPV4-ROUTING
  match access-group name VSL-BFD
  match access-group name VSL-DHCP-CLIENT-TO-SERVER
  match access-group name VSL-DHCP-SERVER-TO-CLIENT
  match access-group name VSL-DHCP-SERVER-TO-SERVER
  match access-group name VSL-IPV6-ROUTING
class-map match-any VSL-MULTIMEDIA-TRAFFIC
  match dscp af41
  match dscp af42
  match dscp af43
  match dscp af31
  match dscp af32
  match dscp af33
  match dscp af21
  match dscp af22
  match dscp af23
class-map match-any VSL-VOICE-VIDEO-TRAFFIC
  match dscp ef

```

```

    match dscp cs4
    match dscp cs5
class-map match-any VSL-SIGNALING-NETWORK-MGMT
    match dscp cs2
    match dscp cs3
    match dscp cs6
    match dscp cs7
!
policy-map VSL-Queuing-Policy
class VSL-MGMT-PACKETS
    bandwidth percent 5
class VSL-L2-CONTROL-PACKETS
    bandwidth percent 5
class VSL-L3-CONTROL-PACKETS
    bandwidth percent 5
class VSL-VOICE-VIDEO-TRAFFIC
    bandwidth percent 30
class VSL-SIGNALING-NETWORK-MGMT
    bandwidth percent 10
class VSL-MULTIMEDIA-TRAFFIC
    bandwidth percent 20
class VSL-DATA-PACKETS
    bandwidth percent 20
class class-default
    bandwidth percent 5
!
interface Port-channel11
description HQ-11-DIST-SW -x- HQ-12-ACC-SW-1
switchport
switchport mode trunk
!
interface Port-channel12
description HQ-11-DIST-SW -x- HQ-12-ACC-SW-2
switchport
switchport mode trunk
!
interface Port-channel13
description HQ-11-DIST-SW -x- HQ-12-ACC-SW-3
switchport
switchport mode trunk
!
interface Port-channel14
description HQ-11-DIST-SW -x- HQ-12-ACC-SW-4
switchport
switchport mode trunk
!
interface Port-channel15
description HQ-11-DIST-SW -x- HQ-12-ACC-SW-5
switchport
switchport mode trunk
!
interface Port-channel16
description HQ-11-DIST-SW -x- HQ-12-ACC-SW-6

```



```

switchport
switchport mode trunk
!
interface Port-channel17
description HQ-11-DIST-SW -x- HQ-13-ACC-SW-7
switchport
switchport mode trunk
!
interface Port-channel18
description HQ-11-DIST-SW -x- HQ-21-ACC-SW-1
switchport
switchport mode trunk
!
interface Port-channel19
description HQ-11-DIST-SW -x- HQ-02-ACC-SW-1
switchport
switchport mode trunk
!
interface Port-channel20
description HQ-11-DIST-SW -x- HQ-01-ACC-SW-1
switchport
switchport mode trunk
!
interface Port-channel21
description HQ-11-DIST-SW -x- HQ-18-IPTV-SW-1
switchport
switchport mode trunk
!
interface Port-channel22
description HQ-11-DIST-SW -x- HQ-13-SRV-SW-1
switchport
switchport mode trunk
!
interface Port-channel23
description HQ-11-DIST-SW -x- HQ-13-SRV-SW-2
switchport
switchport mode trunk
!
interface Port-channel63
switchport
switch virtual link 1
!
interface Port-channel64
switchport
switch virtual link 2
!
interface FastEthernet1
vrf forwarding mgmtVrf
no ip address
speed auto
duplex auto
!
interface TenGigabitEthernet1/1/1

```

```

no lldp transmit
no lldp receive
channel-group 63 mode on
service-policy output VSL-Queuing-Policy
!
interface TenGigabitEthernet1/1/2
description HQ-11-DIST-SW-1 -x- HQ-11-DIST-SW-2 (fast-hello)
dual-active fast-hello
!
interface TenGigabitEthernet1/1/3
description HQ-11-DIST-SW-1 -x- HQ-12-ACC-SW-1
switchport mode trunk
channel-group 11 mode active
!
interface TenGigabitEthernet1/1/4
description HQ-11-DIST-SW-1 -x- HQ-12-ACC-SW-2
switchport mode trunk
channel-group 12 mode active
!
interface TenGigabitEthernet1/1/5
description HQ-11-DIST-SW-1 -x- HQ-12-ACC-SW-3
switchport mode trunk
channel-group 13 mode active
!
interface TenGigabitEthernet1/1/6
description HQ-11-DIST-SW-1 -x- HQ-12-ACC-SW-4
switchport mode trunk
channel-group 14 mode active
!
interface TenGigabitEthernet1/1/7
description HQ-11-DIST-SW-1 -x- HQ-12-ACC-SW-5
switchport mode trunk
channel-group 15 mode active
!
interface TenGigabitEthernet1/1/8
description HQ-11-DIST-SW-1 -x- HQ-12-ACC-SW-6
switchport mode trunk
channel-group 16 mode active
!
interface TenGigabitEthernet1/1/9
description HQ-11-DIST-SW-1 -x- HQ-12-ACC-SW-7
switchport mode trunk
channel-group 17 mode active
!
interface TenGigabitEthernet1/1/10
description HQ-11-DIST-SW-1 -x- HQ-21-ACC-SW-1
switchport mode trunk
channel-group 18 mode active
!
interface TenGigabitEthernet1/1/11
description HQ-11-DIST-SW-1 -x- HQ-02-ACC-SW-1
switchport mode trunk
channel-group 19 mode active

```

```

!
interface TenGigabitEthernet1/1/12
  description HQ-11-DIST-SW-1 -x- HQ-01-ACC-SW-1
  switchport mode trunk
  channel-group 20 mode active
!
interface TenGigabitEthernet1/1/13
  description HQ-11-DIST-SW-1 -x- HQ-18-IPTV-SW-1
  switchport mode trunk
  channel-group 21 mode active
!
interface TenGigabitEthernet1/1/14
  description HQ-11-DIST-SW -x- HQ-14-CCTV-DIST-SW-1
  switchport mode trunk
!
interface TenGigabitEthernet1/1/15
  description HQ-11-DIST-SW-1 -x- HQ-11-ASA-1 (Context 1)
  switchport access vlan 50
  switchport mode access
  spanning-tree portfast
!
interface TenGigabitEthernet1/1/16
  description HQ-11-DIST-SW-1 -x- HQ-11-ASA-1 (Context 2)
  switchport access vlan 60
  switchport mode access
  spanning-tree portfast
!
interface TenGigabitEthernet1/2/1
!
interface TenGigabitEthernet1/2/2
!
interface TenGigabitEthernet1/2/3
  description HQ-11-DIST-SW -x- HQ-13-SRV-SW-1
  switchport mode trunk
  channel-group 22 mode active
!
interface TenGigabitEthernet1/2/4
  description HQ-11-DIST-SW -x- HQ-13-SRV-SW-2
  switchport mode trunk
  channel-group 23 mode active
!
interface TenGigabitEthernet1/2/5
!
interface TenGigabitEthernet1/2/6
!
interface TenGigabitEthernet1/2/7
!
interface TenGigabitEthernet1/2/8
!
interface TenGigabitEthernet2/1/1
  no lldp transmit
  no lldp receive
  channel-group 64 mode on

```

```

service-policy output VSL-Queuing-Policy
!
interface TenGigabitEthernet2/1/2
description HQ-11-DIST-SW-1 -x- HQ-11-DIST-SW-2 (fast-hello)
dual-active fast-hello
!
interface TenGigabitEthernet2/1/3
description HQ-11-DIST-SW-2 -x- HQ-12-ACC-SW-1
switchport mode trunk
channel-group 11 mode active
!
interface TenGigabitEthernet2/1/4
description HQ-11-DIST-SW-2 -x- HQ-12-ACC-SW-2
switchport mode trunk
channel-group 12 mode active
!
interface TenGigabitEthernet2/1/5
description HQ-11-DIST-SW-2 -x- HQ-12-ACC-SW-3
switchport mode trunk
channel-group 13 mode active
!
interface TenGigabitEthernet2/1/6
description HQ-11-DIST-SW-2 -x- HQ-12-ACC-SW-4
switchport mode trunk
channel-group 14 mode active
!
interface TenGigabitEthernet2/1/7
description HQ-11-DIST-SW-2 -x- HQ-12-ACC-SW-5
switchport mode trunk
channel-group 15 mode active
!
interface TenGigabitEthernet2/1/8
description HQ-11-DIST-SW-2 -x- HQ-12-ACC-SW-6
switchport mode trunk
channel-group 16 mode active
!
interface TenGigabitEthernet2/1/9
description HQ-11-DIST-SW-2 -x- HQ-12-ACC-SW-7
switchport mode trunk
channel-group 17 mode active
!
interface TenGigabitEthernet2/1/10
description HQ-11-DIST-SW-2 -x- HQ-21-ACC-SW-1
switchport mode trunk
channel-group 18 mode active
!
interface TenGigabitEthernet2/1/11
description HQ-11-DIST-SW-2 -x- HQ-02-ACC-SW-1
switchport mode trunk
channel-group 19 mode active
!
interface TenGigabitEthernet2/1/12
description HQ-11-DIST-SW-2 -x- HQ-01-ACC-SW-1

```

```

switchport mode trunk
channel-group 20 mode active
!
interface TenGigabitEthernet2/1/13
description HQ-11-DIST-SW-2 -x- HQ-18-IPTV-SW-1
switchport mode trunk
channel-group 21 mode active
!
interface TenGigabitEthernet2/1/14
switchport trunk native vlan 20
switchport mode trunk
!
interface TenGigabitEthernet2/1/15
description HQ-11-DIST-SW-2 -x- HQ-11-ASA-1 (Context 1)
switchport access vlan 50
switchport mode access
spanning-tree portfast
!
interface TenGigabitEthernet2/1/16
description HQ-11-DIST-SW-2 -x- HQ-11-ASA-1 (Context 2)
switchport access vlan 60
switchport mode access
spanning-tree portfast
!
interface TenGigabitEthernet2/2/1
!
interface TenGigabitEthernet2/2/2
!
interface TenGigabitEthernet2/2/3
description HQ-11-DIST-SW -x- HQ-13-SRV-SW-1
switchport mode trunk
channel-group 22 mode active
!
interface TenGigabitEthernet2/2/4
description HQ-11-DIST-SW -x- HQ-13-SRV-SW-2
switchport mode trunk
channel-group 23 mode active
!
interface TenGigabitEthernet2/2/5
!
interface TenGigabitEthernet2/2/6
!
interface TenGigabitEthernet2/2/7
!
interface TenGigabitEthernet2/2/8
!
interface Vlan1
description DATA
ip address 192.168.10.10 255.255.255.0
!
interface Vlan10
description VOICE
ip address 172.16.10.250 255.255.255.0

```

```

!
interface Vlan11
 ip address 10.10.11.10 255.255.255.0
!
interface Vlan18
 ip address 10.18.18.10 255.255.255.0
!
interface Vlan20
 description DATA-NEW
 ip address 10.10.20.10 255.255.255.0
!
interface Vlan22
 description Printers
 ip address 10.10.22.10 255.255.255.0
!
interface Vlan40
 ip address 10.10.40.10 255.255.255.0
!
interface Vlan50
 description ASA-Context-1-Inside
 ip address 10.10.50.254 255.255.255.0
!
interface Vlan60
 description ASA-Context-2-Inside
 ip address 10.10.60.254 255.255.255.0
!
interface Vlan80
 description AWS AP
 ip address 10.10.80.10 255.255.255.0
!
interface Vlan90
 ip address 10.10.90.10 255.255.255.0
!
interface Vlan100
 description CCTV
 ip address 10.10.100.11 255.255.255.0
!
interface Vlan110
 ip address 10.10.110.254 255.255.255.0
!
interface Vlan130
 description Finance
 ip address 10.10.130.10 255.255.255.0
 ip helper-address 10.10.20.211
!
interface Vlan140
 description HR-Admin
 ip address 10.10.140.10 255.255.255.0
 ip helper-address 10.10.20.211
!
interface Vlan150
 description IPTV
 ip address 10.10.150.10 255.255.255.0

```

```

!
interface Vlan160
  description Credit
  ip address 10.10.160.10 255.255.255.0
  ip helper-address 10.10.20.211
!
interface Vlan170
  description Marketing-CC-OS
  ip address 10.10.170.10 255.255.255.0
  ip helper-address 10.10.20.211
!
interface Vlan180
  description Collection
  ip address 10.10.180.10 255.255.255.0
  ip helper-address 10.10.20.211
!
interface Vlan190
  description Audit-Review
  ip address 10.10.190.10 255.255.255.0
  ip helper-address 10.10.20.211
!
interface Vlan199
  description MGMT
  ip address 10.10.199.10 255.255.255.0
!
interface Vlan200
  description ENV MON
  ip address 10.10.200.10 255.255.255.0
  ip policy route-map TEST
!
interface Vlan201
  description PDU
  ip address 10.10.201.10 255.255.255.0
!
interface Vlan210
  description C-Level
  ip address 10.10.210.10 255.255.255.0
  ip helper-address 10.10.20.211
!
interface Vlan220
  description Operation
  ip address 10.10.220.10 255.255.255.0
  ip helper-address 10.10.20.211
!
ip forward-protocol nd
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.10.50.1
ip route 172.31.0.0 255.255.0.0 10.10.60.1
!
ip access-list extended VSL-BFD
  permit udp any any eq 3784
ip access-list extended VSL-DHCP-CLIENT-TO-SERVER

```



```

    permit udp any eq bootpc any eq bootps
ip access-list extended VSL-DHCP-SERVER-TO-CLIENT
    permit udp any eq bootps any eq bootpc
ip access-list extended VSL-DHCP-SERVER-TO-SERVER
    permit udp any eq bootps any eq bootps
ip access-list extended VSL-IPV4-ROUTING
    permit ip any 224.0.0.0 0.0.0.255
!
ipv6 access-list VSL-IPV6-ROUTING
    permit ipv6 any FF02::/124
!
banner motd ^CCC
=====
                This device is property of XXX!
                Unauthorized access prohibited !
                Device name: HQ-11-DIST-SW
                Device description: Midmac DC Core/Distribution Switch
=====
^C
!
line con 0
    exec-timeout 0 5
    login local
    stopbits 1
line vty 0 4
    exec-timeout 0 0
    login local
    transport input ssh
line vty 5 15
    exec-timeout 0 5
    login local
    transport input ssh
!
module provision switch 1
    chassis-type 70 base-mac 70E4.22C6.5240
    slot 1 slot-type 401 base-mac 70E4.22C6.5240
    slot 2 slot-type 400 base-mac B0AA.777D.4C10
!
module provision switch 2
    chassis-type 70 base-mac 70E4.22C6.F400
    slot 1 slot-type 401 base-mac 70E4.22C6.F400
    slot 2 slot-type 400 base-mac A0EC.F9E2.B798
!
    ntp server asia.pool.ntp.org source Vlan50
    ntp server pool.ntp.org minpoll 10 source Vlan50
end

```

Cisco 9800-CL Wireless LAN Controller on AWS Cloud

Current configuration : 17934 bytes
!

```

! Last configuration change at 22:58:09 AST Sun Feb 27 2022
!
version 17.6
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service call-home
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
platform console virtual
!
hostname UofA-C9800
!
boot-start-marker
boot-end-marker
!
logging persistent size 1000000 filesize 8192 immediate
!
no aaa new-model
clock timezone AST 0 0
clock calendar-valid
vtp mode off
!
login on-success log
!
subscriber templating
!
parameter-map type webauth global
  virtual-ip ipv4 192.0.2.1
!
access-session mac-move deny
multilink bundle-name authenticated
!
crypto pki server WLC_CA
  database archive pkcs12 password 7 *****
  issuer-name O=Cisco Virtual Wireless LAN Controller, CN=CA-vWLC_UofA-C9800
  grant auto
  hash sha1
  lifetime certificate 3652
  lifetime ca-certificate 3652
!
crypto pki trustpoint TP-self-signed-2583802388
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-2583802388
  revocation-check none
  rsakeypair TP-self-signed-2583802388
!
crypto pki trustpoint SLA-TrustPoint
  enrollment pkcs12
  revocation-check crl
!
crypto pki trustpoint WLC_CA
  revocation-check crl

```

```

  rsakeypair WLC_CA
!
crypto pki trustpoint UofA-C9800_WLC_TP
  enrollment url http://172.31.68.61:80
  serial-number
  password 7 *****
  subject-name O=Cisco Virtual Wireless LAN Controller, CN=UofA-C9800_WLC_TP
  revocation-check crl
  rsakeypair UofA-C9800_WLC_TP
  eku request server-auth client-auth
!
license udi pid C9800-CL-K9 sn 963CHHJOIJF
service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE
  linksec policy must-secure
service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
  linksec policy should-secure
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
  voice vlan
service-template DEFAULT_CRITICAL_DATA_TEMPLATE
service-template webauth-global-inactive
  inactivity-timer 3600
diagnostic bootup level minimal
memory free low-watermark processor 70663
!
username ec2-user privilege 15
username admin privilege 15 password 7 *****
!
redundancy
  mode sso
!
class-map match-any AVC-Reanchor-Class
  match protocol cisco-jabber-audio
  match protocol cisco-jabber-video
  match protocol webex-media
  match protocol webex-app-sharing
  match protocol webex-control
  match protocol webex-meeting
  match protocol wifi-calling
!
interface GigabitEthernet1
  ip address dhcp
  negotiation auto
  no mop enabled
  no mop sysid
!
interface Vlan1
  no ip address
  shutdown
  no mop enabled
  no mop sysid
!
ip forward-protocol nd
ip tcp window-size 8192

```

```

ip http server
ip http authentication local
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 GigabitEthernet1 172.31.64.1
ip ssh rsa keypair-name ssh-key
ip ssh version 2
ip ssh pubkey-chain
    username ec2-user
        key-hash ssh-rsa EF4AD462604083824796B78383D53C94 ec2-user
ip ssh server algorithm publickey ecdsa-sha2-nistp256 ecdsa-sha2-nistp384
ecdsa-sha2-nistp521 ssh-rsa x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-
nistp384 x509v3-ecdsa-sha2-nistp521
ip scp server enable
!
control-plane
!
line con 0
    stopbits 1
line vty 0 4
    login local
    length 0
    transport input ssh
line vty 5 20
    login local
    transport input ssh
!
call-home
    ! If contact email address in call-home is configured as sch-smart-
    licensing@cisco.com
    ! the email address configured in Cisco Smart License Portal will be used
    as contact email address to send SCH notifications.
    contact-email-addr sch-smart-licensing@cisco.com
    profile "CiscoTAC-1"
        active
        destination transport-method http
ntp server 10.10.80.10
!
wireless aaa policy default-aaa-policy
wireless cts-sxp profile default-sxp-profile
wireless management trustpoint UofA-C9800_WLC_TP
wireless management interface GigabitEthernet1
wireless profile airtime-fairness default-atf-policy 0
wireless profile flex default-flex-profile
    description "default flex profile"
wireless profile mesh default-mesh-profile
    description "default mesh profile"
wireless profile radio default-radio-profile
    description "Preconfigured default radio profile"
wireless profile policy default-policy-profile
    autoqos mode voice
    no central dhcp
    no central switching

```

```

description "default policy profile"
service-policy input platinum-up
service-policy output platinum
no shutdown
wireless tag site default-site-tag
description "default site tag"
no local-site
wireless tag policy default-policy-tag
description "default policy-tag"
wlan UofA policy default-policy-profile
wireless tag rf default-rf-tag
description "default RF tag"
wireless fabric control-plane default-control-plane
wireless country QA
wlan UofA 1 UofA
security wpa psk set-key ascii 0 12345678
no security wpa akm dot1x
security wpa akm psk
no shutdown
ap dot11 24ghz rf-profile Low_Client_Density_rf_24gh
coverage data rssi threshold -90
coverage level 2
coverage voice rssi threshold -90
description "pre configured Low Client Density rfprofile for 2.4gh radio"
high-density rx-sop threshold low
rate RATE_12M supported
rate RATE_24M supported
rate RATE_6M supported
tx-power v1 threshold -65
no shutdown
ap dot11 24ghz rf-profile High_Client_Density_rf_24gh
description "pre configured High Client Density rfprofile for 2.4gh radio"
high-density rx-sop threshold medium
rate RATE_11M disable
rate RATE_12M mandatory
rate RATE_1M disable
rate RATE_24M supported
rate RATE_2M disable
rate RATE_5_5M disable
rate RATE_6M disable
tx-power min 7
no shutdown
ap dot11 24ghz rf-profile Typical_Client_Density_rf_24gh
description "pre configured Typical Client Density rfprofile for 2.4gh
radio"
rate RATE_11M disable
rate RATE_12M mandatory
rate RATE_1M disable
rate RATE_24M supported
rate RATE_2M disable
rate RATE_5_5M disable
rate RATE_6M disable
no shutdown

```

```

ap dot11 24ghz cac voice acm
ap dot11 24ghz rate RATE_12M supported
ap dot11 24ghz rate RATE_24M supported
ap dot11 24ghz rate RATE_6M supported
ap dot11 5ghz rf-profile Low_Client_Density_rf_5gh
  coverage data rssi threshold -90
  coverage level 2
  coverage voice rssi threshold -90
  description "pre configured Low Client Density rfprofile for 5gh radio"
  high-density rx-sop threshold low
  rate RATE_12M mandatory
  rate RATE_24M mandatory
  rate RATE_6M mandatory
  tx-power v1 threshold -60
  no shutdown
ap dot11 5ghz rf-profile High_Client_Density_rf_5gh
  description "pre configured High Client Density rfprofile for 5gh radio"
  high-density rx-sop threshold medium
  rate RATE_12M mandatory
  rate RATE_24M mandatory
  rate RATE_6M disable
  rate RATE_9M disable
  tx-power min 7
  tx-power v1 threshold -65
  no shutdown
ap dot11 5ghz rf-profile Typical_Client_Density_rf_5gh
  description "pre configured Typical Density rfprofile for 5gh radio"
  rate RATE_12M mandatory
  rate RATE_24M mandatory
  rate RATE_6M mandatory
  no shutdown
ap dot11 5ghz cac voice acm
ap dot11 5ghz rate RATE_12M mandatory
ap dot11 5ghz rate RATE_24M mandatory
ap dot11 5ghz rate RATE_6M mandatory
ap tag-source-priority 2 source filter
ap tag-source-priority 3 source ap
ap profile default-ap-profile
  description "default ap profile"
trapflags ap crash
trapflags ap noradiocards
trapflags ap register
netconf-yang
end

```

Cisco ASA 5508-X Firewall

```
: Hardware:   ASA5508
:
ASA Version 9.5(3)9 <context>
!
hostname admin2
domain-name wr
enable password ***** level 7 encrypted
enable password ***** encrypted
names
!
interface Context2inside
 nameif inside
 security-level 100
 ip address 10.10.60.1 255.255.255.0 standby 10.10.60.2
!
!
interface Context2BusInternet
 nameif Internet
 security-level 0
 ip address 78.**.**.** 255.255.255.248
!
dns server-group DefaultDNS
 domain-name wr
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
object network AWS
 subnet 172.31.0.0 255.255.0.0
object network aws-AP
 subnet 10.10.80.0 255.255.255.0
access-list outside_access_in extended permit ip host 3.210.23.93 host
78.1**.**.**
access-list outside_access_in extended permit ip host 54.89.5.163 host
78.1**.**.**
access-list acl-amzn extended permit ip any4 172.31.0.0 255.255.0.0
access-list Internet_access_in_1 extended permit ip any any
pager lines 24
mtu inside 1500
mtu outside 1500
mtu Internet 1500
icmp unreachable rate-limit 1 burst-size 1
icmp permit any inside
icmp permit any outside
no asdm history enable
arp timeout 14400
nat (any,Internet) source static any any destination static AWS AWS no-
proxy-arp
nat (inside,Internet) source dynamic any interface
access-group Internet_access_in_1 in interface Internet
route Internet 0.0.0.0 0.0.0.0 78.100.42.113 1
route inside 10.10.20.0 255.255.255.0 10.10.60.254 1
route inside 10.10.40.0 255.255.255.0 10.10.60.254 1
```

```

route inside 10.10.80.0 255.255.255.0 10.10.60.254 1
route inside 10.10.100.0 255.255.255.0 10.10.60.254 1
route inside 10.10.130.0 255.255.255.0 10.10.60.254 1
route inside 10.10.140.0 255.255.255.0 10.10.60.254 1
route inside 10.10.160.0 255.255.255.0 10.10.60.254 1
route inside 10.10.170.0 255.255.255.0 10.10.60.254 1
route inside 10.10.180.0 255.255.255.0 10.10.60.254 1
route inside 10.10.190.0 255.255.255.0 10.10.60.254 1
route inside 10.10.199.0 255.255.255.0 10.10.60.254 1
route inside 10.10.200.0 255.255.255.0 10.10.60.254 1
route inside 10.10.220.0 255.255.255.0 10.10.60.254 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp
0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
user-identity default-domain LOCAL
aaa authentication http console LOCAL
aaa authentication ssh console LOCAL
aaa authentication telnet console LOCAL
http server enable
http 10.0.0.0 255.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server community *****
sysopt connection tcpmss 1379
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS esp-aes esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS esp-aes-192 esp-sha-
hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS esp-aes-192 esp-md5-
hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS esp-aes-256 esp-sha-
hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS esp-aes-256 esp-md5-
hmac

```



```

crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set transform-amzn esp-aes esp-sha-hmac
crypto ipsec ikev2 ipsec-proposal AES256
  protocol esp encryption aes-256
  protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES192
  protocol esp encryption aes-192
  protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES
  protocol esp encryption aes
  protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal 3DES
  protocol esp encryption 3des
  protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal DES
  protocol esp encryption des
  protocol esp integrity sha-1 md5
crypto ipsec security-association replay window-size 128
crypto ipsec security-association pmtu-aging infinite
crypto ipsec df-bit clear-df Internet
crypto map amzn_vpn_map 1 match address acl-amzn
crypto map amzn_vpn_map 1 set pfs
crypto map amzn_vpn_map 1 set peer 3.210.23.93 54.89.5.163
crypto map amzn_vpn_map 1 set ikev1 transform-set transform-amzn
crypto map amzn_vpn_map 1 set security-association lifetime seconds 3600
crypto map amzn_vpn_map interface Internet
crypto isakmp identity address
crypto ikev2 policy 1
  encryption aes-256
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto ikev2 policy 10
  encryption aes-192
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto ikev2 policy 20
  encryption aes

```

```
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto ikev2 policy 30
  encryption 3des
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto ikev2 policy 40
  encryption des
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto ikev2 enable outside
crypto ikev2 enable Internet
crypto ikev1 enable outside
crypto ikev1 enable Internet
crypto ikev1 policy 20
  authentication rsa-sig
  encryption aes-256
  hash sha
  group 2
  lifetime 86400
crypto ikev1 policy 30
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400
crypto ikev1 policy 50
  authentication rsa-sig
  encryption aes-192
  hash sha
  group 2
  lifetime 86400
crypto ikev1 policy 60
  authentication pre-share
  encryption aes-192
  hash sha
  group 2
  lifetime 86400
crypto ikev1 policy 80
  authentication rsa-sig
  encryption aes
  hash sha
  group 2
  lifetime 86400
crypto ikev1 policy 90
  authentication pre-share
  encryption aes
```

```
hash sha
group 2
lifetime 86400
crypto ikev1 policy 110
authentication rsa-sig
encryption 3des
hash sha
group 2
lifetime 86400
crypto ikev1 policy 120
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
crypto ikev1 policy 140
authentication rsa-sig
encryption des
hash sha
group 2
lifetime 86400
crypto ikev1 policy 150
authentication pre-share
encryption des
hash sha
group 2
lifetime 86400
crypto ikev1 policy 201
authentication pre-share
encryption aes
hash sha
group 2
lifetime 28800
crypto ikev1 policy 65535
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
telnet 10.0.0.0 255.0.0.0 inside
telnet timeout 5
ssh stricthostkeycheck
ssh 10.0.0.0 255.0.0.0 inside
ssh timeout 5
ssh key-exchange group dh-group1-sha1
no threat-detection statistics tcp-intercept
tunnel-group 3.210.23.93 type ipsec-l2l
tunnel-group 3.210.23.93 ipsec-attributes
ikev1 pre-shared-key *****
isakmp keepalive threshold 10 retry 10
tunnel-group 54.89.5.163 type ipsec-l2l
tunnel-group 54.89.5.163 ipsec-attributes
ikev1 pre-shared-key *****
```

```
    isakmp keepalive threshold 10 retry 10
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect ip-options
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
    inspect icmp
!
service-policy global_policy global
Cryptochecksum:8cb887e8d171d15f6e20e3d327c6d2c9
: end
```

Conclusion

To sum it up, we did some retrospection about how wireless technologies got evolved throughout the years to where it is now. Today's wireless technology is much more powerful than a decade ago, but with great power comes the more considerable responsibility of an engineer who is responsible for planning and implementing the Wi-Fi.

We then overlooked the modern-day challenges which we will face while planning and deploying a wireless LAN network and similar discussed solutions to those challenges. While it is not entirely possible to address and eliminate those challenges, but we can improve the quality of experience to a very satisfactory level for a Wi-Fi user.

Lastly, we implemented two latest industry wireless LAN solutions; one is the traditional on-premise wireless LAN solution, and another is Cloud environment based. Both will excellently serve the purpose but depending on the customer's requirement and budget, they can choose whichever suits them the best.

Thank you so much for reading this report. Appreciate the overwhelming support from Mentor Juned Noonari and Dr. Mike MacGregor.

Works Cited

- [1 Cisco, "Cisco Annual Internet Report (2018–2023) White Paper," Cisco, San Francisco, 2020.
]
- [2 U. B. Fritz R. Gfeller, "Wireless In-House Data Communication via Diffuse Infrared Radiation,"
] Proceedings of the IEEE 67(11):1474 - 1486, 1979.
- [3 P. K. Kaveh Pahlavan, "Evolution and Impact of Wi-Fi Technology and Applications: A
] Historical Perspective," International Journal of Wireless Information Networks 28(6):1-17,
Worcester, 2021.
- [4 R. E. D. C. a. P. B. P. Freret, "Applications of spread-spectrum radio to wireless terminal
] communications," Proceedings of the IEEE, 1980.
- [5 K. Pahlavan, "A review of wireless in-house data communications system," Proceedings
] Computer Networking, 1984.
- [6 K. Pahlavan, "Wireless communications for office information," IEEE Communications
] Magazine, 1985.
- [7 N. Abramson, "THE ALOHA SYSTEM - Another alternative for computer communications,"
] 1970.
- [8 M. Marcus, "Recent US regulatory decisions," IEEE GLOBECOM, 1985.
]
- [9 P. Basavaraj, "IP in Wireless Networks," Prentice Hall, 2003.
]
- [1 Wikipedia, "IEEE 802.11," Wikipedia.
0]
- [1 M. Gast, 802.11 Wireless Networks: The Definitive Guide, O'Reilly , 2002.
1]
- [1 L. M. s. o. IEEE, "Wireless LAN Medium access control MAC and PHY specifications," IEEE,
2] 1997.
- [1 Wikipedia, "IEEE 802.11 (legacy mode)," [Online]. Available:
3] [https://en.wikipedia.org/wiki/IEEE_802.11_\(legacy_mode\)](https://en.wikipedia.org/wiki/IEEE_802.11_(legacy_mode)).
- [1 M. Buczkowski, "Wi-Fi Standards Evolution," grandmetric.com.
4]
- [1 Electronic-notes, "Electronic-notes," [Online]. Available: [https://www.electronic-5\] notes.com/articles/connectivity/wifi-ieee-802-11/802-11b.php](https://www.electronic-5] notes.com/articles/connectivity/wifi-ieee-802-11/802-11b.php).
- [1 J. Benett, "Cisco Aironet 350 Series Access Point," Cisco Systems, 3 April 2002. [Online].
6] Available: <https://www.zdnet.com/product/cisco-aironet-350-series-access-point/>.
- [1 Amazon, "SMC Networks SMC2755W EZ Connect Wireless Access Point (802.11a)," SMC, 19
7] August 2009. [Online]. Available: <https://www.amazon.ca/SMC-Networks-SMC2755W-Connect-Wireless/dp/B000063V0E>.
- [1 B. Mitchell, "What Is 802.11g Wi-Fi? A historical look at the Wi-Fi technology," Lifewire - Tech
8] for Humans, 2021.

- [1 Cisco Systems, "Cisco Aironet 3600e Access Point," Cisco Systems, 29 Sept 2011. [Online].
9] Available: <https://www.cisco.com/c/en/us/support/wireless/aironet-3600e-access-point/model.html>.
- [2 B. Mitchell, "What Is 802.11ac in Wireless Networking?," LifeWire Tech for Humans, 2021.
0]
- [2 Cisco Systems, "Cisco will ride the 802.11ac Wave2," Cisco Systems, 7 May 2013. [Online].
1] Available: <https://blogs.cisco.com/networking/cisco-will-ride-the-802-11ac-wave2>.
- [2 TP-Link, "TP-Link® Unveils World's First 802.11ad Router," 6 January 2016. [Online].
2] Available: <https://www.tp-link.com/eg/press/news/16380/>.
- [2 T. Fisher, "What Is Wi-Fi 6?," LifeWire - Tech for Humans, 2022.
3]
- [2 Solutions Review, "Top Three Challenges Facing Large-Scale Campus Wi-Fi Deployment,"
4] Solutions Review, 2016.
- [2 ubuy, "Ubuy," 2021. [Online]. Available: <https://www.ubuy.com.tr/en/product/FYSHD5A-5-engenius-high-powered-long-range-ruggedized-3-x-3-dual-band-wireless-ac1750-outdoor-access-point-29->.
- [2 Wireless-nets, "How to: Minimize 802.11 Interference Issues," Wireless-Nets, Ltd, 2013.
6] [Online]. Available: http://www.wireless-nets.com/resources/tutorials/minimize_802.11_interference_issues.html.
- [2 Linksys, "Getting poor or no Signal on a wireless router due to physical obstructions and
7] interference," Linksys, [Online]. Available: <https://www.linksys.com/ca/support-article?articleNum=141729>.
- [2 D. Mareco, "6 Challenges to Overcome When Deploying Campus-Wide Wireless Networks,"
8] securedgenetworks, 2 Feb 2017. [Online]. Available: <https://www.securedgenetworks.com/blog/6-challenges-to-overcome-when-deploying-campus-wide-wireless-networks>.
- [2 M. Lauronen, "Troubleshooting Non-Wi-Fi Interference Using Spectrum Analyzer," Ekahau,
9] August 2021. [Online]. Available: <https://support.ekahau.com/hc/en-us/articles/115005328348-Troubleshooting-Non-Wi-Fi-Interference-Using-Spectrum-Analyzer>.
- [3 B. Murphy, "Overcoming the Challenges of Wi-Fi Deployment," *ICT Today - The official trade
0] journal of BICSI*, pp. 54-61, May-June 2019.
- [3 W. W. h. TP-LINK EAP115-Wall Access Point, Artist, <https://tienda.siliceo.es/en/wifi-access-point/1142-tp-link-eap115-wall-access-point-wifi-wall-hotels.html>. [Art].
- [3 CWNP, "Information Technology Certifications for Wi-Fi Careers," CWNP, [Online]. Available:
2] <https://www.cwnp.com/it-certifications/>.
- [3 K. T. Hanna, "Shielded twisted pair (STP)," Tech Target, [Online]. Available:
3] <https://www.techtarget.com/searchnetworking/definition/shielded-twisted-pair>.
- [3 ADMINISTRATOR, Artist, *DISCOVER FEATURES & CAPABILITIES - CISCO CATALYST
4] 3850 WITH INTEGRATED WIRELESS LAN CONTROLLER (WLC)*. [Art].
- [3 Ekahau, "Ekahau Pro," [Online]. Available: <https://www.ekahau.com/products/ekahau-connect/pro/>.

- [3 Cisco Systems, "Wireless High Client Density Design Guide," 4 May 2018. [Online]. Available: 6] https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-7/b_wireless_high_client_density_design_guide.html#concept_42C21A900F96426991DA8406A08E4EBB.
- [3 Ekahau, "How to Perform an AP on a Stick Site Survey," 7 April 2020. [Online]. Available: 7] <https://www.ekahau.com/blog/how-to-perform-ap-on-a-stick-survey/>.
- [3 Cisco Systems, "Cisco 2500 Series Wireless Controllers Data Sheet," 13 Feb 2017. [Online]. 8] Available: https://www.cisco.com/c/en/us/products/collateral/wireless/2500-series-wireless-controllers/data_sheet_c78-645111.html.
- [3 Cisco Systems, "Cisco Aironet 1700 Series Access Points," [Online]. Available: 9] https://www.cisco.com/c/en_ca/products/wireless/aironet-1700-series-access-points/index.html.
- [4 NetworkLessons, "Cisco Wireless AP Modes," [Online]. Available: 0] <https://networklessons.com/cisco/ccna-200-301/cisco-wireless-ap-modes>.
- [4 T. G. Peter Mell, "The NIST Definition of Cloud Computing," *U.S. Department of Commerce*, 1] no. Special Publication 800-145, p. 7, 2011.
- [4 R. Hussain, "What Is Cloud Computing? Explore The Services And Deployment Models," 11 2] Feb 2021. [Online]. Available: <https://www.c-sharpcorner.com/article/what-is-Cloud-computing-explore-the-services-and-deployment-models/>.
- [4 Cisco Systems, "Meraki and Cisco Cloud Calling Connected Branch Solution," Cisco Systems, 3] 27 Jan 2021. [Online]. Available: https://documentation.meraki.com/Architectures_and_Best_Practices/Recommended_Topologies/Meraki_and_Cisco_Cloud_Calling_Connected_Branch_Solution.
- [4 Cisco Systems, "Deployment guide for Cisco Catalyst 9800 Wireless Controller for Cloud 4] (C9800-CL) on Amazon Web Services (AWS)," 20 November 2018. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_cisco_catalyst_9800_wireless_controller_aws.html#id_91158.
- [4 Amazon Web Services, "What is Amazon VPC?," [Online]. Available: 5] <https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html>.
- [4 Cisco Systems, "DHCP OPTION 43 for Lightweight Cisco Aironet Access Points Configuration 6] Example," 16 June 2020. [Online]. Available: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/97066-dhcp-option-43-00.html>.
- [4 L. M. S. o. IEEE, "IEEE 802.11a-1999 - IEEE Standard for Telecommunications and Information 7] Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: High Speed Physical Layer in 5GHz," IEEE, 1999.
- [4 O. W.-F. a. p. w. f. a. m. o. s. m. p. p. c. w. c. o. d. trees, Artist, 8] <https://www.dreamstime.com/outdoor-Wi-Fi-access-point-four-antennas-mounted-strong-metal-pole-partially-covered-cobwebs-dense-trees-background-image151751060>. [Art].