White Paper

Advantages of Wi-Fi 6 for Every Network

August 2021

Table of Contents

Intended Audience

This document addresses factors and concerns related to the advancements of Wi-Fi 6. This document is written for and intended for use by technical engineers with some background in Wi-Fi and 802.11/wireless engineering principles.

For more information on how to configure CommScope products, please refer to the appropriate CommScope user guide available on the CommScope support site. https://www.commscope.com/SupportCenter/.

Overview

Wi-Fi 6 is the marketing term assigned to the IEEE Standard of 802.11ax HE by the Wi-Fi Alliance (WFA). While not officially ratified by the IEEE until the end of 2020, 802.11ax products were first seen on the market in the middle of 2019. As the next amendment to the 802.11 standard after 802.11ac in 2013, 802.11ax (Wi-Fi 6) was greatly anticipated by both vendors and network operators alike. While there was much talk around the top end speed and QAM offered in this new amendment, the innovation of this latest offering lies elsewhere.

By utilizing OFDMA, 1024 QAM, and UL/DL MU-MIMO, Wi-Fi 6 networks solve the problem of more devices being able to connect to a Wi-Fi network. These devices can be traditional devices like laptops, tablets, and phones as well as new mobile devices like wearable smart devices or stationary devices related to IoT and Smart Building/Homes. By utilizing the adaptive nature of OFDMA to adjust to the needs at hand, networks will become much more efficient, which leads to a better performing network, which leads to happier end users.

Wi-Fi operates in an unlicensed spectrum set aside by regulatory bodies around the world, but that spectrum isn't an unlimited resource. Even with the additional spectrum allocated with Wi-Fi 6E (more on that later), it is still incumbent on wireless professionals to make better use of the resources we have. This is what the IEEE has introduced with Wi-Fi 6.

To better understand the full impact of what Wi-Fi 6 brings to the market, this paper is broken down into the following topics:

- What problems does Wi-Fi 6 solve today?
- What exactly is High Efficiency?
- What additional improvements in Wi-Fi 6 are on the horizon?

Before delving into what problems are solved by Wi-Fi 6, a brief discussion on where the term Wi-Fi 6 came from.

A Brief History of Wi-Fi Naming

The new Wi-Fi 6 marketing term may seem strange to some and for good reason. Before 802.11ax, the WFA didn't assign any marketing names to the different amendments that define the PHY rate. Wi-Fi standards are defined by the IEEE and follow a specific format based on the group that is formed to focus on a particular standard:

- 802 – The year and month that the IEEE first met. February 1980 is that date, hence "80" + "2".
- .11 – The working group of the IEEE for wireless communications. Other well-known groups are 802.3 (Wired Ethernet on UTP) or 802.5 (Token Ring)
- ax – The latest amendment to the standard. Amendments most known are usually related to the speed at which a station can transmit data over the air, also known as the PHY rate. Other well-known amendments not related to the PHY rate are 802.11i (marketed as WPA2), 802.11s (Mesh), and 802.11w (Protected Management Frames or PMF).

To understand a lot of the hype around Wi-Fi 6, we need to understand the suffixes that have been assigned to the standard by the IEEE.

802.11n **HT** (Wi-Fi 4) is known as "High Throughput" since that standard was a monumental leap forward in the PHY rate taking it from the 54 Mbps offered by 802.11g all the way to 600 Mbps.

802.11ac **VHT** (Wi-Fi 5) is known as "Very High Throughput" as that standard took the PHY rate up to 6.9 Gbps.

802.11ax **HE** (Wi-Fi 6) is known as "High Efficiency". Even though there is an advancement in the maximum speed, which will be covered later, the biggest improvement with this standard was not speed but in the efficiency improvements introduced. Very few devices will be able to achieve anything close to the theoretical top end speed of Wi-Fi 6, but **every device will be able to take advantage of the improvements in spectral efficiency**.

The following chart shows how the previous, well-known PHY rates associate to the new naming convention.

802.11	Suffix	Wi-Fi Alliance Marketing Term	Maximum Speed (PHY)	Year Introduced	Supported Bands
802.11a	N/A	Wi-Fi 2*	54 Mbps	1999	5 GHz
802.11b	N/A	Wi-Fi 1*	11 Mbps	1999	2.4 GHz
802.11g	N/A	Wi-Fi 3*	54 Mbps	2003	2.4 GHz
802.11n	HT	Wi-Fi 4	600 Mbps	2009	2.4 & 5 GHz
802.11ac	VHT	Wi-Fi 5	6.9 Gbps	2013	5 GHz
802.11ax	HE	Wi-Fi 6, Wi-Fi 6E	9.607 Gbps	2020	2.4, 5, & 6 GHz

TABLE 1: WI-FI NAMING CONVENTION

Note: The Wi-Fi Alliance only officially named Wi-Fi 4 (802.11n), Wi-Fi 5 (802.11ac) and Wi-Fi 6 (802.11ax). Wi-Fi 1 – 3 is the assumed naming convention.

Problems Solved by Wi-Fi 6

Previous generations of Wi-Fi focused solely on making connections faster, resulting in faster data transfers and faster networks for the end users. Wi-Fi 6 solves many problems experienced by networks today, which "Spoiler Alert" - aren't related to faster speeds on the network. Between more smart devices needing to connect, inefficient use of spectrum, and the need for a more robust security framework, the Wi-Fi 6 amendment to the 802.11 standard is a monumental leap forward in technology that networks need to start taking advantage of today.

More Devices Need to Connect

In a 2017 Global Web Index1 study, the average number of connected devices per person was 3.2. With the recent explosion of IoT devices and wearable "Smart" devices, the number of connected devices per person is just under 8 and expected to grow to 15 connected devices per person by the year 2030[2]. While some of these devices will utilize new cellular technologies like 5G (not to be confused with 5 GHz Wi-Fi) the truth of the matter is that in 2018 Wi-Fi was estimated to carry approximately 60% of all wireless traffic and that number

[1] https://blog.globalwebindex.com/chart-of-the-day/digital-consumers-own-3-point-2-connected-devices/
[2] https://www.martechadvisor.com/articles/iot/by-2030-each-person-will-own-15-connected-devices-heres-what-that-means-for-your-business-and-content/

was expected to grow to 64% in 2020[3]. Industry experts believe that Wi-Fi will coexist with 5G and be a key part of many 5G use cases[4], not the other way around.

With more devices being used per person, there is more demand on the existing channels in a traditional network. Increases in devices mean an increase in the contention for airtime, which is already a tricky path to navigate in the best of circumstances. This is where Wi-Fi 6 comes into play.

Efficiency

While Wi-Fi 6 does bring about a huge improvement in speed thanks to more radio chains and spatial streams[5] most client devices will never approach these new maximum speeds. For mobile devices, the power and antennas needed are prohibitive to normal operations, and the truth is, the majority of mobile devices in use simply don’t need or can even use the amount of data delivered by a multi-gigabit connection speed.

When examined much closer, Wi-Fi professionals realized that the average size of the data packet being transmitted on the Wi-Fi network is just 300 bytes. To understand the impact of what that means, we need to think about highway systems for a moment. Imagine a massive, high-speed freeway designed with 4 lanes that could easily be expanded to 8 lanes, capable of accommodating large transport trucks crammed full of everything you can think of. Now, picture this same freeway network being used by these large trucks but each truck is only 20% full. All of the efficiency and capacity that is possible with this network is being wasted because while each truck is crowding the road, it’s only carrying a small percentage of what it could carry. Part of the reason for this is each truck can only carry product (or data) for 1 customer (1 device).

While not all trucks are largely empty, the vast majority of these trucks are, and are a waste of the resource. The overall capacity can’t be achieved as designed since the vehicles (devices) using the highway network is very inefficient. For our highway network, the answer is pretty simple. Instead of having one truck per customer, trucking companies will have 1 truck pick up multiple packages from multiple customers, until the truck is full, before sending it out on the road. If parcel companies didn’t do this, they wouldn’t be in business very long. By improving efficiency (have a truck carrying its full capacity) the road network can be used by more vehicles, allowing for better utilization of the resource.

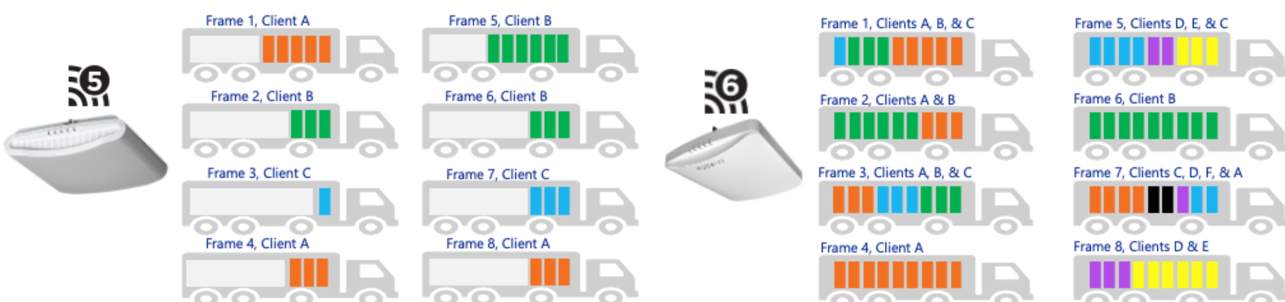

FIGURE 1: RESOURCE UTILIZATION

When it comes to Wi-Fi, the answer wasn’t as easy, until now. The idea of combining multiple devices into a single resource as it existed in the past wasn’t possible. Only 1 device could transmit at a time, whether it had a full payload (full truck) or the average payload (only 20% full), resulting in a lot of wasted resources. The wasted

[3] Wireless Global Congress 2018: Wi-Fi Injecting Itself Deeper into the 5G Mix with 802.11ax. Global Data. Ed Gubbins. (2018).
[4] Will 5G Replace Wi-Fi? https://www.sdxcentral.com/5g/definitions/will-5g-WiFi . SdxCentral.
[5] https://webresources.ruckuswireless.com/pdf/wp/wp-using-all-the-tools-you-can.pdf

resources in Wi-Fi is RF spectrum and time. Often a full 80 or 160 MHz wide channel isn't needed, or even a 20 MHz wide channel, yet devices still occupied that channel to send a small payload. The change introduced in Wi-Fi 6 to address this problem is based in the new modulation scheme introduced to Wi-Fi.

Orthogonal Frequency-Division Multiple Access

Previous modulation schemes in Wi-Fi used Orthogonal Frequency-Division Multiplexing (OFDM), which only allows 1 device to transmit at a time, no matter the size of the payload. When using the previous example of the trucks but mapped to the RF spectrum of a single 20 MHz wide channel, it starts to make sense. With 1 complete frame (the name for a packet while it is in the air) being assigned to 1 client device, whether it needs the full frame or not, the inefficiencies seen from the earlier trucks are seen below. Even though the entire frame isn't being filled, much like our earlier trucks, no other client traffic can be included.

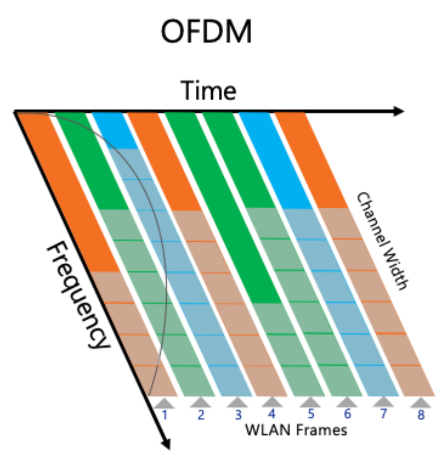

FIGURE 2: OFDM ON A 20 MHZ WIDE CHANNEL

Wi-Fi 6 uses a new modulation scheme known as Orthogonal Frequency-Division Multiple Access (OFDMA) which now allows up to 9 devices to transmit at the same time on a 20 MHz channel, if their payloads meet the requirements. If the payload needing to be transmitted requires more capacity, this is adjusted and scheduled on the fly by the infrastructure to allow for the most efficient combinations of payloads to be transmitted at the same time.

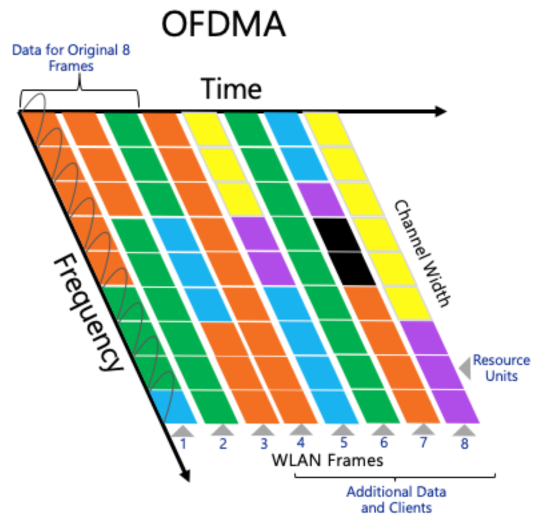

FIGURE 3: OFDMA ON A 20 MHZ WIDE CHANNEL

When Figure 2 is compared to Figure 3, you can see that what took three frames to transport using OFDM can now be combined into one frame. What was a half empty resource (Frame #1 for Client A) is now filled with the additional data for 2 additional clients (Frames 2 & 3 for Clients B & C). Both figures still use a 20 MHz wide channel, but in Figure 3 we see the introduction of the Resource Unit (RU) or that 20 MHz wide channel being broken down into 9 separate frequency allocations.

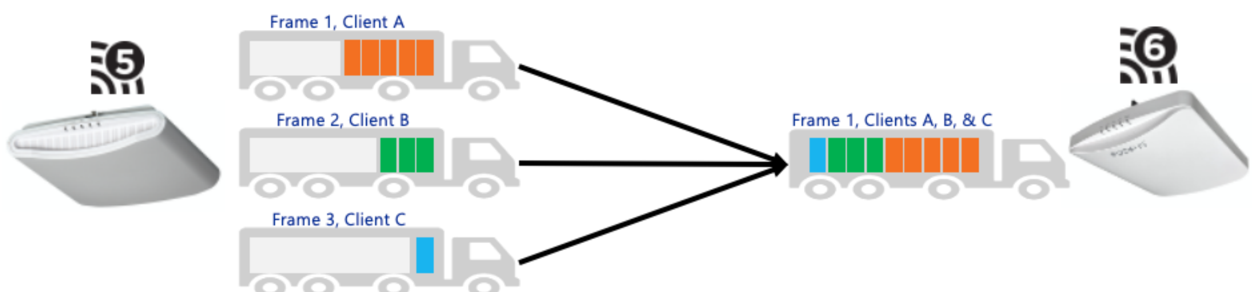

FIGURE 4: CLIENT PAYLOAD COMBINED USING OFDMA

What took eight frames in OFDM can now be accomplished in just three frames of OFDMA. This new efficiency means that starting at Frame #4, by using OFDMA, clients can now send more data or as seen in Frame #5, additional clients can now send their data. By fully utilizing the resources that are available, more data can be sent in the same amount of time (8 Frames for each example) and more clients have an opportunity to send their data. **More data from more clients in less time results in a network that feels faster than previous generations.**

Of note is not all clients need to be using or capable of OFDMA. By grouping the OFDMA (Wi-Fi 6) clients into a single frame, this opens up the remaining frames for an OFDM (Wi-Fi 5) client to utilize the resource. Since all clients can now send their data in less amount of time, the experience is faster. Even though all of this can be done in less than the maximum amount of speed possible (this is still a 20 MHz wide channel), the data is sent or received more often, the end result is a network that “feels” faster for the end user even though, in reality, what is being transmitted is being done at a speed more familiar to older networks, not the latest and greatest.

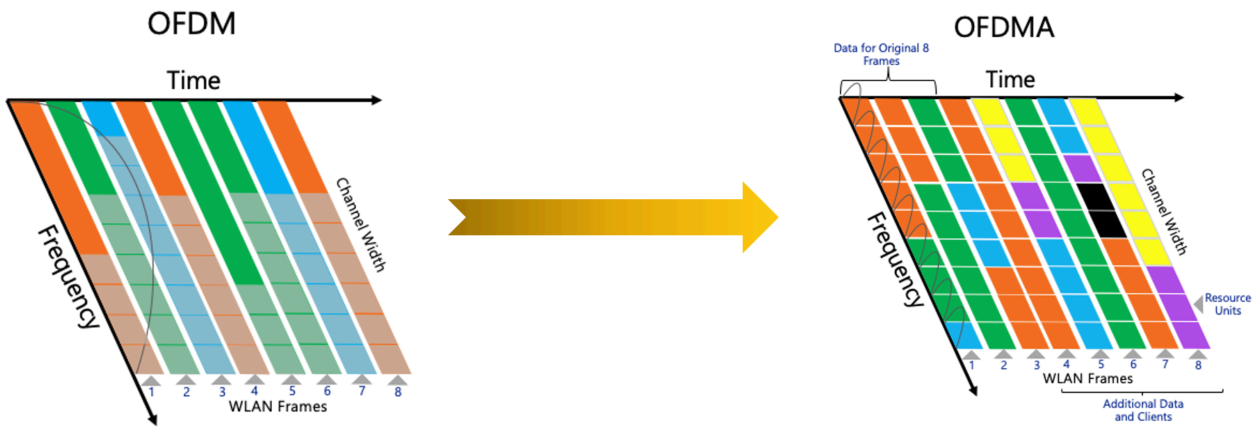

FIGURE 5: OFDM TRANSITIONING TO OFDMA

The way OFDMA does this was borrowed from cellular LTE. The idea isn't new, just the medium it is being implemented on. With the standard channel being 20 MHz wide, and the newer devices having a 2x2 radio set-up, the maximum PHY rate for that device is 173.3 Mbps. What the engineers realized is that type of speed is wasted for frames that are only carrying 300 bytes. Since it isn't practicable to try and change the 2x2 radio configuration on the fly, the other parameter to adjust is the bandwidth. In simple math, if our example device can transmit 173 Mbps on a 20 MHz wide channel, then if the channel bandwidth it transmits on is reduced to just 10% of that, or 2 MHz wide, the resulting throughput is 10% of 173 Mbps, or 17.3 Mbps. While not an impressive number when compared to the top end PHY rate for 802.11ax, the device simply doesn't need it for a 300-byte frame and even then, 17 Mbps could be seen as overkill.

While the AP still maintains control of its original 20 MHz of spectrum, it divides spectrum up amongst numerous clients associated to that AP. Instead of these 9 devices waiting in line to send their data one by one, all devices can transmit their data at once. In return, the AP can then send small amounts of data to these 9 devices at once, instead of spending 9 different time slots (time when the AP contends for time on the air and then is able to send data) sending small amounts of data to 9 different clients. What used to be done in series is now done in parallel, reducing airtime congestion and improving efficiency.

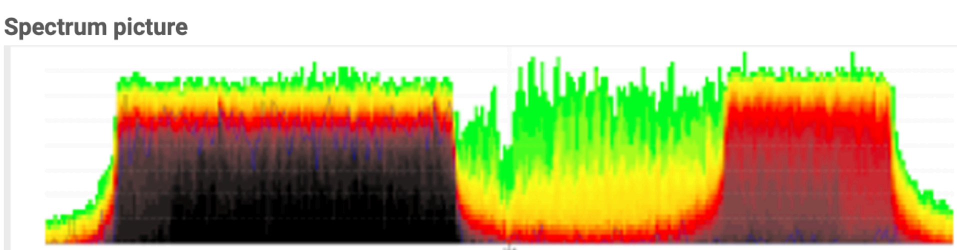

FIGURE 6: OFDMA SPECTRUM UTILIZATION (IMAGE COURTESY OF GJERMUND RAAEN)

These smaller "channels" are known as Resource Units (RUs) and can be adjusted in size, on the fly, by a process where the AP polls the clients and then schedules a time and assigns a specific RU to each device. Figure 6[6] shows two OFDMA clients utilizing the spectrum. Although this is a 20 MHz wide channel, 2 unique signals can

[6] **"UL OFDMA, what do we see in Wireshark" https://gjermundraaen.com/2019/10/10/ul-ofdma-what-do-we-see-in-wireshark/ Gjermund Raaen**

be seen, and each of them are using a different number of RU's to communicate. This also shows additional spectrum available (between the black and red columns) were additional clients could be accommodated. For reference, the black column on the left is using about 10 MHz worth of spectrum (4 RUs) while the red column on the right is using 5 MHz worth of spectrum (2 RUs).

While similar to Downlink Multi-user Multiple-Input and Multiple-Output (MU-MIMO) introduced in 802.11ac, the usage of the RU concept instead of using spatial streams makes this approach more stable and practicable in the real world. **This improved efficiency is at the heart of what Wi-Fi 6 is all about and is the catalyst for other improvements on the network as a result.**

By using a Wi-Fi 6 network and taking advantage of OFDMA, Wi-Fi 6 APs can handle more devices without needing to add more APs later to carry the load as device counts continue to increase.

MU-MIMO

Multi-User Multiple Input and Multiple Output (MU-MIMO) introduced in Wi-Fi 5 had a couple of limitations that impacted how it worked outside of a lab and, in the end, resulted in almost no advantages in a real-world deployment. The first limitation was the direction of the data. It was Downlink (DL) only, meaning it could only be used for sending data from the AP to the client devices. The second limitation was instead of using RUs, as discussed before, it used spatial streams. This means that it would only work if all client devices participating in that group were in the proper orientation to the AP sending the data to allow separation of the spatial streams. As seen below, if clients weren't in the green areas, MU-MIMO wouldn't work. Also, as beams converged, there became more issues. The final limitation was by using those spatial streams to accomplish this, it was limited to a maximum of 4 devices at one time. In addition, this was an optional feature in the IEEE standard which led to many client devices forgoing development support.

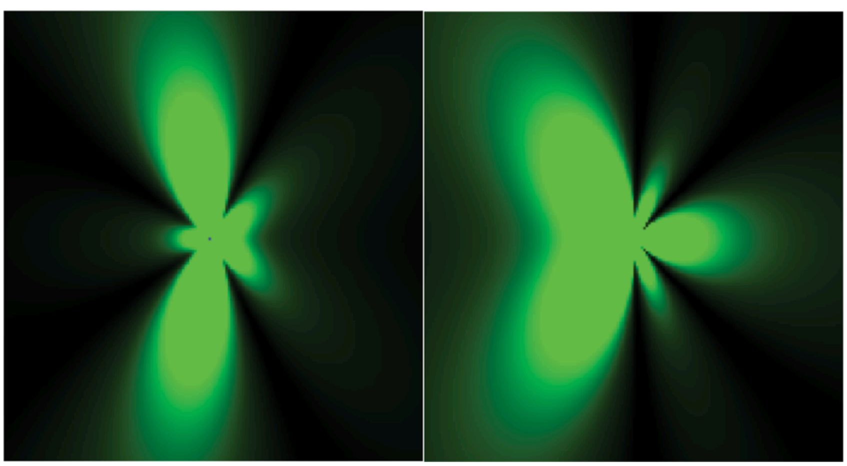

FIGURE 7: WI-FI 5 MU-MIMO USING SPATIAL STREAMS

With Wi-Fi 6 using OFDMA RUs instead of spatial streams (reference Figure 5: OFDM transitioning to OFDMA) the limitations of MU-MIMO in Wi-Fi 5 have been solved. Not only is it Downlink (DL) from the AP to the client, it is also Uplink (UL) from the client to the AP. Wi-Fi 5 used Spatial Streams to separate the data streams, making implementation limited and tough to orchestrate. Using the smaller channel widths of the RUs means the receiving station, AP or client, simply tunes their receiver to the smaller spectrum and will ignore the data being sent to the other devices. This method means it doesn't matter where in relation to the AP and other devices the client is, this method relies on proven RF methodology to accomplish both DL/UL MU-MIMO instead of cruder RF "sleight of hand" as seen in Figure 7: Wi-Fi 5 MU-MIMO using Spatial Streams.

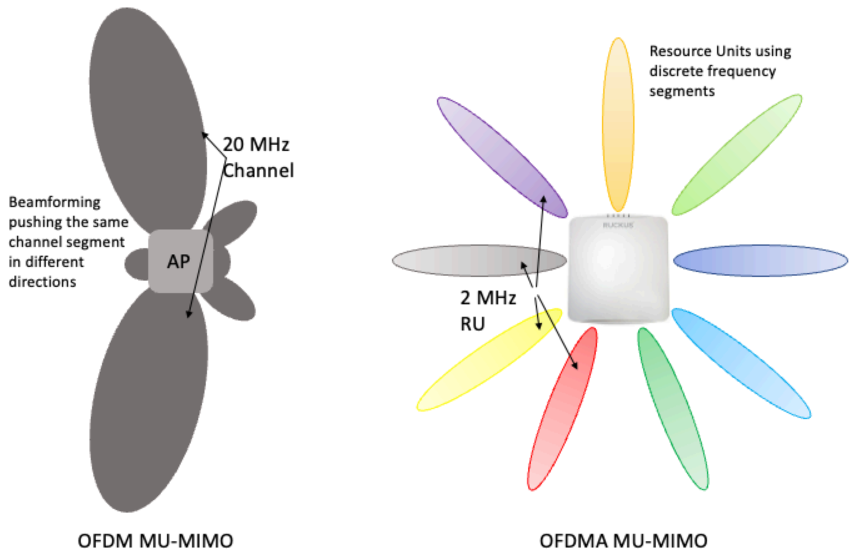

FIGURE 8: OFDM VS OFDMA MU-MIMO

When compared, the limitations of MU-MIMO using OFDM & beamforming can easily be seen. All the data is sent on a single “channel” (same frequency) and the target devices need to be in a specific relation to the AP. If clients aren’t aligned correctly with the AP and other clients (within the dark ellipse), it fails. With OFDMA, clients can be located in any position related to the AP and are assigned their own “channel” (unique Resource Unit or RU) to operate on. By dividing up the spectrum the number of variables needing to align for MU-MIMO to be successful is greatly reduced, allowing for a higher success rate.

As discussed earlier, up to 9 Resource Units can be used at one time on a 20 MHz wide channel. If that channel width is increased to 40 MHz wide, in theory even more devices could be accommodated at the same time which is a vast improvement over a previous limitation of 4 devices.

A long-time advantage of using Ruckus Access Points is the innovation in the antenna arrays of Ruckus APs. BeamFlex + was pioneered and patented by Ruckus, and when Transmit Beamforming (TxBF) used in the original MU-MIMO was combined with BeamFlex+, customers saw an even bigger advantage. OFDMA combined with BeamFlex+ gives networks an even bigger improvement in RF spectrum efficiency.

In fact, all of the Ruckus differentiators that customers know and love aren’t lost with OFDMA, they combine together and work in conjunction to give end users an even better experience.

Overall Network Improvements

While it is hard to quantify exact improvements that can be expected to be seen in each network, testing has shown an improvement during normal operations, even using a Wi-Fi 6 AP in an environment with all Wi-Fi 5 clients. Initial testing has shown increases in speed of up to 20% by simply replacing a Wi-Fi 5 AP with a Wi-Fi 6 AP. Individual networks will see a variation of this improvement owing to the differences in clients and applications running. As a varying mix of Wi-Fi 5 and Wi-Fi 6 client devices are introduced, even more improvements are seen. Improvements are there enough to justify a Wi-Fi 6 AP today while waiting for the influx of Wi-Fi 6 clients that are coming tomorrow.

Critical QoS Applications

Not only has the demand for capacity and throughput increased, critical applications are being transitioned to the wireless network. In a prime example of being victims of our own success, application and service owners see a stable wireless network as a resource they count on, not just a nice resource to have. When viewed with the addition of more and more IoT devices and the increase of smart devices, the demand on the networks of the future won't simply be about the amount of achievable throughput, but also about latency.

Real-time Transport Protocol

Real-time Transport Protocol (RTP) is the method in which audio and video services are delivered over IP networks. For many networks these RTP services used in is considered to be a critical application. As a natural transition from having a Voice over Internet Protocol (VoIP) phone on a wired network to a VoIP phone on your belt or in your pocket, applications that rely on RTP networks represent a service that has increased in prevalence over the years.

Voice traffic has two specific network requirements:

1. Voice traffic is UDP, meaning that it is sent with no expectations of receiving an acknowledgement response from the receiving client (the other device, not the AP).
2. Voice traffic is small. Based on the Compressor/De-Compressor (known as the CODEC) used in the devices, the size of the payload is generally about 64 Kilobytes with an overall size after management headers are added of about 264 Kilobytes.

What this means is that voice traffic places almost no demand on the network from a bandwidth perspective. Any latency on the network, however, is quickly exposed by voice call drops or noise. Or both.

Video applications like Zoom or WebEx have the same requirements as voice traffic, with the added overhead of video being sent along with the audio. Demand for high quality video applications has gone up and there is no expectation this demand will go away anytime soon. Many tasks previously thought to be an "in-person only" have moved to video applications, both real-time meetings and recorded presentations.

With the biggest impact to any service that is based on RTP (video and VoIP calls) being latency and jitter, the High Efficiency of Wi-Fi 6 address both of these issues. As the efficiency of the BSS (Basic Service Set – the AP and clients all operating together) improves the performance of these types of applications improve. By freeing up the airtime on the BSS by grouping low priority traffic, high priority traffic, like RTP, can be delivered on time and on schedule, the 2 issues critical to a good conversation.

Automation

Automation, in this context, is a subset of a topic known as Industrial Control Systems or ICS. Just like other uses of the traditional wired network, ICS is quickly realizing the advantages of a wireless network and multiple end devices being able to access a single wired point (the AP). Again, with stable networks becoming the victim of its own success, mission critical automation services are being added to the network, many times without consideration of if the network can support the needs of these new services.

Much like voice or video, automation traffic is normally very small in size but sensitive to latency. If a safety valve or switch needs to be activated, the resulting data is very small (ON vs OFF can be represented by a single bit of 1 or 0) but making sure that payload is delivered to the intended device without delay can make all the difference in the world. As more and more devices need to access the network with little to no latency, improvements discussed earlier are only going to become more relevant.

Critical Application Solutions with Wi-Fi 6

Whether the application in question is listed above, or is an application that is similar in nature, the way that Wi-Fi 6 can solve all of these issues can be tied into a single graphic.

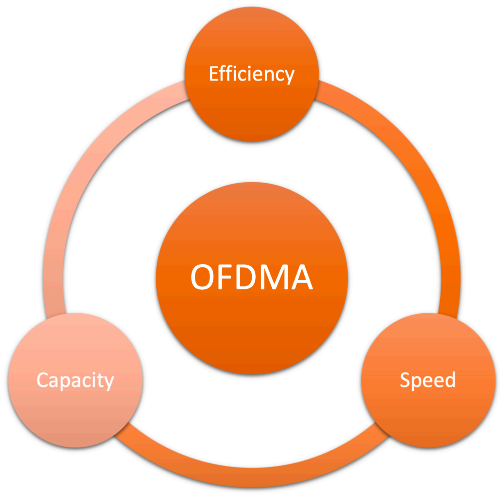

FIGURE 9: WI-FI 6 PERPETUAL IMPROVEMENT

Centered around the new modulation scheme of OFDMA (discussed earlier), as more and more devices join in the circle that revolves around OFDMA, the more efficient the network gets leading to an increase in speed (actual or perceived) which leads to more capacity. Voice, Video, AR/VR, and Automation are all solved somewhere within this circle of improvement. Need stability and low latency for real time applications? Improved efficiency of Wi-Fi 6 networks solves that problem. Need more speed for video and/or AR/VR applications? The increase of speed from a more efficient network solves that problem. Need additional capacity for more and more devices utilizing the network with small, but critical payloads? The capacity gained coupled with a more efficient network solves this problem.

Even though the problems may change, Wi-Fi 6 HE provides an answer, even if it isn't always directly apparent.

Internet of Things

Internet of Things, or IoT as it is better known, is the concept that everything is connected to the internet. Differing from the Automation use case of Industrial Control Systems earlier, IoT is characterized by low bandwidth applications with less critical data. Is your home thermostat now set 2 degrees cooler than earlier? Did someone leave the living room light on? IoT devices are characterized by low throughput and a lower sensitivity to latency. If these notifications are received a full second later thanks to more devices on the network, does anyone really notice? Unlike a one second delay in voice or video causing complaints, these delays are less critical in IoT solutions.

FIGURE 10: 1 FRAME UTILIZED BY 1 CLIENT OR 9 CLIENTS

With a focus on the capacity improvement thanks to OFDMA, more clients sending smaller payloads less often feeds directly into the OFDMA concept. Being able to adapt the number of Resource Units (RUs) needed on the fly perfectly solves this question of the increase of IoT devices on a network. An additional feature that will be covered later that has been introduced in Wi-Fi 6 is known as Target Wake Time, or TWT. TWT will help IoT devices by allowing the device to schedule how much time it will be in power save mode, or sleeping, before it will wake up and send and receive data. For a device that is streaming video, this isn't much help but for a battery operated IoT device that operates on a schedule this can be a game changer. While not all IoT devices will be taking advantage of TWT, or even capable of using TWT in the case of older devices, it is still an advantage that is now available with Wi-Fi 6.

Security Improvements: Mandatory WPA3

WPA2, first introduced in 2004 as an answer to the vulnerabilities of WEP and WPA security, has been the go-to standard for wireless security and is based on the 802.11i IEEE standard. After publication of the WPA2 Key Reinstallation Attacks (KRAck)[7] vulnerabilities in the fall of 2017, engineers realized the WPA2 standard needed a refresh. With that, the Wi-Fi Alliance (WFA) introduced the WPA3 standard as the replacement to WPA2 in early 2018 with certification beginning in June of 2018.

Building off of the lessons learned over the previous 13 years of using WPA2, WPA3 introduced some changes that are designed to correct issues like the one exposed with KRAck. WPA3, while optional for new devices that carry the Wi-Fi 5 certification from the WFA, is mandatory for Wi-Fi 6 certification. While this new security standard is long overdue, with the main advantages being discussed in a moment, the trail to full adoption of WPA3 isn't an easy one, especially with the abundance of Wi-Fi 5 devices still in production and operational in the network.

One of the pain points with this security improvement is the inconsistent device support for the new standard. As of this writing Apple mobile devices that are on iOS 13 or newer, as well as MacOS Catalina (10.15.X) or newer, support WPA3. Support within Android devices is very sporadic without a good way to determine which devices are supporting WPA3 or not. Windows 10 supports WPA3 only **IF** the device has the latest patches **AND** if the device driver for the Wi-Fi NIC has been updated. While WPA3 transition or mixed mode (both WPA2 & WPA3 at the same time) is an option it largely depends on the types of devices using the network. Newer devices that might not support WPA3 by itself can use it but older devices like Windows 7 and IoT type devices struggle with mixed mode.

A full discussion of all of the advantages of WPA3 is beyond the scope of this document but there are a couple of updates that highlight the benefits of WPA3 that should be discussed.

Simultaneous Authentication of Equals

With WPA2, the most common method to join devices to a network is through the use of a Pre-shared Key (PSK). PSK is typically used for in-home networks, many guest networks, as well as Bring Your Own Device (BYOD) networks and involves typing a password into the device. The device would then use that as their access key to the network. The major downfall to this method is how, during the initial connection process of a device, the network, or Access Point (AP) is seen as the authenticator and the device is seen a requestor. The client device blindly trusts whatever it is told by the AP, without establishing any trust with the infrastructure.

In WPA3 this PSK method has been replaced with a method known as Simultaneous Authentication of Equals, or SAE. During the authentication sequence using the WPA2-PSK method, there was a process known as the four-way handshake, where each side would send encrypted data in sequence. KRAck took advantage of a weakness in this implementation where an attacker could reset the counter in the middle of this handshake, and have the device install (or reinstall) an encryption key of all zeros. Once the attacker was able to override the normal encryption process with their own key, they can then decrypt all the traffic. SAE changes this by replacing the 4-

[7] https://www.krackattacks.com by Mathy Vanhoef of imec-DistriNet

Way handshake. Instead, it uses a "Password Authenticated Key Exchange" (PAKE) that is resistant to KRAck as well as offline dictionary attacks. This is a significant improvement over the WPA2-PSK protocol it replaces.

Being able to act as an equal, client devices can now leverage similar mechanisms seen in WPA2-Enterprise (which uses 802.1X mechanisms) where each side can initiate the exchange and each side sends their authentication independently instead of a the back and forth method seen in the WPA2-PSK 4-Way handshake.

Protected Management Frame

Protecting the management frames used in Wi-Fi isn't a new concept. First introduced in 802.11w in 2009, Protected Management Frames, or PMF, is a way to secure the management frames used in Wi-Fi after a device has successfully associated to a network. Many of the attacks against Wi-Fi devices rely on this open management exchange between the devices and the APs to wage attacks. In order to maintain some semblance of order in an open standard communication protocol, most management frames are sent in the clear, and devices inherently trust that what they receive is authentic. This inherent trust is where attackers like to strike the most.

Even though PMF has been around for more than a decade support from the client side has been lacking. While most infrastructures support PMF when using WPA2-Enterprise, many client devices don't. This leads to protection being set as "optional" and just as before, when something is optional, it isn't likely to happen. While WPA2-Enterprise wasn't affected by KRAck the same way WPA2-PSK was (devices in a Dot1X network are treated as equals somewhat) by not protecting the management frames, attackers could still disrupt the network up to and including making it unusable by legitimate devices.

In WPA3-Enterprise, PMF is mandatory. This is a critical change. With WPA3 the length of the key algorithms has also increased from 128-bit to an optional 192-bit. Increased key length is always a good thing, but cryptographic strength wasn't a key weakness of WPA2 networks. This improvement is to align with the Commercial National Security Algorithm (CNSA) suite to maintain data integrity on networks.

To read more about the enhancements of WPA3, this blog is a good place to start https://www.commscope.com/blog/2018/wpa2-wpa3-the-new-the-changed-the-future/

Increased Capacity

In previous versions of Wi-Fi, capacity was dictated by the overall efficiency of the resource the devices were connected to. In this case we are referring to the RF spectrum that the AP and client devices operate on. As more and more devices were associated to an AP, and therefore operating on the same Basic Service Set (BSS), capacity was dictated by how well these devices operated. With poor efficiency, capacity was somewhat limited. With improved efficiency, networks can expect to see more capacity on the APs as they are able to process the devices more efficiently, resulting in a better performing network.

As devices continued to evolve and change, there needed to be an increase in efficiency and capacity to ensure that networks could keep pace with the demands placed on them. As mobility demands and wireless connectivity became the preferred method of connecting to the network, additional capacity is critical. No longer is the wireless network focused on just mobile devices; one study from International Data Corporation[8] estimates that by 2025, there will be 41.6 billion connected IoT devices: everything from machines, to sensors, and cameras. Few of these are considered mobile. In the average enterprise, more than 30% of all network-connected endpoints are IoT devices (excluding mobile devices). These devices will generate almost 80 Zettabytes (ZB) of data in the year 2025. For reference, one Zettabyte is 1000 x 10^7 Kilobytes.

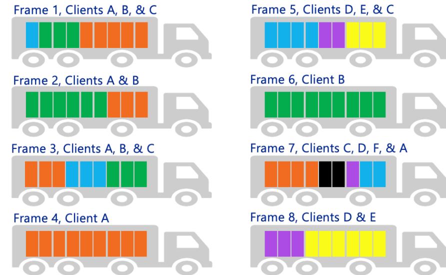

FIGURE 11: ADDITIONAL CLIENTS WITH OFDMA

In order to handle IoT devices as well as the traditional mobile devices, networks needed more efficiency and capacity. Figure 5: OFDM transitioning to OFDMA illustrates how, using OFDMA (Wi-Fi 6), additional devices can be supported in the same amount of time previously used. There is also the added evolution of the hardware used in Wi-Fi. Just as client devices evolve and get better and faster with each release, the same is true for the Wi-Fi infrastructure. With each new generation of Wi-Fi, the hardware used in the APs and devices gets better. Coupled with better and more efficient coding, Wi-Fi 6 APs bring unique advantages. While it might be cool to drive a car from the 1920's, and it will get you to where you are going (eventually) it's never going to have integrated, onboard navigation.

While the additional spectrum promised with Wi-Fi 6E is helpful (more on that later), network designers and operators can't count on additional spectrum allocation every time existing resources are depleted. RF spectrum is a natural resource, and like all of our natural resources, we need to be better stewards of what we have. Thanks to the IEEE and Wi-Fi 6 HE, we now have the tools to do just that.

Increased Speed

While not the primary objective of Wi-Fi 6, additional speed is indeed something that comes with Wi-Fi 6. While it is easy to look at Table 1: Wi-Fi Naming Convention and focus on the maximum PHY rate of 9.6 Gbps, it's not the only place additional speed will be realized. As discussed earlier, better utilization of the resource (the RF spectrum) naturally leads to what feels like a faster network simply because client devices have more opportunities to transmit and receive their data. More opportunities to transmit and receive mean lower latency and reduced jitter, two key components to any stable network.

In previous Wi-Fi standards, additional speed came in the form of extra transmit (TX) radios, receive (RX) radios, and spatial streams (SS); read as "TX x RX : SS" (1x1:1 → 2x2:2 → 3x3:3 →4x4:4 → 8x8:8), additional channel widths (20 MHz → 40 MHz → 80 MHz → 160 MHz → 320 MHz), or increased Quadrature Amplitude Modulation (16-QAM → 64-QAM → 256-QAM → 1024-QAM) this isn't the only place that Wi-Fi 6 networks will see an increase in speed from, and **the increase benefits not only Wi-Fi 6 clients, older devices will benefit as well.**

[8] https://www.idc.com/getdoc.jsp?containerId=prUS45213219

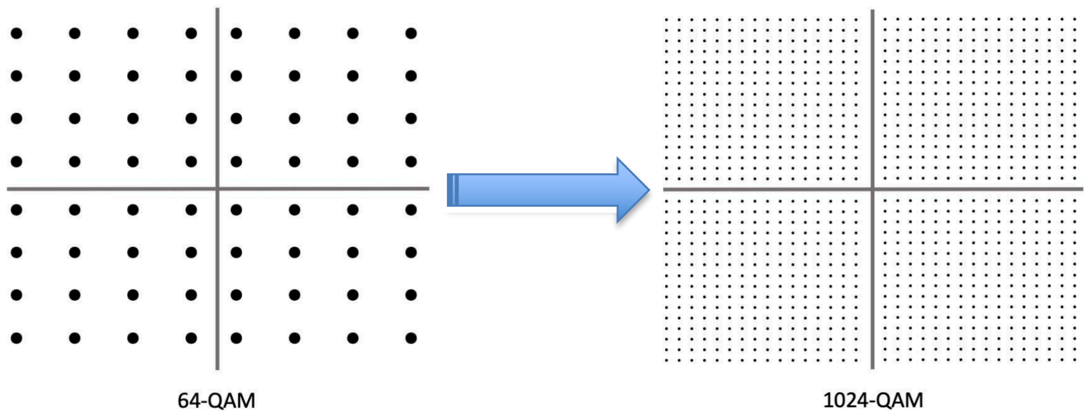

FIGURE 12: QAM CONSTELLATIONS

Pictured in Figure 12 is what is known as the QAM constellations. In order to work, the radios need to be able to hit a specific dot within the constellation and do it on demand. While 64 QAM might be slower, it's much easier to hit that target, making it more robust. If Wi-Fi 6 relied solely on 1024 QAM to achieve an increase in speed, the improvement wouldn't be as great as might be expected. In an attempt to test your eyesight even more, a quick word about the Error Vector Magnitude (EVM) as it relates to the QAM constellation.

Error Vector Magnitude

EVM is an imaginary box drawn around each dot in the QAM constellation. Equidistant from each dot, it actually represents the margin of error a signal has when trying to hit the target. Since perfection in wireless is difficult to obtain the targets (the actual dot in the constellation) doesn't have to be hit exactly in the center. The lower the QAM (16 vs 64) the bigger the target (the EVM), but with a decrease in value or speed. The higher the QAM (64 vs 1024 seen above) the smaller the target. Given the size of the EVM at 64 QAM, imagine the size of the EVM at 1024 QAM!

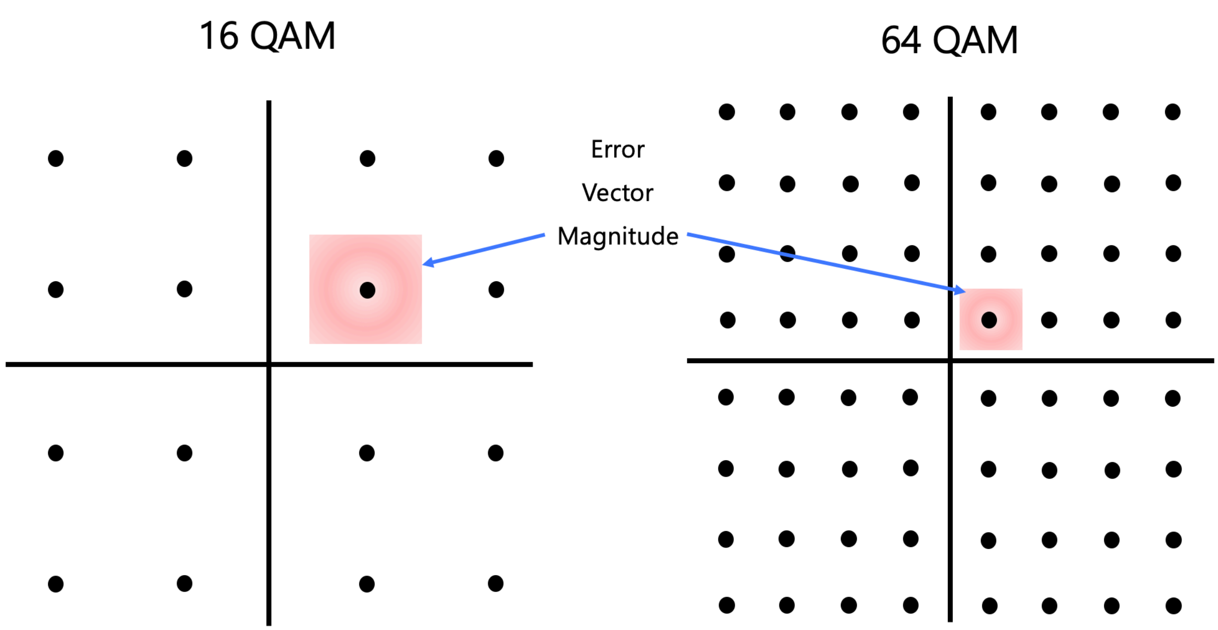

FIGURE 13: ERROR VECTOR MAGNITUDE

At higher QAM rates, client devices need to have very "clean air" (high Signal to Noise Ratio or SNR) to cleanly hit every EVM every time. An example of this would be trying to shoot darts in a bar. Early in the night, when there aren't as many people, it's easier to hit the target. As the number of people increases, the noise and distractions increase, and the visibility of the target at the same distance isn't as good. In order to get back to the same conditions as before, the player needs to move closer to the target, thereby improving their chances of hitting their target more often. When a player (in this case the device) can't consistently hit the target, and moving closer isn't an option, the only alternative is a bigger target. Client devices will do this dynamically. In a cruel twist, not all devices make the decision of when and how to perform this downshift, creating inconsistent performance across different device types.

Some devices will downshift from 1024 QAM to 256 QAM, and then to 64 QAM and finally to 16 QAM. As the QAM number decreases, the size of the EVM in the constellation gets bigger, making it an easier target to hit. Some devices will immediately go from 1024 QAM to 16 QAM and then try to work their way back up. Client device behavior is something that Wi-Fi professionals constantly chase, and still have yet to get a firm grasp on. The common saying is "If it weren't for Wi-Fi clients our job would be much easier!"

Each new amendment to the 802.11 PHY rate introduces a new QAM constellation. Coupled with these new QAMs are new versions of the silicon chips used in both APs and client devices. With each new run of chips, devices get better at targeting the EVM, resulting in stations within the network maintaining higher PHY rates. Even with older clients, a new AP will be much better at hitting its target (or EVM) in the QAM constellation, resulting in a faster experience for all devices, not just those that are capable of Wi-Fi 6 and 1024 QAM.

Luckily, some of these clients are naturally going to be closer to the target. With Wi-Fi 6, not all devices are going to be able to take advantage of 1024 QAM, *but some will*. Ever been waiting in line at the drive through, thinking it was going to take forever, and then the 2 people in front of you suddenly sped through the process? Even though you still needed to pick up the 12 drinks and 2 dozen donuts for the office, your experience was still faster thanks to the people using the drive through window faster than expected. Wi-Fi 6 clients that send their data faster, even some of the time, makes for a more efficient BSS, which makes the experience faster for all.

By not relying solely on faster and higher QAM rates, the additional speed seen in Wi-Fi 6 comes hand in hand with increased efficiency and capacity. As devices are able to utilize the spectrum more efficiently, it opens up more additional time slots for devices to transmit, known as Transmit Opportunity, or TXOP. By utilizing OFDMA, devices with smaller payloads can all transmit their data at the same time, instead of waiting in line for their own TXOP, allowing devices that have the need to transmit more often greater opportunity. More opportunity on the channel means all devices will naturally speed up as more and more time is available for devices that need it.

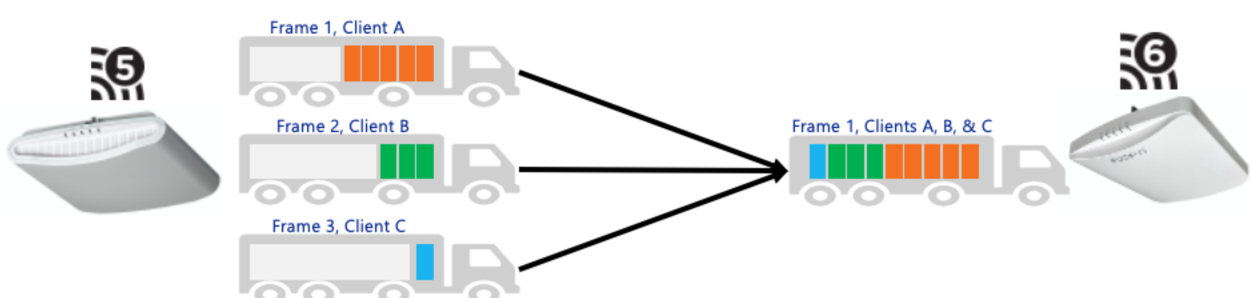

FIGURE 14: RESOURCE UTILIZATION IMPROVEMENT

More TXOP combined with devices that can use higher QAM rates means devices get more data transmitted faster, resulting in a decrease of the TXOP's the device needs. More TXOP for other devices, even Wi-Fi 4 or 5 devices, means they will go faster.

With the combination of improved efficiency, capacity, and speed, whether it happens individually or as a combination of any of the factors mentioned, **problems that are being experienced by networks today can be solved by upgrading to a Wi-Fi 6 network, even if the majority of clients are not Wi-Fi 6 capable.**

What is Coming Next in Wi-Fi 6?

Just like Wi-Fi 5 that came in 2 waves, 802.11ax has some features that are available now and some that are still on the horizon. Wi-Fi 6E has come along at a time when Wi-Fi 6 was just coming into its own and has introduced some confusion that needs to be cleared up. While many think it is the next evolution of the Wi-Fi PHY Rate standard, the actual meaning is more mundane. Wi-Fi 6E stands for the IEEE standard of 802.11ax (Wi-Fi 6) **Extended** into the 6 GHz band, which gives us the Wi-Fi 6E name.

While many in the industry have lamented the lack of realized improvements that was expected with Wi-Fi 6, the majority are looking to Wi-Fi 6E as the "promised land" where they expect to see great improvements. While Wi-Fi 6E does bring a great addition of much needed spectrum, the protocol is still the same. With Enterprise grade APs just now coming to market, with a handful of client devices, what has been lacking for the majority of 2020 and 2021 is the density required to see the full utilization of the 802.11ax standard. The new 6 GHz spectrum, providing additional capacity, will in the long run decrease the effectiveness of Wi-Fi 6 and OFMDA by moving clients from a band (5 GHz) that is only saturated in a handful of cases to a band that is mostly empty. To realize the full capability of a "High Efficient" protocol, the load and demand on the current channels needs to reach a point where the AP, the clients, and the channel will actually show an improvement.

The global pandemic has done one thing that many don't realize. It has cheated Wi-Fi 6 of showing its full potential. Wi-Fi 6 promised a commuter lane, or High Occupancy Vehicle (HOV) lane for Wi-Fi. While that lane is there, and ready to be used, the road that it was built to support has seen a huge decrease in traffic. Extra lanes and space are great to have, but if the normal lanes aren't congested, then users won't see any benefit to these extra lanes.

With consumer hardware just now coming to market for Wi-Fi 6E, and no certification testing in place yet, there are still additional hurdles that may need to be solved before any widespread 6 GHz products are seen in the market. While this new spectrum is considered "Greenfield" for Wi-Fi use (not encumbered by any legacy devices and protocols) that doesn't mean the spectrum is unused by anything else. There are existing users in this new spectrum (incumbents) and Wi-Fi devices will have to follow certain procedures in order to first use that spectrum. Limitations like transmit power being limited in some scenarios as well as the use of Automated Frequency Coordination (AFC) systems are still being fully flushed out.

Organizations that are waiting on Wi-Fi 6E to become a fully realized product line may be waiting longer than expected, and the return on that wait may not deliver on all the expectations of today.

Just like with the commuter or HOV lanes from above, organizations need to look to Wi-Fi 6E the same way civil engineers look at these special lanes on roadways. Not all roadways need these extra lanes the same way not all APs need to have this extra radio. Once life returns to "normal", organizations will be able to mix in Wi-Fi 6E APs in those areas that need it while leaving the rest of their deployment alone. Add additional capacity (the 6 GHz radio of Wi-Fi 6E) only where needed without the disruption to existing channel plans. This is the game changer with Wi-Fi 6E that organizations need to factor in.

Additional information about Wi-Fi 6E can be found in this Tech Brief from CommScope: https://www.commscope.com/globalassets/digizuite/565283-wifi-6e-tech-brief-co-114896-en.pdf .

Summary

With every new ratification of an 802.11 PHY standard, network administrators and engineers face the same challenges and questions. “Should we upgrade or wait?” “When is the right time to upgrade?” “What if I upgrade and things break?”

CommScope RUCKUS products blend the new features of Wi-Fi 6 with patented RF innovations that benefit every device regardless of type or capability. Everything that customers know and love about the RUCKUS product line – BeamFlex+™, ChannelFly™, and PD-MRC still function with Wi-Fi 6 APs. As an added bonus, all RUCKUS Wi-Fi 6 APs come with integrated IoT radios, making your Wi-Fi 6 network IoT ready without needing to add any additional USB dongles or other hardware. Additionally, the main management platforms of the RUCKUS lineup (SmartZone, Cloud, Unleashed) all support Wi-Fi 6 APs.

When Wi-Fi 6E is needed, rest assured that networks can seamlessly integrate this new development into an existing Wi-Fi 6 network by simply replacing the APs in just those specific areas that need the additional capacity without affecting the parts of the network that don’t need that additional capacity.

CommScope RUCKUS has the proven track record dealing with the toughest RF challenges inherent in Wi-Fi to meet your needs today and tomorrow.

Ruckus solutions are part of CommScope's comprehensive portfolio for Enterprise environments (indoor and outdoor).

We encourage you to visit **commscope.com** to learn more about:

- Ruckus Wi-Fi Access Points
- Ruckus ICX switches
- SYSTIMAX and NETCONNECT: Structured cabling solutions (copper and fiber)
- imVision: Automated Infrastructure Management
- Era and OneCell in-building cellular solutions
- Our extensive experience about supporting PoE and IoT

COMMSCOPE® RUCKUS®

commscope.com

Visit our website or contact your local CommScope representative for more information.

Appendix A: Glossary

- EIRP – Effective Isotropic Radiated Power; hypothetical power radiated by an isotropic antenna to achieve the same signal strength. https://en.wikipedia.org/wiki/Effective_radiated_power
- IEEE – Institute of Electrical and Electronics Engineers. https://www.ieee.org
- ISM Band – Industrial, Scientific, and Medical part of the RF spectrum; in Wi-Fi known as the 2.4 GHz band.
- MCS – Modulation and Coding Scheme. Value that combines a number of variables to arrive at a data rate on the channel. First introduced with 802.11n. https://en.wikipedia.org/wiki/IEEE_802.11n-2009#Data_rates
- OFDM – Orthogonal Frequency-Division Multiplexing; modulation method used in 802.11a/g/n/ac.
- OFDMA – Orthogonal Frequency-Division Multiple Access; modulation method used in 802.11ax.
- PHY – Physical Layer, usually used in conjunction with PHY Rate.
- PHY Rate – Physical Layer Rate; the maximum theoretical speed that data can move across a wireless link.
- PSD – Power Spectral Density; method to adjust the transmitted power to accommodate for an increase in the noise floor to maintain a constant RSSI.
- QoS – Quality of Service; refers to traffic prioritization and resource reservation control mechanisms. https://en.wikipedia.org/wiki/Quality_of_service
- RF – Radio Frequency, used at Layer 1 for wireless communications.
- RSSI – Received Signal Strength Indicator; estimated measurement of how well the signal is received.
- SNR – Signal to Noise Ratio; an absolute value of the difference between the signal received and the noise floor at the time. Value is always represented as a positive number.
- TxBF – Transmit BeamForming; introduced with 802.11n, a method in which multiple antennas send the same signal but at slightly different times.
- TXOP – Transmission Opportunity; the amount of time a station can send a frame on the wireless medium.
- U-NII Band – Unlicensed National Information Infrastructure RF spectrum broken into the following ranges:
  - U-NII-1; 5.150 GHz through 5.250 GHz, Ch 36 to 48
  - U-NII-2a; 5.250 GHz through 5.330 GHz, Ch 52 to 64
  - U-NII-2c (Extended); 5.470 GHz through 5.730 GHz, Ch 100 to Ch 144
  - U-NII-3; 5.735 GHz through 5.850 GHz, Ch 149 to Ch 165
  - U-NII-4; 5.850 GHz through 5.925 GHz, Ch 169 to Ch 185
  - U-NII-5 through 8; 5.925 GHz to 7.125 GHz, Wi-Fi 6E
- WFA – Wi-Fi Alliance https://www.wi-fi.org

Appendix B: RUCKUS Wi-Fi 6 Products

All Wi-Fi 6 APs from RUCKUS can operate on the latest version of SmartZone, Virtual SmartZone, RUCKUS Cloud, as well as RUCKUS Unleashed.

RUCKUS Model	Radio Chains	Spatial Streams	Ethernet Ports	Max PHY 5GHz	Max PHY 2.4 GHz	Concurrent Users	IoT Status
R850	8x8	8	1 at 1/2.5/5 Gbps 1 at 1 Gbps	4,800 Mbps	1,148 Mbps	1024	Integrated
R750	4x4	4	1 at 2.5 Gbps 1 at 1 Gbps	2,400 Mbps	1,148 Mbps	1024	Integrated
R730	8x8	8	1 at 1/2.5/5 Gbps 1 at 1 Gbps	4,800 Mbps	1,148 Mbps	1024	Integrated
R650	4x4	4	1 at 2.5 Gbps 1 at 1 Gbps	2,400 Mbps	574 Mbps	512	Integrated
R550	2x2	2	2 at 1 Gbps	1,200 Mbps	574 Mbps	512	Integrated
T750	4x4	4	1 at 2.5 Gbps 1 SFP Interface	2,400 Mbps	1,148 Mbps	1024	Integrated

TABLE 6: RUCKUS WI-FI 6 ACCESS POINTS

RUCKUS Controller	First Supported Version	Platform	Maximum Clients Controller/Cluster	Maximum APs Controller/Cluster
SmartZone Virtual	3.6.2*	Virtual SmartZone Essential Virtual SmartZone High Scale	50,000/120,000 100,000/300,000	2,048/6,000 10,000/30,000
SmartZone Appliance	3.6	SmartZone 144 SmartZone 300	50,000/120,000 150,000/450,000	2,048/6,000 10,000/30,000
RUCKUS Cloud	20.01	Cloud	Unlimited	Unlimited
RUCKUS Unleashed	200.6*	Any Wi-Fi 6 AP	2,048	128
ZoneDirector	10.3*	ZD1200	4,000	150

TABLE 7: RUCKUS WI-FI 6 CONTROLLERS

* Controller version has limited support for Wi-Fi 6 APs, refer to the release notes for further details to ensure the chosen AP is supported.

Appendix C: Referenced Links

- Global Web Index Study: https://blog.globalwebindex.com/chart-of-the-day/digital-consumers-own-3-point-2-connected-devices/
- Number of connected devices: https://www.martechadvisor.com/articles/iot/by-2030-each-person-will-own-15-connected-devices-heres-what-that-means-for-your-business-and-content/
- Will 5G Replace Wi-Fi? https://www.sdxcentral.com/5g/definitions/will-5g-WiFi
- Radio chains & spatial streams: https://webresources.ruckuswireless.com/pdf/wp/wp-using-all-the-tools-you-can.pdf
- UL OFDMA, what do we see in Wireshark: https://gjermundraaen.com/2019/10/10/ul-ofdma-what-do-we-see-in-wireshark/
- KRAck Attack: https://www.krackattacks.com
- WPA3: https://www.commscope.com/blog/2018/wpa2-wpa3-the-new-the-changed-the-future/
- Connected IoT devices: https://www.idc.com/getdoc.jsp?containerId=prUS45213219
- Wi-Fi 6E: https://www.commscope.com/globalassets/digizuite/565283-wifi-6e-tech-brief-co-114896-en.pdf