Electronic Design® LIBRARY

A compendium of articles from *Electronic Design* and *Laird Connectivity.*

Sponsored by Laird™ CONNECTIVITY

Utilizing Wi-Fi 6E for Embedded Applications

Wi-Fi 6/6E with Bluetooth 5.4 for Next-Gen Wireless IoT.

Introducing the Sona IF573 Series: Purpose-built for industrial IoT connectivity, this truly robust module is rugged, small, globally certified, has reliable connectivity and is easy to integrate.

- ✓ Wi-Fi 6E (802.11ax) Tri-band + Bluetooth 5.4
- ✓ M.2 1318 SMT and 2230 Type E Plug-in modules
- ✓ MHF and RF trace pin antenna options
- ✓ Industrial operating temperature range
- ✓ WPA3 Personal and Enterprise security
- ✓ Linux Kernel support up to v6.1
- ✓ Android 12/13 support
- ✓ Fully Certified for US, Canada, Japan, Europe, UK, Australia and New Zealand

Premium Wi-Fi Advantage

The road to bringing wireless to your product is perilous and long – but it doesn't have to be. These are the pillars of our value as a partner and provider: Excellence in development across hardware and software, delivered with industry-best support and certified to regulations around the world in the markets that drive your business success.

Hardware **Software** **Support** **Regulatory**

LEARN MORE ONLINE AT
LAIRDCONNECT.COM/SONA-IF573

Laird™ CONNECTIVITY

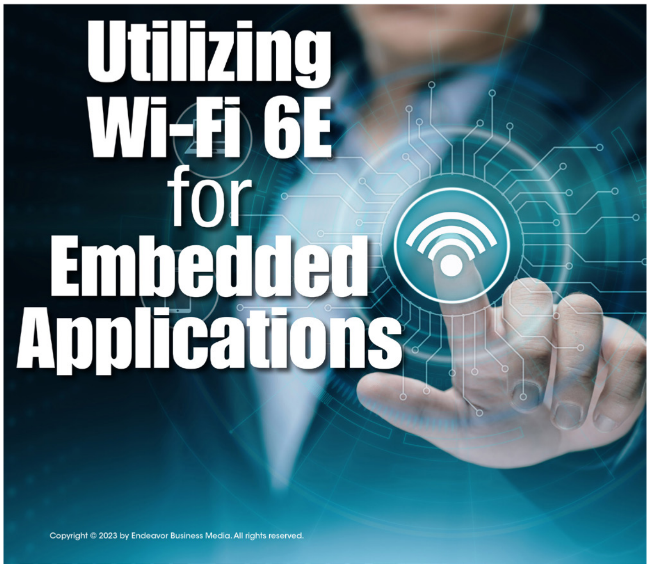


Image courtesy of Dreamstime/ Alexandersikov

INTRODUCTION

Wi-Fi 6E brings a performance boost to this wireless standard with the use of the 6 GHz band, but it also lowers latency. The Target Wake Time feature can provide better battery life for IoT devices, especially in crowded areas. Improvements like these make it more interesting for developers of specialized applications such as medical devices where security, performance, and reliability are critical.

Bill Wong
Editor,
Senior Content Director, Electronic Design & MWRF

CONTENTS

image courtesy of Dreamstime

CHAPTER 1:

Wi-Fi 6E is Reshaping RF Security Requirements

DR. NIKHIL ADNANI, Chief Technology Officer & VP Sales, *thinkRF*

Even as it promises a less-congested Wi-Fi spectrum, the advent of Wi-Fi 6E poses new challenges to RF security professionals. Here's a look at how an SDR-based approach to spectrum analysis can help get the job done.

Fixed and mobile internet usage is growing rapidly as our world depends more on the wireless spectrum, thanks in large part to the great migration to working from home. A May 2020 report found that overall internet traffic grew by more than 40% between February and April, with video streaming accounting for 58% of all traffic.[1] Much of this traffic is being driven away from mobile back to fixed Wi-Fi access points.

The arrival of Wi-Fi 6E will help to alleviate the congestion on existing Wi-Fi networks. In response to the need for greater reliability, access, and performance, the Federal Communications Commission (FCC) voted in April 2020 to open up the 6-GHz band (5.925 to 7.125 GHz) for unlicensed use.[2] Adding more than 1.2 GHz of high-frequency spectrum, the announcement represents the largest addition to Wi-Fi since the original 802.11b standard of the late 1990s and paves the way for the Internet of Things (IoT), virtual and augmented reality (VR/AR), and other high-bandwidth, low-latency applications.

However, the move to the 6- to 7-GHz band and beyond presents a new challenge to RF security and technical surveillance countermeasures (TSCM) professionals. With most previous devices using signals in the 2.4- or 5-GHz bands, spectrum-analysis equipment also was designed to cover up to a maximum of 6 GHz. As a result, many users will need to increase the frequency range of their RF measurement equipment to get a complete view of the spectrum environment in their facility.

This article will introduce the Wi-Fi 6E standard and provide an overview of the new specifications, improvements over previous standards, and potential applications and uses. It will then explore how these new signals will impact RF security professionals before showing how a software-defined approach to spectrum analysis allows for greater performance at a lower cost than traditional hardware.

RF security will always play an important role in corporate offices, government facilities, sensitive compartmented information facilities (SCIFs), and other environments where sensitive information must be protected. By understanding the new standard, security professionals can ensure they have the equipment and performance needed to maintain control of the wireless spectrum.

Understanding Wi-Fi 6E

A recent Cisco report estimates that 5.6 billion people will use the internet by 2023. The number of connected devices is expected to grow from 18.4 billion in 2018 to more than 29 billion by 2023.[3] In addition to this rapid rise in the number of connected devices, high-definition video streams and other high-bandwidth applications have dramatically increased the amount of data flowing at a given time.

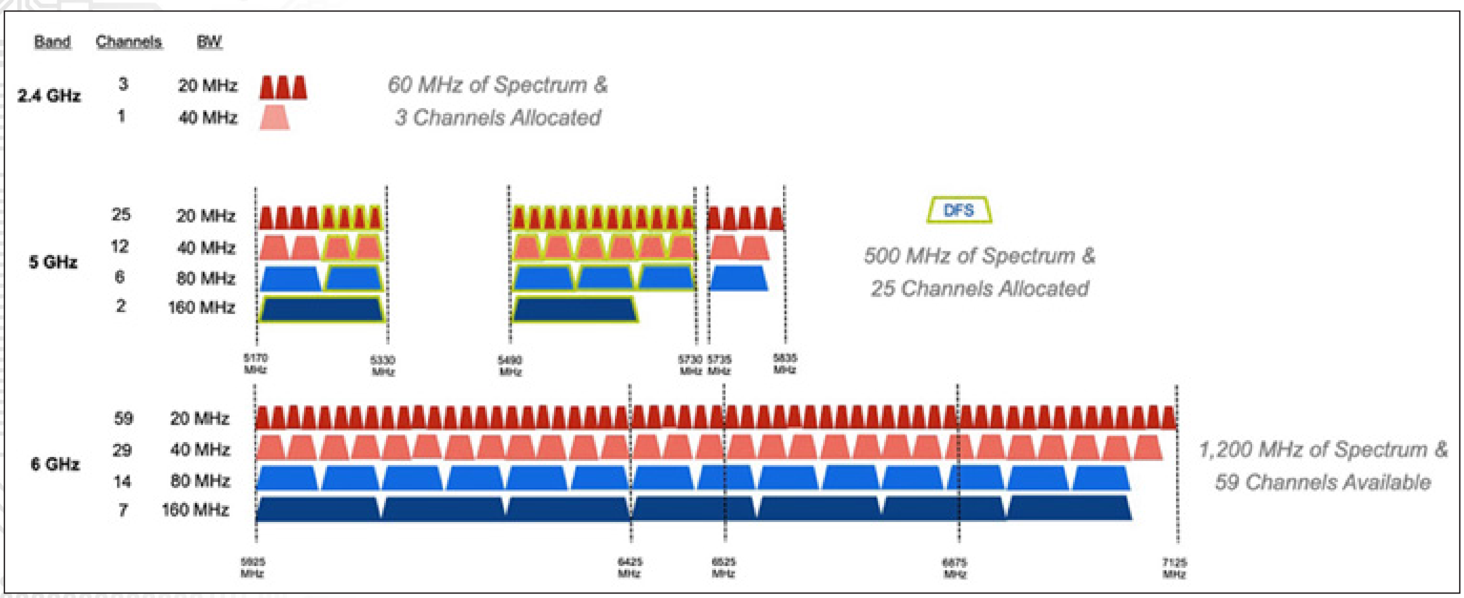
Low-latency applications such as gaming, VR/AR, and autonomous vehicles also require high levels of performance and reliability, whereas IoT applications often have wide networks of low-powered sensors all sharing data in real-time.

In response to these changing requirements, the FCC has authorized a new band of spectrum for unlicensed use. This section will explore the differences and benefits of the new Wi-Fi 6E standard and the 6- to 7-GHz band.

How Wi-Fi 6E Differs from Previous Standards

Early Wi-Fi standards, such as 802.11b, were first deployed in the late 1990s. They operated in a tiny sliver of the unlicensed 2.4-GHz ISM band from 2.400 to 2.495 GHz. With a narrow range and overlapping channels, the ISM band eventually became too crowded to cope with the increasing density of devices and growing bandwidth requirements.[4]

Though the first 5-GHz standards go back to the same period, widespread use became more common with the introduction of 802.11n, known today as Wi-Fi 4.[5] Operating from 5.170 to 5.835 GHz, this higher-frequency standard reduced the strain on the overcrowded



1. Wi-Fi 6E supports 14 non-overlapping 80-MHz channels and seven non-overlapping 1. Wi-Fi 6E supports 14 non-overlapping 80-MHz channels and seven non-overlapping 160-MHz channels, a significant improvement over previous 2.4- and 5-GHz standards.

2.4-GHz band and improved speed, reliability, capacity, and bandwidth. Further performance improvements were realized as technology advanced and new standards were launched, specifically 802.11ac (Wi-Fi 5) in 2013 and the more recent 802.11ax (Wi-Fi 6) in 2018.

With its approval from the FCC, Wi-Fi 6E represents one of the largest and most significant additions to Wi-Fi in its history. It has the potential to dramatically boost speed, bandwidth, capacity, and reliability while reducing congestion, latency, and power requirements. Put simply, it will increase the amount of spectrum available for routers and other devices by nearly a factor of five, resulting in more bandwidth and less interference.[6]

The biggest and more important change for RF security professionals is that Wi-Fi 6E will use the 6- to 7-GHz band ranging from 5.925 to 7.125 GHz. Previously used to support utilities, public safety, and wireless backhaul, unlicensed devices will now be allowed to share this spectrum through a regulatory framework that protects existing users while allowing for more efficient use of the wireless spectrum.

Wi-Fi 6E will support 14 additional non-overlapping 80-MHz channels and 7 non-overlapping 160-MHz channels, a dramatic improvement from the 20-MHz non-overlapping channels currently available in Wi-Fi [5] (**Fig. 1**). Combined with advanced channel-allocation technology, this will greatly reduce congestion and interference for users in high-density environments such as office buildings, apartment complexes, or large public venues.

In addition, Wi-Fi 6E will dramatically improve speed and latency. One industry report suggested that the average fixed-broadband download speed would increase to 280 Mb/s by 2022, more than double the current U.S. average of 137 Mb/s.[7] Tests have demonstrated latency levels as low as 2 to 5 ms.[8]

Of course, the tradeoff when dealing with higher-frequency signals is a decrease in propagation and range. Compared to 2.4- and 5-GHz signals, 6-GHz signals will travel shorter distances and be more susceptible to physical barriers such as buildings, walls, trees, and other obstacles. In larger spaces, multiple access points will be required to ensure coverage and maintain reliability.

Finally, Wi-Fi 6E will only be accessible to new devices that support the standard and will have no backward compatibility. Early entrants should encounter a nearly clear playing field, away from the congestion and interference of the 2.4- and 5-GHz bands.

With so many advantages and the potential for substantial performance improvements, it's no surprise that Wi-Fi 6E devices are expected to become prevalent in 2021. One IDC research director estimates there will be more than 338 million devices entering the market by the end of the year, and nearly 20% of all Wi-Fi 6 device shipments will support the 6-GHz band by 2022.[9]

The resulting increase in broadband speeds, combined with the accelerated deployment of IoT and other advanced technologies, is expected to generate more than US$180 billion in revenue over the next five years.[10] So how does this affect RF security, and how will equipment requirements shift as new Wi-Fi 6E-enabled devices enter the market?

The Changing Nature of RF Security

RF security has evolved over the years as devices, hackers, and covert surveillance products became more sophisticated. For as long as there has been sensitive information, surveillance, and countersurveillance, operators have found new ways to evade and outsmart the other.

The widespread proliferation of low-cost, easy-to-use, and powerful wireless communications technology has made it relatively simple for governments, rival corporations, or even individuals to deploy surveillance devices, transmit sensitive information, and disrupt the wireless signal environment.

The following section shows how the new Wi-Fi 6E standard will change performance requirements for spectrum-analysis equipment used for TSCM and RF security applications.

What the New Standards Mean for Spectrum-Analysis Hardware

As mentioned earlier, the new standard operates in the range of 5.925 to 7.125 GHz, significantly higher than previous standards. Until now, most users were only concerned with signals below 6 GHz. Spectrum-analysis equipment, in turn, also was limited to these ranges. The result is that most existing TSCM and spectrum-analysis hardware deployed and used in the field today will be unable to detect and analyze these new 6- to 7-GHz signals.

This is an obvious issue for RF security professionals because they will basically be blind to these new devices, which presents a serious security vulnerability. It not only limits how users can detect and remove unauthorized devices, but it also prevents them from getting a complete view of the signal environment in their facility.

A second challenge is the width of the new band and channels. With 1.2 GHz of spectrum divided into 80/160-MHz channels, equipment with low instantaneous bandwidth (IBW) and sweep rates may miss out on sporadic and short-duration signals of interest.

Finally, as the requirements for TSCM and RF security rise in complexity and operators become more sophisticated, traditional sweeping techniques must be augmented with continuous, 24/7 coverage. Modern surveillance devices can store information and transmit it in short bursts outside of regular office hours to avoid detection by sweeps. Many also use frequency hopping or low-powered signals to further reduce the likelihood of detection.

Another consideration is that threats to RF security aren't necessarily malicious. For example, an employee may be unsatisfied with the connectivity in their office and decide to bring in a router from home to boost their connection. Similarly, an employee may forget to check their device before entering a SCIF or other restricted facility.

In such cases, the threat to RF security is the result of an honest mistake or accident rather than an intentional event. Continuous monitoring of the facility would allow security professionals to detect the transmitter and then take steps to remove or secure the device.

A Continuous, Software-Defined Approach to RF Security Applications

With much of the existing equipment currently deployed in the field unable to detect and analyze signals in the 6- to 7-GHz band, RF security and TSCM professionals will need to upgrade their capabilities. The question then becomes: What is needed to get the best coverage and ensure effective monitoring of the wireless spectrum?

Traditional, hardware-based spectrum-analysis equipment does provide the frequency range and bandwidth required for Wi-Fi 6E devices, but they are otherwise poorly suited for TSCM and security applications. Large, complex, and expensive, these solutions are designed for lab or manufacturing environments that require extremely high performance. On the other hand, existing handheld and low-cost analyzers do not generally cover the frequency ranges and bandwidths needed. Instead, users should consider the benefits of a software-defined approach to spectrum monitoring.

2. The Surveillance System developed by thinkRF includes real-time spectrum analyzers, a laptop, IP networks for multi-sensor deployments, Kestrel's TSCM Professional Software, omnidirectional antennas, and a carrying case for field deployments.

Real-Time Spectrum Analyzers and Surveillance Systems

In a software-defined spectrum analyzer, the software runs over a hardware layer. The hardware components tend to perform only the RF-to-digital conversion, allowing a standard PC or laptop to provide the necessary computing power.

An example of such an instrument is thinkRF's R5550-408 real-time spectrum analyzer, which provides a frequency range of 9 kHz to 8 GHz, 100 MHz of IBW, and a 28-GHz/s sweep rate. It enables users to monitor, detect, and analyze W-Fi 6E signals. It can be used either as an RF analyzer or as an RF downconverter for existing equipment.

This type of instrument can be integrated with specialized TSCM software such as Kestrel TSCM Professional Software from the Professional Development TSCM Group (PDTG). When combined with directional antennas and other equipment, users gain a complete surveillance system that allows them to conduct full-spectrum scans up to 8 GHz without additional upgrades (**Fig. 2**). Users can distinguish between friendly and unauthorized signals, demodulate the signal if required, and locate the source for removal.

Networked for remote deployment, multiple units can be deployed throughout a facility for continuous, 24/7 coverage. Information from static and roaming units is able to be sent to a centralized location for analysis, while real-time alerts and triggers can be configured to notify security professionals of an unauthorized or unknown signal. Users also can create a signal library, record data for post analysis, and generate reports.

This approach offers numerous benefits when used in addition to regular sweeps by TSCM professionals. Not only does it provide greater coverage, but it also ensures that users maintain a full view of the spectrum environment and can identify unknown signals from new Wi-Fi 6E-enabled devices operating above 6 GHz.

DR. NIKHIL ADNANI has over 25 years of experience in the area of wireless. He has held engineering positions at Nortel and Communications Research Centre Canada. Nikhil has a B.Sc. and an M.Sc. from the University of Manitoba and a Ph.D. from Carleton University, all in electrical engineering.

References

1. https://www.sandvine.com/hubfs/Sandvine_Redesign_2019/Downloads/2020/Phenomena/COVID Internet Phenomena Report 20200507.pdf
2. https://www.fcc.gov/document/fcc-opens-6-ghz-band-wi-fi-and-other-unlicensed-uses
3. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html
4. https://www.actiontec.com/wifihelp/evolution-wi-fi-standards-look-802-11abgnac/
5. https://www.cablefree.net/wireless-technology/history-of-wifi-technology/
6. https://www.fcc.gov/document/fcc-opens-6-ghz-band-wi-fi-and-other-unlicensed-uses
7. http://wififorward.org/wp-content/uploads/2020/04/5.9-6.0-FINAL-for-distribution.pdf
8. https://www.counterpointresearch.com/wi-fi-66e-a-viable-alternative-to-5g-nr-for-low-latency-applications/
9. https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-delivers-wi-fi-6e-certification-program
10. http://wififorward.org/wp-content/uploads/2020/04/5.9-6.0-FINAL-for-distribution.pdf
11. https://www.everythingrf.com/community/what-frequency-band-does-wi-fi-6e-use

to view this article online, click here

BACK TO TABLE OF CONTENTS

image courtesy of Dreamstime

CHAPTER 2:

11 Myths About Wi-Fi 6 and 6E

ANDREW ROSS, Senior Product Manager, *Laird Connectivity*

Laird Connectivity's Andrew Ross dispels common misconceptions about the features and impact that Wi-Fi 6 and 6E will have on IoT design.

The Wi-Fi Alliance has launched two new versions of Wi-Fi that deliver significant advances in performance, efficiency, latency, and other key areas: Wi-Fi 6 and 6E. Because Wi-Fi is such a ubiquitous technology in IoT design, there's always apprehension about changes to this core connectivity technology.

By dispelling the misconceptions, what becomes clear is that these new versions of Wi-Fi provide an even stronger foundation for consumer smart devices, IoT networks, and a wide range of enterprise and industrial use cases.

1. This is a minor update to Wi-Fi. It's really only significant for niche applications.
It's not an exaggeration to compare this upgrade to Wi-Fi to the leap from 4G to 5G in the cellular world. Wi-Fi 6 and 6E will deliver major advances in performance and features that make it enormously impactful across the full range of IoT devices.

2. It looks faster. That's the biggest upgrade.
"Faster" just scratches the surface of why Wi-Fi 6 and 6E are better options. Greater device density and much-increased spectrum gives engineers more flexibility, reliability, and performance, making it the most efficient version of Wi-Fi ever delivered. Don't forget the major gains in energy efficiency, latency, and features that support both existing and new use cases.

3. The claims I've seen about speed feel like hype. It's silly to compare this to the jump in performance in cellular from 4G to 5G.
I'm always skeptical about speed claims in marketing materials, but the boost in speed is legitimate. I've read test results from respected people in the industry who have achieved increases in download speeds of 1,000%. And those results match what my own team has seen working with the technology. Part of how Wi-Fi 6 makes this happen is through its low-power claims, so that the download times and power don't waste energy.

There's a long list of data-intensive IoT use cases that benefit greatly from this increase in speed. Factory and building automation is a key one. So are automation systems in industrial settings, as well as use cases where high-quality video and audio are important requirements.

4. MIMO technology is probably the main driver for such an increase in speed. It's not big news—lots of technologies now have that.

The inclusion of MU-MIMO is a major factor, but just crediting that technology discounts how significant this upgrade is in Wi-Fi 6 and 6E. In addition to doubling the number of spatial streams using MU-MIMO, the performance of those streams is dramatically increased using beamforming techniques. Adding the ability to implement bidirectional MU-MIMO Wi-Fi 6 is the first version of Wi-Fi that allows users to access the full benefit of beamforming in noisy environments. Wider channels that include space in the 6-GHz spectrum also contribute greatly to the boost in speed.

Moreover, Wi-Fi 6/6E's extension of quadrature-amplitude-modulation (QAM) architecture is a big deal. It's the equivalent of putting a much more powerful engine into Wi-Fi, making the massive increase in speed possible.

5. I'll give you that Wi-Fi 6 is faster. But latency is still an issue.

Yes, Wi-Fi isn't yet a fit for ultra-low-latency applications like medical devices, where latency is so vitally important. But that doesn't mean that the latency improvement in Wi-Fi 6/6E isn't significant.

Latency is approximately 3X lower than prior versions of Wi-Fi, so it may not be ready for real-time applications, but it's very close. Just as valuable is how the new version of Wi-Fi manages packets more efficiently, removing empty space so that network utilization nears 100%. Those two factors make this a major upgrade for latency-sensitive applications such as robotics, lighting controls, machine controls, and more.

6. My IoT devices don't have a lot of data to transfer, and I don't need real-time data transmission, so these latency improvements aren't relevant to me.

Wi-Fi's lower latency has a surprise benefit for battery-powered IoT devices: longer battery life. The faster speed and lower latency of Wi-Fi 6/6E reduces the amount of time (and energy) it takes for devices to send and receive data. Even when small batches of data are being sent and received, those small energy savings add up over time.

I expect further testing to reveal that these performance upgrades in Wi-Fi will add months or even years to some of the most common low-energy IoT devices.

7. Greater device density will be great for consumer environments, like when all of the kids in a family are streaming on their devices. But it's not as important for my IoT deployments.

Yes, anything that reduces family fights over connectivity is a very good thing. But every Wi-Fi network experiences congestion, which often creates performance issues that have become frustrating in high-density RF environments like healthcare facilities, airports, and schools.

By using MU-MIMO, beamforming, OFDMA, more efficient packet management, BSS Coloring, and other features allows networks to support far more devices in a given physical space while also reducing the RF noise and interference that often plagued high-density environments in the past. This also can save on the cost of infrastructure deployment, as it requires far fewer access points to support the high client counts.

8. This new version of Wi-Fi is all about speed. Hopefully, they will focus more on battery life in the next version.

No need to wait for a more battery-friendly version of Wi-Fi. This version delivers on it in a big way.

I already mentioned that this is the most efficient Wi-Fi version and discussed the impact of lower latency and packet management on battery life. But Wi-Fi 6 and 6E also have a redesigned architecture that utilizes target-wake-time (TWT) technology to manage sleep and wake cycles in a far more energy-efficient way. In addition, TWT allows you to tailor your power versus performance by application across your network by being on a per device or group level rather than the traditional singular entry access point or network level.

If you like working with prior technologies like PS-Poll (DTIM) and WMM (APSD), don't worry. Both are still available, but TWT is a major step forward because it enables much longer sleep times for clients that preserve battery through extended inactivity while remaining connected to the network.

9. The marketing about Wi-Fi 6 and 6E talks a lot about 6-GHz spectrum, but that's only relevant for advanced wireless engineers.

I don't blame you if all the GHz talk gives you a giga-headache. Discussions of radio frequencies and spectrum bands can get lost in the weeds very quickly but 6-GHz spectrum is big news for every designer of IoT devices.

Wi-Fi 6 and 6E make it simple for engineering teams to have far more wireless real estate for their networks, allowing them to optimize the performance of their devices. Got a low-latency application that you don't want to compete for bandwidth with other devices? Assign it a segment of spectrum dedicated to that use case and keep other devices in other segments of available Wi-Fi spectrum.

The process doesn't require an advanced degree in radio-frequency engineering. The new version of Wi-Fi makes it simple to put networks in portions of spectrum that best suit the application and your preferences.

10. These features may sound great, but antennas will no doubt lag behind and stand in the way of real-world deployments.

In this case, antennas are actually ahead of the curve. Antenna manufacturers have anticipated the use of technologies like MU-MIMO and beamforming, and they laid the groundwork for use of the 6-GHz spectrum by Wi-Fi. A wide range of options exist in the form factors that are most common for IoT devices, including flexible planar inverted-F antennas (PIFAs). The bottom line is that antenna availability thankfully will not hold back your deployment plans.

11. This version sounds plug-and-play. I won't have to alter much in my designs.

Any engineer who has worked with Wi-Fi in the past will feel comfortable working with Wi-Fi 6/6E, but there are some caveats. A few changes to hardware interfaces and logical interfaces have changed from prior versions of Wi-Fi. On the plus side, though, there's much broader OS support for Linux, Android, and RTOS, as well as full support for the latest Bluetooth versions and features.

Using Wi-Fi 6/6E will mean changes for some detailed aspects of your engineering projects. However, the dramatic improvements in speed, latency, performance, battery efficiency, and more make this well worth the adjustments needed to incorporate this new connectivity technology into your IoT strategy.

to view this article online, click here

BACK TO TABLE OF CONTENTS

image courtesy of Dreamstime/Elnur

CHAPTER 3:

Why Wi-Fi 6 Will Be a Key Component of Tomorrow's IoT

KARL H. TORVMARK, Technical Product Manager, *Nordic Semiconductortor*

The champion of consumer connectivity, Wi-Fi's latest version further boosts user accessibility and throughput. But the changes also were made with one eye on wireless sensor networks.

Wi-Fi has a complex history. That's perhaps not surprising since the radio technology represents a melding of many innovations, four of which stand out. The first was the development of a pioneering packet-radio network in Hawaii during the 1970s. ALOHAnet connected seven campuses on four islands across the archipelago, ensuring that they could all communicate with each other through a central computer on Oahu.

Second, in 1985, the U.S. Federal Communication Commission (FCC) formalized the use of the 2.4-GHz spectrum (among other allocations) for unlicensed industrial, scientific, and medical (ISM) use. The move encouraged commercial organizations to consider how they could make use of this new radio resource.

Then, in the 1990s, radioastronomy scientists at Australia's Commonwealth Scientific and Industrial Research Organization (CSIRO) worked out a way to overcome the multipath problems that afflicted indoor, high-throughput radio communications. The invention formed the basis of wireless local-area networks (WLANs) and paved the way for widespread Wi-Fi deployment.

Finally, an Institute of Electrical and Electronic Engineers (IEEE) standards committee was formed and tasked with defining the physical-layer (PHY) and media-access-control (MAC) specification for a WLAN protocol dubbed IEEE 802.11. The target application was "wireless Ethernet," using RF technology to link computers together in the fashion pioneered by wired networking.

The committee's work resulted in the first version of the Wi-Fi specification, IEEE 802.11-1997, which was published in June 1997. Then a 1999 amendment to the standard introduced the technology upon which today's versions of Wi-Fi are largely based. The Wi-Fi Alliance was formed to commercialize the technology.

Power and Deployment Challenges

Now there's a fifth key event influencing Wi-Fi's evolution—the Internet of Things. It's a phrase that was still two years away from being coined—the term was dreamt up in 1999 by Kevin Ashton, an executive working to promote RFID—when the first version of Wi-Fi was officially adopted. Today, connecting billions of devices (or "things") to the established internet is largely being achieved by wireless technology.

For short-range IoT networks, Bluetooth Low Energy (BLE), Thread, Zigbee, and other protocols are shouldering the load. For the IoT's wide-area networks (WANs), LTE-M/NB-IoT (cellular IoT) and LoRaWAN are proving good options. But what of Wi-Fi? At first glance, it would appear to be the perfect option for wireless networks needing greater range than that provided by the short-range, low-power protocols, but not the kilometer-plus range of the WAN technologies. However, closer inspection reveals Wi-Fi has some considerable drawbacks for IoT applications.

The first problem is power consumption. Wi-Fi was primarily designed for good throughput, which costs battery power. In contrast, IoT wireless technologies typically try to limit on-air time to extend battery life and hence minimize maintenance. The tradeoff is lower throughput, but this is hardly an issue for sensors and actuators that only infrequently send small amounts of data.

Second, Wi-Fi struggles in dense deployment scenarios. Many of us are familiar with patchy service when accessing public hotspots in busy malls and libraries. It's annoying, but consumers can typically afford to be tolerant. Industrial networks comprising hundreds of sensors are a different matter.

Built for the IoT

Now a version of Wi-Fi, technically named IEEE 802.11ax and marketed as Wi-Fi 6, promises to address the deficiencies that have hampered the technology's widespread adoption for the IoT. Approved by the Wi-Fi Alliance earlier this year, Wi-Fi 6 was specifically designed to meet the requirements of dense deployments, both public and industrial. The new version offers several enhancements, but the headline features are improvements to throughput and spectral efficiency, which allow for more network connections while still maintaining good service.

For example, with the new orthogonal frequency-division, multiple-access (OFDMA) feature, devices can use less than one channel bandwidth, sharing the bandwidth with other devices on the network to increase capacity. Moreover, these technical advances also enable faster response to and from connected units. Where previous versions of Wi-Fi struggled to cope with more than a few sensors, Wi-Fi 6 can comfortably manage large sensor networks comprising hundreds of devices.

Wi-Fi 6 also brings a key technical enhancement for smart-home and -industry applications. Called "target wake time" (TWT), the advance is a significant evolution over the power-saving efforts of prior generations of Wi-Fi.

When using the TWT technology, client devices negotiate wake-up times with access points (APs). Therefore, the clients needn't stay awake to maintain the wireless connection. As a result, an AP can aggregate large groups of client requests into fewer triggered transmit opportunities. The benefits are more efficient, contention-free channel access and significant client-device power savings—up to 80% in like-for-like applications. That makes IoT devices with long battery lifetimes more practical.

Wi-Fi 6 also brings improved security using Wi-Fi Protected Access (WPA) 3 (although this was rolled out separately to Wi-Fi 6). WPA3 uses the Simultaneous Authentication of Equals (SAE) protocol in place of the Pre-Shared Key (PSK) protocol common to older WPA2 protection. SAE prevents some brute-force attacks that could be used against routers employing PSK.

Another key advantage of Wi-Fi 6 is that it offers IoT sensors direct connection to the cloud through routers without having to pay additional data subscriptions. Furthermore, the technology's higher throughput compared to other short-range wireless solutions enables new use cases like wireless security cameras and high-quality video doorbells. The additional throughput also can be used to complement Bluetooth during the transfer of large amounts of data, such as music streaming in wearables.

Wi-Fi for the Smart Home

The Connectivity Standards Alliance—an organization aiming to ease the challenges of connecting devices using different wireless protocols—is backing Wi-Fi 6 as a foundation technology of the smart home. Matter, the alliance's unified IP-based connectivity protocol, is designed to run over Wi-Fi 6 (and older versions) in addition to Ethernet and Thread (and for ease of commissioning, BLE).

The CSA initiative will see the widespread introduction of "border routers." Such devices aren't a new concept. However, until now, vendors were forced to develop their own solutions. The product is a specific type of router that provides connectivity from an IEEE 802.15.4 network to adjacent networks using other physical layers (such as Wi-Fi). Border routers could be routinely embedded into items such as smart speakers and lighting fixtures, making Internet Protocol (IP)-based connectivity more convenient for both vendors and consumers.

Industrial Wi-Fi 6 products are only just starting to reach the market. In a few years, though, we'll see short-range wireless, Wi-Fi 6, and cellular IoT complementing each other to build the large, robust, and low-latency networks needed for the IoT to deliver on its promise. Nordic Semiconductor, a leading developer and manufacturer of all three wireless technologies, hopes to be in the vanguard of that revolution.

to view this article online, *click here*

BACK TO TABLE OF CONTENTS

image courtesy of AdobeStock

CHAPTER 4:

A Game Changer for Wireless Clinical Devices:

The Impact of Wi-Fi 6/6E on Connected Medical Devices in Hospital Settings

ANDREW ROSS and DAN KEPHART, Senior Product Managers, *Laird Connectivity*

Wi-Fi networks are the indispensable backbone for connected medical devices in hospitals. Because of its performance, reliability, flexibility, security and other advantages, Wi-Fi has become the dominant connectivity technology for clinical devices such as pulse-ox sensors, infusion pumps, patient monitors, defibrillators, ventilators, beds, and more. It has become a victim of its own success in medical environments, leading to the danger of congestion in an environment where the performance of these devices is so vital. As the number of Wi-Fi connected devices increase in hospitals, Wi-Fi networks can become overwhelmed not only by the number of devices making demands on the network but also the RF complexity of so many networks and devices operating alongside one another in close proximity.

Wi-Fi 6/6E delivers significant advancements in performance, efficiency, latency and other key areas of performance that collectively enable far more device density while avoiding network congestion. Simply put, this new version of Wi-Fi is a gamechanger for hospitals because it will enable Wi-Fi to continue serving as the backbone of hospital connectivity, even as device density increases and as new devices put greater demands on networks. The advancements in Wi-Fi 6 and 6E are significant:

- **Dramatic increases in performance**
- **Far lower latency**
- **Wider spectrum for devices to utilize**

- **Extended battery life for mobile devices**
- **Support for much higher device density**
- **And other technical advancements that support new applications**

Before we continue, we should note that the benefits we discuss in this white paper will only be realized once the infrastructure to support Wi-Fi 6/6E is in place and operational in healthcare environments.

UL/DL MU-MIMO

Multi-User Multiple-In Multiple-Out (MU-MIMO) enables Wi-Fi gateways to create spatial streams that focus RF activity in the physical direction of each device in their domain. This is achieved by using two or more antennas and creating an intentional interference pattern to focus signals toward the intended device or groups of devices – creating a stronger link with each device using up to eight spatial streams.. This has the added benefit of reducing the overall volume of interference in environments with many gateways and devices, preventing the physical space from becoming saturated in signals that potentially interfere with the performance of the networks, devices and applications.

OFDMA

Orthogonal Frequency Division Multiple-Access (OFDMA) enables the gateway to talk simultaneously with multiple devices. OFDMA uses different subchannels to allow more devices to send and receive data than the prior version of Wi-Fi. Rather than all devices waiting in line for their turn to send or receive, they do so simultaneously, but in non-interfering subchannel spaces, which means they all enjoy much more immediacy via lower latency in their communications.

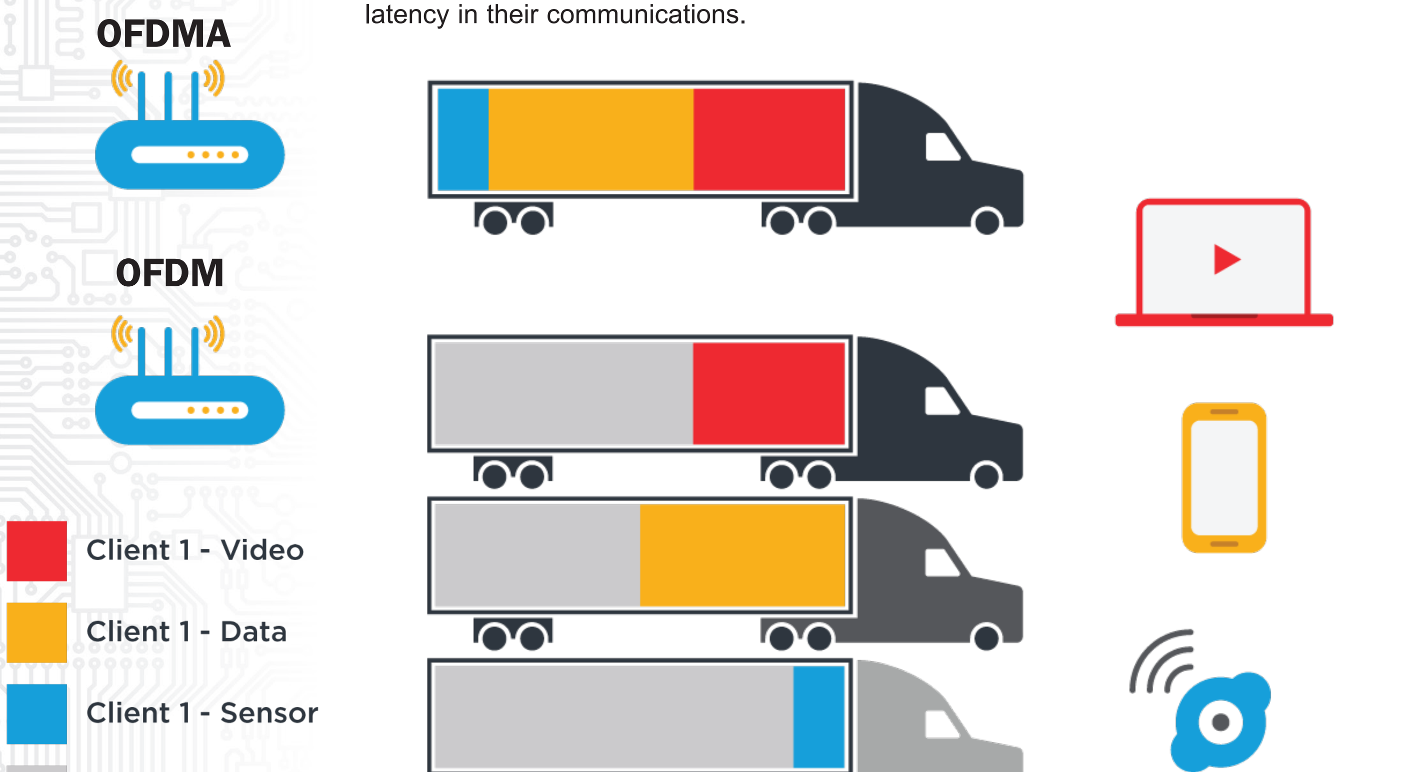
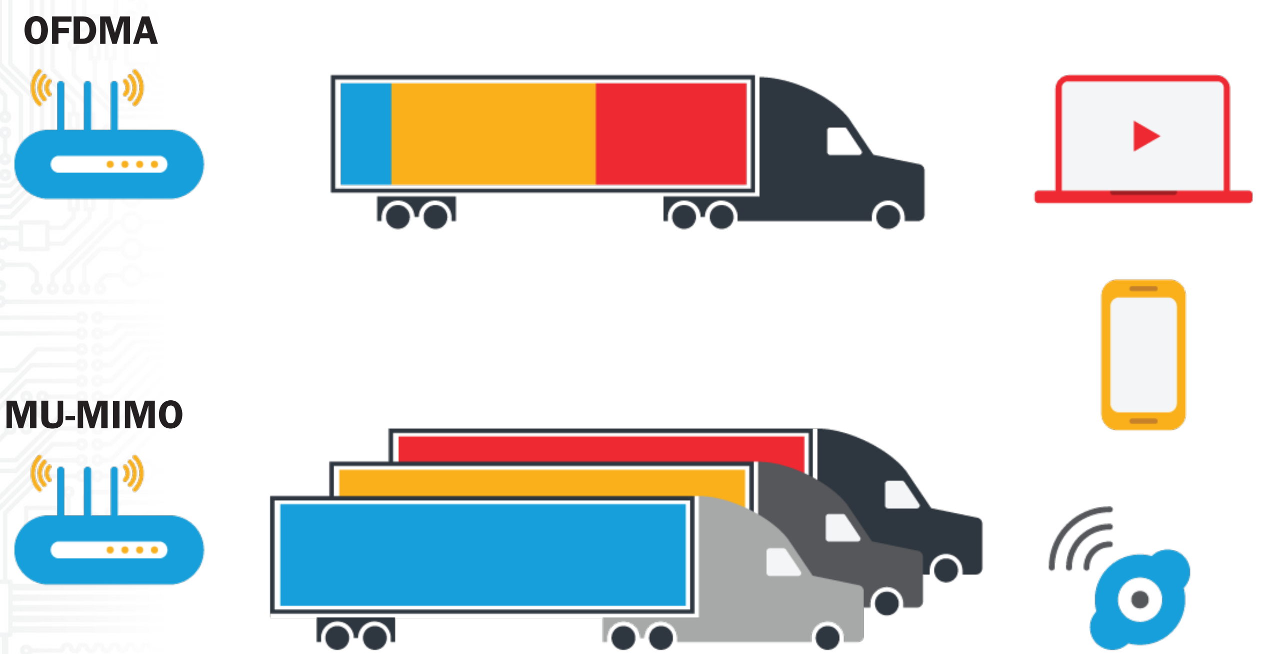


image courtesy of Laird Connectivity



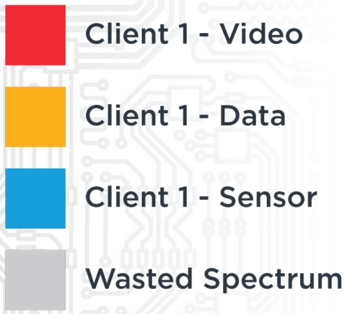


image courtesy of Laird Connectivity

BSS Coloring

Wi-Fi 6/6E is also designed to solve another source of congestion that is common in healthcare settings: overlapping Wi-Fi networks in the same physical space. Environments like clinics and hospitals often have a high proliferation of Wi-Fi gateways whose RF range overlap with one another.

BSS Coloring (Basic Service Set Coloring) addresses those challenges by providing an additional method to identify separate networks in areas where multiple gateways are overlapping. Prior versions of Wi-Fi struggled with overlapping networks, requiring devices communicating on overlapping channels to regularly pause communication. BSS coloring alleviates this issue by allowing the access point to clearly identify itself amongst traffic occurring on the same channel. By doing this clients associated to it can determine if the traffic is for it or another network and not delay transmission.

Faster Data Throughput

Wi-Fi 6/6E delivers a dramatic increase in data speed. On paper, the data throughput of Wi-Fi 6/6E increases to 9.6 Gbps from Wi-Fi 5's rate of 3.5 Gbps. As the number of devices continue to increase and as the applications on those devices become more bandwidth hungry, this massive increase in data speed enables Wi-Fi to continue being a reliable foundation for connectivity in hospitals.

Enhanced Device Roaming

One of the factors that make hospitals a more complex environment for Wi-Fi networks is how often connected devices physically move. Many devices regularly move with staff and patients from room to room or even from floor to floor rather than being in fixed positions.. Wi-Fi 6/6E has enhancements that better support roaming devices as they move into range of new access points. Wi-Fi 6/6E manages roaming devices far more effectively and efficiently through the use of features in 802.11r, 802.11k and 802.11v that manage those connections in automated ways that optimize connectivity for a given device.

Bolstered Security

The new version of Wi-Fi will utilize WPA3-Enterprise 192-bit security in all bands, allowing clinical devices to operate on more secure connections than the open, unencrypted WLANs that prior versions of Wi-Fi employed. Encryption is the centerpiece of WPA3-Enterprise's architecture. This brings encrypted connections to hospitals, ensuring the protection of patient data.

6GHz Spectrum

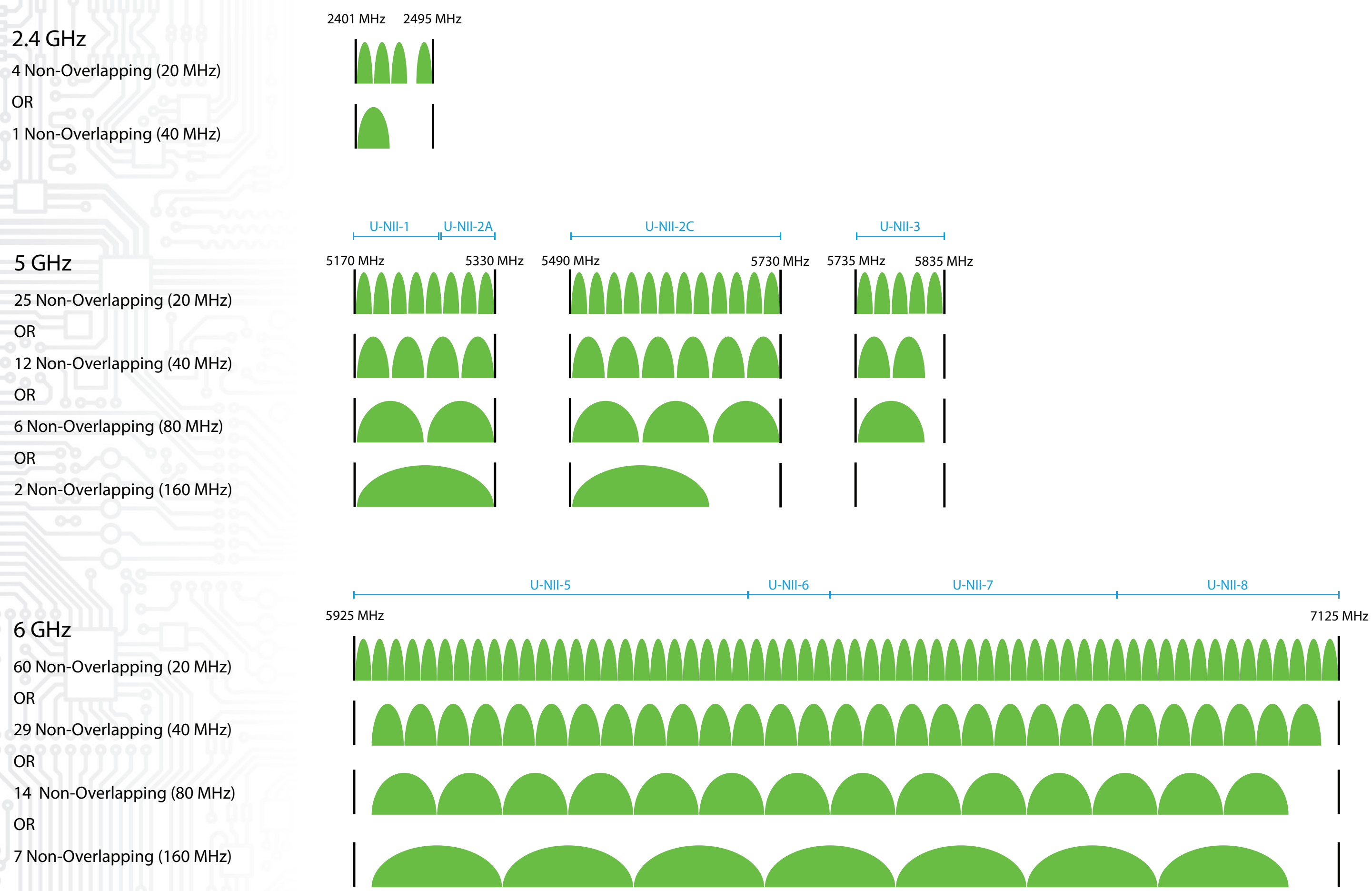
Another key advantage of Wi-Fi 6/6E for hospital environments is the almost doubling of its usable spectrum to include 6 GHz. This provides a tremendous amount of RF green field "real estate" for Wi-Fi networks to operate in, giving organizations a major tool for relieving network congestion

Energy Efficiency

The centerpiece of Wi-Fi 6/6E's low power strategy is Target Wake Time (TWT) technology. Prior technologies like PS-Poll (DTIM) and WMM (APSD) are still supported in the new version of Wi-Fi, but most engineering teams will want to take full advantage of TWT because it enables much longer sleep times for clients, preserving battery through extended inactivity while still remaining connected to the network.

Wi-Fi Channel Map

Note: Channel support varies by region. Channels shown are non-overlapping channels.



Sleep Negotiation with Negotiated Target Wake Time (TWT)

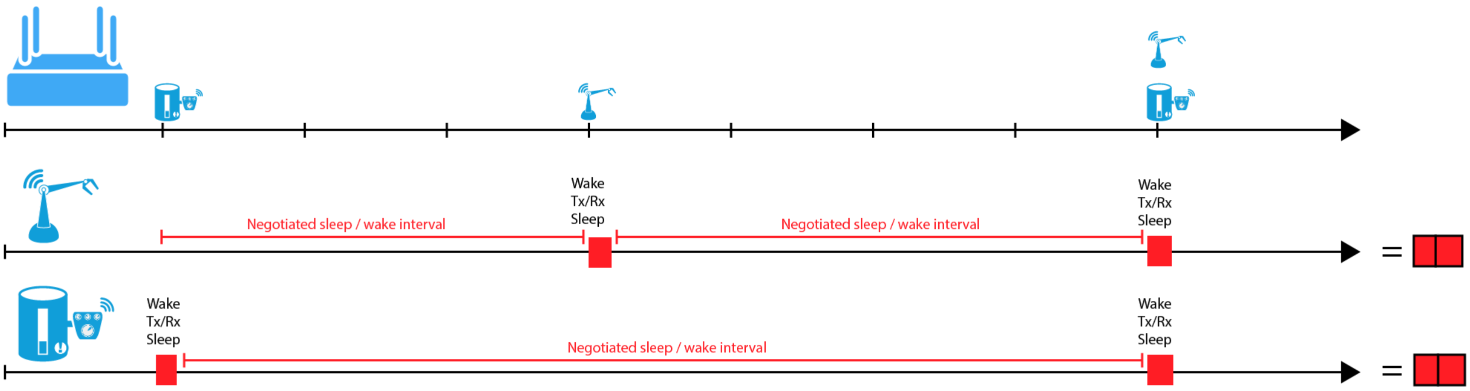


image courtesy of Laird Connectivity

Other Advantage of Wi-Fi 6/6E

In addition to the benefits discussed above, Wi-Fi 6/6E has a number of other advantages for hospitals. One important one is data integrity, which is a critical issue given the mobility of so many medical devices. The enhanced connectivity that Wi-Fi 6/6E delivers ensures that there is no loss of data as a patient or devices moves through a hospital. Another advantage of Wi-Fi 6/6E is its ability to accommodate surges in demand connectivity, for example when there is a surge of patients into the emergency room or during a public health emergency. The faster performance of Wi-Fi 6/6E will make it easier for transferring and accessing large medical files such as MRIs, X-rays, ultrasounds and medical records. Performance will also be better for hospital applications that use the same Wi-Fi networks as clinical devices, including telehealth sessions, calls and videoconferencing.

image courtesy of AdobeStock

About Laird Connectivity's Medical Device Solutions

Laird Connectivity, as a premium module provider, is committed to providing a full and diverse Wi-Fi 6/6E product line to address the demands and applications of the medical market. Our Sona Wi-Fi 6/6E products combine the best technology and module partner together:

- Sona IF573: High Performance Wi-Fi 6E with Bluetooth 5.4 Powered by Infineon
- Sona IF513: Low Power Wi-Fi 6E with Bluetooth 5.4 Powered by Infineon
- Sona MT320: Genio Focused Wi-Fi 6E with Bluetooth 5.3 Powered by Mediatek
- Sona NX611: Flexible Wi-Fi 6E with Bluetooth 5.3 Powered by NXP

Laird Connectivity also provides a range of simple-to-implement antennas that support 2.4GHz, dual-band 2.4GHz/5GHz, and Wi-Fi 6E 2.4/5/6GHz to help your devices achieve optimal performance:

- The FlexMIMO /FlexMIMO 6E MIMO Internal Antennas – The world's first Flexible PIFA antenna for Wi-Fi MIMO applications (patent pending). The FlexMIMO is specifically designed for 802.11 a/b/g/n, 802.11ac, and now Wi-Fi 6E modules that use MIMO or Wi-Fi Diversity.
- FlexPIFA / FlexPIFA 6E Flexible Adhesive-Backed PIFA Internal Antennas – Laird

Connectivity's FlexPIFA™ antennas (patented) are the industry's first flexible Planar Inverted-F Antennas (PIFA). The new 2.4/5/6 GHz tri-band FlexPIFA™ 6E is a true Wi-Fi 6E antenna developed to cover all three Wi-Fi bands 2.4/5/6 GHz (802.11ax standard) in a single, compact format.

- **Mini NanoBlade Flex / Flex 6E Series Internal Antennas** – The Laird Connectivity Mini NanoBlade Flex and Flex 6E Antennas now include models supporting the latest Wi-Fi 6E standard. This new tri-band standard covers 2400-2500, 4900-5925, and 5925–7125 MHz to support the highest data rates possible.

For more information about Laird Connectivity's Wi-Fi 6/6E solutions, visit: https://www.lairdconnect.com/market/wifi-6-and-wifi-6e#follow-our-wifi-6-series.

About the Authors

ANDREW ROSS is a Senior Product Manager at Laird Connectivity, where he leads the company's product development for Wi-Fi technology. He is responsible for development of Laird Connectivity solutions that help companies around the world take advantage of the next generation of Wi-Fi. Ross has more than 30 years of engineering experience in electronic design, including prominent engineering and product development roles at Silex Technology, B&B Electronics, Quatech, DPAC Technologies and Mosaic Semiconductor.

DAN KEPHART is also a Senior Product Manager at Laird Connectivity. In this role, he leads development of solutions utilizing multiple wireless technologies including Wi-Fi, Bluetooth, and cellular. He has 15 years of experience in the engineering and wireless design industry, and he earned his degree in computer engineering from the University of Akron.

BACK TO TABLE OF CONTENTS