

Wi-Fi 6E is Reshaping RF Security Requirements

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.

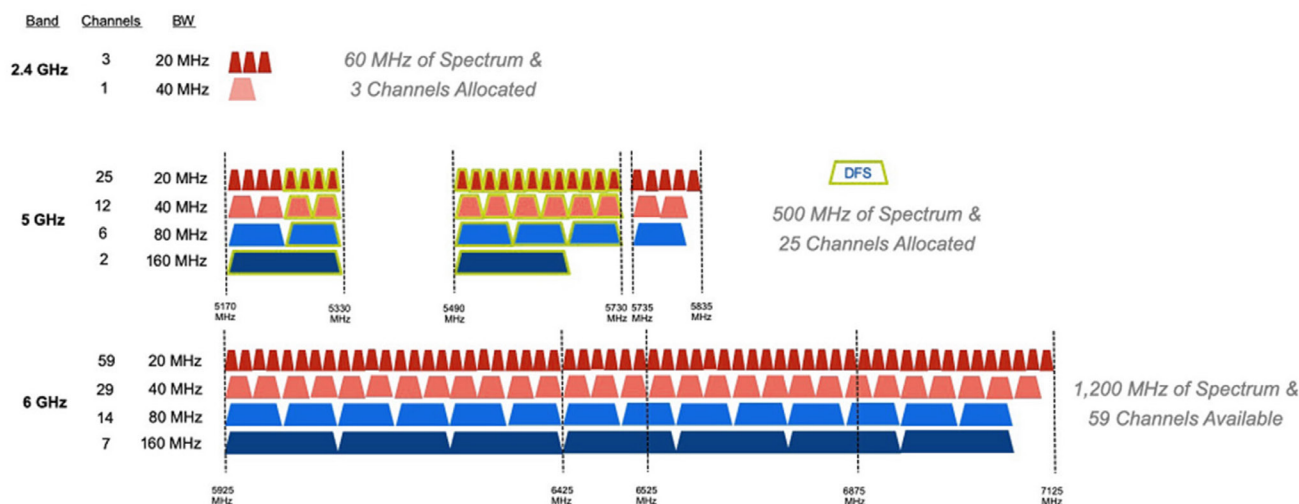
Low-latency applications such as gaming, VR/AR, and autonomous vehicles also require high levels of performance and reliability, whereas IoT applications often have wide networks of low-powered sensors all sharing data in real-time.

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



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.

Operating from 5.170 to 5.835 GHz, this higher-frequency standard reduced the strain on the overcrowded 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.

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



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.

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](https://www.sandvine.com/hubfs/Sandvine_Redesign_2019/Downloads/2020/Phenomena/COVID%20Internet%20Phenomena%20Report%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/](http://wififorward.org/wp-content/uploads/2020/04/5.9-6.0-FINAL-for-distribution.pdf)

[uploads/2020/04/5.9-6.0-FINAL-for-distribution.pdf](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/](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>