Networking Handbook

January 2019

802.11ax Wi-Fi and training act as paths to better security

TechTarget

In this handbook:

Brave new wireless: 802.11ax Wi-Fi promises big LAN changes

ALISSA IREI, SENIOR WRITER

Shakespeare *didn't* have wireless LANs in mind when he wrote *The Tempest*, but the promises of 802.11ax Wi-Fi leave us paraphrasing it:

> O, wonder! / How many goodly [features] are / there here! / How beauteous [ax] is! O brave / new [wireless], / that has such [efficiency] in't!

As a wireless end user with a predilection to Instagram Red Sox games and Beyonce concerts, I'm particularly excited about the orthogonal frequency-division multiple access (OFDMA) feature. While it doesn't roll off the tongue like the lyrics of "Single Ladies," OFDMA should be a crowd-pleasing hit in high-density environments.

Experts say OFDMA puts the "high-efficiency" in high-efficiency Wi-Fi by allowing access points (APs) to multitask and serve multiple clients at once. After an 802.11ax Wi-Fi upgrade, previously overrun 802.11n or 802.11ac APs could theoretically manage heavy user loads with aplomb.

In this handbook:

(No more #latergrams.) OFDMA marries faster speeds with new network smarts, arguably the most substantive functional change in 802.11 standard history.

Speaking of history, wireless technology has come a long way since the late '90s and early aughts, when end users thought of 802.11a/b as a nice-to-have novelty in a wired-first world -- if they thought about it at all. Fast forward two decades: Wireless outstrips Ethernet in many environments and is the need-to-have network, with end users expecting service everywhere, from elevators to public restrooms. Demands on the wireless-first LAN keep growing; it makes sense the next standard should perform not just faster and better, but differently. On paper, 802.11ax Wi-Fi fits the bill.

Of course, we're not there yet. Even assuming timely, meaningful adoption in enterprise networks after the standard's ratification in 2019, features like OFDMA will remain academic without ax-capable clients to bring the benefits to life. To quote the Bard: "All that glitters is not gold." But I'm an optimist. Here's hoping 11ax amounts to more than just the shiny object du jour.

In this handbook:

11 common wireless security risks you don't have to take

KEVIN BEAVER

Wireless security risks are not something we talk much about anymore, but they do have an impact on the overall safety and resilience of your network. I occasionally see overly paranoid IT and security professionals who recommend against using Wi-Fi altogether.

These are the same people who often proclaim the sky is falling due to some niche security vulnerabilities that don't matter to most businesses. Anyway, I'm not a big believer in avoiding something when there are opportunities for compensating controls.

THE MOST COMMON WIRELESS SECURITY RISKS

With that in mind, do you fully understand the wireless security risks associated with your business? In my work performing independent vulnerability and penetration tests, I see a number of wireless-related flaws that create unnecessary business risks:

In this handbook:

1. Wireless access points (APs) and routers that fall outside the organization's patch management standards introduce vulnerabilities that can be exploited by both connected users and outside attackers -- i.e., the KRACK attack for which many systems are still vulnerable.
2. Wireless networks not monitored for attacks and other malicious use could help uncover bigger wireless security risks such as malware infections and data exfiltration.
3. Lack of visibility into the wireless network's signal spectrum can create a lack of control and can unnecessarily expose wireless signals outside of buildings. Knowing the wireless spectrum can also help alert IT and security personnel of new wireless devices -- hosts and APs -- seen in the vicinity.
4. Use of outdated wireless security protocols such as WPA and WEP makes for easy exploitation.
5. Wi-Fi Protected Setup enabled on consumer-grade wireless routers without intruder lockout allows an attacker to crack the WPS PIN and capture the WPA encryption key.
6. Network access control that does not include Wi-Fi in its scope can lead to a false sense of security and allow unauthenticated and improperly secured devices into internal parts of the network.
7. Web content filtering missing within the guest and, sometimes, production wireless networks can create issues with acceptable-usage policies that corporate HR mandates and can increase the risk of malware infections.

8. Guest wireless that allows access into internal production network subnets is brought about by a lack of reasonable network segmentation between the wired and wireless networks.
9. Indirectly, critical business systems like external-facing servers and web applications pose wireless security risks when running weak encryption ciphers and protocols, such as Rivest Cipher 4 and Triple Data Encryption Standard, Transport Layer Security 1.0, and Secure Sockets Layer 2.0.
10. Wireless networks that are out of scope with existing security policies and response plans leave indefensible gaps in the event of an incident or breach.
11. WPA2 -- the most common security protocol currently running on wireless networks -- is vulnerable to dictionary crack attacks. (However, I have found that most businesses that use reasonably long and complex passphrases or keys can minimize this risk.)

Some of these vulnerabilities are more critical in nature than others. It just depends on the context. Regardless, if there are known wireless security risks and there's something that you can do to reduce them (often for free), then why not eliminate them? Formal wireless security vulnerability and penetration testing is one option, but sometimes this task isn't performed at all. But you cannot secure what you don't acknowledge.

HOW CAN WPA3 PREVENT WIRELESS SECURITY WEAKNESSES?

The forthcoming WPA3 wireless security standard can help mitigate current Wi-Fi weaknesses through features such as the following:

- a new key exchange protocol that will effectively eliminate dictionary attacks;
- perfect forward secrecy to help prevent hackers from cracking previously captured traffic;
- Wi-Fi Easy Connect, which simplifies and secures the wireless connectivity process that used to be handled by Wi-Fi Protected Setup; and
- opportunistic wireless encryption that protects unauthenticated or open service set identifier connections.

The best thing is to acknowledge your wireless ecosystem has security holes in it. This is even more likely when you have users connecting to random wireless hotspots at home, while traveling and so on. Even if you eliminate all the above vulnerabilities and implement WPA3, your business can be exposed to someone mimicking a legitimate AP -- the "evil twin" vulnerability, which has been around since the inception of Wi-Fi. Not only can an evil twin attack exploit network systems and information, but when it does happen you'll likely never know about it. The evil twin vulnerability can be mitigated using a wireless intrusion prevention system offered by many of the big networking vendors. Still, these systems won't protect your mobile users when they are out and about.

There's no amount of inherent Wi-Fi security in WPA3 or subsequent wireless security protocols that offsets poor wireless implementation and oversight.

It's not guaranteed to reduce wireless security risks, but some user training can go a long way. Talk to your users about what can happen -- and what has happened -- when connecting to vulnerable or exploitive

wireless environments. Encourage them to use VPN connections. Advise them to only connect to trusted wireless networks, to the greatest extent that you can. Tell them to never disable their endpoint security controls, especially their firewalls and antimalware software.

There's no amount of inherent Wi-Fi security in WPA3 or subsequent wireless security protocols that offsets poor wireless implementation and oversight. If you're smart in your approach to wireless and mobile security, you can keep your business assets under control while affording your users the computing freedom they're looking for. Ignore the known wireless vulnerabilities and you have yourself unmitigated risks that will be difficult to defend when something goes wrong. Wireless security risks are somewhat old-school, but the security spotlight is still on you and your team to mind the gaps and to see things through.

In this handbook:

802.11ax standard promises tectonic shift in wireless

ALISSA IREI, SENIOR WRITER

Longtime wireless LAN pros -- seasoned by years of relentless and frequently unfounded industry hype -- tend to approach the latest shiny new object with a healthy degree of skepticism. So, when network engineer Lee Badman recently asked his Twitter followers for their thoughts on the pending 802.11ax standard, the answers included more than a few digital eye-rolls.

"The hype hasn't even left the gate yet. Wait until it gets wound up," commented Devin Akin, founder and principal Wi-Fi architect of Divergent Dynamics, a Wi-Fi consulting and training firm in Carrollton, Ga. "Can't you hear it now, 'it's like a switch!' and '5 Gbps [access points]! (With dual 2.5G ports),' and 'No more surveys!' and 'heals cancer!' ... blah, blah, blah. #AmIWrong?"

And yet, the proposed 802.11ax standard -- currently in development at the Institute of Electrical and Electronics Engineers (IEEE) -- undoubtedly

has wireless experts' attention. Many, including Akin, have expressed particular interest in a high-efficiency feature called orthogonal frequency-division multiple access (OFDMA).

According to analyst Zeus Kerravala, founder and principal analyst of ZK Research in Westminster, Mass., OFDMA -- a variation on orthogonal frequency-division multiplexing -- helps make 802.11ax the first "fundamentally different" Wi-Fi standard in networking history.

To understand its functionality, Kerravala suggested imagining network clients as grocery-store shoppers and wireless access points as cashiers. Previous wireless upgrades addressed congestion issues by speeding up checkout transactions, with the line for an 802.11n register moving faster than the queue for an 802.11g device. The basic connectivity model stayed more or less consistent, though, with the same single-file lines for service.

Then, there's .11ax.

"If someone in front of you pauses to pull out a checkbook, the cashier can start ringing your stuff up right then and there, then go back to that person," Kerravala said.

In other words, instead of sitting idle during a dead spot in transmission, an 802.11ax access point can skip to another client's request. Kerravala said he expects that extra efficiency to provide better Wi-Fi connectivity for users and improve the battery life of their devices.

BRAVE NEW 'HIGH-EFFICIENCY' WIRELESS

In a world where end users increasingly carry two or three devices apiece -- and expect reliable, ubiquitous Wi-Fi connectivity as a rule, not an exception -- independent analyst John Fruehe said he believes the 802.11ax standard will ultimately transform wireless networking.

"It's a big deal," he said.

As a top use case, Fruehe cited high-density environments prone to intense bursts of user activity, such as event venues, hotels and schools. Picture Gillette Stadium during a Patriots game, for example, with fans uploading and downloading tens of thousands of social media posts, text messages, photos, videos and more.

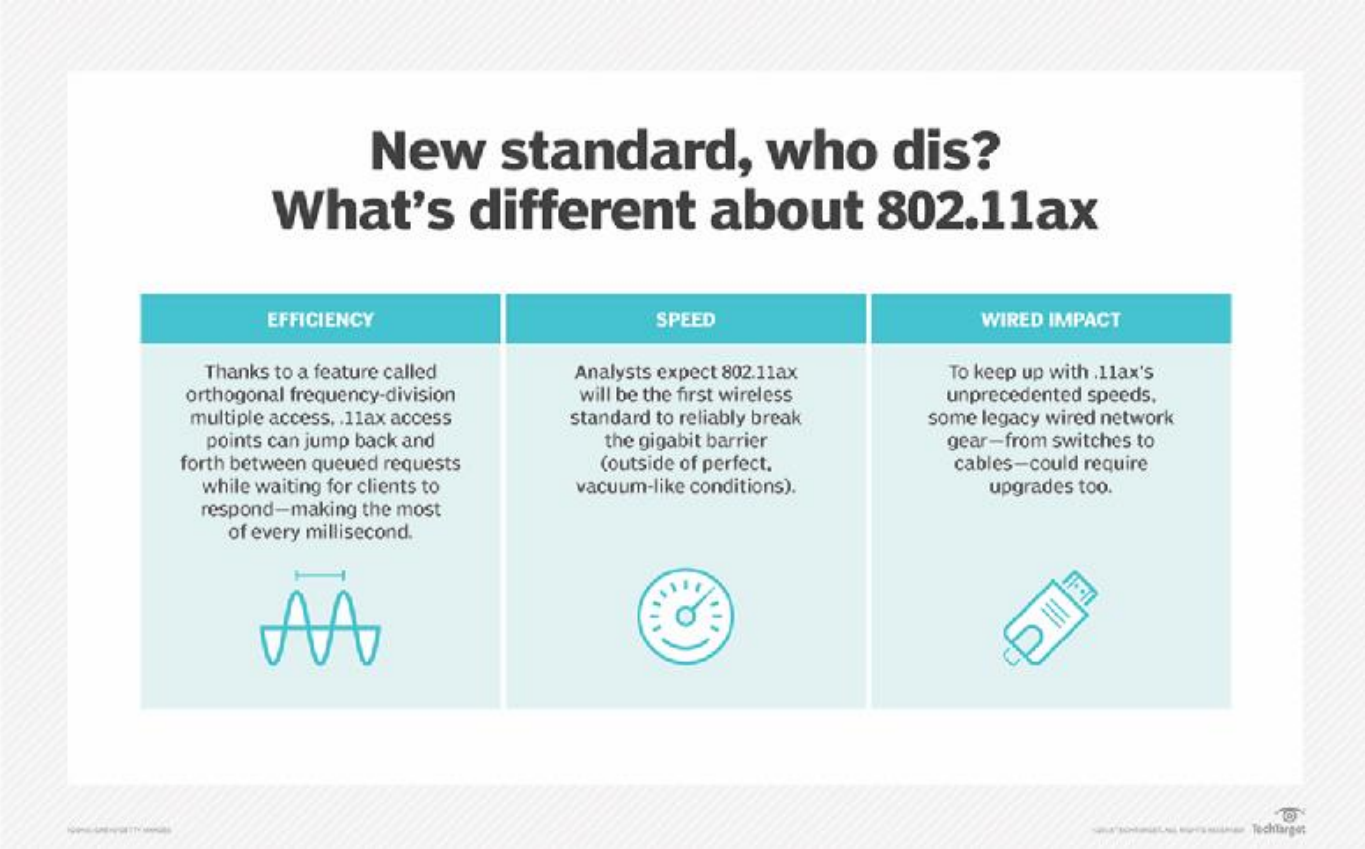
"Those are the places you'll see [802.11ax] become most valuable," Fruehe predicted. "It will be a no-brainer for them to make the jump."

One vendor, Aerohive Networks, started shipping 802.11ax access points in July 2018, reporting particular interest from customers in the education vertical. The company counts at least two academic institutions among its initial buyers -- the University of North Georgia in Dahlonega, Ga., and Wellington College in the United Kingdom.

"Some schools are just starting with .11ax in areas where they have the most density, like auditoriums and cafeterias," said Perry Correll, product management director at Aerohive, based in Milpitas, Calif.

Kerravala said the .11ax specification will also be the first Wi-Fi standard to break the Gigabit barrier -- outside of perfect, vacuum-like conditions. The increased speed has implications for the wired network, as plugging .11ax access points into a switch in which each port has a maximum capacity of 1 Gb each would create a bottleneck.

In this handbook:



"If you're going to do [802.11ax], then you do need to upgrade your wired network ... at least where you're likely to have congestion issues," Kerravala said. "And if you're upgrading your wired network today, you

need to think about it in terms of the next generation of Wi-Fi, which means multigig."

Necessary upgrades might also include network cabling, Kerravala added -- such as replacing any legacy CAT5 cables, which can't handle next-generation speeds.

TIMING IS EVERYTHING

Fruehe said he considers the current draft of the proposed 802.11ax standard stable enough for early adoption, but added he'd pay a premium to get .11ax today only to solve a specific problem, such as overrun access points in a high-density environment.

He also cautioned that despite the promise of 802.11ax standard, it will progress from draft status to widespread adoption like "a slow train."

Kerravala agreed, predicting network managers won't see many .11ax-capable devices until late 2019 or early 2020 -- and lacking clients, benefits of an upgrade will remain minimal.

"If you absolutely need to upgrade your Wi-Fi -- if it's hurting the business -- then, by all means, upgrade," he said. "But I think we're close enough now to having the standard ratified that I'd probably wait a couple of months."

I think we have a six-month-to-a-year window for planning, which is good, because this is such a different type of Wi-Fi.

Zeus Kerravala founder and principal analyst at ZK Research

The Wi-Fi Alliance expects to start its certification program for 802.11ax, which it recently dubbed Wi-Fi 6, in 2019. In the meantime, Kerravala urged networking teams to conduct site surveys ahead of .11ax adoption. Because the new standard has different signal strengths and coverage patterns, using beam-forming technology instead of the traditional cellular approach, an upgrade will require more planning than simply swapping out existing access points.

"I also advise thinking about Wi-Fi in the broader context of 'wireless everywhere,'" Kerravala said, pointing out that most organizations now

have reliable coverage in main areas, but often have dead zones in transitional spaces, like lobbies, hallways and elevators, or between buildings.

The IEEE working group in charge of developing .11ax recently voted to pass Draft 3.0, after two earlier versions failed to muster the necessary 75% approval. At its November meeting, the group plans to initiate a process called Mandatory Draft Review (MDR) -- one of the final steps before it sends the proposal to the Standards Board. According to IEEE procedural guidelines, MDR indicates a working group views a standard as "almost done" and in need of no significant changes.

A working timeline on the group's website suggests it will review the fifth and final draft of the 802.11ax standard in March 2019.

"I think we have a six-month-to-a-year window for planning, which is good, because this is such a different type of Wi-Fi," Kerravala said. "And it does have implications for the wired network, which other Wi-Fi standards didn't."

In this handbook:

The importance of staying up to date with Wi-Fi training

LEE BADMAN

Wireless networking has always required a special skill set. On one hand, it's difficult to remain current, as wireless becomes more complex. On the other, we have to keep track of the technology's development, even as the folks we work for and with are oblivious to it.

Value-added reseller installers and system designers could tell countless tales of horror based on their out-of-touch counterparts in sales, selling Wi-Fi environments that are sometimes impossible to provide as scoped. There is an absolute gap between wireless LAN (WLAN) professionals and the rest of the IT world, and filling that void is a matter of training -- and lots of it.

Even among those making a living in Wi-Fi, there are glaring differences in what we know and what we can do versus our colleagues. The Wi-Fi training each of us has had -- combined with different opportunities to amass various experiences in the field -- makes us better at some things

and weaker in others. But training is foundational to staying credible, and not staying current with wireless training risks stagnancy in a discipline that is getting more complicated, with no relief in sight.

THE ORIGIN OF WI-FI NETWORKING CONFUSION

I've been fortunate to have witnessed the evolution of wireless networking from the early days. I started my wireless career in the days when 802.11b was king. There were a lot fewer wireless client devices back then, range was generally considered more important than capacity because of the low speeds involved, and the WLAN was often an accessory to the Ethernet environment.

It's not news that Wi-Fi caught on quickly. And when 802.11a/g became the standard, those new 54 Mbps data rates really energized the growing WLAN user population. Laptops got smaller, more WLAN vendors joined the market and wireless became mainstream. Then, 802.11n blew it all wide open.

If there was any doubt Wi-Fi could serve as the primary means of network access, 802.11n put an end to that. With smartphones, tablets and high-

powered laptops flooding both business and home networks, we suddenly got really interested in capacity-driven wireless designs and a lot of other important, highly technical details that were never quite that important before.

Through all that, there were good networks designed, implemented and used by even more clients. And there were most assuredly bad networks created. I was fortunate to have managers who valued Wi-Fi training, and I was able to get a lot of it. In turn, I was able to train others in wireless design and support. I was also able to see others' struggles. I watched people and organizations absolutely agonize over some aspect of basic wireless networking, and the underlying cause was often a lack of Wi-Fi training.

That absence opened the door to a lot of miscommunication and crossed signals. Perhaps marketing didn't realize that not every part of every WLAN standard gets implemented in real life, and so they sold promised throughputs that really couldn't get implemented. Maybe the deficiency was on the part of the worker bees who never learned how .11ac differs from .11n, or maybe it was management not realizing the old .11b design doesn't work anymore -- five Wi-Fi generations later. Training looms large in any success or failure, if you zoom out far enough.

THE GROWING COMPLEXITY OF WLAN MAKES WI-FI TRAINING CRUCIAL

Wi-Fi has been getting more complicated since pretty much Day One. Although the Institute of Electrical and Electronics Engineers, the Wi-Fi Alliance, the Federal Communications Commission and vendors have each done a fair job in advancing the collective wireless cause, it hasn't been smooth going. The rough spots are where the confusion comes into play. Without a clear frame of technical reference that comes from training, you can't possibly know how to deal with today's Wi-Fi complications, such as old client drivers, devices that can't do enterprise security, OS updates that cripple some set of clients, controller or access point code bugs and many other oddball variables that are unfortunate parts of wireless life.

Looking down the road a bit, we're about to add the yet-to-be-fully realized madness of the internet of things to the mix. If you are in Wi-Fi and don't really get the true nuances associated with the 2.4 GHz and 5 GHz spectrum, you're going to be in trouble when the 900 MHz 802.11ah arrives. You also won't be able to answer your managers' questions when they ask how LTE-U might affect your WLAN environment.

In this handbook:

Then, there's 802.11ax, which is the next major WLAN standard. Loaded with new, sophisticated features, it makes 802.11.ac look simple. If you don't understand the finer points of .11ac and high-density Wi-Fi, .11ax is likely to blow your mind. All of that is even before we bring software-defined radio, fabric and orchestration to the WLAN. You can't get *there* for any of these technical paradigms without thoroughly understanding *here*. And that only comes with Wi-Fi training.

WILL TODAY'S WI-FI TRAINING OPTIONS SERVE US TOMORROW?

If you're looking for WLAN and Wi-Fi training, I'd recommend everyone in any wireless role take the Certified Wireless Specialist (CWS) course from Certified Wireless Network Professionals (CWNP). Sales, marketers, help desk staff, installers and managers who supervise wireless staff all should take the CWS to get a handle on the technical basics of WLAN. Depending on what you do in wireless, you should also consider obtaining other CWNP certifications, including Certified Wireless Network Administrator, Certified Wireless Design Professional and Certified Wireless Analysis Professional. All of these courses are vendor-agnostic

and will immerse you in the principles you need to understand the many dimensions of today's wireless world.

If your WLAN vendors offer their own specific training programs, those will also help -- although I advise staffers first take CWNP courses. For designers, support staff and anyone in the business of integrating WLAN with the rest of the enterprise, you also need a reasonably strong, fundamental Ethernet and IP background. There's just no escaping it, as Wi-Fi is just a part of the larger network ecosystem.

Where I get worried -- both for myself and for others in my field -- is in thinking about what's next.

Where I get worried -- both for myself and for others in my field -- is in thinking about what's next.

Consider this: Will CWNP or WLAN vendors evolve their Wi-Fi training materials to cover 802.11ah and .11ax in time for us to get up to speed on these? Will CompTIA expand its Mobility+ material to effectively include LTE-U? With concepts like fabric and automation starting to touch the wireless side of the enterprise, should we expect vendors to offer

training on every new major development and its implementation? Hopefully, nobody has to self-start and claw his or her way through learning what's important in the professional WLAN world.

You really can't do well in today's complicated WLAN world without decent Wi-Fi training. There are just too many variables across different environments. Even the best of today's training materials are going to have to be updated if we're to have any chance of staying on top of everything coming our way. Many of us will have to become somewhat proficient in coding, or at least able to understand when coders engage us for changes to the WLAN outside of the command line or UI. Expect to learn new concepts that aren't all just specifically wireless-related and to study more. It's a matter of changing yourself as your chosen field changes -- and as a matter of career survival.