Table Of Contents

The Technology Case For Wi-Fi 6

By Ethan Banks

Wi-Fi 6 is the latest industry standard for wireless networking. Also known as IEEE 802.11ax and “High Efficiency” wireless, this emerging standard is an opportunity for your favorite WLAN vendors to come knocking to talk about upgrades. This is a brief technical overview of Wi-Fi 6 to help get you up to speed and ask the right questions.

In next week’s issue I’ll examine the business case for Wi-Fi 6 and share opinions on whether to deploy now or hold off.

A Technical Introduction To Wi-Fi 6

Wi-Fi 6 improves throughput for wireless networks by enabling a high client density. Wi-Fi 6 efficiencies include breaking up channels into sub-channels and longer sleep intervals for low-power devices.

Wi-Fi 6 is not focused on higher maximum speeds or wider channels. Rather, Wi-Fi 6 enables multiple wireless clients to transmit data simultaneously. A stated goal of Wi-

Fi 6 is a 4x throughput improvement for clients in high-density environments.

Wi-Fi 6 access points will be backwards compatible with 802.11a/b/g/n/ac clients. However, maximum network efficiency will only be reached with Wi-Fi 6 clients.

Perhaps you just yawned. If that's what's notable about the Wi-Fi 6 specification, is it really that interesting? I believe it is.

Meet OFDMA

The cornerstone technology of Wi-Fi 6 is orthogonal frequency-division multiple access (OFDMA). OFDMA is what makes Wi-Fi 6 compelling. OFDMA subdivides a channel into Resource Units (RUs). Those RUs can be allocated to different wireless clients, giving them the ability to communicate at the same time.

OFDMA is the multi-user version of orthogonal frequency division multiplexing (OFDM), which is used in 802.11a/g/n/ac.

The OFDMA tradeoff is in performance. Wireless communications use radio waves to push data. One way

to send more data through the air is via radio channel width. The wider the channel, the more data you can send. Therefore, if a channel is subdivided, a client only get a fraction of the channel, and can only send a fraction of the data it could otherwise send if it had the whole channel to itself.

So why is OFDMA a positive feature? Because wireless clients don't always have a lot to say. We networkers tend to think in terms of maximum throughput, but most of the time, network clients don't need big bandwidth.

Activities like browsing a web site, using social media, or sending a text message need relatively small chunks of data. Just like most wired desktops could get away with 100Mbps or less most of the time, most wireless clients don't need entire channels most of the time.

OFDMA means multiple clients can transmit simultaneously, rather than waiting for the air to clear before they get a turn. OFDMA will reduce collisions in dense environments and should go a long way toward the 4x throughput improvement goal.

Wi-Fi 6 Means Faster Speeds, Right?

While I was sitting on a Wi-Fi 6 industry panel at Cisco headquarters, one of the other panelists said Wi-Fi 6 means faster speeds, just like all previous iterations of the Wi-Fi spec.

That's sort of true. One key issue is quadrature amplitude modulation (QAM). QAM increases throughput in Wi-Fi networks by encoding more bits in a transmission by changing the angle of a wave and the amplitude of a wave relative to a center point. Unique angles and amplitudes are spread over a quadrant grid, creating a constellation. Wireless QAM schemes include 4-, 16-, 64-, and 256-QAM.

The challenge with high-density QAM constellations is that the air must be clear and the signal strength strong between client and AP to experience the throughput benefit. Poor signal quality means that the tiny distinctions between the various angle and amplitude combinations can't be communicated clearly.

Wi-Fi 6 introduces 1024-QAM, which should result in a higher theoretical maximum throughput, but only under ideal conditions. Ideal, as in, there's no one else on the air,

the spectrum is pristine, and the client and AP are within a few feet of each other.

This is why I contend that faster speeds in Wi-Fi 6 are only sort of true. The spec is there to facilitate faster speeds, but in real-world conditions, faster speed in Wi-Fi 6 is closer to fake news.

Target Wait Time Reduces Battery Consumption

An understated feature of Wi-Fi 6 is Target Wait Time (TWT). TWT is a power saving mechanism that schedules a wake time for clients that are sleep capable. The goal of TWT is to optimize how often the client needs to wake up to determine if it has network communication to attend to.

The big idea is to keep clients asleep as long as possible to reduce battery use. Scheduling a specific wake time means the client doesn't have to cycle the radio up as often.

BSS Coloring Puts Others On Ignore

Basic service set (BSS) coloring is a Wi-Fi 6 feature that should improve throughput. The idea is to color your wireless world with a number--a digit for identification. The

client will look to determine if it's a part of the BSS indicated in the frame. If the client is not a part of the BSS indicated by the "color," the client knows it's okay to send.

In theory, BSS coloring will increase throughput. The wireless speaker won't be waiting as long for the air to clear before sending in a busy wireless environment with a large number of BSS's. I found this counterintuitive, because two wireless transmissions happening at the same time can clobber each other, forcing a retransmission--the opposite of increased throughput.

A wireless friend explained to me that there's an assumption built into BSS coloring. The assumption is that the different wireless systems will be physically far enough apart that one system will be much quieter than the other. In that scenario, it's safe to have simultaneous transmissions, because the local, shouty transmission will drown out the whispering transmission from far away. Therefore, if you hear a different BSS color in the air, it's safe to be inconsiderate and shout away.

In that assumption, there is a catch. BSS coloring won't help in scenarios where different wireless systems are right on top of each other. Apartment complexes and multi-

floor, multi-tenant business parks could have systems just as loud as one another and potentially disrupt each other's transmissions. BSS coloring won't replace careful channel planning.

For More Technical Information On Wi-Fi 6

I recommend Clear-To-Send's 802.11ax podcast series very highly. I listened to Rowell Dionicio talk through the Wi-Fi 6 overview episode in detail, taking lots of notes to get up to speed on this topic. The series is a fantastic resource, and I hope I got most of my information right.

I also found this article from Aerohive to be a cut above most of the flotsam turned up by Internet search. The piece is in a Q&A format and is grounded in technology as opposed to marketing puffery.

And I'd be remiss not to mention the Packet Pushers' own episode, Inside The Pros And Cons Of 802.11ax, with guests Devin Akin and David Coleman.

Tech Blogs: How To

MPLS Fun in the Lab: Building a MPLS L3VPN Unicast and Multicast Cloud (6 Part Blog Series) - Networking With Fish

https://www.networkingwithfish.com/fun-in-the-lab-...

Denise Fishburne has written a new multi-part series on building "a full MPLS cloud with L3VPN unicast and multicast" that she was putting together for a customer proof of concept. Being the community maven she is, Denise decided to bring us all along for the ride. That's cool. All six parts are already written, so you may want to bookmark this page as you work through them. In addition to the blogs, she's also included "zip files of the varying configs as we build them," and "sniffer traces for you to download and refer to." Dig in.

And if you want to learn more about Denise as a person, including how she got started in tech, and what it was like to be openly gay in corporate environments in the '80s and 90s, check out Ethan Banks' interview with her in our new Network Neighborhood series. - Drew

Learning how to Incorporate Open Source Tools into a Modern NOS - Network Tech Study

https://networktechstudy.com/Home/learning-how-to-open-tools-nos/

If Linux is the new foundation of network operating systems, then it's time to get familiar with open source tools that help us make the most of the experience. Billy Downing shares an overview of DellEMC's OS10 Enterprise, Cumulus Linux, OpenSwitch OPX, Prometheus, and Grafana. He walks through plumbing them all together in GNS3 and then building simple graphs. - Ethan

Automating Cisco ACI Environment with Python and Ansible - ipSpace.net

http://blog.ipspace.net/2019/03/automating-cisco-aci-environment-with.html

Not a step-by-step guide, but you do get a great high level summary in this guest post by Dave Crown hosted on Ivan Pepelnjak's blog. "Over the course of the last year or so,

I've been working on building a solution to deploy and manage Cisco's ACI using Ansible and Git, with Python to spackle in cracks. The goal I started with was to take the plain-text description of our network from a Git server, pull in any requirements, and use the solution to configure the fabric, and lastly, update our IPAM, Netbox." - Ethan

Prevent route leaks by explicitly defining policy - APNIC Blog

https://blog.apnic.net/2019/03/19/prevent-route-leaks-by-explicitly-defining-policy/

Prefixes announced by an AS that doesn't own the prefix continues to plague Internet routing. This post surveys the available techniques for containing these leaks, with a special focus on RFC 8212. RFC 8212 requires that no routes be exchanged with an eBGP neighbor unless both import and export policies have been assigned to that peering relationship. The assumption is that the policies would prevent inappropriate announcements (leaked routes) from propagating their way across the Internet and making us all sad. - Ethan

Tech Blogs: Opinion

Grey Failure Lessons Learned - Rule 11 Reader

https://rule11.tech/grey-failure-lessons-learne/

Russ White presents his summary with takeaways of a USENIX presentation on the most common IT failure there is--the partial, or “grey” failure. “For instance, a single link that drops 5% of the traffic will impact different applications at different times, depending on variations in flow startup and ECMP hashing.” Been there. Russ also shares his own perspectives, including, “What is not mentioned in the document is that many of these failures are a result of increasing system complexity...Reduce, reuse, and consider complexity in system design.” - Ethan

Scaling Up Smart: 4 key tips on successfully using cloud-native technology to scale your infrastructure - Streamroot Tech Blog

https://medium.com/streamroot-developers-blog/scaling-up-smart-4-key-tips-on-successfully-using-cloud-native-technology-to-scale-your-e4b521003f94

“Cloud native technology is still young, and there are various new components springing up in a different field every month: storage, security, service discovery, package management, etc. Our advice: use these new components with caution, and keep it simple (, stupid). These technologies are new, sometimes still rough around the edges, and are evolving at an incredible pace.” That and several other lessons borne of experience with the bleeding edge make this worth reading and sharing with your management, especially if they like to chase shiny objects. - Ethan

Cloud Field Day – NGINX - Ned In The Cloud

https://nedinthecloud.com/2019/03/21/cloud-field-day-nginx/

Ned Bellavance will be attending Cloud Field Day 5. One of the presenters is NGINX, and Ned’s got questions. What about you, especially considering that F5 just bought

NGINX? Let Ned know via @ned1313 or comment on his post. BTW, Ned is the host of Day Two Cloud (latest episode) on the Packet Pushers network, currently incubating in our Community channel. - Ethan

The Cloud Is (Not) Magic - NetCraftsmen

https://www.netcraftsmen.com/the-cloud-is-not-magic/

Pete Welcher points out what some of the clouderati have a hard time grasping. Latency matters. You can't expect users in APAC to have a great experience using your intense UI app housed in Virginia. Of course, when you try to overcome latency with geo-sharding (a term Pete made up that I love), you introduce additional complexity...which introduces fragility. Nothing is free. The cloud's not magic. Find the tradeoffs. - Ethan

Common misconceptions about IPv6 security - APNIC Blog

https://blog.apnic.net/2019/03/18/common-misconceptions-about-ipv6-security/

David Holder talks through wrong ideas folks (maybe you!) have about IPv6, including addressing, IPSEC, subnet scanning, and NAT. Short, to the point, no words minced. - Ethan

Apple's Services Event - Stratechery

https://stratechery.com/2019/apples-services-event...

Apple recently announced new services including AppleTV+. Ben Thompson argues that Apple is deviating from its core (and very successful) business model as iPhone sales flatten and the company looks for new revenue sources to maintain growth. His overall point is that Apple would've been better off just buying Netflix outright instead of trying to compete with it. - Drew

New Packet Pushers Podcasts

We recently launched two new podcast series at PacketPushers.net. If you haven't listened yet, here's a

nudge to check them out.

IPv6 Buzz

IPv6 is here, it's real, and if you haven't started grappling with the inevitable transition to v6, this podcast might help get you in gear. Hosted by Ed Horley, Tom Coffeen, and Scott Hogg, IPv6 Buzz dives into issues including address planning, IPv6 security, troubleshooting, and other practical topics.

Day Two Cloud

If you believe the hype, public cloud services are all unicorns, rainbows, and free cotton candy. Host Ned Bellavance digs deeper to reveal the messes that unicorns eating cotton candy can make. Like any other technology, cloud has advantages and drawbacks, so you need to know what you're getting into. Currently featured in our Community channel, Day Two Cloud will graduate to its own channel in April.

The Lulz

IT News

Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers - Motherboard

https://motherboard.vice.com/en_us/article/pan9wn/...

Motherboard reports on research from Kaspersky Labs that claims attackers compromised Asus servers that push software updates to customers. According to Kaspersky, the attackers were able to push malicious software disguised as an update, and digitally signed the malware using legitimate Asus certificates. Kaspersky estimates that 500,000 machines were compromised, but also speculates that the attack was targeted at specific MAC addresses. - Drew

Huawei bungled router security, leaving kit open to botnets, despite alert from ISP years prior - The Register

But wait, there's more! The Register reports on security vulnerabilities in Huawei home routers left unpatched for years, despite warnings from an unnamed ISP and other security researchers. It appears that Huawei took a

piecemeal approach to addressing the vulnerability by patching some models, but leaving other models unfixed even though they shared the same code flaw. - Drew

U.S. Must Put a Ban on Google Helping China Develop a Global Digital Dictatorship - The Daily Beast

https://www.thedailybeast.com/google-snubbed-the-pentagonbut-not-the-chinese-military

This story illustrates the deepening intersection of technology and global politics. What duty do US tech companies have when it comes to cooperating with foreign governments on building technologies that could be used for surveillance, local repression, or to advance that government's global interests over the tech company's home country? What responsibility, or legal power, does the United States government have over how and where US tech companies sell their products or share intellectual property? This is going to be messy. - Drew

New Products & Industry Takes

Kubernetes 1.14: Production-level support for Windows Nodes, Kubectl Updates, Persistent Local Volumes GA - Kubernetes Blog

https://kubernetes.io/blog/2019/03/25/kubernetes-1-14-release-announcement/

“Kubernetes 1.14 consists of 31 enhancements: 10 moving to stable, 12 in beta, and 7 net new. The main themes of this release are extensibility and supporting more workloads on Kubernetes with three major features moving to general availability, and an important security feature moving to beta.” Read all about it and decide if it’s solving problems you’ve got. If not, be frightened that of the 31 enhancements, 12 are BETA and 7 are NEW. This is not a maintenance release--that’s not how cloud native works yet. Deploy to production with extreme caution. - Ethan

Untangle Introduces Network Security Framework - Untangle

https://www.untangle.com/press-releases/untangle-introduces-network-security-framework/

Untangle has released a new software-based SD-WAN router that also includes an L3 firewall. Untangle targets SMBs and larger organizations with distributed offices or retail sites. As you'd expect with an SD-WAN product, Untangle lets administrators send traffic across multiple links (broadband, MPLS, LTE) based on policy, application type, or link performance. Traffic can switch between links on a per-session basis if the primary connection falls below administrator-defined performance levels. - Drew

OpenDaylight, Most Pervasive Open Source SDN Controller, Celebrates Sixth Anniversary with Neon Release - The Linux Foundation

https://www.linuxfoundation.org/press-release/2019...

OpenDaylight (ODL) has reached Neon, ODL's tenth release. Features will be of primary interest to service providers, the folks that have been most eagerly consuming ODL since its inception in 2013. "Neon includes updated features important to networking use cases, such as optical transport networking, WAN connectivity and routing, as well as virtual networking in cloud and edge environments. Neon also features new stability and scalability enhancements." ODL's an established fixture in the telco space these days, with an estimated impact to over a billion network users. - Ethan

The End Bit

Human Infrastructure is bi-weekly newsletter with view, perspectives, and opinions. It is edited and published by Greg Ferro and Drew Conry-Murray from PacketPushers.net. If you'd like to contribute, email Drew at drew.conrymurray@packetpushers.net.