ASPIRE
Powering Business Transformatio

Enterprise Wireless: Wi-Fi 5 & 6 Selection and Implementation

Problem Statement

Wireless technology is rapidly evolving, along with the requirements for enterprises that require upgrades to either an existing or a new architecture. The challenge for any upgrade to your wireless environment is determining your organization's needs and desires, including legacy hardware and software requirements which may have caveats of their own.

Background

In a world where wireless technology has become a driving force of enterprise business requirements, so too has the technology evolved from legacy hardware options and wireless technology, holistically, into new and exciting options on both the physical hardware and wireless standards front. It seems relatively intuitive to invest in either a predictive, active, or passive survey, but once you have a solution that fits the needs of your enterprise, what next?

Looking beyond the technology and understanding the logistics of how next generation wireless platforms have evolved from a hardware and implementation perspective to newer platforms with much more built-in robust technology will help you make an informed decision as to what works best for you as an engineer architecting the solution for your enterprise.

Wireless has evolved sharply since the days of legacy technologies utilizing 802.11b, a, g, and n standards – and even today with the advent of 802.11ax and Wi-Fi-6. Chipsets have become stronger and more robust. True mobility functionality determines how the enterprise networking environment will be developed and deployed. Guest access and expandability have also become deciding factors for your enterprise solution, as has the decision between on-premises versus cloud-based solutions.

Other considerations include the number of clients that need to be supported in each wireless location, what services they can access, and whether specific access points require external antenna capability or outdoor placement in potentially inclement weather situations.

No matter what choice you make for your enterprise, understanding the key components of each model, the limitations, the enhancements, and other requirements, is part of the overall process in the evolution of the wireless enterprise environment and decision-making process.

Dipping in and deciding what access point works best for the needs of the enterprise can be challenging, at best. Often, a researching engineer will not only reference Cisco documentation, but invest time looking into solutions and testimonies that have worked for other customers and engineers that have faced similar situations.

Solution

The solution involves educating yourself, obtaining the opinion and assistance of a certified enterprise networking professional organization, and referencing Cisco documentation for best practices when it comes to upgrading an environment with legacy hardware or software. This is important as issues arising from some situations, such as upgrading Wireless LAN Controllers, have the potential to cause major network outages based on feature parity and lack of support for newer versions of software for legacy access points.

It is imperative when investing in your wireless enterprise, whether to upgrade or implement new hardware or software, to reach out to a certified enterprise networking professional organization to ensure the success and stability of your overall enterprise networking and wireless environment.

As of today, Cisco recommends several options for access points geared specifically to the needs of developing a new wireless network or enhancing an existing enterprise with newer, more powerful technology. The Cisco Aironet 1800, 2800, and 3800-series access points utilize 802.11ac Wave 2 standard, while the newer Catalyst 9100-series access points leverage next generation Wi-Fi 6 (802.11ax) technology.

What does all this mean?

In 2018, the Wi-Fi Alliance began leveraging a numbering scheme for the 802.11 protocols that we have all come to know. Chronologically speaking, Wi-Fi generations 1–6 refer to the 802.11b, 802.11a, 802.11g, 802.11n, 802.11ac, and 802.11ax protocols, respectively. It is important to note that newer technologies, such as Wi-Fi 5 and 6, are backward compatible with older IEEE protocols – which is important for legacy technology that requires coverage on, for example, the 2.4 GHz band.

Wi-Fi 6 (802.11ax) Next Generation Wireless Standard (Chart A)

PHY	Bandwidth (as number of data subcarriers)		Data bits per subcarrier		Time per OFDM symbol (800ns GI)		1 SS	3 SS	4 SS	8 SS
802.11ac	234 (80 MHz) 2 x 234 (160 Mhz)	x	5/6 x log2(256) = 6.67	/	4 µs	=	390 Mbps 780 Mbps	1.17 Gbps -	1.56 Gbps 3.12 Gbps	- -
802.11ax	980 (80 MHz) 2 x 980 (160 Mhz)	x	5/6 x log2(1024) = 8.33	/	13.6 µs	=	600 Mbps 1.2 Gbps	1.8 Gbps 3.6 Gbps	1.56 Gbps 4.8 Gbps	4.8 Gbps -

The challenge we face here is determining which of the newer technologies to implement: Wi-Fi 5 (“ac”) or 6 (“ax”)? What are the advantages of one or the other? To answer this question, we need to understand the capabilities of each technology. Chart A (above) explains some of the key differences with both technologies.

As the chart above shows, Wi-Fi 6 effectively allows more bits to be sent with each transmission for bolstered speed. In environments where crowding is an issue, you can count on Wi-Fi 6 to better utilize the wireless spectrum for overall performance. It builds on Wi-Fi 5 – which is already more than suitable for most environments – by accounting essentially for more congested environments and bolstering performance better than its predecessor.

This is imperative when you consider that the “smart home” or “smart enterprise” grows smarter. Assume for a minute that you do decide to invest into Wi-Fi 6 access points, such as the Cisco Catalyst 9100-series APs.

There are always certain software limitations based on the model of access point you are selecting or already have deployed. The best place to refer to in these circumstances is the **Compatibility Matrix**, which outlines distinctly what minimal levels of software are required for certain access points to function properly and associate with your controller(s).

Cisco WLC Software Releases, AP IOS Releases, and Supported Access Points (Chart B)

Cisco WLC Release	Access Point IOS Release	Supported Access Points
8.3.150.0	15.3(3)JD17 15.3(3)JDA17	Lightweight APs: 1040, 1140, 1260, 1600, 1700, 1810 OEAP, 1810W, 1815i, 1830, 1850, 2600, 2700, 2800, 3500e, 3500i, 3500p, 3600e, 3600i, 3600p, 3702e, 3702i, 3702p, 3800, 600 OEAP, 700, 700W, AP802, AP803, ASA5506W-AP702 Outdoor and Industrial APs: 1532E, 1532I, 1552E, 1552H, 1552I, 1552C, 1552EU, 1552CU, 1552S, 1560, 1570, and IW3700 Modules: AIR-RM3010L-x-K9 and AIR-RM3000M The Cisco 1040 Series, 1140 Series, and 1260 Series access points have feature parity with Cisco Wireless Release 8.0. Features introduced in Cisco Wireless Release 8.1 or later are not supported on these access points.
8.3.143.0	15.3(3)JD16 15.3(3)JDA16	
8.3.141.0	15.3(3)JD14 15.3(3)JDA14	
8.3.140.0	15.3(3)JD13 15.3(3)JDA13	

The Compatibility Matrix is critical. Aspire has addressed forced upgrade halts on existing Wireless LAN Controllers (WLCs) to prevent incongruencies and feature parity for legacy access points when moving to a new platform piece by piece as per customer request. When opting to move in the direction of newer access points, it is always best to reference the Compatibility Matrix first to ensure your existing deployment – if present – is compatible with any upgrades to your controller while simultaneously considering adding new access points into the environment.

Assume you decide to deploy Cisco 9100-series Catalyst access points (utilizing Wi-Fi 6 technology) into an

architecture comprised of legacy Aironet 1142N access points, for example. This represents a major change because, per the matrix, the last supported wireless release was the 8.3.150 version of software (see chart) –prohibiting you from upgrading your controllers to support newer access points. Assume also that your WLCs are in a high availability (HA) pair of 5520-series controllers on the earlier version of software. In the event of a partial 9100-series AP implementation, first carefully consider the ramifications of an enterprise-wide loss of wireless coverage.

Cisco WLC Software Releases, AP IOS Releases, and Supported Access Points (Chart C)

Cisco WLC Release	Access Point IOS Release	Supported Access Points
8.9.100.0	15.3(3)JJ	Lightweight APs: 9115, 9117, 1700, 1800i, 1810 OEAP, 1810W, 1815i, 1815m, 1815t, 1815w, 1830, 1850, 2700, 2800, 3702e, 3702i, 3702p, 3800, 4800, 700, 700W, AP803, Integrated Access Point on Cisco 1100 ISR, Cisco 1101 ISR, ASA5506W-AP702 Outdoor and Industrial APs: 1532E, 1532I, 1540, 1560, 1570, and IW3700 Modules: AIR-RM3010L-x-K9 and AIR-RM3000M

After review, 8.9.100 is the first train of software that allows for compatibility with Catalyst 9100-series access points (see above). So, in this situation, you would not (and should not) upgrade your controllers without losing your entire wireless enterprise in the process (!)– assuming your controllers sit on the earlier variation of code supported for 1140-series APs. This is where the problem arises when integrating newer access points into an environment comprised predominantly of legacy access points. You would avoid under these circumstances upgrades of any kind until a proper plan was developed and planned maintenance windows have been put into place to support the upgrade of the newer Catalyst 9100-series access points in conjunction with a proper software upgrade path based on the procedurals laid out by Cisco for your WLCs.

Conclusion

It is often best to take the time to understand your organization's wireless needs and requirements to satisfy the ultimate goal of conducting an upgrade with minimal disruption. When faced with situations where you may have independently upgraded your WLCs and lost connection to your legacy access points, referring to the matrix helps tremendously in pinpointing the problem to identify the existing inventory of your current wireless environment and code limitations back to the controllers.

This is the logistics part of pre-deployment and deployment. To mitigate these issues, you must consider whether you want to invest in newer technology implementation as a whole and decide whether to keep legacy access

points in place and pepper the enterprise with newer APs because of budgetary concerns – which is very challenging. It is always best to refer to Cisco documentation and have your wireless network needs and setup reviewed prior to any major architectural changes objectively – especially ones that involve holistic or even partial changes.

In the end, remaining patient is the best option whenever possible for implementing a new wireless solution, whether it is Wi-Fi 5 or 6 technology. The crossover between legacy and newer technologies is a daunting task – arguably more so than determining which technology suits the enterprise best. It can seem like buying a new car: sometimes the newest and best-looking is not what is in your budget or suits your needs as a consumer.

Consider instead what will work best for your enterprise, and what you need to do to make that transition. Those are two considerations that merit much thought and research, no matter how large or small your wireless deployment.

References

https://www.cisco.com/c/en/us/products/wireless/access-points/index.html#~products

https://en.wikipedia.org/wiki/IEEE_802.11#Generations

https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/why-go-wireless.html#~overview

https://en.wikipedia.org/wiki/Wi-Fi_Alliance#

http://ciscorouterswitch.over-blog.com/2019/03/more-reliable-wi-fi-802.11ax.html

https://www.router-switch.com/media/upload/product-pdf/cisco-indoor-access-points-comparison-chart.pdf

Michael Keller

Senior Consulting Engineer

Aspire Technology Partners

Michael Keller is a solutions-driven network architect, engineering professional and consultation expert. For more than two decades, he has supported a wide array of enterprise clients that have expressed the need to upgrade their existing wireless architecture from both a hardware and software perspective. He has validated and overseen countless architectural optimization efforts through surveys, calibrations, configuration, and installations. His experience includes developing, monitoring, and managing enterprise networking equipment for commercial companies and the United States Military.

ASPIRE TECHNOLOGY PARTNERS

25 James Way, Eatontown, New Jersey 07724

www.AspireTransforms.com

(732) 847-9600

Gold Certified

Master Specialized in Security

Master Specialized in Networking