How Wi-Fi 6, WWAN and 5G Make All-Wireless Offices Possible

In this handbook:

Learn about the advantages and possibilities of an all-wireless office

How Wi-Fi 6, WWAN and 5G Make All-Wireless Offices Possible

JOHN BURKE, CTO AND PRINCIPAL RESEARCH ANALYST

Even though some old-school IT folks don't fully accept it yet, it's a fact: All-wireless connectivity for office staff is possible and practical for most offices and use cases. Especially with the availability of Wi-Fi 6 or private 5G, performance, security and reliability are all sufficient for nearly all modern office work. Most organizations can adopt a wireless-by-default standard with wired connectivity on an as-needed basis.

WHY GO ALL WIRELESS? DEMAND AND SAVINGS

Staff expect and increasingly demand a ubiquitous and high-performing wireless LAN (WLAN). New work patterns -- conceived around dynamic, spontaneous collaboration and a work-where-you-are philosophy -- require a reliable wireless network.

With the assumption of an ongoing buildout of ubiquitous, up-to-date Wi-Fi in most organizations, IT can flip its perspective: Wi-Fi as main connectivity mode, wired as secondary and provided only as required. This leads logically to the savings question, "If the wired network exists mainly to power the WLAN, how much less can IT spend on it?" The answer is *a lot*.

Most switch ports connect to user endpoints. In a wireless world, most of those switch ports would vanish. In this case, fewer switch ports means fewer switches to buy, power up, cool down, maintain, manage and secure. Additionally, organizations can reap substantial per-drop savings on cabling and re-cabling endpoint connections in greenfield office buildouts as well as remodels and reconfigurations.

HOW TO GO ALL WIRELESS

With current WLAN technology and devices -- and the advent of Wi-Fi 6 -- Wi-Fi capabilities have surpassed the baseline needs of most knowledge workers and shared office equipment, such as multifunction devices, smartboards and conferencing gear.

Wi-Fi 6 aims to address certain office challenges and demands, including wider reach, higher device density, more simultaneous uses and broad ranges of demand patterns. For example, some of the key Wi-Fi 6 features include the following:

- Multi-user multiple input, multiple output (MU-MIMO) enables an access point (AP) to serve multiple devices simultaneously by sending physically separated, or *beamformed*, signals at them.
- Multi-user orthogonal frequency division multiple access (MU-OFDMA) enables an AP to carve each primary frequency channel into 256 subcarriers and bundle them into different-sized resource units based on each client's needs.

- Renewed incorporation of the 2.4 GHz channels, which the previous standard -- 802.11ac -- did not use, serves the needs of lower-power, long-distance or interference use cases that are common in IoT systems.
- Compared to earlier standards, Wi-Fi 6 employs a different method to identify potential collisions on a data channel. This should improve overall efficiency from 70% of theoretical maximum capacity at best to 90% or more.

Despite these promising features, the big catch is organizations need both clients and infrastructure to support Wi-Fi 6.

For previous Wi-Fi generations, the general design guideline was about 30 clients per AP -- roughly one AP per 800 to 1,600 square feet. Wi-Fi 6 networks are designed for 50 or 60 laptop/mobile clients per AP, plus a larger number of low-load IoT devices, and one AP per 2,000 to 3,000 square feet.

Of course, these are rough guidelines. Much of this varies by product. And, in the end, the physics of the space drive every Wi-Fi design problem. Wi-Fi engineers need to consider the office size, shape, construction materials used, furnishings and surroundings -- as well as the needs and usage patterns of the population served.

IMPROVED WLAN SECURITY

Wi-Fi 6 drives some significant security enhancements in the WLAN by requiring Wi-Fi Protected Access 3 instead of WPA2 or older. WPA3 has higher encryption levels, beefed-up client authentication and resistance to brute-force attacks.

In the long term, the key is to make the WLAN part of a comprehensive zero-trust architecture. WLAN use should just be another aspect of zero-trust network access and ideally supported by the same platform as wired systems and users off premises -- for example, those using a software-defined perimeter (SDP) system. SDP services provide session-level encryption of data independent of network medium and location, supplementing the improved encryption protections in Wi-Fi 6.

THE RISE OF WWAN AND FALL OF WLAN

In recent years, several factors have converged to increase the use of wireless WAN (WWAN) connectivity, including the following trends:

- Software-defined WAN (SD-WAN) emerged to help manage the integration of multiple connection media at single-location organizations and provide policy-based control.
- 4G became ubiquitous and 5G is spreading rapidly.
- Many organizations shifted to cloud applications.
- More people work from home, and many organizations have replaced larger, centralized offices with smaller, more dispersed offices.
- Wireless pricing plans have become like wired pricing plans, with fixed rates for a given capacity and no rate-capping or overage costs based on the volume of data transferred.

In this handbook:

Learn about the advantages and possibilities of an all-wireless office

With or without SD-WAN, organizations of all sizes are increasingly folding WWAN into their branch connectivity strategies, whether as backup, overflow or primary connectivity.

The next logical step is to explore a no-WLAN environment in which end-user devices are connected with 4G or 5G in either a private or public carrier service.

Keep in mind, 5G offers some distinct advantages over 4G, in much the same way Wi-Fi 6 offers advantages over older Wi-Fi standards. 5G offers higher speeds, better security, better performance management and the ability to support higher densities of devices. In fact, 5G and Wi-Fi 6 use many of the same technologies and strategies.

Private 5G, thanks to the added control an organization would have over the infrastructure, could provide better security than public carrier services, whether an organization manages it or contracts for it as a service.

THE CHALLENGES OF GOING ALL WIRELESS

Wi-Fi 6 APs require more power than previous generations of APs because of increased numbers of radios and processing power, despite power-conserving technologies that optimize radio use. Older 802.3af standard Power over Ethernet needs to be bumped up to 802.3at, which can be costly if it means replacing PoE switches or their power feeds.

With the increasing density of service via each AP, uplinks to campus aggregation or backbone switches need to bear higher loads. Organizations may find a single Gigabit Ethernet link may not suffice and may need to plan for higher capacity links or -- if the APs enable it -- bonded sets of GbE connections.

Additionally, specific locations will continue to have issues, such as poor reception in some areas due to space geometries or construction materials. Remediations, such as deploying extra APs or different kinds of antennas, are well understood.

Interference from a variety of devices, ranging from wireless subwoofers to microwave ovens, can still be an issue as well. And, even with Wi-Fi 6, wireless networks can be swamped more easily than wired ones -- for example, by a broad simultaneous software download, like a Patch Tuesday.

To minimize such issues, a proper WLAN design requires site mapping with the right tools to test radio reception and then mapping APs to cover the space, users and device populations properly. Likewise, troubleshooting requires Wi-Fi-specific equipment and software.

In this handbook:

Learn about the advantages and possibilities of an all-wireless office

WIRELESS FIRST, WIRED ONLY AS NEEDED

In just a few situations, wireless cannot yet cover all enterprise office needs. Some problematic scenarios might include business operations that generate huge amounts of radio frequency interference or building construction that's unkind to Wi-Fi, such as walls packed with pipes or plastered walls over chicken wire.

In reality, most organizations only have to worry about use cases that require high-speed transfers of large volumes of data; one example of this is if sustained transfer speeds exceed 1 Gbps. This might involve moving high-resolution imaging data from an MRI machine to a workstation for analysis, or transferring large video files around special effects labs.

However, such situations tend to be edge cases, even for media-intense companies. These are the exceptions, not the rule. In these edge cases, any branch office strategy that's primarily focused on wireless should dictate that the branch has one or more wired workstations to support the required work.

Alternatively, the branch could have places where a normally wireless workstation can connect to a network cable for as long as needed -- basically, connectivity-dictated hoteling. The wired infrastructure supporting the APs can probably accommodate these edge cases, often without added cost given their paucity.

Going forward, given the capabilities of Wi-Fi 6 and 5G, most organizations can -- and should -- adopt a wireless-by-default standard with wired connectivity pulled only when needed.