WHITE PAPER

A division of Chatsworth Products

Optimizing Next-Generation Wireless Deployments for the Digital World

By Scott Thompson
President, Oberon, a Division of Chatsworth Products (CPI)

Published: May 2022

oberonwireless.com

Over the past two decades, wireless technology has evolved as an essential means to provide internet connectivity and transmit voice, data, and video to and from people and devices. According to Statista, the number of wireless local area network (WLAN)-connected devices is estimated at more than 22 billion globally[1], with smartphone users alone surpassing 6 billion in 2022[2], equating to more than 83% of the world's population[3]. Now with trends like remote and hybrid working fueled by the pandemic, global e-commerce, and emerging Internet of Things/ Industrial Internet of Things (IoT/IIoT) applications that are increasing demand for more wireless connectivity, it's no wonder that a recent report by Markets and Markets estimates the wireless market to grow from $69 billion in 2020 to $141 billion by 2025[4].

While the proliferation of smartphones and other wireless devices continues to increase the need for more wireless connectivity, there is also a growing demand for greater bandwidth and high-speed internet access to support a broader range of applications— from video conferencing and streaming to online learning, virtual/augmented reality, and gaming. At the same time, demand for low- and medium-speed wireless connectivity is also on the rise for emerging IoT/IIoT wireless sensor networks used to support a variety of monitoring, metering, and tracking applications across a wide range of environments and industries. In response, high-throughput Wi-Fi, cellular, and low-speed short- and long-range wireless technologies have advanced to support a broader range of devices and applications than ever before.

Today's enterprise businesses are adopting next-generation wireless connectivity throughout their facilities and campuses to support more users, devices, and use cases. In doing so, they need to ensure that the wireless access points (APs) and underlying infrastructure that support current and emerging wireless applications are deployed in a manner that optimizes their investment and meets requirements for coverage, security, accessibility, code compliance, and aesthetics across a variety of environments.

Next-Generation Wi-Fi

Wi-Fi is by far the most ubiquitous in-building and near-building means of wireless connectivity found across every commercial enterprise facility and campus. This includes corporate offices, hospitals and healthcare facilities, educational institutions, industrial/manufacturing sites, and hospitality, entertainment, and retail venues like convention centers, hotels, malls, and restaurants. It's also the primary wireless connectivity deployed in homes and across a range of public spaces—from municipal downtowns and parks to transportation modes and hubs (e.g., airports, planes, trains, and buses).

Wi-Fi is a LAN-based wireless application that offers high throughput capability and operates within an unlicensed frequency spectrum, with no limit on data usage or required data plans associated with mobile service provider licensed cellular communications. Wi-Fi is therefore the most cost-effective and preferred method for connecting laptops, tablets, smartphones, gaming/virtual reality consoles, and other data-intensive devices. Wi-Fi technology has advanced over the past two decades from both a generational and industry standards perspective. The consumer-friendly designations for Wi-Fi that make it easy to identify the Wi-Fi generation supported by a given device and facilitate network deployments comes from the Wi-Fi Alliance®. This worldwide network of Wi-Fi equipment and device vendors collaborate to improve and drive global adoption of Wi-Fi through spectrum advocacy with government entities such as the Federal Communications Commission (FCC) and through the development of specifications that ensure standards-based interoperability, security, and reliability.

As shown in Figure 1, the naming system for Wi-Fi generations uses a numerical sequence that corresponds to major advancements based on the IEEE 802.11 set of wireless application standards that specify communication protocols, speeds, transmission ranges, and operating frequency. It should be noted that there are some key differences in the specific operating frequency band spectrum (i.e., 2.4 or 5 GHz) used for each generation of Wi-Fi. Since path loss is lower at lower frequencies, 2.4 GHz offers more than two times the range and better propagation (i.e., penetration through building materials) compared to 5 GHz. However, the 2.4 GHz spectrum offers very few non-overlapping channels and is congested with more devices compared to the 5 GHz spectrum. Consequently, 2.4 GHz is more susceptible to interference and reduced transmission rates.

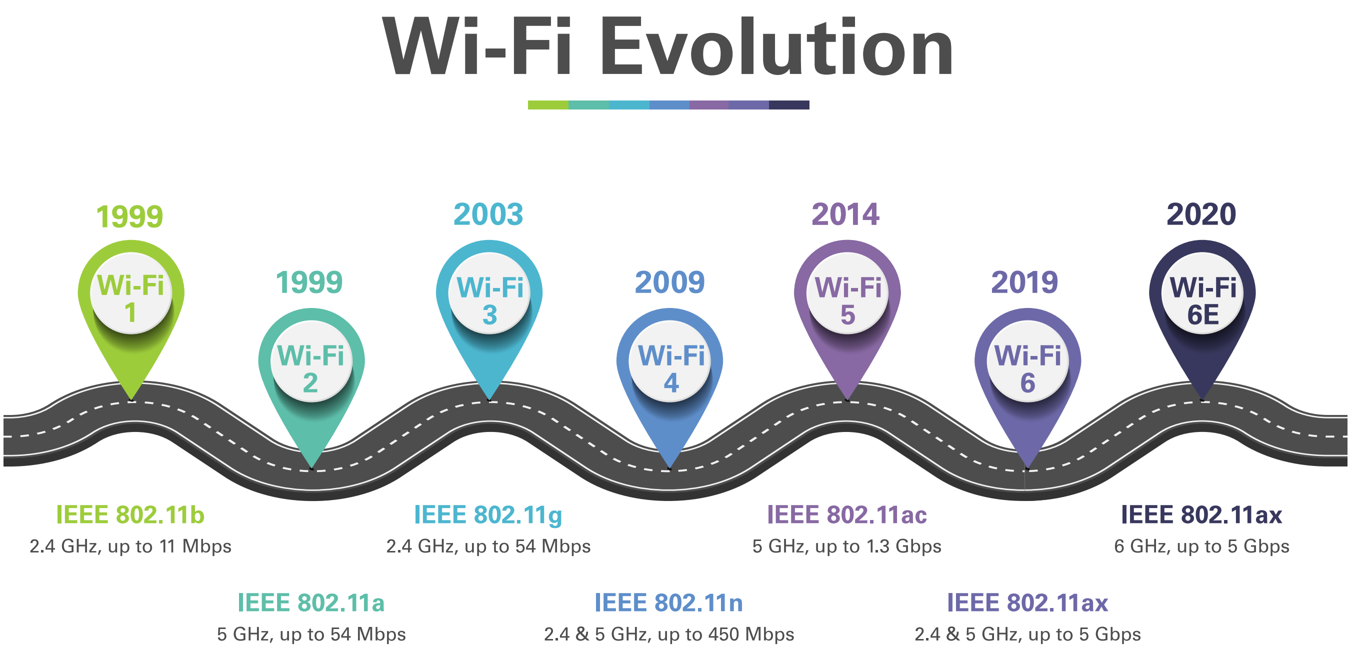


Figure 1: The Evolution of Wi-Fi Generations and IEEE 802.11 Standards

Wi-Fi 6 Improvements

Wi-Fi 6 is the latest approved generation supporting the IEEE 802.11ax standard. The main goal of the Wi-Fi 6 amendment is to improve overall throughput in a given area, and satisfy the connectivity needs of mobile devices, particularly in congested areas. Several enabling technologies (see below) provide the following improvements for Wi-Fi 6 compared to Wi-Fi 5:

- **Higher throughput**
  Wi-Fi 6 offers higher data rates per spatial stream for as much as four times (4X) the data rate compared to Wi-Fi 5.
- **Greater capacity**
  Wi-Fi 6 can support four times (4X) the number of simultaneously connected client devices compared to Wi-Fi 5.
- **Improved performance in dense environments**
  Wi-Fi 6 devices engage advanced coding methods to perform better in congested venues.
- **Better battery life and power efficiency**
  Wi-Fi 6 offers an improvement in device battery life performance for devices.
- **Better support for IoT/IIoT applications**
  Use of the 2.4 GHz frequency band spectrum with longer range and better propagation, combined with the ability to increase sleep time and battery life, is ideal for supporting low-data rate battery-powered IoT/IIoT wireless sensors that often require greater reach and the need to send data only at certain intervals.

Wi-Fi 6 Enabling Technologies

- **Orthogonal Frequency Division Multiple Access (OFDMA)**
  Encodes digital data on multiple subcarriers within frequencies, allowing simultaneous transmission to and from multiple devices.
- **Basic Service Set (BSS) Coloring**
  Reduces latency and optimizes spectrum use in dense environments by intelligently "color coding" shared frequencies that are detected by devices, allowing them to ignore traffic that does not have the same "color" rather than waiting for channels to be clear.
- **Improved Beamforming**
  Detects the location of a device requesting data and leverages multiple antennas (up to 8 per frequency) to transmit in the direction of the device.
- **Scheduling**
  Uses deterministic Media Access Control (MAC) to segment service and quality of experience to different users, with optimized packet scheduling achieving less than 2 ms of latency.
- **Target Wait Time (TWT)** – Allows devices to negotiate when and how frequently to wake up for sending and receiving data, allowing increased sleep time and better battery life.
- **Dual 2.4 and 5 GHz Operation**
  Leverages more non-overlapping channels and reduced interference available in the 5 GHz spectrum, while still taking advantage of the greater range.

The Need for Wi-Fi 6E

Since 1985, the unlicensed 2.4 GHz and 5 GHz frequency band spectrums for Wi-Fi use have been limited to less than 600 MHz of total bandwidth. While the narrow 20 MHz channels within these spectrums can be aggregated to support higher throughput using channel bonding, there are a limited number of these channels available.

As defined by the FCC, there are also certain channels unavailable for Wi-Fi use within the Unlicensed National Information Infrastructure (U-NII) radio bands that comprise the entire 5 GHz spectrum, resulting in a non-continuous band. These unavailable channels limit the ability to use channel bonding at 5 GHz. For example, there are only six 80 MHz and two 160 MHz channels available in the 5 GHz spectrum using channel bonding as shown in Figure 2.

FCC U.S. 5 GHz Channel Plan

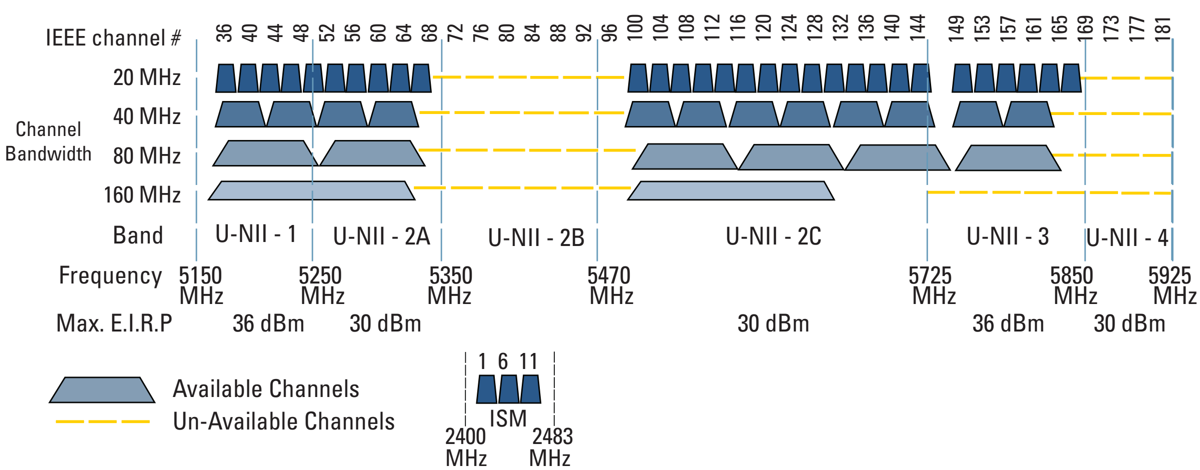


Figure 2: FCC 5 GHz Channel Plan
Information on these tables includes data and figures previously presented in
https://www.fcc.gov/document/fcc-opens-6-ghz-band-wi-fi-and-other-unlicensed-uses

With the number of wireless devices increasing exponentially, the Wi-Fi Alliance and other industry stakeholders advocated for additional continuous spectrum, which would accommodate more channel bonding. As a result, the FCC opened the 6 GHz frequency band spectrum in April 2020 for Wi-Fi use, which adds an additional fifty-nine 20 MHz channels. With the additional spectrum available, the Wi-Fi Alliance introduced the Wi-Fi 6E designation for devices to operate within the 6 GHz spectrum per 802.11ax standards, using the same technology advancements of Wi-Fi 6. In other words, Wi-Fi 6E is not a new wireless protocol but an expansion of Wi-Fi 6 into the new, wider 6 GHz spectrum that increases available bandwidth to 1200 MHz.

With the continuous 6 GHz spectrum, the smaller channels can be more easily bonded, enabling fourteen 80 MHz and seven 160 MHz channels as shown in Figure 3. Indoor Wi-Fi 6E also permits greater transmit power in bonded channels by expressing power limits as power spectral density, or PSD. While wider channels receive more noise, thereby reducing throughput, expressing power limits as PSD offsets that additional noise to encourage the use of bonded channels. Wi-Fi 6E is targeted to support the use of high-speed applications such as ultra-high-definition video streaming, online gaming, and augmented/virtual reality. It will also support high-density IoT/IIoT wireless sensor networks with large quantities of connected devices and provide better coverage for crowded spaces, such as large arenas and stadiums, since the 6 GHz spectrum is less congested.

Wi-Fi 6E devices, which may operate in the 6 GHz spectrum, must also support Wi-Fi 6 capability in the 2.4 GHz and 5 GHz bands for backwards compatibility. However, earlier generations of Wi-Fi cannot operate in the 6 GHz spectrum, which prevents these legacy devices from competing for bandwidth and slowing down the entire network. Additionally, power level restrictions have always been an FCC regulation to prevent interference with other services operating in the same band. Wi-Fi 6E retains this restriction using four defined power modes, including standard power for indoor/outdoor use (limited to UNII-5 and UNII-7 bands), low power for indoor only use (limited to UNII-6 and UNII-8 band), very low power for indoor/outdoor use, and client power for indoor/outdoor use.

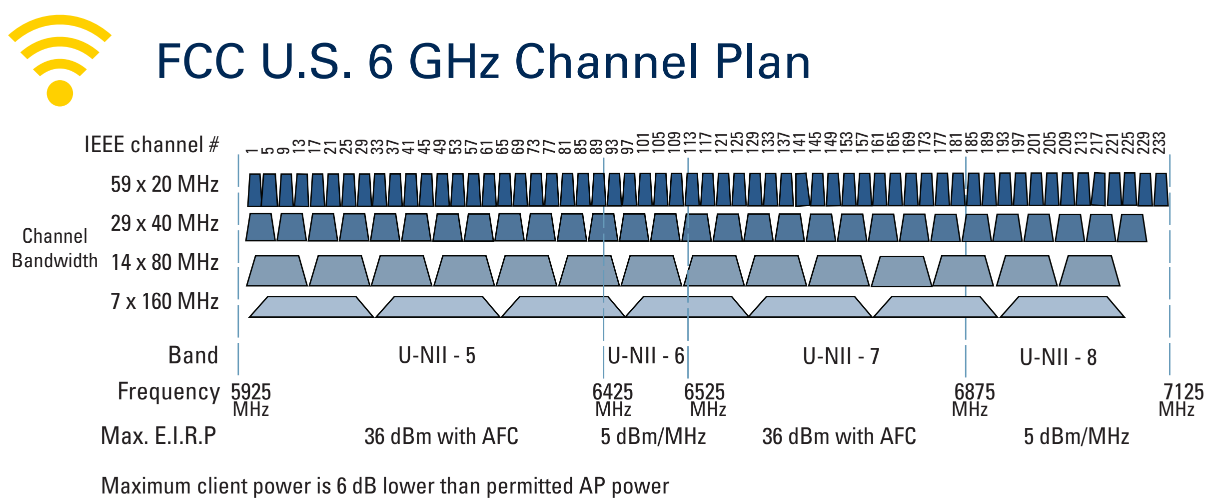


Figure 3: FCC 6 GHz Channel Plan
Information on these tables includes data and figures previously presented in
https://www.fcc.gov/document/fcc-opens-6-ghz-band-wi-fi-and-other-unlicensed-uses

The Wi-Fi Alliance has already launched its Wi-Fi 6E certification, and several chip set manufacturers announced 6 GHz chipsets in 2021. Wi-Fi 6/6E APs and devices are shipping from all leading vendors and expected to quickly become the mainstream technology as 41 countries have already authorized use of the 6 GHz spectrum. The industry is already predicting at least 20% of Wi-Fi 6 devices shipments in 2022 will support 6 GHz. Considering the speed at which Apple and Android smartphones evolve to support newer technologies and remain competitive, it's not off the mark to also expect smartphone support for Wi-Fi 6E in the near future.

Infrastructure Requirements

Back in 1999 when 5 GHz devices were first introduced, the reduced range capability due to higher path loss of the higher frequency, compared to 2.4 GHz operation, required twice the number of APs to be deployed to maintain the coverage for a given space. The doubling of AP density and associated cabling and connectivity needed to connect the APs had a significant impact on budgets at the time. Now, the transition to Wi-Fi 6E will be much less painful. With only slightly higher path loss at 6 GHz versus 5 GHz, and the advantages of the aforementioned higher PSD, leading AP vendors indicate that there is no need to further increase the number of APs, change AP locations, or redo wireless site surveys for environments with established 5 GHz technology typical to most enterprise businesses today.

While the number and location of APs fortunately does not need to change, the cabling infrastructure must support the higher throughput capabilities of Wi-Fi 6/6E. While a single Category 6A connection will support the 1.3 Gbps speeds for Wi-Fi 5, TIA industry standards and BICSI guidelines recommend a minimum of two Category 6A connections to each Wi-Fi 6/6E AP. This is the only way to effectively achieve redundancy and support the 5 Gbps throughput of Wi-Fi 6, while also supporting the potential higher speeds of future Wi-Fi 6E. Industry standards also recommend a minimum of a 25 Gbps uplink capacity within the fiber backbone infrastructure to support the increased amount of traffic and higher speeds that come with Wi-Fi 6/6E and more connected devices. It's important to consider that while Wi-Fi APs are often refreshed every 3 to 5 years, the underlying cabling infrastructure should have a typical lifecycle of 10 to 15 years. It is therefore vital to follow industry standards and best practice when designing and deploying the infrastructure.

Additional Wireless Technologies

While Wi-Fi 6/6E is the primary wireless technology to support everyday business applications and high-level user experiences across in-building and near-building environments, it is not the only wireless technology available. There are several wireless technologies that operate within various licensed and unlicensed frequency bands across the broader electromagnetic spectrum—from cellular communications and global satellites to a variety of short- and long-range low-power wireless applications.

5G Cellular Communications

Cellular technology has advanced from 3G and 4G/LTE to now high-band 5G cellular being rolled out across the country by mobile carriers like AT&T, T-Mobile, and Verizon. Operating within licensed high-frequency spectrums from 24 to 47 GHz, 5G aims to deliver 1 to 10 Gbps speeds and much lower latency—up to one-fiftieth the latency of previous 4G/LTE. However, due to its higher frequency, 5G has a shorter range than previous 3G and 4G/LTE cellular communications and therefore requires more small cell sites in more locations.

5G cellular is best suited for public outdoor mobile communications on roads and highways but can also deliver broadband access in some areas and support emerging outdoor IoT/IIoT applications like connected cars, smart traffic systems, and other smart city applications. While the high-frequency nature of high-band 5G offers poor propagation into and through buildings, the service can be brought into a building using small cell enterprise technologies or distributed antenna systems (DAS) with nodes throughout the building to boost cellular coverage. Most of these in-building cellular systems are deployed in more heavily-populated public spaces such as stadiums, arenas, and airports to support mobile traffic. Unlike Wi-Fi however, cellular communications require the Radio Access Network (RAN) and paid service provider plans, which often have limitations on data usage.

CBRS

Cellular-based technology can also be private through the Citizen's Broadband Radio Service (CBRS), also sometimes referred to as private LTE. CBRS operates in the 3.5 to 3.7 GHz frequency spectrum and is considered "lightly licensed" since it is prioritized for incumbents like the U.S. Navy, followed by licensed bidders, and general access. CBRS can allow an enterprise to establish their own private cellular network, which can be ideal for providing coverage at remote industrial locations, bringing connectivity to students in rural municipalities, or for supporting secure outdoor business needs like push-to-talk communications at large industrial sites, fleet management, or IoT/IIoT sensor technologies in the agriculture industry.

Long-Range, Low-Speed

Long-range, low-speed wireless technologies are ideal for connecting battery-powered IoT/IIoT sensors in large-scale industrial, agriculture, campus, and smart city environments across greater distances. Some technologies like NB-IoT are cellular based and require licensed frequency bands, while the Sigfox service and LoRaWAN protocol maintained by the LoRa Alliance® use networked gateways that collect the data and then backhaul via a cellular, Wi-Fi, or wired network. Because these applications operate at low frequencies and have low data rates that range from 50 to 200 Kbps, they offer superior propagation through building materials and can support distances up to 40 km in some instances.

The Wi-Fi Alliance is also addressing the need to support low-speed IoT/IIoT sensor applications with the introduction of Wi-Fi HaLow. Based on IEEE 802.11ah technology, Wi-Fi HaLow operates in the sub-1 GHz frequency spectrum using narrower channels to offer up to 100 times longer range and superior propagation to penetrate building materials compared to Wi-Fi 6/6E technology. A single Wi-Fi HaLow AP can connect hundreds of IoT/IIoT wireless sensors that use coin-sized batteries to distances up to 1 kilometer and speeds up to 150 Kbps. It also features enhanced TWT sleep-mode technology to ensure maximum battery life for these devices. Wi-Fi HaLow is an attractive alternative to other long-range, low-power wireless because it maintains the existing security features, IP-based protocols, and unlicensed spectrum of existing Wi-Fi technology.

Short-Range, Low-Speed

Short-range, low-speed wireless communications used primarily for device-to-device connections and tracking include familiar technologies like Bluetooth, Zigbee, Z-Wave, and RFID. Typically supporting speeds from 100 Kbps to 1 Mbps and distances around 100 meters or less, these short-range, low-speed applications are primarily deployed for specific purposes. Some common uses include inventory tracking systems in warehouses, mobile payment machines, hands-free mobile phone communications, access control card readers, and asset tracking. They can however also be used for short-range IoT/IIoT sensor communications within buildings.

Leveraging the Range of Options

Wi-Fi remains the predominant wireless technology for in-building and near-building communication in commercial, industrial, and residential environments. However, in every environment, multiple wireless technologies coexist and complement each other—rarely is there only one type of wireless communication deployed. For example, a university campus will typically have cellular coverage for larger outdoor spaces (e.g., athletic fields), but due to the expense of service provider data plans, students switch to Wi-Fi for near-building areas like courtyards and parking garages. Once inside the dorm or classroom, Wi-Fi supports virtually all student networking and connectivity needs. However, that same university may have long-range, low-speed wireless to connect campus-wide meters used for waste management and other monitoring capabilities. Short-range, low-speed wireless will also be prevalent across campus for everything from access control to point-of-sale machines.

Some wireless technologies today even coexist within a single wireless AP. It's not unusual for a Wi-Fi AP to support 802.11 wireless applications in conjunction with Bluetooth and Zigbee, enabling the AP to also function as a gateway for collecting and transmitting data from local IoT/IIoT sensors or other low-speed devices within a given space. Wi-Fi APs spread throughout a building for connecting laptops, tablets, smartphones, and other devices, provide an ideal and cost-effective building-wide platform for layering on IoT/IIoT technologies.

The key to cost-effectively deploying blended wireless technologies is to identify the range of applications, determine the bandwidth and distance required for every device, and work with your integration partners and vendors to come up with the right strategy and supporting solutions.

Optimizing Wireless Deployments

Wired connections will always have their place for fixed devices needing secure, dedicated bandwidth, but the fact is that we live in a modern digital world—and it's one where people want to remain connected without being tethered and where more IoT/IIoT devices are being deployed in more locations. With wireless becoming ubiquitous across every enterprise commercial space in every vertical market—from finance, healthcare and education, to industrial, hospitality, and retail—it's important to remember that every wireless application also needs an AP (e.g., wireless AP, gateway, or antenna) to send and receive information to and from devices.

Given the breadth of wireless connectivity, wireless APs are now deployed across a wider variety of controlled and uncontrolled environments and spaces. Considering that they are vital network endpoints in today's digital world, it's imperative to deploy these devices in a manner that optimizes coverage while meeting unique, and often critical, requirements for protection, security, accessibility, code compliance, and aesthetics.

Coverage Considerations

To optimize coverage, wireless APs, by their very nature, must be exposed to provide best line of sight and prevent obstruction by the building structure. This means ensuring that they are deployed at the proper location and height determined by a wireless design or plan and unobstructed by wall board, soffits, ceiling tiles, joists and other ceiling components. Other building components that comprise mechanical, electrical, and plumbing (MEP) systems must also not obstruct the wireless signal.

To optimize coverage, wireless APs are best mounted to the ceiling. In high and open ceiling environments, optimum position can be maintained using hanging conduit mounts. For large spaces and high-bay deployments common in warehouses, manufacturing facilities, and sports venues, wireless APs can be mounted using mounting frames in conjunction with beam clamp, threaded rod, or cable hanging kits. Wireless APs can also be mounted to walls if ceiling mount is not feasible but leading AP vendors recommend the AP should be mounted in a horizontal orientation whenever possible to maintain optimum coverage. This can be achieved using right-angle wall-mount solutions.

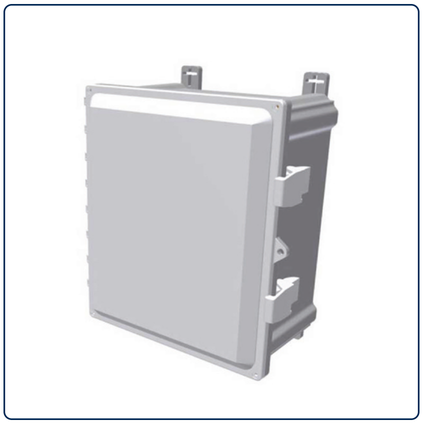
When mounting wireless APs in enclosures, it's also imperative to ensure that the enclosure is designed specifically for wireless communications, and that the enclosure or mounting solution does not degrade the wireless signal.

Harsh Environment Considerations

Certain environments can expose wireless APs to harsh elements such as extreme temperatures, dust, moisture/liquid, contaminant, and vibrations. These elements are common in spaces such as healthcare facilities, laboratories, gymnasiums/fitness centers, locker rooms, cafeterias, warehouses, and industrial spaces.

For outside near-building deployments such as parking garages, courtyards, outdoor eateries, and sports venues, it's extremely important to protect wireless APs from elements like rain, snow, sunlight, and extreme temperature. Per FCC rules, in the 6 GHz band, only APs intended for outdoor operation shall be operated outdoors. These APs will engage Automatic Frequency Control (AFC) to avoid interfering with incumbent operators.

When deploying wireless APs in harsh environments, they can be mounted in an enclosure suitable for the environment. The National Electric Manufacturers Association (NEMA) has a rating system that can provide guidance to the protection provided. NEMA 12 rated enclosures provide protection from dust and splashing or dripping water in indoor environments. NEMA 4 enclosures provide protection from spraying water in outdoor environments. NEMA 4-PW rated enclosures provide protection from high pressure sprays or washdown.



Another key specification includes the ingress protection, or IP, rating. The IP rating consists of the letters IP followed by two digits, whereby the first indicates protection against solids such as dirt and dust and the second indicates protection against liquids as shown in Figure 4. NEMA 4 and 4X enclosures have an IP rating of at least IP55.

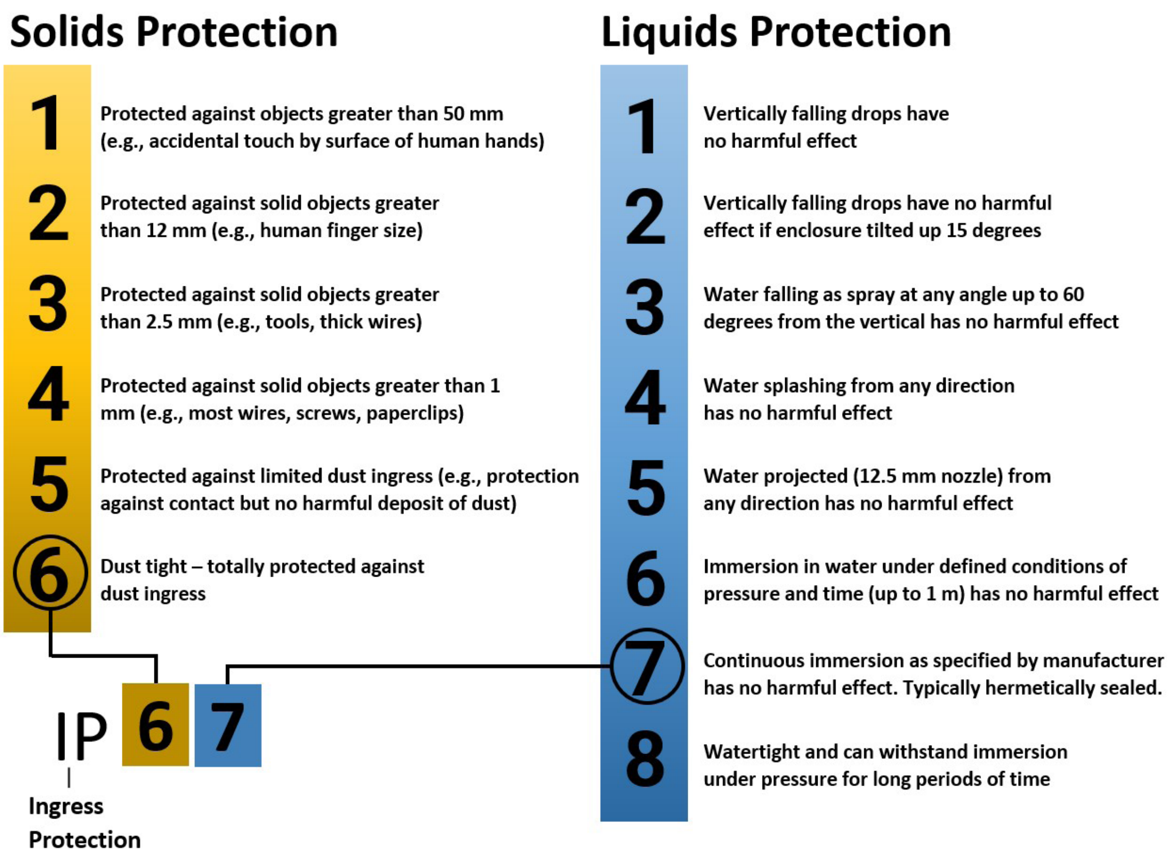


Figure 4: Developed by the European Committee for ElectroTechnical Standardization (CENELEC), IP ratings indicate ingress protection against solids and liquids.

Security Considerations

In open spaces such as schools, universities, retail establishments, hospitality venues, and other public spaces, it is vital to protect wireless network equipment from theft, vandalism, and accidental damage. Wireless AP enclosures in these areas should include locking mechanisms to prevent unauthorized access to equipment and the supporting infrastructure. When it comes to security, the priority is typically to reduce local network downtime and prevent unauthorized access to the larger network, rather than just physically securing the AP as property.

Compliance Considerations

Specific types of spaces may have regulatory requirements that need to be met when deploying wireless APs. For example, hospital and healthcare facilities need to comply with the Health Insurance Portability and Accountability Act (HIPAA), and electronic and physical security safeguards need to be in place for wireless networks, which can require the use of secured enclosures.

Many healthcare spaces also need to comply with infection control risk assessment (ICRA) requirements that aim to prevent the spread of airborne infectious diseases, dust, and spores from the plenum space above the ceiling or behind walls. To comply with these requirements, wireless APs and associated cabling must be deployed in a manner that avoids creating gaps and holes in suspended ceiling, hard ceilings, and walls that will allow contaminants to disperse or that can compromise differential air pressure in these spaces. Enclosures designed to allow access to the wireless AP without breaching space above the ceiling or behind walls should be used in these spaces. Features to look for include solid back boxes rather than vented boxes, as well as intumescent foam plugs for cable entry that maintain a seal and fire rating of the ceiling. In addition to healthcare regulations, there may also be state and local codes that can impact deployment. It's therefore vital to understand all local codes and requirements of the authority having jurisdiction.

Aesthetics Considerations

Many commercial buildings are designed to high architectural standards where ceilings and walls must remain aesthetically pleasing. In these scenarios, it is typically not acceptable for technology to be visible to building occupants. With the amount of technology now deployed in a single facility, this presents a challenge for wireless APs that must remain exposed for unobstructed line of sight to maintain coverage.

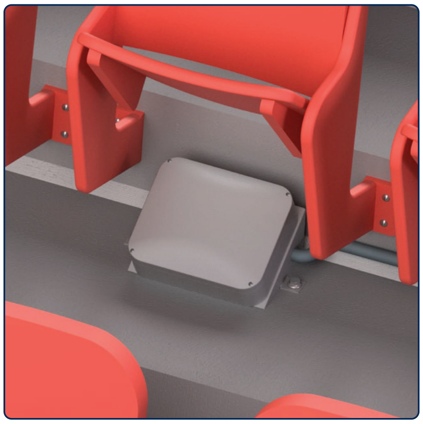
Wherever aesthetics is a requirement, wireless AP enclosures should emulate the appearance of the wall or ceiling via features like recessed panel installation, tegular flanges that match the surrounding ceiling tiles, attractive texture powder coat, or custom colors to match the surrounding decor. Stick-on and paintable vanity covers that do not block wireless signals or void vendor warranties are also ideal for complementing interior design.

Mounting Considerations

In addition to mounting wireless APs to ceilings or walls in the horizontal position to maintain optimum coverage, the proliferation of wireless communications can also require mounting wireless APs in unique locations.

Open outdoor spaces such as public parks, courtyards, campus greens, and other outdoor spaces where there is no feasible option for ceiling or wall mount may require outdoor wireless APs to be mounted on light poles or in free-standing bollards. Bollards should be rugged, weather proof, and tamper resistant while allowing wireless signals to easily propagate. Custom colors and heights can help bollards blend into the surrounding environment to improve security and maintain aesthetics.

Indoor and outdoor entertainment areas such as large sports arenas also often present the challenge of no ceiling or wall-mount option for ensuring adequate wireless coverage. One option for mounting wireless APs in this scenario is the use of stadium underseat enclosures. Like bollards, these enclosures should also be rugged, weather proof, secure and inconspicuous. They should also be small enough for mounting to seat bottoms or risers in a way that does not impede foot space.



Getting it Right

Wi-Fi 6/6E is a game changer for in-building and near-building wireless communications that will provide the bandwidth, performance, and reliability to truly untether just about any connected device and meet today's demand for greater bandwidth and high-speed internet access to support emerging applications—from video conferencing and streaming to online learning, virtual/augmented reality, and gaming. At the same time, Wi-Fi 6/6E will coincide with a range of other wireless technologies like 5G cellular and short- and long-range low-speed communications that support emerging real-time and IoT/IIoT technologies across the globe.

With the proliferation of wireless communications and the need to deploy wireless APs in nearly every environment, it's important to ensure optimum coverage and understand the unique environmental, security, compliance, aesthetics, and mounting requirements of each space. Optimizing next-generation wireless deployments in today's digital world is easier with the right partner and solutions. Oberon can help enterprise entities prepare for next-generation wireless deployments in just about any venue with its comprehensive range of wireless AP enclosures, mounting solutions, and accessories:

- Right-angle wall-mount and ceiling-mount solutions for suspended ceiling, hard ceiling, open ceiling, warehouse, and high-bay environments to ensure optimum wireless coverage
- Wireless AP enclosures designed to offer protection in industrial, wet, dusty, and outdoor locations
- Secure locking ceiling and wall-mount wireless AP enclosures to prevent tampering and unauthorized access
- Ceiling wireless AP enclosures that simplify ICRA, HIPAA, and code compliance in healthcare environments
- Low-profile and recessed wall- and ceiling-mount solutions and vanity covers that allow wireless APs to blend into the surrounding décor for superior aesthetics and improved security
- Free-standing bollards for mounting outdoor wireless APs in public parks and other outdoor open spaces
- Discreet underseat mounting solutions for indoor and outdoor entertainment and sports venues

References

[1] *Statista. WLAN connected devices worldwide 2016-2021. Jul 17, 2020.*
https://www.statista.com/statistics/802706/world-wlan-connected-device/

[2] *Statista. Smartphone Subscriptions Worldwide 2016-2027. February 23, 2022.*
https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

[3] *How Many Smartphones are in the World? https://www.bankmycell.com/blog/how-many-phones-are-in-the-world*

[4] *"Wireless Connectivity Market by Connectivity Technology (Wi-Fi, Bluetooth, NFC, ZigBee, GNSS, LTE CAT-M1, NB-IoT, LoRa, SigFox), Type (WLAN, WPAN, LPWAN), End-use (Wearables, Consumer Electronics, Healthcare), and Region - Global Forecast to 2025". October 2020.*

About Us

Oberon partners with leading technology vendors to support today's businesses with their technology migration and next-generation wireless deployments—from Wi-Fi and 5G cellular for today's bandwidth-intensive requirements, to short- and long-range low-speed wireless technologies for connecting emerging IoT/IIoT wireless sensors that improve efficiency and optimize operations. Visit oberonwireless.com to learn more about how Oberon can help you optimize next-generation wireless deployments for the digital world.

oberonwireless.com

sales@oberonwireless.com

877-867-2312

A division of Chatsworth Products