Warehouse & Manufacturing Wi-Fi

Wi-Fi Network Design and Deployment Best Practices

iBwave

Table of Contents

A high-quality wireless network can be the key to the efficient operation and the bottom line within the high-tech wired warehouse and manufacturing facility of the 21st century.

The list of potential issues a warehouse & manufacturing Wi-Fi network designer can encounter are nearly endless. What if wireless inventory control apps lose a signal or automated equipment that depends on seamless communication suddenly encounters a dead spot? Warehouse Wi-Fi network design cannot be left to chance and "good enough", it has to be done right the first time.

In fact, reliable, resilient wireless warehouse and manufacturing networks have become business critical.

Wireless network design in an industrial environment is challenging in the best of conditions, and unfathomably complex when care is not taken to anticipate all that can go wrong. Harsh industrial environments, the reality of the manufacturing floor, countless moving parts such as forklifts, constantly changing stock levels that create fluctuating RF signal propagation, architectural elements such as metal girders and corrugated metal walls, outdoor processing areas, and an increasing dependence on robotic technology that handle stock, control inventory, and rely on a rock-steady Wi-Fi network to operate at all.

In this eBook we're going to address the following crucial questions:

- What are the different types of manufacturing environments to consider?
- What are the most common challenges of designing Wi-Fi networks in a manufacturing environment?
- What are best practices to help overcome them?
- How does using a software like iBwave make warehouse Wi-Fi network planning design and validation easier and more efficient?

Understanding The Warehouse & Manufacturing Environment

For the purposes of this eBook, '*warehouse & manufacturing*' will serve as an umbrella term to describe a range of large plant-type facilities where products are manufactured and/or stored for eventual distribution and subsequent resale. But the modern definition of warehouse & manufacturing goes beyond either and into the office spaces that support it, as well as the distribution centers that manage post-production and logistics.

In this eBook the following examples will serve to represent the range of industrial warehouse environments:

Manufacturing Plants

These are where goods are produced for distribution and eventual resale. Manufacturing plants exist to produce most everything sold and used today, including; semiconductors (microchip and processors), consumer electronics, automotive, aeronautic and marine products, medical equipment and pharmaceutical, clothing, plastic/cardboard for food and consumer product packaging, and of course food.

Distribution Centers

In many cases production plants do not handle the storage and distribution of the products they manufacture and choose to delegate the role to a distribution center. Whether these are located adjacent the plant in question or in a completely different location they require the same high-performance wireless network, and the same rigor in planning, designing and validating it.

Back-Office

Both manufacturers and distribution centers are controlled by back-office areas and buildings that support their efficient operation. Typically these consist of open-area or closed offices, storage, exterior or interior single or multi-level parking lots and usually a secured perimeter. A single plant can often include two or more back-office locations and most will require that their Wi-Fi network successfully connect manufacturing, distribution, and back office areas while taking into consideration the vastly different environments presented by each.

Warehouse & Manufacturing Wi-Fi Network Challenges

Designing Warehouse & Manufacturing Wi-Fi Networks

Production plants are busy, crowded places where activity is complex and non-stop, space is at a premium, and the environment is subject to change on a scale many others that employ Wi-Fi networks never encounter. Forklifts, robotic technology, miles of shelving with constantly changing inventory levels, high ceilings, and metal everywhere; from girders and walls to shelves and products including the machinery and processes that do the manufacturing of a myriad of products. Add to this the presence of mobile inventory scanners and devices and it is apparent that any Wi-Fi network in a warehouse & manufacturing environment must exist within a constantly shifting landscape of machines and materials that can challenge the best Wi-Fi network engineer.

A new network design absolutely must have built-in flexibility that anticipates current and possible future needs for expansion.

The Importance of Wireless Networks In Warehouse & Manufacturing Environments.

Just as consumers must cope with an ever-changing sales landscape, so do businesses that create, store, and distribute the products they purchase. Consumers have more products to choose from, more ways to get them, and expect to get them in a timely, efficient way. Business is engaged in a never-ending race to keep up with, exceed, and even anticipate consumer expectations – and technology is proving to be the only way they can do it. Increasingly companies are deploying robotics, installing wireless applications, IoT hardware, and mobile devices including wearables to perform everything from inventory tracking to barcode scanning, dimensioning, systems & logistics management, and a host of other operational uses in warehouses, manufacturing facilities, distribution centers and back office areas. It's a trend that will only grow.

All of these mission-critical applications & wireless technologies, and indeed the very operation of any of the warehouses and factory area we've described ultimately rely on the Wi-Fi network that enable them. If the backbone of a network is insufficiently reliable or resilient, then production, distribution, competitiveness, and potentially the bottom line and viability of the company is put at risk.

Warehouses and manufacturing facilities are a dangerous place for Wi-Fi networks, and a lot can go wrong.

Warehouse Wi-Fi Best Practices will focus on four different areas that pose a challenge in the warehouse-type environment:

1) Business Challenges
2) Capacity and Performance Challenges
3) Security Challenges
4) Backhaul & Cabling Challenges

Business Challenges

The warehouse & manufacturing Wi-Fi network environment is unique in that it may have a connected device density higher than most any other. Not only are staff employing a myriad of devices, but the production area may be home to a sea of equipment that connects to the network, and each other, in a variety of ways. Adding to the complexity is the rate at which this equipment is updated and new technology, like IoT devices, folded into the mix. New equipment might require physical connections, while some are able to communicate wirelessly. A new network design absolutely must have built-in flexibility that anticipates current and possible future needs for expansion.

Equipping the information age are plants that make semiconductors, processors and a long list of other electronic components, all of them relying on clean-room environments in which it can be difficult to introduce new equipment, or, in the case of wireless engineers, use site survey tools to capture accurate data.

Tangentially, the way warehouses and manufacturing facilities do business is changing nearly as fast as the technology it relies upon, and this too places stress on a wireless network, with new business practices adding to the volume of traffic and creating troublesome bottlenecks.

Security also poses significant challenges. Levelling and zoning provide a certain measure of compartmentalization which helps secure a network, but device access also needs to be properly authenticated before authorization is granted while limiting the propagation of RF signals. Much of this is governed by the ISO/IEC 27001 Information Security Management System standards that cover 14 separate security domains.

Capacity & Performance Challenges

It all starts at the access point (AP) where devices & equipment link to a warehouse & manufacturing Wi-Fi network, and because Wi-Fi is a shared medium it is imperative that connected devices are able to communicate with each other. Improper AP planning and deployment can create "hidden nodes", where devices are known to the AP, but invisible to one or more other connected devices sharing the AP. Insufficient APs, less-than-optimal AP and/or client localization, client density (# of connected devices per AP), and AP/client power balance can all trigger warehouse & manufacturing Wi-Fi network issues, all of which can be anticipated by analysis, planning before a single network component is installed, and thorough validation once it is in place.

Capacity is a key challenge for many venues, but in particular for a warehouse & manufacturing environment where a host of people and equipment, each equipped with devices, converge, flow in, then out, often in an unpredictable way. Traffic density, or the number of physical devices connected to each AP, and that in turn share a common network, can serve to throttle performance, and as the amount of data travelling over networks increases exponentially so does the stress upon them. Each AP is limited to a set number of connected clients, and total AP count can often fall below what's required during peak demand. Staff use (official & personal), those who bring their own devices, the number of devices per person, the explosion of IoT devices, and the massive bandwidth requirements exacted by data from video, voice over Wi-Fi, inventory control, and manufacturing equipment can tax a network, so planning must take into consideration that the total amount of throughput will only continue to increase over time.

Architectural design of any industrial or warehouse building can have a marked effect on connection integrity & propagation. Everything from construction materials to ceiling height, metal elevators and structural components, fire-rated doors, tinted windows to furniture in office areas, storage area racks, automated production equipment and the presence of other radio spectrum transmission equipment can impede connection and propagation. Things in plain view, as well as many hidden structural elements can impede the propagation of Wi-Fi radio signals, furthermore, signal attenuation through various materials differ widely across both 2.4 GHz and 5 GHz bands.

Plants manufacturing electronic components of all kinds not only employ equipment that needs to connect to the Wi-Fi network, but ironically create products that themselves are embedded with wireless technology and just about every RF signal propagation-hindering material in existence. Case in point; retail Wi-Fi networks have a hard-enough time penetrating through racks of sweatshirts and coffee drinkers, imagine the challenges facing one that needs to operate seamlessly and reliably in a manufacturing environment filled with component metals and materials designed to absorb, transmit or carry RF signals!

Complicating the equation is the presence of production equipment of all kinds which pose a risk as they can generate radio signals simply through their operation and cause interference across the crucial 2.4 GHz and 5 GHz spectrums. Warehouses and manufacturing facilities are a dangerous place for Wi-Fi networks, and a lot can go wrong.

Multiplying the challenges are the different packet sizes created by the variety of connected devices and equipment and their end-use that a network must accommodate. Automated equipment, robotics, inventory control, email, video and voice over Wi-Fi all impact network performance and capacity differently, and this must be factored into initial network planning and design.

As fast as Wi-Fi technology can change, the backlog of still usable legacy devices grows. The cost of replacing structural network components, such as costly custom-built automated manufacturing equipment, sorting and storage machinery, and inventory scanners can be prohibitive, so it's good practice for any business to make use of them for as long as they remain compatible with the newest components of the network. Ensuring backward, and forward compatibility is simply part of sound warehouse and manufacturing Wi-Fi network planning. We're on the cusp of the IEEE 802.11ax release, heralding the advent of HEW (high-efficiency wireless) across 2.4 and 5 GHz spectrums and the accompanying devices, and while functioning at much higher data rate requirements networks will still need to interface with legacy devices.

Years of accrued experience have demonstrated time and again that a lack of a rudimentary Wi-Fi skill set among staff, and the reluctance to employ full-time or third-party ICT personnel to properly, survey, design and validate the plan for a warehouse or manufacturing Wi-Fi network are at the root of most capacity and performance issues.

Then there are the unknown unknowns… new equipment, IoT appearing in new device types, innovative technology applications for business, and business processes, client devices with increasing capabilities, new capabilities, and the consumers, staff and intermediaries all connecting to the warehouse and manufacturing Wi-Fi.

Security Challenges

The difficulty of securing a network increases exponentially along with the complexity of the network, the number and variety of devices that need to connect to it and the legacy technologies that must be accommodated which may heighten network vulnerability.

Other factors such as rogue hotspots and rogue APs, usually the result of staff or clients with their own APs, anyone enabling their smartphones with a mobile hotspot, using a Mi-Fi device to set up their own network and using their mobile cellular network to backhaul to the internet can create serious connection bottlenecks. Convergence of several devices transmitting simultaneously on the medium frequency spectrum can also impact network integrity and impede security.

Segmentation of a network into production floor, warehouse, and back-office streams through the use of separate physical cabling, or VLANs can alleviate these issues and are best determined by an evaluation of the relevant security requirements of each individual network.

Securing a warehouse & manufacturing Wi-Fi network requires insight and forethought if the numerous variables are to be properly accounted for and weaknesses anticipated.

Backhauling & Cabling Challenges

Backhaul cabling also figures into the warehouse & manufacturing Wi-Fi network equation. It's crucial to be fully aware of the capacity of locally-based servers with centralized management systems, wireless LAN controllers, client IP address assignment, and just as importantly, network speed (10Mbps to 10Gbps), and the inevitable presence of switchers and routers.

Newer plants and warehousing facilities are in the best position to host flexible, resilient and reliable Wi-Fi networks through the use of the latest technology and adherence to the rigorous TIA TR-42.9 Industrial Infrastructure and ANSI/TIA-1005 Telecommunication Standard for Industrial Premises criteria as well as their use of high-capacity fiber-optic and copper cabling backbones. Conversely, older installations often simply add to their cabling infrastructure in order to handle the increase in automated equipment, robotics, and growth in the use of IoT devices which creates jerry-built infrastructures vulnerable to performance and security shortfalls.

Now, it's time to get down to the business of planning, designing, and validating a warehouse & manufacturing Wi-Fi network, which together can limit and often eliminate the numerous potential issues outlined above.

Warehouse & Manufacturing Wi-Fi Network Best Practices

Regardless of end-use, size, or complexity, it takes the right tools that equip one with the proper vigilance and foresight required to plan, design, and validate a world-class Wi-Fi network. However complex or sprawling your production facility or warehouse, it's possible to cover a lot of ground by following a comprehensive checklist. Ours will help you evaluate your needs, anticipate growth, and design a warehouse & manufacturing Wi-Fi network that is robust, reliable, resilient, and more than able to meet the standards for coverage, capacity, compatibility and confidence.

Gathering Network Requirements

Understanding the current situation is the first step to properly evaluating the needs of any warehouse Wi-Fi design project. Customer expectations, now, and in the future allow you to configure a new network design that can respond to both. Gathering network requirements in any number of different warehouse environment types is step one, and can determine the success of the project.

There are many aspects to consider in order to ascertain current and future warehouse Wi-Fi network design requirements; production floor staff, operational equipment, deployed wireless apps, end-users, peak operational hours, and outdoor, back-office, and storage areas. And that's just for starters…

Our planning checklist should go a long way to helping you prepare this first phase of your warehouse Wi-Fi network design project. You'll find a handy tear-out copy of this planning checklist complete with space to fill in the answers that reflect your current network situation in the addendum at the end of this publication.

Planning Checklist

What to Know

- Evaluate and anticipate the services you'll need to offer over your network. (Voice over Wi-Fi, email, internet access, inventory control, work orders, etc.)
- Evaluate and anticipate the application types you'll be deploying. (Voice, video, data)
- Evaluate the optimal segmentation of data and number of logical networks your setup may need upon launch, and as the demand on the network grows.
- Evaluate the location and architectural parameters

1) Building materials – presence of concrete, metal, tinted windows, high ceilings, fire-rated doors and any other RF propagation inhibitors)
2) Assess the immediate vicinity surrounding your location. Is it urban with a lot of bleed over from competing Wi-Fi networks?
3) Do you have a digital version of a current floor plan of your location that can be imported into our iBwave Wi-Fi® design software for AP placement and RF predictive modeling?
4) Do you foresee high-density areas within the warehouse that may need to host many client devices? (e.g.; a production floor with multiple Wi-Fi enabled devices) Are there any other current or projected higher-density areas? (e.g.; shipping & receiving, back offices, exterior operational spaces)
5) Do you want to include exterior as well as interior network coverage?
6) Is there an existing network infrastructure, including legacy or other, and backhaul cabling? Does the client have a preferred vendor?
7) Will existing backhaul cabling restrict the optimal localization of APs along its backbone? It is recommended to use a professional grade Wi-Fi RF design tool like iBwave Wi-Fi® to best determine AP positioning to ensure proper coverage and capacity requirements.
8) Is it a requirement for your APs to have a look & feel that is in harmony with architectural design, fit, and finish? Does the building owner/design approver prefer them to be out of the way and invisible? Does your installation's propagation profile permit hidden APs?
9) Will exterior APs be required, and if so need to be equipped with protection from the elements?
10) Can you consult with the current network, server, and storage administrators and personnel that have an intimate knowledge of the existing network infrastructure, potential extant issues and its compliance with ISA-95?
11) Do you have access to a site or facility manager who understands the current location's infrastructure and can advise on the placement of APs, power supply, and other equipment that may need to be installed?
12) How many active Wi-Fi devices currently exist in all zones across the network?

- Evaluate and anticipate your warehouse & manufacturing Wi-Fi network's connection and capacity needs.

1) How many active client devices do you estimate might connect to the network at peak hours? Are there specific areas that will have more connections than others?
2) Do you know what those peak hours will be? Is the venue a 24-hour distribution center or is your network limited to normal store hours?
3) Are you subject to local regulations (FCC, CRTC) governing RF propagation, frequency limitations, maximum allowable transmission power and EIRP (Equivalent Isotropically Radiated Power) or other relevant limitations?
4) Will you require seamless roaming capability?
5) Will you require location-based services or real-time location services such as asset tracking?
6) Will you build-in sufficient failover ability and redundancies, particularly in the case of warehouses and distribution centers, to ensure seamless operation even at peak critical times where the network is subject to higher stresses?
7) What are the current and future performance targets for the network as a whole, and subsequently for each network type?

- Evaluate and anticipate your warehouse & manufacturing Wi-Fi network's backwards and forwards compatibility requirements.
  1) Should you plan for full IEEE 802.11-1997 to IEEE 802.11ax compatibility?
  2) What's your cut-off for backwards compatibility?
  3) Will you support a wide range of legacy devices?
  4) Do you anticipate the need for PoE (Power over Ethernet) capabilities?
  5) Which protocols will your network need to support? (IPv4 / IPv6)

- Evaluate and anticipate your warehouse & manufacturing Wi-Fi network's security needs.
  1) Will your network require the hiring of a Security Manager that understands your current and future security needs, compliance with security regulations and their integration into the network, and stay abreast of rapidly changing network security technology?
  2) Are you hoping to include a wireless intrusion detection and prevention system?
  3) Have you factored in the need for preventing unlawful signal interception?
  4) Is there value in hardening your network equipment and infrastructure against present and future vulnerabilities?
  5) What about other security requirements such as captive portals, guest access control, RADIUS ability (Remote Authentication Dial-In User Service) and secure billing.
  6) Is the network located in an area where intermittent power outages might require that it be equipped with a UPS backup?

- Operationally speaking…
  1) Has a finance manager or CFO made sufficient allocation of funds available for the design, deployment and continued maintenance of a robust warehouse & manufacturing Wi-Fi network?
  2) Have you weighed leasing versus purchasing a network setup?
  3) Is a project manager entrusted with control and coordination of the myriad of details on which the successful implementation of your new network depends?
  4) Will 24/7 monitoring be needed from on-site IT professionals, or outsourced to on-call service providers?
  5) Will personnel be available to assist during the planning, design, deployment and validation of the new network?

Conquering A Challenging Landscape

Factory Floors

In the warehouse & manufacturing environment, the factory floor is truly where the rubber hits the road, or, in this case, the metal meets the concrete. It's a complex, and in many cases, a continuously operating place filled with machinery – much of it emitting radio frequencies simply by running, robotic assembly equipment, fork-lifts, and all of it housed within buildings that are cages built of metal and concrete that reflect, intercept, and scatter an RF signal. In short, it's a trap ready to ensnare anyone who installs equipment in areas of high signal attenuation vulnerability, such as between metal pipes, on metal cabinets, adjacent to air ducts or equipment that may inadvertently transmit an RF signal that interferes with the network. Predictive RF planning relies on access to current floor plans, and detailed building materials at the prospective network site.

One common error is APs interfering with each other because they are mounted in close proximity, a problem that is compounded if they happen to be operating on the same frequency and channel. But that's just the tip of the Wi-Fi hazard iceberg.

Specific environments may necessitate the use of external directional antennae that connect to APs, extending their range and quality of propagation by limiting multipath issues, along with co- and adjacent channel interference (CCI & ACI). Client devices by default roam to the channel with the strongest signal, and advanced Wi-Fi solutions can use band steering to balance devices between 2.4 GHz and 5 GHz to optimize network performance. Airtime Fairness also comes into play, helping to balance time and data throughput across devices that use different generations of technology, and hence operate at a range of communication speeds. Interference can be counteracted by Radio Resource Management (RRM) that allow for the detection of interference while automatically allocating Wi-Fi channels to devices in the most efficient way.

Automated robots, fork-lifts, voice over Wi-Fi, tablets and a host of other monitoring devices that oversee production and warehousing need trouble-free roaming ability with seamless handover between APs, so it's always wise to build in sufficient overlap when determining AP coverage. Data throughput, whether it be voice, device-to-device, or IoT communication can create operational difficulties that cost time, and money.

An always-on warehouse & manufacturing Wi-Fi network is best able to manage things by performing status updates which allow operators to be warned of potential problems long before they cause a production shutdown that could cost millions. The most expensive plant is an idle one, and the cheapest way to prevent it is with a well-designed warehouse & manufacturing Wi-Fi network that can anticipate issues.

Warehouses especially are filled with ceiling-high industrial grade shelving which introduces addition surfaces to interfere or reflect RF signals, and those shelves are filled to capacity with a host of products with a vast range of attenuation values. Add to that the fact that shelf stock levels vary, as does the nature of the stock being stored (e.g.: liquids, solids, metals, wood, electronic components) which together contribute to an ever-changing RF signal propagation environment and steep demands on devices that rely on a stable connection. Directional antennae can focus the signal down corridors and help alleviate this pitfall.

Directional antennae can also serve to help reduce or eliminate RF leakage, and hence maintain security of the network. Creating a Faraday cage in order to limit RF propagation beyond the facility is highly recommended and easily achieved by applying metallic paints or installing wire mesh lining on predetermined wall surfaces. Warehouse & manufacturing Wi-Fi network security is not complete without proper data and communication encryption protocols in place so it's imperative they be implemented into Wi-Fi network layers.

The most expensive plant is an idle one, and the cheapest way to prevent it is with a well-designed warehouse & manufacturing Wi-Fi network that can anticipate issues.

It's also recommended that a warehouse & manufacturing Wi-Fi network operate APs with dual 2.4 GHz and 5 GHz bands. The 2.4 GHz spectrum simply doesn't have enough available channels and is limited to a maximum of 4, while the 5 GHz band enjoys 23. That said, the 2.4 GHz channel does offer a longer range, but is generally slower than the 5 GHz spectrum. Newer devices are appearing in increasing numbers and often support the 5 GHz frequencies.

Certain AP designs already sport advanced designs and are able to serve as virtual controllers, completing automatic channel selection and allocation, network assurance from the perspectives of client and host, offering captive portal technology, management dashboard interfaces and a host of cutting-edge security features. Cost of these full-featured AP units is usually directly proportional to how advanced they might be.

Offices

Office areas adjacent warehousing & manufacturing facilities are as vulnerable to performance and security issues as any other part of the network and require the same care and consistency of planning rigor as do factory and storage areas. Crucial to an uninterrupted production process is the separation of office network zones from those covering the plant floor. That way failure of the first needn't be the trigger that creates a cascading shut down of the entire network, and in turn, production.

Like the warehouse, storage, shipping, and external areas, it is best to provide connectivity at both the 2.4 GHz and 5 GHz level with dual-band interior APs. Because the layout of office areas will differ from the warehousing & manufacturing areas the rules that dictate AP use and localization will resemble that of a large shopping mall *(see Retail Wi-Fi Network Best Practices).*

Voice over Wi-Fi, video, audio, file transfer, email, and real-time inventory and security require multiple APs, and this can engender interference, channel overlap, and countless other potential propagation issues and throughput bottlenecks. The use of additional external direction antennae is a good practice for use in specific targeted locations to avoid signal bleed and potential security lapses. Don't be shy to use enough APs, choosing units that can handle a high volume of concurrent connections and support QoS (Quality of Service) technology that work to prioritize data.

Outside Areas

Exterior areas associated with warehouses & manufacturing need to be able to rely on a stable, secure Wi-Fi network every bit as much as the enclosed production and office areas do. Warehouses in particular count on an uninterrupted link to and from your premises to the immediate exterior around it so that stock is able to be moved in a timely way from factory floor to warehouse, eventually on for shipping to intermediaries or to market. Warehouses and factories go beyond the walls that enclose them, and those exterior areas place very different demands upon hardware, connectivity, and network capacity.

The first challenge is an obvious one; weather. The elements can spell trouble for the exterior components of your warehouse & manufacturing Wi-Fi network. Cold, heat, direct sunlight, excessive dryness and of course humidity all take their toll on equipment, so ensure that it's protected, and accessible for easy maintenance. It's recommended to opt for APs hardened for outdoor use that meet or exceed NEMA or IP ratings for ingress protection. Needless to add that exposed cabling should also be weather and UV resistant.

Availability of reliable power and backhaul data cabling or meshed wireless backhauls are must-haves. Certain jurisdictions may regulate the standards of exterior APs, so be aware of the rules in the area where you're designing the Wi-Fi network.

Warehouse & manufacturer Wi-Fi network designers working in countries within the European Union should take note that ATEX 95 and ATEX 137 outline separate safety directives for indoor and outdoor electrical equipment in potentially explosive atmospheres for makers and users respectively.

For more of ATEX 95 & ATEX 137 see: *http://ec.europa.eu/DocsRoom/documents/16402/attachments/1/translations/en/renditions/native*

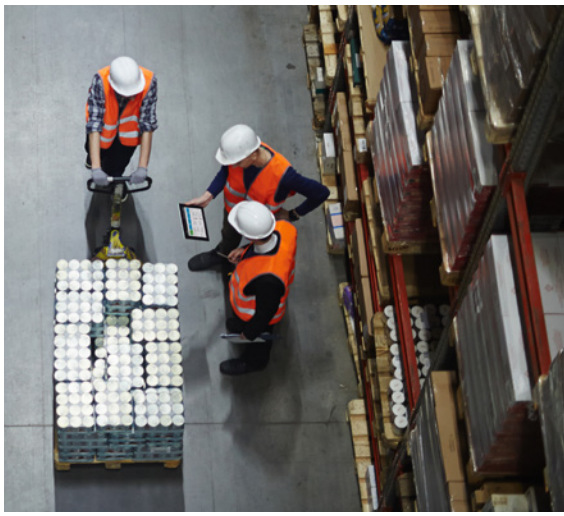
Warehouse & manufacturing are punishing environments for Wi-Fi network infrastructure and RF signal propagation, a fact that is only exacerbated by the conditions that exist in outdoor areas. Add to that the increasing number of severe weather events and weather extremes, and the need for hardened outdoor Wi-Fi network components becomes clearer.

Warehouse & Manufacturing Wi-Fi Network Technology

Essential Technologies

No matter the venue, it's essential to equip your network with as modern a technology toolkit as possible. Cost is always a factor, with more advanced systems and features invariably being more expensive, both to acquire and to train personnel in its use. But what you invest up front in modernization you save on the other end by being able to keep a system relevant and viable for longer periods. The first technology to be superseded and deprecated will always be the oldest, and least advanced. Something to think about…

So what should a well-designed warehouse & manufacturing Wi-Fi network include? What are the must-haves and nice-to-haves of a happy, healthy network? Here's a quick point-form guide to those features that should be seriously considered, plus a checklist of additional important technology best-practices that can add flexibility and resilience to your network design.



Key Technical Features

Location-Based Services

An important bedrock of data collection, location-based services provide additional depth & breadth to the precision of the conclusions that can be drawn from the analysis of the raw data compiled. Consumer traffic and density patterns, geofencing data and purchase patterns can all be readily determined from the use of location-based services.

Management & Analytics Support

This is crucial for the efficient and seamless operation of your warehouse & manufacturing Wi-Fi network, the collection of data, and just as importantly, its distillation, analysis and finally the formulation actionable conclusions. No network runs itself! Yet…

VPN

Virtual Private Networks have been leading technology headlines for some time, and while the need for individuals to acquire their services for private use is questionable, the need for a warehouse & manufacturing Wi-Fi network to operate one are less ambiguous. A warehouse & manufacturing Wi-Fi network already is a VPN of sorts but wrapping it in an actual VPN framework can add to its security, and the subsequent compartmentalization can serve to mitigate the issues created by complexity.

Gigabit Ethernet Port Count

Nothing ruins a warehouse & manufacturing Wi-Fi network's day like dropped connections, DoS (Denial of Service) due to traffic surging over capacity, or the complete lack of essential failsafe redundancies. It may not be an exaggeration to say you can never have enough gigabit Ethernet ports. You can always count on needs eventually meeting and surpassing whatever capacity was initially built into them. Maxing out your gigabit Ethernet port count helps forestall the inevitable.

Power Over Ethernet

IEEE 802.3 standardized power-over-Ethernet in 2003, allowing for the convenience of concurrent data and power transmission over a common Ethernet cabling. It can save on infrastructure costs and time required for installation – plus it can keep a network up and running during shortages if connected to a backup power source.

Swimming The IEEE Sea

IEEE 802.11 governs most of the world's wireless networks. It's a comprehensive set of standards, and many of its amendments were established to regulate those systems subordinate to the core Wi-Fi network. Here are a few:

- **IEEE 802.11ac** MU-MIMO (Multi-User Multiple Input Multiple Output)
- **IEEE 802.11ax** HEW (High Efficiency Wireless)
- **IEEE 802.11v** Client management
- **IEEE 802.11k** Radio resource management
- **IEEE 802.11w** Management frame protection
- **IEEE 802.11i** Data frame security

Want to know more?: An overview of the IEEE 802.11 standards and its amendments can be found at *https://en.wikipedia.org/wiki/IEEE_802.11*

Manufacturing Framework Standards For Automation, Operational Technology & Control

Several international bodies regulating and overseeing industrial standards & practices have developed guidelines that serve as benchmarks for warehouse, manufacturing and associated segments, and many of them enter into play when planning and designing a robust Wi-Fi network.

International Society of Automation

- **ANSI/ISA-95**
  A set of standards governing a range of processes and charged with developing automated interfaces between enterprise and control systems.
- **ISA-99/IEC 62443**
  Global standards for security for organizations who are part of the Industrial Control Systems in the Operational Technology group.

Third-party vendors, such as Rockwell Automation and CISCO have collaborated to develop and elaborate the Converged Plantwide Ethernet architecture model which provides both network and security services for industrial automated control system devices, equipment, and associated applications. This architecture specifies layers, levels, and zones, echoing the terminology of both the ISA-95 and the Purdue Reference Model For Control Hierarchy. ISA-99 further segments these levels into zones that serve to establish trust domains for security access used by smaller LANs to manage network traffic.

Manufacturing Framework Zones & Level Hierarchy

Cell/Area Zone: Level 0,1 & 2 - Manages industrial control devices and multi-disciplined control applications.

Manufacturing Zone: Level 3 - Manages plant-wide applications that are comprised of multiple cell/area zones.

Enterprise Zone: Level 4 & 5 - Manages IT networks, business apps, servers, and intranet.

Industrial Demilitarized Zone: AKA the IDMZ. A buffer zone between the manufacturing and enterprise zones data can be shared securely. The IDMZ processes all incoming traffic but permits no direct throughput between isolated zones.

Technology Best-Practices Checklist

Do:

- Use the 20 MHz channels (1,6,11 and/or 1,5,9, 13) exclusively within the 2.4 GHz range. Never use the 40 MHz channels in the 2.4 GHz range.
- Use the 20 MHz and 40 MHz channels within the 5 GHz range. There are over 23 to choose from!

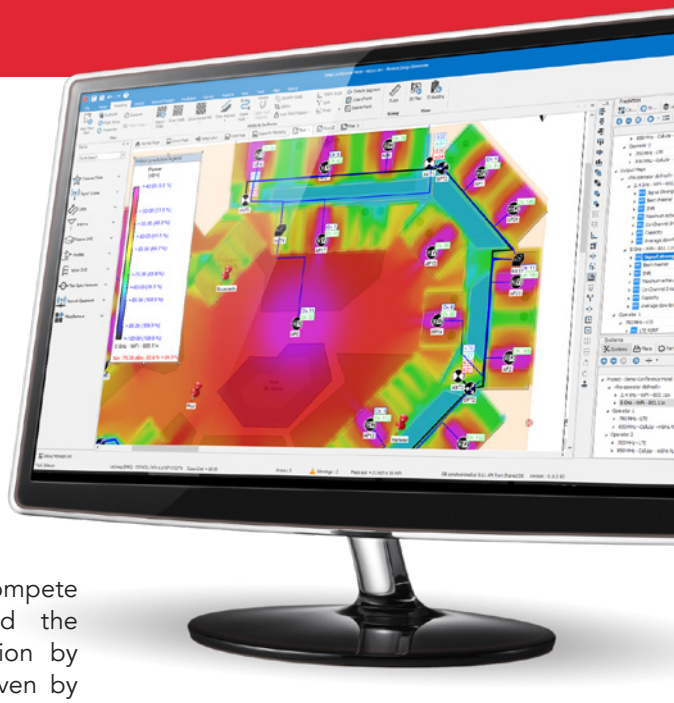
  Did you know? 80 MHz channels are often used but because it occupies a wider range of the spectrum there is no increase in data transfer rates.
- Set the 2.4 GHz and 5 GHz SSIDs as separate networks, giving them similar names (e.g.: Guest_2.4GHz & Guest_5GHz).
- Choose equipment that supports band steering to dynamically allocate channels.
- Include support for DFS (Dynamic Frequency Selection) channels (52-144) in the 5 GHz range.

Want to know more? *http://clients.mikealbano.com* has an extensive list of devices that operate in this spectrum.

Ensure that all AP equipment also supports DFS.

- Implement DHCP (Dynamic Host Configuration Protocol) so that a range of free and working IP addresses are reserved and assigned in order to assure client devices detect and acknowledge connection. Assigned IP addresses that are not renewed return to the pool of available addresses ensuring a continuous supply for devices seeking connection.
- Think in 3-dimensions when designing your warehouse & manufacturing Wi-Fi network. Office spaces are very different from the factory floor and can be tricky places for RF signal propagation. A reliable network designer acknowledges the ABCs of the X, Y and Z axes!
- Use separate channels for APs located on different floors to prevent co-channel interference and avoid impeding network performance.
- Include Wi-Fi network access in elevators and service elevators. This can be accomplished via a shaft-certified cable or using a wireless backhaul.
- Always make good use of monitoring tools to ensure a reliable, seamless experience for connect devices and consumers. Vigilance is key for the proper operation of wired and wireless networks, from the connection to the IP, to server use, backhaul use and reliability, and efficient problem-free RF signal propagation.

Design & Validation with iBwave Wi-Fi®



Using iBwave Wi-Fi® For Warehouse & Manufacturing

Wi-Fi Network Design

We've gone over the issues and obstacles facing any warehouse & manufacturing Wi-Fi network, travelled the halls & open spaces of the multiple venue types and their specific challenges, and touched upon a few of the many best-practices that go into the planning of a successful deployment and operation. This is dense, demanding material, and a rigorous approach to design isn't merely good thinking, it's absolutely essential.

But a warehouse & manufacturing Wi-Fi network can in some ways be seen as organic in nature. It grows, evolves, and must compete against its surroundings and the constant challenge of extinction by obsolescence. In this case driven by the relentless advance of technology. The complex clockwork of what is a functioning, reliable, forward-thinking warehouse & manufacturing Wi-Fi network has countless moving parts – and so ensuring its proper design means a myriad of details come into play, all of them governed by the uncertainties of locale, regulation, architecture, use, traffic and how these might change over the short and long term.

It's not comforting to have to consider that the Wi-Fi network approaches the definition of a classic study in chaos theory. What is comforting is that we've developed our network design software with exactly this in mind; the streamlining & simplification of planning, designing, validating, and deploying superior Wi-Fi networks. That's the sole focus of our iBwave Wi-Fi® software. So, what does that look like in practice?

iBwave Wi-Fi®: Network Design Multitasker

iBwave Wi-Fi® is a 3D Wi-Fi network planning and design software solution. It's hard to think that any high-performance network could be realized without the invaluable assistance of such a tool, determining the right design based on those countless mutable parameters, conditions and limitations discussed in previous chapters.

iBwave Wi-Fi® helps pull it all together; from advanced 3D predictive modeling, radio frequency choice to channel planning, cable routing, AP placement, switches, PoE switches, wireless LAN controllers, and how all of them work together within a defined physical space. It takes a powerful solution to let you explore multiple configurations for optimal RF signal propagation based on network traffic vs. capacity at peak on/off periods, bandwidth consumption estimates, anticipated applications, technology options and allows you to tweak each of those variables ad infinitum and achieve a level of customization and optimization that every ideal warehouse & manufacturing Wi-Fi network should enjoy.

In short, planning with purpose, design that delivers, and validation you can rely upon, every time.

iBwave Wi-Fi®: A Virtual Network Design Sandbox

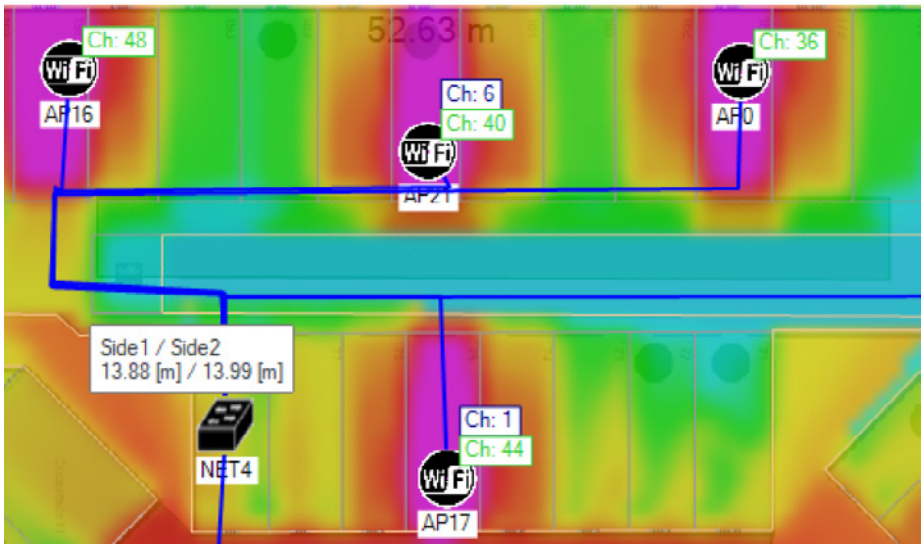
Picture it. The clean slate that is your new warehouse & manufacturing environment – every last architectural detail, materials, exterior and interior areas. That's what iBwave Wi-Fi® does, and it's that environment that becomes the framework upon which iBwave Wi-Fi® plans 3D visualizations of your network's components letting you test each against all the different locales that make up a warehouse & manufacturing space and other network elements, all in real time. Add network infrastructure, APs, cabling, switches and instantly understand RF signal propagation issues and other potential problems.

Let's look at the key features of the software to help you design Wi-Fi within warehouse & manufacturing environments.

In the floor plan simulation above we've added 4 APs; iBwave Wi-Fi® can do this automatically by predetermining their best localization based on estimated highest RF propagation values, or it can be done manually. In the resulting Signal Strength heatmap, the purple areas indicate better propagation areas (-40 to -45dBm) and so a strong, reliable RF signal, while the blue ones point to less desirable propagation areas (-80dBm). iBwave Wi-Fi® software determines probable signal strength according to the size of the area requiring coverage, coverage requirements, selected APs, building material, cable length, anticipated traffic & traffic density patterns, and any other structural and physical restrictions that can serve to help describe the operational environment to iBwave Wi-Fi®.

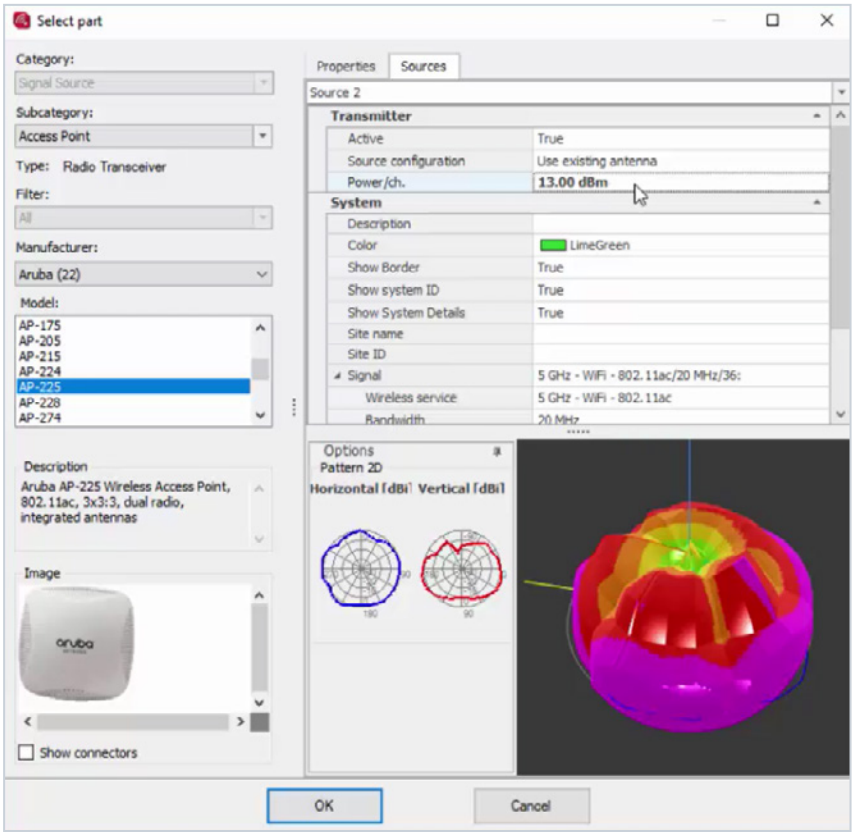
iBwave Wi-Fi® can also automatically calculate channel allocation to ensure that there is no overlap, reducing the risk of co-channel interference. In this example, four of the allocated channels occupy the 20 MHz bandwidth in the 5 GHz spectrum and do not overlap, while channels 1 and 6 operate in the 2.4 GHz range and are also non-overlapping. AP 16 and AP 0 have switched off their 2.4 GHz radios and so are not actively assigning channels in that spectrum, again, to limit RF propagations and prevent channel co-channel interference.

Beyond software, iBwave Wi-Fi® is a guide, mentor, educational tool, and the ultimate warehouse & manufacturing Wi-Fi network planning multitasker.



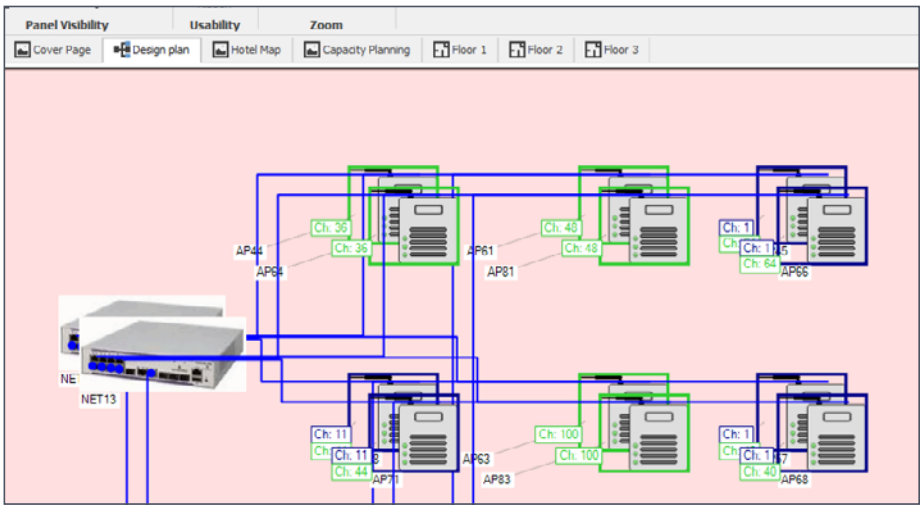
AP Placement Made Simple

This is an example of an individual AP properties window in iBwave Wi-Fi®. It presents the user with clear, detailed AP technical description on the left and lists the manually configurable values in the 2 tabbed panels on the right. Transmission power, dual band support, supported technologies, and the presence of enterprise-level APs give iBwave Wi-Fi® network designers the flexibility and precision required to fine tune efficiency, throughput, and propagation in this dynamic sandbox environment. Here, 2D and 3D antenna patterns are illustrated. Nothing comes closer to the real thing, short of deploying a true physical prototype, testing it, debugging, reinstalling, and testing it again.



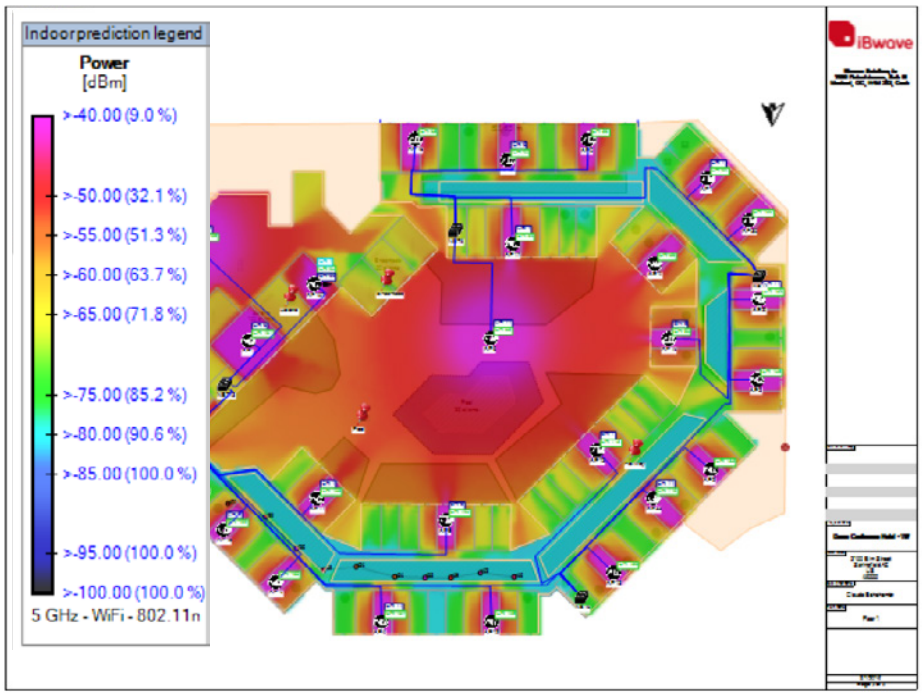
APs From The Ground Up & Inside Out.

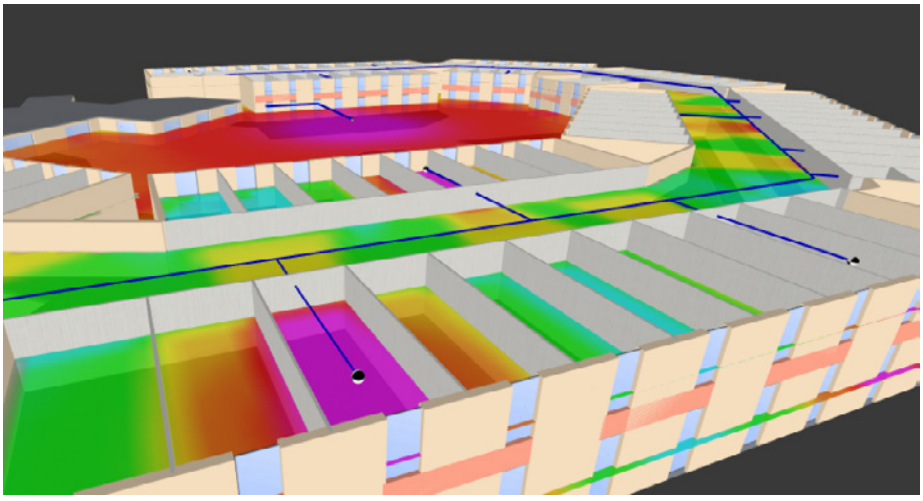
Port planning between PoE and normal switches or APs is also made simpler and more intuitive. At a glance an iBwave Wi-Fi® network designer can determine if sufficient port capacity has been built into the virtual network or if additional switches might be required.



Port Planning For Optimal Capacity

With all of the components in place, or even during the incomplete active design stage, it's a snap to gain an insight into how the network will perform across both the 2.4 GHz and 5 GHz bands. Running individual heatmaps for signal strength, SNR, co-channel interference, among others, and displaying the prediction results gives the user an accurate gauge of network performance once installed. Used before actual construction of the physical space it can even serve to guide architects so that RF signal propagation is actually improved by intentional design decisions. The 3D prediction view can display other important RF signal information such as; best channel, signal-to-noise ratio, maximum achievable data rate, the presence of co-channel interference, client capacity/zone, and average downlink data rate.





3D Predictive Modeling

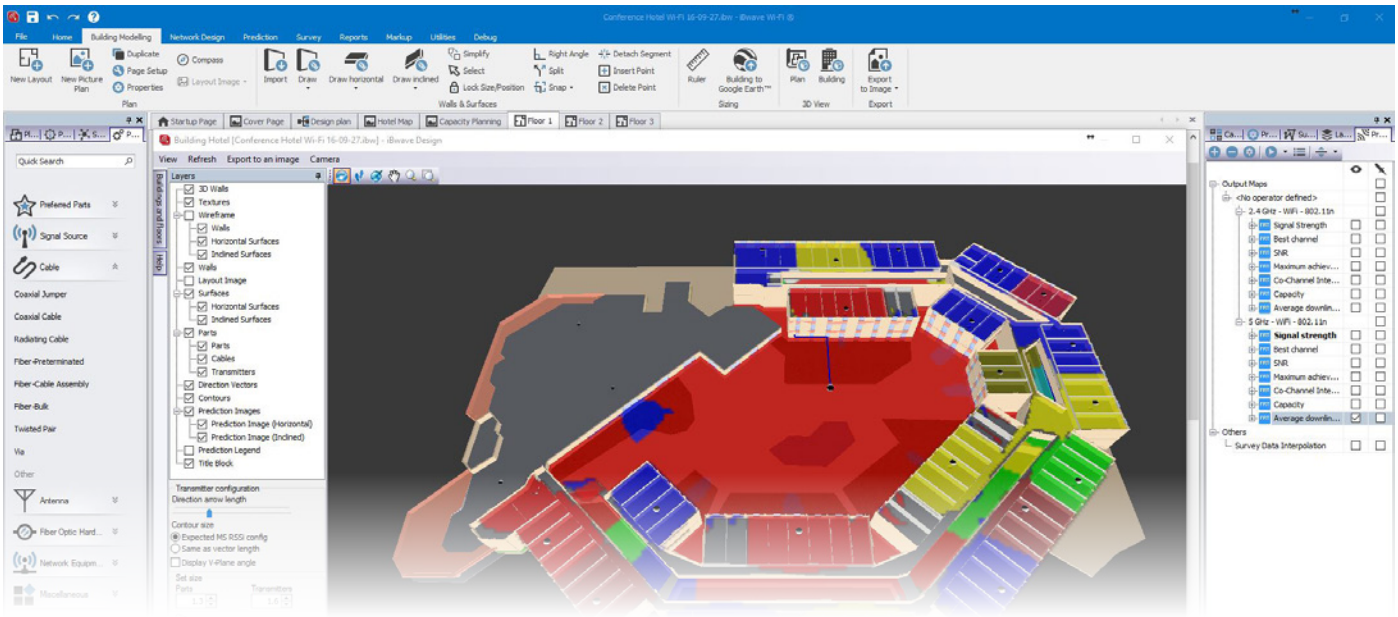
iBwave Wi-Fi®: Validation

Validation is among the most important final steps in the deployment of a warehouse & manufacturing Wi-Fi network, and iBwave Wi-Fi® or its companion, iBwave Wi-Fi® Mobile for Android™, make quick work of it.. While iBwave Wi-Fi®'s network design simulation determines the optimal localization for the server, APs and all related infrastructure, only real-world, real-time testing can offer final validation.

iBwave Wi-Fi®'s interpolation feature allows the user to visualize actual RF signal propagation during a site walk and ascertain channel allocation, signal-to-noise ratio, and signal strength at specific areas where interference due to limitations in floor plan or architectural design in order to evaluate their impact on client reception, and ultimately, user experience.

Active site surveys can also be completed using either iBwave Wi-Fi® or iBwave Wi-Fi® Mobile, which tests network bandwidth between client and multiple server locations in an effort to best compensate for fluctuations in Local-Area and Wide Area Networks (LAN / WAN).

Validation represents the concretization of the physical emplacement of a warehouse & manufacturing Wi-Fi network designed on iBwave Wi-Fi® and ensures that the network is performing as designed. Too often a failure to obtain accurate prediction is the result of insufficient time given to the modelling and design a venue. Subsequent validation of the network can lead to costly redesign and troubleshooting which may delay final activation. With iBwave Wi-Fi®, the accuracy of prediction has been tested over and over again and proven to be incredibly precise – meaning only nominal tweaks or troubleshooting are required once the network is live.



iBwave Wi-Fi® & Other Wi-Fi Services: Playing Nice

iBwave Wi-Fi® focuses primarily on the infrastructure that supports Wi-Fi networks, and so the viability and inter-operability of the myriad of hardware and service options a warehouse & manufacturing client decides to add to that framework are not covered by iBwave Wi-Fi® but fall under the domain of a comprehensive ICT system. Validation of a wireless network's routing, access control lists, firewall settings, AP testing, performance management, assurance, and seamless monitoring & reporting among many others, need to be undertaken separately to assure the network and peripherals together still meet customer requirements.

Any new or upgraded wireless or wired network installation should, as a rule, be subject to a usage-trend analysis as traffic and density patterns are apt to change over time, or as new services, technologies, and device types become available. Moore's Law is the top of the iceberg, technological innovation for new-adopters is usually a generation beyond whatever network you're likely to install, so periodic, systemic evaluation of your networks performance across all its parameters is imperative; once a year at minimum, more often should you feel that technology is outpacing it at more substantial rates. Vigilance, caution, and a firm grasp on the fact that change is imminent no matter how up-to-date you are.

Thanks

We admit it. Any book is as subject to the effects of rapid change in the world it seeks to describe as the technology it hopes to explain. Ours is no different. That applies more today than it did a decade ago, and less so that it will in a year. Warehouse & Manufacturing Wi-Fi Network Best Practices places into context many of those things you'll need to know before you begin planning any Wi-Fi network – indeed, before the first concrete is poured in your new location. What can go wrong, what's known, what's unknown, what's unknowable, and proposes the best ways to address these, and the countless other issues sure to be encountered during the planning, design, and deployment of a network.

We're here to make life, and Wi-Fi networks a little easier. Thanks for taking the time to read Warehouse & Manufacturing Wi-Fi Network Best Practices, and here's to seamless factory and warehouse operation with no signal loss, service interruptions, or production downtime

NOTE: No matter which option you choose for the planning checklist the tear-off version on the next page would probably be useful to users.

ADDENDUM: Handy Tear-Off Planning Checklist

1) What kind of services currently rely on the Wi-Fi network? These can include voice over Wi-Fi, email, internet access, work orders among others.

- Voice Over Wi-Fi? ☐ _____
- Email? ☐ _____
- Internet? ☐ _____
- Work Orders? ☐ _____
- Others? (List beside) ☐ _____

2) What types of applications are currently being used for voice, video and data?

- Voice ☐ _____
- Video ☐ _____
- Data ☐ _____

3) What types of equipment already exists onsite, and does the client have a preferred vendor?

A Equipment type & model: _____
Vendor: _____
Specifications: _____

B Equipment type & model: _____
Vendor: _____
Specifications: _____

C Equipment type & model: _____
Vendor: _____
Specifications: _____

D Equipment type & model: _____
Vendor: _____
Specifications: _____

E Equipment type & model: _____
Vendor: _____
Specifications: _____

Others _____

_____

_____

_____

_____

_____

_____

4) Are there high-density areas within the warehouse that need to be considered?
(e.g.; a production floor with multiple Wi-Fi enabled devices)

Location & Description of High-Density Areas:

_____

_____

_____

_____

_____

5) Are there any other current or projected higher-density areas?
(e.g.; shipping & receiving, back offices, exterior operational spaces)

Location & Description of Other High-Density Areas:

☐ Current / ☐ Projected _____

☐ Current / ☐ Projected _____

☐ Current / ☐ Projected _____

☐ Current / ☐ Projected _____

☐ Current / ☐ Projected _____

6) How many active Wi-Fi devices currently exist in all zones across the network?

Offices _____

Product Plant/Factory _____

Distribution Center _____

Outside _____

Other _____

7) What are the peak on/off hours on the plant floor, back offices and distribution center?
(i.e.; are they uniformly staffed and operational 24/24 & 7/7, or does each have a unique peak hour profile?)

Offices _____

Product Plant/Factory _____

Distribution Center _____

8) What is the total number of active devices the network can presently handle and expects to handle in the future. Do estimated active-device-connections differ widely across different areas such as; shipping & receiving, plant floor, back offices, exterior operational spaces?

Current Device Capacity _____

Projected Device Capacity _____

9) Is the building located in a high-density urban area adjacent to other buildings which may create Wi-Fi bleed?

Location & description of adjacent structures:

_____

_____

_____

_____

_____

_____

_____

10) What are the current and future performance targets for the network as a whole, and subsequently for each network type?

_____

_____

_____

_____

_____

11) What is the total surface area to be covered by the network, including interior and exterior, and multi-level structures?

_____

Interior surface area coverage requirements: (list sites separately)

_____ _____ m2 / _____ ft2

_____ _____ m2 / _____ ft2

_____ _____ m2 / _____ ft2

_____ _____ m2 / _____ ft2

Total: _____ m2 / _____ ft2

Exterior surface area coverage requirements: (list sites separately)

_____ _____ m2 / _____ ft2

_____ _____ m2 / _____ ft2

_____ _____ m2 / _____ ft2

_____ _____ m2 / _____ ft2

Total: _____ m2 / _____ ft2

Total surface area coverage requirements (int./ext.) _____ m2 / _____ ft2

12) Is there an accurate digital or hardcopy floorplan available? Floorplans can be imported into the iBwave Wi-Fi® Design tool to perform crucial predictive RF planning.

☐ Yes ☐ No

Floor plan file types:

_____

_____

_____

13) Can you obtain a list of all incorporated building materials used in the facility? The quantity and location of windows, concrete walls, metal infrastructure, fire-rated doors, and elevators can affect RF signal propagation.

☐ Yes ☐ No

Original contractor and/or architect:

_____

14) Are you subject to local regulations (FCC, CRTC) governing RF propagation, frequency limitations, maximum allowable transmission power and EIRP (Equivalent Isotropically Radiated Power) or other relevant limitations?

Applicable regulations:

_____

_____

_____

_____

15) Will existing backhaul cabling restrict network design including the optimal localization of APs along its backbone?

☐ Yes ☐ No

Original contractor and/or architect:

_____

16) Do you anticipate the need for PoE (Power over Ethernet) capabilities?

☐ Yes ☐ No

17) Is it a requirement that your APs have a look & feel in harmony with the existing architectural design, fit, and finish.

☐ Yes ☐ No

Does the building owner/design approver prefer them to be out of the way and invisible?

☐ Yes ☐ No

Does your installation's propagation profile permit hidden APs?

☐ Yes ☐ No

18) Will exterior APs be required, and if so will they need to be hardened with protection from the elements?

☐ Yes ☐ No

19) Will you install other security requirements such as captive portals, guest access control, and RADIUS ability (Remote Authentication Dial-In User Service)?

☐ Yes ☐ No

Additional security requirement and/or measures:

20) Are you hoping to include a wireless intrusion detection and prevention system?

☐ Yes ☐ No

21) Do you intend to include provisions for the prevention of unlawful signal interception?

☐ Yes ☐ No

Unlawful signal deterrence options:

22) Are you planning to harden your network equipment and infrastructure against present and future vulnerabilities?

☐ Yes ☐ No

23) Will you recommend to your client the hiring of a Security Manager that understands their current and future security needs, compliance with security regulations and their integration into the network while staying abreast of rapidly changing network security technology?

☐ Yes ☐ No

24) What is the optimal segmentation of data and number of logical networks (SSIDs) your setup may need upon launch, and as the demand on the network grows.

Description of data & logical network segmentation:

Projected data & logical network segmentation:

25) Will your network require seamless roaming capacity?

☐ Yes ☐ No

26) Will your network require location-based services or real-time location services such as asset tracking?

☐ Yes ☐ No

27) Have you determined the network's support requirements, including support for legacy devices? Will 24/7 monitoring be needed from on-site IT professionals, or outsourced to on-call service providers?

Description of network support requirements:

Description of legacy device support requirements:

Will 24-hour monitoring be required? ☐ Yes ☐ No ☐ On-site IT ☐ Outsourced IT

28) What is your cutoff for backward compatibility? List compatibility specifications:

29) Will personnel be available to assist during the planning, design, deployment and validation of the new network?

Planning:	☐ Yes	☐ No
Design:	☐ Yes	☐ No
Deployment:	☐ Yes	☐ No

30) Is the network located in an area where intermittent power outages might require that it be equipped with a UPS backup?

☐ Yes ☐ No

31) Which protocols will your network need to support?

☐ IPv4 ☐ IPv6

32) Will you be planning for implantation of full IEEE 802.11-1997 to IEEE802.11ax compatibility?

☐ Yes ☐ No

33) Have you planned for failover ability and redundancies to ensure seamless operation even at peak critical production times where the network is subject to higher stresses?

☐ Yes ☐ No

34) Can you consult with the current network, server, and storage administrators and personnel that have an intimate knowledge of the existing network infrastructure, potential extant issues and its compliance with ISA-95?

☐ Yes ☐ No

35) Do you have access to a site or facility manager who understands the current location's infrastructure and can advise on the placement of APs, power supply, and other equipment that may need to be installed?

☐ Yes ☐ No

36) Has a finance manager or CFO made sufficient allocation of funds available for the design, deployment and continued maintenance of a new Wi-Fi network?

☐ Yes ☐ No

37) Will a project manager be put in place to control & coordinate the successful implementation of the new warehouse & manufacturing network?

☐ Yes ☐ No

38) Have you weighed the pros & cons of leasing versus purchasing a network setup?

Leasing Pros: _____

Leasing Cons: _____

Buying Pros: _____

Buying Cons: _____


iBwave
www.ibwave.com