

# Deploying High-Performance Wi-Fi Networks: 5 Critical Steps

## Introduction

For over 20 years, the Wi-Fi industry has been marketing Wi-Fi on how “easy” it is to deploy. Most IT professionals with a wired networking background have been sold on the concept that Wi-Fi is a “black box” (though physically, typically an off-white box) that you can simply plug into your network anywhere you please, and magically have wireless connectivity for all your users.

While Wi-Fi has been designed to be an ultra-robust protocol, the last 20 years have seen advertised half-duplex speed improvements in the technology from 1-2 Mbps to now  $\gg 1$  Gbps. Furthermore, Wi-Fi was originally offered as a best effort tool of convenience, but its use case has morphed into needing Wi-Fi for performance-critical infrastructure to support real-time applications, such as video streaming and voice calling applications, as well as being the primary source of simple Internet connectivity for an ever-increasing array of wireless client devices.

These improvements in potential Wi-Fi performance were achieved over 20 years by increasing “complexity,” which at its core ultimately means using ever-increasingly

complex mathematics to bend the laws of physics. Increasing complexity, however, comes at the price of increased sensitivity and fragility; the more performance we want to squeeze out of the Wi-Fi, the more sensitive that performance becomes to factors in its environment. This is most notable in terms of interference, which come from several sources:

- **External non-Wi-Fi Interference:** These are the interference effects from unrelated radio networks operating on the unlicensed band, such as microwave ovens, baby monitors, Bluetooth, cordless phones, etc.
- **External Wi-Fi Interference:** The interference effects of neighboring or co-located (but separate) Wi-Fi networks operating on the same frequency bands.
- **Self Interference:** The interference effects of your own neighboring APs on the same network.

When somebody declares that “the Wi-Fi sucks” at a particular location, it almost always comes down to a matter of interference from one or more of these sources.

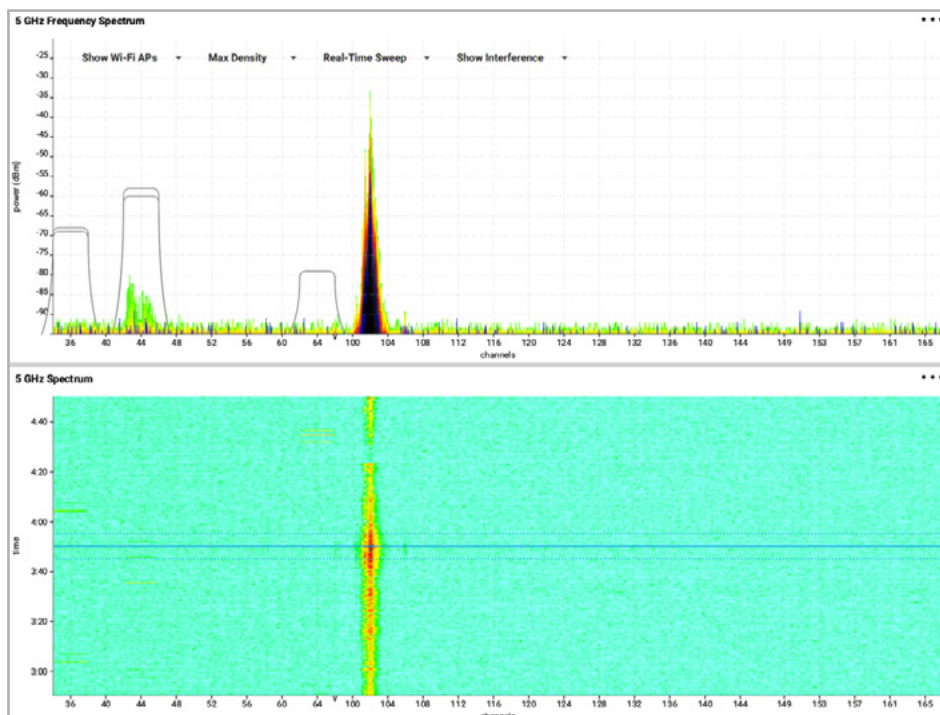


Figure 1: An analog video camera is shown interfering with two Wi-Fi channels.

While every facility is different and thus every Wi-Fi deployment must be uniquely “tuned” to its location, there are general requirements applicable to virtually all types of Wi-Fi networks, as is illustrated below.

Therefore, to achieve good Wi-Fi performance, the Wi-Fi network must be designed to minimize self-interference and to accommodate the effects of external networks. The quality of the IT infrastructure can only ever be as good as its design. Engineers do not build highways by just paving roads and building bridges wherever they feel like it, and architects don't build buildings by just randomly throwing together whatever materials that happen to be lying around.

How, therefore, can we possibly expect our digital wireless infrastructure network (ie Wi-Fi) to just work by random chance?

## Wi-Fi Design as a Formal Process

Design, in any engineering venture, is not a random activity. Rather, design is a well-defined process by which requirements and constraints are gathered, the best options available to meet those requirements and constraints are evaluated and selected, the system is deployed, and the deployed system is measured to ensure it meets the original requirements and is adapted to changes in requirements over time.

For the design of Wi-Fi networks, there are numerous resources available. The Wireless LAN Association (WLA) has recently published a design lifecycle process called the “Standardized WLAN Enterprise Engineering Process,” or “SWEEP.” SWEEP is intended to standardize the design process for Wi-Fi networks and to encourage best practices across the industry, independent of vendor choices or specific applications.

## 5 Steps to Better Wi-Fi

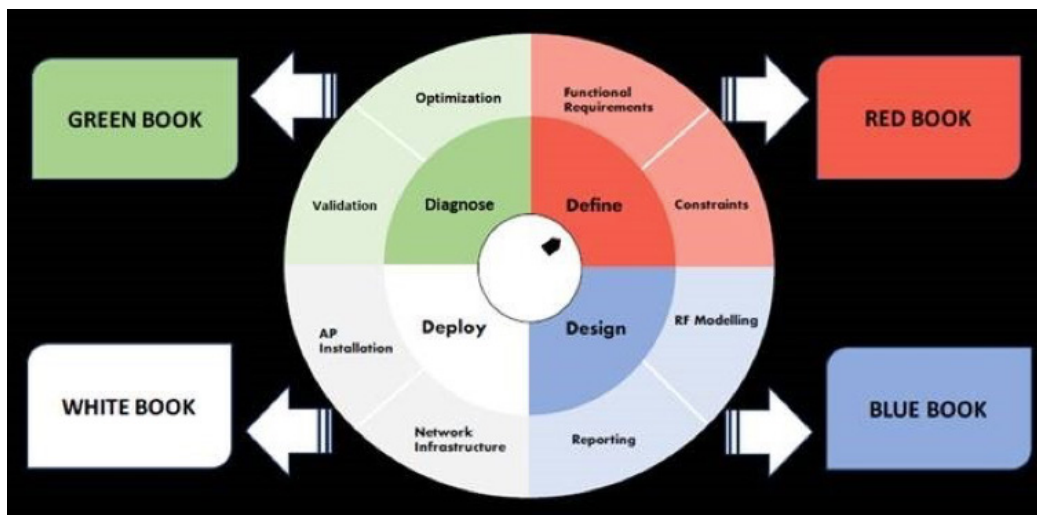


Figure 2: SWEEP design lifecycle process for Wi-Fi networks.<sup>2</sup>

<sup>2</sup> <https://wlanassociation.org/blog/,2/19/2018>

<sup>3</sup> WLA – Transparent Book v1.0. <https://wlanassociation.org/blog/,2/19/2018>

# Define



The define step requires understanding the “what” of the system, which can be understood in two general categories:

- **Functional Requirements: What does the system have to do**
  - **Constraints: What does the system have to work around**
- Available budget
  - Aesthetics
  - Inability to run Ethernet cabling to specific locations
  - Building materials
  - Pre-selection of a particular AP vendor (e.g. all of our deployments utilize “Acme AP”)

Strictly speaking, requirements are both independent of each other and independent of the design choices you select in later steps. Functional requirements should always be phrased as actions (verbs). Some typical functional requirements for a Wi-Fi network may be as follows:

- **Connect smartphones and tablets to the Internet**
- **Provide at least 5 Mbps downstream / 5 Mbps upstream bandwidth to each client device**
- **Cover all pre-defined areas with Wi-Fi signal measured at -67 dBm or stronger**

These requirements are independent of each other and must be satisfied by whatever design solution you develop (e.g. what vendor you select for your APs).

While every facility is different and thus every Wi-Fi deployment must be uniquely “tuned” to its location, there are general requirements applicable to virtually all types of Wi-Fi networks, as is illustrated below.

By contrast, constraints are highly coupled, usually to one or more requirements and often to each other, and will limit your design options. In extreme cases, the constraints will drive the design and may compromise the ability to satisfy one or more requirements. Common constraints encountered in Wi-Fi deployments are as follows:

## Functional Requirement 1: Usage

One of the key requirements in defining a Wi-Fi system is to identify the types of devices that will be using the network, the types of applications to be run on those devices, and the level of security that needs to be provided. Usage is naturally unique to each environment, though tends to cluster around the needs of particular vertical markets. As an example, a hotel will have a different set of users and devices on a nightly basis, but the types of devices brought in (e.g. smartphones, laptops) and the need to separate the network for guests from the network for hotel staff (e.g. maintenance, housekeeping, front desk, etc.) are common across different hotel properties.

When more than one type of network is needed in a facility, which is increasingly common even in small deployments, each wireless service is provided with its own SSID and placed on its own virtual local area network (VLAN), which allows the division of one physical Wi-Fi system into multiple parallel virtual systems that are normally isolated from each other, as illustrated in Figure 3. Generically, most enterprise Wi-Fi environments will have some or all of the following types of network usage requirements.



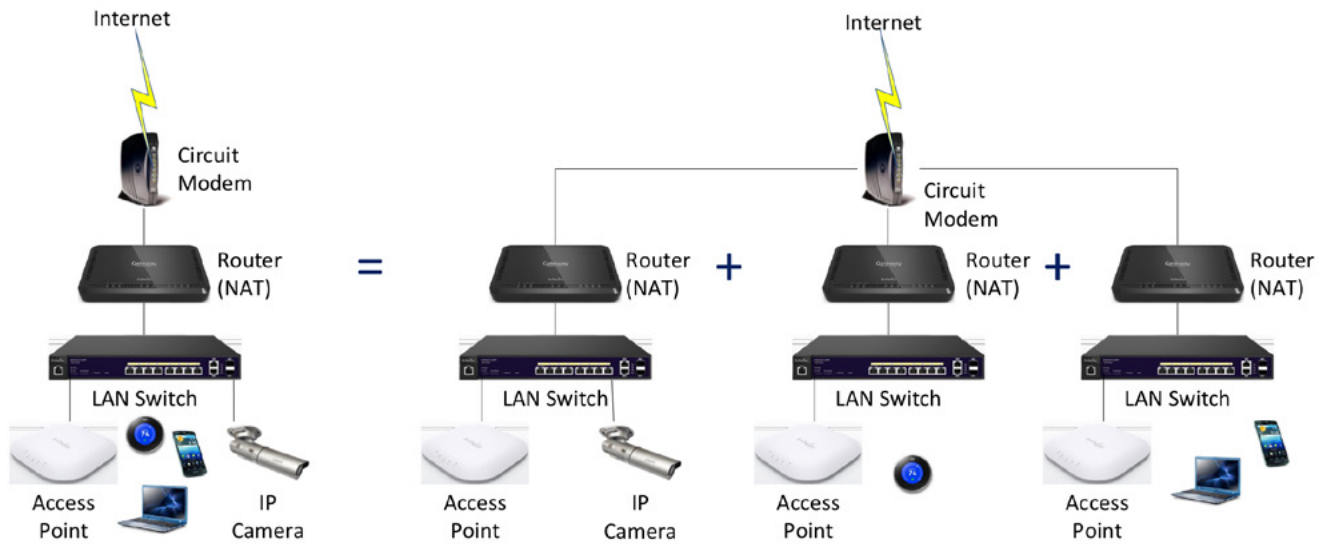


Figure 3: Concept of Virtual Local Area Networks (VLANs). One set of hardware is used to create multiple parallel virtual networks, each with their own unique set of usage requirements.<sup>4</sup>

- **Visitor/Guest Network:** This network is for people visiting the facility on a temporary basis, generally with smartphones, tablets, and/or laptops, and typically require access to the Internet but not access to any other resources on the internal network.
- **Staff Network:** This network is for the staff of the facility, and is intended for devices necessary for operations, which can include tablets, laptops, PCs, and/or dedicated network appliances. This network is typically encrypted to prevent unauthorized access, utilizing either pre-shared key security or access control via a RADIUS or Active Directory Server.
- **Voice Network:** For facilities using Voice over IP and/or Voice over Wi-Fi devices (VoIP or VoWiFi), a dedicated SSID is established with network traffic prioritization. Wireless traffic is usually encrypted with a pre-shared key to facilitate roaming between access points.
- **Security Network:** This network utilizes both appliances (e.g. IP cameras, access control locks, etc.) which may be connected wired or wirelessly, along with monitoring from fixed and/or portable security stations.

Wireless traffic is usually encrypted with a pre-shared key to prevent unauthorized access.

- **Network Appliances:** As IoT becomes more commonplace, enterprises start using appliances for improving operational efficiencies. This network generally contains appliances for lighting and temperature control (e.g. NEST thermostats), along with multimedia and other “smart home” appliances. These appliances may not individually be passing a lot of data, but there could potentially be quite a lot of them on the network, depending on the size of the facility.

## Functional Requirement 2: Coverage

There is a requirement to provide coverage in all of the locations of a facility where Wi-Fi devices and applications are to be used. This requirement may seem straightforward, but is influenced heavily by two types of constraints:

<sup>4</sup> <https://www.imperialnetsolutions.com/portfolio/>

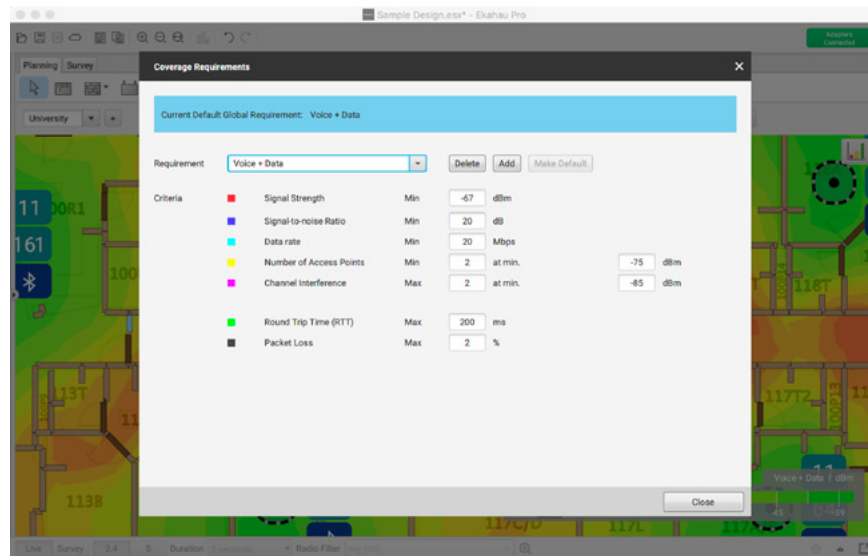


Figure 5: The process of defining coverage requirements in a network design.

- **Physical Constraints:** These are the physical attributes of the facility, including the layout and the (lack of) availability of cabling paths to connect access points. If the facility is new, wiring can often be run inexpensively before the walls are fully erected and sealed. In an existing facility, running new wiring can often be extremely challenging and/or expensive. Even more importantly, however, are the building materials that make up the walls, ceilings, and floors, because radio signals pass much more easily through certain types of materials than others. As an example, open air cubicles, uncoated glass windows, and even drywall are fairly transparent to RF, whereas brick or concrete will highly attenuate Wi-Fi transmissions. There are some materials, like wire-mesh stucco, low-e glass commonly used for outer windows of LEED-certified buildings, and reinforced concrete that serve to block virtually all RF penetration.
- **Logical Constraints:** These are the constraints imposed by owners and operators of the facility. The largest of these is generally budget, though aesthetics, especially in high end properties, can be a major factor. There may also be other radio systems that have to be worked around, such as a legacy or neighboring Wi-Fi or unrelated radio systems using the same frequencies.

## Functional Requirement 3: Capacity

In addition to the types of devices, the number of simultaneous devices and the average and peak traffic loads expected by those devices is a critical factor to designing a Wi-Fi network. In high capacity areas, such as classrooms, conference centers, or stadiums, one AP may be more than sufficient to provide coverage, but multiple APs could be needed to handle the high number and traffic volume of devices.

Accordingly, the area may need to be covered in smaller “cells” in order to handle the quantity of devices and the traffic volume they generate.

Within this capacity requirement is a projection of how capacity needs are going to grow over time. Large enterprise Wi-Fi deployments have a typical expected lifespan of 3-5 years, and smaller enterprise deployments have an expected lifespan of 5-7 years. Meanwhile, the requirements for both bandwidth consumption and quantity of devices tends to more closely follow Moore’s Law (i.e. doubling every 18 months). Accordingly, the network installed today may be perfectly adequate and have margin for today’s need, but will be inadequate in perhaps only 2-3 years.

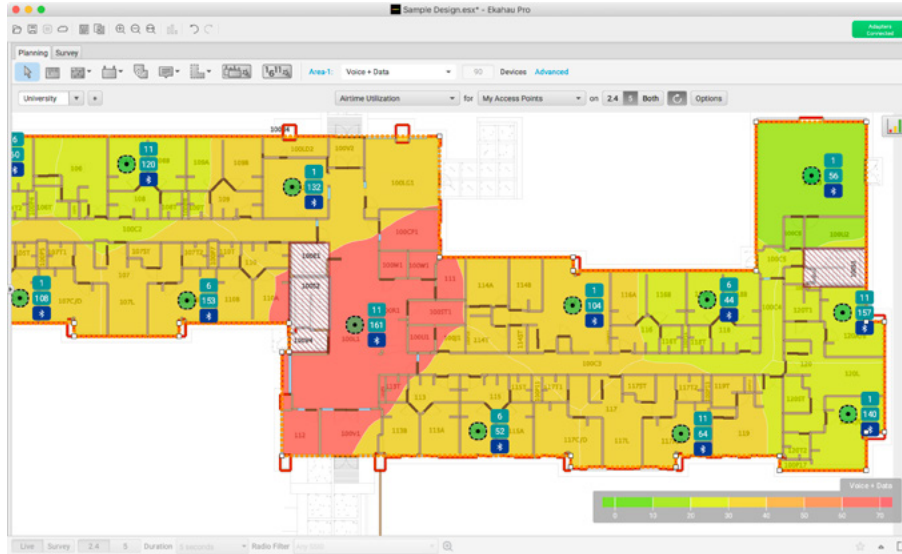


Figure 6: Airtime visualization in this example forecasts the available capacity of a wireless network.

Hence, when selecting components and designing for capacity, it is tomorrow's loosely defined, requirements, not today's, which drive the design.

## Functional Requirement 4: Control

Consideration needs to be made during the requirements definition phase as to how client devices will access the network, and how the network itself will be monitored and managed.

- **Authentication/Association:** A client device is required to establish and maintain a connection to the network.
- **Access Control:** Generally, there is a need to control who (i.e. what devices) are allowed to access the network. When there are multiple VLANs in place, these user types must be distinguished and placed on the appropriate virtual local area network.
- **Security/Encryption:** Many applications require the use of encryption across the wireless link to prevent unauthorized access to data.

- **Roaming:** When devices move from one area of the facility to another, they will eventually lose contact with the original access point. Hence, there are typically requirements for client devices to move around the facility and roam between access points without a noticeable impact on application performance.
- **Monitoring and Maintenance:** Most Wi-Fi systems need to be monitored to ensure that all components are online and functioning properly. In case of failure events, some systems may need automatic processes enabled to attempt to resolve the issue or fail into a reduced, but still functional, state.

When assembling a Wi-Fi design, there are only a few fundamental “knobs” that can be controlled, making up the design parameters.

## Functional Requirement 5: Support & Integration

This category of requirements covers how the APs will be supported and integrated into the rest of the network. Common considerations are as follows:

- Provide power to access points
- Provide data connectivity to access points
- Provide infrastructure to facilitate communication between the access points and the central router, central controller, and/or the Internet
- Provide enclosures to protect access points from physical tampering and/or environmental effects (e.g. harsh temperature or weather conditions)

### Design



Once the requirements and constraints are quantified, an appropriate design solution can be determined. When assembling a Wi-Fi design, there are only a few fundamental “knobs” that can be controlled, making up the design parameters.

### Design Parameter 1: Access Point/Antenna Type

There are multiple access point (AP) vendors providing products with multiple types of capabilities. Many vendors focus their product lines to meet particular types of challenging environments (e.g. stadiums / arenas, K-12 education, etc.), and are optimized and priced accordingly. The most critical, and often most challenging, design decision is the decision of vendor and product line.

While not comprehensive, the following list characterizes the major differences between most product vendors and models.

- **Wi-Fi generation:** The IEEE has extended the original 1997 definition of Wi-Fi numerous times, sometimes with small changes, and other times with entire new product generations. At the time of this writing, 802.11ax (also known as “Wi-Fi 6”) is the newest generation, supplanting 802.11ac (retroactively known as “Wi-Fi 5”) products that were introduced in 2014. 802.11ax AP’s are currently considered to be “cutting edge” or premium hardware, while 802.11ac products still make up the majority of access point and Wi-Fi client device offerings (although this is expected to shift in the next few months). Most 802.11ac (Wi-Fi 5) APs on the market today will likely be 2-3 generations behind in 4-5 years. Newer generations allow for more complex modulation and coding schemes, which enable faster data rates.
- **Frequency band(s):** 802.11n (Wi-Fi 4) allowed the use of both the 2.4 and the 5 GHz frequency bands, and 802.11ac (Wi-Fi 5) worked entirely on the 5 GHz frequency band (though virtually all access points from this generation incorporated 802.11n support in 2.4 GHz). 802.11ax (Wi-Fi 6) on the other hand goes back to supporting both 2.4 and 5 GHz. As a result, virtually all access points will support both 2.4 and 5 GHz. As a result, the current key differentiator is 802.11ac (Wi-Fi 5) versus 802.11ax (Wi-Fi 6).
- **MIMO:** 802.11n (Wi-Fi 4) introduced MIMO (multi-in / multi-out) to allow for parallel data transmissions between multiple transmit and receive antennas. More radios allow for higher throughput, at the expense of power consumption and space. 802.11ac introduced multi-user MIMO (MU-MIMO), allowing the AP to talk to simultaneously communicate with multiple clients in the same environment, for client devices that support the technology. MIMO and MU-MIMO allow for denser utilization of the channel, thus increasing total potential channel capacity and throughput per client device. 802.11ax (Wi-Fi 6) continues to support MIMO and MU-MIMO.



- **External vs. Internal Antennas:** From an aesthetic standpoint, most people don't want to see antennas, so built-in antennas are quite popular. External antennas, however, offer additional flexibility for mounting, along with the ability to add 3rd party antennas with particular profiles for custom applications.

## Design Parameter 2: Locations

This design parameter covers the number and layout of the access points within the facility. While seemingly straightforward, there are many factors to consider. First and foremost, where can APs be placed such that cabling can reach it to provide power and data backhaul.

Aesthetic constraints may also limit where APs can be placed within a facility. Placing APs near, or on, metal objects such as pipes, ductwork, I-beams, etc., can change its coverage profile, as those materials serve to act as antennas and distort the coverage profile. Furthermore, APs with internal antennas are generally designed for a particular orientation (e.g. a horizontal ceiling mount), and thus mounting them differently (e.g. vertically on the wall) will change the coverage profile. Finally, APs that are in line of sight of each other (e.g. APs mounted down a long hallway) are more likely to interfere with each other than if there is a physical structure between the APs (e.g. APs mounted every few rooms on alternate sides of the hallway).

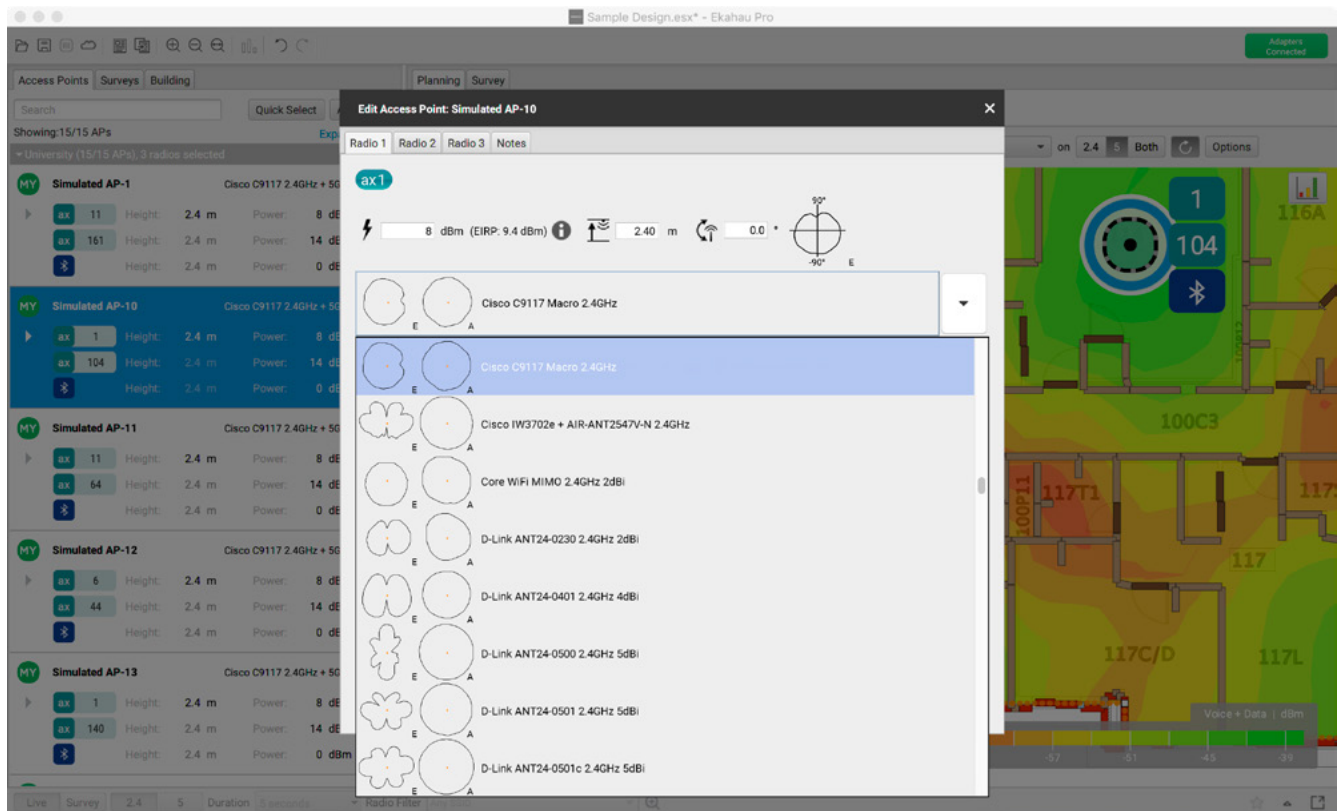


Figure 7: The selection of an antenna to simulate.

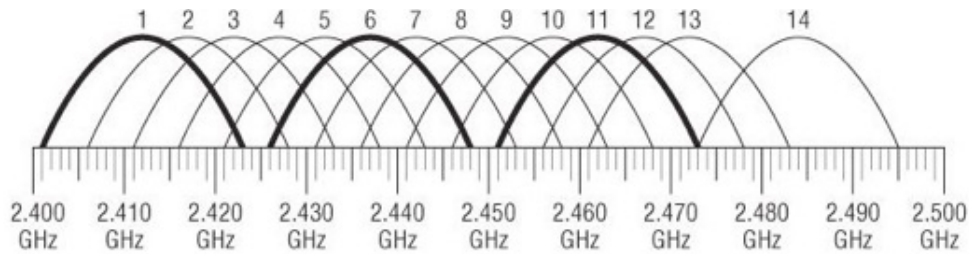


Figure 7: 20 MHz channels on the 2.4 GHz frequency band. <sup>4</sup>

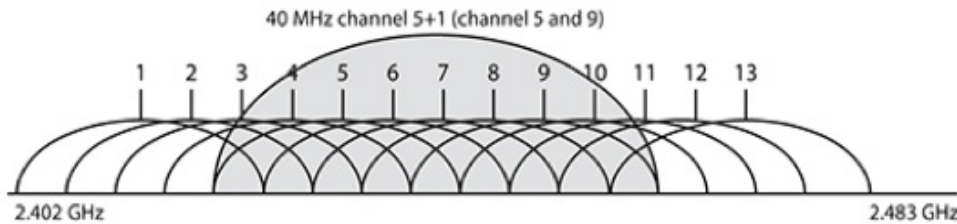


Figure 8: 40 MHz channels on the 2.4 GHz frequency band. <sup>5</sup>

## Design Parameter 3: Channel

Each access point broadcasts a signal on a particular channel, which is specified as a particular center frequency and channel width. On the 2.4 GHz band (802.11b/g/n/ax) in North America, there are 11 channels of 20 MHz size allowed by the FCC. (Channels 12-14 are allowed in some other countries, such as Japan). However, the center frequencies of channels 1-13 are only 5 MHz apart, leading to only three non-overlapping channels, as shown in Figure 7.

The 802.11n spec allows for the optional use of 40 MHz channels on the 2.4 GHz band, by bonding two neighboring channels together. However, given that the entire usable band is only 72 MHz wide, there are no two 40 MHz channel sizes that are independent, as shown in Figure 8. This makes the use of 40 MHz channels impractical in multi-AP deployments, though it is still unfortunately fairly common to see in practice as many vendors allow this channel width in their default settings.

The 5 GHz band is much larger (over 555 MHz, semi-contiguous), and thus makes selecting independent channels and using larger channel widths via bonding neighboring channels much simpler. 802.11a allowed the use of 20 MHz channels. 802.11n allows the use of 40 MHz channels, and 802.11ac (and in turn, 802.11ax) allows the use of up to 80 MHz or 160 MHz channels. This is shown in Figure 9. Note that over 2/3 of the frequency space, however, is also used by legacy military, radar, and weather systems, leading to FCC requirements to detect and move off those channels if such external systems are detected. As a result, much of the UNII-2 and UNII-2e bands are not supported by some consumer devices, leading to only two 80 MHz channels and zero 160 MHz channels.

<sup>4</sup> Coleman, D. and Westcott, D. CWNA Certified Wireless Network Administrator Official Study Guide: Exam CWNA-106. 4th edition. John Wiley & Sons, Inc., Indianapolis, IN. ISBN 978-1-118-89370-8. Copyright 2014.

<sup>5</sup> Coleman, D. and Westcott, D. CWNA Certified Wireless Network Administrator Official Study Guide: Exam CWNA-106. 4th edition. John Wiley & Sons, Inc., Indianapolis, IN. ISBN 978-1-118-89370-8. Copyright 2014.

5 GHz Channel Allocations																									
Frequency (GHz)	5.150				5.250				5.470				5.600				5.640		5.725				5.850		
	UNII-1				UNII-2a				UNII-2c (Extended)												UNII-3				
Center Frequency	5180	5200	5220	5240	5260	5280	5300	5320	5500	5520	5540	5560	5580	5600	5620	5640	5660	5680	5700	5720	5745	5765	5785	5805	5825
20 MHz	36	40	44	48	52	56	60	64	100	104	108	112	116	120	124	128	132	136	140	144	149	153	157	161	165
40 MHz	38		46		54		62		102		110		118		126		134		142		151		159		
80 MHz	42				58				106				122				138				155				
160 MHz	50								114																
FCC	1,000 mW Tx Power Indoor & Outdoor No DFS needed				250 mw w/6dBi Indoor & Outdoor DFS Required				250mw w/6dBi Indoor & Outdoor DFS Required 144 Now Allowed				120, 124, 128 Devices Now Allowed								1,000 mW EIRP Indoor & Outdoor No DFS needed 165 was ISM, now UNII-3				
DFS Channels					DFS Channels																				

Source: Wireless LAN Professionals

Source: Wireless LAN Professionals

Figure 9: Channels on the 5 GHz frequency band.<sup>6</sup>

## Design Parameter 4: Transmit Power

Transmit power of a radio is proportional to its effective range – the higher the transmit power the more distance that a signal can travel, and/or the more physical materials that it can penetrate, and still be resolved at the receiver. Additionally, a stronger signal at a given distance generally results in a higher signal to noise ratio, allowing for more complex modulation and coding schemes and thus faster data speeds.

In early Wi-Fi deployments, which were primarily driven by the functional requirement for coverage, it was common to turn up the power on the AP transmitter as high as is allowed by FCC and IEEE regulations. This approach was sufficient when most clients had reasonably strong transmitters themselves, such as laptops.

With the emergence of smartphones, tablets, and network appliances, however, there is often a transmit power mismatch that leads to a range mismatch. Most smartphone, tablet, and appliances use relatively weak transmitters in order to

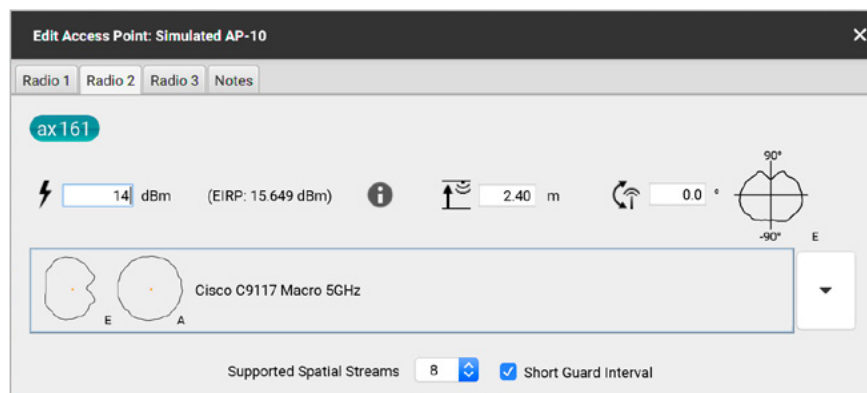


Figure 10: The process of configuring simulated access point transmit power.

<sup>6</sup> Source: Wireless LAN Professionals, [www.wlanpros.com](http://www.wlanpros.com)

preserve both space and battery life. As a result, the situation develops where the client device can receive the relatively strong transmissions of the access point, but the access point cannot receive the relatively weak transmissions of the client device in response. Accordingly, though non-intuitively, the effective coverage area is driven more by the client devices, and the AP power levels should be set to better match the limitations of the clients.

Finally, as compared to 5 GHz, 2.4 GHz has less free space path loss and attenuation through standard building materials, giving it a larger effective range at a given transmit power level. When using a dual band access point, one generally wants to have the coverage area equivalent for both bands. This generally leads to a 4-6 dB difference in power levels on the 2.4 GHz band as compared to the 5 GHz band. In high density environments, it is not unusual to install a denser deployment of APs and then disable the 2.4 GHz band on some of them.

## Design Parameter 5: Network Management System

Wi-Fi network activities need to be controlled, coordinated, and monitored. Some access point vendors use access point controllers with relatively “thin client” APs, so that the intelligence of the network is coordinated by a central appliance. Other vendors use standalone APs (i.e. “thick client” APs) where the APs coordinate directly amongst themselves, using a network management system (NMS) to collect usage statistics and log data. There are three types of AP controller architectures that are commonly implemented:

- **Central Architecture:** In this architecture, all of the intelligence of the network is at the AP controller appliance on the network, and all traffic from the access point is tunneled to the AP controller before being routed to the appropriate destination. As Wi-Fi speeds have increased, the AP controller can become the bottleneck for performance, so this approach is generally no longer used.

When requirements are being gathered and design solutions are being evaluated, it is very typical to do one or more types of site surveys.

- **Distributed Architecture:** In this architecture, all of the intelligence of the network is at the APs themselves, and an AP controller may not even be installed on the network, or if it is, only serves to collect usage statistics and coordinate AP configuration and firmware upgrades. This approach can prove problematic in more complex environments, due to the difficulties in coordinating operational functions across APs, such as client device roaming.
- **Split Architecture:** In this architecture, the intelligence of the network is split between the AP controller and the individual APs. The implementation of this varies by vendor, though typically all data handling functions would be handled by the AP, while management and control functions are handled by the AP controller.

It is also common for wireless networks to be monitored and managed remotely from a remote location, such as a centralized network operations center (NOC). Many vendors have also introduced “cloud controllers,” which are AP controllers that are located on a hosted server on the Internet, managing multiple individual network locations, each consisting of multiple APs.



## Design Parameter 6: Wired Network

Fundamentally, an access point is a device that allows one or more wireless client devices to connect to a wired network. The wired network supporting the wireless access points is, in and of itself, a complex system that requires many components, such as cabling, switches, routers, and modems. The application, coverage, capacity, and control functional requirements drive the need to provide a low-voltage cabling and switch infrastructure that meets these requirements and does not itself become a bottleneck in communications.

### Deploy



When requirements are being gathered and design solutions are being evaluated, it is very typical to do one or more types of site surveys. Depending on the project size and scope, funding may not be available on a project to do all of these steps, though performing these surveys are highly recommended, as they can prove invaluable in validating and tuning the network design before and/or during installation.

There are generally three types of site surveys that can be performed with specialized software, such as Ekahau. These surveys all generally require accurate floor plans (to scale), and most of them require site access to take measurements.

**Predictive modeling:** This involves building a mathematical model of the facility, using a software package such as Ekahau Pro shown in Figure 11. The floor plans are loaded in, and the building materials of the walls are specified so as to account for their attenuation characteristics. If CAD drawings are available, Ekahau Pro can automatically draw in the walls, though if not, walls can also be placed manually.

Once the walls and their characteristics are defined, access points are placed to see how the signal will propagate and self-interfere.

Ekahau Pro has a library of the antenna patterns for most common AP vendors and models. APs can be moved around in the model, and their channel and transmit power settings varied, to evaluate how those changes impact the coverage and interference characteristics. These models are fairly straightforward and inexpensive to generate and do not require a site visit, making them fairly easy to perform.

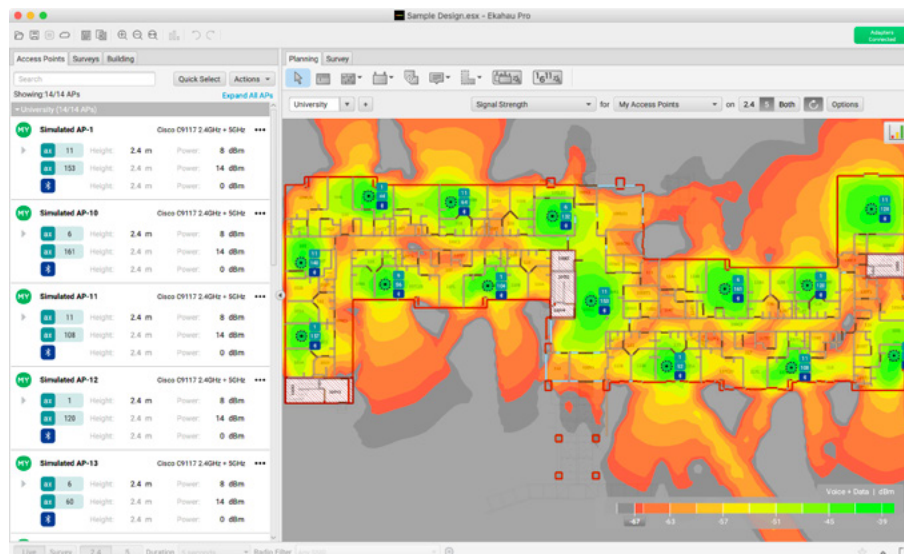


Figure 11: A predictive model of a wireless network in Ekahau Pro.

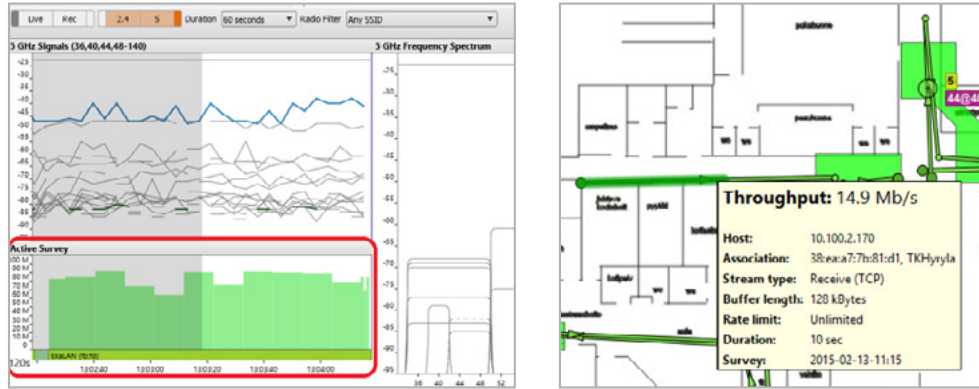


Figure 12: Ekahau Pro showing active and passive survey data.

**Pre-deployment or “AP on a Stick” Survey:** This is an on-site survey. If there is no existing Wi-Fi, an AP is temporarily positioned in the environment, and measurements of the room and surrounding rooms are taken to measure actual signal coverage in the environment.

The results can be used to refine the predictive model by measuring actual attenuation characteristics of the walls. This type of survey can also be used to find third party Wi-Fi and non-Wi-Fi devices in the area, so that their presence can be accommodated in the design. Tools like Ekahau Pro are specifically designed for these types of measurements, though keep in mind it is only a

snapshot in time. Thus, the survey may not be accurate if construction changes are made to the facility or if new neighboring Wi-Fi or other RF systems are installed after the survey is done.

**Post-deployment Survey:** This survey is performed after the network is installed and operational. This is typically performed immediately after network installation to validate that requirements are being satisfied, as well as later on as a diagnostic tool in case of future performance issues. Mechanically, this works very similarly to a pre-deployment site survey, in that the surveyor is walking around the facility with a tool like Ekahau Pro and marks their position on the floor plan, so as to build up

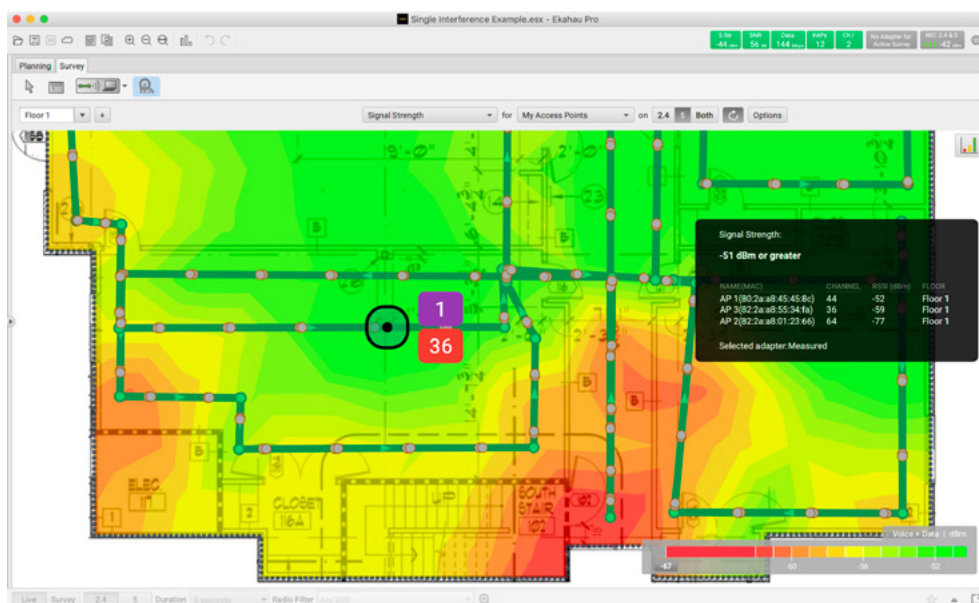


Figure 13: Review of results from a post-deployment site survey in Ekahau Pro.

a complete picture of Wi-Fi performance throughout the facility. Again, keep in mind that this measurement is a snapshot in time, and thus may not reflect performance at a future time.

## Survey Hardware

In order to perform a site survey, a device that can perform Wi-Fi measurements is required. Traditionally, off-the-shelf USB Wi-Fi adapters were used. Today, they've been largely replaced by standardized, purpose-built site survey hardware.

## USB Wi-Fi Adapters

While USB Wi-Fi adapters are inexpensive, they have major drawbacks for performing site surveys. First, USB Wi-Fi adapters are not calibrated, so they each see Wi-Fi signal strength differently than other, seemingly identical adapters.

USB Wi-Fi adapters will also interpret signal strength differently depending on how they are oriented. For example, a USB adapter that is oriented horizontally will report a different signal strength than an adapter that is oriented vertically. There is no standardized orientation for USB adapters, so it isn't possible to orient them correctly.

Finally, many modern operating systems do not support USB adapters. iOS (the operating system for iPhone and iPad) and macOS (the operating

system for Apple laptops and desktops) simply do not have systems in place to support USB Wi-Fi adapters, so they can't be used to survey from these systems. USB Wi-Fi adapters also draw power from the laptop they are connected to, shorting the laptop's battery life.

## Ekahau Sidekick™

The Ekahau Sidekick™ is a standardized measurement device that is specifically designed to perform Wi-Fi site surveys. It features enterprise-grade Wi-Fi radios, but unlike USB Wi-Fi adapters, they don't rely on USB Wi-Fi adapter support from the host operating system, so the Ekahau Sidekick™ can be used with laptops running Windows and macOS, as well as iPad (which runs iOS).

The Ekahau Sidekick™ uses 7 antennas, providing it with extremely consistent signal strength measurements, no matter which direction the survey technician is facing. This is in stark contrast to the nature of USB Wi-Fi adapters, which exhibit varying receive sensitivity, depending on how they are oriented, and the direction of the technician. The Ekahau Sidekick™ also provides its own power via a built-in battery. The battery provides continuous power to the Ekahau Sidekick™ for over 8 hours.

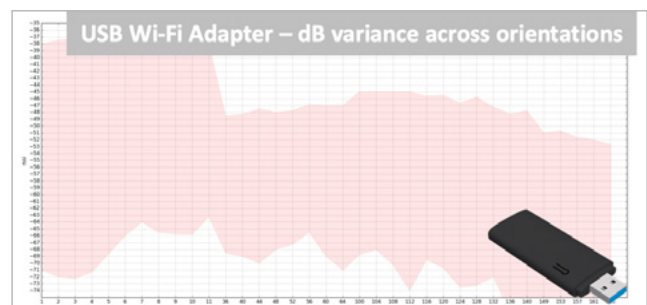
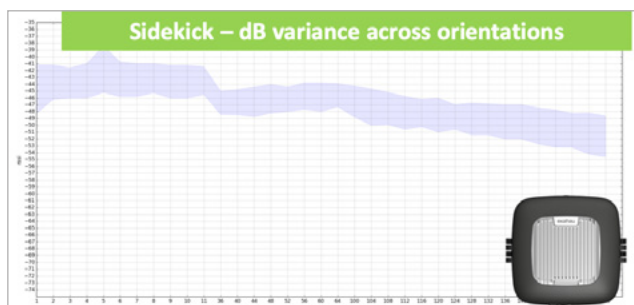


Figure 14: This comparison graph shows signal variance in the Ekahau Sidekick and a USB Wi-Fi adapter. While the Ekahau Sidekick shows very little variance, the USB Wi-Fi adapter shows a high variance in received signal strength, which depends on the angle it is held.



## Optimize



Most of us are not just in the business of designing and deploying networks, but also in maintaining those networks. MSPs (managed services providers) make money by having customers pay support contracts, but these are only profitable if the network is working and customers aren't actually pestering you for support issues. A good quality design can help avoid many support problems. Nonetheless, even with a good quality design, networks occasionally need maintenance and tuning, especially as new client devices get added over time, or changes are made to the existing Wi-Fi network (e.g. new coverage areas, AP model upgrades, etc.).

One of the key challenges in Wi-Fi is that there is a perpetual stream of new client devices being added to the network, but the Wi-Fi network itself is essentially static once it is deployed. Thus, the expectations for the Wi-Fi network (i.e. the functional requirements) are changing over time while the network itself (i.e. the design parameters) are fixed.

To accommodate this, some level of margin / overcapacity needs to be designed in, as this excess

capacity will, in most cases, get consumed over time. When there are issues on the network, the site survey tools such as Ekahau Pro and the Ekahau Sidekick™ can be used to re-perform an onsite survey. If prior surveys exist, these measurements can be invaluable in determining whether anything has changed in the environment. Measurements such as interference and signal strength can be compared to determine what has changed in the environment since the last survey was completed.

## Maintain



### Troubleshooting

Like just about any system or construct, wireless networks require maintenance to continue functioning as designed. For example, since both the 2.4 and 5 GHz frequency bands are "unlicensed spectrum", they're open for use from all kinds of wireless devices, Wi-Fi and otherwise. As a result, non-Wi-Fi interference can disrupt a wireless network, often with no warning. Most disruptions to a wireless network are due to interference and are of the non-malicious sort. A typical scenario is that where an unknowing office worker brings a new wireless headset to work, or a building maintenance manager installs an inexpensive analog wireless video camera.



In both of these cases, the office worker or maintenance personnel have no idea that they're introducing interference, but wireless network administrators know as soon as users begin to complain about slow and unreliable Wi-Fi.

Since good wireless networks are always designed to work in the context of a specific building, changes to a floorplan can negatively impact the performance of a wireless network and must be addressed. Both adding new walls to a floorplan or removing existing walls to enlarge rooms significantly alters how radio frequency (e.g. Wi-Fi) propagates through the structure. When floor plans are changed, the wireless design must be altered to address the changes. In many cases, some buildings are modified without the wireless network administrator's awareness, leaving wireless teams to fix problems after new construction has already been completed. Additionally, the needs of wireless networks are ever-changing and must be addressed. Users continue to demand more throughput, more speed, and room for more devices on wireless networks. As discussed in the design section, wireless networks should be designed to accommodate a specific number of devices with a certain amount of required throughput, per device.

Invariably, more devices will be added to the network, and applications will require more bandwidth to continue functioning. As the requirements of the wireless network change, it will have to be continuously monitored, updated, and in some cases, redesigned to accommodate the additional demands.

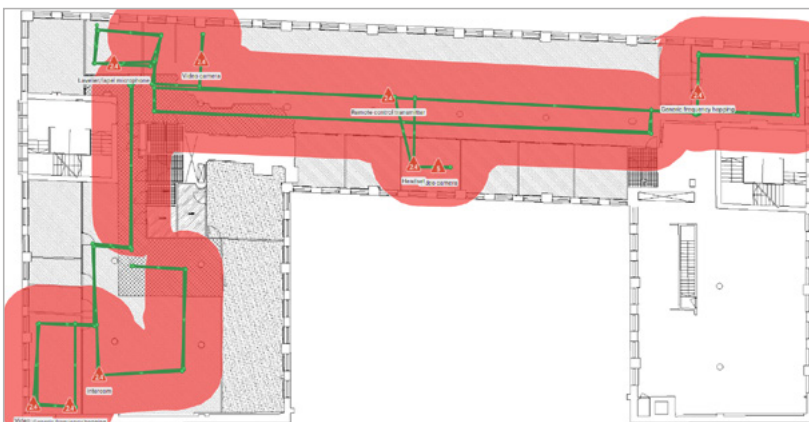
Whether a wireless network engineer is dealing with non-Wi-Fi interference, interference from new neighboring wireless networks, changes to the physical layout of the building, or increased demands on the network, wireless networks require troubleshooting and regular and ongoing maintenance.

## Regular Reporting

Part of maintaining a fast and reliable wireless network is keeping detailed snapshots of network status. For example, when Wi-Fi is deployed in a building, the wireless landscape in the building might be a very quiet and optimal environment to deploy in. There might be few neighbors, few wireless devices, and very little traffic in the spectrum to compete with.

Months later, the environment could have changed significantly. There could be a new organization on the floor above, and they could have added their own access points, client devices, and traffic. They may have even added their own non-Wi-Fi devices, including cordless phones and wireless video cameras.

This leaves a remote wireless expert in the dark. Having no visibility into what has changed in the environment leaves the wireless expert with no explanation of why the once-functioning network is now slow and unreliable. If the expert had snapshots of data, they could form a report of why the network isn't functioning, and create a plan to remediate the problem.



*Figure 15: This example shows sources of non-Wi-Fi interference in Ekahau Pro, which are automatically detected and classified during a site survey with Ekahau Sidekick.*



## Getting Site Survey Data

Gaining snapshots of the current status of a network involves performing a site survey with Ekahau Sidekick™. In the past, the only way to perform a site survey was to send a wireless expert to the site, and perform a walkthrough survey of the environment to collect the data. This was a difficult task, as most organizations only kept one or two wireless experts on staff, so the resources were not available to achieve regular, normal surveys.

With the advent of Ekahau Connect, surveys can now be performed by a technician equipped with an Apple iPad, an Ekahau Sidekick, and Ekahau Connect. The technician can perform a site survey with the easy-to-use Ekahau Survey for iPad, and then synchronize the results of the survey to Ekahau Cloud.

A senior network engineer could then access the results of the survey from the cloud, and perform in-depth analysis and reporting on the survey from his or her office.



## Reporting

Once the site survey has been collected and automatically synchronized to Ekahau Cloud, it can then be synchronized down to Ekahau Pro for in-depth analysis on a Mac or PC. Using these key visualizations, a network expert can quickly determine what the problem at the remote location is.

## Network Health

This simple visualization shows whether the network is meeting requirements or not. It is an excellent way to quickly spot problem areas on a wireless network.

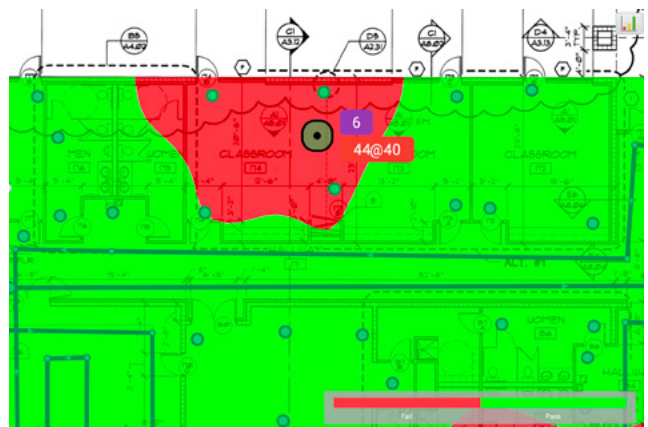


Figure 16: The Network Health visualization in Ekahau Pro shows an area that is failing to meet network requirements. This is an excellent way to quickly spot problem areas on a wireless network.

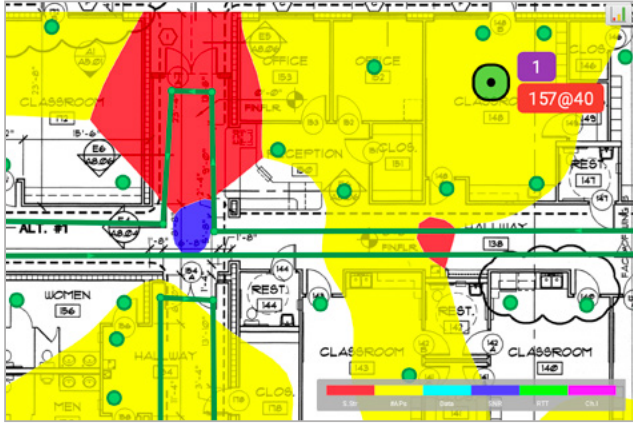


Figure 17: The Network Issues visualization in Ekahau Pro shows several failures in network requirements, including Signal Strength (red), number of access points (yellow), and signal-to-noise ratio (blue).

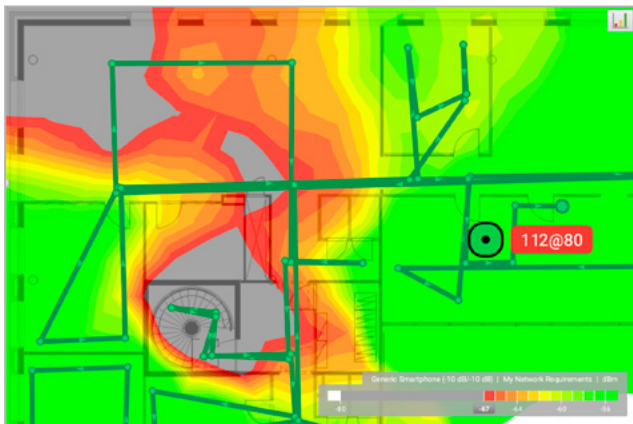


Figure 18: The Signal Strength visualization in Ekahau Pro shows several areas that have poor signal strength.

## Signal Strength

Representing the classic “heatmap” is the Signal Strength visualization. This visualization is instrumental in showing where signal strength requirements are met, and where they do not.

Signal strength can be affected by a number of changes to the physical environment, including changes to the physical environment, including changes to objects in the building (large furniture, warehouse inventory) and changes to the building itself.

## Channel Interference

Given the half-duplex nature of Wi-Fi, knowing how many access points are sharing the same channel is extremely important. Seeing channel interference can help a Wi-Fi expert understand how many access points are having to take turns, including access points that are part of neighboring networks. A network that had virtually no channel interference when it was deployed could suddenly become plagued by it when a neighbor installs their own wireless network.

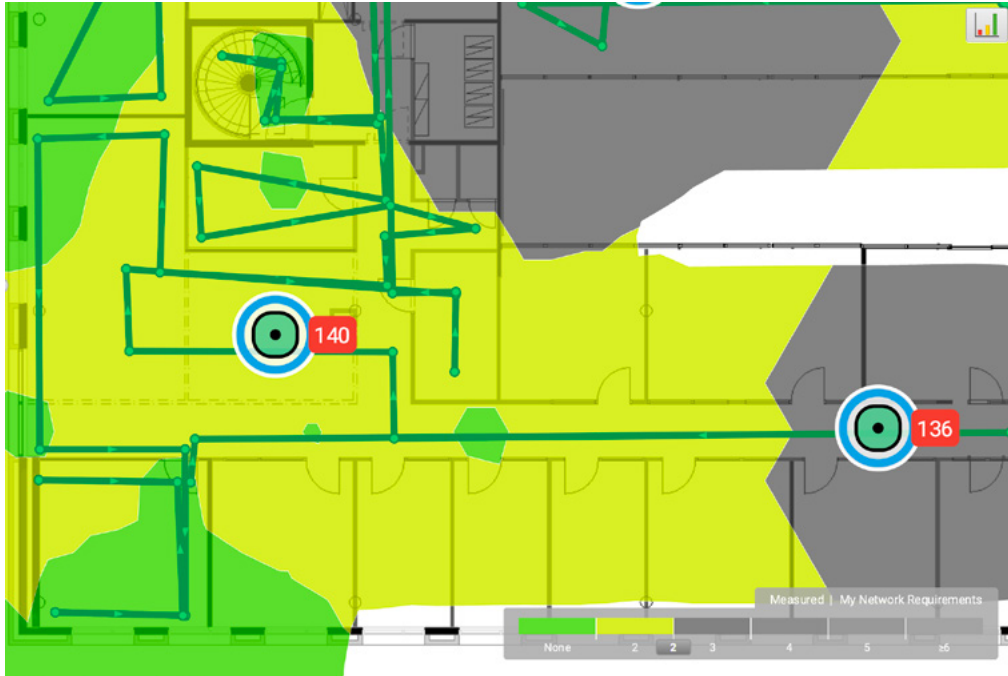


Figure 19: The Channel Interference visualization in Ekahau Pro shows the grey areas where three or more access points share the same channel (and thus take turns transmitting).

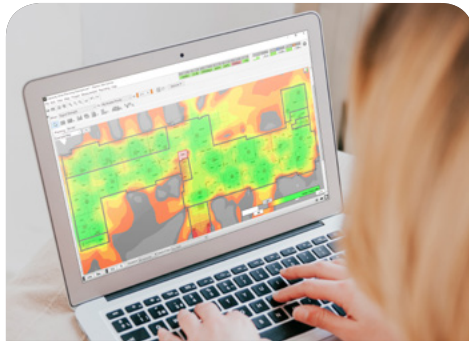
## Conclusion

The design of a high-performance Wi-Fi network is a complex engineering task subject to ever-increasing demands on its requirements and constraints. As such, design processes and measurement tools are necessary to identify and validate best practices in Wi-Fi design,

and to troubleshoot problems in existing deployments, and thus maximize the performance of the network. Using these tools, high quality Wi-Fi designs can be generated and deployed to maximize the customer's expectations for performance.

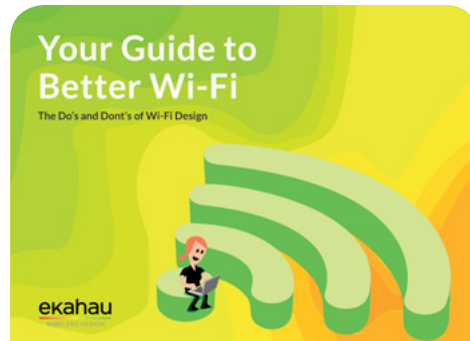


# Additional Resources



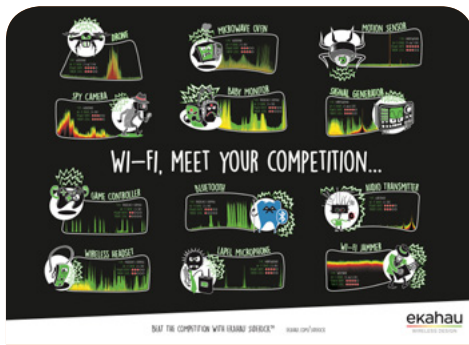
Guide

A Beginner's Guide  
to Wireless Tools



eBook

Your Guide to Better Wi-Fi: The  
Do's and Don'ts of Wi-Fi Design



Infographic

Wi-Fi: Meet Your Competition






Case Study

Healthcare Provider Improves  
Wireless Network

# Ekahau Can Help

Ekahau Connect™ is a suite of Wi-Fi tools that enable you and your team to design, optimize and troubleshoot any Wi-Fi network faster and easier than ever before.

-  Design reliable, high capacity Wi-Fi networks
-  Validate a new Wi-Fi deployment or optimize an existing Wi-Fi network
-  Analyze and troubleshoot Wi-Fi issues in real-time

Learn more about how Ekahau can help you design, validate, analyze, report and troubleshoot Wi-Fi networks:

Learn more

iPad is a trademark of Apple Inc.

## Ekahau Connect™

The All-in-One Product Suite  
for Better Wi-Fi

**Ekahau Pro™** - the industry standard tool for designing, analyzing, optimizing and troubleshooting Wi-Fi networks

**Ekahau Sidekick®** - precise Wi-Fi diagnostic and measurement device used by professionals for site surveys, spectrum analysis and packet capture

**Ekahau Survey™** - first ever professional Wi-Fi site survey and analysis tool for iPad

\*Requires Ekahau Sidekick, Ekahau Pro and Ekahau Cloud

**Ekahau Capture™** - easy to use packet capture tool helps anyone detect complex problems without waiting for a Wi-Fi expert

\*Requires Ekahau Sidekick

**Ekahau Cloud™** - choose a collaboration method that works best for you - cloud or local



# What Can Ekahau Do for Your Organization?

**35%** of Fortune 500 companies run their networks with Ekahau Wi-Fi planning and measurements solutions.



We are recognized for delivering the easiest-to-use, most reliable solutions for Wi-Fi planning, site surveys, troubleshooting and optimization.



Our solutions minimize network deployment time and ensure sufficient wireless coverage – across all industries, project sizes, building infrastructures and level of complexity.



Our enterprise tools are ideal for wireless professionals designing and deploying small to large Wi-Fi networks and troubleshooting Wi-Fi issues.

**Schedule a demo  
today to see the  
complete Ekahau  
Wi-Fi toolkit  
in action.**



**Schedule a demo**

## About Ekahau

Ekahau is the global leader in solutions for enterprise wireless network design and troubleshooting. More than 15,000 customers, including 35% of Fortune 500 companies, run their networks with Ekahau's Wi-Fi planning and measurement solutions. Our software and hardware solutions design and manage superior wireless networks by minimizing network deployment time and ensuring sufficient wireless coverage across all industries, project sizes, building infrastructures and levels of complexity. We are recognized for delivering the easiest-to-use, most reliable solutions for Wi-Fi planning, site surveys, troubleshooting and optimization. Whether a corporate office, hotel, hospital or university – if the Wi-Fi works well, it has likely been built using Ekahau's Wi-Fi Design solutions.

Ekahau is headquartered in Reston, Virginia and has much of its R&D and product related functions in Helsinki, Finland.

### Ekahau Headquarters

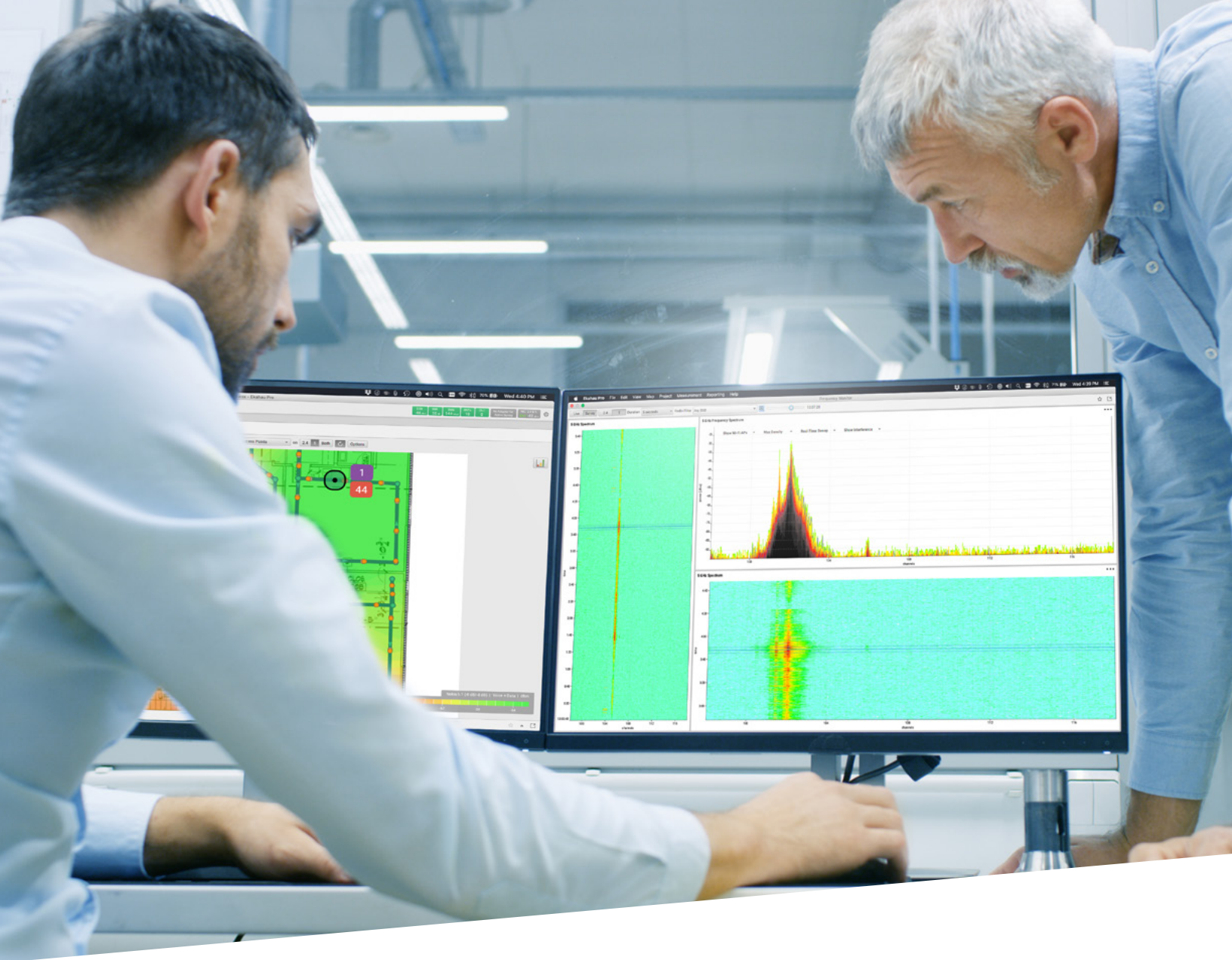
1925 Isaac Newton Square E.  
Suite 200  
Reston, VA 20190  
Tel: 1-866-435-2428  
Americas: [salesamericas@ekahau.com](mailto:salesamericas@ekahau.com)

### Ekahau Europe

Jaakonkatu 5  
00100 Helsinki, Finland  
Tel: +358-20-743 5910  
EMEA/APAC: [sales@ekahau.com](mailto:sales@ekahau.com)







Find out more

[www.ekahau.com](http://www.ekahau.com)

**ekahau**  
WIRELESS DESIGN