ekahau

Wi-Fi Performance and Security PLAYBOOK

28 Pages of Wi-Fi Best Practices

THE Wi-Fi LIFECYCLE

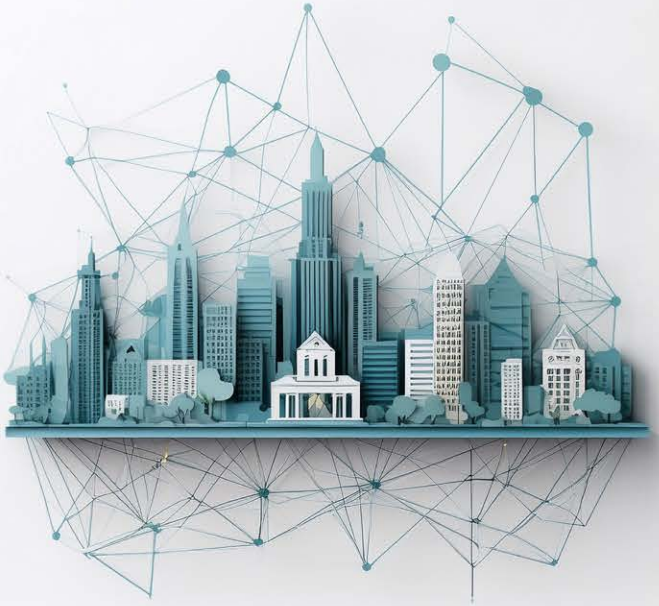
Maximizing Your Wi-Fi Investment ROI

NETWORK SECURITY

Reducing Your Exposure to Hacking Risks

TIME TO REDESIGN?

Assessing Your Aging Infrastructure



Executive Summary

The path to maintaining a strong Wi-Fi network is filled with evolving challenges. Requirements change, usage patterns shift, and new security threats emerge. What was once a high-performing, secure network can quickly become a bottleneck and a liability if not properly maintained and optimized.

This playbook is your guide to navigating the critical "Day 2 to Year 5" phase of your Wi-Fi network's lifecycle, covering everything from post-deployment optimization to preparing for a network redesign. It's a comprehensive resource that empowers you to extract maximum performance, fortify security defenses, and future-proof your network for emerging technologies and escalating demands.

Within these pages, you'll find proven strategies, best practices, and actionable insights to:

- Continuously monitor and optimize your network for peak throughput and reliability
- Identify and mitigate performance bottlenecks before they impact user experience
- Implement robust security measures to safeguard against threats like rogue APs

We'll also showcase the latest products from Ekahau that can help you get the best network possible. Ekahau helps businesses build and maintain high-performing Wi-Fi networks. Businesses of every size — including the world's biggest brands and events — use our software and hardware products to design, validate, optimize, and troubleshoot their Wi-Fi.

Table of Contents

Chapter 1: So, You've Got a Wi-Fi Network! › 4
The Network Lifecycle › 4
Network Management: Access Points and Dashboards › 5
Network Management: Wi-Fi Optimization Tools › 5
Maximizing Your Wi-Fi Investment › 6

Chapter 2: Understanding Your Network › 7
Wi-Fi 101: What is Enterprise Wi-Fi? › 7
It All Starts With a Wi-Fi Survey › 7
Tips for Accurate Surveys › 8

Chapter 3: Optimizing and Troubleshooting Your Network › 10
Understanding Symptoms of Underlying Wi-Fi Issues › 10
Reviewing Data in Ekahau Optimizer › 10
Primary Coverage › 11
Secondary Coverage › 11
Channel Widths › 12
Channel Interference › 12
Signal to Noise Ratio › 14
RF Interferers › 14
Minimum Basic Rate › 15
SSIDs Configuration › 16
Making Changes in Your Controller › 16
Provisioning APs in your Dashboard With Ekahau Data › 17
Challenges and Opportunities in Large Network Wi-Fi Management › 18

Chapter 4: Securing Your Network › 19
Vulnerabilities Are Everywhere › 19
Rogue APs › 19
Encryption Strength › 19
Management Frame Protection › 21
Reducing Your Hacking Risk › 21
Securing Your Network with Ekahau › 22

Chapter 5: When It's Time to Redesign › 23
Introduction to Redesign › 23
Product Highlight: Ekahau AI Pro Online › 23
Partial Network Upgrades › 24
Access Point Upgrades › 25
Full Redesigns › 25
Assessing Your Aging Infrastructure › 26

Conclusion › 27
Network Decision Tree › 28

Chapter 1: So, You've Got a Wi-Fi Network!

Congratulations! After months of planning, design, and deployment, your shiny new Wi-Fi network is up and running. Or, maybe you inherited a network that has some...ahem...issues. Or perhaps you've inherited a network and don't even know yet if there are issues lurking beneath the surface. Whatever your situation, this guide will help you through this critical phase: ongoing network management and optimization.

The reality is that your Wi-Fi network should be treated like a living, breathing entity that requires constant care and attention to maintain peak performance and security. Evolving usage patterns, new applications, and emerging threats will inevitably put pressure on even the most carefully engineered wireless designs.

Reactive network management, where issues are addressed only after they've already impacted users and operations, is a recipe for frustration, productivity losses, and increased security risks. Instead, this playbook advocates for a proactive approach that continuously monitors, optimizes, and fortifies your network — a strategy that empowers you to stay one step ahead of emerging challenges.

In this chapter, we'll start with an overview of the different parts of network management and how you can maximize your return on your investment. In the next chapters, we'll jump into your specific requirements, understanding your current network, and how to move forward making changes that will optimize and secure your Wi-Fi.

The Network Lifecycle

Wi-Fi isn't set-it-and-forget-it. Your network lifecycle is a continuous process of monitoring, fine-tuning, and future-proofing to ensure your network remains high-performing, secure, and aligned with your organization's ever-changing needs.

The Wi-Fi network lifecycle can be broadly divided into three key phases:

1. **Design and Deployment**
   In this phase, requirements are gathered, predictive models are created, and access points (APs) are strategically placed to establish a robust wireless infrastructure tailored to your unique environment and use cases. After deployment, networks are validated to ensure they are performing as designed.

2. **Continuous Optimization and Troubleshooting**
   Often underestimated, this phase of a network's lifecycle is just as vital as the initial design. Usage patterns shift, new applications are adopted, sources of interference emerge, and physical environments evolve. Continuous management through optimization tools and regular troubleshooting and security audits are essential to maintaining peak wireless performance. We often refer to this phase as "Day 2 to Year 5", but your network lifecycle might be cut short due to quickly shifting technology requirements or extended due to budgetary constraints.

3. **Network Refresh or Redesign**
   Eventually, even the most meticulously managed network will reach the limits of its capabilities. This phase involves strategic upgrades, expansions, or full redesigns to support next-generation wireless standards, increased bandwidth demands, and emerging use cases like AR/VR or IoT.

The wireless network lifecycle is a constant cycle of adaptation. By embracing this mindset and leveraging the strategies outlined in this playbook, you'll ensure your Wi-Fi network remains a high-performing, secure, and future-ready asset that drives your organization's success.

Network Management: Access Points and Dashboards

At the heart of every Wi-Fi network is a fleet of access points — devices that enable wireless data transfer between clients (phones, computers, etc.) and the rest of your network infrastructure (and ultimately the internet). While physical AP placement and channel planning are crucial, equally important is the ability to centrally manage and monitor these devices.

Every major Wi-Fi access point vendor provides a cloud-based controller dashboard that serves as a command center for your wireless network. With these central dashboards, you can view and adjust a wide range of configuration settings for each AP.

Through your AP dashboard, network administrators can perform these critical tasks:

- Adjusting radio transmit power levels to optimize coverage and manage interference
- Setting authentication and encryption protocols to secure the wireless environment
- Enabling/disabling specific Wi-Fi bands (2.4 GHz, 5 GHz, 6 GHz) and configuring channel selections
- Pushing firmware updates to keep APs current with the latest security patches and feature enhancements
- Monitoring AP status, client connections, data rates, location-based analytics like traffic, and more

Network Management: Wi-Fi Optimization Tools

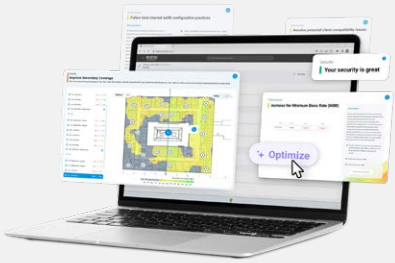
While vendor access point dashboards provide valuable visibility and control over the wireless infrastructure itself, true network optimization requires an outside-in perspective combined with advanced analytics capabilities.

By leveraging real-world data collected by specialized Wi-Fi measurement devices, these solutions deliver unparalleled insights into your network's performance, the full RF environment, potential security threats, and key areas ripe for improvement. This multi-dimensional visibility is critical for accurate analysis and intelligent optimization.

Ekahau Sidekick 2

Ekahau Sidekick 2 is the world's fastest, most accurate, and easiest-to-use Wi-Fi testing and measurement device. The Sidekick 2 enables you to collect real-world data to validate and optimize any wireless network by simply walking through the site. With Sidekick 2, you can identify Wi-Fi signal strength at every point of your network, measure network performance, and detect environmental RF that may negatively impact your network.

Ekahau Optimizer



Ekahau Optimizer dives deep into your unique network, analyzes mountains of Sidekick 2 data, and serves up instant and actionable recommendations that increase the performance and security of your network. With Optimizer, problems that used to require massive amounts of time and expertise to identify are uncovered and addressed with lightning speed.

Ekahau AI Pro Online

Ekahau AI Pro Online simplifies network upgrades and redesigns by leveraging real-world survey data and AI machine learning to create accurate RF models of your environment. Its intuitive interface and powerful modeling capabilities allow you to visualize Wi-Fi designs addressing coverage gaps and ensure optimal results for any redesign scenario.

Maximizing Your Wi-Fi Investment

Enterprise Wi-Fi networks aren't cheap. Each AP can be a couple of thousand dollars USD and often has a subscription cost associated with management software, not to mention the cost of installation. The cost of a network redesign is tens or even hundreds of thousands of dollars for large networks. Large public venues can even run into the millions of dollars for their wireless network deployments.

Given these substantial price tags, it's crucial to maximize the lifespan and extract full value from your wireless infrastructure investments. This is where Wi-Fi optimization solutions prove their worth — bridging the gap between costly redesign cycles and saving your budget in the process.

By continuously monitoring and fine-tuning your network through advanced data-driven optimization, you can:

+ **Extend Your Network Lifecycle**
  Even the most meticulously designed Wi-Fi network will eventually hit a performance ceiling as new technologies, usage patterns, and facilities evolve. Proactive ptimization delays this expiration, significantly extending your network's viable lifecycle before replacements are required.

+ **Enhance User Experience**
  Optimization ensures your Wi-Fi keeps pace with changing demands, delivering a consistently great experience as throughput needs and bandwidth-hungry applications increase over time.

+ **Identify Upgrade Triggers**
  When optimization alone can no longer compensate, these network analysis tools objectively highlight deficiencies, arming you with data-driven justifications for targeted upgrades or full redesigns.

+ **Maximize Network Security**
  Beyond performance tuning, Wi-Fi optimization platforms also scan for and mitigate potential security vulnerabilities — ensuring your network remains a hardened, policy-compliant environment.

Investment in robust Wi-Fi optimization solutions provides immense ROI by squeezing every ounce of potential from your wireless infrastructure until the next refresh cycle.

.

"Using Ekahau, we reduced our troubleshooting time dramatically, from an average of over twenty hours a week to addressing just one ticket every two to six months, which now only takes us five to ten minutes to resolve. Our ROI was less than 90 days."

Aaron Brown
Senior Network Engineer, Premiere Health

Chapter 2: Understanding Your Network

Wi-Fi 101: What is Enterprise Wi-Fi?

At Ekahau, we want to ensure that everyone — from newly minted network technicians, to experienced Wi-Fi professionals — get the most out of our resources. These next few pages describe how Wi-Fi works; with a good understanding of the basics of Wi-Fi, you'll be better equipped to optimize an enterprise wireless network.

Enterprise wireless networks typically use cloud-based controllers, switches, routers, dedicated security hardware, and access points.

Made Possible by the Electromagnetic Spectrum

So how do access points communicate with client devices like laptops and phones? They transmit and receive signals across specific Wi-Fi bands within the electromagnetic spectrum.

The RF spectrum is divided into different bands, each with its range of frequencies. Wi-Fi networks operate in 3 bands: 2.4, 5, and 6 GHz. Within these bands, Wi-Fi networks utilize multiple channels — specific frequencies on which APs and clients can communicate. Proper channel planning and configuration are crucial to minimize interference and maximize performance.

Are you a total Wi-Fi newbie? We've got you covered. Read our blog on Wi-Fi fundamentals and common acronyms you'll encounter on your wireless journey.

It All Starts With a Wi-Fi Survey

Whether you need to optimize, secure, or even redesign your network, it all starts by capturing Wi-Fi data in your network environment. Your wireless network is a complex web of invisible spectrum that keeps your organization connected and productive. But without the right tools and insights, your Wi-Fi remains a mystery, hiding potential issues and opportunities for improvement.

The first step to understanding your current network is to capture accurate network data with a purpose-built Wi-Fi measurement tool. This data capture is called a "Wi-Fi survey" and all it takes nowadays is going for a walk with the Ekahau Sidekick 2 and your phone or tablet. The Sidekick 2 listens for beacons transmitted by all enabled radios inside the access points and identifies their precise locations. It measures their received signal strength, identifies sources of RF interference, and captures the full picture of your network configurations so you can visualize your invisible Wi-Fi network through heatmaps.

Figure: Primary Signal Strength Heatmap in Ekahau AI Pro Online

Heatmaps are used to visualize Wi-Fi data in an easy-to-interpret format layered on top of your site's floor plan. In this example, areas in green are receiving great signal, while areas in gray have fallen below the threshold for adequate signal and represent a gap in coverage.

All you need to perform the world's most accurate Wi-Fi survey is the Sidekick 2 and whatever phone is in your pocket. Using the Sidekick 2 with the Ekahau Survey App on your phone or tablet is super easy, with 5 intuitive survey modes for any situation.

- **Just Go Survey**
  This survey mode leverages augmented reality technology in the Apple ARKit and LiDAR scanning to dynamically create a floor plan as you walk through your environment. Simply take your Sidekick 2 for a walk around your network and watch as your floor plan sketch and Wi-Fi data get captured automatically. Just Go Surveys are accurate, fast, and hassle-free.

- **Autopilot Survey**
  Autopilot survey mode automatically tracks your location on your uploaded floor plan map while continuously collecting survey data at every step. This survey mode is easy, hands-free, and perfect when you have a floor plan to work from. Just scale your floor plan, calibrate your location, and walk your site.

- **Continuous**
  Continuous surveys collect data at every step along the path marked by the surveyor. Just tap your location on the floor plan anytime you start, stop, or turn to capture a new line segment. Continuous surveys are a great alternative for devices that don't support Autopilot mode.

- **Stop & Go**
  Stop & Go allows the surveyor to collect data limited to certain areas. Click your location on the floor plan and wait as the data is collected before moving to a new location.

- **GPS**
  This survey mode is extremely valuable in outdoor areas or vast open spaces where there are limited landmarks available for orientation. Available for devices with GPS radios.

Tips for Accurate Surveys

Accurate surveys are the foundation of a well-optimized Wi-Fi network. To ensure you collect the most precise and comprehensive data, keep these essential tips in mind:

- **Walk on both sides of walls and other attenuating materials.**
  Measure signal strength on both sides of the attenuating material that you care about to determine the attenuation values. The attenuation value is the absorption of a signal by obstacles like walls or shelving racks. Never assume that measuring just one side of a wall or obstacle will capture all of the data needed for accurate optimization.

- **Survey Every Room**
  If a space needs Wi-Fi, include it in your survey. For buildings divided into many different offices or rooms, it's important to enter each room to let the Sidekick capture data. And if it's large enough, be sure to walk the entirety of the room and not just in and out the center.

- **Utilize an S Formation in Large, Open Areas**
  For large, open spaces like cafeterias, auditoriums or open floor plan office seating areas, it's important to divide the room into multiple passes for complete survey coverage. We recommend walking an S formation of the area doubling back every 3-5 meters to avoid gaps. Think of these large rooms like you're playing the snake game on your old Nokia — you don't need to get a high score but you're going to want to collect data throughout the room for accurate optimization and troubleshooting.

Use the Ekahau Sidekick 2

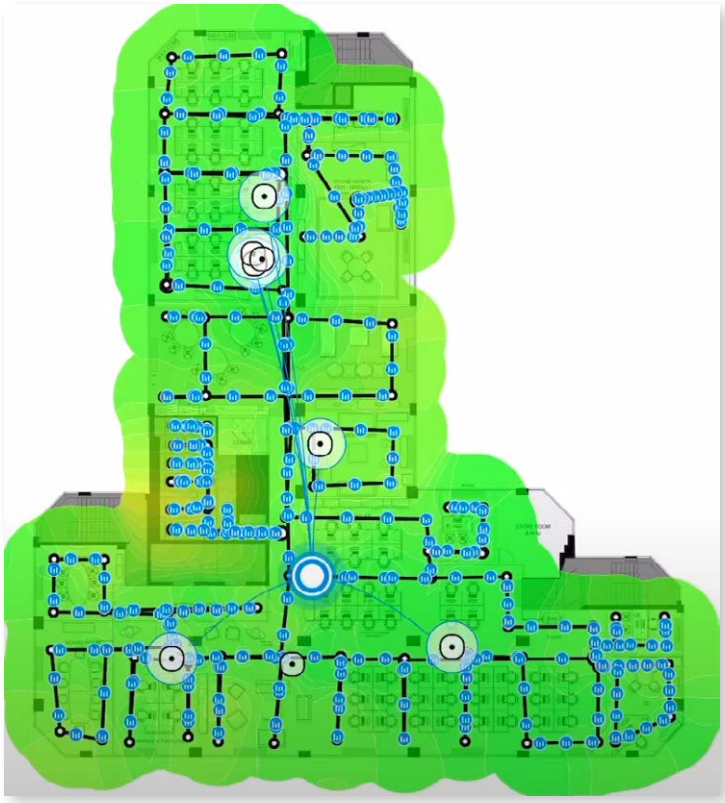
The Ekahau Sidekick 2 is the premier Wi-Fi measurement device, providing highly accurate data for Wi-Fi surveys and spectrum analysis. The Sidekick 2 stands alone for proven speed, accuracy, and reliability. Each unit is rigorously tested and calibrated against published third-party accuracy data, includes a built-in spectrum analyzer, and offers a full day's battery life. The Sidekick 2 delivers consistent and accurate results every time.

Using Just Go survey mode? Walk the whole floor in one go.

The 'Just Go Survey' approach is designed for simplicity and efficiency, allowing anyone to gather Wi-Fi data effortlessly — no scaling or floor plan needed. One key aspect to note is that Just Go Survey treats each walk-through as an entirely new site. This allows the augmented reality engine to accurately map your surroundings without any prior spatial data. However, it also means you'll need to traverse the entire floor or area during that single survey pass. The augmented reality platform cannot recognize if you're revisiting the same location from a previous survey. By walking the full site in one continuous survey, Just Go Survey collects a complete RF dataset for that environment.

Using any other survey mode? Ensure you have properly scaled your floor plan.

Accurately scaling the floor plan is critical to ensuring precision in your surveys. Don't pick a small measurement for scaling your floor plan. If you scale a door at 1 meter but are off by 0.2 meters, your 100-meter building can be off by 20 meters! Laser measurement tools can ensure your floor plan is accurate and lengths are properly defined. For Autopilot survey mode to be as accurate as possible, be sure to calibrate it correctly with your first few steps of the survey. Start by clicking your exact location on the floor plan, then walk a few meters and click again matching your exact location to your surroundings. By calibrating, you're setting the tracking capabilities to your floor plan scale and ensuring great results.



Chapter 3: Optimizing and Troubleshooting Your Network

Understanding Symptoms of Underlying Wi-Fi Issues

From the user's perspective, a Wi-Fi issue often first rears its head through a vague symptom: frustratingly slow speeds, intermittent disconnects, poor voice or video calls, or being unable to connect at all. However, these surface-level complaints are typically just the tip of the iceberg.

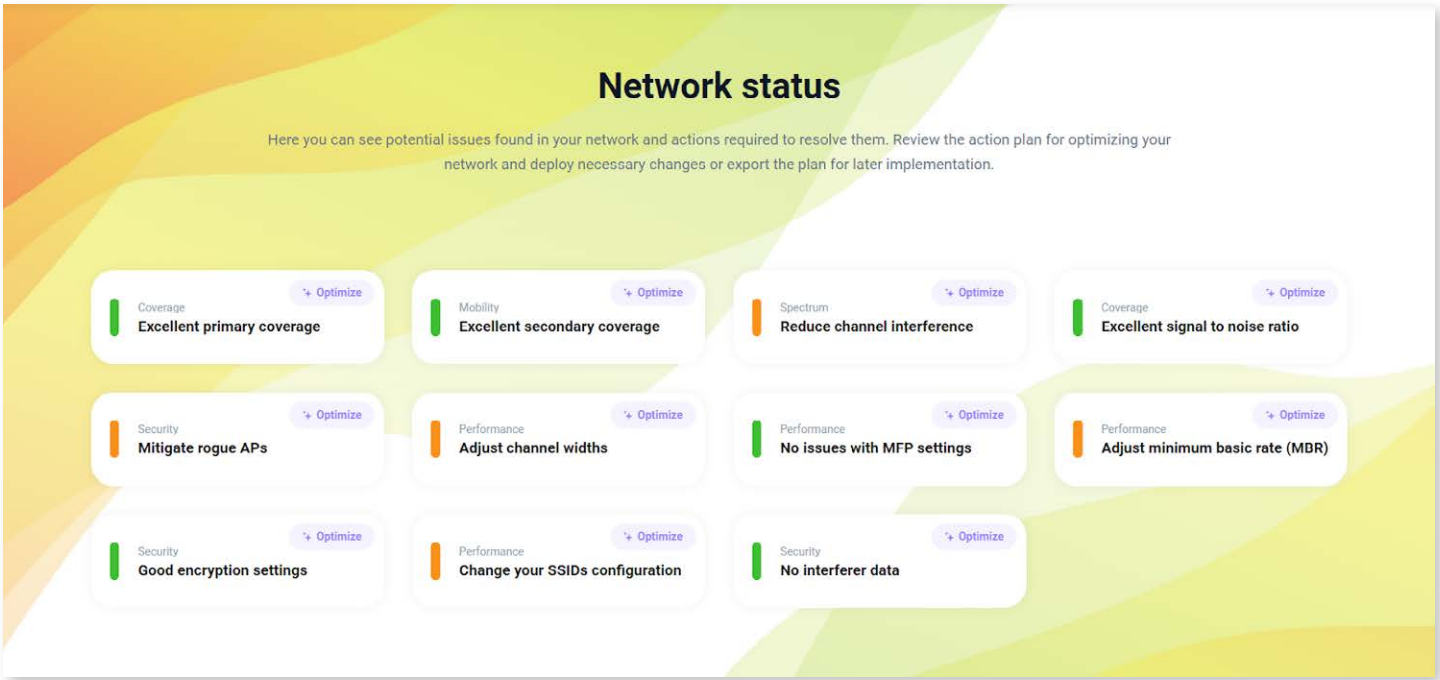
All too often, organizations try to remedy Wi-Fi performance and connectivity complaints using guesswork and brute force. Without proper site survey data, spectrum analysis, and optimization tools, the knee-jerk reaction is often to throw more access points at the problem. This can actually create new problems! The real culprit could be something like co-channel interference from a neighboring network or from RF interferers; simply adding more APs does nothing to address those foundational flaws.

Intelligent Wi-Fi tools that combine site surveys, spectrum analysis, and configuration assessments empower you to remedy the core issues your network is facing.

Reviewing Data in Ekahau Optimizer

After performing a site survey, sync your project data to Ekahau Cloud and put your feet up: Ekahau Optimizer analyzes extensive data from the Sidekick 2 to provide you with instant and actionable recommendations that will have the maximum impact on your network's performance. Whether you're a seasoned Wi-Fi professional or new to network optimization, Optimizer is the powerful tool you need to enhance your wireless performance. Problems that used to require a lot of time and expertise to identify (i.e. coverage gaps, performance issues, mobility misconfigurations, security vulnerabilities) are uncovered and addressed with lightning speed.

In this next section, we'll walk through all of the Wi-Fi performance-related optimizations you can identify in Optimizer, followed by security-related optimizations. Here's the configuration ptimizations summary you'll see when you open Ekahau Optimizer.



Primary Coverage

Primary coverage is all about ensuring there is sufficient signal strength for Wi-Fi-enabled devices to connect and transmit data. For many devices, a measured signal strength of -67 dBm represents the lower limit of a healthy signal. It's always important to remember that different wall materials and physical obstacles absorb Wi-Fi at different rates. An empty drywall will attenuate Wi-Fi signals way less than a concrete wall or elevator shaft.

By walking with the Sidekick 2 throughout your network, you'll identify the exact Wi-Fi coverage throughout your environment. Optimizer will show you a visualization of where the connection is strong, and where you might be having some challenges.

If you're lacking primary coverage, Optimizer will provide you with the following recommendations:

- Ensure that your access points and antennas are all installed correctly, that there aren't any loose connections, and that they are all online and broadcasting (you'll be able to see this in your network controller).
- Try increasing the transmit power of your access point radios to between 14-17dBm (25-50mW) if they are currently set lower.

Still have major coverage gaps? Chapter 5 is all about how to overcome these challenges, from simple fixes of adding additional access points to complete redesigns.

Secondary Coverage

Secondary coverage is critical to ensure you have great roaming between APs, redundancy in the event an AP has a failure, and to assist with higher capacity needs.

Roaming

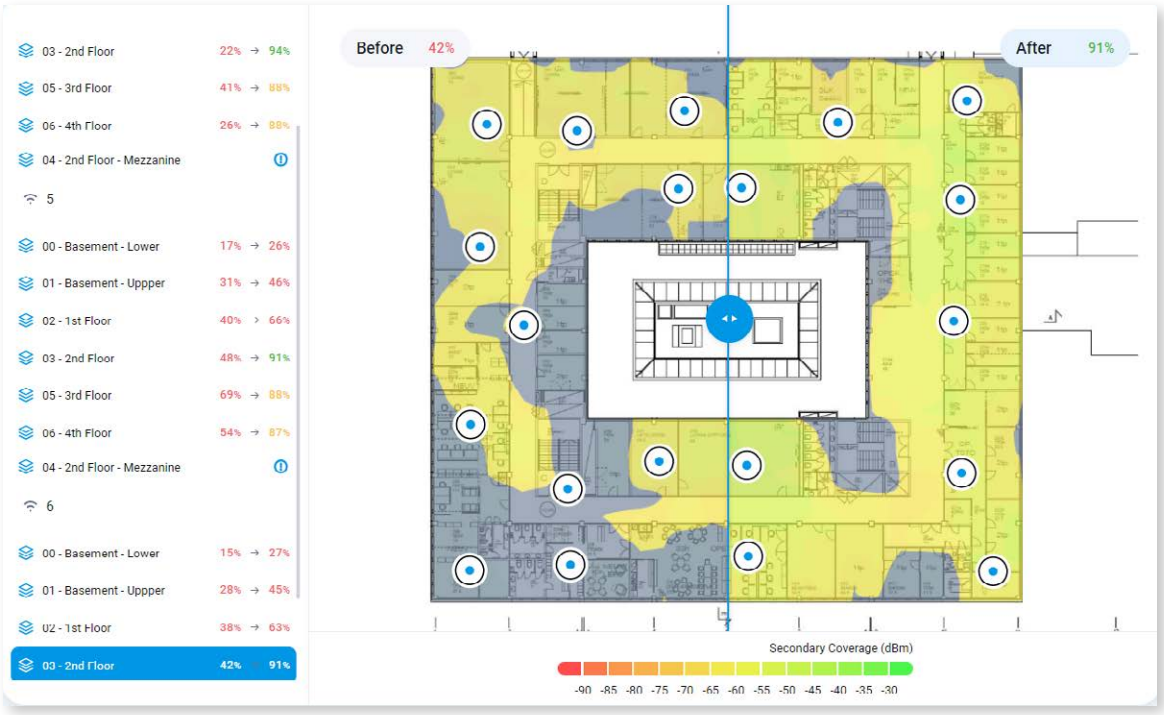
Roaming happens when your device's connection jumps between access points. Roaming is especially important if you're doing tasks like walking around the office while on a voice call or carting hospital devices from room to room. To enjoy smooth roaming, you need decent primary and secondary signal strength. Ideally, you want to have both primary and secondary signal strength hitting close to -67 dBm so that every time you get to the edge of your existing coverage cell, you always have a great alternative to roam to.

Redundancy

Secondary coverage is also critical for coverage redundancy. Meaning, if one AP were ever to fail, you will still have coverage from that secondary access point. We talk all the time about how Wi-Fi is business critical, and this is exactly what we mean — if an AP goes down, work does not have to go down with it.

Capacity

Lastly, secondary coverage can help you with your capacity needs. High-quality primary plus secondary coverage will most likely mean that your connected devices will now be spread between two APs instead of just one. When you need to support more people in the same area, proper secondary coverage will help your network keep up with all these added devices and new types of applications.



Secondary coverage as seen in Ekahau Optimizer.

Channel Widths

Whether you are using a static channel plan or a vendor's RRM for dynamic channel assignment, there are a few things to consider besides just picking Wi-Fi channels. One of the most important is deciding on the proper channel width to use.

Think of Wi-Fi channels like lanes on a highway. Standard 20 MHz channels are like individual lanes, each allowing a certain amount of data (cars) to pass through at a given time. These 20 MHz channels can be combined (bonded) to create wider channels, such as 40 MHz, 80 MHz, or even 160 MHz. The wider the channel, the more data can be pushed through it. You know those impressive throughput numbers vendor's love to tout in the AP datasheets? Those are achieved by using these wide channels. Some vendors' equipment these days is even set to these wide channels by default right out of the box.

It's important to carefully consider your network requirements and environment before selecting a channel width. Wider channel widths provide higher throughput but reduce the number of non-overlapping channels, can result in a shorter range, are more susceptible to interference, and may not be compatible with all Wi-Fi client devices.

Channel Interference

There are many tasks associated with properly managing a wireless network—one of the most important is developing a channel plan. A carefully designed channel plan is crucial for optimizing the use of limited wireless spectrum, one of the foundations of high-performing Wi-Fi networks.

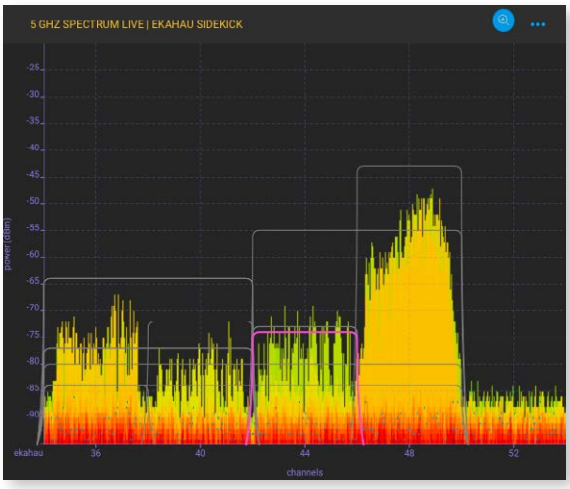
In wireless networks, channel interference occurs when multiple nearby APs operate on overlapping channels, leading to reduced performance and connectivity issues. To ensure optimal Wi-Fi performance, it's crucial to minimize channel overlap and implement effective channel planning strategies. Here are three types of channel interference that could be causing you issues:

Adjacent Channel Interference
Adjacent Channel Interference (ACI) occurs when APs are operating on channels that are too close to each other in the frequency spectrum. This results in the signals from neighboring channels bleeding over and interfering with each other. Think of ACI like having two competing radio stations and having a mix of country music overlapping on your favorite metal station.

Co-Channel Interference
Co-Channel Interference (CCI), on the other hand, is when two or more APs that are in the same area are operating on the same channel. This essentially turns both cells (a cell is the coverage area for an AP) into one big cell, degrading your network performance. That's because Wi-Fi is very polite and clients won't talk over each other: every device must wait to transmit on a specific channel until other devices have finished transmitting. When you have a large cell from multiple APs on the same channel, every device will be waiting longer to transmit data.

OBSS

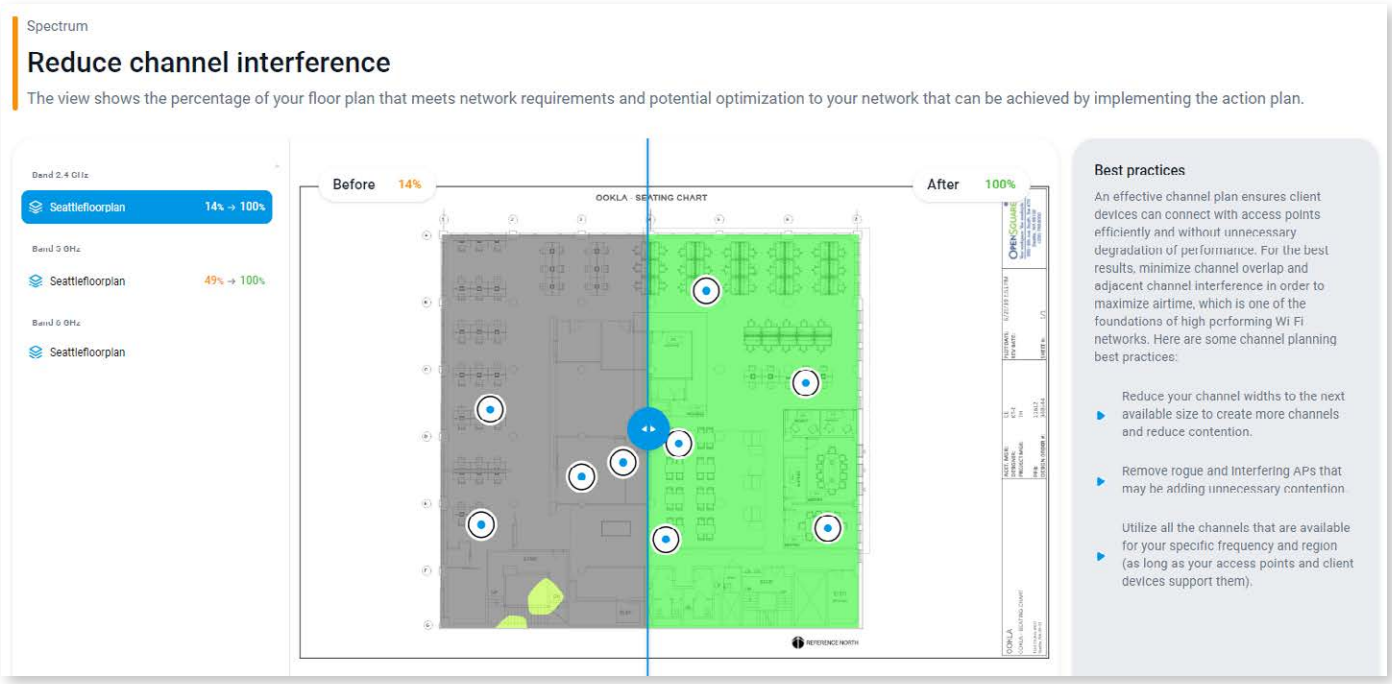
Overlapping Basic Service Set (OBSS) occurs when non-primary channels of different access points overlap, and it can be even more destructive to network performance than standard channel overlap. Imagine two APs in the same area both using 40 MHz bonded channels: AP1 uses channels 36 (primary) and 40 (secondary), while AP2 uses channels 40 (primary) and 36 (secondary). Devices associated with AP1 listen on channel 36 before transmitting, and those with AP2 listen on channel 40. Since both APs are operating in the same room and using overlapping channels, devices from both APs might decide to transmit at the same time after checking their respective primary channels.. This will lead to a signal collision, no acknowledgement, and retransmission. The more retransmissions we have, the slower the Wi-Fi is.



In certain wireless environments, using an AP vendor's radio resource management (RRM) within their dashboard can be useful for reducing your adjacent channel, co-channel, or OBSS interference. RRM is an automated system that dynamically adjusts radio configurations, such as channel assignments and transmit power levels, based on real-time RF conditions.

However, in other environments, relying on RRM may not be sufficient to effectively mitigate interference. This is particularly true in complex, high-density networks or in situations where there are multiple Wi-Fi networks from different vendors operating in close proximity. In such cases, turning off RRM and using a static channel plan can be beneficial.

Ekahau Optimizer action plans are personalized to your unique network down to the individual radio settings in each of your access points and can help mitigate a number of common Wi-Fi issues like channel interference.



Signal to Noise Ratio

Signal to Noise Ratio, or SNR, plays a critical role in determining the data rates and throughput that users can achieve in a given area. SNR is a measure of the usable signal strength relative to the level of background noise. A higher SNR indicates a stronger, cleaner signal, which translates to better signal quality and faster transmissions.

If the SNR is too low in certain areas, it could cause data-hungry applications like video calling or high-definition streaming to fail or experience significant quality issues. By identifying areas with poor SNR, you can take targeted actions to improve signal strength, reduce noise or interference, or both, ensuring that your users can enjoy fast, reliable connectivity throughout your network.

To accurately measure SNR, you need a Wi-Fi measurement device with built-in noise detection capabilities of a spectrum analyzer. Without a spectrum analyzer, noise levels are merely guessed or calculated, rather than directly measured. This can lead to inaccurate SNR values and a misunderstanding of the true network performance.

The Ekahau Sidekick 2 is the only Wi-Fi measurement device on the market with a built-in spectrum analyzer. This means that when you perform a site survey with the Sidekick 2, you get exact, measured SNR values at every point in your network. By capturing real-world noise levels and correlating them with signal strength, the Sidekick 2 provides you with precise SNR data, which is essential for understanding and optimizing your network's throughput and data rates.

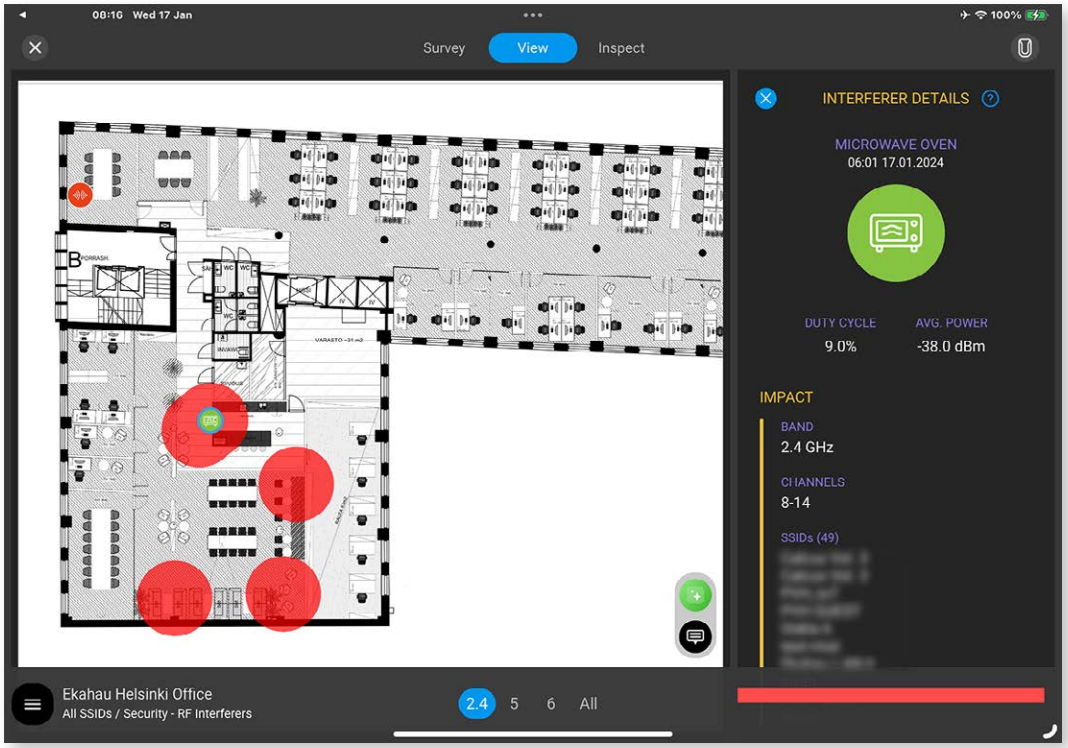
RF Interferers

Have you ever experienced sudden drops in your Wi-Fi performance or connectivity issues that seem to appear out of nowhere? Does your 2.4 GHz network mysteriously get devoured as soon as you start microwaving your frozen burrito? Welcome to the world of RF interferers — the hidden troublemakers that can wreak havoc on your wireless network.

While Wi-Fi is a marvel of modern technology, it has a weakness: it exists in the so-called "unlicensed spectrum". Meaning, you don't need a license from the government to transmit at these frequencies. This means that other devices can legally operate alongside (or even on top of) your Wi-Fi, causing interference and disrupting your performance. Devices such as motion sensors, wireless headsets, leaky microwaves, motion detectors, and Wi-Fi jammers are just a few examples of things you might be unaware of without having data captured with a spectrum analyzer.

RF interference can manifest in various ways, such as reduced signal to noise ratio, increased latency, lower data rates, and even complete connectivity dropouts. These issues can be frustrating for end-users and can significantly impact productivity in business environments. In some cases, RF interference can be so severe that it renders a Wi-Fi network virtually unusable.

Being able to identify interferers is a huge component of troubleshooting Wi-Fi issues. Using your Sidekick 2 and Survey App, or while reviewing your survey data in Ekahau Optimizer, you can identify sources of RF interference in your environment, with their location pinpointed on your floor plan.



Minimum Basic Rate

Before we jump into Minimum Basic Rate, we need to explain frames. Frames are the basic units of data transmission in Wi-Fi networks, and they come in three main types:

1. Management frames handle the connection between devices by establishing and maintaining communication. Examples include beacon frames, which announce the presence of a Wi-Fi network, and authentication and association frames, which facilitate device connections.

2. Control frames assist in delivering data by managing access and ensuring data integrity. Examples are Request to Send (RTS) and Clear to Send (CTS) frames, which prevent collisions, and Acknowledgement (ACK) frames, which confirm the successful receipt of data frames.

3. Data Frames carry the actual payload — the information users are sending or receiving. Everything from cat memes to mission-critical robotics sensors.

Minimum Basic Rate (MBR) dictates the data rate at which your control and management frames are transmitted. While data frames will be transmitted at highest available data rates (potentially faster than 1Gbps), control and management frames will be transmitted at Minimum Basic Rates (MBR) allowed.

Minimum Basic Rate (MBR) controls the speed of your control and management frames. While data frames will be transmitted at highest available data rates (potentially faster than 1Gbps), control and management frames will be transmitted at Minimum Basic Rates (MBR) allowed.

Its important to note that some old devices will be unable to access a network if the MBR is set higher than the device can transmit. When possible, the best practice for MBR is to always use at least 12 Mbps MBR across all frequency bands: Disable all lower rates, and support all higher rates. In higher density Wi-Fi networks with a good quality physical design, MBR should be set to 24 Mbps.

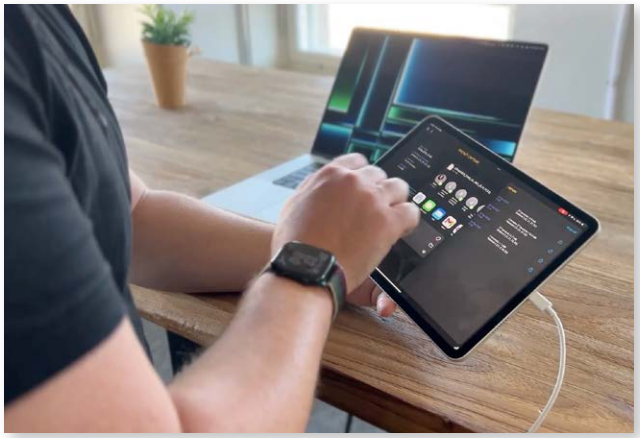
By disabling low data rates, you can ensure client devices will only connect to an access point when they are close enough to receive an adequate signal. Allowing low rates can cause client devices to cling to a particular access point even if it's far away, monopolizing network resources and reducing overall performance for all nearby clients.

Disabling low data rates can also help improve overall network performance by reducing airtime consumption. Airtime consumption is an important concept in Wi-Fi networks that refers to the amount of time a device spends transmitting frames. In a Wi-Fi network, multiple devices share the same wireless channel, and each device must take turns transmitting. When a device is transmitting, it consumes airtime, preventing other devices from using the channel simultaneously. The more airtime a device consumes, the less time is available for other devices to transmit their frames. Lower data rates require more airtime to transmit the same amount of data, which can slow down the entire network.

SSID name ↓	2.4 GHz	5 GHz	6 GHz
Ekahau Guest		6 Mbps	
Ekahau LAN		6 Mbps	
Ekahau LAN 6			6 Mbps
Ekahau-IoT	1 Mbps		
Ookla	1 Mbps	6 Mbps	
Ookla 6			6 Mbps
Ookla Guest	1 Mbps	6 Mbps	
sktest5	1 Mbps	6 Mbps	

SSIDs Configuration

When configuring your wireless network, it's essential to pay attention to how you set up your Service Set Identifiers (SSIDs). An SSID is the name of your wireless network that clients see and use to connect to your Wi-Fi. However, if you use the same SSID across different frequency bands, such as 2.4 GHz, 5 GHz, and 6 GHz, you may encounter some issues with client device behavior.



If the same network name is used across frequency bands, some of your client devices may opt for the 2.4 GHz network, even if the 5 or 6 GHz network is typically faster and more reliable. That's because the 2.4 GHz band is more prone to interference and congestion than the 5 GHz or 6 GHz bands, has less usable bandwidth, less non-overlapping channels, and can lead to suboptimal performance. Additionally, devices connecting to the 2.4 GHz network may have slower connection speeds and higher latency, which can negatively impact the user experience. When clients connect to 2.4 instead of 5 or 6 GHz, they may also experience additional roaming issues.

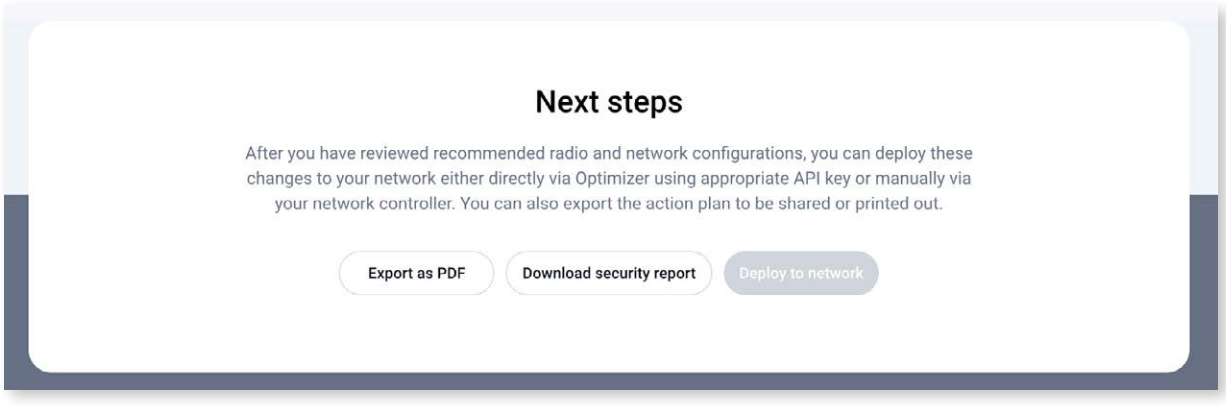
Moreover, with multi-band SSIDs in use, Wi-Fi clients will sometimes roam between different frequency bands, and this will cause roaming to be slow, potentially affecting or breaking connectivity. Your voice or video call might struggle from poor quality, can end abruptly or you can even disconnect from Wi-Fi for a few seconds.

To address this issue, it's recommended that you assign a unique SSID name to each network for each frequency band. For example, you could use "YourNetworkName_2.4" for the 2.4 GHz network, "YourNetworkName_5" for the 5 GHz network, and "YourNetworkName_6" for the 6 GHz network. By doing this, you give your users the ability to explicitly choose which network they want to connect to based on their device's capabilities and the available signal strength. Once your device connects to Wi-Fi on one frequency band, like 6 GHz, it will stay connected there and won't try to roam to a different band.

Making Changes in Your Controller

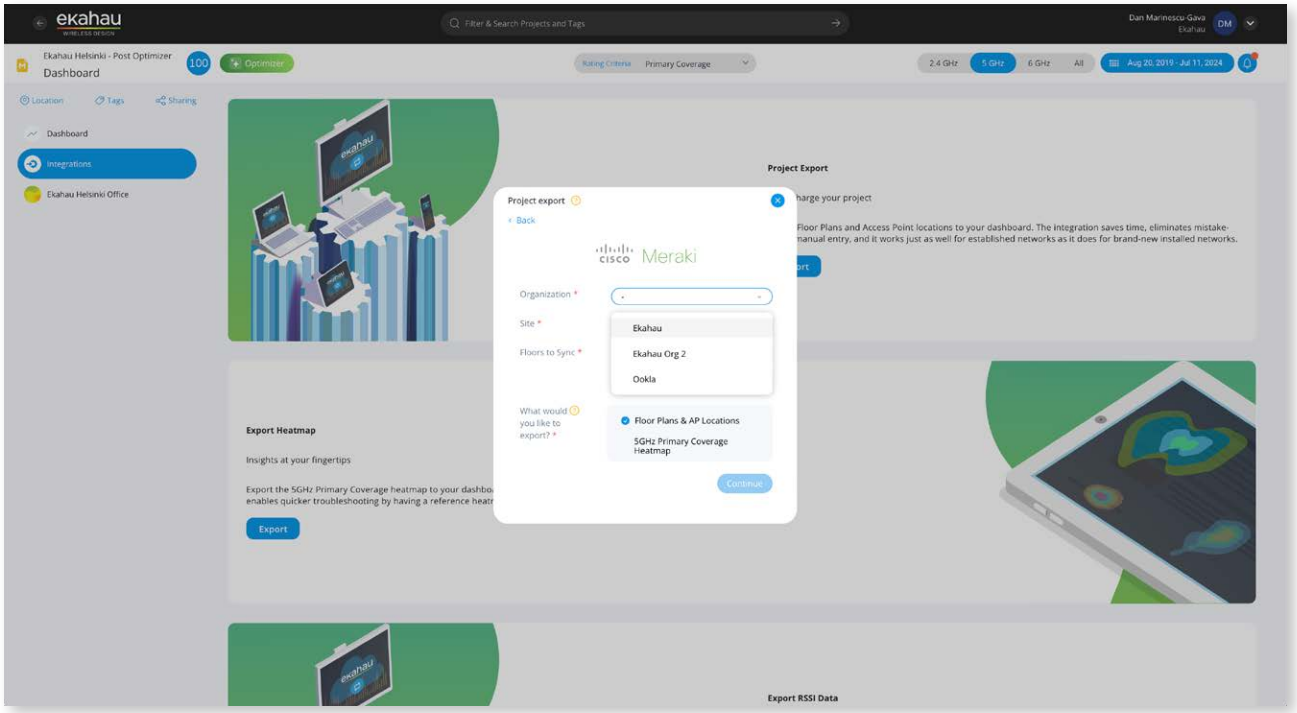
Ekahau Optimizer's action plans make it easy to change settings in your cloud-based controller. With Optimizer, you get powerful optimizations personalized to your unique network down to the individual radio settings in each of your access points.

Simply make the recommended changes in your vendor's controller settings to quickly and easily improve your Wi-Fi. Optimization action plans can be viewed in the browser or exported to PDF to share with colleagues or customers.



Export summary of changes or automatically deploy via API

Provisioning APs in your Dashboard With Ekahau Data



Provisioning is a process where you correlate your access point locations to the map inside your vendor dashboard. It used to be a tedious process, and was a bottleneck to using highly valuable location-based features in your vendor's dashboard.

Provisioning your dashboard used to be a lot like a game of "Pin the Tail on the Donkey," but instead of trying to stick a paper tail on a cartoon donkey, you're trying to accurately match your APs serial numbers and place your APs on a floor plan in your dashboard without mistaking a capital O for a zero. While time-consuming and error-prone, accurate access point placement on your vendor's dashboard floor plan is crucial for unlocking valuable features like location-based services and advanced analytics.

We knew there had to be a better way. By simply walking your site with the Ekahau Sidekick 2, you can capture precise AP location data that can be exported to your vendor's dashboard with just a few clicks via your vendor's dashboard API. These integrations ensure that your dashboard is instantly and accurately provisioned based on trusted, verified measured data.

The benefits of provisioning your dashboard with Ekahau data are numerous:

Enable location-based services: With accurately placed APs, you can unlock powerful features like asset tracking, wayfinding, and proximity notifications, helping you optimize operations and enhance user experiences.

Unlock advanced analytics: Precisely located APs enable granular insights into traffic patterns, space utilization, and client behavior, empowering you to make data-driven decisions about your Wi-Fi environment.

Streamline troubleshooting: Many vendors' root cause analysis and troubleshooting tools rely on accurate AP placement. By provisioning your dashboard with Ekahau data, you can ensure that these features work optimally, helping you quickly identify and resolve issues.

By leveraging Ekahau's integration with your vendor's dashboard, you can unlock the full potential of your Wi-Fi dashboard, enabling advanced features and analytics that drive performance, security, and business value.

Challenges and Opportunities in Large Network Wi-Fi Management

Large organizations face two additional challenges when it comes to Wi-Fi management — geographical diversity and complexity of scale:

Geographical Diversity:
For organizations with a global or widely distributed footprint, managing Wi-Fi across numerous, often distant locations presents significant logistical and operational challenges. From offices in major cities to remote facilities in hard-to-reach areas, ensuring consistent Wi-Fi performance and security across all sites can be a daunting task. When your office with Wi-Fi issues is across an ocean, what are you gonna do? Hop on a 13-hour flight every time someone can't connect to Zoom? That's not just impractical; it's bad for business.

Complexity of Scale:
Even within a single location, many organizations grapple with the challenges of managing Wi-Fi across vast campuses or sprawling facilities. These large-scale environments — whether corporate headquarters, university campuses, or extensive manufacturing plants — often require multiple technicians working together to effectively survey the wireless network to properly optimize and maintain Wi-Fi networks.

Both of these scenarios share common pain points: the impracticality of centralized, in-person management for every issue, varying levels of Wi-Fi expertise across different teams or locations, and the need for consistent, high-quality data collection to inform decision-making. By equipping on-site staff with user-friendly tools to collect high-quality Wi-Fi data, organizations can enable remote analysis and problem-solving by central experts.

Ekahau's Measure licenses offer powerful solutions for large organizations to streamline Wi-Fi measurement and optimization. The Measure license provides access to Ekahau's data collection software and complements the full Ekahau AI Pro and Connect suite, enabling senior network managers to delegate data collection to on-site staff while focusing on analysis and optimization.

This approach significantly reduces travel needs, expedites troubleshooting, and allows teams to efficiently survey large, complex environments. Using the Sidekick 2 and the intuitive Just Go survey mode, local teams can quickly collect comprehensive network health data with a simple walk-through. All collected data can be seamlessly synced via Ekahau Cloud, with Ekahau Insights and Optimizer providing valuable summary statistics across projects, enabling a more distributed and cohesive approach to Wi-Fi management.

Chapter 4: Securing Your Network

Vulnerabilities Are Everywhere

Ask the IT crowd about the most important things in Wi-Fi and you'll get a mixed bag of answers — some will say throughput, some will say latency, others might say fast roaming or high capacity, but most will place security near the top of their lists.

Wi-Fi security is easily the most important thing in Wi-Fi. After all, it doesn't matter how fast your roaming is if your business suffers from a security breach.

Wireless vulnerabilities are everywhere. Just a few years ago, hackers accessed a casino's database through a Wi-Fi-enabled aquarium thermometer. Businesses have had confidential data exposed via Wi-Fi-enabled printers and TVs. These devices can turn vulnerable after routine firmware updates. Moreover, employee devices are regularly compromised to breach company data. And when enterprise Wi-Fi is poor-performing, employees have been known to bring in easily exploited rogue APs. This is known as Shadow IT and can be a huge problem for your IT team's ability to keep your network secure, primarily because they don't know what these devices are or even if they are present.

There are three major wireless security risks to mitigate:

1. Rogue Access Points
2. Poor Encryption Strength
3. No Management Frame Protection

1 Rogue APs

Rogue access points are unauthorized wireless access points which are present on your floor plan but do not belong to your network, and pose a significant security risk. APs that are not your network's APs that are broadcasting from within your premises are considered either a rogue AP (broadcasting and connected to your wired network) or an interfering AP (broadcasting but not part of your network).

Rogue APs can provide dangerously easy access to your infrastructure, and don't always look like standard access points! You might have rogue APs like Wi-Fi-enabled printers or smart TVs that are cabled into your network. These can provide an easy entry point for hackers through Wi-Fi by broadcasting open or poorly secured SSIDs. They also increase airtime utilization by broadcasting beacons, slowing the network down for everyone operating on the same Wi-Fi channel in the area. You probably want to disable Wi-Fi on them, and continue to perform ongoing security surveys to ensure they don't revert back to default broadcasting state after a firmware update.

Interfering APs might present themselves as mobile hotspots or old infrastructure that is no longer in use but is still powered on. Interfering APs will also contribute to higher network contention by increasing airtime utilization. Ideally, you want these interfering APs gone, too.

2 Encryption Strength

Wi-Fi encryption is a security measure that helps protect the wireless data traffic on a Wi-Fi network from being intercepted and accessed by unauthorized parties. It works by encrypting (scrambling) the data being transmitted over a Wi-Fi network using encryption algorithms and keys.

Think about every piece of sensitive information that goes across your organization's Wi-Fi network. Private personal information like social security numbers, credit card information, trade secrets, and more.

Without proper encryption, you are broadcasting that information to anyone within reach of your wireless network: in your lobby, in the parking lot, or across the street. Weak and old security standards (like no encryption/open, WEP, WPA, or weak passwords on WPA2/3-Personal networks) might encourage attackers to exploit your network. They can simply connect to your network and wreak havoc, or silently capture Wi-Fi frames to then decrypt them and see all Wi-Fi transactions in clear text.

Here are the security methods available, from least secure to most secure:

Open
No authentication, no encryption, typically used for guest networks. Not recommended for enterprise networks.

Enhanced Open
Same user experience as Open networks, and still no authentication. However, Enhanced Open uses strong encryption.

WEP
Wired Equivalent Protection (WEP) was introduced back in 1999 and is not recommended by today's standards. WEP is crackable in seconds.

WPA
Wi-Fi Protected Access (WPA) was released in 2003 as a temporary fix for WEP but is still not secure by today's standards. WPA introduced two flavors: WPA-Personal (secured with password) and WPA-Enterprise (authentication through RADIUS server). WPA encryption mechanisms are not as strong as WPA2, and are deprecated and not recommended for your network.

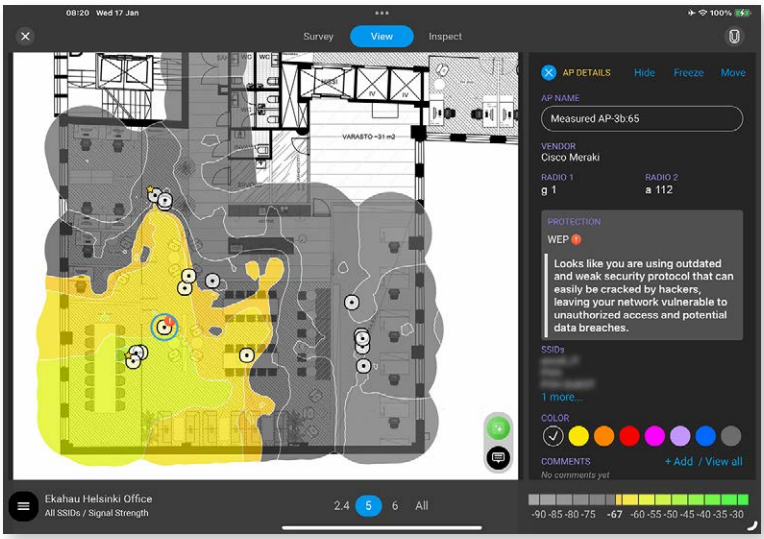
WPA2
WPA2-Personal (Pre-Shared Key, or PSK) is considered secure if the password is strong and meets security recommendations. The password is used for both authentication and directly to create encryption keys. WPA2-Personal can be a target of password guessing (like brute force or dictionary) attacks, so choosing a strong and secure password is very important

WPA2-Enterprise is considered secure, especially if you follow industry best practices and use protected authentication variants (e.g. using EAP-TLS, which uses digital certificates on both the server and the client).

WPA3
WPA3 is the latest security standard, offering the highest levels of security and encryption, but not all devices support it in legacy 2.4 and 5 GHz frequencies.

WPA3-Personal (Simultaneous Authentication of Equals, or SAE) is considered secure if the password is strong and meets security recommendations. The password is used for authentication, but not directly for encryption keys as in WPA2. Encryption is enhanced by a one-way Diffie-Hellman algorithm that is more resistant to password guessing (like brute force or dictionary) attacks.

WPA3-Enterprise is considered as secure as WPA2-Enterprise was, but it mandates the use of Management Frame Protection (MFP – more on that next). It also has an option to use military-grade 192-bit encryption instead of standard (still extremely secure) 128-bit encryption used as default in both WPA2 and WPA3-Enterprise.



3 Management Frame Protection

Wi-Fi technology uses small packets of information called "management frames" to establish and maintain the connection between devices like laptops/phones and access points. These frames are used to handle connection and disconnection of clients.

Management Frame Protection (MFP), also known as Protected Management Frames (PMF), is a Wi-Fi security feature designed to safeguard management frames from being forged or tampered with.

Here's how a real attack exploiting a network's lack of MFP could play out:

> An attacker near your office broadcasts a deauthentication or dissociation frame, immediately kicking everyone off the Wi-Fi network if MFP is not enabled. Then, using a strong directional antenna, they could spoof your SSID and broadcast this signal from a van outside, appearing as a legitimate access point with better signal strength.
>
> Devices would automatically try to reconnect to this rogue access point. However, users would then be prompted for their network login credentials. If employees fall for this and enter their usernames/passwords, the attacker has now harvested their login details, potentially gaining access to email, corporate accounts, and sensitive data — a major security breach.

MFP prevents such attacks by cryptographically validating the source of each management frame. It blocks rogue deauthentication frames and only allows legitimate ones from authenticated access points, securing the connection process.

While MFP provides essential security benefits, it may not be compatible with older devices that don't support the feature. Some older and cheaper devices simply won't be able to connect to MFP-enabled SSIDs. Organizations must carefully consider the balance between security and device compatibility when deciding whether to enable MFP on their wireless network.

It's important to note that MFP is mandatory for devices operating on the 6 GHz frequency band, ensuring a higher level of security for networks using this newer spectrum.

Reducing Your Hacking Risk

In the world of Wi-Fi, security and performance are often seen as opposing forces. Tighten security too much, and you risk hampering user experience. Prioritize performance at all costs, and you might leave your network vulnerable to attacks. The key is finding the right balance, and understanding that a high-performing network can actually contribute to better security.

You might be wondering, "How does a fast network make me more secure?" The answer lies in human behavior. When your corporate Wi-Fi is slow, unreliable, or difficult to use, employees are more likely to seek alternatives. This could mean:

- Using personal mobile hotspots
- Connecting to unsecured public Wi-Fi networks
- Bringing in consumer-grade routers from home

"The Sidekick 2 gives you the fundamental performance of a wireless intrusion protection system (WIPS) out of the box. You can just walk around the building running this tool and it will show you what's doing what, what is misbehaving, then you can turn on the scanner and look at the frequencies to see if you have any Wi-Fi jammers."

Phil Morgan
Wi-Fi Security Expert, CTO/CSO, NC-Expert

Each of these “solutions” introduces new security risks to your environment. By maintaining a high-performing Wi-Fi network, you reduce the temptation for employees to circumvent your security measures in search of better connectivity.

By striking the right balance between security and performance, and by leveraging tools like Ekahau’s suite of products, you can create a Wi-Fi environment that is both secure and user-friendly. This approach not only reduces your hacking risk but also ensures that your network remains an asset rather than a liability to your organization.

Securing Your Network with Ekahau

Maintaining a secure wireless environment requires vigilance, but identifying potential security risks doesn’t have to be complicated. A quick survey with the powerful Ekahau Sidekick 2 device is all it takes to expose vulnerabilities across your Wi-Fi network.

Once you’ve completed a survey collecting data at your site, Sidekick 2 immediately flags any security threats: Rogue access points, interference sources, encryption concerns — they’re all visualized in the Survey application’s security tab for rapid threat assessment. After syncing your survey data to the cloud, Ekahau Optimizer provides a comprehensive security report for each of your network sites, which you can also download for offline access and sharing.

Regular security checkups are critical for keeping your data, users, and networks safe from evolving threats. Ekahau streamlines this vital best practice, guiding you from security scans all the way through implementing properly secured configurations. No assumptions, no guesswork — the most straightforward method of validating and fortifying your Wi-Fi security.

Chapter 5: When It's Time to Redesign

Introduction to Redesign

Even optimized networks eventually need upgrades or redesigns. But don't throw away your access points just yet! In this chapter, we'll cover the steps you can take to mitigate the challenges of an aging or poorly-designed network before moving forward with a complete redesign.

There are several key factors that drive the need for Wi-Fi network redesigns:

- **Poor Wi-Fi Design**
  Sometimes networks are just designed poorly from the start, resulting in coverage gaps, interference issues, and sub-par performance from day one. You might have inherited a network like this, or your former self might have thought, "APs just go on the ceiling, right?" Even after optimization, there's only so much you can do to fix a bad design.

- **New Technology Standards**
  The Wi-Fi ecosystem is constantly evolving, with new standards introducing higher throughputs, increased capacities, and enhanced security features like WPA3. Upgrading your infrastructure enables you to unlock new wireless capabilities and take advantage of new performance benefits.

- **Increased Bandwidth Demands and Changing Workplace Dynamics**
  Video calls, HD streaming, bandwidth-heavy applications, and data consumption are all on the rise. What was a high-performing network during deployment may become a bottleneck as bandwidth demands escalate exponentially. Redesigns allow you to scale up infrastructure to meet contemporary throughput requirements. Workplace models like hybrid environments, open office layouts and hotdesking, and increased mobile device usage can dramatically impact Wi-Fi requirements. A redesign optimizes the network for shifts in usage patterns and device populations.

- **Evolving Facilities**
  Physical environment changes like office relocations, building renovations, and new construction all impact RF signal propagation. A facility's structural evolution necessitates redesigning wireless infrastructure for maximum performance in the new environment.

If any of these scenarios resonate with your current network challenges, it may be time to consider a partial upgrade, network refresh, or complete redesign. In the following sections, we'll dive deeper into each of these approaches, helping you determine the best path forward for your organization's unique Wi-Fi needs. With the right strategy and tools, you can transform your wireless network into a high-performing, future-proof asset that drives your business forward.

Product Highlight: Ekahau AI Pro Online

At Ekahau, we build the best Wi-Fi tools on the planet. So when it comes time to redesign your network, we've got you covered.

With Ekahau AI Pro Online, you can turn Wi-Fi survey data into the most accurate RF model of your environment. By understanding how the RF performs in your space, with the help of some AI machine learning, you can accurately predict how modifying, adding, or replacing access points will impact your network performance.

One of the standout features of AI Pro Online is its ability to provide the most accurate RF model without the need for manual wall drawing or measuring the attenuation impact of objects. The tool leverages real-world attenuation values from your site's walls, desks, shelves, and all other signal-impacting materials, gathered during the Sidekick 2 survey. This, combined with our advanced AI propagation model, forms the foundation for your redesigns, resulting in the most accurate network visualizations possible.

AI Pro Online is the perfect tool for any network redesign scenario. Whether you're looking to upgrade your network to the latest 6 GHz technology or simply aiming to extend the life of your existing network by addressing coverage gaps, Ekahau AI Pro Online simplifies the process and ensures optimal results.

With its intuitive interface and powerful AI-driven modeling capabilities, AI Pro Online enables you to create, optimize, and visualize Wi-Fi designs in real-time, all from the convenience of your web browser. Instantly see the impact of moving or adding access points, and simulate changes to your network configuration with just a few clicks.

Partial Network Upgrades

In the world of Wi-Fi, coverage gaps can be a real headache, especially when they occur in high-profile areas like the CEO's office. (Why is it always the CEO's office?) But before you start considering a complete network overhaul, let's explore the power of partial upgrades.

In some cases, addressing significant primary or secondary coverage gaps doesn't require a massive investment in an all-new wireless infrastructure. Instead, a partial upgrade may be all that's needed to improve your Wi-Fi performance. This targeted approach involves strategically installing additional access points and updating your channel plan to optimize coverage and minimize interference.

By focusing on specific problem areas, you can extend the life of your current infrastructure while improving overall network performance. This means you can tackle those pesky dead zones or slow spots without the expense and disruption of a full-scale redesign.

Using Ekahau AI Pro Online, you can easily identify coverage gaps and simulate the impact of adding new access points to your existing network. The tool's advanced AI-driven modeling capabilities allow you to visualize the optimal placement of additional APs, ensuring they provide the desired coverage without introducing new issues.

Once you've determined the ideal locations for the new access points, AI Pro Online helps you update your channel plan to optimize performance and reduce co-channel or adjacent-channel interference. The tool's intelligent algorithms consider factors like signal strength, channel overlap, and AP density to recommend the best channel assignments for your updated network.

Access Point Upgrades

When your wireless network starts to show its age, it may be time to consider a "rip-and-replace" approach. In many cases, refreshing your network can simply involve replacing your aging access points with newer models while keeping the existing cable infrastructure in place.

This type of rip-and-replace is ideal when your current AP locations are still suitable for your coverage and capacity needs, but the hardware itself is no longer up to par. Here are a few reasons why you might consider this approach:

- **Outdated technology:** If your APs are more than a few generations old, they may not support the latest Wi-Fi standards. Plus, the latest APs take advantage of newly unlocked 6 GHz spectrum, which can be a game-changer for minimizing interference and unlocking wider channels for higher throughput. Upgrading to newer APs can bring immediate performance and security benefits without the need for a full-scale redesign.
- **End-of-life equipment:** As APs reach the end of their supported lifespan, they may no longer receive firmware updates or security patches. Replacing these devices with newer models ensures that your network remains secure and compatible with the latest client devices.
- **Improved performance:** Newer APs often come with more advanced features, like support for faster modulations, OFDMA, MU-MIMO, beamforming, and higher antenna counts, which can significantly improve performance and capacity, even without changing the physical placement of the devices.

When planning an access point upgrade, Ekahau AI Pro Online takes the guesswork out of replacing your wireless infrastructure. Our software allows you to accurately simulate the impact of replacing your existing access points with new models, all without having to physically install a single device. Whether you're switching vendors or just upgrading your APs to the latest flagship model, AI Pro Online has you covered.

By replacing aging APs with newer, more advanced models and using Ekahau AI Pro Online to optimize your configuration, you can achieve significant performance and security improvements while minimizing disruption to your environment.

Full Redesigns

Sometimes, a simple refresh or partial upgrade just won't cut it. When your wireless network is struggling to keep up with the demands of your users, or your environment has undergone significant changes, it may be time to consider a full Wi-Fi redesign. This comprehensive approach involves rethinking every aspect of your wireless infrastructure, from AP placement and cabling to technology choices and configuration settings.

A full redesign can be a daunting prospect, but it's also an opportunity to create a truly modern, high-performing Wi-Fi network that's tailored to your organization's unique needs.

To streamline and optimize this critical redesign process, harness the unparalleled capabilities of the most powerful Wi-Fi software tool available — Ekahau AI Pro Online. This cutting-edge solution allows you to:

- **Model your environment with precision:** Use your Sidekick 2 survey data to create a highly detailed, accurate representation of your physical space, taking into account walls, obstacles, and other factors that impact Wi-Fi performance.
- **Simulate and optimize AP placement:** Determine the ideal locations for your access points, ensuring optimal coverage, capacity, and performance throughout your environment.
- **Evaluate technology options:** Compare different Wi-Fi standards, AP models, and antenna configurations to find the best fit for your needs and budget.

So, if your current Wi-Fi is holding you back, don't be afraid to start from scratch. With a full redesign powered by Ekahau AI Pro, you can create a wireless network that's faster, more reliable, and better equipped to support your business now and in the future.

Assessing Your Aging Infrastructure

If you have ancient APs…you might have a total aging infrastructure issue. When considering a rip-and-replace upgrade for your Wi-Fi network, it's crucial to assess your existing infrastructure to ensure that your new access points won't be throttled by outdated switches, cabling, or power limitations.

Switches

APs are connected to switches on the local area network (LAN), which play a vital role in the performance of your Wi-Fi network. Older-generation switches will be unable to keep up with many network demands.

Most modern switches support 1 Gbps speeds, which is sufficient for most current Wi-Fi deployments. However, with the advent of Wi-Fi 7, combined theoretical throughputs of up to 14.4 Gbps may be achievable. In such cases, multi-gigabit switches may be necessary (for the first time in the history of Wi-Fi) to avoid bottlenecks.

Cabling

The type and quality of your network cabling can significantly impact the performance of your Wi-Fi network. If you're using outdated cabling that only supports 100 Mbps, you won't be able to take full advantage of the high data rates offered by newer Wi-Fi standards. Modern Ethernet cables, such as CAT5e, CAT6, or higher, can support gigabit or multi-gigabit speeds and are recommended for optimal performance.

If you need new cabling, you will not be able to save your budget by going for a rip-and-replace vs a full network redesign. So if you are going to need to pull cables, make sure those APs are in the best possible locations for your network!

Power over Ethernet (PoE)

PoE allows network cables to carry both data and power to devices like APs, cameras, and other networked equipment. With PoE, you only need one cable to provide both data connectivity and power to your APs.

When upgrading to newer APs, it's essential to ensure that your switches can provide adequate PoE power. Older APs typically required around 15.4 watts (802.3af standard), while modern APs often need 30 watts (802.3at standard) or more. Some Wi-Fi 6E tri-band APs may even require PoE++, which delivers more than 30 watts.

Other Considerations

While switches and cabling are critical components, other factors can also affect the end-to-end performance of your Wi-Fi network. These include:

- **Firewalls and routers:** The performance of your firewalls and routers, especially when routing traffic, can impact overall network speed.
- **Broadband limitations:** The capacity and quality of your internet connection can limit the maximum throughput achievable by your Wi-Fi network.

When planning a rip-and-replace upgrade for your Wi-Fi network, it's essential to evaluate your entire infrastructure stack. If your APs are ancient, you will want to look into your switches and cabling to ensure your rip-and-replace won't hit bottlenecks from these technologies!

Conclusion

In the world of Wi-Fi, a network's success is determined not just by its performance on launch day, but by its consistent performance and reliability from Day 2 to Year 5 and beyond. During this critical period, organizations must navigate the challenges of evolving requirements, shifting usage patterns, and emerging security threats.

But with the right tools and a proactive approach, you can not only overcome these obstacles but also unlock the full potential of your wireless network. This proactive approach ensures a consistently high-quality user experience and maximizes the return on your wireless infrastructure investments.

Ekahau's suite of tools provide unparalleled visibility into your network's performance and security. These tools empower you to continuously monitor, optimize, and troubleshoot your Wi-Fi infrastructure, ensuring that it remains high-performing, secure, and future-ready.

Whether you're managing an existing network or planning a brand-new one, Ekahau has you covered. For those starting from scratch in a location without Wi-Fi, or even planning for a space that hasn't been built yet, our advanced Wi-Fi tools allow you to design and visualize your future network with precision. From Day 0 planning to Year 5 optimization and beyond, Ekahau provides the comprehensive solutions you need to create and maintain amazing Wi-Fi networks.

Network Decision Tree

Navigating the complexities of Wi-Fi network management can be challenging. Is it time for an upgrade? Should you optimize your current setup? Or is a complete redesign in order? Whether you're dealing with the dreaded slow zones, mysterious dead spots, or the ever-frustrating intermittent issues, this decision tree will help you chart the best course of action.