LEARNING MADE EASY

Ekahau Special Edition

Wi-Fi Network Design

for dummies®
A Wiley Brand

See how Wi-Fi functions

Implement your own Wi-Fi network

Get ten Wi-Fi performance boosts

Brought to you by

ekahau
WIRELESS DESIGN

Joel Crane
Bryan Harkins
Jussi Kiviniemi
Jerry Olla
Chris Harkins

About Ekahau

Ekahau enables the designing of wireless networks simpler and smarter.

As a pioneer in the Wi-Fi industry, Ekahau was first to develop and introduce the original enterprise-grade site survey and planner tool to market. Since then, it has become the global leader in Wi-Fi network design solutions from wireless local area network planning to troubleshooting.

Ekahau is headquartered in Reston, Virginia, and has much of its R&D and product-related functions in Helsinki, Finland. Visit **www.ekahau.com** for more information.

Wi-Fi Network Design

Ekahau Special Edition

by Joel Crane, Bryan Harkins, Jussi Kiviniemi, Jerry Olla, and Chris Harkins

for dummies®
A Wiley Brand

Wi-Fi Network Design For Dummies®, Ekahau Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN: 978-1-119-45056-6 (pbk); ISBN: 978-1-119-45067-2 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor: Carrie A. Burchfield

Acquisitions Editor: Katie Mohr

Editorial Manager: Rev Mengle

Business Development Representative: Ashley Barth

Table of Contents

INTRODUCTION 1

About This Book 1

Icons Used in This Book 2

Beyond the Book 2

CHAPTER 1: **Wi-Fi: It's Everywhere** 3

Business Wi-Fi 3

Industrial and Manufacturing Wi-Fi 4

Medical and Assisted Living Wi-Fi 5

Education Wi-Fi 6

CHAPTER 2: **Understanding Wi-Fi Technology** 7

Frequency 7

Wi-Fi Is Half-Duplex 8

Data Rates 9

Acknowledgements 9

Signal Strength and Signal-to-Noise Ratio (SNR) 9

Unlicensed Spectrum Bands 10

Channels and Channel Bonding 10

Overhead 11

CHAPTER 3: **The Fundamentals of Better Wi-Fi** 13

Measuring Signal Strength 13

Understanding Noise 14

Understanding Signal-to-Noise Ratio 15

Using Spectrum Efficiently 16

The Effect of Technology Choices and Configurations 17

Choosing Automatic versus Manual Wi-Fi Configuration 17

CHAPTER 4: **Building an Awesome Wi-Fi Network** 19

Introducing the Wi-Fi Network Design Life Cycle 19

Defining the Requirements 20

Designing the Plan 21

Creating a predictive design 21

Performing a pre-deployment site survey 22

Deploying and Optimizing 22

Documenting, Monitoring, and Maintaining the Network 23

CHAPTER 5: **Troubleshooting Wi-Fi Problems** 25
Applying Logic and Discipline 25
Common Causes of Wi-Fi Problems 26
User device problems 26
Network problems 27
Resolving Common Problems 27
Driver problems 27
User-created problems 28
Troubleshooting with Packet Analysis 28
Troubleshooting with Spectrum Analysis 29
Solving Problems by Redesigning the Network 30
The “no-survey” problem 30
The “requirements changed over time” problem 31

CHAPTER 6: **Ten of the Biggest Wi-Fi Mistakes (and How to Avoid Them)** 33
Not Conducting a Survey 33
Poor Design 34
Improper Installation 34
Just Adding More APs 34
Full Transmit Power 35
Wired Infrastructure Issues 35
Authentication Problems 35
Firmware Update Problems 35
Using the Wrong Data Rates 36
Using Wide Channels Incorrectly 36

CHAPTER 7: **Ten Wi-Fi Performance Boosts** 37
Understanding and Designing for Requirements 37
Checking and Building Your Wired Network 38
Maximizing Signal Strength 38
Finding a Better Place for Your Gear 38
Choosing Channels Wisely 39
Using Just Enough Power 39
Using 5 GHz More and 2.4 GHz Less 39
Maximizing Airtime Efficiency 40
Getting Modern Devices 40
Learning More about Wi-Fi 40

Introduction

Wi-Fi is everywhere, from warehouses to waiting rooms and from conference centers to your local mall. Employees and consumers alike are increasingly expecting Wi-Fi availability and Internet access wherever they go — and if it doesn't work right, or isn't available, they won't be shy about letting you know and going elsewhere to get it.

If your business offers Wi-Fi — or needs to in the near future — you might be feeling a little overwhelmed by the prospect of planning and implementing a wireless network. That's understandable. There's a lot to think about. Designing and implementing a Wi-Fi network the right way can satisfy your stakeholders and minimize future problems. Getting it wrong can be a headache for everyone from your CEO to your IT department staff.

But don't worry. We've got you covered. Welcome to *Wi-Fi Network Design For Dummies*, Ekahau Special Edition.

About This Book

This book is designed for a company's top-level decision makers (such executives and owners) and for the people who make the IT decisions (such as network engineers and IT managers). It provides an overview of Wi-Fi networking, including expert advice for creating or expanding a Wi-Fi network the *right* way, with careful planning and analysis. If you read this book all the way through, you discover

- How different business types use Wi-Fi
- How Wi-Fi functions
- What factors affect network performance
- How to build a better Wi-Fi network
- The key components of a good network plan
- How to resolve some of the most common problems

Icons Used in This Book

To make it easy to navigate to the most useful information, these icons highlight key text:

REMEMBER

Take careful note of these key takeaway points.

WARNING

Watch out for these potential pitfalls on the road ahead.

TECHNICAL STUFF

Read these optional passages if you crave a more technical explanation.

TIP

Follow the target for tips that can save you time and effort.

Beyond the Book

After reading this book, you may want to learn more about Wi-Fi and consult with solutions providers who can help you get your Wi-Fi network off to a good start. One good place to start is Ekahau's training and video guide series: `www.ekahau.com/training/videos-guides`.

After you've used these materials to become more confident with your Wi-Fi project, check out the Products menu to learn about some tools that can make Wi-Fi planning and implementation a lot more painless and foolproof.

IN THIS CHAPTER

- » Thinking about how businesses and industry use Wi-Fi
- » Considering how medical facilities use Wi-Fi
- » Looking at Wi-Fi usage in education

Chapter 1
Wi-Fi: It's Everywhere

Wireless local area networks (often referred to as *Wi-Fi*) really is everywhere today, from your workplace to your child's school to your dentist's office. That's a huge change from only a decade or so ago, where wired networks were the default, and Wi-Fi was the "nice-to-have" alternative. They've effectively switched places, such that Wi-Fi is now the default, and wired networking supports it behind the scenes. Many new laptops don't even come with a wired network port anymore, in fact, because consumers just aren't demanding it.

The places where Wi-Fi is required vary as much as the people requiring it, so in this chapter, you examine the places Wi-Fi is used today, including some places that are less obvious.

Business Wi-Fi

Businesses began to install Wi-Fi and saw both productivity boosts and cost savings. Hardware costs were greatly reduced because they no longer needed to run a cable to each desk. After seeing the advantage of Wi-Fi, businesses couldn't go back.

Lately we're witnessing a massive transition from "wired by default" to "wired to support wireless." People no longer ask where to plug in; instead, they ask *how* to connect to the Wi-Fi.

As a result of the modern office space going wireless, users now want to connect their personal devices as well to take advantage of the company's Internet connection and save data usage on personal cellphone plans. The usage of personal devices on enterprise networks has grown to the point that it has its own name: Bring Your Own Device (BYOD).

The scope of BYOD began with Internet access, but it has grown to include access to corporate resources. If personal devices are to be allowed on the business network, they must meet the corporate security standards. Many organizations have implemented Mobile Device Management (MDM) to improve security and better manage devices on their network.

Industrial and Manufacturing Wi-Fi

Wireless networking has a long history of use in industrial and manufacturing operations. Decades before the carpeted spaces embraced wireless networking via the current 802.11 standards, warehousing and logistics systems were using old 900 MHz wireless equipment to track and monitor materials, products, and shipments.

Just as wireless has improved productivity in business networks, it has also improved productivity in industrial and manufacturing networks. Network owners and users alike are always looking for ways to leverage new technologies for greater efficiency and customer satisfaction.

From managing machines to tracking product shipments, Wi-Fi is an integral part of daily operations. In manufacturing environments, there may not be any local IT support staff, meaning that network implementations must be simple and robust. Remote management and administration of factory Wi-Fi devices is commonplace in these environments.

WARNING

Manufacturing and warehousing are also forced to deal with many types of obstructions not found in traditional office spaces. In addition to the sources of interference found in offices (microwaves, cameras, alarms, and so on), the business-critical machinery and lighting used in and around industrial and manufacturing networks produce radio frequency (RF) "noise" within the same frequencies used by Wi-Fi. This additional noise makes designing and implementing wireless networks more challenging than in an office space. Any implementation of wireless networking in an industrial environment must be done using enterprise-quality systems that can withstand dust and extreme temperature variations, as well as provide remote management capabilities. If the Wi-Fi is down here, business stops.

Medical and Assisted Living Wi-Fi

Long gone are the days of patients' charts hanging on the foots of their beds or in slots on their doors. Thanks to new patient privacy laws and newer technologies, medical staff members now typically access patient records electronically. Staff members can use Wi-Fi-connected tablets or laptops in patient rooms to enter information and retrieve test results.

The use of wireless technology has improved patient care, and it saves lives every day because it decreases the opportunities for human error. A sad phenomenon in the medical professions called "death by decimal" used to be all too common, wherein the caregiver would dispense the wrong amount of medication by not reading the charts correctly. For example, a dose of .01ml could be administered as .10ml — ten times the prescribed dosage, potentially placing a patient in grave danger. Wireless technology makes it possible for more aspects of patient care to be computerized, minimizing such errors. When dispensing medicine, for example, Wi-Fi allows the caregiver to scan the patient armband and have medical equipment dispense the correct amount of medication.

Wireless usage has expanded from just a few computers on wheels (COWs) a decade ago to a multitude of medical devices that all rely on Wi-Fi to collect and share information. The increase in devices needing connectivity has made designing and implementing Wi-Fi more challenging than ever before in medical environments. There are sources of non-Wi-Fi interference that must be designed around, and it's rare to find any hospital that uses some sort of frequency regulation.

Despite the challenges of wireless networking in healthcare, Wi-Fi must work flawlessly here. It is not merely a matter of business or customer satisfaction; timely access to data can save lives.

Wi-Fi in a medical facility isn't just for collecting and sharing medical data; patients and visitors use Wi-Fi, too, for Internet access and other forms of communication. Many patients entering the hospital or assisted living today are coming from generations that depend on Internet connectivity. Having reliable guest wireless networks available increases patient satisfaction. In long-term rehabilitation and assisted living situations, giving patients the ability to communicate with their offices, families, and friends improves their outlook and allows them to be productive while recovering.

Education Wi-Fi

Wireless communication has become an important part of how students access information for learning and testing. From kindergarten through graduate school, wireless networks have become as expected as homework and exams.

Today, many K-12 schools equip students with tablets or laptops as tools for learning. Wireless networks provide connectivity to student devices in classrooms, so they can access tests, lessons, digitized textbooks, and videos. Teachers can use the wireless network to push content to students, retrieve assignments, and track scores.

Educational Wi-Fi presents the challenge of user density; deploying a Wi-Fi network that can stream high-quality video to 30 student devices in one room is difficult, but achievable with careful network design and consideration.

Beyond providing a wireless connectivity by which students and staff access information, Wi-Fi enhances the learning opportunities for students of all ages. Wi-Fi in education removes communication barriers.

IN THIS CHAPTER

- » Learning how Wi-Fi functions
- » Exploring some factors that affect Wi-Fi performance

Chapter 2 Understanding Wi-Fi Technology

The Institute of Electrical and Electronics Engineers, IEEE, is an international, non-governmental body that creates industry standards. It has created a plethora of standards, supporting everything from megabit connectivity of the late 1990s with 802.11 and 802.11a/b, all the way into the hundreds of megabits per second with 802.11ac.

While wired networks use physical cabling as a transmission medium, wireless networking uses the air. Wired networking signals are contained in cabling, so they're rarely interfered with. Wireless, on the other hand, is completely different because it's "unbounded" by cables and commonly suffers from interference.

This chapter exposes you to some basic concepts that apply to wireless networking.

Frequency

Frequency specifies how quickly the wave oscillates. This is identical to how a sound wave changes pitch. In the context of wireless communication, the frequency is how long it takes the wave to oscillate, or go through an entire wave cycle in relation to one second. So, in 2.4 gigahertz (GHz), this means that the wave oscillates from the valley to the peak roughly 2,400 times a second. In 5 GHz, that is roughly 5,000 times a second.

In Figure 2-1, you see a low frequency waveform and a high frequency waveform. The shorter each wavelength, the higher the frequency.

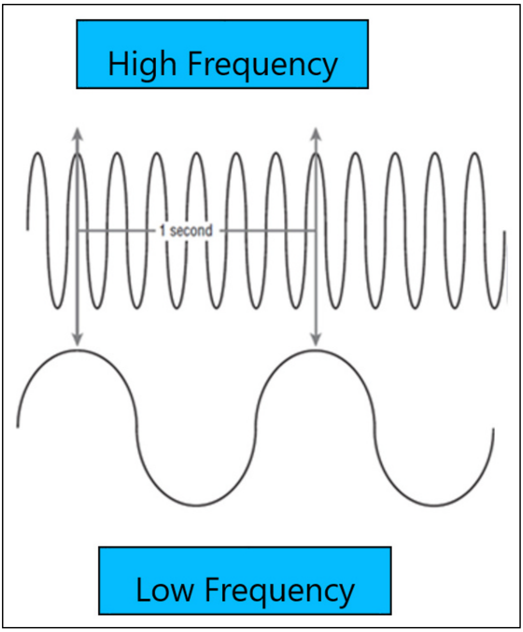


FIGURE 2-1: High and low frequencies.

Wi-Fi Is Half-Duplex

Ethernet cables can support *full-duplex* transmissions, which means they can send traffic bidirectionally on the same cable, at the same time. Wi-Fi, on the other hand is *half-duplex*, which means traffic can be transmitted in only one direction at a time. It's like a human conversation. If you and a friend say something at the same time, you cancel each other out.

Half-duplex limitations apply for an entire Wi-Fi channel: Only one device can talk on a channel at a time. Therefore, all devices on a channel within range must take turns in a process called *carrier-sense multiple access with collision avoidance* (CSMA/CA) in which Wi-Fi devices compete for the opportunity to transmit on the channel.

Data Rates

When Wi-Fi devices transmit, they have many data rates to choose from. For example, an 802.11g device can transmit at 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 megabits per second (Mbps). The advantage of slower data rates is that they are robust at lesser signal strengths; faster rates are more difficult to understand, and require better signal strength. If a device doesn't understand a received transmission, the sending device will retransmit the same data but usually at a slower data rate.

REMEMBER

Devices constantly adjust their data rates to help the receiving device on the other end understand them. When devices are far away from each other, or if there is a lot of background noise, they'll fall back to slower and slower data rates.

Acknowledgements

When a Wi-Fi device receives data, it must transmit an *acknowledgement* (also known as *ACK*) to let the transmitting device know that it received the data. If the receiving device doesn't understand the data, it won't transmit an ACK. The transmitting device will notice, and it will retransmit the data again and again until the receiving device responds with an ACK.

Signal Strength and Signal-to-Noise Ratio (SNR)

To communicate, wireless devices need to be able to hear each other. The better they can hear each other, the faster data rates they'll be able to use, which means that *signal strength* is very important. However, signal strength alone isn't a measurement of transmission quality. You must also look at signal-to-noise ratio (SNR).

Even in a quiet room, you can still hear background noises, from traffic rumbling on the nearby street to birds chirping in the trees to your AC unit turning on and off. Similarly, in radio frequency (RF) data transmission, behind the data itself is a *noise floor,* which is the extraneous noise in the radio spectrum. The SNR is a measurement of how much signal there is compared to how much background noise. A higher SNR results in greater transmission efficiency. We cover these factors in Chapter 3 in greater detail.

Unlicensed Spectrum Bands

Most parts of the RF spectrum are *licensed,* meaning that you must purchase and hold a license to operate in that frequency band. For example, a cellphone company might purchase a license to operate in the 1.7 GHz band. If others were to interfere with that band, they would be fined.

Both 2.4 and 5 GHz are *unlicensed spectrum,* which means that as long as you follow basic rules, you don't need a license to transmit in those frequency bands. This makes both 2.4 and 5 GHz convenient for things like baby monitors, cordless phones, wireless video cameras, and of course, Wi-Fi.

WARNING

The bad side of unlicensed spectrum is that you must be willing to accept interference if you operate in it. This is why ordinary home and office equipment like cordless phones can interfere with Wi-Fi. More importantly, other Wi-Fi devices — for example, your neighbors' — will likely interfere with yours.

Channels and Channel Bonding

The frequency space in which Wi-Fi works is divided into *channels.* In 2.4 GHz, there are either 11 or 14 channels (depending on local regulations). There's a major problem, though: Most of them partially overlap. Putting two networks on partially overlapping channels will result in interference, so the recommended solution is to use the three non-overlapping channels: 1, 6, and 11. The 5 GHz band is a lot bigger; there can be up to 25 non-overlapping channels available, depending on local regulations.

REMEMBER

Wi-Fi is half-duplex. Each channel's throughput is limited, and after the channel has been saturated, adding another access point on that channel won't increase throughput. The only way to add more throughput is to add an access point on another channel. In 2.4 GHz, where there are only three non-overlapping channels, this is challenging. In 5 GHz, with up to 25 channels, it's easier but can still be an issue in very dense environments.

Channel width varies depending on the wireless standard being used. 802.11 and 802.11b used 22 megahertz (MHz) channels. 802.11a and 802.11g were slightly narrower at 20 MHz, but things changed with 802.11n. *Channel Bonding* in 802.11n allowed two 20 MHz channels to be combined to make a 40 MHz channel. This offered more throughput, just like a 4-lane highway accommodates more traffic than two lanes.

802.11ac expanded on this concept by offering 20, 40, 80, and even 160 MHz channels via channel bonding. While wider channels do offer higher speeds, remember that only one device can transmit on a channel at a time. In environments with a lot of access points, you'll quickly run out of wider channel options. An 80 MHz channel consumes four 20 MHz channels, eating up available frequency space. Usually, it's best to start with 40 MHz channels, and then if channels become scarce, back off to 20 MHz channels.

Overhead

You've probably wondered why your network adapter is connected at 54 Mbps to the network, but when you perform a throughput test (such as speedtest.net), you notice that you're only getting 10 or 25 Mbps of throughput. Why is that?

First, your Wi-Fi network may be faster than your network provider's Internet connection plan. For example, you may only have purchased a 10 megabit Internet connection plan, so your 54 megabit Wi-Fi connectivity isn't the bottleneck.

The other reason is overhead. The signaling rate is 54 Mbps, which is the rate at which your machine is transmitting. However, there's a lot of management overhead or non-data involved in the transmission and even some tiny bits of dead air between transmissions.

REMEMBER

For Wi-Fi to work smoothly, management overhead must have these components:

- **Beacon frames:** Transmitted by an access point at regular intervals to advertise a network
- **Probe request frames:** Transmitted by clients looking for available access points
- **Probe response frames:** Transmitted by an access point, replying to a client's probe request
- **Acknowledgement frames:** Transmitted by a station to confirm that data was received
- **Interframe spaces:** Tiny bits of idle time between transmissions
- **Network allocation vector (NAV):** A timer that stations set and wait to expire before transmitting to avoid interrupting other stations on the channel

It takes a lot of extra communication for wireless network interface controllers (NICs) to work together, and ultimately, that management overhead eats away at throughput. So, in Chapter 7, we give you some ways to minimize overhead and maximize transmission efficiency.

IN THIS CHAPTER

- Defining signal strength, RF noise, and signal to noise
- Determining spectrum usage
- Learning the impact of technology choices
- Considering automatic and manual Wi-Fi configurations

Chapter 3 The Fundamentals of Better Wi-Fi

In this chapter, you explore the building blocks of better Wi-Fi, such as signal quality and proper frequency reuse. Although most access points and controllers are capable of configuring features like channel selection and transmission power automatically, some potential performance enhancements are found by understanding and strategically configuring these settings manually.

Measuring Signal Strength

In Wi-Fi, signal strength is measured in either milliwatts (mW) or decibels relative to a milliwatt (dBm). While mW is great for representing things like transmit power, dBm does a better job of describing Wi-Fi's big changes in signal strength without requiring a ton of decimal places. Take a look at Table 3-1 to see how they compare.

TECHNICAL STUFF

Although dBm makes more sense for measuring signal strength, it has a couple of quirks:

- Wi-Fi works with an incredibly small amount of power, so for Wi-Fi, dBm dips well into the negatives. Thus, -90 is a much lower signal strength than -65 dBm.

- It isn't a linear scale; it's logarithmic, which means that small number changes in dBm can mean big changes in signal. That's dBm's advantage. Here are two examples:
  - **+3 dB, -70 to -67 dBm:** Double the signal strength
  - **-3 dB, -70 to -73 dBm:** Half the signal strength

TABLE 3-1 Wi-Fi Signal Strengths in dBm and mW

Decibels Measured (dBm)	Milliwatts (mW)
-30 dBm	0.001 mW
-70 dBm	0.0000001 mW
-90 dBm	0.000000001 mW

REMEMBER

You need to have a certain amount of signal for devices to reliably understand incoming transmissions. If the incoming transmission is too quiet, the receiving device won't understand what it heard, and it won't transmit an Acknowledgement (ACK), thus causing a retry.

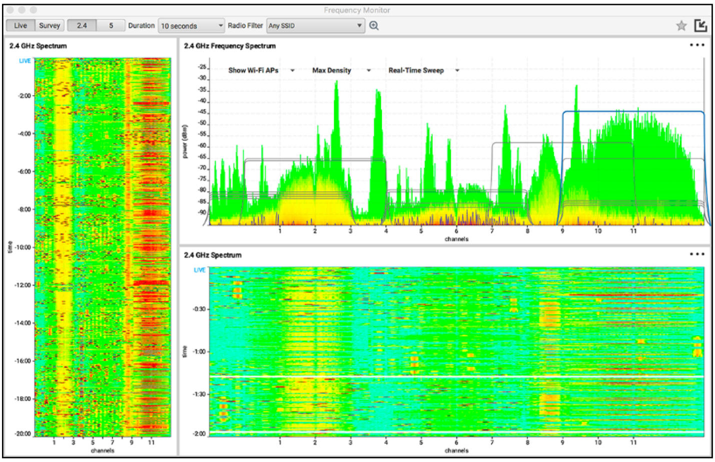
Different network applications require a certain amount of reliability (that is, sufficiently few retries) to work properly. For example

- **Web browsing, instant messaging, email:** These services can put up with a few retries or the occasional lost data frame, so -70 dBm is a good starting point.
- **Streaming video and VoIP:** These services require very consistent and timely packet delivery to work properly, so -67 or better is usually required.

Understanding Noise

Background noise and noise from other devices that are transmitting make it difficult for Wi-Fi devices to hear each other. In the context of Wi-Fi, *noise* is any signal that isn't Wi-Fi. This could be a microwave oven, a cordless phone, a video transmitter on a quadcopter, or a Bluetooth device. Ultimately, they're signals that Wi-Fi isn't able to demodulate, so it's just noise to the Wi-Fi device.

Both background noise (usually known as the *noise floor* as we mention in Chapter 2) and noise from interfering devices are visible with a spectrum analyzer — a device that can detect and visualize radio frequency (RF) energy, so you can identify and locate the source. In Figure 3-1, you see a spectrum analysis visualization in the Ekahau Site Survey and 3D Planner.

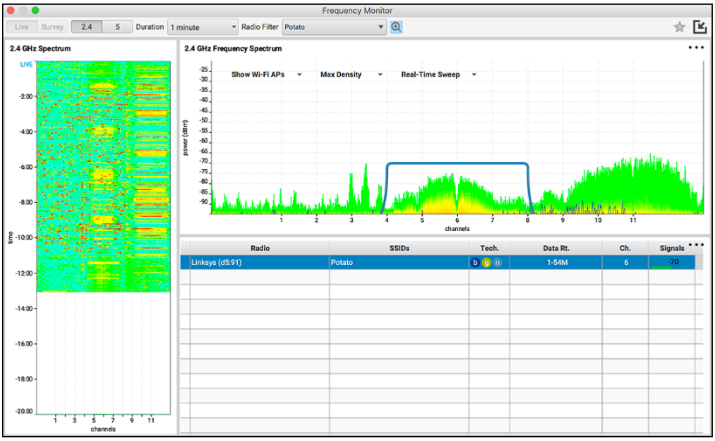


Duration 10 seconds
Radio Filter Any SSID

FIGURE 3-1: A spectrum analysis visualization in Ekahau Site Survey and 3D Planner.

Understanding Signal-to-Noise Ratio

A low signal-to-noise ratio (SNR) means that there isn't enough signal to overcome the background noise. Just like people having a conversation, Wi-Fi devices need sufficient signal strength to overpower the background noise to have an efficient conversation. Best practices require a minimum SNR of 20 or 25 dB to achieve high data rates, which is usually achieved when the receiving station has -70 dBm of signal strength, if the noise floor is -95 dBm (which is very common in an office). As shown in Figure 3-2, the SNR would be 25 dB.



Duration 1 minute

Radio Filter Potato

Radio	SSIDs	Tech.	Data Rt.	Ch.	Signals
Linksys (d5:91)	Potato	b g n	1-54M	6	-70

FIGURE 3-2: An SNR of -25 dBm.

Voice transmissions usually require a better SNR of 28 dB, meaning that -67 dBm of signal would be required if the noise floor was -95 dBm. What if the noise floor was higher, such as at -80 dBm? To achieve an SNR of 28 dB, the signal would have to be -52 dBm.

TIP

Higher SNR can be achieved in a number of ways:

- Improving the placement of the Wi-Fi routers/access points
- Increasing transmit power on Wi-Fi devices (but remember to stay within legal power levels)
- Changing the channel to avoid noise

Using Spectrum Efficiently

Wi-Fi, as used today, works in two frequency ranges: 2.4-2.5 GHz (referred to in Wi-Fi as the 2.4 GHz band) and 5.15-5.875 GHz (referred to in Wi-Fi as the 5 GHz band). As we mention in Chapter 2, there's a limited amount of bandwidth space to use in Wi-Fi. Getting the most out of that space isn't always easy, due to RF noise and other competing Wi-Fi networks. In addition to working around noise, you need to carefully reuse channels on your network to keep same-channel coverage cells from having to take turns talking.

The Effect of Technology Choices and Configurations

Adding new technology to a network that must also support legacy devices can have an impact on the network. Older devices can't communicate at the same speeds as newer devices; they take longer to transmit the same amount of information. Because only one device can access the channel at a time, the older devices can slow down the network by using the channel more than their fair share of the time. For example, an 802.11g client device may only transmit at 54 Mbps, but an 802.11ac client can theoretically transmit at 800 Mbps. Even in a best-case scenario, the 802.11g device will take more than 15 times longer to transmit the same amount of data as the 802.11ac device.

In addition, some newer devices aren't able to reach the data rates that you would expect from them. Internet of Things (IoT) has introduced a lot of small battery-powered devices, such as watches and fitness monitors, which struggle with battery life. To save battery power, manufacturers might implement 802.11b instead of 802.11n, which would consume more power. Mixing legacy technology with new technology is like putting modern sports cars and antique cars from the 1930s on the same roads. Ultimately, the modern cars will be drastically slowed down by the antique cars.

Choosing Automatic versus Manual Wi-Fi Configuration

With all that IT professionals have on their plates, it's nice to have some devices that just work when you plug them in, without a lot of configuration hassle. Many wireless access points and other devices answer this request by providing automatic channel and power selection. These features allow the access points to automatically configure their own channels and maximum transmit power settings. You, as the administrator, can set thresholds that force changes when certain events occur, perform configuration changes on a schedule, or even turn the automatic settings off once the access points have reached a workable configuration.

WARNING

But, of course, with automatic setups, some problems still exist:

- Access points are usually placed in the network with no planning, with the assumption that the automatic features will make up for the lack of planning. This leads to the wrong amount of access points being deployed and to access points being deployed in the wrong places. Even with automatic tuning, proper design is required.
- The algorithms that controllers and access points use to configure settings are proprietary and sometimes don't provide a satisfactory result. Each vendor has its own criteria for automatic configuration decisions. While a vendor might consider noise, neighboring networks, and the amount of connected clients, it may force changes to one access point that necessitate changes to others as well, causing a configuration change ripple across the network. In a densely populated urban area, the changes might happen so often that they interrupt client devices, which must reconnect after each change.

Automatic configurations can still save a lot of time and effort if they're used in the right situations and if they're configured to modify the network as needed. It's even possible (and time-saving) to use automatic features once for an initial network, and then turn them off once the automatic configuration is complete.

On the other hand, manual planning enables you to configure each access point according to your network design. It takes more work to do that, but it's the preferred method for typical high-density deployments and demanding environments such as warehouses and manufacturing plants. With this method, you're assured that configurations will stay locked in place and under your control.

A predictive network planning tool can help you quickly develop channel plans and strategize the maximum transmit power settings. Then you simply follow your network design when you deploy the network. The downside? If interference is introduced, or if an access point stops working, your network won't be able to dynamically address the problem on its own.

REMEMBER

The key takeaway from the debate of automatic versus manual configuration is that survey and design work are required for both types.

IN THIS CHAPTER

- Understanding the Wi-Fi network design life cycle
- Defining the requirements and developing your plan
- Deploying and optimizing the Wi-Fi network
- Documenting, monitoring, and maintaining the network

Chapter 4
Building an Awesome Wi-Fi Network

Suppose that you were hired to construct a new road. What would be your first step? Would you start by ordering the concrete? How would you know how much to order, what type to order, where to start pouring it? No, your first step would be to carefully plan, so you would know what supplies and equipment you needed. The same wisdom applies to building a Wi-Fi network. To avoid costly mistakes, you wouldn't order network equipment until you had a proper plan in place.

To create such a plan, you begin by defining some requirements. In this chapter, we cover how to build an awesome Wi-Fi network. We explain the Wi-Fi design cycle and show you how its steps make for a great way of thinking about network creation and maintenance.

Introducing the Wi-Fi Network Design Life Cycle

The Wi-Fi network design life cycle is a way of thinking about Wi-Fi network creation as a repeatable process with well-defined stages.

Following the steps in the Wi-Fi design life cycle will ensure the Wi-Fi network will be the right size for the environment and meet the needs of the users.

The basic stages in this process are as follows:

- Define the requirements.
- Design the plan.
- Deploy and optimize.
- Document, monitor, and maintain.

Wi-Fi technology is continuously evolving and improving, which is why network design is best represented as a life cycle rather than a linear start-to-finish methodology. Each time you finish the cycle, it's time to start over again, looking at the network in terms of new technologies and potential improvements.

By following this life cycle, you avoid the risks of blindly following general guidelines that might not be appropriate for your situation — things like "One access point (AP) per classroom" or "One AP per 2,000 square feet." The problem with these and other similar guidelines is that they don't take your specific needs into account. They're shortcuts, not properly designed solutions, and they'll likely either fail to meet your needs or end up costing you more than necessary. Failure to adequately plan is often the most expensive part of a Wi-Fi deployment.

In the remaining sections of this chapter, we explain each step of the Wi-Fi network design life cycle.

Defining the Requirements

Determining the requirements and constraints of a Wi-Fi network is a critical first step because it steers the rest of the project. Unfortunately, many people overlook this step entirely or fail to adequately define all requirements from both a business objectives and a technical standpoint.

REMEMBER

Be sure to speak to all stakeholders, including both end-users and leaders. The end-users often provide the most valuable information because the leaders may not have good insight into the applications needed or the end-user expectations.

Consider the requirements and constraints in these key areas:

- **Usage:** Who will use the network and how?
- **Coverage:** What is the physical area to receive coverage?
- **Capacity:** How much bandwidth is required to support the needed capacity?

After these questions have been answered, you're ready to proceed to the design phase.

Designing the Plan

Step 2 in the Wi-Fi network design life cycle is to create a comprehensive plan for the network design. The easiest way to accomplish this is to use a Wi-Fi planning application, such as *Ekahau Site Survey Pro.* You can input the defined requirements and constraints to put together a predictive design in 3D. The application helps you determine how many APs are needed, the suggested install locations, and the optimal radio configuration.

Creating a predictive design

Start by importing accurate floor plans into your Wi-Fi planning application.

TIP

You can optionally save time by using CAD files and automatically importing the walls.

REMEMBER

Wi-Fi works differently in areas where there are physical barriers than it does in wide-open spaces. You can enhance the 3D modeling accuracy by keeping that in mind and defining specific attenuation areas such as cubicles and open areas such as atriums. For example, the *Ekahau Site Survey Pro* planning tool includes multiple types of walls and attenuation area profiles, but you can also customize the existing database of attenuation objects or create your own object types to meet the needs of the project.

Next, you can automatically generate the network plan with the Auto-Planner feature. The Auto-Planner makes a suggestion of AP locations and configurations based on the previously defined requirements and constraints. When using *Ekahau Site Survey Pro,* you can then visualize the predicted coverage and performance.

You can manually adjust AP locations and configurations or manually create a network plan with simulated APs where desired.

Performing a pre-deployment site survey

Before you order all that equipment and do all that installation labor, one way to make sure that your plan is a workable one is to conduct a pre-deployment site survey. The goal of such a survey is to verify the predictive design's accuracy by measuring the radio signal propagation in the real world.

By conducting a pre-deployment site survey, you can be more confident of the number of APs and that their installation locations are optimal. The survey also helps you discover all the neighboring or rogue APs, as well as non-Wi-Fi related interference that could impact Wi-Fi performance.

You can perform a pre-deployment site survey through several possible methods. The most common is typically referred to as the *AP-on-a-stick* method. You power up an AP in one of the locations determined in the predictive design phase and determine its coverage area by performing a walk-through site survey. You fix that location in your survey tool. Then, you move the AP to the next location. Repeat this process as necessary until the predictive design's accuracy is confirmed.

An alternative testing method is to utilize a Wi-Fi signal generating device to measure the obstruction loss of individual objects in the environment, such as walls, doors, and furniture. After these attenuation measurements have been obtained, they can be input into the predictive design to improve the accuracy.

Deploying and Optimizing

After completing the predictive design and the pre-deployment site surveys (see the preceding section), you're ready to deploy the wireless network infrastructure. After you have physically installed and configured the network hardware, follow these steps:

1. **Verify the network coverage and performance by conducting a validation site survey throughout the entire site.**

2. **Analyze the results to verify that the network coverage, performance, and capacity requirements are met.**
3. **If the verification survey reveals that the network still doesn't meet the requirements, fine tune and resurvey until it does.**

Typical methods of optimization include fine-tuning the AP channels and transmit powers; strategically turning off unnecessary, interfering 2.4 GHz radios; and coping with sources of non-Wi-Fi interference.

Use the simulation and optimization features of your Wi-Fi planning application to perfect the network.

Documenting, Monitoring, and Maintaining the Network

After installation, you must continue supporting the network by documenting your work, monitoring the network's performance, and performing routine maintenance tasks. Fortunately, however, easy-to-use Wi-Fi tools simplify the following important operations:

- **Documentation:** Use the reporting feature to create complete documentation of the network installation, coverage, and performance with the click of a button.
- **Monitoring:** Problems will occur that can't be "seen" from the Wi-Fi Controller; you must investigate these on the client side. Use client-side survey and troubleshooting tools in combination with your Wi-Fi controller to keep your wireless network up and running.
- **Maintenance:** Conduct periodic site surveys to ensure flawless operation. Design for additional coverage or performance using the network planning features by simply opening the surveyed project file and adding simulated APs on the surveyed data.

IN THIS CHAPTER

- » Troubleshooting in a logical, disciplined way
- » Identifying the most common Wi-Fi problems
- » Resolving common problems
- » Troubleshooting with packet and spectrum analysis
- » Redesigning the network to solve problems

Chapter 5 Troubleshooting Wi-Fi Problems

Wi-Fi can be influenced by outside sources of interference, so you'll have to troubleshoot Wi-Fi issues sooner or later. This chapter presents some troubleshooting advice and techniques for bringing your network back to proper functionality as quickly as possible.

Applying Logic and Discipline

Just like a physician uses a process of elimination to resolve health problems, a wireless network engineer should also use a process of elimination to discover the root cause of Wi-Fi problems. You may have noticed that help desk technicians typically follow a script to resolve problems. This is due to the development of consistent problem-solving techniques.

TIP

Test simple theories first and then move on to more complex theories that are harder to test. For example, does the access point (AP) need to be rebooted? Try that first. Is there a new source of interference such as a microwave oven, cordless phone, or wireless video camera? Check the area with a spectrum analyzer to see if any interference is present. Has the switch that the AP is connected to failed? Check other devices on the same switch to see how widespread the failure is. Continue creating and testing theories until you find the source of the problem.

By following your own problem-solving techniques or "scripts," you can quickly resolve network issues and return to your normal work.

Common Causes of Wi-Fi Problems

REMEMBER

When network users have technical issues, they usually blame the Wi-Fi. The wireless network is the only piece of the puzzle that they're exposed to, so they only know to blame it. Sometimes it actually is the Wi-Fi's fault, and sometimes it's the user's device, the wired network, the Internet connection, or even a specific website or service. Until you investigate the problem, it's hard to know for sure.

User device problems

The first step in troubleshooting is to determine whether the problem resides on the user's device or somewhere on the network. Has anyone else reported issues? If you test the network, do you have the same problem? If the issue seems to only affect a single user's device, it probably isn't the network.

If the problem seems limited to the user device, check for common client device problems:

- **Have you turned Wi-Fi off and back on?** This can resolve common Wi-Fi adapter driver issues.
- **Have you tried turning the device off and back on again?** Yep, we're serious! Rebooting a device can also fix Wi-Fi adapter driver problems.
- **Is Wi-Fi turned on?** Older laptops had a physical "Wi-Fi" switch, and more modern laptops make it very easy to turn Wi-Fi off by accident via keypresses.
- **Have you installed any new software?** New software could disable the Wi-Fi adapter without the user knowing it.

- **Have you installed any updates?** While updates are usually a good thing, they can introduce new bugs.
- **Are you typing your Wi-Fi password correctly?** We've all typed passwords incorrectly, so this is worth asking!

Network problems

If more than one device is having the same problem, the underlying issue may be on the network. If the network has never worked well, then there's probably a design issue. If it has worked in the past, something must have changed, like a configuration change, an infrastructure update, or a new source of interference.

Some common network issues that can affect wireless are

- Invalid or expired security certificates
- Server or online service is down
- Not enough IP addresses in the DHCP pool
- Incorrect time setting on security devices
- Incorrect protocols allowed or blocked on a firewall
- Incorrect channel configurations on APs
- Incorrect transmit power settings on APs
- Wrong SSID and VLAN configurations on APs
- Router or switch misconfigurations

Resolving Common Problems

After you determine whether your issue is a device or the network, then take a look at some of the most common issues and how to resolve them.

Driver problems

One of the most common points of failure on a Wi-Fi-enabled device is the Wi-Fi adapter driver, which is the software that manages the Wi-Fi adapter. If it doesn't start properly, it won't be able to manage the device, causing the Wi-Fi adapter to fail. Disabling and reenabling the Wi-Fi adapter (turning the adapter off and back on) reinitializes the driver and fixes most driver quirks.

TIP

In the same vein, reboot the device entirely. It does the exact same thing, is easier for most users, and ultimately reinitializes the driver.

User-created problems

Users typically aren't computer or Wi-Fi experts, so they're bound to accidentally cause some problems on their own. Some common ones include

- Connecting to the wrong network
- Using the wrong username or passphrase
- Not inserting an access card into the card reader
- Leaving the wireless card turned off
- Blaming the WLAN for something else that's down
- Blaming the WLAN for denied access
- Trying to access blocked website
- Not being in the building (yes, this happens)
- Disabling automatic connection options

If the user can't get connected, have her walk you through the connection process to see if she's missing a step. Find out what resource she's trying to access, and make sure that she's authorized to access it. Check on the simple problems first, such as a Wi-Fi adapter that's disabled or switched off.

Troubleshooting with Packet Analysis

When wireless stations communicate, they transmit pieces of information called *packets* (although *frames* is a more technically accurate term when referring to 802.11). Packet capture and analysis can enable you to see conversations between 802.11 stations on a network. As packets are transmitted through the air, eavesdropping on those transmissions is easy (just like you can eavesdrop on two people having a conversation).

Packet analysis is most useful when you've exhausted remote and over-the-phone troubleshooting options. To perform a packet capture, you need a laptop, a Wi-Fi adapter that's capable of capturing packets, and software to capture and analyze the packet capture.

With all the necessary equipment assembled for the packet capture, you can start capturing packets, reproduce the problem (such as trying to connect a client device to an AP), stop the packet capture, and view the conversation between the AP and client to discover the problem. For example, if a user is seeing poor performance, a packet capture might reveal a high retransmission rate. If an 802.11 station transmits a data frame but never receives an acknowledgement in return, it will retransmit the data frame until an acknowledgement is received (up to 32 times). While some retransmissions are normal, anything above a 5 percent retransmission rate could be caused by interference, and packet analysis would reveal the retransmission rate.

Knowing what different kinds of conversations are supposed to look like will help you spot problems with packet analysis. For example, if you know what kinds of data the clients and APs exchange when a client tries to join a network, you'll be able to see why the client association failed. To become proficient in packet analysis, time and practice are required.

Troubleshooting with Spectrum Analysis

Whereas packet analysis enables you to view conversations between wireless stations, spectrum analysis gives you a look into the raw radio frequency activity in the spectrum. Whether it is a Wi-Fi device, Bluetooth, cordless phone, wireless video camera, or any other device that might transmit in the radio spectrum, a spectrum analyzer will show activity from it. Spectrum analysis is especially useful for troubleshooting interference issues.

For example, an observed 5 percent retry rate could be caused by non-Wi-Fi interference. While this interference won't be visible on a packet analyzer, a spectrum analyzer would enable you to detect the interference, determine the severity of the interference, and identify and locate the source. Figure 5-1 illustrates what a spectrum analyzer can show you.

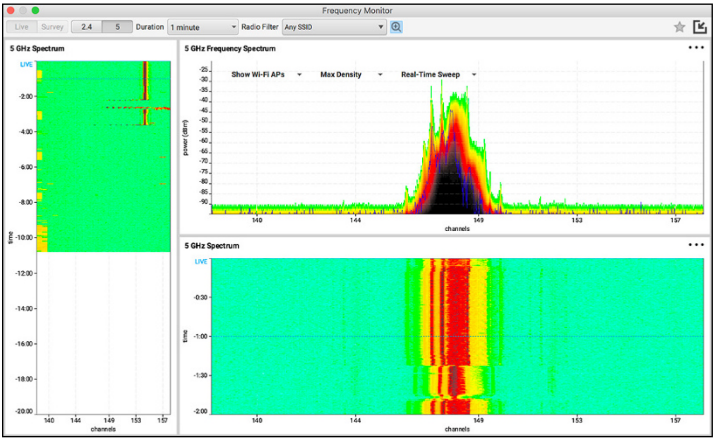


FIGURE 5-1: Interference from a wireless video camera on a spectrum analyzer.

Solving Problems by Redesigning the Network

Another place where the network can fail is in the network design itself. The network could've been improperly designed from the beginning, with poor AP placement, incorrect number of APs, and incorrect AP configurations. Even if the network was properly designed and deployed in the first place, the requirements of the network might have changed, requiring a redesign that accommodates more users with higher throughput needs.

The following sections explain two very common reasons why you might need to redesign a network: Either you didn't get it right in the first place (probably due to not doing a proper survey before deployment), or it used to be right but things changed over time.

The "no-survey" problem

Perhaps someone didn't perform a predictive network design on the network initially. Instead he just mounted APs where he thought they should be placed, and then relied on the automatic power and channel selection features, or the "magic" of Wi-Fi, to correct his mistakes. While such a design strategy might work in low-density deployments, such as a small or home office, it often creates frustrating, difficult-to-troubleshoot problems in larger installations.

WARNING

Skipping a predictive design (and the post-deployment validation survey that accompanies it) isn't a good idea, even in smaller deployments. Accepting the standard defaults doesn't factor in noise in the area, neighboring networks, or the amount of users. If you hear someone say, "The network worked great until we hired all these new people," then you have a good indication that you need to redesign the network.

The "requirements changed over time" problem

Perhaps the WLAN was designed properly, including a predictive design and post-deployment survey to validate the results. Over time, however, the number of devices on the network increased, and users shifted to higher-bandwidth network applications, such as Voice over Wi-Fi (VoWiFi), which weren't part of the original design. Because the network wasn't designed for high-bandwidth applications like VoWiFi, the user experience begins to suffer.

In such cases, you might need to completely redesign the network to meet the new requirements. It might mean new APs, new locations, and new supporting infrastructure like switching and cabling. It would definitely include new channel and transmit power plans. In some cases, the only way to resolve widespread wireless issues is to redesign the network.

IN THIS CHAPTER

» Identifying common design-phase mistakes

» Avoiding mistakes in installation and configuration

Chapter 6
Ten of the Biggest Wi-Fi Mistakes (and How to Avoid Them)

Successful Wi-Fi deployment and management is a science, not an art. You can do (or not do!) specific things to determine the success or failure of your endeavor. In this chapter, we give you a quick look at ten common mistakes in Wi-Fi and how you can avoid the problems they introduce.

Not Conducting a Survey

Without a pre-deployment survey, you won't know what the building is made of, where communication closets are, how high the ceilings are, or if there are any non-Wi-Fi sources of interference.

After you've deployed the network, you also want to do a post-deployment survey. Doing so helps you be confident that you have met all requirements. These surveys are covered in more detail in Chapter 4.

Poor Design

Even with a fantastic site survey, poor design will create problems for the network. Too many access points (APs) will cause excessive co-channel interference, and too few APs won't provide enough coverage. And don't forget about proper AP locations. Don't try to guess where they go. Always use a planning tool to determine the correct number of APs in the correct locations.

Improper Installation

APs are designed to be mounted in a certain way (usually on the ceiling) in open areas, as close to the client devices as possible. Putting them in equipment racks, in the ceiling between HVAC ducts, or underneath desks decreases their range and efficiency. You need to consider many specifics in AP installation, and that includes proximity to other APs, external antenna connections, and orientation.

For examples of improperly mounted APs (and a lot of laughs), visit `www.badfi.com`.

Just Adding More APs

Before Wi-Fi invaded the enterprise Wi-Fi space, it sent a few APs on reconnaissance missions to places like conference rooms. As demand for Wi-Fi grew, administrators began to simply add more APs. In the wired networking world, if you needed more connections, you would simply add more switches and Ethernet runs.

WARNING

Unfortunately, such an approach doesn't work well for expanding Wi-Fi networks. Connections are limited by channels and not by APs, so adding another AP won't increase bandwidth to support more users. Always perform proper design when adding new coverage areas.

Full Transmit Power

In the early days of Wi-Fi, the only design consideration was coverage. To provide coverage, engineers would mount one AP in the middle of a warehouse or other area and turn the power all the way up for maximum range. Today, such an approach doesn't work. It creates large coverage cells in which all client devices must contend for airtime.

Wired Infrastructure Issues

It seems that no matter the actual cause of a Wi-Fi user's problem, the wireless network will always get the blame. Any problem on the wired network backbone will affect the Wi-Fi, which is the only part that users are aware of because they interface with it. Solid Dynamic Host Control Protocol (DHCP), Domain Name Service (DNS), routing, and switching are critical to good wireless performance.

TECHNICAL STUFF

DHCP manages addresses on a network, and DNS associates names to machines on networks.

Authentication Problems

To keep unwanted users and malicious hackers off your network, strong authentication is essential. Unfortunately, more complex systems are known to break. Creating detailed documentation about authentication systems will make network hardware easier to access when troubleshooting is needed.

Firmware Update Problems

When deploying new firmware or drivers, it should be done in a controlled manner with lab testing before a wide rollout. If you roll out an update to all devices and then find that the update causes system problems, you've just created days and weeks of work for yourself cleaning up the mess. Roll out any updates cautiously to a few test machines, and then check for problems before you update the entire network.

Using the Wrong Data Rates

Most APs enable you to specify which transmission rates they will allow devices to use for connections. Leaving slow data rates enabled ensures range and backward compatibility, but remember that transmissions at slower rates take longer and consume more airtime. Slower data rates can be disabled to force devices to talk faster.

Using Wide Channels Incorrectly

Wider channels (popularly known as *channel bonding* in 802.11n's heyday) take up a lot of frequency space but can provide faster data rates. There are two problems with this thought:

- Some clients don't support wider channels.
- In a high-density deployment, wider channels don't leave enough channels for each AP to have their own channel. As a result, it's best to use 20 MHz channels (with 40 MHz being possible in low-density environments).

IN THIS CHAPTER

- » Designing for your requirements
- » Placing devices for maximum signal strength
- » Planning channel usage
- » Taking advantage of the 5 GHz band
- » Maximizing airtime efficiency

Chapter 7 Ten Wi-Fi Performance Boosts

Several factors can impact wireless communications performance. This chapter lists ten simple, yet important, things you can do to give your network a boost and increase user satisfaction and productivity.

Understanding and Designing for Requirements

When designing a system, it'll likely have a mixture of qualitative and quantitative requirements. A qualitative requirement might be something like "voice quality needs to be good." A quantitative requirement might be "This ballroom must support 400 devices." Your job as the Wi-Fi engineer is to turn the qualitative requirements into quantitative ones. For example, you'll translate the non-technical requirement of "good voice quality" into the minimum hardware specifications you need to achieve that goal, such as "We'll need -67 dBm of signal strength and latency of less than 150 milliseconds."

To make that translation, you need to gather all the pertinent facts:

- How many users?
- Which areas *don't* need coverage?
- What applications will be used?
- Is seamless roaming required?

Checking and Building Your Wired Network

A 10 megabits per second (Mbps) wireless connection used to be great a decade ago, but today it can barely support a single 4K video stream. Remember, if the network is slow, users will think it's the Wi-Fi's fault, even if it isn't.

Provide a large enough pipe to the Internet to support your users so there's no question that the Wi-Fi isn't to blame for any slowdowns.

Maximizing Signal Strength

Signal strength is the primary building block of your wireless network. When referring to "signal strength," we typically mean signal from the loudest access point (AP) at a given location.

If you want users to remain connected while they walk around, you need good signal strength from two APs in any location. This ensures smooth roams from one AP to another without interrupting video calls. You can check signal strength, as we describe in Chapter 3, and verify signal strength in various locations with a site survey (check out Chapter 4).

Finding a Better Place for Your Gear

Don't put your APs on the floor, behind furniture, inside cabinets, or close to metal objects. Instead, mount them on the ceiling, where they belong. Then again, in high-ceiling warehouses and factories, don't mount them *too* high, unless you want to give excellent coverage for Spider-Man.

Choosing Channels Wisely

The biggest source of interference for your Wi-Fi isn't microwave ovens! It's interference from other Wi-Fi devices — either the ones that belong to your neighbors or the other radios that you have installed. The least you can do is open a free app to check which channels your APs are occupying. Put them on their own channel with no overlap. To discover how, flip back to Chapter 2 if needed.

Using Just Enough Power

For good Wi-Fi, you need maximum transmit power and signal strength, right? Nope! Remember, the client needs to hear the AP, and the AP needs to hear the client. So as long as you have adequate transmit power for that to happen, it doesn't help to turn up the power.

REMEMBER

Also, remember that only one device can transmit on a channel at a time. Lower power means smaller coverage cells, which means fewer devices have to share a channel. Sometimes more APs with lower transmit power is the way to go.

Using 5 GHz More and 2.4 GHz Less

As we talk about in Chapter 2, the 2.4 GHz band is very small (approximately 3 channels), and the 5 GHz one is huge (approximately 25 channels). Because only one device can transmit on a channel at a time, because 2.4 GHz has overlapping channels, it's like a slow dirt road. The 5 GHz band, on the other hand, is a modern freeway.

TIP

Today, it's best to design for 5 GHz and either disable 2.4 GHz or provide it only for basic backward compatibility. Turn the transmit power of 2.4 GHz radios down by about 6 dB, which will give both 2.4 and 5 GHz about the same coverage.

Maximizing Airtime Efficiency

REMEMBER

Only one device can talk on a channel at a time, so when devices talk, they need to do so as quickly and efficiently as possible. There are two ways to achieve this:

- Keep infrastructure close to client devices so they can communicate at high speeds.
- Minimize the number of SSIDs that broadcast (one or two is perfect).
- Disable slower data rates to force devices to talk more quickly.

Getting Modern Devices

Don't be fooled by promises of "7 gigabits per second over Wi-Fi." There's a lot of marketing hype out there. That said, remember that old infrastructure and old client devices force things to slow down for backward compatibility — and slow devices end up hogging the channel's time. An 802.11b device, for example, can only hit 11 Mbps, which means everything else has to wait while it slowly transmits. Make sure all the APs are running modern 802.11n or 802.11ac gear.

Learning More about Wi-Fi

Learning more about Wi-Fi may not be an immediate boost, but you'll thank us later. The more you understand about how Wi-Fi actually works, the more you can boost it. But how do you learn?

The most important place is Twitter. It's not your everyday social network . . . this is where the "Wi-Fi gurus" hang out. You don't even need to Tweet if you don't want to. Just go follow the right people. It's easy. Tweet this:

"I just read *Wi-Fi Network Design For Dummies*, Ekahau Special Edition, and I want to learn more! Where do I start? Cc: @jussikiviniemi @80211university @jolla @Potato_Fi"

We'll help you follow the right people!

TIP

Some other amazing learning resources include the following:

- **Certified Wireless Network Professional (CWNP):** The de facto, vendor-neutral Wi-Fi training authority; visit `www.cwnp.com`.
- **Wi-Fi vendor websites:** Search for Wi-Fi vendor websites and get free guidelines and best practices.
- **Wireless LAN Professionals:** This source provides videos, podcasts, conferences, and more. Visit it at `www.wlanpros.com`.
- **Blogs:** Wi-Fi experts love to blog, and you can find a complete list of blogs at `https://gcatewifi.wordpress.com`.

Notes

Notes

Better Wi-Fi

Enterprise tools to design, optimize, and troubleshoot Wi-Fi networks

Whether a corporate office, hotel, hospital or university – if the Wi-Fi works well, it has likely been built using Ekahau's Wi-Fi solutions.

Ekahau is the global leader in solutions for enterprise wireless network design and troubleshooting.

Today, 30% of Fortune 500 companies run their networks with Ekahau's Wi-Fi planning and measurement 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 levels of complexity.

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

www.ekahau.com

ekahau
WIRELESS DESIGN

Design and implement a Wi-Fi network

Wi-Fi is everywhere, and most people expect Wi-Fi availability and Internet access wherever they go. If they don't get it, they will go elsewhere or give you an ear full about the lack of service! If your business offers Wi-Fi — or needs to in the near future — there's a lot to think about. Design, optimize, and troubleshoot better Wi-Fi networks. This book has you covered. Welcome to *Wi-Fi Network Design For Dummies,* Ekahau Special Edition.

Inside…

- How different business types use Wi-Fi
- What factors affect network performance
- How to build a better Wi-Fi network
- Key components of a good network plan
- How to resolve common problems

ekahau
WIRELESS DESIGN

for dummies®
A Wiley Brand

Also available as an e-book

ISBN: 978-1-119-45056-6
Not for resale