The Basics of WiFi

From the Concepts, and how they relate to produce Reliable connectivity

Version 1.0

April 15, 2019

Table of Contents

1 Document Conventions

Alerts readers to take note. Notes contain helpful suggestions or references to material not covered in the document.

Alerts readers to be careful. In this situation, you might do something that could result in equipment damage or loss of data or not acting will cause instability

Alerts the reader that they can save time by performing the action described in the paragraph affixed to this icon.

Alerts the reader that the information affixed to this icon will help them solve a problem. The information might not be troubleshooting or even an action, but it could be useful information similar to a Timesaver.

Alters the reader that the information contained in this area is a best practice and should be followed an implemented

2 Basic WiFi Concepts

Wi-Fi is one of the most important technological developments of the modern age. It's the wireless networking standard that helps us enjoy all the conveniences of modern media and connectivity at the tips of our fingers without the high cost of cellular data charges. But what is Wi-Fi, really?

The term "Wi-Fi" is a marketing name, but it stands for "wireless fidelity." Similar to other wireless connection types, like Bluetooth, it's a radio transmission technology that's built upon a set of standards to allow high-speed and secure communications between a wide variety of digital devices, access points, and hardware. It makes it possible for Wi-Fi capable devices to access the internet without the need for restrictive wires.

It can operate over short and long distances, be locked down and secured, or open and free. It's incredibly versatile and yet is easy enough to use. So much so that it's found in the most popular of consumer devices. Wi-Fi is ubiquitous and exceedingly important for the way we operate our modern connected world.

2.1 How does Wi-Fi work?

Although Wi-Fi is typically used to access the internet on portable devices like smartphones, tablets, or laptops, in actuality, Wi-Fi itself is used to connect to a router or other access point (APs) which in turn provides the internet access. Wi-Fi is a wireless connection to that device, not the internet itself. It also provides access to a local network of connected devices, which is why you can print pictures wirelessly or look at a video feed from Wi-Fi connected cameras with no need to be physically connected to them.

Instead of using wired connections like Ethernet, Wi-Fi uses radio waves to transmit information at specific frequencies, most typically at 2.4GHz and 5GHz, although there are many others used in more niche settings. Each frequency range has a number of channels which wireless devices can operate on, helping to spread the load so that individual devices don't see their signals crowded or interrupted by other traffic — although that does happen on busy networks, the how and why we will get into later in the document.

The typical range of a standard Wi-Fi network can reach up to 100 meters in the open air. Buildings and other materials reflect the signal however, making most Wi-Fi networks far narrower than that. Typically 10-35 metres is more common. The strength of the antenna and the frequency broadcast can also impact the effective range of the network. Higher frequencies like 5GHz have far shorter effective ranges than 2.4GHz.

Everyone within a network's range and a compatible Wi-Fi device can detect the network and attempt to connect to it. That's what allows it to operate in both private and public settings, but it does raise concerns over security. That's why standards like WPA and WPA2 exist and why it's important to change your password if you think someone's accessing your network without permission.

2.2 What is 802.11?

Often talked about in conjunction with Wi-Fi, 802.11 or IEEE 802.11, is a set of protocols that specifies the sort of communications that can occur on a Wi-Fi network on various wireless frequencies.

Before the recent change in naming convention, 802.11 was also a major component of the name for each successive generation of Wi-Fi connectivity. Typically followed by a letter or series of letters, it continues to be part of the technical name for each generation of Wi-Fi, although there are now simpler naming schemes used, labeled by generations.

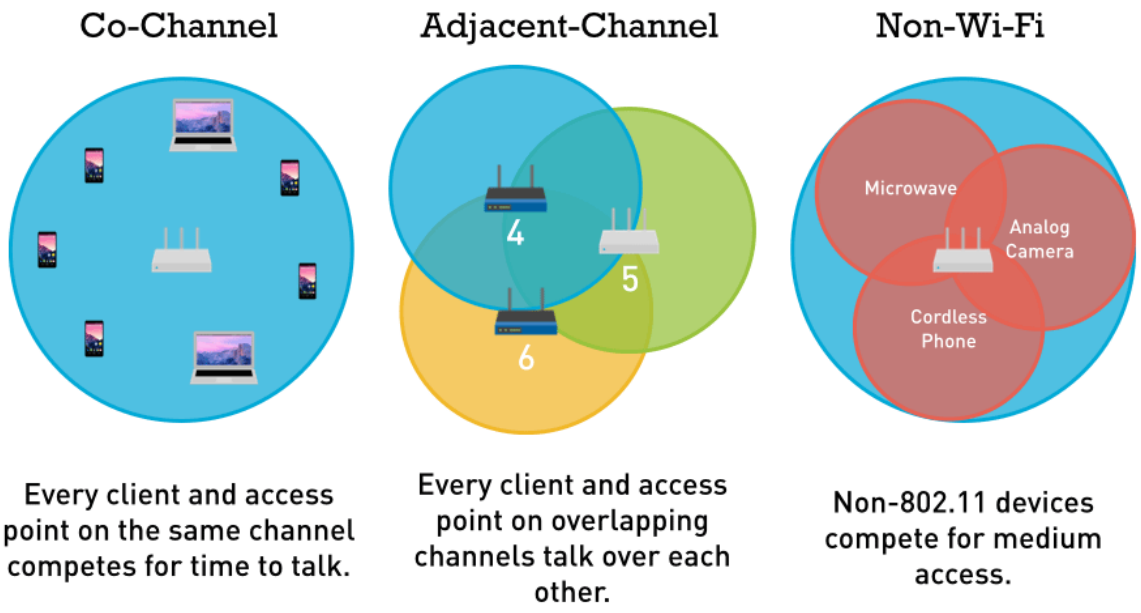
- 802.11n (2009) = Wi-Fi 4
- 802.11ac (2014) = Wi-Fi 5
- 802.11ax (upcoming 2019) = Wi-Fi 6

When we discuss WiFi, we typical are talking about two channel bands or frequency, 2.4 GHz and 5GHz. These are the FCC frequency that these devices operate in and hence have been adapted as the naming convention.

2.3 Understanding the 2.4 GHz frequency space

In the 2.4 GHz band, channels 1, 6, and 11 are the only non-overlapping channels. Selecting one or more of these channels is an important part of setting up your network correctly. Currently, many wireless routers automatically select the channel for you upon initial setup, where depending on your wireless environment, it could lead to slow WiFi speeds and interference. This document will describe what interference you're dealing with and takes you through the steps to selecting the right channel, so you can understand why you should choose between channel 1, 6, and 11 on 2.4 GHz band network.

2.4 The Three main causes of WiFi interference



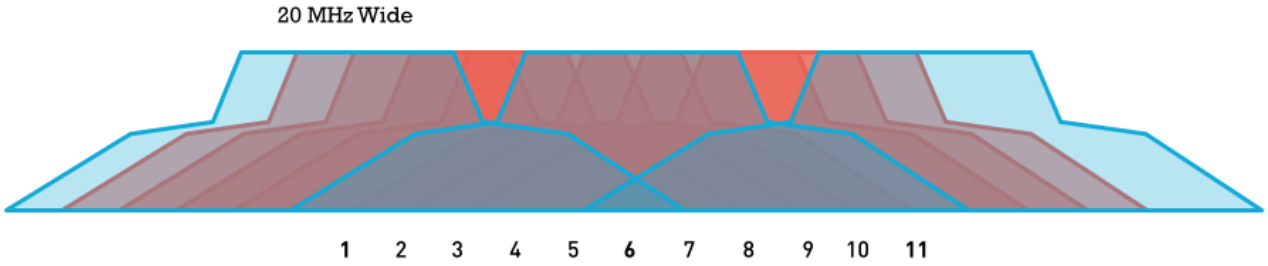
Co-Channel interference isn't a major problem until there are too many WiFi devices on the same channel. Adjacent-Channel interference, on the other hand, is where you run into problems and channel selection becomes critical. This is one of the major problems we face in the arena that was identified in our assessment. Luckily, these channel related interferences can be reduced or eliminated by selecting the proper WiFi channel for your network.

Using a spectrum analyzer like Ekahau or Netscout AirCheck G2 will allow you to see this wireless environment, so you can either select the right channel or mitigate WiFi interference, ultimately improving your 2.4 GHz WiFi network performance. However, most modern phones and tablets generally support 5 GHz WiFi so the decision was made to turn off 2.4 GHz on

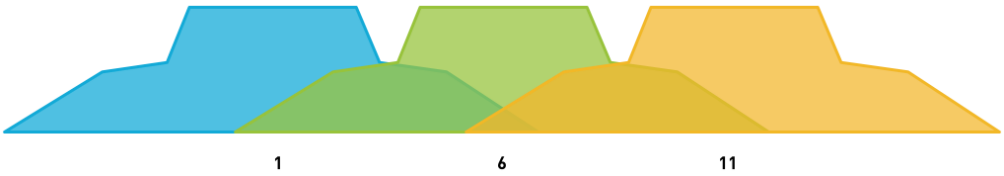
"FreeMSGWiFi" where our guest attach. We do enable 2.4 GHz on certain SSIDs like Appetize because the POS terminals in the arena only support 2.4 GHz and are used as a backup in the event a physical cable issue occurs to a terminal

2.5 Non-Overlapping Channels

Each channel on the 2.4 GHz spectrum is 20 MHz wide. The channel centers are separated by 5 MHz, and the entire spectrum is only 100 MHz wide. This means the 11 channels have to squeeze into the 100 MHz available, and in the end, overlap.



However, there are three channels that don't overlap: 1, 6 and 11, as you can see in the image below. Co-channel interference is where devices take turns talking, so the more devices on one channel, the longer it takes for a device to talk since it has to wait for its turn.



Armed with the above information, you've narrowed your selection down to three channel choices (1, 6 and 11) without using any software! Unfortunately, this doesn't mean neighboring networks aren't using non-standard channels. That's where monitoring with our NetScout Devices can help out. More advanced toolsets like an Ekahau Sprectrum Analyzer helps you visualize every network within reach, however, these are more advanced toolsets and require more specialized training.

If properly used, tools like Aircheck G2 and Ekahau can help you see what is causing your WiFi problems and fix them fast. There are additional tools on the market which will automatically recommend the optimal channel for you.

.

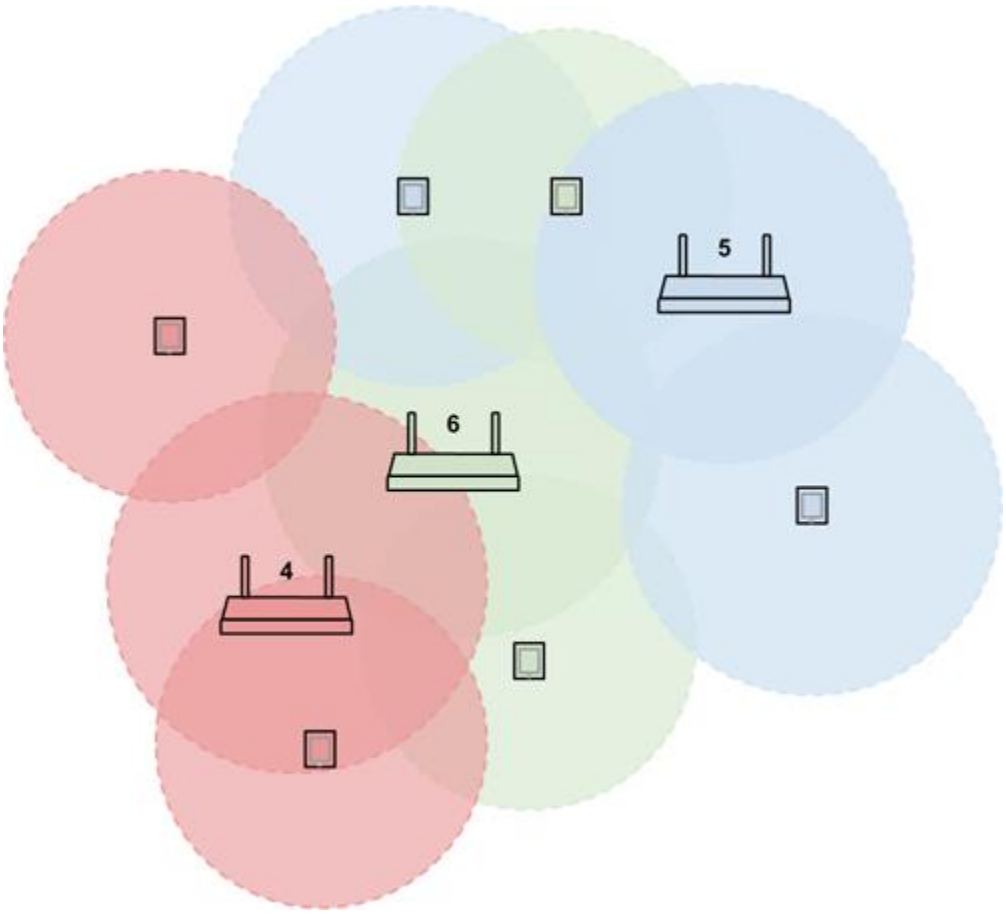
2.6 Adjacent and Co-Channel Interference

Now that you understand a little about channels in the 2.4 GHz space and why channels 1, 6, and 11 are the best choices for operating your wireless network, let's talk about interference and congestion.

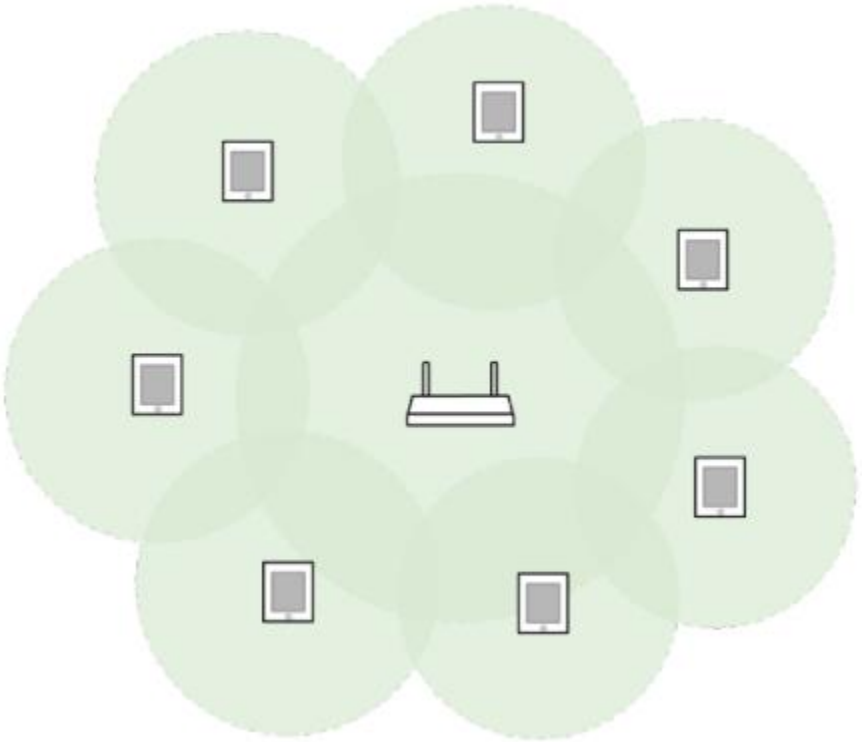
Recall that channel overlap is bad because of the "conversational" way that WiFi operates, and often times you will find yourself having to manage congestion. In this article, you'll learn about adjacent and co-channel congestion and interference, using conversation as a metaphor.

Adjacent channel congestion is the worst type of WiFi interference. To illustrate, think about being at a concert in the Garden – there's a band playing really loud, and tons of people, each with their own group of friends. With this much going on, it's difficult to talk to your friends, and when you start to talk louder, the person next to you has to raise his voice to talk to their group. You're hearing multiple conversations happening, as well as music from the band, and it seems impossible to communicate. This is exactly what happens to wireless devices trying to communicate in a congested environment.

The diagram below shows a model of how the above conversation scenario looks when access points on channel 4 (red), channel 6 (green), and channel 5 (blue) are all active at once. As one of these APs tries to talk to its clients, its transmissions become garbled because of the transmissions of the other two. This harms the performance of all of the networks.

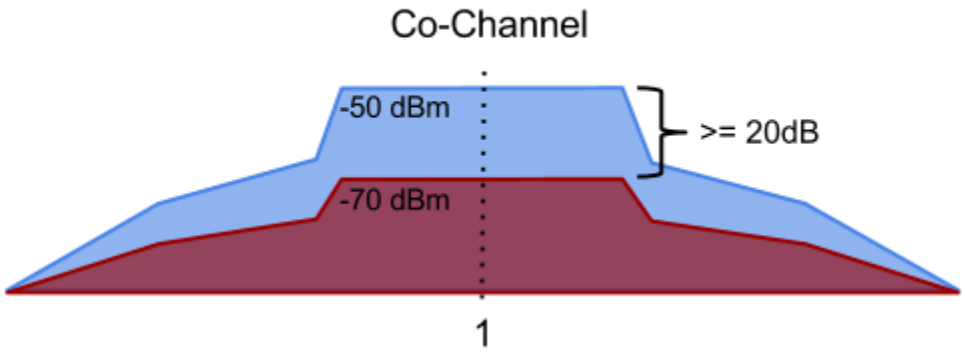


In order to explain co-channel congestion, we'll move our imaginary conversation from a concert venue to a classroom. Think back to your school days – chances are you can think of at least one class that had a student who would talk slower than the other kids, and everyone else would have to wait for their turn to ask a question. Co-channel congestion works in a similar manner: the performance is hindered by the wait times, but the bandwidth is managed, and every device will get a chance to talk to its associated AP. This is why when running speed tests in the Arena we are seeing wild variation of results from minute to minute and from different sections. It is also the reason why just adding another access point to solve for poor WiFi performance is a really bad idea. The diagram below depicts a wireless access point and its associated clients, which can only talk one at a time.

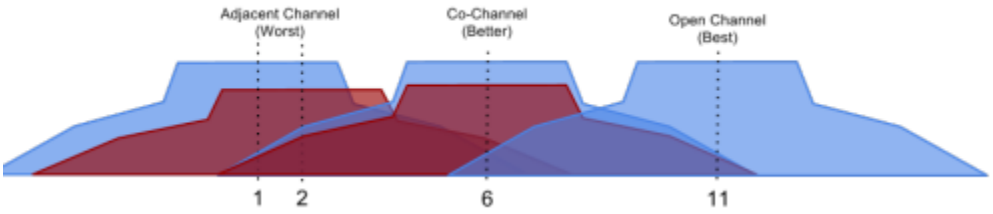


Co-channel congestion is preferable to adjacent channel congestion because of the way the wireless conversations are managed. As mentioned above, when choosing a channel that has other networks active, try to keep at least 20 dB between the RSSI [1] (Received Signal Strength Indicator) levels of the networks, as illustrated below:

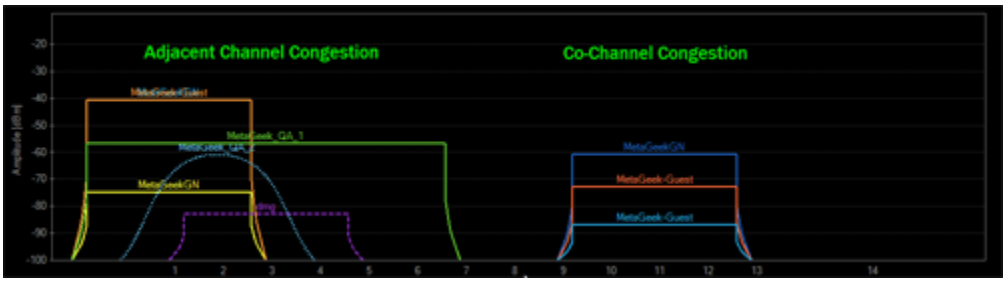
[1] In telecommunications, received signal strength indicator (**RSSI**) is a measurement of the power present in a received radio signal. **RSSI** is usually invisible to a user of a receiving device



To recap, an open channel will always be best when deploying your wireless network, but if you have to share a channel, that's okay too. Adjacent channel congestion is the one you'll want to avoid if at all possible.



The image below shows what adjacent channel and co-channel congestion looks like. Having a visual representation of where neighboring wireless access points are active is an invaluable tool when planning your own network. It's easy to see how chaotic adjacent channel congestion is compared to co-channel! This is why, limiting the number of SSIDs being broadcasted is so important.



Hopefully you now have a good understanding of how WiFi congestion is caused, and how to best deal with it in the 2.4 GHz Band.

3 Understanding WiFi Signal Strength

What is an acceptable WiFi signal strength for a specific application?

What signal strength should I try to achieve in my wireless deployment?

These common questions illustrate the somewhat confusing nature of signal strength. First, we must understand the units of measurement, and what those measurements mean when deploying, managing, or diagnosing problems in a typical WiFi environment. Only then can we understand what signal strength is needed for specific uses.

3.1 Planning

The key to any good wireless deployment is proper planning, which requires a set of goals and requirements to achieve. Determining minimum signal strength requirements in the coverage area is almost alway part of the network requirements list.

3.2 Requirements and Variables

Desired signal strength for optimal performance varies based on many factors, such as background noise in the environment, the amount of clients on the network, what the desired data rates are, and what applications will be used. For example, a VoIP (Voice Over IP) or VoWiFi (Voice Over WiFi) system may require much better coverage than say a barcode scanner system in a warehouse.

3.3 Understanding Signal Strength

WiFi signal strength is tricky. The most accurate way to express it is with **milliwatts** (mW), but you end up with tons of decimal places due to WiFi's super-low transmit power, making it difficult to read. For example, -40 dBm is 0.0001 mW, and the zeros just get more intense the more the signal strength drops.

RSSI (Received Signal Strength Indicator) is a common measurement, but most WiFi adapter vendors handle it differently, as it isn't standardized. Some adapters use a scale of 0-60, and others 0-255.

Ultimately, the easiest and most consistent way to express signal strength is with **dBm**, which stands for **decibels relative to a milliwatt**. Since RSSI is handled differently by most WiFi adapters inclusive of iPhones, iPads, there are even differences between different manufacturers of Android devices. For consistency and readability it is usually converted to dBm. See below for signal range settings:

- **mW** - milliwatts (1 mW = 0 dBm)
- **RSSI** - Received Signal Strength Indicator (usually 0-60 or 0-255)

- **dBm** - Decibels in relation to a milliwatt (usually -30 to -100)

3.4 Reading dBm

The first thing to understand about dBm is that we're working in negatives. -30 is a higher signal than -80, because -80 is a much lower number.

Next, it's important to know that dBm does not scale in a linear fashion like you'd expect, instead being logarithmic. That means that signal strength changes aren't smooth and gradual. **The Rule of 3s and 10s** highlights the logarithmic nature of dBm:

3 dB of loss = -3 dB = halves signal strength
3 dB of gain = +3 dB = doubles signal strength
10 dB of loss = -10 dB = 10 times less signal strength (0.1 mW = -10 dBm, 0.01 mW = -20 dBm, etc.)
10 dB of gain = +10 dB = 10 times more signal strength (0.00001 mW = -50 dBm, 0.0001 mW = -40 dBm, etc.)

3.5 Ideal Signal Strength

So what signal strength should you shoot for? For simple, low-throughput tasks like sending emails, browsing the web, or scanning barcodes, -70 dBm is a good signal strength. For higher-throughput applications like voice over IP or streaming video, -67 dBm is better, and some engineers recommend -65 dBm if you plan to support mobile devices like iPhones and Android tablets.

Note: The numbers in this chart are suggestions only. The desired signal strengths will vary, based on the requirements for the network.

Table 1.0

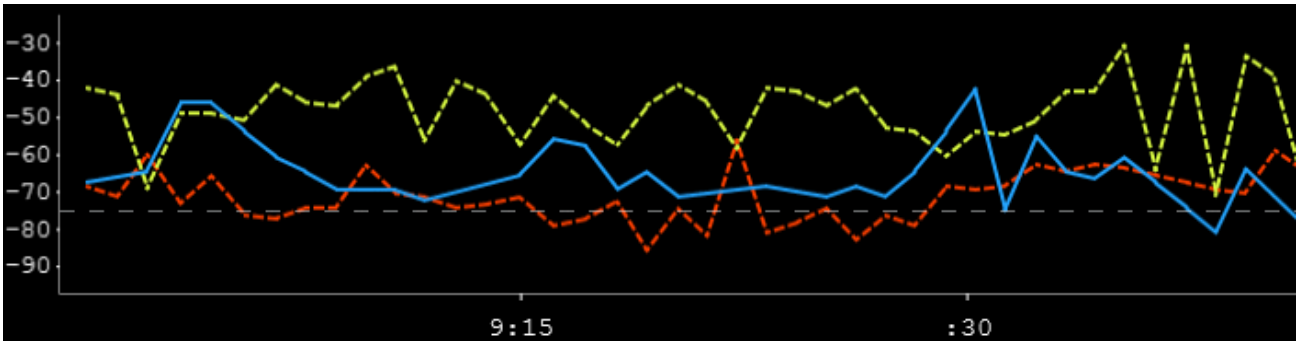
Signal Strenght	Performance	Description	Required For
-30 dBm	Amazing	Max achievable signal strength. The client can only be a few feet from the AP to achieve this. Not typical or desirable in the real world	Everything works well at this signal strenght
-67 dBm	Very Good	Minimum signal strength for applications that require very reliable, timely delivery of data packets.	VoIP/VoWiFi, streaming video
-70 dBm	OK	Minimum signal strength for reliable packet delivery.	Email, Web Surfing
-80 dBm	Not Good	Minimum signal strength for basic connectivity. Packet delivery may be unreliable.	N/A

-90 dBM	Unusable	Approaching or drowning in the noise floor. Any functionality is highly unlikely	No modern application will perform well with this signal strength

Modern iPhone wont start look for a stronger signal (another Access Point) until signal strength falls below -73dBm. Android threashold are a bit higher, around -80dBm, but varies based on your manufacturer.

4 Tracking Signal Strength

Signal strength is easy to track. Advanced tools like an Ekahau will do it, our Aircheck G2 devices will also track on an individual SSID. Simple tools like MetaGeek inSSIDer Plus is a simple tool to graph signal strength, but will require you to carry around a laptop. If you are OK carry around a laptop, you can configure the signal strength threshold to whatever signal strength you require, select your network, and walk the desired coverage area.



If the blue line falls below the dotted line, you know you have a dead spot. That's it!

4.1 What is RSSI and what does it mean for a WiFi network?

RSSI, or “Received Signal Strength Indicator,” is a measurement of how well your device can hear a signal from an access point or router. It’s a value that is useful for determining if you have enough signal to get a good wireless connection.

Because an RSSI value is pulled from the client device’s WiFi receiver (hence “received” signal strength), it is not the same as transmit power from a router or AP.

4.2 RSSI vs dBm

dBm and RSSI are different units of measurement that both represent the same thing: signal strength. The difference is that RSSI is a relative index, while dBm is an absolute number representing power levels in mW (milliwatts).

RSSI is a term used to measure the relative **quality** of a received signal to a client device, but has no absolute value. The IEEE 802.11 standard specifies that RSSI can be on a scale of 0 to up to 255 and that each chipset manufacturer can define their own “RSSI_Max” value. Cisco, for example, uses a 0-100 scale, while Atheros uses 0-60. It’s all up to the manufacturer (which is why RSSI is a relative index), but you can infer that the higher the RSSI value is, the better the signal is.

Since RSSI varies greatly between chipset manufacturers, WiFi troubleshooting tools software uses a more standardized, absolute measure of signal strength: received signal power, which is measured in decibels, or **dBm** on a logarithmic scale. Basically, **the closer to 0 dBm, the better the signal is**. Refer to table 1.0 for signal strength reference

4.3 What if I have an acceptable signal strength but I’m still having problems?

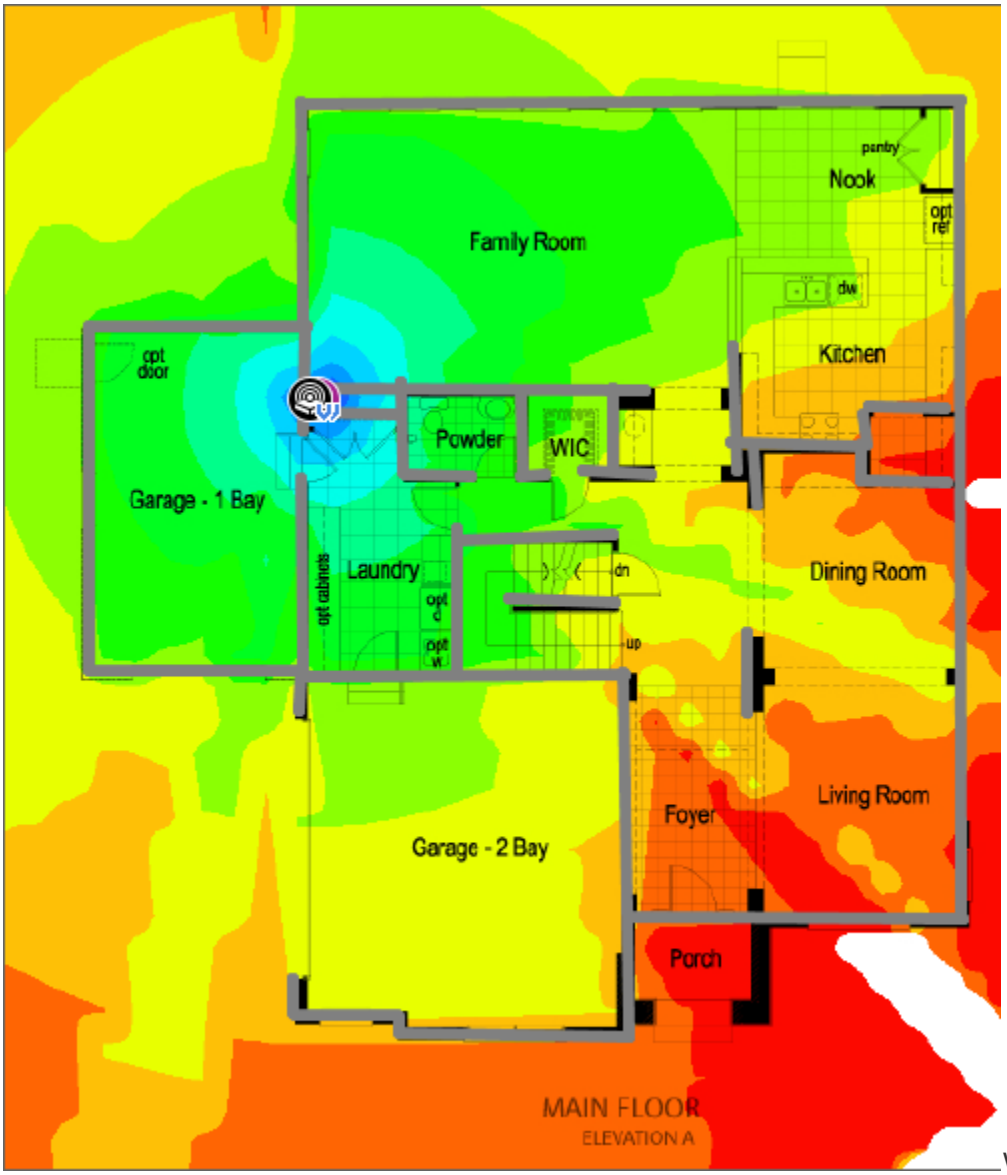
If you’ve already checked your signal strength using a WiFi scanning app like our NetScout AirCheck G2 and concluded that you have acceptable WiFi signal strength, then interference may be to blame. Your devices WiFi adapter can help you see some types of interference, but for finding non-WiFi interferers, you’ll need a spectrum analysis tool like an Ekahau.

4.4 Diminishing Signal Strength

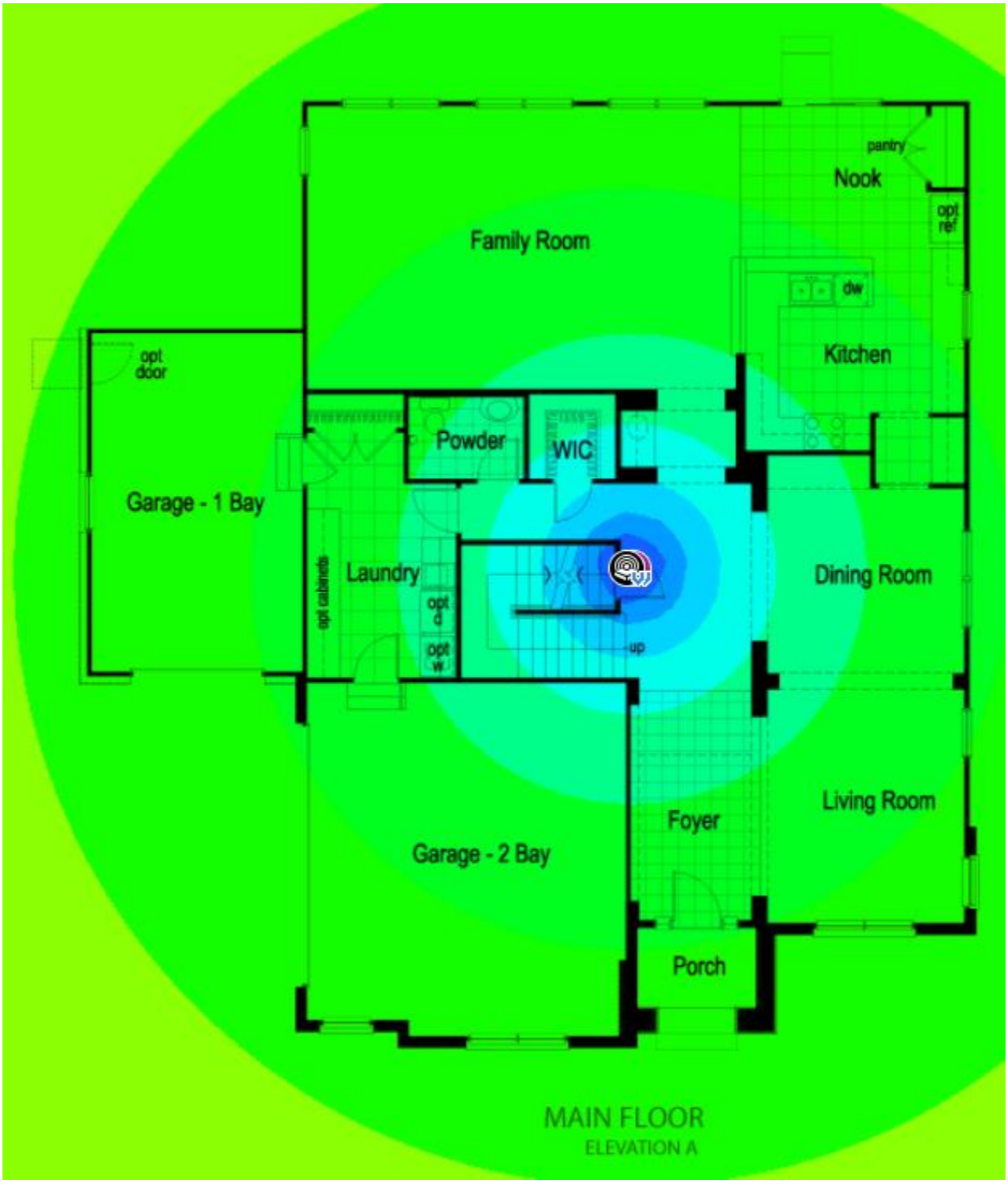
A strong signal is often a good indicator that the WiFi connection will be fast and reliable instead of slow and intermittent. We can compare this to hearing other people talk – in a quiet, open area, you can hear someone’s voice fairly well. On the other hand, in a building with thick walls, listening becomes more difficult. The same is true for indoor WiFi. As distance increases, the wireless signal strength decreases, and different types of obstructions will further reduce signal strength.

4.5 Dead Spots and Slow Speeds

Many WiFi users experience poor connectivity and slow speeds. In one room it doesn’t work at all, and in another speed may be too slow. To achieve a good connection, WiFi has to overcome barriers and obstacles - some of which can’t be eliminated by simply purchasing a new wireless router or relocating an access point. The below example is a WiFi heat map of the same structure. You can see, that simply relocating an Access Point (AP) to a better position can significantly improve performance.



WiFi Signal Strength Loss From Indoor Walls



Free Space Path Loss With No Attenuation from Walls

This example shows what WiFi signal strength would look like with and without building walls. The red colors represent a signal strength too low for good WiFi connectivity.

Use the following guidelines to gauge how different materials in your home affect the signal strength of WiFi. Keep in mind that a 3 dB drop is equivalent to a 50% reduction in power!

- Dry Wall: 3 dB
- Hollow Wood Door: 4 dB
- Brick Walls: 6 dB
- Concrete: 8 dB
- Refrigerator: 19 dB

What To Do

Changing the location of a wireless router can improve the speed and connectivity for most users. You should try to put the wireless router in a more centralized location.

- *Take that Wireless Router out of the cabinet in the laundry room and find the right spot for it!*
- Decide which rooms need WiFi the most and measure their signal strength using NetScout AirCheck G2
- To improve the signal strength for every room, find a central location for the wireless router with as few brick walls and metal objects in the way as possible.
- Verify you're getting higher signal strength with NetScout AirCheck G2

5 Understanding Noise Levels in WiFi Networks

The Noise level is the amount of outside interference detected at each measurement point. High noise levels can interfere with your network signal strength and cause areas of poor connectivity — or "dead zones" where there is no connectivity. Noise in a WiFi network is typically referring to those non-network RF interference levels. Noise can be caused by any electronic device, including microwave ovens, cordless phones, Bluetooth devices, wireless video cameras, wireless game controllers and fluorescent lights.

Identifying and removing the source of noise might not be an easy task. In practice, the easiest solution is usually increasing the signal level rather than decreasing the noise level. But this must be carfully considered as raising the signal strength too much will lead to channel overlap and channel interference.

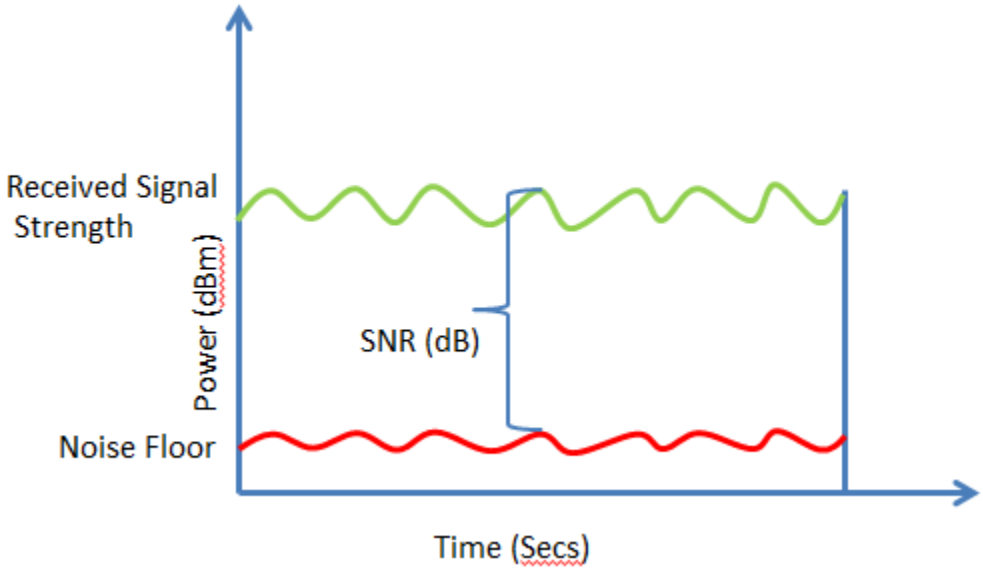
Note that other Wi-Fi networks are not included when measuring noise, but they are included in the Signal to Noise Ratio (SNR) which is covered next

5.1 Strategies for decreasing noise level

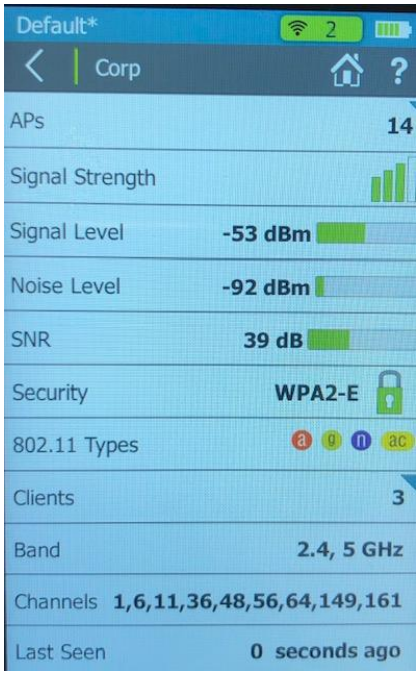
- Switch your network from the 2.4 GHz frequency band to 5 GHz. The 2.4 band tends to have a lot more noise. Both your APs and client devices will need to be capable of using the 5 GHz band. If you can't ensure that, at least try to install double-frequency APs that cover both bands and inform users that connecting to the network at 5 GHz is preferable.
- This approach was a quick fix that was taken in the Arena on "FreeMSGWiFi". Eliminating 2.4 GHz on the guest network significantly improved performance. However we must keep 2.4 GHz enabled on the "Appetize" SSID for the use of older POS terminal that use WiFi as a backup in the event of a hard wire failure. However, steps are being taken to hardcode these known devices to a known WiFi network. This action will allow us to stop broadcasting out the "Appetize" SSID and better control signal overlap and congestion.
- If switching to the 5 GHz band is not an option, try switching the affected APs to a different channel in the 2.4 GHz band.
- Check the environment and attempt to identify sources of noise. Turn them off one at a time (if possible) and use your NetScout to quickly measure for improvements in noise level in the particular areas.
- Once you identify a source of noise, your choices are to move, replace or shield the source of noise, or to move the affected AP.

5.2 Understanding Signal to Noise Ratio (SNR)

SNR is not actually a ratio but the difference (Delta) in decibels between the received signal and the background noise level (noise floor). For example, if a radio (client device) receives a signal of -75 dBm and the noise floor is measured at -90 dBm, the SNR is 15 dB. Data corruption and therefore re-transmissions will occur if the received signal is too close to the noise floor. In 802.11 networks, re-transmissions adversely affect throughput and latency.



The WLAN card on a laptop is not designed to measure the noise floor of its surrounding and special adapters like the NetSout AirCheck G2 are needed. As explained above, Cisco access points use SNR to measure the signal strength on a particular client. Using our NetScout or similar tools, one can find the received signal strength on a client and therefore calculate the noise floor at a location by subtracting the SNR value from the received signal value.



5.3 Signal Levels for SNR

dB Signal Level	Result
25 – 40 dB	Very Good Signal
15 – 25 dB	Low Signal
10 – 15 dB	Weak Signal
5 – 10 dB	No Signal

5.4 Slow Zones from Competing Networks

Slow connectivity in an area can be caused by competing networks on the same or overlapping channel. When a WiFi channel has a lot of active users on several networks, the speeds decrease for everyone. Unfortunately, the channel doesn't belong to just you, and you can't stop other networks from using it.

Your best option is to use a channel with no overlapping networks or share a channel that has networks with low signal strength. There are two types of WiFi interference that can slow you down:

Co-Channel Interference - Networks sharing a channel cooperate and take turns talking. Channel bandwidth is shared between every WiFi device.

Overlapping Interference - Networks on non-standard or overlapping channels are unable to cooperate, and will cause interference on neighboring networks. They share bandwidth with networks on standard channels.

To avoid WiFi slowness, find a channel that has the least amount of co-channel and overlapping interference. That means you want the fewest networks to be on your channel - and if they are, you want them to be relatively quiet (lower signal strength).

5.5 Dead Spots from Non-WiFi devices

Sometimes you may have excellent signal strength, but little to no connectivity. These dead spots can be caused by competing wireless devices that use the same frequencies as WiFi, but do not cooperate with WiFi. Here are a few common devices that cause dead spots in the home:

- Cordless Phones

- Wireless Audio Systems
- Microwave Ovens
- Wireless Security Systems

Only a spectrum analyzer can show you non-WiFi interference

5.6 Should I just let my router/ controller auto-select the right WiFi channel?

In short - no! Many wireless Access Points and controllers have an auto-channel selection algorithm in order to provide a better connection, but this can cause more headaches than it solves. Auto channel selection is blind to non-WiFi sources, and makes its selection only on the number of interfering networks sharing the same channel. It may also put your wireless network on a non-standard channel, which introduces even more interference from multiple sources. In the end, auto channel selection does not solve any problems. If anything, it makes the problem more intermittent and extremely difficult to troubleshoot. The best long-term solution is to use a tool like NetScout AirCheck G2 (small networks) or a combination of NetScout and an Ekahau for complex networks such as our Arena's and Venues to monitor the WiFi environment and assign access point to the channel with the least interference.

6 WiFi Security

There are several types of wireless security that you'll come across – here's a quick rundown on the details.

6.1 WEP

Wired Equivalent Privacy, aka WEP, is the grandfather of wireless security types, dating back to 1999. When a client connects to a WEP-protected network, the WEP key is added to some data to create an "initialization vector," or "IV" for short. For example, a 128-bit hexadecimal key is comprised of 26 characters from the keyboard (totaling 104 bits) combined with a 24-bit IV. When a client goes to connect to an AP, it sends a request to authenticate, which is met with a challenge reply from the AP. The client encrypts the challenge with the key, the AP decrypts it, and if the challenge it receives matches the original one it sent, the AP will authenticate the client.

This may sound secure, but there was room in this scheme for an exploit to be discovered. The risk presents itself when a client sends its request to the access point – the portion containing the IV is transmitted wirelessly in clear-text (not encrypted). In addition, the IV is simple compared to the key, and when there are several clients using the same WEP key on a

network, IVs have an increased probability of repeating. In a busy environment, a malicious user wishing to gain access to a network utilizing WEP security can passively eavesdrop and quickly collect IVs. When enough IVs have been collected, the key becomes trivial to decrypt.

Clearly, WEP is not the correct choice for securing your network, and in light of this, other types of wireless security were created.

6.2 WPA

WiFi Protected Access (WPA) was ratified by the WiFi Alliance in 2003 as a response to the insecurities that were discovered in WEP. This new security standard, the Temporal Key Integrity Protocol (TKIP), included several enhancements over WEP, including a new message integrity check nicknamed “Michael.”

While Michael offered a great deal of improvement over the old way of securing networks, there was still some worry about some security issues with using a similar (though much stronger) implementation.

6.3 WPA2

The concerns about Michael led to WPA2’s introduction in 2004. At the center of WPA2 is its use of a security protocol based on Advanced Encryption Standard (AES), the U.S. Government’s preferred choice of encryption.

As it stands now, the only people who should still be using TKIP on a wireless network are those who are dealing with hardware that is rated for 802.11g only.

6.4 WPS

In 2007, a new security method - WiFi Protected Setup (WPS) - began to show up on wireless access points. With this type of security, a user is able to add new devices to their network by simply pushing a button (within administration software or physically on the router) and then typing in an 8-digit PIN number on the client device. The PIN feature acts as a sort of shortcut for entering in a longer WPA (WiFi Protected Access) key. The basic idea behind WPS is that having physical access to the AP to hit a button and reading a sticker would provide a more secure implementation of WiFi authentication. Everything was well and good in the WPS world, until last winter, when a security researcher discovered the Achilles Heel in the implementation.

Here's how it works:

The eighth and final digit of the PIN number is a checksum, which is used to make sure the 7 digits that matter don't get corrupted. From these 7 digits, we can see that there are 10,000,000 possibilities (since each of the 7 digits can be 0-9, with repeats allowed). This is still a pretty huge amount of possibilities, and alone could arguably still be considered quite safe -- but there's a flaw in the checking process. When a PIN is being examined by the AP, the first 4 digits (10,000 possibilities) are checked separately from the last 3 digits (1,000 possibilities). This translates into a malicious user only needing to make at most 11,000 guesses, which a computer can handle in a matter of hours!

As you can see, if you or someone you know is currently using WPS on an access point, you should disable the feature ASAP.

Recommendation

If your access point or clients are only capable of using WEP, it's time for you to look at upgrading your technology, for the sake of increased security – not to mention increased throughput speeds on newer devices.

Right now, the best security for your WiFi network is **WPA2 with WPS disabled** . Using this security combination provides the most secure WiFi network possible today, and gives you the peace of mind you need to "set it and forget it."

7 Designing a Dual-Band Wireless Network

Design for Both Capacity and Coverage

Needs for wireless networks are growing. Previously, we were able to design wireless networks to simply provide coverage for the desired coverage area. Now, with the demands placed on our networks, we need to design for network capacity, not just coverage.

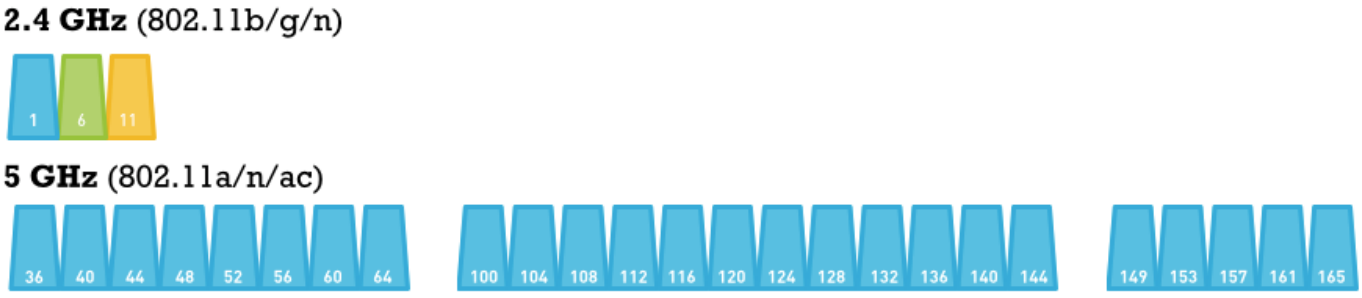
By correctly utilizing both the 2.4 and 5 GHz bands, we can:

- Double the potential available wireless bandwidth
- Maintain 802.11b/g/n compatibility for older 2.4 GHz devices
- Provide better performance for newer 802.11a/n/ac compatible devices

2.4 and 5 GHz Comparison

2.4 GHz	5 GHz
802.11b/g/n	802.11a/n/ac
Greater Range (~300 ft)	Lower Indoor Range (~90 ft)
Universal Compatibility	Limited Compatibility (a/n/ac devices only)
3 non-overlapping channels	24 non-overlapping channels
Congested with WiFi	Little WiFi congestion
Plagued by non-WiFi interference	Very little non-WiFi interference

2.4 GHz has three non-overlapping channels to work with, while 5 GHz has 24. We don't always get to use all of the 5 GHz channels, but overall it offers a lot more space.



Channel Capacity

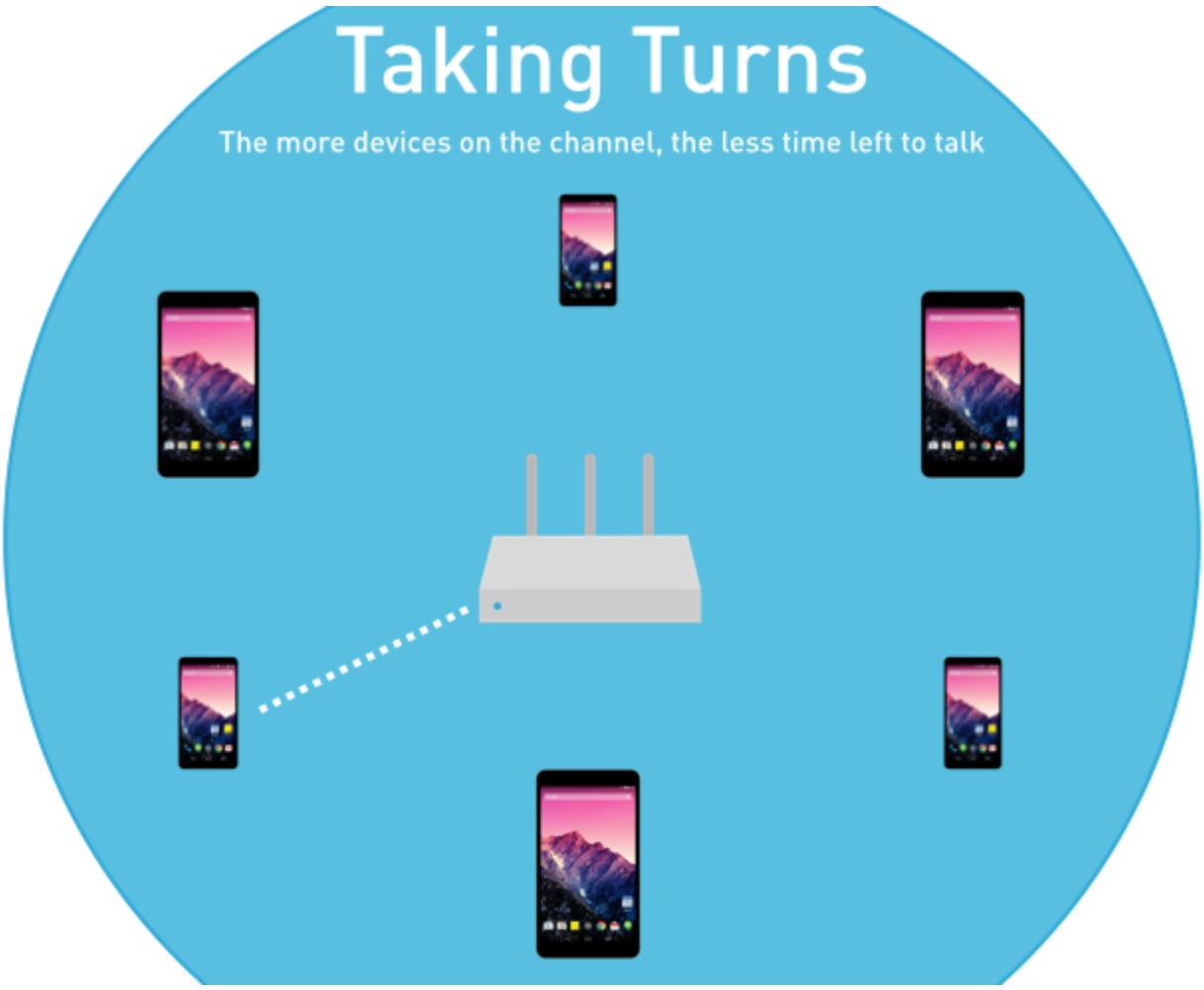
Many of us are familiar with an ethernet cable, which has multiple twisted pairs of copper wires in one cable. This allows for bi-directional or **full-duplex** communication. Network devices on either end of the cable can talk at the same time, much like a two-lane highway.

Only One Device at a Time

WiFi is **half-duplex**, which means that on any channel, only one device can talk at a time. If two devices try to talk at the same time, they would interrupt each other. WiFi is more like a one-lane highway; traffic can only flow in one direction at a time.

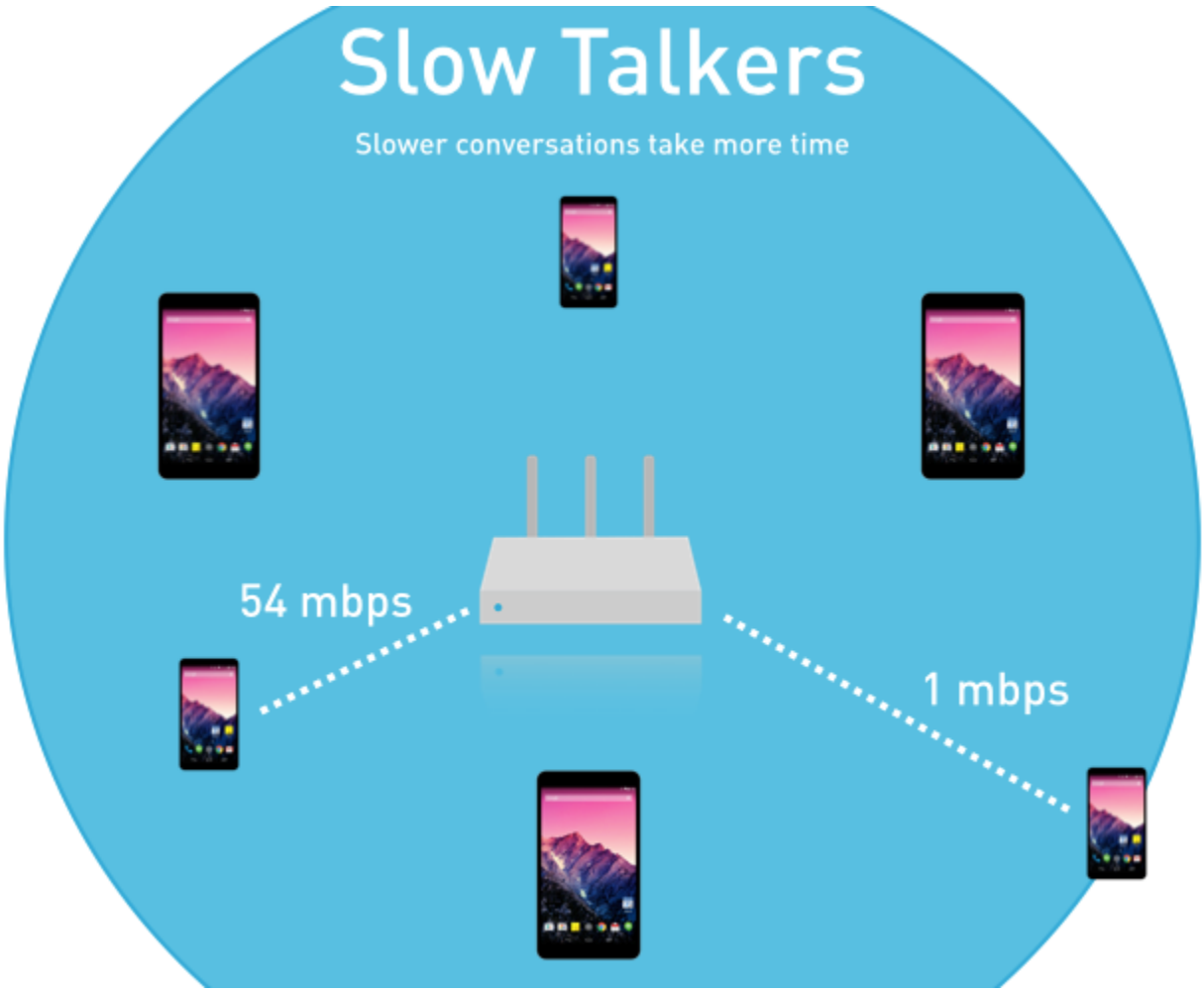
Since WiFi is half-duplex, only one WiFi device can transmit on a channel at a time. The more WiFi devices we add to a channel, the more we reduce opportunities for each device to talk. This is known as **co-channel interference**. This is another challenge we face in the arena.

Since only one device can talk on a channel at a time, we need to limit the amount of devices on each channel. By ensuring our channel isn't too crowded, we can reduce co-channel interference. During the arena redesign much thought has to be put into how channels are defined in order for devices to have enough space for all devices to communicate effectively in.



Devices transmit data at different data rates depending on how new they are (N devices can talk faster than B devices, for example), how close they are to the access point, and how noisy the RF environment is.

Slow devices take longer the transmit the same amount of data. We need to keep our data rates fast to force clients to talk faster and save time, which also reduces co-channel interference.



We can reduce co-channel interference by:

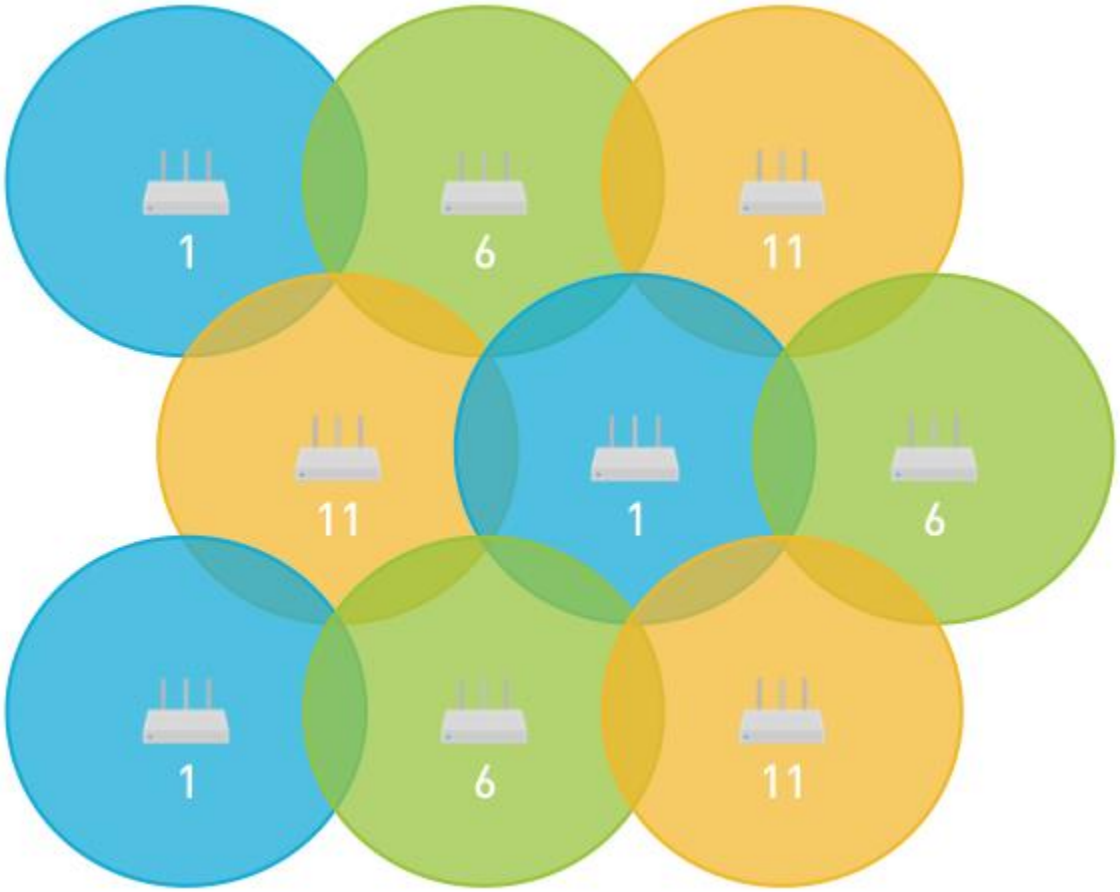
- Disabling slower data rates like 1, 2, 5.5, or 11 mbps
- Creating smaller coverage cells, so fewer devices share the channel
- Creating effective coverage cells where devices are able to always talk quickly
- Offering both 2.4 and 5 GHz support, effectively doubling available throughput
- Performing effective channel planning to keep cells from having to take turns

8 Channel Planning

2.4 GHz

To eliminate adjacent-channel (also called cross-channel) interference, we only use channels 1, 6, and 11 (1, 5, 9, and 13 in some parts of the world).

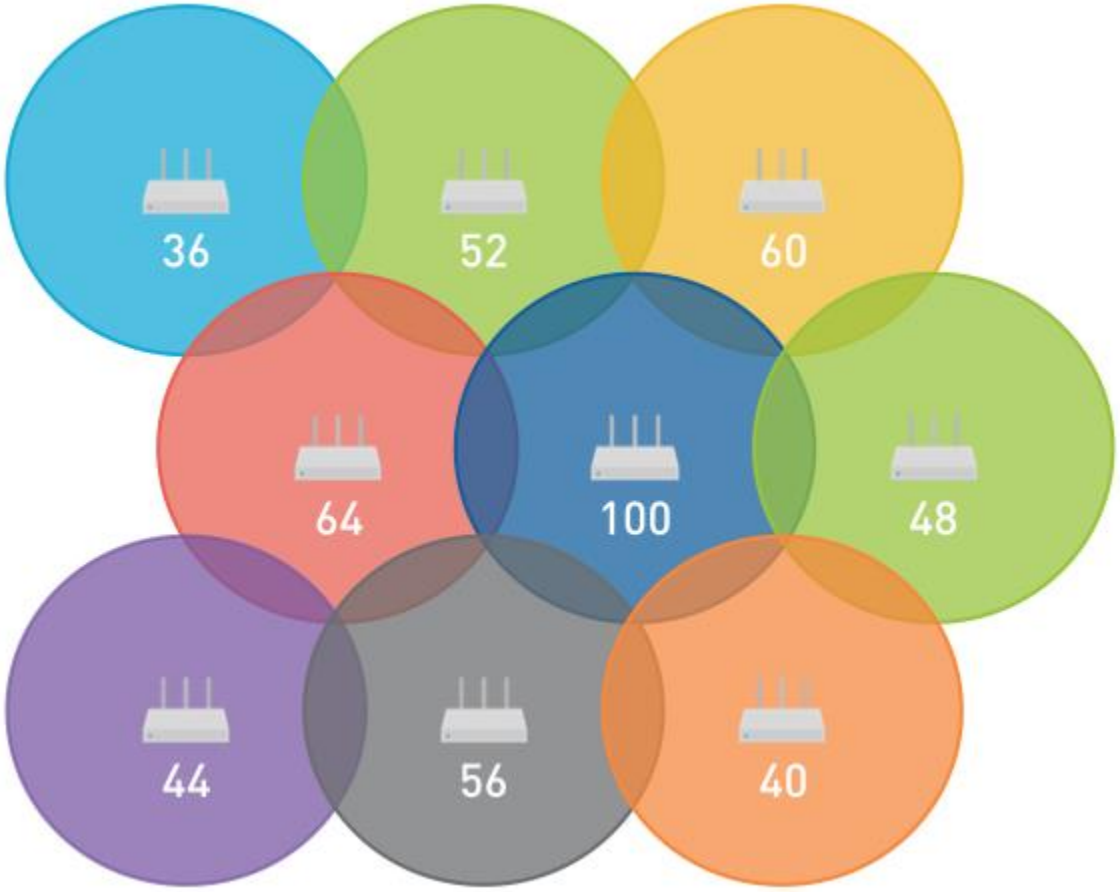
To minimize co-channel interference, same-channel access points will be placed as far away from each other as possible. This divides the coverage area into smaller cells. Each small cell has only a few clients, and same-channel cells won't have to take turns with other cells.



Same-channel cells are as far away from each other as possible.

5 GHz

In the 5 GHz band, no 20 MHz channels partially overlap. In addition to this, there are 24 non-overlapping channels to work with, so making sure no same-channel cells touch is much easier.



With 24 non-overlapping channels to choose from, it is much easier to keep same-channel cells touching.

9 Dual-Band Network Design Checklist

Action	Result
Dual-band APs deployed	• Doubled potential wireless bandwidth • b/g/n devices get compatibility • a/n/ac devices get better performance
All 2.4 GHz radios on 1, 6, and 11	Adjacent-channel interference eliminated
2.4 GHz channels planned	Co-channel interference minimized
5 GHz channels planned	Co-channel interference minimized

2.4 GHz power turned down to match 5 GHz coverage area	Even 2.4 and 5 GHz coverage

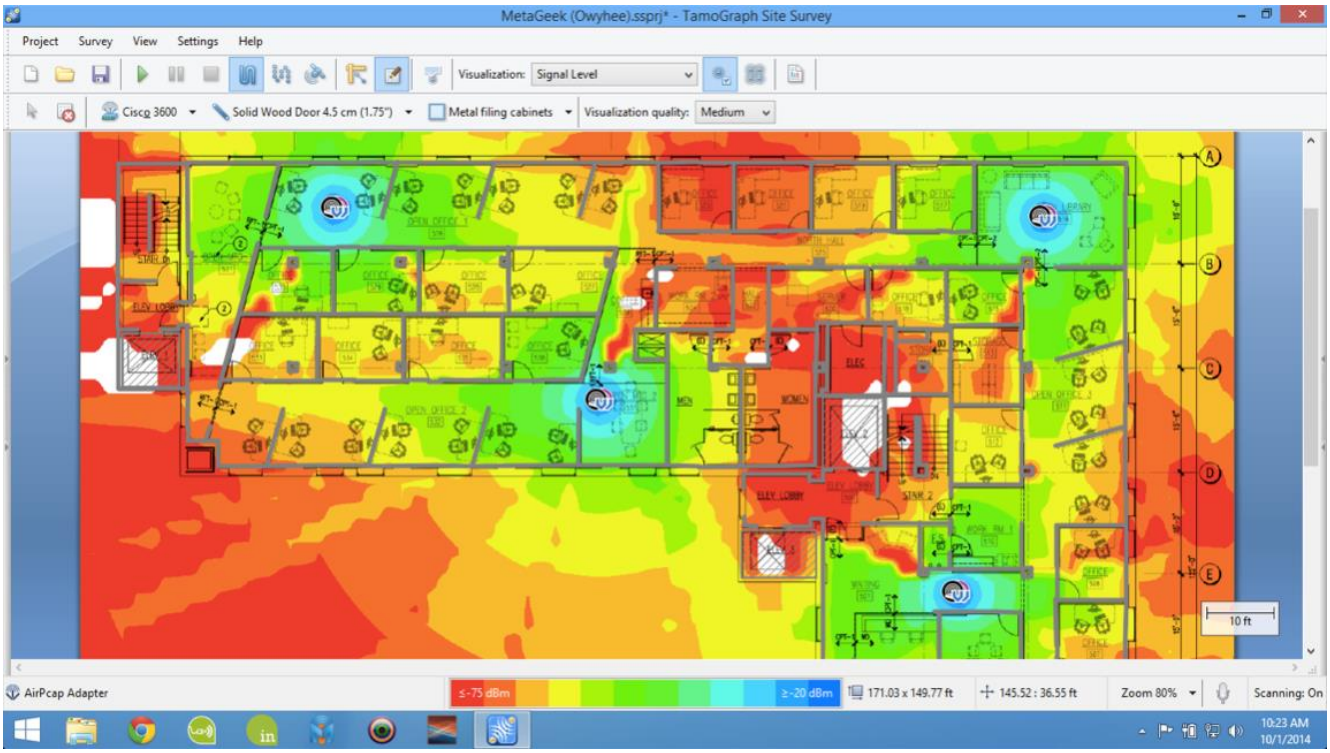
9.1 Tools

Designing and maintaining a dual-band wireless network requires a good toolset. Fortunately, there are many different types of tools from which you can choose.

9.2 Site Survey/Virtual Site Planning Tool

A Site Survey tool allows you to upload a floor plan of a building, and walk through the building to perform a survey. The result is a map of coverage or "heatmap," allowing you to view network coverage and cell overlap. Site survey tools are generally used for post-installation network validation or assessing the coverage of an existing installation.

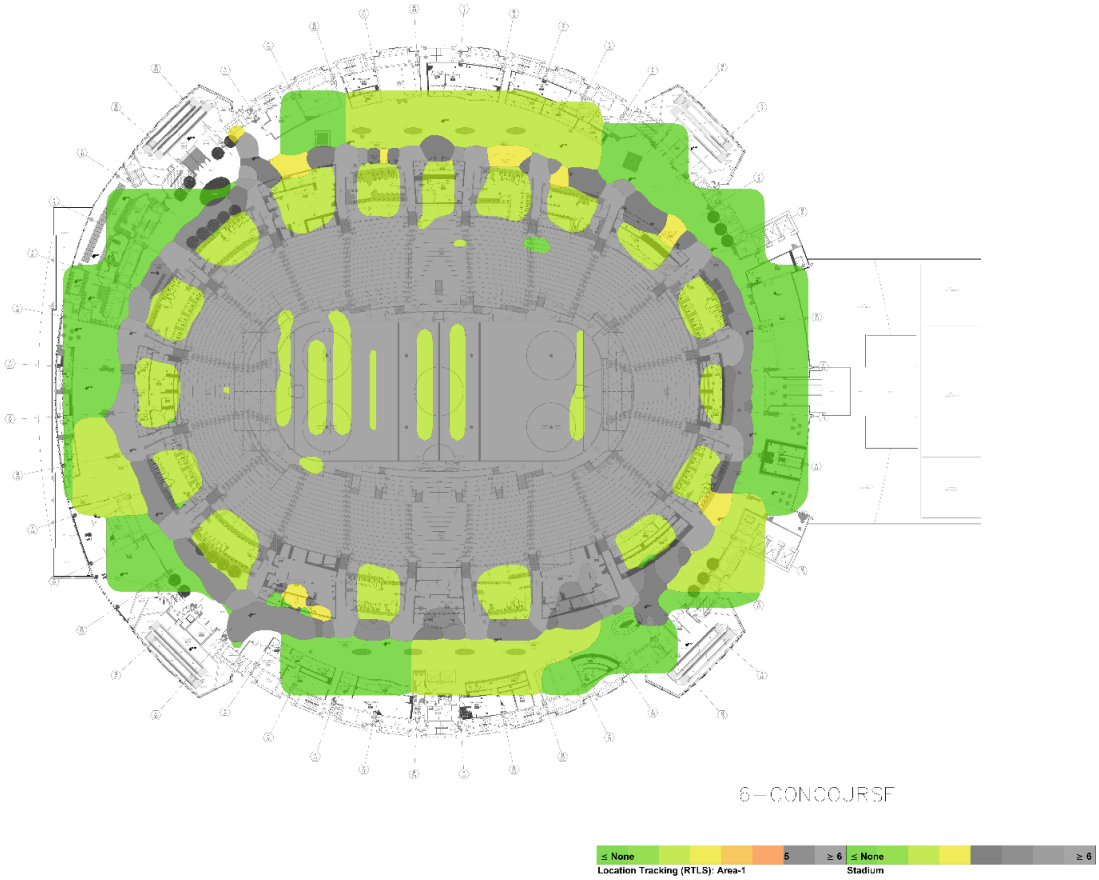
A Virtual Site Planning Tool (usually built into a site survey tool) allows you to draw wall types on a floor plan image and place virtual access points. The tool will then calculate approximate coverage in the building. Site planning tools are used for network planning, before the hardware is deployed.



Above is an example of a heat map generated by a site survey tool

9.3 Spectrum Analyzer

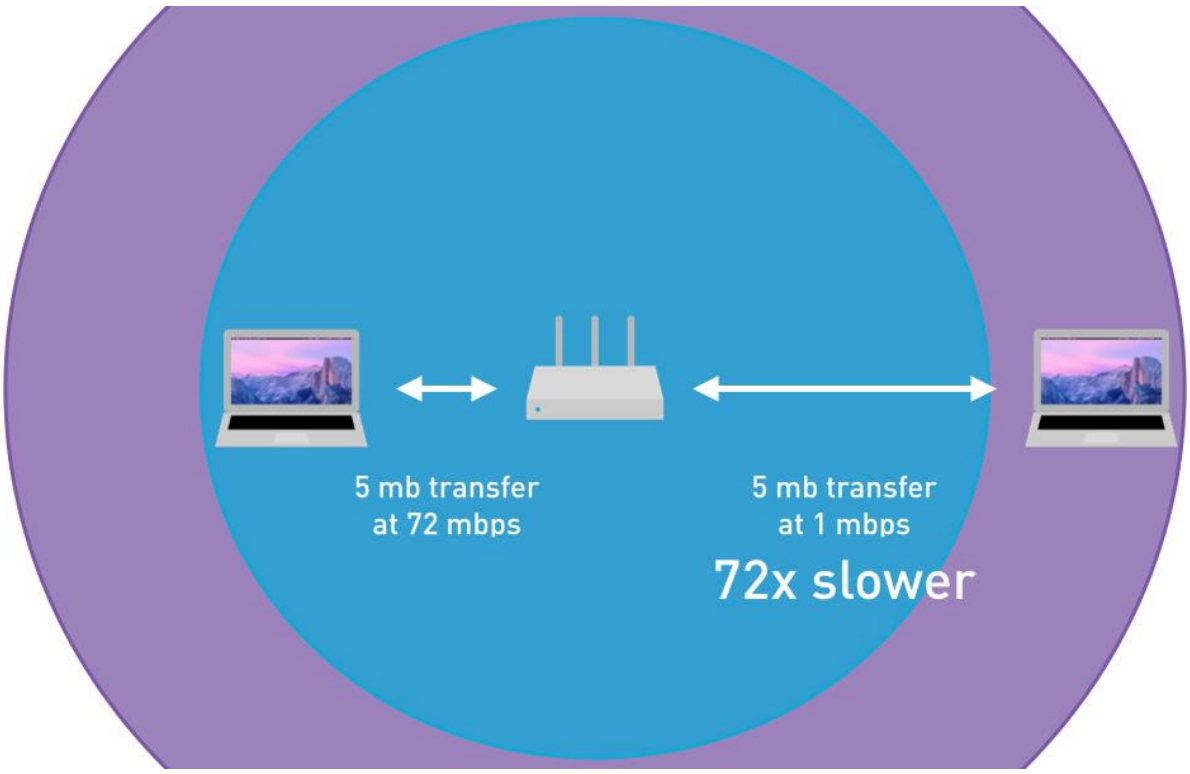
A spectrum analyzer, like an Ekahau Sidekick Pro, is a special piece of hardware that can visualize raw radio frequency activity. While commonly used to detect non-WiFi devices that might cause interference, a spectrum analyzer is also great for viewing channel utilization to see how busy a channel is.



Spectrum Anaylsis of the Garden during a Ranger Game

9.4 Access Points Support Legacy Data Rates

On each WiFi channel, only one device can talk at a time. Devices talking at slower data rates will take longer to transmit data than devices talking at faster data rates.



Allowing devices to talk at slower, legacy data rates can increase WiFi overhead by up to 40%.

Recommended Action

Disable legacy 802.11b data rates (1, 2, 5.5, and 11 mbps). Disabling slower data rates will force all devices to either talk faster, or disassociate from the network, which will increase overall network performance.

General Warnings

1. When legacy data rates are disabled, the coverage area will be slightly reduced (distant clients won't be able to fall back to slower but more reliable data rates)
2. Disabling legacy data rates will break compatibility for 802.11b devices (rarely an issue)

SOHO (Small Office/Home Office) Warnings

1. Most SOHO (small office/home office) routers won't allow you to disable legacy data rates
2. Most SOHO rates will allow you to "disable 802.11b", but usually the setting is ambiguous or doesn't really change anything

10 Conclusion

In this document I have attempted to explain the basics of WiFi connectivity and describe each of the components and how they are inter-related. Each component plays a critical role in producing a reliable dependable WiFi infrastructure that will meet our business needs.

Operating WiFi in an Arena or Stadium is much more complex than in a office building. Given the general round or spherical shape of most areans and stadium the propensity for channel overlap is high and is a common problem. Thus, the placement of APs and the associated signal strength and channel definition is a critical consideration in the design.

In this document I stuck to explaining the basic components of RF connectivity, from the client to the AP. Although not discussed in this document but equally as critical is the wired network. Your VLAN design, uplinks to the core, path to your wirless controller and your connectivity to the Internet (circuit sizes) will all play a significant role in developing and maintaining reliable WiFi performance.