WHITE PAPER

7 KEY FACTORS TO CONSIDER WHEN DESIGNING Wi-Fi NETWORKS

by Vladan Jevremovic, PhD

TABLE OF CONTENTS

01. INTRODUCTION 3

02. THE KEY NETWORK DESIGN CONSIDERATIONS 3

- 2.2 AP COVERAGE CONTROL 4
  - 2.2.1 Mismatched AP-Client Power 4
  - 2.2.2 RF Co-channel Overlap 4
  - 2.2.3 Hidden Nodes 6
- 2.3 THE DOMINANT USE CASE 7
- 2.4 VERTICAL MARKETS 8
  - 2.4.1 Educational/Classroom 8
  - 2.4.2 Warehouse/Manufacturing 8
  - 2.4.3 Retail 9
  - 2.4.4 Healthcare 9
  - 2.4.5 Stadiums 9
- 2.5 INTERFERENCE MANAGEMENT 10
- 2.6 RF BAND STEERING 10
- 2.7 CAPACITY PLANNING 11
- 2.8 DIFFERENCES BETWEEN DAS AND Wi-Fi NETWORK DESIGN 13
  - 2.8.1 Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) 13
  - 2.8.2 RF channel re-use plan 13
  - 2.8.3 RF Interference 14
  - 2.8.4 Ambient (Background) Noise 14
  - 2.8.5 RF Design Target KPIs 14
  - 2.8.6 Hidden Nodes 14
  - 2.8.7 Legacy Data Rates 14
  - 2.8.8 Layer 3 Roaming 14
  - 2.8.9 Power over Ethernet (PoE) 15
  - 2.8.10 Backhaul 15

03. CONCLUSION 15

04. ACKNOWLEDGMENT 15

01. INTRODUCTION

In the past, Wi-Fi network design meant little more than placing access points (APs) in conference rooms and break rooms, thereby providing isolated islands of Wi-Fi coverage in areas where people converged. In the age of smartphones and tablets, data usage has become so heavy, and use cases so diverse, that Wi-Fi network design requires strategic thinking. This white paper addresses the following seven Wi-Fi network design topics in detail and outlines best practices for Wi-Fi network design.

1 AP placement
2 AP coverage control
3 Dominant use case
4 Vertical markets
5. Interference management
6 Radio-Frequency (RF) band steering
7 Capacity planning

While this white paper addresses these seven common topics and factors that contribute to good Wi-Fi design, there are many more not included in this paper that should also be considered when designing a network. Therefore, this white paper does not intend to say that these seven factors are the only factors that matter, but that they are key considerations to make when designing a high-performance Wi-Fi network.

It also addresses a bonus topic:

8. The difference between Distributed Antenna System (DAS) and Wi-Fi network planning and design.

02. THE KEY NETWORK DESIGN CONSIDERATIONS

One potential source of AP interference is scattering and reflection from metal objects such as chain-link fences, wire mesh, and large metal surfaces. The latter are especially problematic if they are located near an AP because nearby RF reflection alters the AP's antenna pattern, thereby changing the RF coverage from what is expected.

Another potential source of interference is placing an AP near another RF source. Most APs have configurable RF channels, which means that any RF channel from the entire unlicensed band can be set to be operational by the network administrator. Such APs do not have specific hardware channel filters; for example, an AP configured to operate on Channel 6 in the 2.4 GHz Industrial, Scientific and Medical (ISM) band does not have a 20 MHz hardware pass-through filter centered on Channel 6. Consequently, having another AP nearby that transmits on Channel 1 or Channel 11 is likely to cause significant noise at the first AP.

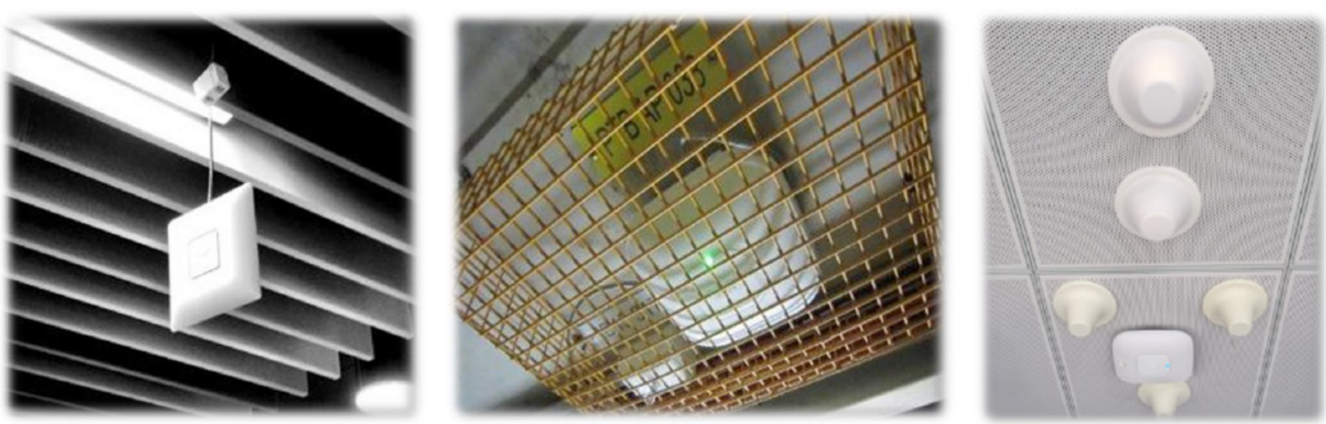

Figure 1: Examples of Incorrect AP Placement (Source: 7signal Solutions)

2.2 AP COVERAGE CONTROL

In the early days, APs were routinely installed with their default transmit power, often the maximum transmit power of 10 or even 20 dBm. However, due to densification of Wi-Fi networks, this is no longer recommended because leaving APs to transmit at maximum power may have adverse effects on network performance. Three issues stand out: mismatched AP-client power; RF co-channel overlap; and hidden nodes.

2.2.1 Mismatched AP-Client Power

If AP power is set at a fixed level, all clients should also transmit at that same level. If some clients transmit at lower power than the AP, there is a zone where those clients can hear the AP but the AP cannot hear them. This power mismatch creates a "dead zone" for those clients. Let's assume, for example, that an AP is transmitting at 10 dBm, and that the AP coverage edge is at -70 dBm. This is the boundary between the yellow and green areas in Figure 2. A client also transmitting at 10 dBm can be located right at the coverage edge, where the black smartphone symbol is, and still maintain connectivity with the AP. However, to maintain connectivity, a client that can transmit at only 5 dBm must be closer to the AP (where the blue smartphone symbol is). The coverage edge for the blue phone is -65 dBm. The yellow area between the two phones is the "dead zone", where the black phone can operate but the blue phone cannot. To eliminate the dead zone, AP transmit power should be set to the lower value, 5 dBm.

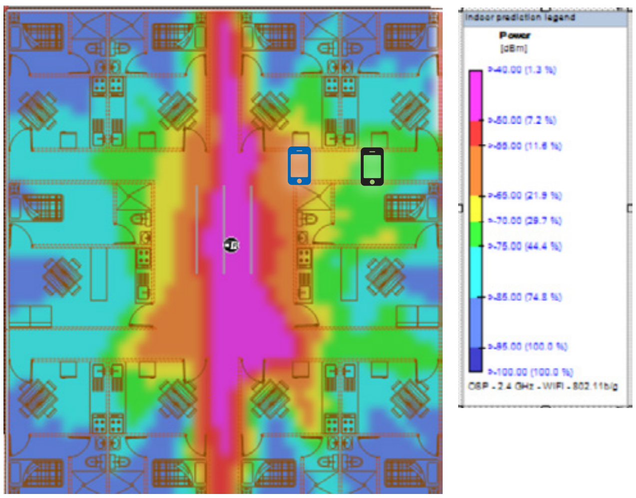

Figure 2: Mismatch in Power between AP and Client

2.2.2 RF Co-channel Overlap

Co-channel overlap is of great concern at 2.4 GHz where only 3 non-overlapping channels exist. As the channel reuse factor is only N=3, it is likely that a client may find itself in a location where it can "hear" two APs transmitting on the same channel. In that case, both APs will defer transmitting when the client is transmitting. Because this prevents both APs from transmitting, each such client accounts for double the airtime, thereby reducing network capacity. This is depicted in Figure 3. The smartphone is operating on Channel 6 and is located midway between the AP at the top left and that at the bottom right, both of which are also operating on Channel 6. It does not matter which Channel 6 AP the phone is associated with because it can be heard by both, and therefore both APs need to defer transmitting whenever the phone is transmitting.

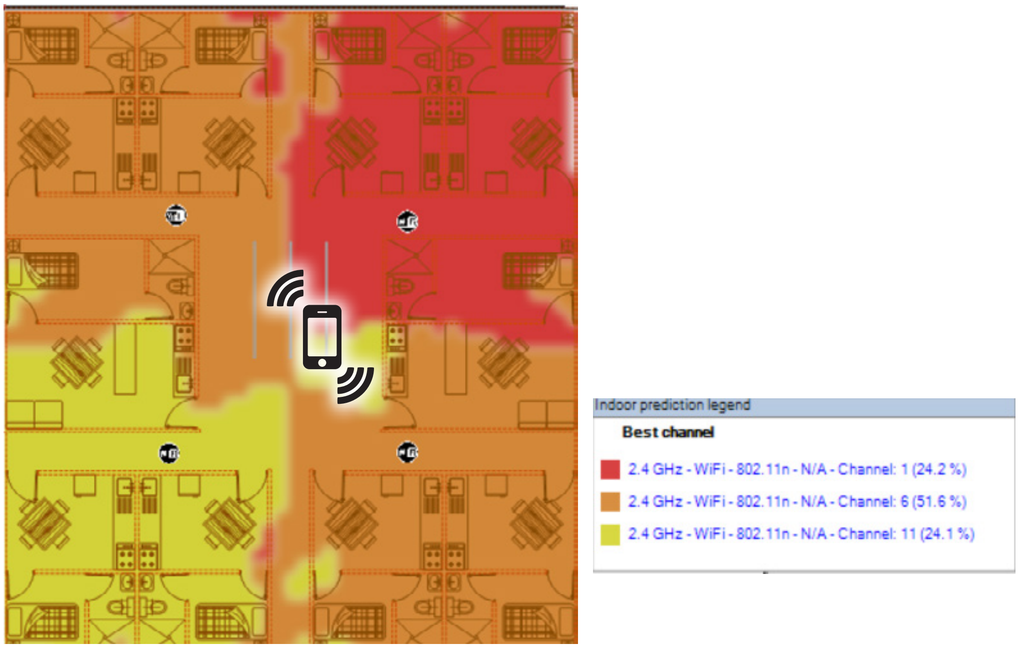

Figure 3: Clients at Cell Edge and Co-channel Interference (CCI)

The solution is to isolate signals from co-channel APs by at least 20 dB, as shown in Figure 4. Of interest are three APs: those at the top left and bottom right are operating on Channel 6 (orange coverage), while the one between them is operating on Channel 1 (red coverage). The middle AP serves as a buffer between the two co-channel APs. The signal difference between the co-channel APs should be at least 20 dB at the red coverage boundary.

The pushpin is located at the red coverage boundary. At this location, the top left AP signal level is -59.5 dBm while the bottom right AP signal level is -79.65 dBm. Thus, the difference between the two Channel 6 AP signal levels is approximately 20 dB, the desirable signal delta between the two. The 20 dB signal delta is easier to achieve if AP coverage is smaller, which is another reason to set the AP transmit power to less than its default value.

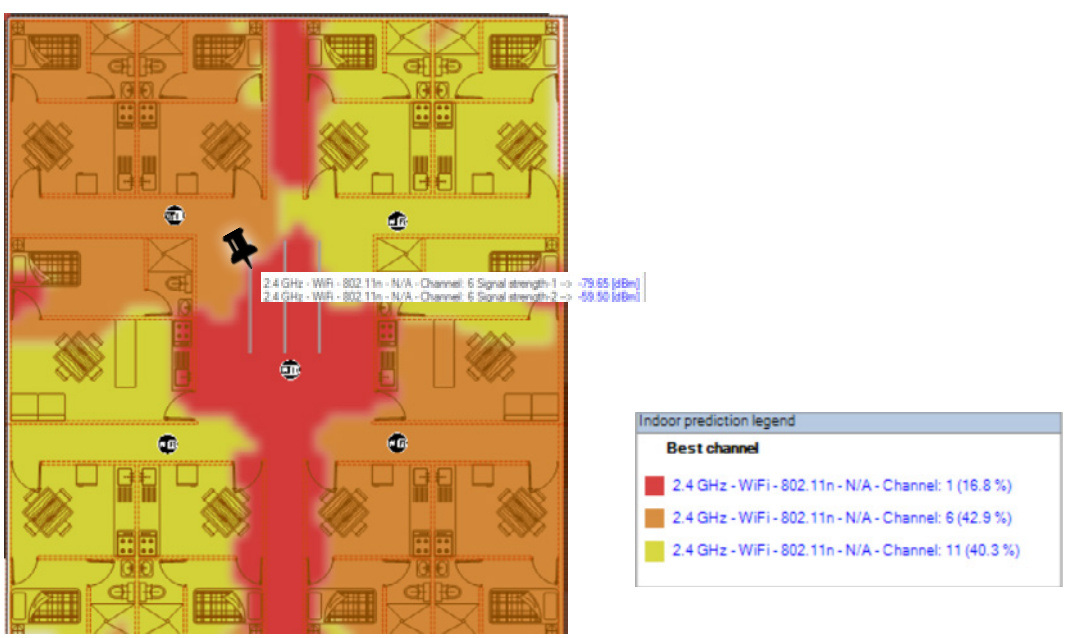

Figure 4: Recommended Co-channel Signal Isolation

2.2.3 Hidden Nodes

"Hidden node" refers to a phenomenon that occurs when two clients cannot hear each other, but the serving AP can hear them both. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is a fundamental mechanism that allows clients and APs to transmit one at a time. To minimize packet collisions, it is paramount that each client be able to hear all other clients within the AP coverage. If AP coverage is too large, clients at opposite ends of the coverage cannot hear each other and may therefore attempt to transmit packets simultaneously. This can cause packet collisions at the AP receiver, a condition which leads to packet retransmission, thereby slowing down all clients in the AP coverage area.

Figure 5 shows an example of a hidden node in a hotel. The AP is centrally located and has sufficient transmit power to provide plenty of coverage in the opposing hallways. The two clients, shown by the two black smartphone symbols, are located at the far end of each hallway. If they have the same transmit power as the AP, both can easily connect to the AP. However, due to the length of the hallways, the clients are unable to hear each other and their packets will often collide at the AP, causing retransmission. The solution is to install two APs, one in each hallway.

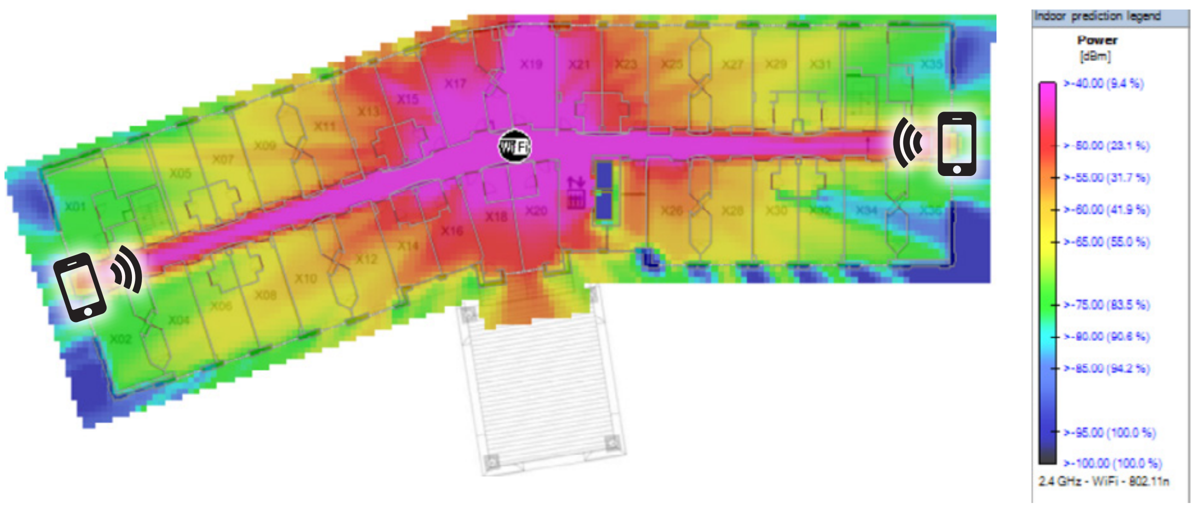

Figure 5: Clients and the Hidden Node Problem

Apart from reducing transmit power, AP coverage can also be controlled by disabling the lower data rates. As one moves away from the AP, Signal-to-Noise Ratio (SNR) drops and the data rate dynamically switches to a lower value. The lowest data rate is different for different 802.11 networks; for example, it is 1 Mb/s for 802.11b, but it is 6 Mb/s for 802.11a and g. In Figure 6, all data rates, 6 through 54 Mb/s, are initially enabled for the 802.11g AP, as shown in the screenshot on the left. To control the coverage, data rates 6 through 18 Mb/s are disabled, which shrinks the coverage slightly, as shown in the screenshot on the right. The resultant coverage is much tighter and the available data rates (24-54 Mb/s) are much higher.

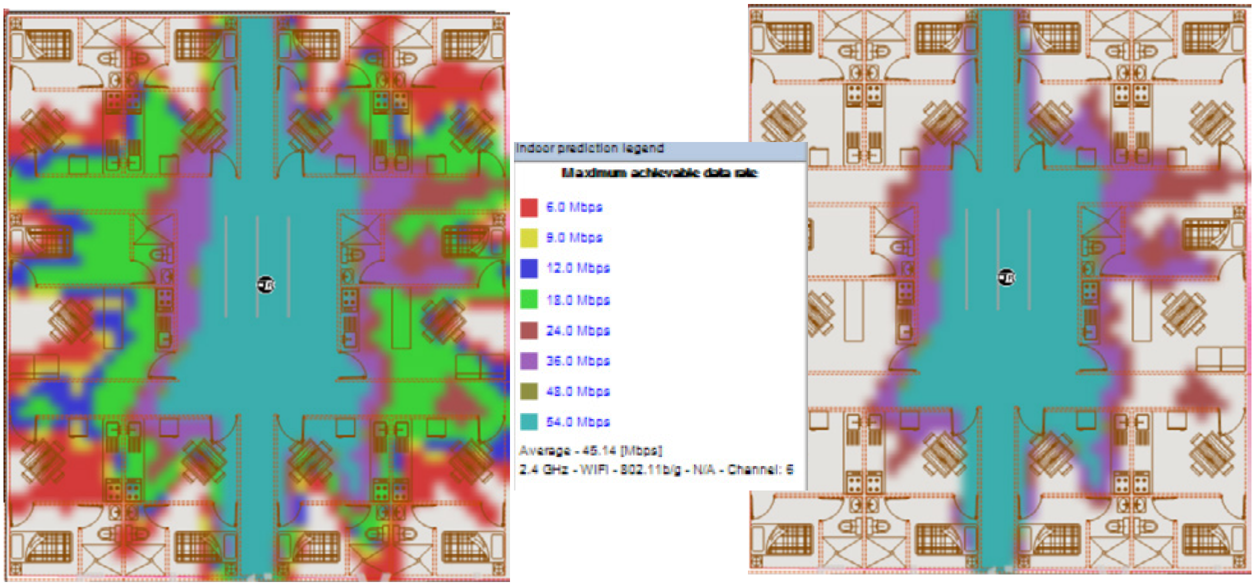

Figure 6: Coverage Control by Disabling Lower Data Rates

2.3 THE DOMINANT USE CASE

The dominant use case in a Wi-Fi network determines coverage design parameters. As a rule of thumb, the number of APs required for low-data-rate networks is fewer than the number required for high-data-rate networks, which is fewer than the number required for Voice over Wi-Fi (VoWi-Fi) networks. Most manufacturers recommend the following target signal levels:

- For low-data-rate networks, as is the case in warehouses, the minimum received signal strength should be -73 dBm.
- For networks with heavy file-sharing, as is the case in stadiums, the minimum received signal strength should be -70 dBm.
- For VoWi-Fi networks, as is the case in call centers, the minimum received signal strength should be -67 dBm.

However, these minimum signal-strength requirements are only helpful under the assumption of modest ambient noise (sometimes called background noise), -90 dBm or less. In a noisy environment, SNR should be used as the figure of merit rather than signal strength. Some OEMs recommend the following SNR values:

- Low-data-rate networks should have a minimum SNR of 18 dB.
- Networks with heavy file-sharing and downloading should have a minimum SNR of 20 dB.
- Networks in which VoWi-Fi use predominates should have a minimum SNR of 25 dB.

These Key Performance Indicators (KPIs) are summarized in Table 1 below.

USE CASE	LOW NOISE (< -90 dBm)	HIGH NOISE (> -90 dBm)
	Signal Strength, dBm	SNR, dBm
Low Data Rate (Handheld scanners, POS)	-73	18
High Data Rate (Video Streaming, File sharing)	-70	20
VoWi-Fi	-67	25

Table 1: Typical Design Key Performance Indicators (KPIs)

Thus, for a stadium network with a measured ambient-noise level of -70 dBm, the minimum signal level should be -70+20 = -50 dBm. This minimum received signal strength value is very high, which will consequently require many APs in the network. However, had we simply assumed a background noise level of -90 dBm (instead of the measured -70 dBm), and therefore designed for -70 dBm, the SNR would be -70+70=0 dB, and the network would be practically unusable. This example underscores the importance of bringing a spectrum analyzer to a site visit, an instrument capable of measuring not only ambient noise, but also in-band non-802.11 interference, as further discussed in section 2.5 below.

2.4 VERTICAL MARKETS

While identifying proper design target KPIs (received power or SNR) and setting AP transmit power to a value much lower than the maximum power provide a good starting point, design specifications must also consider vertical market specifics. This should be done because vertical markets differ in terms of user density (hotels versus warehouses, for example), use cases (Real-Time Location, VoWi-Fi, data), and RF environment (noisy versus average noise).

2.4.1 Educational/Classroom

Computer tablets have become common educational devices at all levels of education. Tablets rely exclusively on wireless connectivity to provide internet access. The number of tablets in a classroom is equal to the number of students, and it is reasonable to assume that at least occasionally all these devices will try to access the network at once. Most classroom walls are made of cinder blocks to attenuate noise during class. This material also attenuates RF propagation very effectively, thereby reducing channel overlapping to a great degree. To address the capacity and RF propagation specifics of classroom use, a general rule of thumb is to place one AP in every other classroom.

2.4.2 Warehouse/Manufacturing

Warehouses and manufacturing venues often deploy wireless handheld devices such as the bar code scanners which are used for taking inventory. These devices require only a low data rate, so this design is for coverage, not capacity. Care should be taken not to place APs near metal racks or heavy machinery, as metal surfaces affect antenna patterns and cause excessive interference.

2.4.3 Retail

Wi-Fi networks have several use cases in retail locations:

- Retail operations support equipment such as cash registers, time clocks, inventory control scanners;
- Tracking retail analytics, used to monitor customer movement and behavior. An example of retail analytics is shopper retention (i.e., how quickly shoppers return to a store after their initial visit);
- Location-based mapping and tracking services, used to provide turn-by-turn directions to the store from anywhere inside the shopping center;
- Internet connectivity

All the above, except the last, require only low-data-rate connectivity.

2.4.4 Healthcare

The primary healthcare use case is quick and secure access to patient medical data, and accurate tracking of patients admitted to the facility. Real-Time Location (RTL) solutions using 802.11 tags to locate patients are common. Medical equipment that is used to monitor patients' vital information often use integrated 802.11 wireless adapters to send data back to the nursing station. Medical carts used to enter patient information also connect to the network wirelessly. Various types of hospital equipment operate on proprietary or industry-standard wireless technology, thereby constituting a significant potential source of RF interference.

Because of the presence of wireless medical equipment, it is important to bring a spectrum analyzer to a hospital site visit and survey both the 2.4 and 5 GHz bands in all areas where the network is to be installed. Many hospitals also have a person or a department that keeps track of wireless medical equipment. To help identify the frequencies used at the hospital, this person should be interviewed during a site survey visit.

2.4.5 Stadiums

Currently, stadiums are by far the densest Wi-Fi networks being built. During the peak-usage hour at Super Bowl 2017, 30% of the attendees were simultaneously connected to the network. Stadiums are also by far the noisiest venues; it is common to find ambient noise between -80 and -70 dBm during an event. These very high values must be considered when designing a stadium network, so taking a spectrum analyzer to a stadium site survey is a must. Most stadium data traffic is video and picture upload and download, generated by the general audience. However, the network also needs to provide reliable connectivity for points of sale, video surveillance, ticketing, and other stadium infrastructure services.

Vertical market characteristics are summarized in Table 2 below.

Vertical Market	AP Density	Use Case	Design criteria
Educational	High	Low to High data rate	Capacity
Warehouse	Low	Low data rate	Coverage
Retail	Low	Low data rate	Coverage
Healthcare	High	VoWi-Fi, RTL	Coverage
Stadium	High	High data rate (high noise)	Capacity

Table 2: Summary of Vertical Market Characteristics

2.5 INTERFERENCE MANAGEMENT

Two types of interference can affect the operation of an 802.11 network: broadband and narrowband.

Broadband interference affects most or all RF channels in the band, and can knock out all APs in the network. One example of broadband interference is Bluetooth. Bluetooth operates on 79 pseudo-randomly chosen RF channels spaced 1 MHz apart between 2.402 and 2.480 GHz. As all 2.4 GHz Wi-Fi channels fall within this same frequency span, Bluetooth interference is broadband interference. The practice of transmitting on randomly chosen RF channels is called Frequency-Hopping Spread Spectrum (FHSS).

Other sources of broadband interference include medical telemetry and Digital Enhanced Cordless Telecommunications (DECT) cordless phones, which also use FHSS. While a single FHSS device may not affect the network, many FHSS devices in a limited space can do just that; for example, Bluetooth headsets and DECT cordless phones in a call center. It is easy to see why those two device types should be banned in any call center that relies on VoWi-Fi for voice calls.

Narrowband Interference affects only a portion of the spectrum and may therefore affect only some channels. An example of narrowband interference is that from microwave ovens, as their radiation usually affects only the upper portion of the 2.4 GHz spectrum.

Potential interference sources in the 2.4 GHz and 5 GHz bands are listed in Table 3.

2.4 GHz	5 GHz
Bluetooth radios (cordless mouse, keyboard, headset...)	Cordless phones
Cordless phones	Radar
Wireless video cameras	Perimeter sensors
Nearby WLAN	Digital satellites
Microwave ovens	Nearby WLAN
Fluorescent bulbs	Outdoor wireless 5 GHz bridges
Elevator motors	
Plasma cutters	

Table 3: Sources of Interference in the 2.4 and 5 GHz Bands

2.6 RF BAND STEERING

"Friends don't let friends use 2.4 GHz" is a slogan that is popular in the Wi-Fi community for good reason. With only 3 non-overlapping 20 MHZ channels in the 2.4 GHz band, and up to 22 non-overlapping 20 MHz channels in the 5 GHz band, it is clear which network has less co-channel interference (CCI). As more than 80% of the clients in today's market are dual-band, it is imperative to design and deploy APs with dual-band radios. The actual number of non-overlapping channels in the 5 GHz band can be 8, 12, 17, or 22, depending on the region and whether clients are certified for Dynamic Frequency Selection (DFS) for channels shared with Terminal Weather Doppler Radar (TWDR).

If both radios transmit at the same power level, approximately twice as many 5 GHz radios are needed as 2.4 GHz radios for the same RF coverage. The 2.4 GHz network has less capacity (fewer radios) than the 5 GHz network, and it also has higher interference (higher CCI) than the 5 GHz network. As RF conditions are more favorable for the 5 GHz network, it is clear that more clients should be attached to that network than to the 2.4 GHz network.

The practice of directing a dual-band client to connect to a network using a preferred spectrum band is called "RF band steering". This is done by manipulating the MAC sublayer. When a dual-band AP hears probe requests to both bands from the same client radio, it responds by using only 5 GHz transmissions. The percentage of clients to be directed to the 5 GHz band is a configurable parameter on APs from many vendors.

Band steering is simply another name for load balancing between the frequency bands. It should not be confused with load balancing between APs.

2.7 CAPACITY PLANNING

"How many APs am I going to need for this venue?" is the first question that many Wi-Fi network planners hear from the IT manager. Many OEMs specify the maximum number of concurrent clients for a specific application. For example, Cisco recommends a maximum of 27 VoWi-Fi calls when connected at 24 Mb/s or higher in the 5 GHz band. If connected at 12 Mb/s or higher, a maximum of 20 VoWi-Fi calls is recommended. These guidelines may be sufficient to determine the required number of APs in a call center, where VoWi-Fi is by far the most dominant application. However, in most venues, traffic is a mix of various applications: VoWi-Fi; email; web browsing; file downloading; video streaming; etc.

To calculate capacity with any precision, several parameters must be specified/assumed:

- Specify the amount of traffic, in MB, that an active client will transmit/receive during busy hour.
- Specify the percentage of active users during busy hour. At the 2017 Super Bowl, 30% of the attendees were active during busy hour.
- Specify busy-hour airtime utilization percentage; to allow room for growth, this is usually set to a value somewhat less than 100%.
- Hotspots at the venue should be identified, and the number of clients within each hotspot should be specified. The number of clients in the remaining area should also be specified.
- The client split between the 2.4 GHz and 5 GHz bands should be assumed.
- Specify the network overhead. 802.11ac and 802.11n have about 20% overhead; 802.11b/g and 802.11a have about 50% overhead. The overhead is due to airtime contention and control and management frames, as specified in the CSMA/CA algorithm.
- Finally, a mix of 1, 2, 3 and 4-stream client devices should be assumed; simply deploying 802.11ac does not mean that every client in the venue can support four MIMO streams!

A good starting point is to design the network for coverage first and then calculate the capacity coverage map (Figure 7). This map will show if an AP can support the specified data traffic load (green), or if it will fail either because it exceeds the specified airtime percentage utilization (bright red) or because it connects to too many clients (hardware limit, dark red).

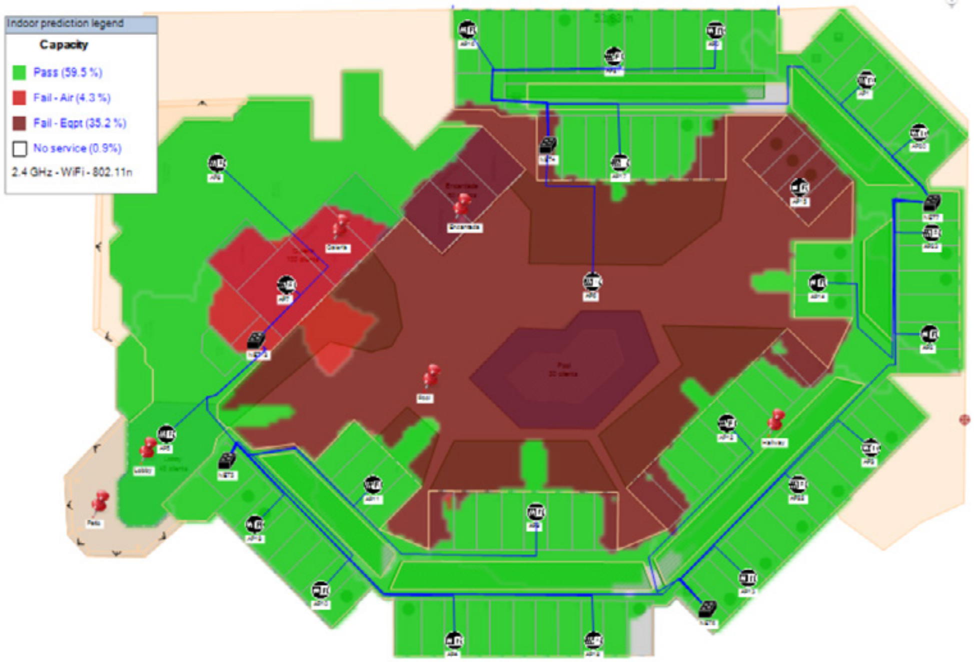

Figure 7: Capacity Coverage Map Identifies Passing (green) and Failing 2.4 GHz APs (light & dark red)

In the example shown in Figure 7, we used dual-band radios and assumed a high ratio of 2.4 GHz to 5 GHz clients (80%-20%), which leads to several 2.4 GHz APs failing. All that is needed to remedy the situation is to change the ratio to 40-60%, and all 2.4 GHz APs pass (Figure 8):

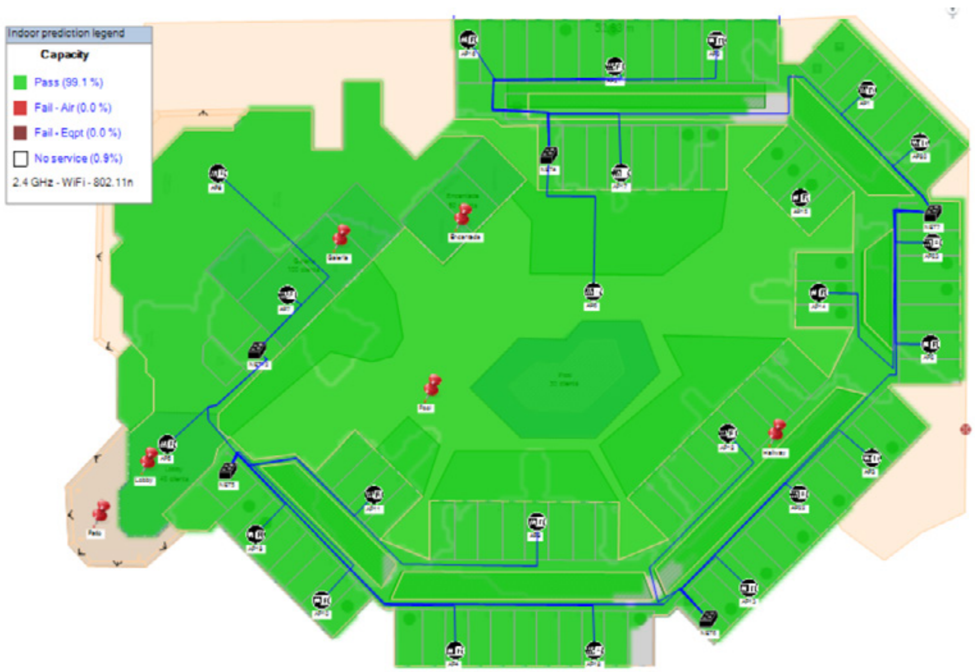

Figure 8: After changing the ratio of 2.4 GHz to 5 GHz clients, all 2.4 GHz APs pass

Once all APs pass, the minimum number of APs needed to support the busy hour traffic has been determined.

Another question that the IT manager may ask is "what is the average data rate for my clients?" An average-data-rate-per-client coverage map (Figure 9) answers that question.

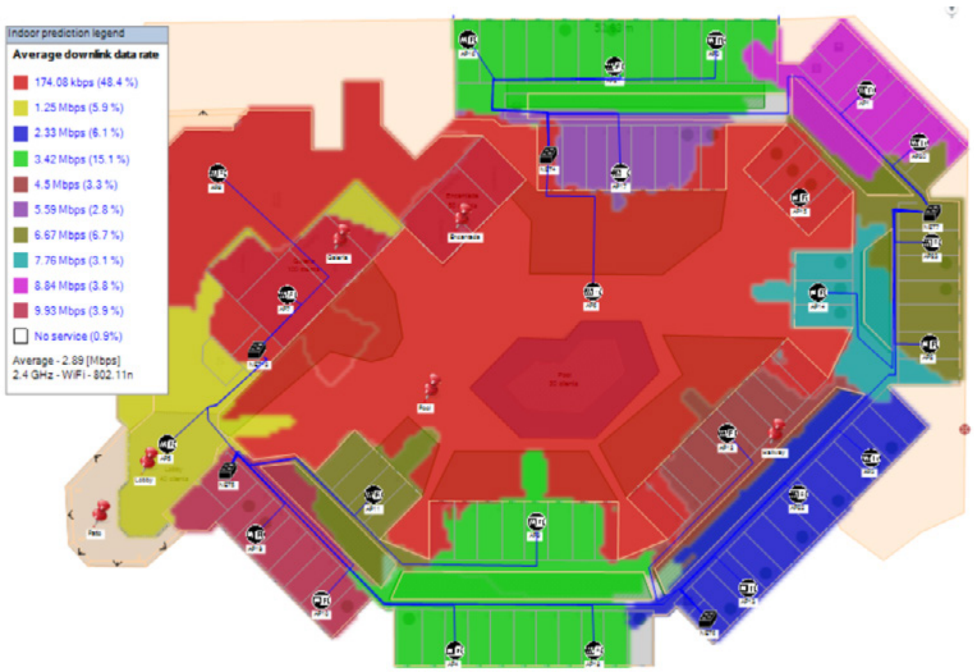

Figure 9: Average Data Rate per Client during Busy Hour

The average data rate per client coverage map is valid for the specified data traffic during busy hour. It should not be confused with the instantaneous client data rate during active transmission, higher than the average data rate.

2.8 DIFFERENCES BETWEEN DAS AND Wi-Fi NETWORK DESIGN

For the benefit of DAS engineers, we underscore the major differences between DAS and Wi-Fi network planning and design:

2.8.1 Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

APs and clients compete for airtime. The CSMA/CA mechanism brings order to the chaotic nature of airtime competition to ensure that clients and APs transmit one at a time. DAS and small cells can simultaneously address multiple clients by using different sub-channels of a licensed band.

2.8.2 RF channel re-use plan

RF planning for Wi-Fi networks must include an RF channel re-use plan. Unless a DAS carries GSM signal, RF channel planning is not needed for DAS networks. Cell ID planning is however needed for LTE small cell networks.

2.8.3 RF Interference

Since 802.11 networks share the band with non-802.11 transmitters, there are many instances where the latter interfere with the former. Bluetooth and DECT devices can easily slow down a nearby AP, while an old or leaky microwave oven can completely knock it out. Detection of potential interferers in the Industrial, Scientific and Medical (ISM) and Unlicensed National Information Infrastructure (U NII) bands should be done by surveying the venue with a spectrum analyzer.

2.8.4 Ambient (Background) Noise

A DAS network must deal with uplink noise caused by Remote Unit amplifiers. Once a DAS network is installed, the amount of uplink noise it contributes to an RF receiver is constant, and is solely a function of the DAS architecture and the number of amplifiers. Unlike DAS networks, Wi-Fi networks must deal with noise caused by RF and non-RF transmitters that operate alongside 802.11 in the unlicensed band. This ambient noise is venue-specific and, even within the venue, may fluctuate significantly between quiet and busy hours. It is important to determine busy-hour background noise before proceeding with the design, as it may affect target KPIs.

2.8.5 RF Design Target KPIs

Wi-Fi RF design target KPIs are different for voice and data applications. DAS design target KPIs are not application-specific.

2.8.6 Hidden Nodes

DAS remote units always transmit at full power. Wi-Fi APs cannot be left to transmit at default full power because doing so increases the chance that some clients within the AP coverage will not hear others. When this happens, the clients' packets collide at the AP receiver, which causes retransmission, which slows everybody down.

2.8.7 Legacy Data Rates

A Wi-Fi network planner must decide whether to enable or disable low legacy data rates such as 1Mb/s. Allowing this data rate to be "ON" slows everybody down and may cause the "sticky client" problem, where low-data-rate clients stay connected to an AP instead of handing off to a much closer AP. DAS planning does not need to consider low legacy data rates.

2.8.8 Layer 3 Roaming

Handing off a client from one AP to another is a Layer 2 (MAC) functionality. However, if the two APs belong to separate IP (Layer 3) subnets, a client station must re-establish IP connectivity while roaming from one AP to another. In that case, any connection-oriented applications that are in active session must be restarted when crossing Layer 3 subnets. The solution to that problem is Layer 3 roaming based on the Mobile IP standard, which allows the client to move from one IP subnet to another while maintaining the original IP address. Determining IP subnet boundaries is an integral part of Wi-Fi network planning. DAS network planners do not need to consider IP subnet boundaries.

2.8.9 Power over Ethernet (PoE)

Power over Ethernet is a preferred method for powering enterprise-class access points. Access points get their power from switches and controllers via low voltage Ethernet cables. A typical enterprise grade switch can have multiple 48-port line cards that are housed in a chassis. If the switch is PoE grade, the ports can provide up to 15.4 W of power, and the chassis itself may require up to 2 kW of power. The wiring closet has its own power specification, between 1650 and 3300 W. Aside from APs, PoE switches also provide power to desktop VoIP phones and video cameras. A Wi-Fi network planner has to include them all in the PoE power budget to ensure that enough power is available at the switch ports to supply all power devices, including APs.

2.8.10 Backhaul

Backhaul requirements must be considered by both cellular and Wi-Fi network planners. However, there are differences. Backhaul dimensioning of all RF sources that connect to the DAS network is done by backhaul engineers working for network operators. These are not the RF engineers that designed the DAS. On the other hand, the same person who designs the Wi-Fi network must also dimension the backhaul for each AP in the network. The AP backhaul calculations must take into account realistic RF channel widths 802.11 overhead and MIMO order to get realistic throughput rates in both spectrum bands, if the AP is dual-band. Based on these calculations, the optimum backhaul solution that matches or exceeds this throughput is chosen.

03. CONCLUSION

Wi-Fi network densification, along with proliferation of non-802.11 devices operating in the ISM and U NII unlicensed bands, has made Wi-Fi network planning a much more complex task than it was just a few years ago. Planning of 802.11 networks will become even more complex with upcoming mass deployment of License Assisted Access LTE (LAA-LTE) small cells and LTE-enabled devices in the 5 GHz U NII band. This white paper discusses seven topics that need to be considered when planning and designing Wi-Fi networks, and gives best practice recommendations. For the benefit of DAS RF engineers, the major differences between designing DAS and Wi-Fi networks are also outlined.

04. ACKNOWLEDGMENT

Figure 1 has been taken from a presentation at the 2015 Wireless LAN Professionals Conference (WLPC) by Veli-Pekka Ketonen, the CTO of 7signal Solutions, Inc.