Divergent Dynamics
The Time Has Come

Advisory & Design Services • Education • Diagnostics & Optimization • Security & Compliance • WLAN Infrastructure

2.4GHz is Dead

Abandoning the 2.4GHz ISM Band for Greener Wi-Fi Pastures

Devin K. Akin, CEO
Devin@DivDyn.net

November 14th, 2014
Version 1.00

Preface

The 2.4GHz ISM is dead for Wi-Fi connectivity. If you disagree, then perhaps your experience with implementing 2.4GHz in schools, hospitals, retailers, warehouses, manufacturing facilities, and multi-tenant office buildings differs from ours. One thing is undeniable: the 2.4GHz ISM band is getting so crowded, and the characteristics of 2.4GHz channels are such that interference (even with itself) makes it a sub-par choice for high performance Wi-Fi connectivity. As an industry, we've outgrown the venerable 2.4GHz ISM band, with its measly 83.5MHz of spectrum and three non-overlapping channels. It's our assertion that there are only two kinds of 2.4GHz Wi-Fi networks: 1) those that are extremely congested and unsuitable for Wi-Fi client connectivity, and 2) those that will be that way soon.

Divergent Dynamics focuses on designing and super-charging Wi-Fi infrastructures. The number one problem we have with enhancing overall Wi-Fi network performance is coping with the limitations of the 2.4GHz band, both from the infrastructure and client perspectives. A large effort must go into extracting a small overall performance gain from the 2.4GHz band. In this white paper, I will go into many reasons why. It's time for us to remove 2.4GHz from mainstream Wi-Fi connectivity use, and this whitepaper will discuss a significant number of reasons why.

Why is 2.4GHz Dead?

There are some specific limitations of the 2.4GHz ISM band that deserve to be called out right in the beginning:

- Not enough channel space, limiting channel reuse
- Too much penetration, limiting channel reuse
- Too much interference in the band, and getting worse

Channel Space in the 2.4GHz ISM Band

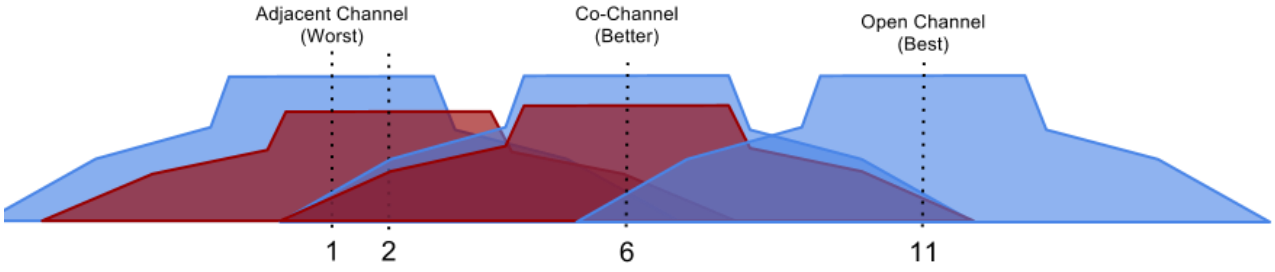
The 2.4GHz band only has 83.5MHz of usable channel space, and in contrast to the 5GHz UNII bands, which now have 25 usable 20MHz channels with 12 more proposed by the FCC, for a total of 740MHz of spectrum that can be carved up into 20MHz, 40MHz, 80MHz, and 160MHz channels as supported by the equipment in use. Due to signal penetration characteristics and not having enough non-overlapping channels (three in North America) for adequate channel reuse, 2.4GHz has become inadequate for high-density deployments and high channel load scenarios.

2.4GHz Signal Characteristics

2.4GHz signals penetrate walls (of many kinds), shelved products, and other obstacles much better than an equivalent signal amplitude at 5GHz (4.3X in open space). The result of this penetration is adjoining collision domains. This happens when APs can hear each other, when client devices can hear each other, or when an AP & client can hear each other (on the same channel, at a signal level sufficient to cause back-off to occur). We have traditionally designed for APs not to interfere with each other, called co-channel contention (CCC), using -87dBm as an industry standard, same-channel, signal level. Today's Wi-Fi chipsets, especially when they are paired with good antennas, can have receive sensitivity levels (at low and mid data rates) that are well below the typical 2.4GHz noise floor (~93dBm). With this information, you can quickly deduce that our -87dBm threshold is often not low enough. Consider that Wi-Fi client devices often move directly between APs that are appropriately spaced, where a client device can effectively adjoin two AP collision domains into one. If the APs and other clients within either Basic Service Set (BSS) had newer chipsets (e.g. 802.11n), then there would be a need to further reduce the output power of the APs and to space them even further apart.

The problem with CCC is that when more client devices and Access Points share the same channel, they share the channel's data throughput capacity. As the device density on a channel increases, associated client devices each get a smaller piece of the capacity pie and the negative effects of medium contention (e.g. retransmissions) increase. This further degrades the performance and capacity of the channel and all radios using it. Marcus Burton wrote an excellent white paper on the IEEE 802.11 protocol contention process.

2.4GHz channels also experience Adjacent Channel Interference (ACI), which is more detrimental to the user experience than CCC. Referencing the graphic below (from MetaGeek's excellent blog), you can visualize the difference between ACI and CCC. CCC adjoins multiple Basic Service Sets (BSS), also known as "cells", into one big collision domain. The 802.11 protocol is designed to deal with contention quite well. ACI, caused by channel overlap, will result in many corrupted frames and retransmissions on both channels. This will cause devices on both channels behave erratically and often ruins the user experience.



Credit: Metageek

Protection Mechanisms

Protection mechanisms, such as RTS/CTS and CTS-to-Self are used to notify legacy stations to be quiet. Use of these protection mechanisms are necessary in cases where newer stations would like to use modern forms of modulation that are not understood by the legacy stations. In 2.4GHz, this is worse than with 5GHz because we have to deal with 802.11b, 802.11g, 802.11n, and even non-standard implementations of 802.11ac in 2.4GHz (e.g. Broadcom's TurboQAM). Having so many supported modulation types in 2.4GHz (e.g. DSSS, HR/DSSS, ERP-OFDM, HT-OFDM, and even VHT-OFDM) means that protection mechanisms at both the Layer-1 (PHY) and Layer-2 (MAC) layers are constantly in use. In fact, they're so pervasive that some chipset vendors have stopped supporting Greenfield Mode altogether.

Why are we discussing protection mechanisms? Because they cause BSS capacity losses of 40-60%, depending on which type and how many are active at any given time. In other words, the less protection mechanisms are in use, the better our Wi-Fi performance. Unlike with 802.11g, there were very few 802.11a-only client devices released into the market. 5GHz went prime time with the mainstream adoption of 802.11n dual-band adapters. For this reason, it's not uncommon to see 802.11n-only or 11n/11ac environments in 5GHz, and such environments can be tuned for very high performance.

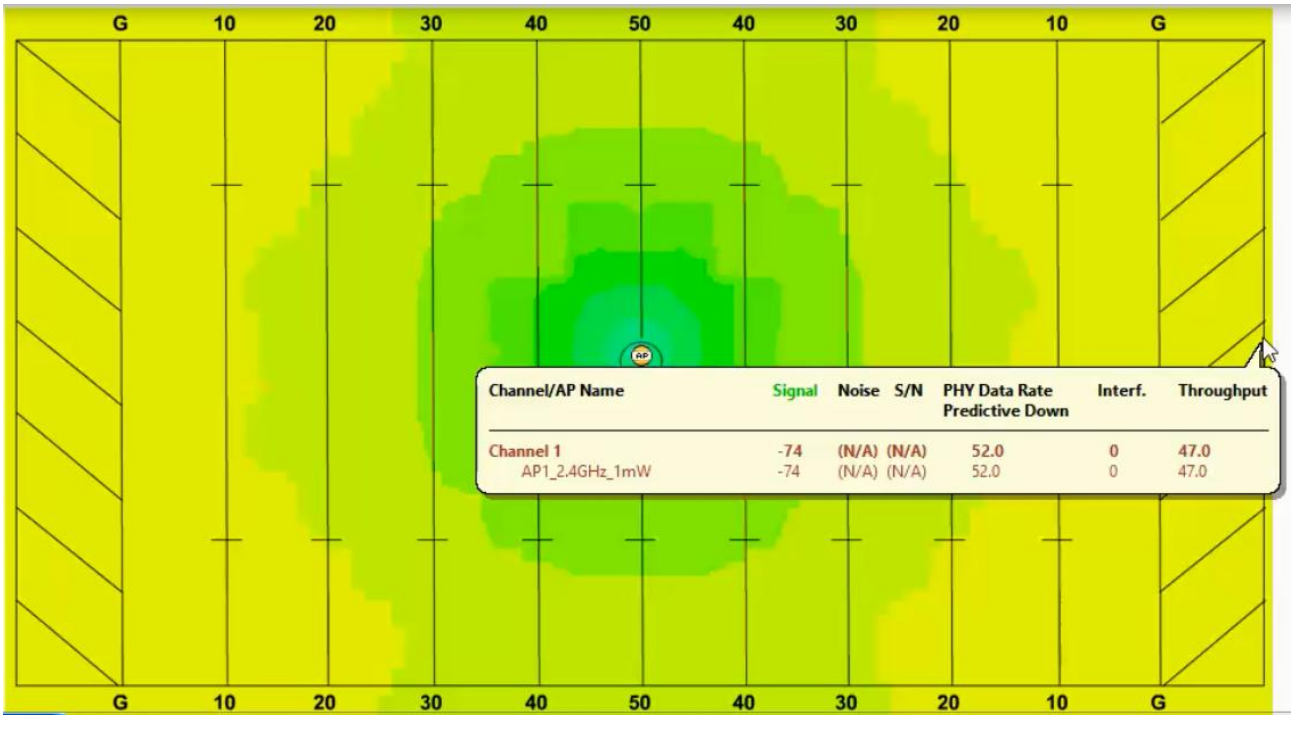
Channel Reuse

Channel Reuse is the ability to reuse the same channels within areas of desired Wi-Fi coverage. In order to successfully effect channel reuse, we need to consider antenna types, output power, and AP placement (at a minimum) within our design. The goal is to have a desirable amount of RF coverage where we want it and to minimize RF coverage where we don't want it. Less channel reuse results in less performance and capacity.

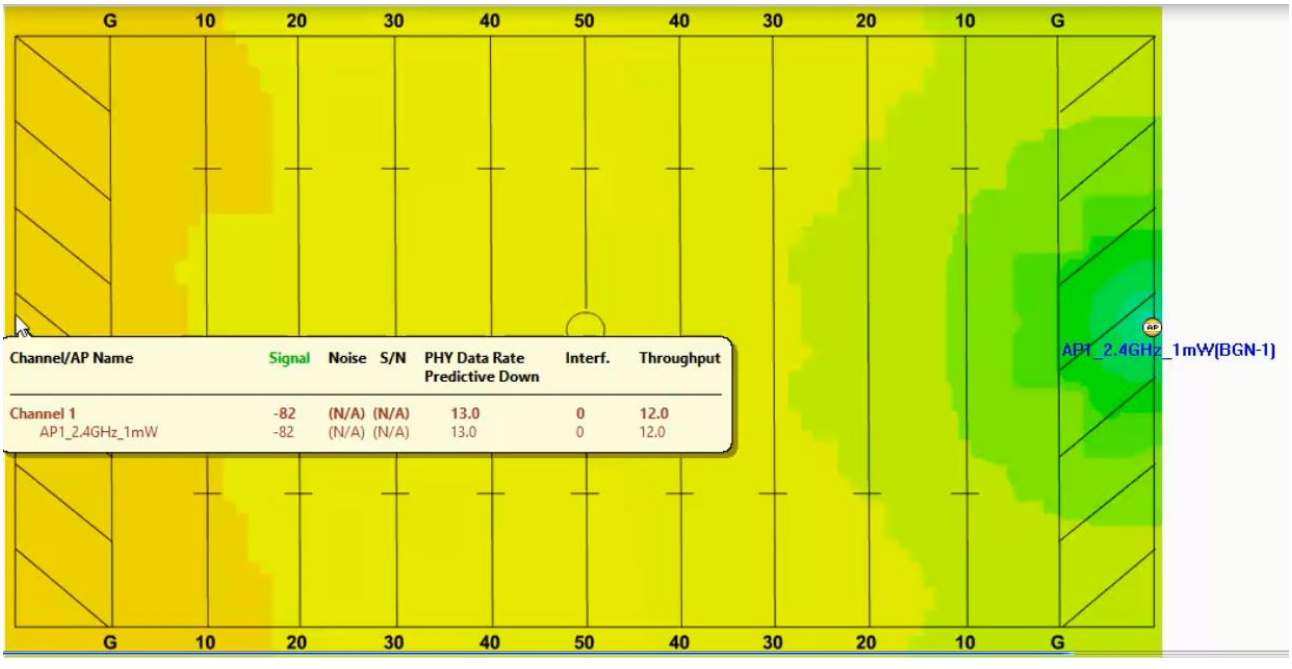
When using the 2.4GHz ISM band in North America, only three non-overlapping channels exist: 1, 6 and 11. If you want to limit your use of the 2.4GHz band to a single AP on each of these three channels, with the APs appropriately spaced apart, then that will be a fine design, with the exception that there will be very little data capacity across your enterprise. Even in such an extreme scenario, you may have neighbors who are using 2.4GHz who will interfere (i.e. CCC) with at least one (but probably all three) of your APs. If you have a large facility, with very thick walls, and your APs have low output power, low radio sensitivity, low antenna gain, and are spaced as far apart as possible, then you may be OK to have two APs using the same channel (for a total of 6 APs using 2.4GHz within the facility). 2.4GHz penetrates well, and thus is great for a coverage-based design

where capacity doesn't matter. The problem is that capacity matters greatly in many markets and scenarios. 2.4GHz's high penetration characteristics are a bad thing for networks designed for capacity because it introduces CCC, which is essentially the "sharing of the channel."

To illustrate the extent to which CCC is a problem in 2.4GHz, consider the following illustrations. The first graphic shows an Access Point, located in the middle of a football field (120 yards / ~110 meters wide including end zones), with a 2.15dBi antenna (minimum gain), using only 2.4GHz, at 1mW output power.



60 yards (~55 meters) away from the AP, at the end of the end zone, we see that we still have -74dBm of signal level. This is good enough signal level, assuming a good SNR (due to a reasonably low noise floor), to achieve fairly high data rates. Consider Cisco's AP3700 receive sensitivity chart, which shows that the AP can properly decode a 6Mbps transmission at -91dBm. So even if you disable 802.11b data rates (1, 2, 5.5, & 11Mbps), which is a recommended practice for most modern networks, we're still dealing with -91dBm. Let's move our AP over to the end of one end zone, and take a look at the signal level (RSSI) at the end of the other end zone.



As you can see, we are still receiving -82dBm when separated by the full 120 yards. Keep in mind that this is at 1mW of output power, and it's extremely common to find networks configured for 100mW and a minimum data rate of 1Mbps. Referring back to Cisco's receive sensitivity chart, 1Mbps transmissions can be decoded with signal levels of -101dBm or greater, and in 2.4GHz, where the noise floor is often -85 to -93dBm, such a receive sensitivity means "if I can hear it, I can decode it." If an AP can decode the transmission, it will back off, giving way to that transmission. Even at modest output power levels (e.g. 20-50mW), this means that oftentimes, every AP on a channel within a building (depending on the building size, shape, and building materials) can hear every other AP on that channel – one giant collision domain. When doing Wi-Fi performance optimization, it's our "Prime Directive" to divide collision domains – e.g. preventing CCC. Andrew Von Nagy wrote an excellent blog on receive sensitivity here.

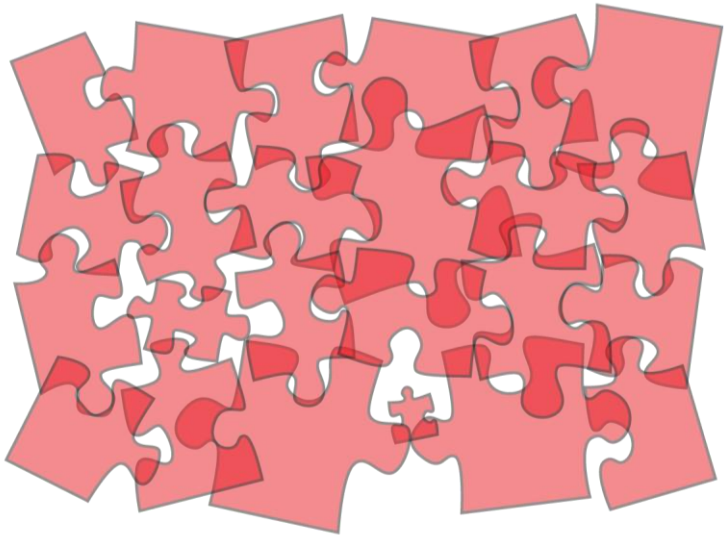
Even when the APs are appropriately powered and spaced, such that they cannot hear each other above the contention threshold (an amount of power that causes them to back off), when clients roam between the two APs, while associated to either AP, all three devices (along with any other client devices that can hear either AP) now share the channel's contention domain for however long both APs can hear the client device. How often does this happen? Constantly…. continually…. always! There are almost always client devices somewhere between two APs using the same channel. This is why high penetration characteristics are so detrimental to performance. The ideal capacity scenario is for there to be no penetration of walls by the RF. The ideal *coverage* scenario is to have maximum penetration. As an industry, we transitioned from coverage-based to capacity-based designs more than a decade ago.

If we mentally take this a step further, we quickly figure out that 2.4GHz has no reasonable solution for handling capacity (high throughput and/or high density). Trying to maximize capacity across 2.4GHz is like applying a couple of boxes of Band-Aids to a neck laceration. If APs can hear each other or client devices that are located between APs on the same channel, we will have one big collision domain across those two APs and most, if not all, of their collective clients. The same could hold true of 10 APs within the same facility due to output power, wall penetration, physical proximity of the APs, and receive sensitivity.

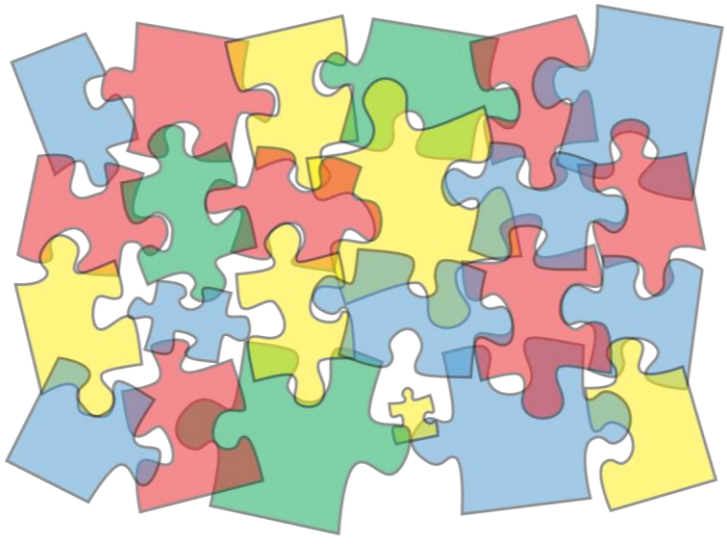
Typically "experts" will instruct you to turn down the power on the 2.4GHz AP radios, but turning down the output power can lower the data rates that will be used by the AP & clients. Using lower data rates results in more airtime utilization by each client, which limits the capacity of the channel. Turning down the output power often doesn't help with the CCC problem at all unless it's also used in conjunction with disabling lower orders of modulation (e.g. turning off data rates like 1, 2. 5.5, 11, 6, and 9 Mbps – at a minimum) and using physical spacing and building materials to divide the collision domains. Use of lower order modulation often results in *sticky* clients, which will refuse to roam to a better AP in an appropriate manner. This can cause very large collision domains.

At the opposite extreme, it's not uncommon to see the noise floor rise to -65dBm or higher in high-density 2.4GHz scenario because of the collisions and client probing. This then requires that AP power be turned up (to increase SNR), which then results in CCC, which then results in a system-wide reduction of capacity. There's really no way to win with 2.4GHz because its propagation characteristics are not suitable for capacity-based designs.

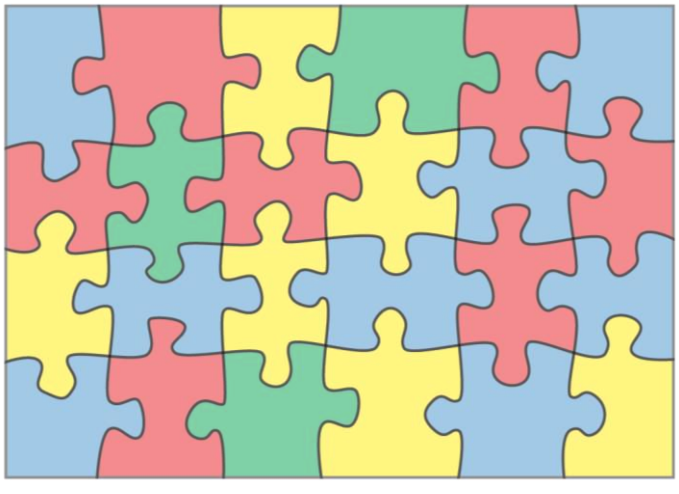
If an improper design is implemented, as represented in the Single Channel Architecture (SCA) below, as championed by two industry vendors, higher output power will increase the size of the collision domain, which will cause lower throughput due to more devices sharing the same channel.



This same CCC problem is experienced when client devices roam between APs using the same channel (channels are represented by various colors in the graphic below) while associated to either one of them. The client device essentially adjoins the two contention domains into one.



When using an optimal channel reuse design, APs can use higher output power, which will result in higher SNR, which will mean higher data rates (due to use of higher order modulation), and typically means lower retry rates. This is all good, except that with 2.4GHz, signal penetration prevents optimal channel reuse designs.



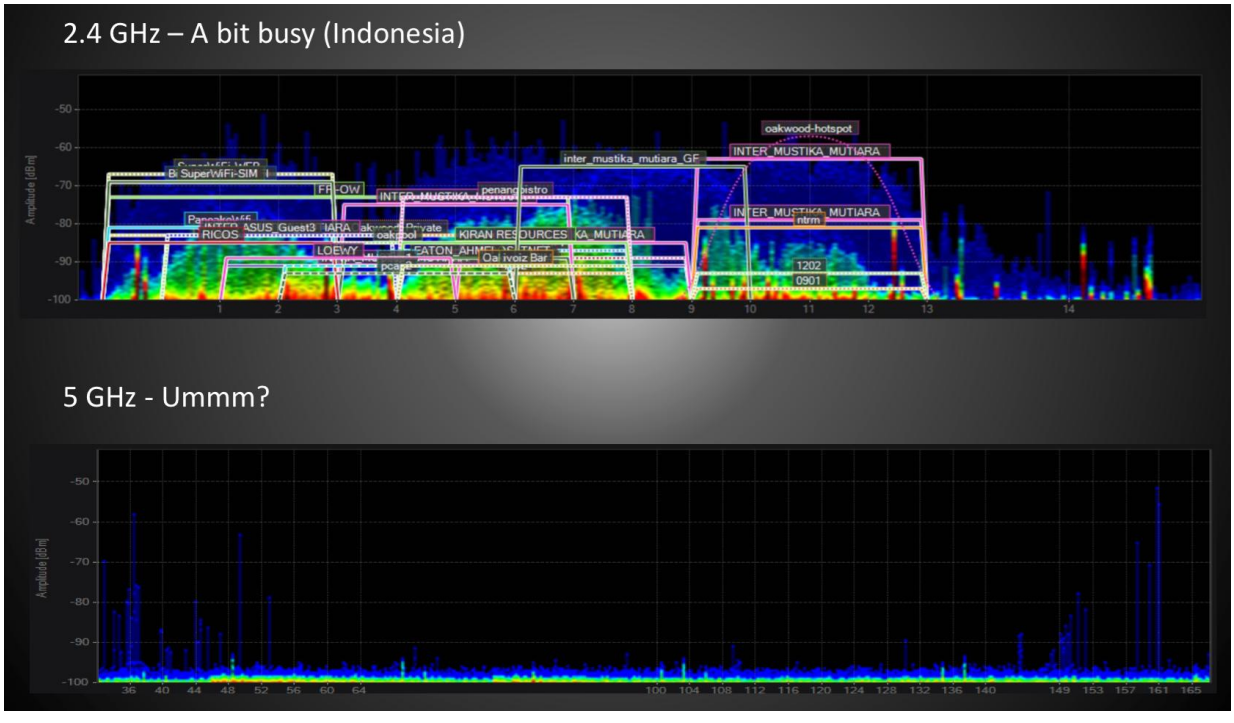
The next point that is often surfaced is when walls are made of substances such as poured concrete or cinder block, which partially acts as an RF absorber. The average cinder block wall or poured concrete wall drops 20-30 dB, depending on thickness (e.g. one or two cinder blocks thick).

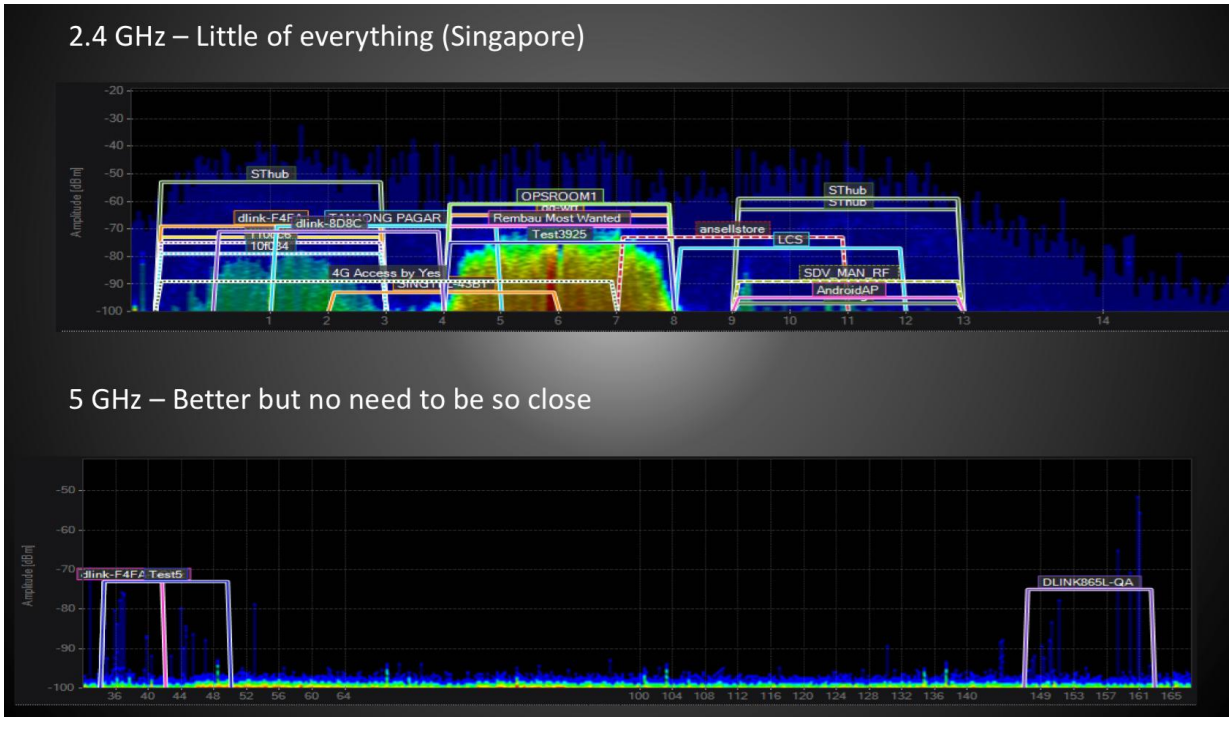
Interference in the 2.4GHz ISM Band

Because the 2.4GHz band was the first used by the 802.11 standard, and it has been in continuous use by 802.11-compliant systems since 1997, it's use is pervasive in both homes and businesses globally. Because of 2.4GHz's signal penetration characteristics, and most early network designs centering on coverage (rather than capacity), it's been the default band of choice since day 1.

The 2.4GHz ISM band is far over-used as compared to the 5GHz UNII bands. In a recent industry event, Stoney Tuckness gave an excellent presentation that addressed over-use of the 2.4GHz band

here. Specifically he gave three examples of how use of the 2.4GHz and 5GHz bands is disproportionate in various geographic regions.

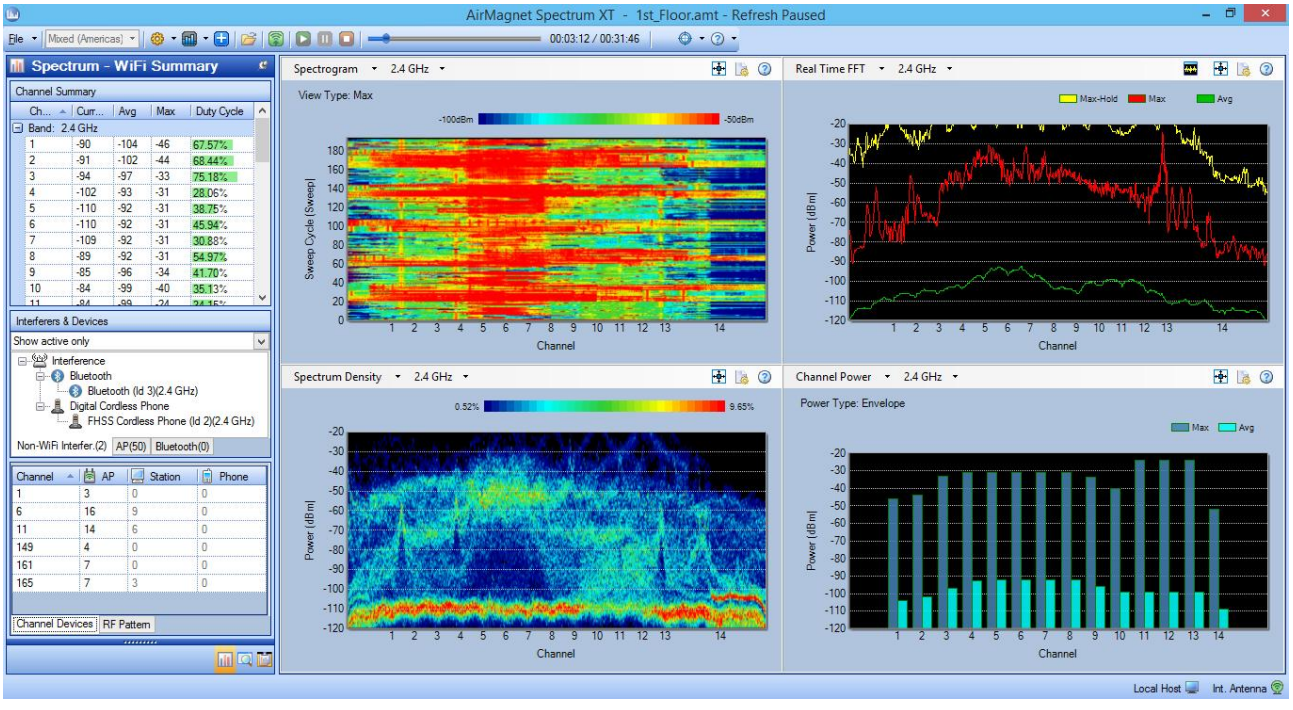




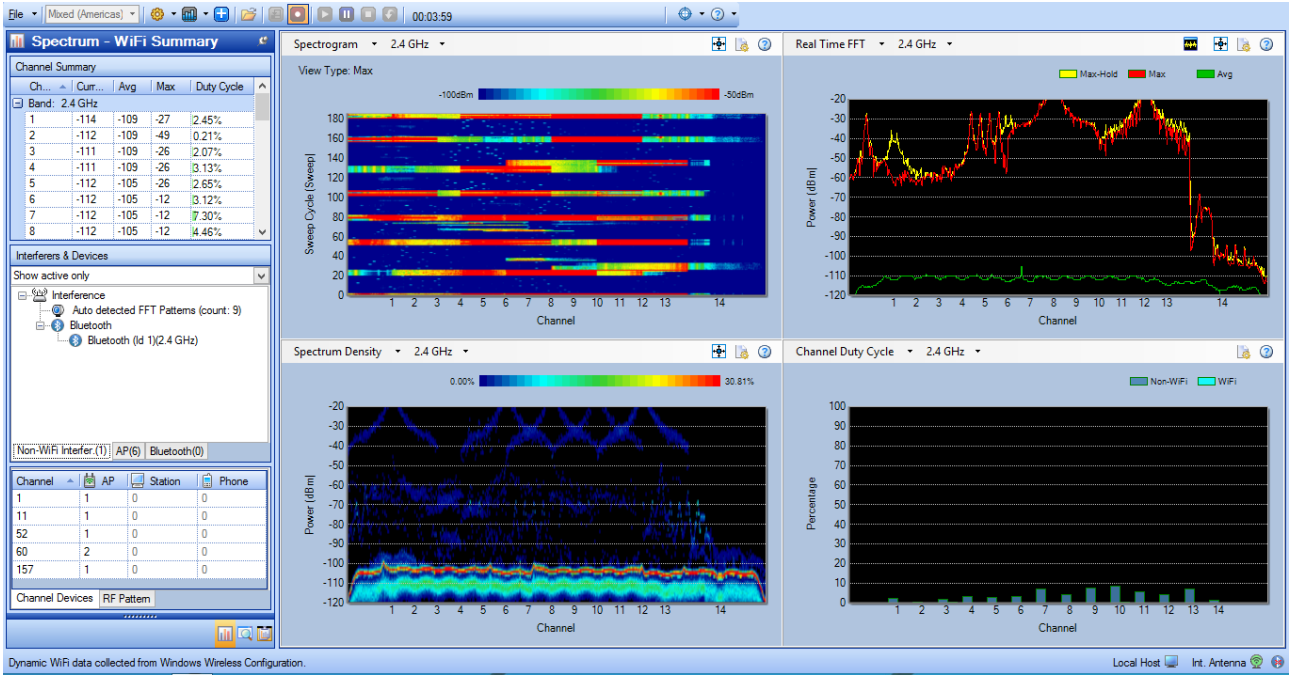
Credit: Stoney Tuckness

Unfortunately, other Wi-Fi systems are not the only interference concern in the 2.4GHz ISM band. There are a wide variety of standardized and proprietary technologies, other than Wi-Fi, that purposefully and successfully use the 2.4GHz band. Well-known technologies include Bluetooth, Zigbee, and Frequency Hopping (FHSS) WLANs. Common devices that use proprietary protocols within the 2.4GHz band include cordless phones & headsets, baby monitors, and video cameras. There is a wide variety of consumer, commercial, and industrial devices that emit interference into the 2.4GHz band. We're also now starting to see many Bluetooth Low Energy (BLE) enabled devices on the market, including iBeacons used for location services.

During a recent performance assessment for a customer, we found the reason why their 2.4GHz wasn't getting the expected throughput. They had five floors of a building that each looked similar to the screenshot below - almost no usable spectrum due to interferers operating on channels 1-14.



While trying to understand why my home Wi-Fi network's performance was suddenly so sporadic, I found the cause, as shown in the spectrum analyzer below: very high power Bluetooth. It's wrecking the entire 2.4GHz spectrum every 10-15 seconds, throughout my entire neighborhood.



As a corporate IT Director, Manager, or Administrator, an important question you should ask yourself is, "How much time do I want to spend troubleshooting something that I already know is permanently broken?" When your users complain about connectivity and/or performance issues, will it come as a surprise? Spending your valuable time fixing holes in worn-out tires is not how you win a race. The only real solution is to move your users to 5GHz bands, without delay.

IoT Will Make Things Much Worse

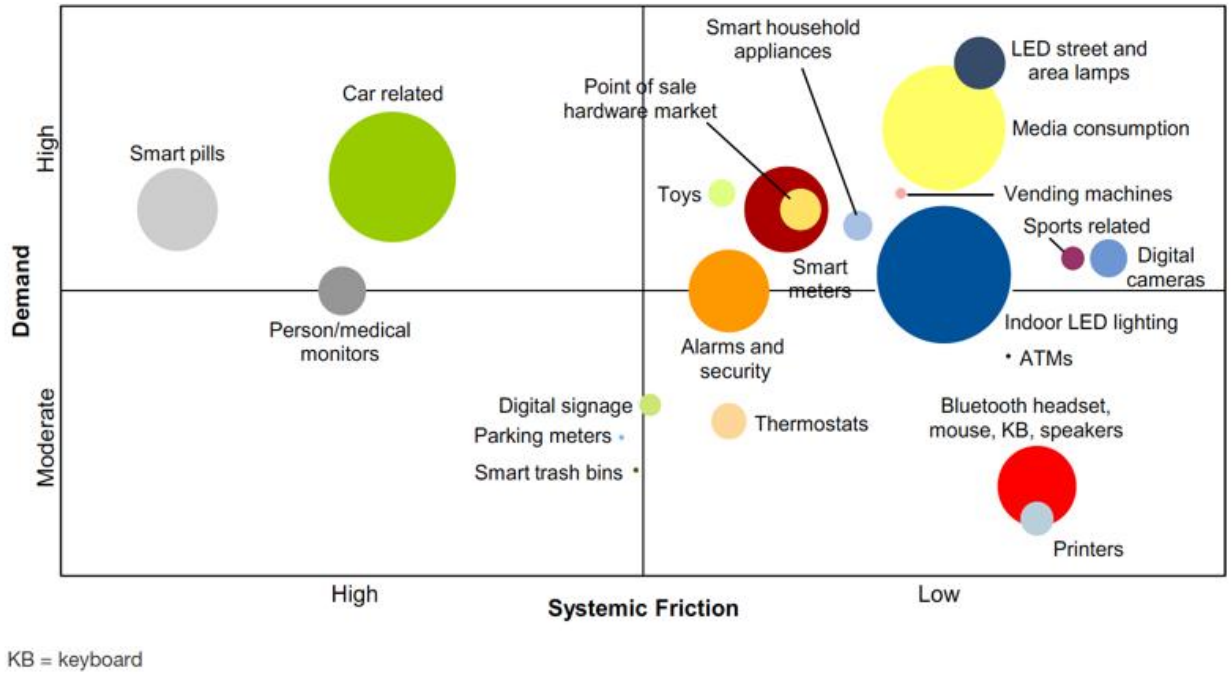
The Internet of Things (IoT) is an amazing phenomenon that will change the face of society. It will also utterly and completely wreck what's left of the 2.4GHz ISM band. There are endless numbers of devices that fall under the IoT category, with many using proprietary communication technologies and many using standardized technologies like Bluetooth.

Consider the Apple Watch - an amazing piece of engineering, worn on millions of wrists - as if iPhones, iPads, Apple TVs, and their ilk weren't throwing enough Bluetooth transmissions into the 2.4GHz spectrum already.

Credit: Apple, Inc.

The most important thing to understand about IoT is that it will never stop, or even slow down. It will continually accelerate, exacerbating the 2.4GHz problem, until such devices are forced to use 5GHz or other bands. Since devices such as the Apple Watch are tied to phones (e.g. iPhone), which have larger batteries that can support extended use of 5GHz frequencies at higher power as needed, manufacturers don't have to worry with integrating 5GHz Wi-Fi radios into such small devices. It seems that a good direction for manufacturers would be to use BLE in 5GHz bands.

Within homes, 2.4GHz devices penetrate walls quite well, usually meaning 1-2 APs to cover most homes. Both homes and businesses alike must move away from 2.4GHz Wi-Fi use, but businesses have harsher consequences for delaying the inevitable. Mobility drives productivity in many businesses today. With so many vertical and geographic markets being hyper-competitive, businesses can't afford to be slow, inefficient, or to have higher costs of doing business. If 2.4GHz won't get the job done, then they will be forced to move away from it.



Credit: Gartner (Nov 2013)

IoT device adoption will be widespread and will occur at different rates, as shown in the excellent graphic above from Gartner. Due to low power consumption, low manufacturing costs, widespread infrastructure support, and broad compatibility, IoT device manufacturers are still producing devices with 2.4GHz-only support. If such 2.4GHz-only devices use Wi-Fi radios for connectivity, they should be avoided, leaving 2.4GHz for non-WiFi devices and non-mission-critical devices only. Gartner and other analyst firms are predicting unthinkable numbers of IoT devices on the immediate horizon, as outlined in the image below.

Gartner: Top 10 Strategic Technology Trends For 2013

- **Internet of Things**: Internet of things is already here. Over 50% of Internet connections are things. In 2011, over 15 billion things on the Web, with 50 billion+ intermittent connections. By 2020, over 30 billion connected things, with over 200 billion with intermittent connections. Key technologies here include embedded sensors, image recognition and NFC. By 2015, in more than 70% of enterprises, a single exec will oversee all Internet connected things. Becomes the Internet of Everything.

It's difficult to stress enough that 2.4GHz's future is bleak. It's impossible to find clean 2.4GHz spectrum today, but within 5 years, using 2.4GHz for Wi-Fi connectivity will be unthinkable.

What about 5GHz?

5GHz has far more available spectrum (and thus available channels), with much less utilization in most environments and with lesser penetration characteristics than with 2.4GHz. This is an all-around win for network designers.

Note: *Some older client devices are not capable of using DFS channels (UNII-2 and UNII-2e) or the 5GHz ISM band (now being phased out), and when that is the case, network designers are left with only 8 channels (within UNII-1 and UNII-3) to work with. While the April 2014 FCC Report & Order rearranged and added spectrum (UNII-1 through UNII-4), there is currently no equipment available on the market capable of taking advantage of this new spectrum.*

It's a recommended practice to check all of your 5GHz capable client devices and APs to assure that they are capable of using UNII-2 and UNII-2e channels. Note that if your infrastructure is capable and configured to use these two 5GHz bands, and some of your client devices are not DFS capable, then these specific client devices will experience coverage gaps.

Note: *It's important to the industry at large, that everyone purchase only devices that support all 5GHz UNII bands. There is no added expense, network capacity is greatly enhanced, and it allows network designers to more quickly and successfully move networks away from 2.4GHz for mission-critical users/devices.*

We aren't downplaying having only eight 20MHz channels, but it's hard to disregard the scalability of having 25 channels (currently, including DFS channels) with an additional 12 channels forthcoming. This amount of channel space, and the lesser penetration characteristics, means a proper design can yield far less CCC.

Transition Options

Getting away from 2.4GHz Wi-Fi connectivity is more difficult than dieting, and we here at Divergent Dynamics understand the pain of both very well. Going cold turkey, without a proper network redesign, may cause withdrawal symptoms – starting with coverage. 5GHz signals, at the same output power, penetrate walls and open space far less than 2.4GHz. It's human nature to focus on the pain and to forget the ultimate goal. If we start out with a network design based around the propagation properties of 5GHz, then the pain of withdrawal symptoms is much less.

Some recommended steps in moving to a 5GHz-only network include the following:

Understand Your Client Devices

The first step in any Wi-Fi network design is to understand your client devices & users. If there are 2.4GHz-only devices being used on the WLAN, you should try to upgrade the client radios in as many of them as possible, as quickly as possible, with dual-band 802.11ac/n radios. In many environments, there are 2.4GHz-only client devices that cannot be removed or upgraded, and there are special considerations for those devices listed below.

Perform an RF Site Survey

When moving to a 5GHz-only or a transitional Wi-Fi network design (discussed below), then an RF Site Survey is warranted to prevent coverage gaps and to enhance performance through optimal AP placement.

System Configuration

When transitioning to a 5GHz-only Wi-Fi network, an important step is to configure the existing network for reasonably aggressive band steering toward 5GHz. Enterprise-class Wi-Fi networks usually have configurable band steering settings that allow an administrator to adjust how aggressively client devices are pushed toward 5GHz connections. This is not to say that these settings should always be set to "*Force*", but that's absolutely a reasonable choice unless there are client devices that will remain disconnected in the face of such AP configuration.

Turn off all SSIDs on 2.4GHz except one, which will be used to connect 2.4GHz-only devices while they are monitored and transitioned off the network. This SSID should abide by industry-standard high-density design guidelines (such as 12, 18, or 24 Mbps minimum Basic Rate with all rates below it disabled and all rates above it enabled as optional) unless there are 802.11b-only client devices on the network that cannot be removed at the present time. This "transitional" SSID should use PSK security with appropriate filtering/firewalling and should NOT be enabled on 5GHz.

5GHz radios should never have more than 4 SSIDs, and those SSIDs should likewise be configured within industry-standard high-density design guidelines. Disable band steering. All SSIDs that were originally enabled on both 2.4GHz and 5GHz should now only be enabled on 5GHz (up to a maximum of 4). Andrew Von Nagy's SSID Overhead Calculator is a valuable tool that we here at Divergent Dynamics use regularly.

As many 2.4GHz radios as possible should be disabled. Our best suggestion is to disable them everywhere that 2.4GHz coverage is not specifically needed. For the 2.4GHz radios that remain enabled, their output power should be minimized to the fullest extent possible while still providing the necessary coverage.

Monitor Your Spectrum

After creating a 2.4GHz-only transitional SSID, disabling other SSIDs on 2.4GHz, properly configuring the 5GHz radios, doing a site survey, and optimally deploying your APs, you will have the minimum number of Wi-Fi client devices on 2.4GHz and have high performance 5GHz Wi-Fi. From that point, help desk calls and complaints will decrease, and your network will run much better. Thereafter, it's important to monitor your 2.4GHz spectrum (e.g. channel utilization, types of interferers, etc.) so that you can understand how the remaining 2.4GHz Wi-Fi client devices (and any other mission-critical 2.4GHz non-WiFi devices) are likely to perform and at what rate you need to transition 2.4GHz-only Wi-Fi clients over to 5GHz.

A Different Kind of AP

This section will be less than popular among access point (AP) vendors, and the louder they shout against it in protest, the more they have to lose by its mention. Two-radio APs now need to house two dual-band, band-unlocked radios where the minimum combinations shown in the table below are possible. Of course there should be configuration logic that prevents two 5GHz radios from transmitting on the same band (e.g. UNII-1, UNII-2, UNII-3) simultaneously.

Radio 1 Mode	Radio 2 Mode
5GHz access, mesh, or both	2.4GHz access, mesh, or both
5GHz access, mesh, or both	5GHz access, mesh, or both
5GHz access, mesh, or both	Dual-band WIPS Scanner
Dual-band WIPS Scanner	Dual-band WIPS Scanner

For a vendor to say that it's "too hard to build" or "wouldn't work" is hogwash, because four vendors in the market have already released such products into the market, touting high performance. I would certainly rather have a dual 5GHz capable AP, even if some amount of intra-AP interference was experienced, because the 2.4GHz band is currently, and will forever more be, soaked in RF interference of all kinds.

2.4GHz Radios in Every AP

Having 2.4GHz radios in every dual-radio, enterprise-class AP is a waste of money. It's quite silly in fact, and yet most vendors' entire portfolio consists of exclusively this design.

For many years we have designed enterprise Wi-Fi networks around 5GHz radio propagation, with the understanding that 2.4GHz radios have more range, so coverage will easily be provided to the same area. There's so much coverage in 2.4GHz in fact that we end up with huge amounts of CCC, to which AP vendors respond with some of the following suggestions:

- Turn off some 2.4GHz radios
- Convert some radios to WIPS or spectrum sensors
- Turn down the power on the 2.4GHz radios

Most of those 2.4GHz radios are band-locked, and therefore they can only scan (for WIPS or spectrum) the 2.4GHz ISM band. Can intruders not place 5GHz rogue APs on your network? Is there no chance that the 5GHz bands can get congested? Each of those items listed above are silly excuses to ease the customer's pain and remorse of purchasing so many unusable radios.

Further, each AP has a set of associated costs, which includes the AP itself, cabling, installation/configuration, switch port, management licensing, and support/maintenance. After spending all of that money, you're going to turn off radios in most of the APs? Yes, you should. However, the feeling of loss in disabling all of those radios is often so great that administrators can more readily cope with leaving 2.4GHz turned on and constantly troubleshooting connectivity issues. Sometimes it's good to have some professional counseling skills when architecting a network around 5GHz only.

Conclusion

2.4GHz is Dead. Bury it and move on.