20 Myths of Wi-Fi Interference: Dispel Myths to Gain High-Performing and Reliable Wireless

The growing ubiquity of wireless devices combined with the advent of mobility applications requires businesses to be diligent in managing inference throughout their deployments. The many wireless technologies and commonplace electric devices already in use and newly emerging impede wireless performance.

RF interference can be a major inhibitor to wireless performance, creating security vulnerabilities and wireless network instability.

This paper exposes the top 20 most pervasive myths around wireless interference.

Myth #1: “The only interference problems are from other 802.11 networks.”

There are a tremendous number of 802.11 devices out there. It is true that the other 802.11 networks can cause interference with your network. This type of interference is known as co-channel and adjacent channel interference. But since other 802.11 devices follow the same protocol, they tend to work cooperatively—that is, two access points on the same channel will share the channel capacity.

In reality, the many other types of devices emitting in the unlicensed band dwarf the number of 802.11 devices. These devices include microwave ovens, cordless phones, Bluetooth devices, wireless video cameras, outdoor microwave links, wireless game controllers, Zigbee devices, fluorescent lights, WiMAX, and so on. Even bad electrical connections can cause broad RF spectrum emissions. These non-802.11 types of interference typically don’t work cooperatively with 802.11 devices, and can cause significant loss of throughput. In addition, they can cause secondary effects such as rate back-off, in which retransmissions caused by interference trick the 802.11 devices into thinking that they should use lower data rates than appropriate.

Summary: The unlicensed band is an experiment by the FCC in unregulated spectrum sharing. The experiment has been a great success so far, but there are significant challenges posed by RF interference that need to be given proper attention.

Myth #2: “My network seems to be working, so interference must not be a problem.”

The 802.11 protocol is designed to be somewhat resilient to interference. When an 802.11 device senses an interference burst occurring before it has started its own transmission, it will hold off transmission until the interference burst is finished. If the interference burst starts in the middle of an ongoing 802.11 transmission (and results in the packet not being received properly), the lack of an acknowledgement packet will cause the transmitter to resend the packet. In the end, the packets generally get through. The result of all these hold-offs and retransmissions, however, is that the throughput and capacity of your wireless network are significantly impacted.

For example, microwave ovens emit interference on a 50 percent duty cycle (as they cycle on and off with the 60-Hz AC power). This means that a microwave oven operating at the same frequency as one of your 802.11 access points can reduce the effective throughput and capacity of your access by 50 percent. So, if your access point was designed to achieve 24 Mbps, it may now be reduced to 12 Mbps in the vicinity of the microwave when it operates. If your only application on the WLAN is convenience data networking (for example, Web surfing), this loss of throughput may not be immediately obvious. But as you add capacity and latency-sensitive applications such as voice over Wi-Fi your network, controlling the impact of interference will become a critical issue.

Summary: Interference is out there. It's just a silent killer thus far.

Myth #3: "I did an RF sweep before deployment. So I found all the interference sources."

One of the most troubling issues about interference is that it is often intermittent in nature. The interference may occur only at certain times of day—for example, when someone is operating a device such as a cordless headset—or on certain days of the week. So, unless an initial sweep is done for an extended time, it's very easy to miss sources of interference. And even if the sweep was extensive (for example, making measurement in each area for 24 hours), things change over time. It's very easy for someone to introduce one of the many devices that operate in the unlicensed band into your environment. No amount of periodic sweeping can truly guarantee that you have an interference-free environment.

Summary: You can't sweep away the interference problem. Microwave ovens, cordless phones, Bluetooth devices, wireless video cameras, outdoor microwave links, wireless game controllers, Zigbee devices, fluorescent lights, WiMAX devices, and even bad electrical connections—all these things can cause broad RF spectrum emissions. These non-802.11 types of interference typically don't work cooperatively with 802.11 devices.

Myth #4: "My infrastructure equipment automatically detects interference."

Some of the newer, switch-based WLAN infrastructure products provide a level of RF interference management. With their 802.11 chipsets, these solutions detect the presence of non-802.11 signals. And in response to detection, they can change the 802.11 channel of the APs in the area of the interference. An issue with this approach is that it doesn't solve many of the problems that are out there. Some interfering devices—for example, Bluetooth devices, cordless phones, 802.11FH devices, jamming emissions) are broadband, so it's not possible to change channels away from them: they are everywhere in the band. And even for devices that operate on a static frequency, it can be challenging to manage channel assignments in a large, cell-based network. In the end, it's critical that you be able to analyze the source of interference—that is, identify what the device is and where it is located—in order to determine the best course of action to handle the interference. In many cases, this "best action" will be removing the device from the premises. In other cases, the response may be to move or shield the device from impacting the network.

Summary: Simple, automated-response-to-interference products are helpful, but they aren't a substitute for understanding of the underlying problem.

Myth #5: “I can overcome interference by having a high density of access points.”

The inexpensive nature of 802.11 access points makes it tempting to deploy them with very high density. For example, some networks are being deployed with an AP in every room. This type of deployment has the benefit of greatly increasing the capacity of the network by allowing “spatial reuse” of the spectrum. It seems intuitive that by having more APs spread around, it’s more likely that a client will be able to operate successfully even when interference is present.

Unfortunately, when you deploy a dense network of access points, it’s necessary to reduce the transmit signal power of each of the access points. If you don’t reduce the power, the access points generate interference to each other, a phenomenon known as co-channel interference. The reduction in the transmit power of the access point exactly offsets the potential benefit of interference immunity. So in the end, the interference immunity of a network with a dense deployment of access points is not significantly better than that of a less dense deployment.

Summary: It’s reasonable to over-design your network for capacity, but a high density of access points is no panacea for interference.

Myth #6: “I can analyze interference problems with my packet sniffer.”

802.11 packet sniffer products suffer from the same problem as WLAN infrastructure equipment: they can see only what the 802.11 chips tell them. They can tell you about secondary indicators of interference, such as increased retransmissions and lower data rates, but they can’t analyze interference problems, determine the cause of the interference, and help you find where the interfering device is located.

A second problem with the data from 802.11 chips is that power measurements are typically uncalibrated. This means that the data you receive from an 802.11 chip about the signal strength of an access point (or other device) can usually not be expressed reliably in absolute dBm units. As a result, it is very difficult to put meaning on the numbers that packet sniffer devices report.

Summary: You need the right tool for analyzing interference. In the end, it’s critical that you be able to analyze the source of interference in order to determine the best course of action to handle the interference. In many cases, the best action will be removing the device from the premises.

Myth #7: “I have a wireless policy that doesn’t allow interfering devices into the premises.”

Having a wireless policy is a good first step in tackling the interference problem. But no policy is effective without enforcement. One of the great attributes of unlicensed band wireless devices is that they are inexpensive and widely available. As a result, it’s very easy for employees to purchase these devices and bring them to work. In many cases, these employees are not even aware that a particular device may cause interference with your wireless network. And some devices like cordless headsets and microwave ovens may be a necessary part of your business, so they can’t be completely disallowed.

Summary: You have to expect that interfering devices will sneak onto your premises.

Myth #8: "There is no interference at 5 GHz."

It is generally true that fewer devices currently operating at 5 GHz are causing interference as compared to 2.4-GHz devices. But this will change over time. Just as everyone moved from 900 MHz to 2.4 GHz to avoid interference, the "band jumping" effect will catch up with 5 GHz. Some devices that already exist at 5 GHz include cordless phones, radar, perimeter sensors, and digital satellite.

Summary: You can run, but you can't hide.

Myth #9: "I'll hire a consultant to solve any interference problems I run into."

If you have been running a WLAN for some time, you will know that there are frequent instances where your network doesn't operate perfectly. Without having your own visibility into interference, you are left to guess about whether or not interference is the problem. Lack of visibility is an issue for IT personnel, especially when the CEO is asking why he was having trouble yesterday connecting in the conference room. And beyond the issues of control, it's expensive and time-consuming to bring in a consultant to debug these kinds of problems. A single visit and trip report can cost on the order of US $5000 to $10,000.

Summary: You can't afford to rely on a third party to debug your network.

Myth #10: "I give up. RF is impossible to understand."

Don't despair. Tools are now available that make RF easier to understand, even for those who consider themselves wired network specialists, not wireless experts. For example, Cisco® Spectrum Expert Wi-Fi classifies the sources of your interference, so you don't need to read the "wiggly lines." And after we've identified the interference, we help you find and eliminate it.

Summary: The cavalry is here!

Myth #11: "Wi-Fi interference doesn't happen very often."

There is a growing body of evidence that points to the fact that Wi-Fi interference is an extremely common and troublesome issue. Here are a few recent examples:

- The technical support engineers at a major Wi-Fi infrastructure vendor reported to Cisco that in a recent service call to a major customer they found almost 20 sources of interference, contributing to over 50 percent of the problems on the customer's Wi-Fi network.
- The manager of a large group of outsourced wireless service representatives stated to Cisco that "one out of every three Wi-Fi problems our service technicians get called out for is related to interference."
- In a recent survey of 300 of their customers, a major Wi-Fi tools provider reported that "troubleshooting interference won 'top honors' as the biggest challenge in managing a Wi-Fi network."
- Jupiter Research reports 67 percent of all residential Wi-Fi problems are linked to interfering devices, such as cordless phones, baby monitors, and microwave ovens.

Summary: There's no point burying your head in the sand: Wi-Fi interference happens.

Myth #12: "I should look for interference only after ruling out other problem sources."

In any networking system, it's critical that the physical layer is solid. When the physical layer is not operating properly, the higher protocol layers tend to operate in inefficient and sometimes confusing ways. For this reason, it always makes sense to verify your physical layer first before going on a wild-goose chase looking higher layer problems.

As an analogy, when you hook your computer up to an Ethernet cable and the network does not appear to be working, your first diagnostic step is to look at the lights on the side of your Ethernet adapter. If the lights are not on, there is no point looking for a subtle network configuration problem: you simply don't have physical layer connectivity.

The potential for physical layer problems with Wi-Fi is much worse than with Ethernet. With an Ethernet cable, you worry about the physical-layer connectivity issue only the first time you plug in the cable. If the connection was working that first day, it's reasonable to expect it will keep working day after day. But in the RF world, the quality of the physical connection can change hour by hour, as people introduce other devices or obstructions into the environment.

Summary: Avoid wasting your time. Fix your RF physical layer first.

Myth #13: "There's nothing I can do about interference if I find it."

The most common cure for interference is simply to replace or remove the offending interference device. For instance, you might replace an old leaky microwave oven or a 2.4-GHz cordless headset used by the receptionist with a different model that operates in a non-Wi-Fi frequency band. Many times interference is caused unwittingly by well-intentioned employees. One Wi-Fi administrator found an employee who sat with his back to his door, and had brought in a wireless camera so he could see behind him. Unfortunately, it operated at 2.4GHz. In this case, a policy was created to ban these types of devices on the campus.

Another solution is to work around the interference device by moving the affected access point, or changing its operating channel to a frequency that is not impacted by the interfering device. This is simple once you understand the location and frequency parameters of the interfering device. Note that because some devices frequency-hop (for example, Bluetooth devices) it's not always possible to change channels and eliminate the interference.

A final cure is to move or shield the offending device. For example, in a hospital, a piece of equipment that causes RF interference might be isolated to a particular room where Wi-Fi network access is not critical. If that's not possible, adding electromagnetic interference (EMI) shielding can limit propagation of the interference to a small area. You can implement shielding with grounded mesh or foils in the walls (essentially Faraday cages) or with insulating foams or paints.

Summary: There's always a cure for interference, but you need to know what's ailing you.

Myth #14: “There are just a few easy-to-find devices that can interfere with my Wi-Fi.”

With the huge proliferation of wireless devices in the unlicensed band, it is no longer obvious what might be a source of interference—wireless links are now embedded in watches, shoes, MP3 players, and many other tiny consumer devices.

In some cases, previously benign devices have been updated with RF technology. Motion detectors, which appear in many offices for lighting control, are a good example. A new breed of hybrid motion detectors uses a combination of passive infrared sensor (PIR) and 2.4-GHz radar to detect motion. These devices, which look identical to their benign predecessors, generate significant interference that can disrupt your Wi-Fi network.

Unintentional emitters are also hard to find. A defective ballast on a fluorescent light fixture can generate broadband RF interference that can impact Wi-Fi. This is impossible to identify by simply looking at the device. “Hidden devices” are becoming more common as well. We have seen numerous instances where a security group has hidden wireless cameras—unbeknownst to the networking group—not realizing that they are jamming the Wi-Fi network.

Summary: You need the right tool to find interference fast, and it’s not a magnifying glass.

Myth #15: “When interference occurs, the impact on data is typically minor.”

The impact of a single interferer on data throughput (or data capacity) of your Wi-Fi network can be astounding.

There are three major factors that determine the impact of an interference device:

- **Output power.** The greater the output power, the larger the physical “zone of interference” the device creates.
- **Signal behavior with respect to time.** Analog devices, such as some video cameras and older cordless phones, have a constant always-on signal. Digital devices, such as digital cordless phones, tend to “burst” on and off. Different devices have varying durations of on-time and off-time. In general, the greater the percentage of time that the signal is “on” and the more frequently it bursts, the greater the impact it will have on throughput.
- **Signal behavior with respect to frequency.** Some devices operate on a single frequency, and impact specific Wi-Fi channels. Other devices hop from frequency to frequency and impact every channel but to a lesser degree. Some devices, such as microwave ovens and jammers, sweep quickly across the frequency spectrum, causing brief but serious interruptions on many frequencies.

A recent study undertaken by Farpoint Research measured the impact of various interference devices on the data throughput of Wi-Fi. At 25 feet from the AP or client, a microwave oven was found to degrade data throughput by 64 percent, a frequency-hopping phone degraded throughput by 19 percent, and an analog phone and video camera both degraded throughput by 100 percent (in other words, no ability to connect).

Summary: Interference can really take the zip out of your Wi-Fi data throughput.

Myth #16 “Voice data rates are low, so the impact of interference on voice over Wi-Fi should be minimal.”

With modern voice coding, the data rate of an individual voice call is on the order of 8 Kbps. Compared to the maximum throughput of a Wi-Fi network, this seems like a trivial amount, and it therefore seems reasonable to expect that a Wi-Fi access point can handle many concurrent voice-over-IP (VoIP) calls.

Unfortunately, many factors reduce the number of calls that an access point can handle. First, there is significant VoIP protocol-level overhead, which increases the typical stream to 100 Kbps. Then there is additional protocol overhead imposed by Wi-Fi. Second, voice traffic is very sensitive to jitter and delay, requiring extra capacity in the network to minimize congestion. The typical number of voice calls that vendors advertise they can handle with a Wi-Fi access point is only 15. When interference is introduced, the number of calls that can be handled drops from there.

In addition, small amounts of interference seriously impact voice-over-Wi-Fi voice quality. A recent study undertaken by Farpoint Research measured the impact of various interference devices on the mean opinion score (MOS) for voice-over-Wi-Fi calls, and found the voice quality falling to unacceptable levels when a microwave, cordless phone, video camera, or co-channel Wi-Fi device was within 25 feet of the access point or phone. And perhaps more importantly, interference creates coverage holes where phone calls will be dropped. An in-house study showed that the effective range of a VoWi-Fi phone drops by 50 percent with an interference device (cordless phone or video camera) at a distance of 75 feet from the access point. This 50 percent reduction in the range of your phones would likely result in coverage holes over 75 percent of your floor space.

Summary: Can you hear me now? Voice over Wi-Fi and interference don’t mix.

Myth #17: “Interference is a performance problem, but not a security risk.”

If an Internet worm got through your corporate firewall and was using up 50 percent of your corporate network bandwidth as it spread from machine to machine, would you consider that a security or a performance concern? The point here is that anything that impacts mission-critical corporate IT systems is a security concern. As your corporate Wi-Fi network becomes more and more mission-critical, any possible interference device—whether the interference is malicious, as in the case of a jammer, or accidental—must be viewed as a potential security issue. In addition to RF denial of service, there are several other risks related to non-Wi-Fi RF devices, including:

- **Multiprotocol devices.** Wi-Fi networks are typically locked down with secure access controls, but devices that run on non-Wi-Fi networks, such as Bluetooth devices, are not. A notebook computer with Wi-Fi and Bluetooth connectivity may act as bridge, allowing an intruding device onto the corporate LAN or WLAN. Preventing accidental bridging between insecure networks and the corporate networks requires: 1) client-based tools that control configuration of wireless network interfaces, and 2) RF monitoring that watches for suspicious non-Wi-Fi activity indicating possible bridging.
- **Non-Wi-Fi rogues.** Most enterprises implement some form of Wi-Fi rogue access point detection to find unauthorized (and frequently unsecured) access points on the corporate network. But there are non-Wi-Fi devices (such as Bluetooth access points) that can open up a similar security hole. Like Wi-Fi rogues, these devices must be detected and eliminated.

- **Leakage of sensitive data.** Certain non-Wi-Fi devices such as cameras and cordless phones can be used to carry sensitive data out of a restricted area, bypassing corporate security policies. When this is a concern, a zone of restricted wireless operation should be established, and that zone should be enforced through monitoring of the spectrum for unauthorized devices.

Summary: RF security doesn't stop with Wi-Fi. Do you know who is using your spectrum?

Myth #18: "802.11n and antenna systems will work around any interference issues."

Systems that use multiple antennas or smart antennas are able to increase immunity to interference by boosting the desired signal seen at a receiver. When the desired signal is stronger, the ratio of that signal to interference (referred to as signal-to-noise ratio or SNR) is also improved. Effectively, this reduces the zone of interference associated with a particular interference device to a smaller area. But the gain achieved by a smart antenna system is typically only on the order of 10 dB of enhanced signal power. This means that the range of interference might be shrunk by a factor of 2 over a traditional antenna system, but even then the interference problem is far from solved. For example, if a device would have previously caused problems at a distance of 80 feet from the receiver, it will still cause problems up to 40 feet from the receiver. Thus you would have 5000 square feet of floor space where the interference is still a problem!

Summary: Antennas are a pain reliever, but far from a cure.

Myth #19: "My site survey tool can be used to find interference problems."

A standard Wi-Fi site survey tool is designed to measure Wi-Fi coverage. It uses a Wi-Fi chipset to measure the signal strength of access points as you move around the building. Unfortunately, Wi-Fi chips are designed to see Wi-Fi signals only, and can't tell you much about interference from other non-Wi-Fi devices. (This is the same limitation experienced when using a Wi-Fi packet analysis tool). A Wi-Fi site survey tool might indicate a general area where a non-Wi-Fi signal was observed. But the tool can't help you determine the nature of the interference, the type of device causing it, or where the device is located. So you are left without a solution. You really need an RF-level tool to diagnose interference problems. The good news is that a few of the next-generation Wi-Fi site survey tools are being more closely integrated with RF-level tools in order to implement a complete solution.

Summary: Site survey tools measure coverage, but don't solve your RF needs.

Myth #20: "RF analysis tools are too bulky and too expensive."

Many RF analysis tools (such as large and expensive spectrum analyzers) are not enterprise friendly.

But Cisco's RF spectrum analysis tools are designed to fit both your desired form factor (small cards that plug into your laptop) and your IT budget. And to make things even better, Cisco's spectrum intelligence solutions makes being a RF expert unnecessary.

Summary: Learn more about Cisco's Spectrum Intelligence solutions at: http://www.cisco.com/en/US/products/ps9393/index.html

Conclusion

There are many myths about the obstacles to high-performing and reliable WLAN services. A misunderstanding of the nature Wi-Fi interference underlies many of these myths, as does the belief that better visibility into RF spectrum is a difficult and costly proposition. In fact, the idea that RF spectrum visibility is prohibitively difficult and expensive to achieve may be the most malicious myth of all.

Cisco Unified Wireless Network supports real-time spectrum intelligence for Wi-Fi networks. industry-leading solution detects, classifies, and locates devices causing RF interference in the unlicensed 2.4-GHz and 5-GHz bands.

For information on ways to manage wireless interference, visit the Cisco RF solution page at: http://www.cisco.com/en/US/netsol/ns736/networking_solutions_package.html

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-449271-00 12/07