White Paper

Demystifying Interference Problems in the RF Spectrum

As network managers strive to understand interference problems in the RF spectrum, they are confronted with rumors regarding the impact of interference on the wireless network. This white paper helps demystify the top 20 rumors network managers discover as they explore interference issues.

Table of contents

FLUKE networks

Demystifying Interference Problems in the RF Spectrum

As a network manager, you are concerned about your WLAN's performance. You want to optimize its performance so end user complaints regarding speed and/or connectivity are minimized. While designing and deploying your wireless network, you hear numerous "rumors" or "myths" regarding interference issues associated with wireless networks. This white paper demystifies the top 20 interference rumors associated with wireless networks.

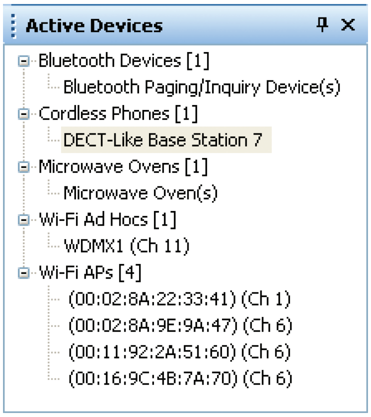
#1 – "The only interference problems are from other 802.11 networks."

There are a tremendous number of 802.11 devices installed worldwide and other 802.11 networks can cause interference with your wireless network. This type of interference is known as co-channel and adjacent channel interference. Since all 802.11 devices follow the same protocol, they tend to work cooperatively – ie. two Access Points (APs) on the same channel will share the capacity of the channel.

There are many types of devices operating in the unlicensed ISM (industrial, scientific and medical) band in which 802.11 networks operates. These devices include microwave ovens, cordless phones, Bluetooth devices, wireless video cameras, outdoor microwave links, wireless game controllers, Zigbee, fluorescent lights, WiMax, and more. Even bad electrical connections can cause broad RF spectrum emissions (interference).

These non-802.11 sources of interference typically do not work cooperatively with 802.11 devices, and can cause significant throughput loss in an 802.11 network. In addition, they can cause secondary effects such as rate back-off – where retransmissions caused by interference trick the 802.11 devices into thinking they should use lower than anticipated data rates.

Summary: The unlicensed ISM band is an experiment by the FCC in un-regulated spectrum sharing. We are still waiting to see how it works out. The best way for an 802.11 network to function optimally is to remove or minimize all sources of interference impacting the network.



Active Devices

- Bluetooth Devices [1]
  - Bluetooth Paging/Inquiry Device(s)
- Cordless Phones [1]
  - DECT-Like Base Station 7
- Microwave Ovens [1]
  - Microwave Oven(s)
- Wi-Fi Ad Hocs [1]
  - WDMX1 (Ch 11)
- Wi-Fi APs [4]
  - (00:02:8A:22:33:41) (Ch 1)
  - (00:02:8A:9E:9A:47) (Ch 6)
  - (00:11:92:2A:51:60) (Ch 6)
  - (00:16:9C:4B:7A:70) (Ch 6)

Figure 1: AnalyzeAir Wi-Fi Spectrum Analyzer lists all the devices found in the 802.11 spectrum – both network devices and interfering devices.

#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), then 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 is that the throughput of the wireless network is significantly impacted. For example, microwave ovens emit interference on a 50% duty cycle (as they cycle on and off with the 60 Hertz AC power). This means a microwave oven operating at the same frequency as one of your 802.11 access points (APs) can reduce the effective throughput of your network by 50%. So, if your network 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 (web surfing, for example), this loss of throughput may not be immediately obvious. But, as you add capacity and latency sensitive applications such as voice over wireless lan (VoWLAN) to your network, controlling the impact of interference will become a critical issue.

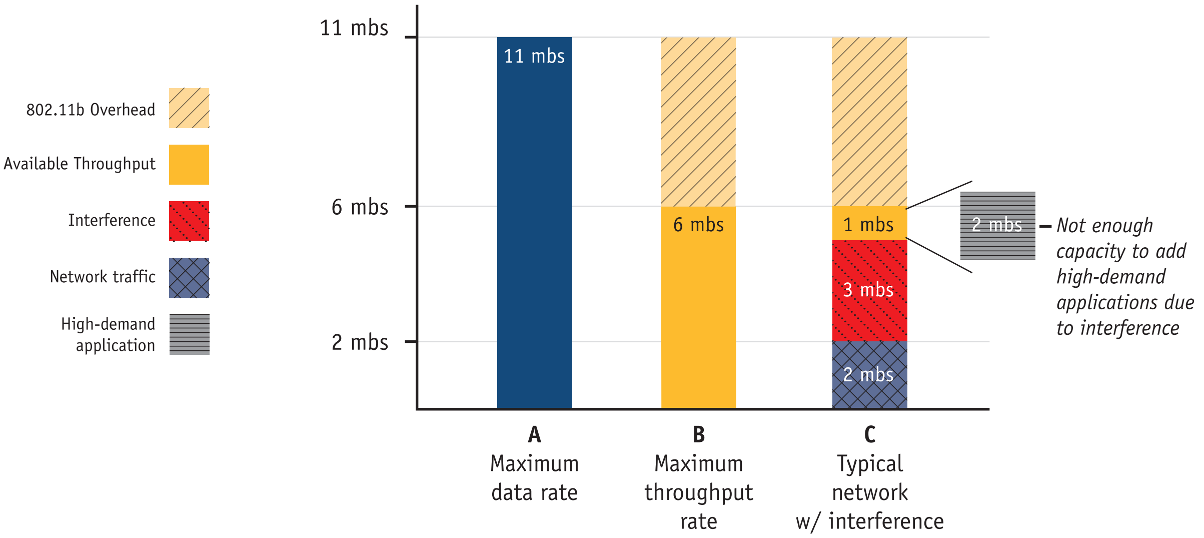


Figure 2: An 802.11b wireless network is designed to have a maximum data rate of 11 Mbs (Graph **A***) and can typically sustain a data rate resulting in throughput speeds of up to ~ 60% of the maximum data rate or ~6 Mbs. Once you approach data rates exceeding 60% of the maximum data rate, your network's performance will start to drastically decline to the point of being unusable. Graph* **B** *shows an 802.11b wireless network's 60% sustainable throughput. Graph* **C** *shows an 802.11b wireless network with typical network traffic plus interference issues. Using Graph* **C** *as an example, there is not enough available capacity to add high-demand or mission critical applications such as VoWLAN to the network without removing its interference problems.*

Summary: Interference is out there … perhaps the capacity of your WLAN is masking the problem. Most likely, interference will cause problems when you add high-demand applications like VoWLAN to you wireless network.

#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 they are often intermittent in nature. The interference may occur only at certain times of day (when someone is operating the device – for example, a cordless headset or microwave oven), or on certain days of the week. Unless an initial RF sweep is done for an extended time, it is very easy to miss intermittent sources of interference.

Even if the RF sweep was extensive (for example, making measurements in each area for 24 hours), things change over time. It is very easy for someone to introduce an interfering device, such as a Blueberry headset, into your wireless environment. No amount of periodic sweeping can truly guarantee that you have an interference-free environment at all times.

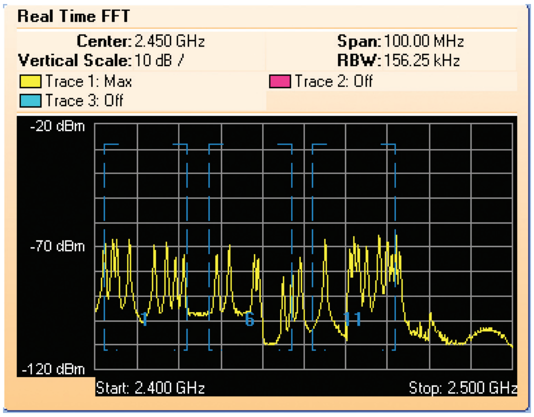
Summary: You cannot sweep away interference problems. You need a quick, simple method to periodically check for interference problems impacting your wireless network.

Figure 3: Microwave ovens are used throughout the day. If the microwave is an older model, chances are it will interfere with your 802.11 wireless network since it emits RF interference. If an RF sweep is not performed for an extended time period, the microwave's interference may be missed.

#4 – "My infrastructure equipment automatically deals with interference."

Many of the newer switch-based WLAN infrastructure products claim to manage RF interference problems. In reality, they are somewhat limited by the capabilities of the 802.11 chipsets they are based on, and the 802.11 protocol itself.

With their 802.11 chipsets, the infrastructure providers can detect the presence of non-802.11 signals – which is interference. In response to this interference, they can try to change the 802.11 channel of the APs in the areas impacted by the interference.



Real Time FFT

Center: 2.450 GHz Span: 100.00 MHz
Vertical Scale: 10 dB / RBW: 156.25 kHz
🟨 Trace 1: Max 🟥 Trace 2: Off
🟦 Trace 3: Off

Figure 4: AnalyzeAir's Real Time FFT shows the frequency hopping characteristics of a Bluetooth® phone. The spikes in the waveform represent the power of the Bluetooth phone at different frequencies as it hops from one frequency to the next.

The problem with this approach is that it does not solve the real problem. Some interfering devices (for example, Bluetooth®, cordless phones, 802.11FH) are frequency hopped as shown in Figure 4. It is not possible to change the channel away from these types of devices – they are everywhere in the band. Even for devices that operate on a static frequency, it can be quite a challenge to manage channel assignments in a large cell-based network.

To truly solve the problem, it is critical that you can ***analyze*** the source of interference (i.e., identify the device and where it is physically 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 so it does not impact the network.

Summary: Automated response to interference is the desired state, but it is not a reality today.

#5 – "I can overcome interference by having a high density of APs."

The inexpensive nature of 802.11 access points makes it tempting to deploy them with very high density. For example, some networks are 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 is more likely that a client will be able to operate successfully even when interference is present.

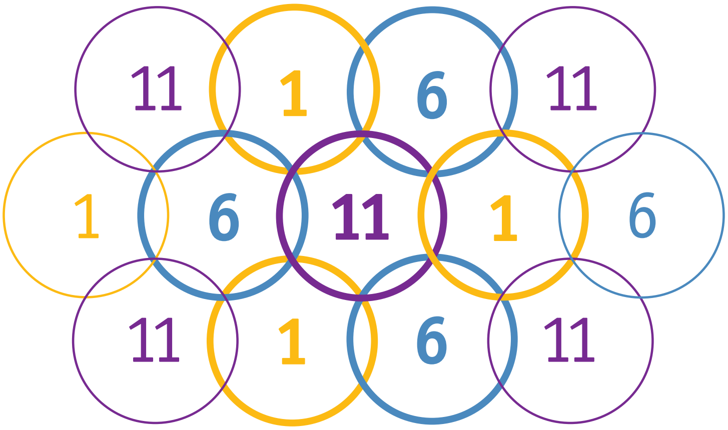


Figure 5: When designing a wireless network one must be careful to limit co-channel interference. This figure represents how APs should be placed to minimize co-channel interference.

Unfortunately, when deploying a dense network of APs, it is necessary to reduce the transmit signal power of each of the access points. If you do not reduce the power, the access points generate interference with each other – this is known as co-channel interference.

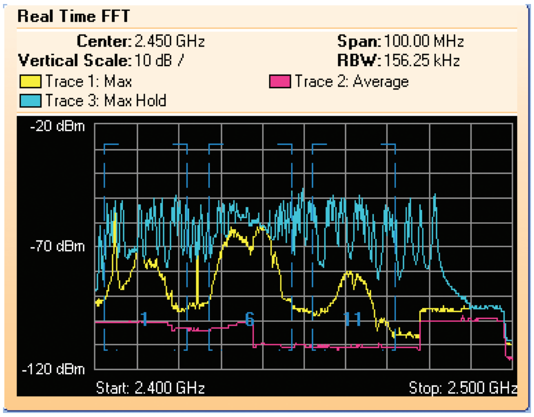
The reduction in the transmit power of the AP exactly offsets the potential benefit of interference immunity. So in reality, the interference immunity of a network with a dense deployment of APs is not significantly better than that of a less dense deployment.

Summary: It is reasonable to over-design your network for capacity, but it is not the solution for solving interference issues.

#6 – "I can analyze interference problems with my packet sniffer."

802.11 packet sniffers suffer from the same problem as WLAN infrastructure equipment. They can only see what the 802.11 chips tell them and can tell you about secondary indicators of interference such as increased retransmissions and lower data rates. But, they cannot analyze interference problems, determine the cause of the interference, or help you find the physical location of an interfering device.

A second difficulty with the data from 802.11 chips is that their power measurements are not calibrated. Therefore, the data you receive from an 802.11 chip regarding the signal strength of an AP (or other device) cannot be expressed in absolute dBm units. This makes it very difficult to put meaning on the numbers they report. To accurately express signal strength in absolution dBm units, you need a tool such as a spectrum analyzer, which is a calibrated measuring device.



Real Time FFT

Center: 2.450 GHz **Span:** 100.00 MHz

Vertical Scale: 10 dB / **RBW:** 156.25 kHz

Figure 6: AnalyzeAir's Real-Time FFT displays the power generated in the RF spectrum with absolute dBm units.

Summary: You need the right tool for analyzing interference – a simple-to-use spectrum analyzer.

#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 an interference problem. However, no policy is effective without enforcement. So, how would do you enforce a "no wireless policy"?

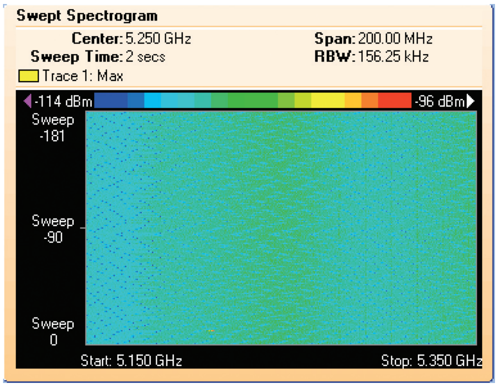
One of the great attributes of wireless devices is that they are inexpensive and widely available. As a result, it is very easy for employees to purchase these devices (Blackberry devices, cordless phones) and bring them to work. In many cases, employees do not mean to cause problems and are not even aware a particular device may cause interference with your wireless network.

Be aware that some devices like cordless headsets and microwave ovens may be a necessary part of your business, so they cannot be completely disallowed.

Figure 7: Examples of wireless devices that are not allowed in a Wireless Free Zone. People may not be aware they are violating the wireless free policy when bringing these items into the location.

Summary: You have to expect that interfering devices will sneak onto your premises. You need a method for finding these unauthorized devices and dealing with their interference by removal or shielding.

#8 – "There is no interference at 5 GHz."



Swept Spectrogram

Center: 5.250 GHz
Span: 200.00 MHz
Sweep Time: 2 secs
RBW: 156.25 kHz
Trace 1: Max

Figure 8, AnalyzeAir's Swept Spectrogram shows minimal interference at 5 GHz since the colors shown are only blues and greens which represent low emmisions.

It is true that there are fewer interfering devices currently present on the 5 GHz band as compared to the 2.4 GHz band. However, this will change over time. Just as everyone moved from 900 MHz to 2.4 GHz to avoid interference, this "band jumping" effect will catch up to the 5 GHz band.

Some devices that already exist at 5 GHz include cordless phones, radar, perimeter sensors, and digital satellites.

Summary: Interference may not be a problem at 5 GHz right now, but it will be in the future.

#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 know there are frequent instances where your network does not operate perfectly. Without having visibility into interference, you are left conjecturing on 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.

In addition, beyond the control issue, it is expensive and time consuming to bring in a consultant to solve these kinds of issues. A single visit and trip report can cost on the order of $5,000 - 10,000.

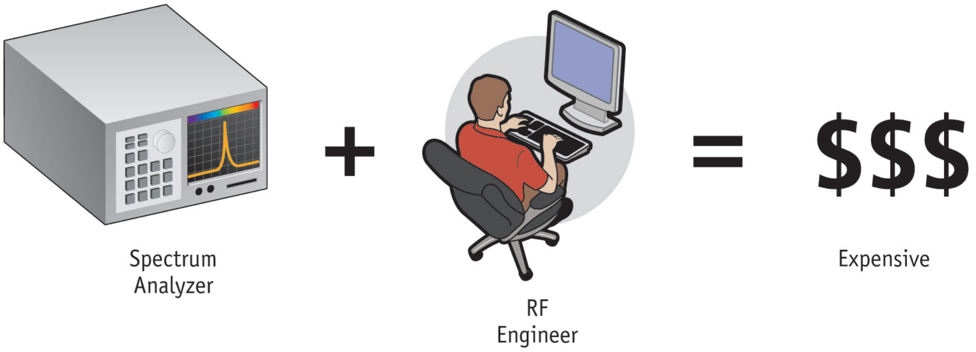


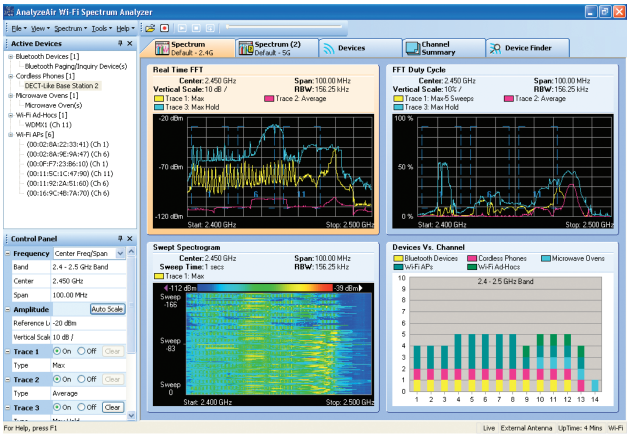
Figure 9: Why pay for an expensive RF engineer when you can own the tools which quickly solve your interference problems? You need to be able to address your interference issues quickly, on your own timeline and not be limited by an RF engineer's availability.

Summary: You cannot afford to rely on a third party to solve your network's interference problems. You need to be able to quickly and easily find and locate interference on your network.

#10 – "I give up. RF analysis is too hard for me to understand."

Do not despair. Tools are now available to make RF analysis easier to understand, even for those who consider themselves wired network specialists – not wireless experts. For example, Fluke Networks' AnalyzeAir™ Wi-Fi Spectrum Analyzer detects, identifies, and locates the physical sources of interference in your 802.11 WLANs. For more information, go to **www.flukenetworks.com/analyzeair**.

Summary: The correct tool, such as AnalyzeAir Wi-Fi Spectrum Analyzer, will greatly simplify your task of detecting, identifying, and locating RF interference in 802.11 WLANs.



AnalyzeAir Wi-Fi Spectrum Analyzer

Active Devices
- Bluetooth Devices [1]
  - Bluetooth Paging/Inquiry Device(s)
- Cordless Phones [1]
  - DECT-Like Base Station 2
- Microwave Ovens [1]
  - Microwave Oven(s)
- Wi-Fi Ad-Hocs [1]
  - WDMX1 (Ch 11)
- Wi-Fi APs [6]
  - (00:02:8A:22:33:41) (Ch 1)
  - (00:02:8A:9E:9A:47) (Ch 6)
  - (00:0F:F7:23:B6:10) (Ch 1)
  - (00:11:5C:1C:47:90) (Ch 11)
  - (00:11:92:2A:51:60) (Ch 6)
  - (00:16:9C:4B:7A:70) (Ch 6)

Control Panel

Frequency	Center Freq/Span
Band	2.4 - 2.5 GHz Band
Center	2.450 GHz
Span	100.00 MHz
Amplitude	Auto Scale
Reference L	-20 dBm
Vertical Scal	10 dB /
Trace 1	● On ○ Off Clear
Type	Max
Trace 2	● On ○ Off Clear
Type	Average
Trace 3	● On ○ Off Clear

Real Time FFT — Center: 2.450 GHz Span: 100.00 MHz Vertical Scale: 10 dB / RBW: 156.25 kHz

FFT Duty Cycle — Center: 2.450 GHz Span: 100.00 MHz Vertical Scale: 10% / RBW: 156.25 kHz

Swept Spectrogram — Center: 2.450 GHz Span: 100.00 MHz Sweep Time: 1 secs RBW: 156.25 kHz

Figure 10: AnalyzeAir makes finding interference in 802.11 WLANs simpler by listing all active devices in the spectrum, both network devices and interfering devices. AnalyzeAir software wraps the tools RF experts use in an easy-to-use interface putting the power of automated RF analysis in your hands.

#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:

- Technical support engineers at a major Wi-Fi infrastructure vendor reported that in a recent service call to a major customer, they found almost 20 sources of interference, contributing to more than 50% of the problems on the customer's Wi-Fi network.
- The manager of a large group of outsourced wireless service representatives stated 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.
- Yankee Group, April 2007, reports that "interference is the root of most wireless outages. Whether the source is natural (e.g., trees, buildings) or unnatural (e.g., microwaves, cordless phones), these kinds of outages present a serious problem for a WLAN environment and can cost an enterprise thousands of dollars in downtime."

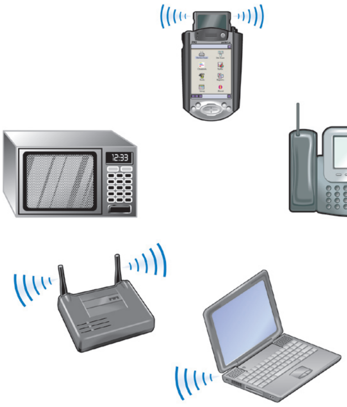


Figure 11: Examples of common items that cause RF interference. You will be amazed at all the items that cause interference.

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

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

In any networking system, it is critical that the physical layer is solid. When the physical layer is not operating properly, the higher protocol layers tend to operate inefficiently and in confusing manners. Whether you are running a wired or wireless network, it always makes sense to verify your physical layer first before going on a wild-goose chase looking for higher layer problems.

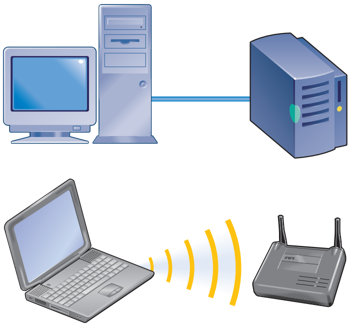


Figure 12: Verify your physical layer first. In a wired network, check your cabling run for link. In a wireless network, check the RF spectrum for interference.

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, then 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 connect the cable. If the connection works 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 ... verify your RF physical layer first.

#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 interfering 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. The majority of the time, interference is caused unintentionally by employees. For example, a 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, the camera operated in the 2.4 GHz frequency space and interfered with the Wi-Fi network. The problem was solved by creating a policy to outlaw these types of devices.

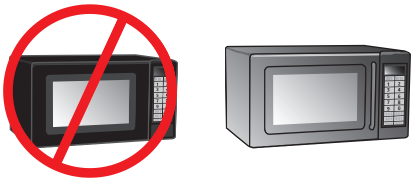


Figure 13: When possible, replace the interfering device. In the case of microwaves, replace consumer grade ovens with commercial grade ovens that provide better shielding.

Another cure is to work around the interference device by moving the affected AP, or changing its operating channel to a frequency not impacted by the interfering device. This is simple once you understand the location and frequency parameters of the interfering device. Note that some devices frequency hop (for example, Bluetooth), so 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 moving the device is not possible, adding EMI shielding can limit propagation of the interference to a small area. Shielding can be implemented via grounded mesh or foils in the walls (essentially Faraday cages), or with insulating foams or paints.

Summary: There is 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 Wi-Fi 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 PIR and 2.4 GHz radar to detect motion. These devices, which look identical to their benign predecessors, generate significant interference that can disrupt a Wi-Fi network.

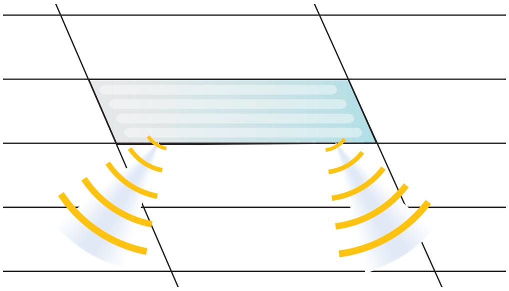


Figure 14: The number of devices that cause RF interference is staggering. Even a faulty fluorescent light can radiate enough RF interference to impact a Wi-Fi network!

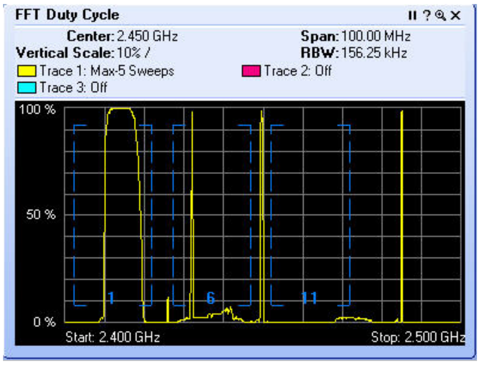
Unintentional emitters are also hard to find. A defective ballast on a fluorescent light fixture can generate broadband RF interference that can impact Wi-Fi. This is impossible to see by simply looking at the device.

"Hidden devices" are becoming more common, as well. There have been numerous instances where a security group has hidden wireless cameras – unbeknownst to the networking group – not realizing that they are interfering with 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 the data throughput (or data capacity) of your Wi-Fi network can be astounding.



Center: 2.450 GHz
Vertical Scale: 10% /
Span: 100.00 MHz
RBW: 156.25 kHz
🟨 Trace 1: Max-5 Sweeps
🟥 Trace 2: Off
🟦 Trace 3: Off

Figure 15: AnalyzeAir's FFT Duty Cycle shows that the analog video camera has a constant "always on" signal as shown by the 100% duty cycle. This constant source of interferences severely impacts the affected channels.

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. 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 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%, a frequency-hopping phone degraded throughput by 19%, and an analog phone and video camera both degraded throughput by 100% (in other words, no ability to connect).

Summary: Interference can severely degrade the performance of your Wi-Fi network.

Myth #16 – "Voice data rates are low, so the impact of interference on VoWLAN should be minimal."

Figure 16: RF interference can reduce the range of VoWLAN phones resulting in unacceptable voice quality or lost of service.

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 AP can handle many concurrent VoIP calls. Unfortunately, many factors reduce the number of calls an AP can handle. First, there is significant VoIP protocol-level overhead, which grows the typical stream to 100 Kbps, and 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 vendors advertise they can handle with a Wi-Fi AP is only 15. When interference is introduced, the number
of calls that can be handled significantly decreases.

In addition, small amounts of interference seriously impact VoWLAN voice quality. The impact of various interference devices on the MOS (mean opinion score) for VoWLAN calls 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 AP or phone.

Perhaps more importantly, interference creates coverage holes where phone calls are dropped. On average, the effective range of a VoWLAN phone drops by 50% when an interfering device (cordless phone or video camera) is within 75 feet of the AP. This 50% reduction in the range of your phones would likely result in coverage holes over 75% of your floor space.

Summary: VoWLAN 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% of your corporate network bandwidth as it spread from machine to machine, would you consider it a security or a performance concern? 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 malicious like a jammer, or accidental like a cordless headset – 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:

Figure 17: Do you know what is in your RF spectrum? If you have a spectrum use policy how do you enforce it? How would you enforce the wireless-free zone shown in this building? You can with AnalyzeAir – it can alert you when someone violates the policy and brings a wireless device into the area.

- **Multi-protocol devices:** Wi-Fi networks are typically locked down with secure access controls, but non-Wi-Fi networks such as Bluetooth 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 client based tools that control configuration of wireless network interfaces, and 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 AP detection to find unauthorized (and frequently unsecured) APs on the corporate network. But there are non-Wi-Fi devices (such as Bluetooth APs) 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.

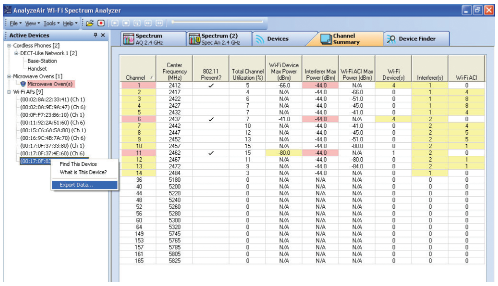
Summary: RF security doesn't stop with Wi-Fi. Do you know who's using your spectrum?

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, then 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.

However, 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 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, will still cause problems up to 40 feet from the receiver.

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



Cordless Phones [2]
DECT-Like Network 1 [2]
Base-Station
Handset
Microwave Ovens [1]
Microwave Oven(s)
Wi-Fi APs [9]
(00:02:8A:22:33:41) (Ch 1)
(00:02:8A:9E:9A:47) (Ch 6)
(00:0F:F7:23:B6:10) (Ch 1)
(00:11:92:2A:51:60) (Ch 6)
(00:15:C6:6A:5A:B0) (Ch 1)
(00:16:9C:4B:7A:70) (Ch 6)
(00:17:0F:37:33:80) (Ch 1)
(00:17:0F:37:4E:60) (Ch 6)
(00:17:0F:83

Find This Device
What is This Device?
Export Data...

Channel	Center Frequency (MHz)	802.11 Present?	Total Channel Utilization (%)	Wi-Fi Device Max Power (dBm)	Interferer Max Power (dBm)	Wi-Fi ACI Max Power (dBm)	Wi-Fi Device(s)	Interferer(s)	Wi-Fi ACI
1	2412	✓	5	-66.0	-44.0	N/A	4	1	0
2	2417		4	N/A	-44.0	-66.0	0	1	4
3	2422		6	N/A	-44.0	-51.0	0	1	8
4	2427		7	N/A	-44.0	-45.0	0	1	8
5	2432		7	N/A	-44.0	-41.0	0	1	4
6	2437	✓	7	-41.0	-44.0	N/A	4	2	0
7	2442		10	N/A	-44.0	-41.0	0	2	4
8	2447		12	N/A	-44.0	-45.0	0	2	5
9	2452		13	N/A	-44.0	-51.0	0	2	5
10	2457		15	N/A	-44.0	-80.0	0	2	1
11	2462	✓	15	-80.0	-44.0	N/A	1	2	0
12	2467		11	N/A	-44.0	-80.0	0	2	1
13	2472		9	N/A	-44.0	-84.0	0	2	1
14	2484		3	N/A	-44.0	N/A	0	1	0
36	5180		0	N/A	N/A	N/A	0	0	0
40	5200		0	N/A	N/A	N/A	0	0	0
44	5220		0	N/A	N/A	N/A	0	0	0
48	5240		0	N/A	N/A	N/A	0	0	0
52	5260		0	N/A	N/A	N/A	0	0	0
56	5280		0	N/A	N/A	N/A	0	0	0
60	5300		0	N/A	N/A	N/A	0	0	0
64	5320		0	N/A	N/A	N/A	0	0	0
149	5745		0	N/A	N/A	N/A	0	0	0
153	5765		0	N/A	N/A	N/A	0	0	0
157	5785		0	N/A	N/A	N/A	0	0	0
161	5805		0	N/A	N/A	N/A	0	0	0
165	5825		0	N/A	N/A	N/A	0	0	0

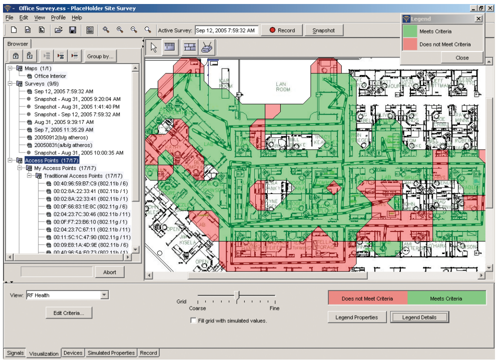
Figure 18: AnalyzeAir's Interference Power chart shows the total interference power by device type on each channel. In addition, the Interference Power chart displays the received signal power of the strongest Wi-Fi AP in each channel. This allows you to determine the amount of separation between the total interference and AP signal strength. Under best conditions, you need a buffer of at least 20 dB.

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

A standard Wi-Fi site survey tool, such as Fluke Networks' InterpretAir WLAN Site Survey Software, is designed to measure Wi-Fi coverage and performance. It uses a Wi-Fi chipset to measure the signal strength of APs 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.

A Wi-Fi site survey tool might indicate a general area where a non-Wi-Fi signal was observed. But the site survey tool cannot help you determine the nature of the interference, the type of device causing it, or where the device is physically located. So, you are left without a solution to your interference problem. You really need an RF level tool to diagnose interference problems.

Summary: Site survey tools measure coverage and performance … but don't solve your RF interference problems.



Active Survey: Sep 12, 2005 7:59:32 AM

🟩 Meets Criteria
🟥 Does not Meet Criteria

Maps (1/1)
Office Interior
Surveys (9/9)
Sep 12, 2005 7:59:32 AM
Snapshot - Aug 31, 2005 9:20:04 AM
Snapshot - Aug 31, 2005 1:41:40 PM
Snapshot - Sep 12, 2005 7:59:32 AM
Aug 31, 2005 9:39:17 AM
Sep 7, 2005 11:35:29 AM
20050912(b/g atheros)
20050831(a/b/g atheros)
Snapshot - Aug 31, 2005 10:00:35 AM
Access Points (17/17)
My Access Points (17/17)
Traditional Access Points (17/17)
00:40:96:59:B7:C9 (802.11b / 6)
00:02:8A:22:33:41 (802.11b / 1)
00:02:8A:22:33:41 (802.11b / 1)
00:0F:66:83:1E:8C (802.11g / 6)
02:04:23:7C:30:46 (802.11b / 11)
00:0F:F7:23:B6:10 (802.11g / 1)
02:04:23:7C:67:11 (802.11b / 11)
00:11:5C:1C:47:90 (802.11g / 11)
00:09:E8:1A:4D:9E (802.11b / 6)

View: RF Health

☐ Fill grid with simulated values.

Does not Meet Criteria | Meets Criteria

Figure 19: Site survey programs, such as InterpretAir, can show your WLAN's coverage and performance statistics but can not solve your RF interference issues. In this screen capture, InterpretAir's RF Health enables the visualization of multiple measurement criteria into a single view, simplifying analysis and accelerating decision making.

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

Many RF analysis tools (such as large expensive spectrum analyzers) are not enterprise friendly. Fluke Networks' AnalyzeAir is designed to fit both your desired form factor (small cards that plug into your laptop or OptiView Network Analyzer) and your IT budget. To make things even better, Fluke Networks tools have built-in intelligence, so that you don't have to be an RF expert in order to use them.

Summary: Take a look at Fluke Networks' AnalyzeAir Wi-Fi Spectrum Analyzer (**www.flukenetworks.com/analyzeair**)

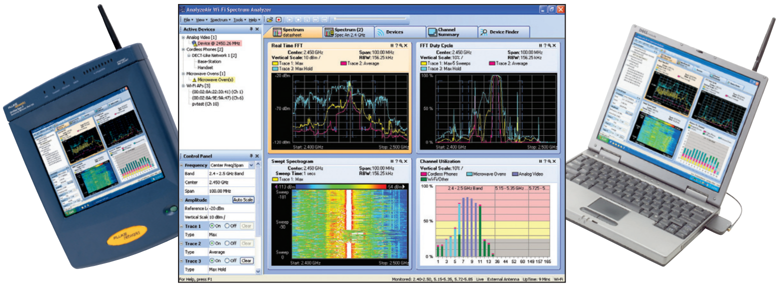


Figure 20: AnalyzeAir provides IT professionals with vision into the hidden world of RF, and lets you see the spectrum in a visible and intelligent format. AnalyzeAir lets you see, monitor, analyze, and manage all the RF sources and wireless devices that influence your Wi-Fi network's performance and security – even if those devices are unauthorized or transient.

AnalyzeAir™ Wi-Fi Spectrum Analyzer

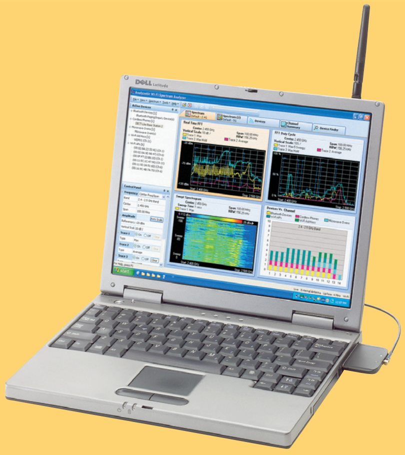
Detect, identify, and locate RF interference in 802.11 WLANs

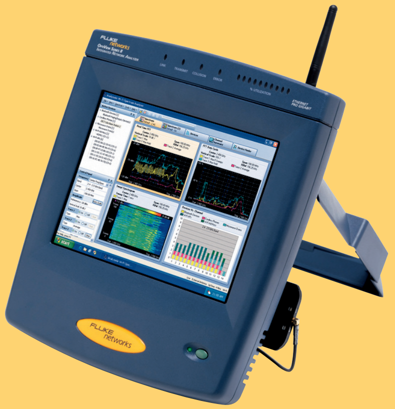
AnalyzeAir provides IT network professionals with the vision they need into the hidden world of RF, providing them with the ability to see the spectrum in a visible and intelligible format. AnalyzeAir software lets you see, monitor, analyze, and manage all the RF sources and wireless devices that influence your Wi-Fi network's performance and security, even if those devices are unauthorized or transient.

Are you receiving end user complaints about WLAN performance? Take AnalyzeAir to the problem location and quickly solve physical layer RF problems that prevent optimum wireless connectivity. AnalyzeAir Device Finder function will lead you to the offending device allowing you to quickly locate troublesome or unauthorized devices.

Are you preparing for a new wireless deployment or expansion of an existing wireless network? Knowing what is in your RF spectrum ahead of time will help prevent performance problems later on. Find out what may cause interference so it can be removed or shielded before the users start complaining.

AnalyzeAir software takes the cost and complexity out of spectrum analysis. Unlike single-function RF analyzers or expensive tools that provide RF information without device identification and location, AnalyzeAir provides an easy-to-understand, fast-start solution, allowing users to quickly resolve RF problems that prevent WLAN connectivity and impact performance.





Printed in U.S.A. 11/2007 2719971 D-ENG-N Rev B