Wi-Fi Spectrum Management

A Webtorials Thought Leadership Discussion Digest

Discussion and comments through July 26, 2010

This Thought Leadership Digest is made possible in part due to the generous support of:

CISCO

AIRMAGNET
now part of Fluke Networks

Contents

Introduction

Joanie Wexler, Moderator

Welcome to this Thought Leadership Discussion about managing the unlicensed RF spectrum in wireless LANs (WLANs).

Wi-Fi networks operate in unlicensed wireless frequencies in the 2.4GHz and 5GHz bands. Because these bands are unlicensed, everyone has equal rights to use them. As more Wi-Fi networks get deployed, the more crowded these "free" frequencies get. So it's important to protect communications growing increasingly prone to interference that can cause connectivity and performance problems.

This discussion addresses approaches to successfully managing spectrum and discovering and acting on sources of interference so that businesses can optimize performance and lower the risk of their Wi-Fi connections. Please feel free to participate by posting your own questions and comments, which our participating thought leaders will answer in a timely fashion.

In addition to me, our core panel of thought leaders discussing managing the unlicensed RF spectrum includes:

Dilip Advani
Product Manager
AirMagnet/Fluke Networks

Neil Diener
Technical Leader
Wireless Networking Business Unit
Cisco Systems

And below is a sampling of questions that are already posted and that *you can comment on*:

- **Do the Wi-Fi airwaves need to be scanned 24x7?**
- **Is it adequate for an enterprise to scan only the channels that it is using?**
- **How is spectrum analysis different from wireless resource management or RF management?**
- **Are spectrum analysis capabilities better, worse, or the same, depending on whether they are implemented in ASIC or software? Why/why not?**
- **How labor-intensive is spectrum management if done right (what do you have to do)? What can be successfully automated?**
- **What about other RF management approaches?**
- **What about smart antennas as an alternative?**

Please enrich our wireless security round-table discussion by posting your own questions and adding insight to the discussions already under way.

24x7 Scanning?

Joanie Wexler, Moderator

Do the Wi-Fi airwaves need to be scanned 24x7? Why or why not?

Dilip Advani, AirMagnet/Fluke Networks

Both mobile spectrum analyzers and 24 X 7 distributed spectrum solutions (sensors with built-in spectrum analysis adapters) have significant benefits and advantages. The choice between them may ultimately come down to the preference of the user and their business and/or technical requirements for their WLAN deployment. These include:
1) Need for remote monitoring as compared to on-site monitoring, which may be influenced by the number of sites that need to be monitored and the availability of IT staff members
2) Budget for RF spectrum monitoring
3) Need for 24 X 7 monitoring for security purposes
4) Number of RF related problems occurring in the network
5) Time between RF spectrum scans
6) Need for pin-pointing the location of the interference source

The use of mobile spectrum analyzer solutions, like AirMagnet Spectrum XT, in the WLAN deployment phase is mandatory. Results from the initial RF spectrum sweep go a long way in making the right choices for a successful and optimally performing WLAN. RF energy levels and the presence of interference sources detected by the spectrum analyzer influence the location of the APs and their channel and power settings. Mobile solutions also work great when you are trying to physically locate interference sources, so that they can be stopped from operating or can be quickly removed from the facility. So, even if the source is hidden inside a drawer, on top of a bookshelf or is built inside some other office equipment or fixture, the “Geiger-counter” based device locator feature can lead the IT staff member to the exact location. Also, many of the non Wi-Fi interference problems are location specific and require spectrum solutions to travel to the location of reported problems. For example, with a mobile solution, one can precisely measure the level of interference and other RF specific parameters at a location, instead of relying on reports from sensor hundreds of feet away.

A 24 X 7 distributed monitoring solution, which includes RF spectrum sensors reporting back to a centralized server, has its own advantages. Sites that need remote monitoring due to unavailability of IT staff or lack of RF expertise at every location may benefit from a centralized spectrum solution. Some corporations may also mandate continuous monitoring to detect any unauthorized activity, such as layer 1 DoS attacks from unintentional or intentional transmitters

(like RF jammers), or may implement a “no wireless or RF” policy (commonly seen in Federal or military deployments) and need to be alerted to the presence of RF emitting devices. The use of mission-critical applications (for example healthcare applications or even voice over WLAN) warrant for continuous monitoring of the network. Distributed 24 X 7 spectrum solutions, such as AirMagnet Enterprise, send alerts (emails, page messages, etc.) to the IT staff as soon as interference sources are detected and even allow saving of RF data as forensic information for post-capture or post-incident investigation.

AirMagnet provides best of both world industry-leading solutions (i.e. 24 X 7 distributed solution and mobile spectrum analyzers) to provide users with a complete arsenal of solutions to deal with any interference related problem. Users commonly start with the mobile spectrum solution, and, realizing the potential and benefits of spectrum monitoring and management in their network, move to the distributed solution as the number of sites that need to be monitored increases.

Neil Diener, Cisco Systems

Yes. An initial or periodic scan is insufficient because 1) new devices can be introduced at any time as someone walks into the enterprise carrying a device, 2) lots of devices are used intermittently (ex. cordless phones) and might be missed during a periodic scan.

Also, 24x7 scanning gives you: pro-active alerting as soon as a problem occurs and history over time of how often similar problems occur.
History is also important when you have a trouble ticket from a day or two ago, and want to understand what was happening in the RF during that window.

Scan only Used Channels?

Joanie Wexler, Moderator

Is it adequate for an enterprise to scan only the channels that it is using? Why or why not?

Dilip Advani, AirMagnet/Fluke Networks

There are 2 main reasons for monitoring the entire frequency bands for spectrum management, instead of just narrowly focusing on the channels that are being used by the enterprise.

1) Paint the complete picture of the entire frequency band to empower IT staff members to make sound channel planning decisions. In a situation where the AP needs to switch its operation from one channel to another for any reason, maintaining that detailed information on the "cleanliness" of the new channel is very critical to be able to continue to operate the network at its top performance.

2) Many of the non Wi-Fi interference sources operate on more than a single channel or hop around different frequencies in the entire spectrum. Even though the center frequency of the interference source may not be the same as that of the corporate or authorized channels, the RF energy from these sources may bleed over or be a part of the hopping sequence, leading to disturbances on the corporate channels. By monitoring the entire frequency range, the enterprise IT staff can expand their "point of vision" for the frequency band and determine the root cause for lowered performance in their WLAN, which may be due to interference sources that may not be operating on the corporate channels.

Joanie Wexler, Moderator

Dilip - can you think of any pros/cons to getting this 24x7 monitoring capability from a third party such as AirMagnet/Fluke rather directly from the WLAN systems vendor - either from a functional standpoint, cost perspective, or something else?

Dilip Advani, AirMagnet/Fluke Networks

PROS

1. Independent 3rd party monitoring: With overlay spectrum monitoring or management solutions like the ones offered by AirMagnet/Fluke, users get an independent and unbiased view of the RF environment as seen by the AirMagnet sensors. The important thing to remember is that it can also be used as an overlay solution for any WLAN Infrastructure vendor, so this is a solution for every WLAN deployment even if the deployed AP vendor does not offer any spectrum monitoring capability.

2. Zero-downtime for upgrades: When spectrum capability is built inside the AP that is providing client data access, any new spectrum features, including any new signatures needed to classify new RF interference sources will call for upgrading the AP's firmware/software or, in certain cases, even the hardware. This system-wide upgrade of an active WLAN deployment may not be feasible or acceptable for most users. On the other hand, AirMagnet is a dedicated monitoring overlay system, that delivers best-of-breed air monitoring, with easy updating to the latest features and signatures, and most importantly with zero downtime or upgrades to the existing active WLAN infrastructure.

3. Dedicated active spectrum development and innovation: This has been proven in the industry with the AirMagnet spectrum solution being the first and the only 24 X 7 dedicated spectrum monitoring solution in the last 4+ years. AirMagnet has continued innovating in the RF spectrum analysis field, with the best example being the introduction of classification for new interferers, Wi-Fi impact analysis (visualization of impact of RF interference on Wi-Fi performance) and many more. Also being an overlay solution does not limit any innovations or updates to the solution to solve new interference issues, as compared to infrastructure solutions that may have to time these updates with general AP updates (which don't happen very frequently).

4. Complete troubleshooting solution combining spectrum and Wi-Fi intelligence: With dedicated and specialized spectrum monitoring solutions, like the those offered by AirMagnet, users can get the best-of-both worlds, layer 1 and layer 2 information and how they correlate to each other. Not only can users detect RF interference sources, but at the same time they can correlate that information with detailed Wi-Fi statistics for corporate devices. For example, users can see if an RF jammer wipes out signals for the corporate AP or leads to excessive errors or retries on the AP or its operating channel. This makes troubleshooting RF issues very quick and efficient, allowing users to prioritize their troubleshooting activities in the detection and location of interference sources.

5. Total cost: The total cost of a spectrum solution from a WLAN Infrastructure vendor may include the purchase of new AP hardware with spectrum capability and/or analysis engine servers, making the overall purchase very expensive. On the other hand, software based spectrum solutions may appear to be cheaper, but lack any true RF spectrum capabilities to solve any real RF problems. With overlay spectrum solutions, users are powered not only with a feature and benefit-rich application that can actually troubleshoot RF performance and security problems in their network, but also a very affordably priced product.

6. Companion troubleshooting tools: With the AirMagnet solution, users can also get the companion field spectrum analyzer tool, AirMagnet Spectrum XT, which can travel to the location of the problem for on-site location specific troubleshooting. The mobile tool, as mentioned in the previous topic also works great for pin-pointing the location of interference sources.

CONS

The only con, in my mind, would be the need for a specialized sensor, as it is an overlay solution. But with the AirMagnet solution, the sensors serve a dual purpose, and not only monitor the RF environment for interference issues, but also perform layer 2 security and performance analysis.

This bullet-proof security, performance, compliance and RF-monitoring solution is definitely worth the investment for an overlay solution.

Neil Diener, Cisco Systems

No. From a security standpoint, it is important to scan all frequencies for rogue RF devices. For example, a proprietary bridge operating on an off frequency may represent a security breach to your network.

It is also beneficial to scan additional channels beyond where your wireless network is operating so that you can monitor performance and prepare for future interference. For example, some devices such as cordless phones and wireless video cameras have the intelligence to try and operate on channels that will not interfere with your Wi-Fi network; however if someone later manually changes the operating channel of the device, it may suddenly start causing interference. Since new devices may enter your Wi-Fi network at any time, and current devices can randomly switch channels and interfere with your network, scanning outside your Wi-Fi networks channels plays an important role in proactively detecting and avoiding interference.

Joanie Wexler, Moderator

OK, looks like you're agreed that all frequencies should be scanned. Neil, is the 24x7 scanning capability available from Cisco and, if so, do customers have to pay extra for it?

Neil Diener, Cisco Systems

Yes, Cisco CleanAir is based on a 24x7 scanning capability. If the AP is operating in Local Mode (serving traffic), then the AP performs 24x7 scanning on the active channel. If the AP is operating in Monitor Mode, then the AP performs 24x7 scanning on all channels. In either case, this 24x7 spectrum information is reported up to the controller, and then to the WCS management server where it is stored in a database for reporting.

There is no charge for the CleanAir capability, other than the requirement that you use the 3500 series AP.

Steven Taylor, Webtorials

In the event that you are operating in "Local Mode," is there an option for changing the active channel in the event that severe interference is detected?

If so, is this advisable? I can see some advantages to the automation, but I'm also sufficiently "old-school" to be a little bit nervous about too much automation.

Neil Diener, Cisco Systems

Yes, the Cisco system has the capability to change the active channel in the event that severe interference is detected. We refer to this feature as "Event Driven RRM".

We feel very confident in this feature, because it only reacts when the interference: 1) has been classified, and 2) is seen to be causing a major impact.

In the past, systems without spectrum analysis capability were reluctant to implement a feature like this for fear that they would react accidentally to heavy WiFi traffic on a nearby AP, and thereby cause the system to be unstable.

How is spectrum analysis different?

Joanie Wexler, Moderator

How is spectrum analysis different from wireless resource management or RF management?

Dilip Advani, AirMagnet/Fluke Networks

Spectrum analysis is all about interference and how to minimize it in your network to ensure top performance. This includes detecting the source, understanding its impact on the network and then removing the source of the problem. Wireless resource management, on the other hand, includes dynamic changes in the configuration settings of the network (changing channel or transmit power based on noise or interference in the environment) to be able to cope with temporary changes in the environment or network. So, while resource management solutions can provide temporary relief to a WLAN problem, the ever-critical thing is to quickly find and remove the problem source. Delving into the impact of interference on your network and solving the root cause of the problem is the recommended methodology to ensuring a trouble-free WLAN. And spectrum analysis ensures that layer 1 operates efficiently.

Neil Diener, Cisco Systems

Spectrum analysis provides data about RF spectrum activity, including both Wi-Fi and non-Wi-Fi interference.

Wireless resource management (or RF management) is the active use of this spectrum intelligence data to improve wireless network performance.

The best systems combine both spectrum intelligence technology (integrated within the infrastructure), and RF management software that uses this information to optimize performance. For example, the spectrum analysis may determine that an interference device is causing a serious outage at a particular AP, and then the RF management system will immediately change the channel of the AP to move away from the interference.

Neil Diener, Cisco Systems

One thing I may not have clearly pointed out is that traditional RF management systems did not have information on specific devices in the environment. Typically, all they could see was that there was some kind of "noise" out there.

Spectrum analysis adds this key piece of information -- what is the source of the noise? This classification of the interference is extremely important in two ways:

1) Classification provides meaningful information to IT. If IT is able to understand the source of the interference, they can take actions such as turning it off, replacing with another type of device, etc.

2) Classification provides more detailed information to the RRM system. If the RRM system knows that this is real interference (as opposed to heavy WiFi traffic on a nearby AP), it can be more confident that changing channels will have a positive impact. Also, RRM can make intelligent assumptions based on the type of device -- Is it likely to stay in this spot? Is it likely to come back tomorrow? Is it likely to be impacting all channels (as in the case of a frequency hopping device)?

So, as you can see both human and automated responses are improved when the source of the interference is understood.

How do spectrum analysis capabilities vary with implementation in ASIC vs software?

Joanie Wexler, Moderator

Are spectrum analysis capabilities better, worse, or the same, depending on whether they are implemented in ASIC or software? Why or why not?

Dilip Advani, AirMagnet/Fluke Networks

Spectrum analysis capabilities implemented in custom silicon is the recommended implementation. These hardware-based solutions speed up data collection and processing of RF information (FFT of the spectrum and RF energy bursts) as compared to software-only based solutions. This is also directly reflected in the granularity of resolution of the RF data that is presented to the user. With these capabilities, the spectrum solution is able to keep up with all the dynamic or transient changes that are occurring in the RF environment. In ASIC based solutions, it is important to remember that the firmware also plays a major role and is responsible for the actual device classification, giving the entire solution the flexibility to receive updates as new interference devices need to be added to the default classification database. If this capability were not available, hardware upgrades would be needed every time the vendor has new entries for the classification database, which in most cases would be unacceptable.

Software-based spectrum solutions using Wi-Fi adapters that are traditionally built to see only Wi-Fi signals may see certain bursts of RF energy that may not be deciphered, but can somehow still be used to calculate basic interference levels or scores. It cannot deliver the critical information to solve any real issue, which includes accurate detection of non Wi-Fi interference sources, the channels they impact, level of impact, location capabilities, etc. Software-based spectrum capabilities are used more as a feature check-box item for RFPs or websites that are used by vendors when they are asked about their RF spectrum management capabilities. Novice users may be influenced by this and accept these solutions, regretting it later when faced with the challenge of solving a real problem.

Neil Diener, Cisco Systems

Effective spectrum analysis solution requires ASIC capabilities, including hardware accelerators and dedicated capture memory.

The variety of interference devices in the unlicensed band is broad, and is only growing over time. For this reason, a simplistic and small set of classifiers is not sufficient. Software-only spectrum analysis solutions do not have sufficient capability to scale to a large set of classifiers and operate effectively.

The first reason software solutions can't scale is that the total horsepower (MIPS/capture-memory) required grows with the number of classifiers. Think of each classifier as a theory that must be tested vs. an unknown energy source. In other words, when we see energy, we must test: Is it Bluetooth? Is it a cordless phone? Is it a jammer? Is it WiMax? This causes the amount of processing to grow with the *number* of classifiers.

The second reason software solutions can't scale is that when you start to add more classifiers you need to change the way you perform the analysis. With a simple small set, it's possible to look only at the "fingerprint" of the interference – the timing of pulses and center frequency. But when you add more classifiers and need to separate between devices that are similar from an RF perspective (or to detect how many devices are actually present), you need to do deep "DNA" analysis of the signals. This takes a tremendous amount of DSP processing power.

When a software-only solution runs up against the wall in terms of MIPS and/or capture-memory, it starts to do one of two things: A) it does not run all the tests, or B) it cuts back on the quality of analysis it runs before declaring a particular device is present. Not running all the tests results in non-detects – i.e. missing devices. Cutting back on the quality of analysis results in false detects – seeing ghosts. Both of these affects are intensified in a busy RF environment, where there is a lot of activity, and it's very easy to confuse normal activity with interference.

Non-detects are a big issue. When a user calls in with a wireless problem, IT wants to diagnose the source of the problem. The first thing IT wants to determine is whether the problem is at the physical layer. So, Spectrum Intelligence is supposed to reveal whether the physical layer is OK or not. But if the system is subject to non-detects, it can't be trusted. The system reports nothing, but IT is still left with the nagging feeling that interference might be the issue. In other words, the use case has not been solved.

False detects are also a big problem. In the end, the model of a customer calling with a problem (reactive model) is undesirable. What IT wants is a system that can be more proactive, and alert about interference before it becomes a problem. But a system that false detects is one that sends IT on a wild goose chase. Every time there is a false detect, IT wastes time chasing down a ghost. IT must trust that the system does not "cry wolf", or they will simply turn off pro-active alerts.

To summarize, the only effective spectrum analysis solution that can scale to a large set of classifiers, without false detects and non-detects is a system with sufficient ASIC and memory horsepowe

Steven Taylor, Webtorials

On the question on ASIC vs. software, both seem to agree strongly. So does anybody do this via software?
What's the advantage of software? Easier upgrades?
And if the ASIC is programmable, doesn't this imply "software"?
So doesn't the ASIC lead to a more extensive/expensive upgrade?

Dilip Advani, AirMagnet/Fluke Networks

There are WIDS/WIPS vendors that claim to perform professional spectrum analysis at the software level inside their sensors. With this solution, you do not have the granularity to see the true nature of the physical RF environment and the solution faces major limitations, including inaccurate detection of interference sources, inability to detect most interference sources, poor and imprecise spectrum resolution, etc. Regarding upgrading an ASIC or other hardware accelerated solution, firmware upgrades are simple to apply and can be augmented by enhancements to application software as well.

Neil Diener, Cisco Systems

There is no advantage to a software-only solution. Some WiFi vendors are limited by the capabilities of their WiFi chipsets, and so are trying to make do with what they have. But the performance of these software-only solutions will not meet Enterprise requirements.

In terms of upgrade, the Cisco solution consists of both ASIC HW and software. The software portion is upgradeable to add more classifiers over time (as new types of unlicensed band devices are introduced). There is no cost to these upgrades.

How labor-intensive is spectrum management?

Joanie Wexler, Moderator

How labor-intensive is spectrum management if done right (what do you have to do)? What can be successfully automated?

Dilip Advani, AirMagnet/Fluke Networks

This is dependent on the actual application for the spectrum analysis product.

Let us consider the case of a pre-deployment scenario, where the IT staff member has to manually walk around the facility with the product to perform the initial RF spectrum sweep. This may appear to be labor-intensive and does involve spending time, effort and money on the project, but it is absolutely worth the investment. It empowers the staff to make sound RF and WLAN design decisions and to avoid any pitfalls with the operation of the WLAN network in the future. This additional effort can be mitigated by the fact that there are site survey tools that integrate with mobile spectrum analyzers, allowing the collection of RF spectrum information at the same time as the WLAN site survey, in a single walk through the facility. AirMagnet Survey PRO integrates with all industry-leading spectrum solutions like AirMagnet Spectrum XT, AirMagnet Spectrum Analyzer, Fluke Networks AnalyzeAir and Cisco Spectrum Expert, to provide this unique and important phase in the design of the WLAN. This one-time sweep is no different than planning out a wired network in terms of the level of detail and time involved.

Removing the interference source, or shielding the network from it, is one of the best solutions for dealing with interference issues and requires devices to be physically located. Let us consider a case where the interference source maybe hidden from normal view and a mobile spectrum analyzer is needed to pinpoint its location. This will call for the IT staff member to walk around the facility using the device locator, or find a tool built inside the spectrum analyzer product. However, best practices, as recommended by the spectrum vendor and the ease of use of this feature within the spectrum product, go a long way in making device location quick, efficient and effective.

Let us consider the next case, where users have a distributed spectrum solution deployed in their facility. This implementation is very helpful when 24 X 7 monitoring is needed for the network or the IT staff is responsible for monitoring multiple floors or buildings across a campus or

branch offices. In this scenario, dedicated spectrum sensors are placed in different locations on the floor to monitor the RF environment on a continuous basis. They alert the user automatically as soon as the interference source is detected. As mentioned in the first section, this alert can be delivered to the user via email, page messages or even sent to a centralized SNMP or syslog server. Users could also choose to capture and save all of the RF information as forensic evidence for any remote location.

The important thing to remember is that whatever maybe the effort or automation involved, spectrum solutions must be on the mandatory list of monitoring solutions for every IT staff member responsible for the successful operation of the WLAN. A well-planned solution that includes RF spectrum sweeps can continue to be successfully managed and maintained with the automated spectrum management solution.

Neil Diener, Cisco Systems

If spectrum management is well integrated into the system, then it should classify and locate devices without requiring any effort. The system should also have some abilities to automatically mitigate interference where possible.

The labor part comes into play when manual intervention is required. Not all devices can be easily mitigated (ex. jammers). And even when automated mitigation is possible, it’s a good idea to remove the interfering device eventually since it is taking up some of your RF capacity. At this point, the human gets into the loop to remove, disable, move, replace, or shield the interfering device. For example, if someone outside of the IT departments sets up a video camera that is jamming all your Wi-Fi channels you can either have it replaced with a wired camera or select another wireless camera that does not use the same 2.4 GHz frequency as your wireless network.

Joanie Wexler, Moderator

Neil - your example of the wireless/wired camera begs the age-old question as to whether wireless LANs can ever really approach the reliability of wired Ethernet. What if that camera were installed by someone in the office next door? It's great that spectrum analysis can discover equipment interfering with your network, regardless of whose it is. But what can you do about it if that equipment belongs to someone else? The unlicensed airwaves are an equal-opportunity medium.

Neil Diener, Cisco Systems

In a single tenant building, you can create and enforce a spectrum utilization policy. But as you point out, in a multi-tenant building this can be harder to control.

One thing that helps is that there is a good amount of spectrum in the unlicensed band, and so in most cases it's not likely that a neighbor would cause interference on all channels.

But if you did run into this kind of situation, a few other potential solutions would be: 1) talk to your neighbor and explain the problem, and see if they are willing to change their devices 2) put some RF shielding in place to minimize the impact of their devices, and 3) work through your landlord to resolve the situation -- similar to the way you might handle it if you having a neighbor tenant who bangs on the walls or plays loud music.

At the end of the day, the unlicensed band does have limited regulations and so limited recourse when you are being interfered with. But in most realistic cases these kinds of issues can be worked out amicably.

Other RF management approaches?

Joanie Wexler, Moderator

What about other RF management approaches?

Other vendors take different approaches to spectrum management. One, for example, uses an architecture whereby the controller manages both APs and clients and puts all APs on a single channel far apart from one another at full power. The vendor says this approach eliminates most interference. What is your argument against this architecture and in favor of your own approach to spectrum management?

Dilip Advani, AirMagnet/Fluke Networks

Spectrum management involves much more than just maintaining acceptable RF interference levels in the environment. While it does sound interesting that a user can reduce the amount of interference by configuring the wireless devices to operate on a single channel, it needs to be clarified that this only relates to adjacent channel interference and not the overall interference in the RF environment. Interference encompasses multiple sources, and Wi-Fi based adjacent channel interference is just one piece of the puzzle. A large contributor to lowered WLAN performance is interference arising from non Wi-Fi devices operating in the same spectrum band. These are sources that should not be ignored and have the capability of wiping out all signals, not only in the single channel where all the devices may be operating, but also the entire frequency range. These “hidden” or “invisible threats” are present in everyday corporate environments and are commonly implemented inside everyday devices or equipment. They include Bluetooth or zigbee devices, microwave ovens, cordless phones, wireless cameras, motion detectors, etc. Simply moving all devices on to a single channel cannot prevent these non Wi-Fi sources from impacting performance.

In certain deployments, single channel architecture may be required or preferred to satisfy a particular business or technical requirement, but for thorough interference monitoring and network management, “true” spectrum analysis solutions like AirMagnet Spectrum XT, or the spectrum sensors as part of AirMagnet Enterprise that monitor for all sources of interference in the RF environment, must be implemented.

Neil Diener, Cisco Systems

Tool-based solutions can be effective; however they require travel to the source of interference and are highly manual intensive. When spectrum intelligence is fully integrated into the network architecture it operates 24/7, constantly monitoring for interference and air quality issues. This allows IT to take a more proactive approach to spectrum management. Instead of waiting for interference to be reported by an end user and then dispatching a tool to analyze the problem, IT can find interference as soon as it occurs and take immediate action. Having a 24/7 history also makes it possible to look back in time. Using historical data, it's easy to perform analyses of trends over time.

Whether it is tool based or infrastructure based, the only way to effectively manage RF interference in the unlicensed band is to classify and understand the sources. First, understanding the device type is important when the human needs to take action. Second, understanding the source is critical to enforce spectrum security policy. And third, knowing the source of the interference is important in order to be able to implement intelligent mitigation policy based on the type and characteristics of the device. For example, if a device is of the non-mobile type and tends always to operate on the same frequency (e.g. microwave oven), then when I see it once I will tend to see it again. So, knowing a device like this is operating in a certain part of the network can be factored into channel assignments, even when the device is not currently active.

LinearBob, WattMinder

One of the often overlooked aspects of wireless network design is antenna choice and placement. In general, properly placed directional antennas will produce a more robust and reliable network than one based on randomly placed omni antennas. While it takes time to design a wireless network using directional antennas, the resulting network can be less susceptible to outside interference, less likely to cause interference to other networks in close proximity, and much more secure than the simple design based on omni antennas. One metric worth considering is antenna gain. The more directional an antenna is, the higher the antenna gain it exhibits. Antenna gain is the direct result of restricting where the signal does and does not go. Two neat aspects of antenna gain are that it is noise free and that it requires no external power.

Devin Akin, Aerohive Networks

While directional antennas are sometimes useful (outdoor and specific indoor use cases), it's impractical to use them en total for an indoor deployment. If you're going to take that approach as a network designer, Ruckus's beam steering solution is a better fit because it's a dynamic, rather than static solution. At least that way, you'd get the benefit of both

directional and omni antennas at the same time. Ruckus should now send me a gift basket. :)

GT Hill, Ruckus Wireless

Hey Devin... thanks! You saved me a lot of typing. By the way, I did send you a gift basket. It's not my fault you didn't want our cheapest 11b/g AP. :)

GT

What about smart antennas?

Joanie Wexler, Moderator

What about smart antennas as an alternative?

Another vendor uses a smart-antenna architecture it says doesn't propagate energy in directions other than toward the receiving clients, keeping interference to a minimum that way. What is your argument against this architecture and in favor of your own approach to spectrum management?

Dilip Advani, AirMagnet/Fluke Networks

It is critical for IT staff members to detect all possible sources of interference in the environment. By directing the RF energy from the AP to the receiving clients, vendors may claim to be effective in increasing the Signal to Noise Ratio at the client device, thus contributing to increased throughput or minimized interference in certain directions, but it cannot be the only mitigation method for dealing with RF interference. How does such a solution handle wide-band interference over the entire frequency band? Those wide-band sources wreak havoc in the RF environment, leaving WLAN networks unusable. It is better to find the problem and remove it from the environment, instead of just avoiding its path assuming that transmissions will not be interfered or interrupted. That can be achieved only with an RF spectrum management solution. “Detect, locate and classify” should be the anthem for any IT staff member to handle WLAN performance and security issues at layer 1.

Neil Diener, Cisco Systems

Smart antennas , beam forming, MIMO can all help in getting some improvement to SNR, which helps with interference. But at the end of the day, interference signals are typically very hot, and “burning through” interference is not a reality. At best, these processing gains can be used to somewhat reduce the “zone of impact” of an interference device – ie. how much of the floorspace is taken out by the device. But there will always be a zone of impact, and the key is to understand and deal with the source of interference.
In a retail environment if a 100 Mw cordless phone is 4 feet away from a bar code scanner, the interference from the phone will drop the Wi-Fi connection between the scanner and the AP.

CleanAir technology can solve this interference by changing channels away from the cordless phone , wheareas an antenna system will not be capable of resolving the interference.

With smart antennas the zone of impact may shrink a tiny bit but the interference is still there. So if wireless users are spread out the interference will go down a small amount but the interference will still impact the user closest to the source of interference.

Joanie Wexler, Moderator

Neil, you mention that CleanAir can solve interference problems by changing channels away from the source of the interference. What is the impact of such channel hopping on real-time traffic; namely, voice over IP over WLAN (VoWLAN) conversations?

Neil Diener, Cisco Systems

CleanAir will not change channels unless the interference is severe -- and in this case VoIP and VoWLAN will be experiencing serious issues anyway.

After the channel change, there will be a brief loss of service as the client probes and finds the AP again, and then service should resume (with much better quality, since the AP has moved away from the interference).

GT Hill, Ruckus Wireless

Dilip,

Spectrum analysis doesn't fix or mitigate interference. It is a necessary part of a toolkit, but it is a reactive solution, not proactive like beam steering.

What would be the difference between increasing the SINR when the source of interference is wide band vs. only on one channel? None that I am aware of, but if I am wrong I will stand corrected. SNR/SINR is key to Wi-Fi connection and performance. I do agree that tools to detect, classify and locate are valuable for sure. However, having some extra signal to each STA does mitigate the effects of regular interference. (e.g. Bluetooth,

low power cordless phones, microwave ovens etc)

Neil,

If you think about it, ALL Wi-Fi transmission burn through interference. Whether it is white Gaussian noise or a cordless phone, we are all overcoming interference of some type.

I'm not sure that I agree that most sources of interference are "hot" and disable the channel. In fact, I love it when the source of interference is so high that it basically acts as a DoS? Why? Easy to find and easy to shut down. What is a real killer is all of the general noise that is added from devices that slow down performance, but typically is just accepted by the net admin staff. Very few organizations have the resources to act on the information gained through system wide spectrum analysis.

Changing channels to avoid interference? I think that a spectrum analyzer in the AP is cool and all, but all vendors of significance have been able to change channels in response to interference for years without any special sauce.

One major problem is most vendors (including us) don't know if the channel they are moving to is actually better. You may be jumping from a room full of smoke to a room full of fire. Channel changes are necessary to combat strong noise, but should only be used as a last resort, not the only resort.

GT

Integrated vs. separate management?

Steven Taylor, Webtorials

It seems that having an independent system (AirMagnet) provides a truly independent view of the network regardless of the AP supplier. However, the Cisco approach only works if it's used with Cisco APs (I assume). This also could lead to a follow-up on economics. Which is the more cost-effective method? What are the pros and cons? Can CleanAir work in conjunction with non-Cisco APs?

Neil Diener, Cisco Systems

With the Cisco solution, you can actually deploy in three ways:
1) Deploy 3500 APs in Local Mode, where they serve traffic and monitor spectrum on the active channel.
2) Deploy an overlay of 3500 APs in Monitor Mode, where they monitor spectrum on all channels.
3) Do both (1) and (2).

In terms of capability, option (3) is the best.
In terms of cost, option (1) is very cost effective.
If you have an existing network that you don't want to replace, then option (2) can make a lot of sense. And to your question, the existing network does not necessarily need to be Cisco.

Steven Taylor, Webtorials

Thanks, Neil.

Can you say a bit more about "Local Mode" versus "Monitor Mode"?

In "Local Mode," are only selective channels monitored? (Why would I ever want to do this?)

Is there a price differential depending on which modes are activated?

If not, then if I were to choose option (2) then wouldn't I be essentially "wasting" the capability to serve traffic?

Neil Diener, Cisco Systems

In "Local Mode", the AP does 2 things at the same time: 1) serves traffic, and 2) monitors for interference on the current (active) channel. The reason a Local Mode AP does not perform spectrum scanning on other channels is because this would impact the ability of the AP to serve traffic.

In "Monitor Mode", the AP is dedicated to scanning. Since it is not serving traffic, it is free to scan on all channels without impacting performance.

There is no price difference depending on which mode is activated. But since Monitor Mode APs do no serve traffic, they are typically "extra" APs that are added to the deployment (in addition to the traffic-serving APs).

Steven Taylor, Webtorials

Thanks for the clarification!