Cisco CleanAir Technology: Intelligence in Action

This white paper addresses the RF interference challenges that result from high usage of a shared spectrum. It explores the limitations of standard Wi-Fi chip design and how this affects the ability of an IT organization to gather critical, actionable data about the wireless spectrum for effective troubleshooting. Finally, it introduces Cisco® CleanAir technology and explains how by integrating RF intelligence into the network, users gain tremendous insight into actual usage of the wireless spectrum. This insight is critical to proactively managing Wi-Fi networks to support mission-critical and latency-sensitive applications needed in today's hospitals, distributed enterprises, manufacturing sites, retail stores, and offices.

Wi-Fi Becomes Mission-Critical

The first enterprise Wi-Fi networks were an added convenience used for web surfing in the lobby or conference rooms. For these applications, a best-effort level of performance was acceptable.

Now Wi-Fi has matured to the point that it is being deployed for many mission-critical applications. Hospitals use Wi-Fi for mobile access to patient files and to remotely monitor secondary bedside systems. In retail and manufacturing, Wi-Fi is used for logistics and business transactions. Small branch offices are beginning to use Wi-Fi as the exclusive network access method, forgoing wired connections. And increasingly, Wi-Fi is being used for voice and video, which is sensitive to the impact of interference.

In all these examples, Wi-Fi networks are expected to run with very high reliability. It's no longer acceptable for Wi-Fi networks to have unexpected downtime due to interference.

Defining the Solution

Spectrum intelligence (SI) is data about RF spectrum activity derived from advanced interference identification algorithms similar to those used in the military. SI provides visibility into all the users of the shared spectrum—both Wi-Fi devices and non-Wi-Fi interferers. For every device operating in the unlicensed band, SI reveals: What is it? Where is it? How is it impacting the Wi-Fi network?

Spectrum management is the active use of spectrum intelligence data to improve performance and lower the operational costs of Wi-Fi networks. Information about the severity and duration of interference can be used to calculate its impact on the network and to troubleshoot problems. This information can also be stored for back-in-time analysis and trending. Combined with contextual data like physical location and systemwide correlation, spectrum management is a powerful, proactive tool that increases WLAN reliability, performance, and security.

While external or standalone SI tools have existed for some time, Cisco has taken the bold step of integrating SI directly into the chipset of new access points. Cisco CleanAir is a revolutionary technology and industry first that provides IT managers with access to rich spectrum information that is automatically gathered on every non-802.11 interference source. The spectrum intelligence provided by CleanAir technology enables a new level of spectrum management. In contrast to previous spectrum management tools that could understand and adapt only to other Wi-Fi devices and were usually separate from the wireless network, the new integrated spectrum management is part of the fabric of the wireless network. Second-generation spectrum management is fully aware of all the users of the wireless spectrum, and is able to take action to optimize network performance by mitigating or avoiding interference.

© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Charter Communications, Inc.
Exhibit 1020
Page #1

Performance and Reliability

Beyond understanding interference issues, IT wants the network to address interference issues automatically when possible—both to save on operating expenses (OpEx) and to minimize network downtime. This type of automated tuning is the domain of radio resource management (RRM), which is a layer of software in the infrastructure that automatically adjusts network parameters to maintain RF performance. Older generations of RRM were largely blind to interference issues, other than some crude awareness of “noise.” With integrated SI, a new generation of RRM is able to use detailed knowledge of interference sources to make truly intelligent decisions and achieve new levels of reliability.

In addition to automated RRM, integrated spectrum intelligence can be used systemwide for a broader set of spectrum management tasks. These may be new to Wi-Fi but are familiar to wired network managers:

- Troubleshooting performance problems in real-time
- Performing forensic analysis on intermittent or past problems
- Reporting on usage and interference trends
- Correlating interference problems across multiple access points both to hone in on impact and to reduce excessive alarms

Wireless Security

Ultimately, the challenge of Wi-Fi is not just about performance; it’s also about security. There has been a good level of industry focus on how rogue access points can open up security holes in an enterprise network. Wireless intrusion detection systems and intrusion prevention systems (wIDS/wIPS) have been designed to address this issue. But current IDS and IPS solutions have significant blind spots that cannot be addressed without the addition of spectrum intelligence.

Current IDS/IPS systems cannot detect access points running with proprietary extensions such as Super G (from Atheros). These readily available devices go undetected. Additionally, it’s possible for a hacker to take standard Wi-Fi equipment (for example, running Linux) and modify it to operate on nonstandard channels or with other nonstandard modulation schemes. These extended or modified devices can be detected only if you analyze the RF physical layer.

Beyond Wi-Fi devices, many other types of non-Wi-Fi equipment—including Bluetooth access points, access points running older standards such as 802.11FH, and proprietary wireless bridges—can also be used to open up holes in the network. In the case of bridges, these devices can send data to an attacker who is miles from your building. Again, these types of devices can be detected only if you analyze all the devices that are present in your spectrum.

In addition to the threat of rogue devices, there is always the threat that someone malicious will try to disable your Wi-Fi network with an RF denial-of-service (DoS) attack. Although IDS/IPS systems monitor for many “protocol layer” DoS attacks, they do not detect RF layer DoS attacks that can be implemented through jammer devices or Wi-Fi devices that have been set in a diagnostic jamming mode.

In addition to purposeful attacks, some simple devices like wireless video cameras or analog cordless phones can accidentally cause a total jamming of your network. Integrated spectrum intelligence and spectrum management is very effective for identifying these types of RF-level DoS security threats.

How Is Integrated Spectrum Management Implemented?

Limitations in Standard Wi-Fi Hardware

At a fundamental level, a standard Wi-Fi chipset has limited ability to implement SI. The reason is that Wi-Fi chipsets are specifically designed to receive Wi-Fi signals only—they do not recognize other types of signals (with the

© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

exception of Dynamic Frequency Selection [DFS] radar). Standard chipsets are not even designed to pass up enough information for SI to occur at higher levels of software.

To be specific, when a standard Wi-Fi chipset sees a transmission burst that cannot be understood, it is typically able to report only a few things: 1) that an incomprehensible burst has occurred; 2) the power level of the burst; and 3) the start and stop time of the burst. Note that the burst may actually have been from a Wi-Fi device on another channel or on the same channel, but too far away to be properly received. Or the burst may have been from a non-Wi-Fi device. Detailed information about the modulation type of the burst, where it occurred within the channel, and so on, is typically not available. And there is no ability for software to access the actual data received from the burst for further analysis.

Despite these limitations, it is possible using a Wi-Fi chip to add up the unidentified bursts, and to calculate a total amount of interference, as well as the average strength of interference. Unfortunately, this approach doesn't provide the necessary information to actually solve a problem. For example, the "total interference" approach can't tell you the specific type of the interference (for example, is it just co-channel Wi-Fi interference or something else?), whether the interference is coming from one source or many, where the interference is located, and so on. As this list suggests, the level of SI that can be gathered with a standard Wi-Fi chipset is quite limited.

Cisco CleanAir Technology: A Custom Hardware/Software Solution

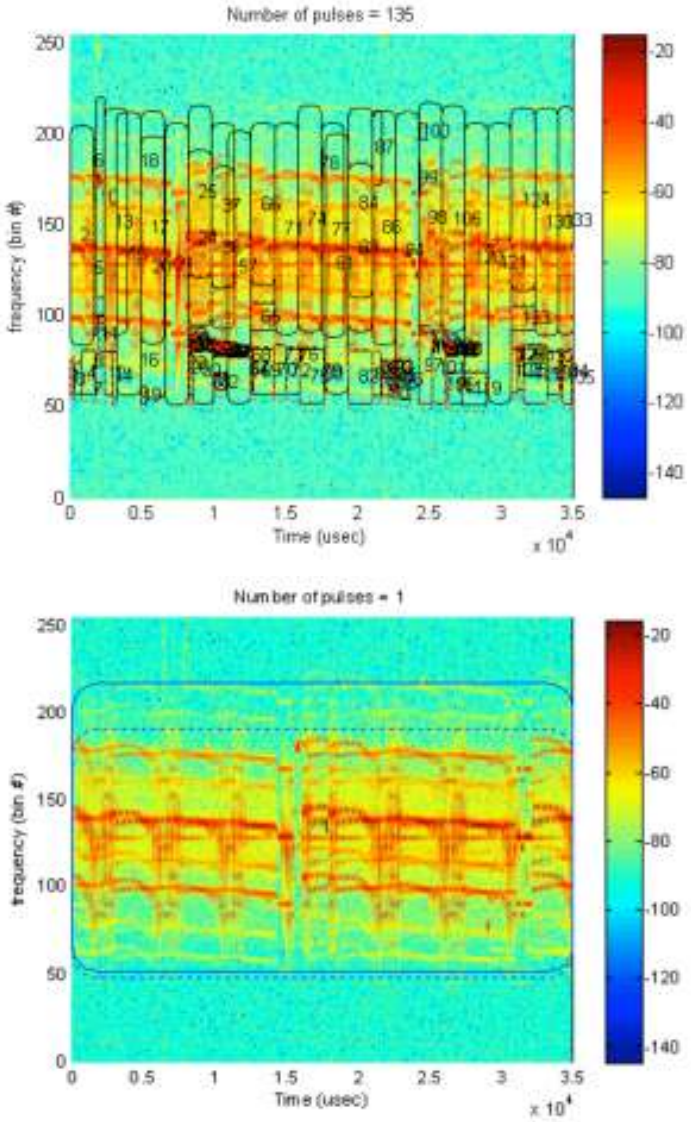
To overcome the visibility limitations inherent to standard Wi-Fi chipsets, Cisco has created an integrated solution with patented chips and software that has been specifically designed to analyze and classify all RF activity. (More than 25 patents have been issued for this technology to date). Essentially, Cisco has taken the technology behind the Cisco Spectrum Expert analysis tool, and integrated it directly into the infrastructure, including deep integration within the Wi-Fi chipset. This is a significant development, and demonstrates that as wireless has transitioned from nice-to-have to business-critical in the enterprise. Consumer-grade Wi-Fi silicon is no longer good enough.

The custom solution starts with the Cisco Spectrum Analysis Engine (SAgE) hardware core, which has been integrated directly into Wi-Fi chipset of the new Cisco Aironet® 3500 Series Access Points. The SAgE core handles very compute-intensive operations such as performing high-resolution Fast Fourier Transform (FFT) and pulse-detection operations. (A pulse is a burst of RF energy in frequency and time.) Essentially, the SAgE core handles a base level of spectrum analysis operations that are so processing-intensive they can be prohibitive to handle in real-time software.

Figure 1 graphically demonstrates SAgE identifying pulses of energy. The first image shows the data from the hardware pulse detector block, and the second image shows the data after software has combined pulses that match closely enough to be considered a single pulse

© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 1. Detected Pulses of RF Energy Before and After Filtering



Once SAgE processing has completed, the radio samples of interesting pulses are passed to the software level for detailed fingerprint analysis. Performing this processing on the main radio CPU would negatively affect Wi-Fi performance. To eliminate this impact, the Cisco hardware solution includes a custom processing core called the DSP Vector Accelerator (DAvE), which is integrated directly into the access point's Wi-Fi chipset. The DAvE core is able to perform intensive signal processing operations, referred to as "Davelets"—such as filtering, decimation, rotation, sync-word detection, and modulation detection—without burdening the main CPU. The DAvE handles CPU-intensive signal processing operations that would otherwise be a burden to the main CPU.

The final processing level occurs in a software module that runs on the main CPU and is referred to as "Sensord." Note that because the heavy lifting has been accomplished by the SAgE and DAvE hardware blocks, the overhead on the CPU is now very low. The Sensord software looks at the timing and frequency of interference bursts, and the discovered attributes of the bursts such as the modulation type and identified sync words. This high-level information

© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

is then used to perform the final identification and separation of one device from another. This final classification step provides the powerful features of SI: telling you the specific source of the interference, where it is located, and how it can be mitigated.

Performance Aspects of SI Implementations

Number of Classifiers

CleanAir technology includes a robust suite of 20 non-Wi-Fi classifiers. Because the analysis takes place in software, the list of classifiers may be expanded as new interference sources become relevant in the market. In other words, the underlying hardware solution is capable of detecting any kind of interference that might be introduced in the future, and requires only updated software.

Simultaneous Detection

CleanAir technology classification is able to distinguish several different interferers—either of the same type or different types—that are operating at the same time. In fact, CleanAir technology is capable of reporting 10 simultaneous interference devices per radio. This is important, because in the real world the amount of simultaneous RF activity can be quite high. Any competing solutions that are not sophisticated enough to distinguish multiple simultaneous devices will quickly fall apart in the field and are only good enough for demos and lab tests.

Time to Detect

Interference devices can be transient, either because they are turned on and off quickly, or because the user is moving through the floor space. For this reason, classification must occur quickly, before it is missed. CleanAir technology enables access points to classify devices within 30 seconds, and is often able to perform classification in less than 5 seconds. (Note that reporting may be slightly delayed when consolidating data across multiple access points).

Probability of False Detection

It is important to not miss a source of interference, and it's equally important to not report "phantom" interference when none exists or to mislabel interference, causing IT to look for the wrong type of device. CleanAir technology is designed to produce low false-detection rates, even in very busy RF environments where hundreds of Wi-Fi and non-Wi-Fi devices are operating simultaneously. By reducing false detection, CleanAir technology saves IT time.

CleanAir Technology: The Importance of Integrated Spectrum Intelligence and Spectrum Management

While the Spectrum Expert product and tool-based solutions play an important role prior to deployment of a network, integrating the SI technology into the Wi-Fi infrastructure provides much more compelling advantages. In the CleanAir integrated solution, the SI engine is built directly into the access points, and SI information is then fully integrated into the network architecture and management systems to enable intelligent spectrum management.

An advantage of CleanAir technology is that it operates 24/7, constantly monitoring for interference and air quality issues (see Figure 2). This allows IT to take a more proactive approach to spectrum management. Instead of waiting for interference to be reported by an end user (in the form of a trouble ticket) 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.

© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 2. Monitoring Interference Devices, Air Quality Trends, and Alerts in the Cisco Wireless Control System

Ability to Match Detected Devices Across Access Points

In a WLAN with integrated spectrum management, it's quite likely that the same interference device will be detected across multiple access points. If each of these devices was reported separately, it would generate too many alerts to the administrator. With CleanAir technology, each device that is detected by an access point is assigned a pseudo-MAC (PMAC) address based on the device attributes. PMACs are then compared across access points. When the PMACs of two devices match (and the access points are in reasonable proximity to each other), the reports from the two access points are "clustered" together. Now the cluster can be reported as a single device to the administrator.

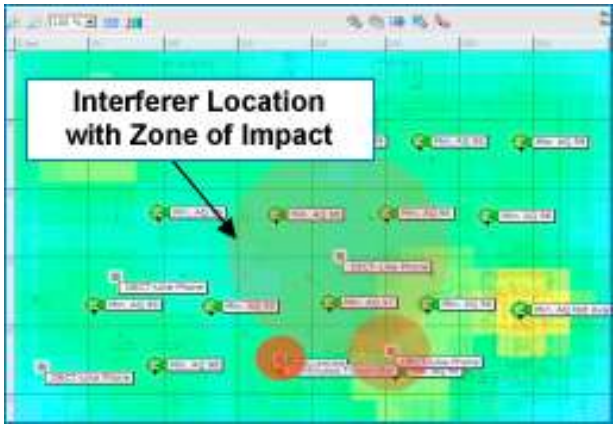
Clustering also plays a significant role in locating devices. A cluster of matching PMACs provides the system with multiple power measurements on the same device, which then makes it possible to triangulate on the location of the device. Important characteristics of device clustering are the ability of the network to cluster devices properly, without overclustering (merging devices together that shouldn't be merged), or underclustering (reporting multiple devices when only one exists).

A second advantage of CleanAir technology is that it can be operated remotely. For many Wi-Fi deployments, the IT staff at one location manages equipment at multiple buildings in a campus or multiple geographical locations, and it can be difficult to physically take a tool to these remotely managed sites. This is particularly true for deployments with many branch offices, or when the interference is transient in nature. By having spectrum management integrated into the infrastructure, IT is able to remotely view interference conditions anywhere on the network.

Cisco CleanAir technology can also physically locate interfering devices (Figure 3). In most cases, multiple access points will observe the same device causing interference. Cisco has developed sophisticated technology to compare the devices reported from multiple access points, and to determine which reports are actually caused by the same device. Once the devices have been correlated, it makes it possible to pinpoint the exact location of the device using triangulation, similar to the way that infrastructure systems are currently able to locate Wi-Fi clients and tags.

© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 3. Locating Interference Devices and Their Zone of Impact



Perhaps the biggest advantage of the CleanAir technology integration into the WLAN is that SI data becomes available to the access point RRM system, where it can be used to implement 24/7 automated mitigation of interference. This is truly the next generation of RRM, allowing for much greater reliability than previous versions, which were blind to interference. With CleanAir technology, it's possible to tune the network to automatically work around many types of interference.

Features of the Cisco Unified Wireless Network with CleanAir Technology

Air Quality and Performance Alerts

Cisco CleanAir technology provides a lot of detailed information about interference. But to facilitate an "at a glance" understanding of where interference problems are impacting the network, it rolls up the detailed information into a high-level, easy-to- understand metric referred to as Air Quality (AQ). AQ is reported at a channel, floor, and system level and it supports AQ alerts, so that you can be automatically notified when AQ falls below a desired threshold.

Map-Based Visualizations

In a CleanAir technology-enabled WLAN, devices that have been analyzed and detected are also integrated with the visual mapping displays provided by the Cisco Wireless Control System (WCS) and Mobility Services Engine (MSE) management systems. In addition to seeing access points and clients on a map, you can track where interference devices exist on the same map. In terms of performance, the ability to see interference devices on the map (as well as their zone of impact) lets you determine what access points, clients, and areas of your floor space are impacted.

From a security perspective, tracking devices on a map lets you know immediately where to dispatch your security personnel.

Security Alerts

In addition to displaying on a map any devices that affect security, you can customize alerts by location—for example, a specific floor of your building. This is a powerful feature since certain devices may be considered a threat in some areas of your building—for example, trading wing—but not in other areas, such as the building's lobby.

Mitigation Features

In addition to flexible deployment, CleanAir technology offers advanced automated response to interference. These automated responses include persistent device avoidance and event-driven RRM.

Persistent device avoidance recognizes that certain devices tend to be static in location and frequency—for example, microwave ovens and wireless video cameras. For this reason, even when these devices are not currently

© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

being detected on a specific channel at a specific location, it's known that they are likely to return at locations in which they have been detected previously. The system tracks these kinds of devices, and when channel selection is performed, tries to avoid channels at locations where persistent devices have been observed.

Event-driven RRM recognizes that some interference events are severe and catastrophic in nature. For example, a cordless phone with a continuous FM signal can cause an outage of several minutes (as long as the phone is active). For this reason, a dramatic drop in air quality causes the system to immediately evaluate changing the channel for the impacted access point. Note that if a channel change occurs, it is done only for the impacted access point, while avoiding any cascading impact to the channel plan of neighboring access points.

Although in many cases the best response to interference is for the administrator to manually move, remove, replace, or shield the interfering device, automated mitigation is highly desirable to maintain short-term performance until other actions can be taken. And in certain cases, it may not be possible to ever remove the source of interference—for example, if it comes from outside the building.

Access Points as Analyzers

Finally, CleanAir technology continues to offer an expert view of low-level spectrum plots comparable to that offered by the Spectrum Expert analyzer tool. Any CleanAir access point can be configured as a network-connected sensor to see the spectrum plots directly as received by the radios on the access point.

While it is true that the system provides a great deal of higher-level analyzed data, including classified devices and air quality, there will always be cases where it is desirable to look at the raw spectrum data itself in real time. Even for enterprises that do not have an RF expert on staff, the Spectrum Expert Connect feature, shown in Figure 4, can be used by an expert who is brought in to help with a particularly difficult-to-diagnose problem.

Figure 4. Using the Spectrum Expert Connect Feature to Diagnose a Problem at an Access Point

Conclusions

Because Wi-Fi operates in a shared unlicensed band, integrated spectrum intelligence and spectrum management are a "must haves" to enable a high level of performance, security, and reliability in your Wi-Fi network. Spectrum management is critical for providing a rich and dependable mobility experience to end users with business-critical wireless applications.

Because the limited RF visibility capabilities of commercial Wi-Fi chipsets are not sufficient, Cisco has integrated patented spectrum processing hardware and software specially designed for analyzing interference, and created a

© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

true enterprise-class Wi-Fi chipset. With this underlying silicon capability, Cisco CleanAir technology classifies and locates individual sources of interference and tells you how it impacts the performance or security of your network.

While SI can be acquired in the form of tools like Spectrum Expert that are useful in the predeployment phase, the best option is to have SI technology integrated directly within the infrastructure. Cisco CleanAir technology provides powerful spectrum management features such as 24/7 proactive monitoring of interference, spectrum security and performance alerts, remote management, and interference device location. Most importantly, integrated SI enables a new level of automated spectrum management that is able to understand and intelligently mitigate the impacts of interference.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1002R)

Printed in USA C11-599260-00 04/10

© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.