

## The Cisco Premium

By Marcus Burton—April 2010

In the vendor scramble towards low-priced commoditized 802.11n hardware, one vendor is drawing a line in the sand and bucking the trend. Perhaps the only vendor that could stand resolute with this decision, Cisco is foregoing the sprint to status quo (low priced 2x2) by introducing the antithesis of commodity, something that fits by itself in a category called “premium.”

Since the Cognio acquisition back in 2007, Cisco stands as the only vendor with the unique position and opportunity to seamlessly embed their own true *spectrum analysis chipset* into the Wi-Fi chipset. And capitalizing on this unique position is exactly what they’ve done by integrating the spectrum analysis hardware from Cognio into the Marvell radio. This integrated feature set is available in their new 3500-series APs, which are beautiful to behold. The 3501i and 3502i (that “i” is for integrated antennas) look similar to the 1142s, with some subtle updates. The 3501e and 3502e (betcha can’t guess what the “e” is for) also took their styling cues from the 1142, again with some subtle updates and well-designed, recessed antenna connectors on top. In addition to the hundreds of thousands of added logic gates in the Wi-Fi radio, I should also mention that Cisco took advantage of this radio update to improve other features as well, such as RRM and ClientLink.



As for compatibility with other components of the CUWN, all WLCs are supported (even the lowly 2106) with new v7 firmware. The WCS also got a bump to v7, and has several new enhancements. You’ll also notice that Cisco Spectrum Expert got a major code revision (up to 4.x) to support remote sensor connectivity. More on that later. After releasing the 1142 AP a while back, Cisco has been an advocate of marrying 802.11n with 802.3af, a trend they’re continuing with the 3500 APs. Yes, this means the Marvell chipset is still 2x3, a fact that doesn’t surprise me. Another transmitter doesn’t give you much in this case, other than a higher power budget. I should also note that they updated their 1252 AP to a 1260-series AP, which is also 802.3af compatible.

While other vendors have previously claimed spectrum-level visibility in their APs, they suffer from the unfortunate effect of ill-advised marketing. What is billed by some as “spectrum analysis” is nothing

more than 802.11 Wi-Fi utilization analysis, or very, very minimal spectrum data. A good feature, but it's not true, useful spectrum analysis. As a side note, this does not include Aruba, who I believe will have legitimate, though limited, spectrum analysis later this year.

As a slight diversion, I have a few comments about Aruba's announcement. One of Aruba's key messages is that they will offer spectrum analysis with existing hardware...no need to buy new hardware. Seriously, that's great! However, existing hardware always has a ceiling on its limitations. With improvements in technology, new hardware for new features is always inevitable. Aruba is eeking out every bit of Layer 1 information from their existing Wi-Fi chipset in order to pitch integrated spectrum analysis with existing hardware. However, they'll quickly reach the ceiling on the hardware's capabilities. Cisco's spectrum analysis hardware is considerably superior to Atheros' current hardware because Atheros designed a Wi-Fi chipset, whereas Cisco/Cognio designed a spectrum analysis chipset. Different purpose, different capabilities. Further, at some point, you have to replace hardware in pursuit of a higher ceiling. The fact that Cisco has integrated Cognio into an AP is a major step in the right direction. This is important stuff, and they're leading the pack in this category by a mile.

Obviously, Aruba knew about Cisco's developments and pending press at Interop, so their preemptive release was intended to take the wind out of Cisco's sails. It's a classic [red herring](#). Poor form, Aruba. I realize this is fundamental aggressive and strategic business marketing (everyone does it), but I'm not a big fan of marketing vaporware. Market what you have when you have it—or at least when you can provide beta releases for third-party validation. No less, I'm talking about Aruba in my review of Cisco, so I guess their marketing worked. DOH!

And now, we're onto the good stuff. By now, we all know that the Cognio chipset has been the de facto standard in mobile (WLAN, anyway) spectrum analysis now for the past many years. This leaves us with little need to verify the quality of Cisco's RF visibility. It's good. I've seen it with my own eyes, touched the APs with my own hands, and put the "dirty air" through its paces. Speaking of dirty air, that is the whole point. In unlicensed frequencies, the RF spectrum is dirty (filled with myriad RF sources), which leads us to Cisco's branding. CleanAir™ is the trademarked term for their integrated spectrum analysis technology. With all the new L1 and L2 horsepower provided by 802.11n, we're in need of some better RF headlights to optimize the network. Clean air is exactly what we need.

When I first heard about CleanAir, I had to stop and first ask about price. In the absence of a low-cost AP solution to compete with the \$500 APs—as well as new architectures—from other vendors, Cisco is releasing a more expensive AP? Further, it is [common—and public—knowledge](#) that Cisco gear comes with a price premium. Or does it? I have to admit that Cisco really surprised me with their prices. Given the value of integrated spectrum analysis, I don't see a price premium with their new APs. Considering that Meru's 320i APs were released a few months ago at ~\$1499 because of internal antennas, CleanAir AP pricing between \$1095 and \$1495 is looking pretty darn good. And as John Chamber's said, though there may be a price premium, true *value* can only be measured as a comparison of "your total cost of ownership v. your productivity." If innovative features like CleanAir™ and ClientLink™ allow employees to be more productive and profitable, and your WLAN to be more resilient and agile in the face of

interference, then the tradeoff of slightly higher cost is moot. Integrated spectrum analysis without a big price premium...very nice!

Cisco's employees are usually well educated, so I think the value of embedded spectrum analysis will be made evident fairly quickly. Let me help demonstrate their value claim with a quick question. What do WMM, airtime fairness, band steering, RRM, and inter-AP roaming have in common? Answer: they are all L2 functions that are designed to optimize multi-service WLANs. If you rely on your wireless network for mission-critical client access, these features are important, right? So, just as a house requires a solid foundation, all L2 WLAN features—as well as all functions at layers 3-7—must be built on a solid RF foundation at L1. Instability in the RF foundation leads to instability in higher layer functions. In other words, if you want your network to support robust applications reliably, layer 1 must be reliable. MIMO helped us out a lot here, but the RF medium is still inherently unpredictable, and it always will be. If you can't predict or control it, the next best thing is to monitor it, to know what is going on at the RF level, and to respond accordingly. RF visibility is what CleanAir offers, and IMHO this is very, very good.

Analysts have predicted that end-user network access will move increasingly towards wireless, and I agree wholeheartedly. This continuing shift demands that we improve our use and understanding of the RF medium. Embedded spectrum analysis is a great place to start. CleanAir provides us with L1 monitoring, but it doesn't stop at monitoring. If you remember the basic history of wireless intrusion detection, you might recall that everything started as a WIDS—wireless intrusion detection—which offers monitoring and reporting, but not preventative response. As WIDS matured, engineers took advantage of the 802.11 protocol, and the WIDS evolved into a responsive solution, a WIPS (wireless intrusion *prevention*). Now WIPS provide monitoring and reporting, as well as automated response (prevention). Reaction is huge. Cisco learned from WIDS/WIPS history and bypassed the lesson at the RF level, taking us straight to RF monitoring, reporting, *and automated response*.

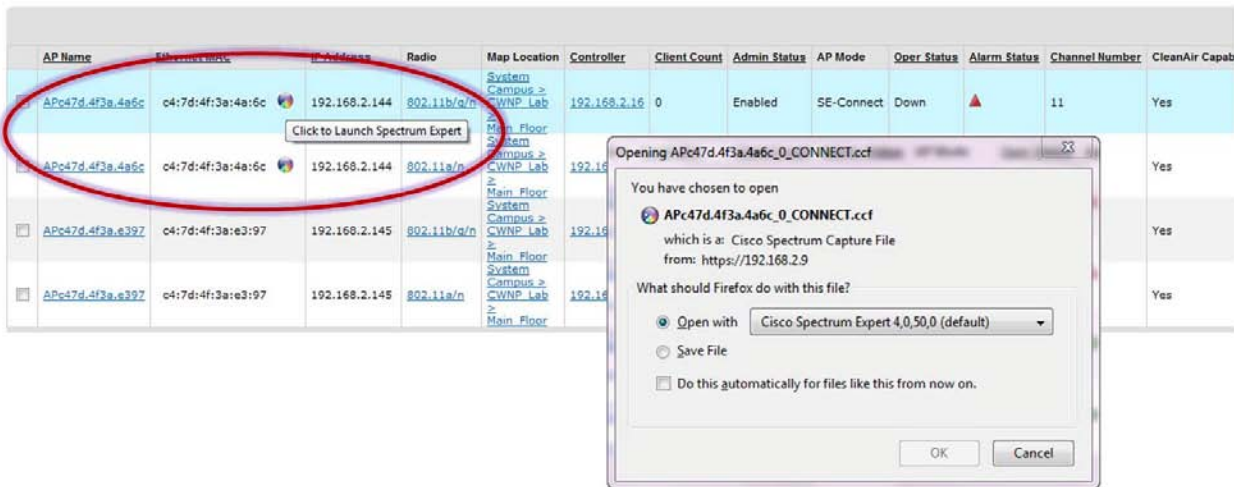
So, if you're already familiar with the Cisco Unified Wireless Network (who isn't these days?), you know that Cisco APs support different "modes." These include Local, Monitor, H-REAP, etc., and allow your AP to support specific functions based on the use case. With the introduction of CleanAir, a new mode, called SE-Connect, has been added.

General		Versions	
AP Name	APc47d.4f3a.e397	Primary Software Version	7.0.93.113
Location	default location	Backup Software Version	0.0.0.0
AP MAC Address	c4:7d:4f:3a:e3:97	Predownload Status	None
Base Radio MAC	04:fe:7f:48:cb:60	Predownload Version	None
Admin Status	Enable	Predownload Next Retry Time	NA
AP Mode	local	Predownload Retry Count	NA
AP Sub Mode	local	Boot Version	12.4.2.4
Operational Status	monitor	IOS Version	12.4(20100329:182527)
Port Number	Rogue Detector	Mini IOS Version	0.0.0.0
	Sniffer		
	SE-Connect		

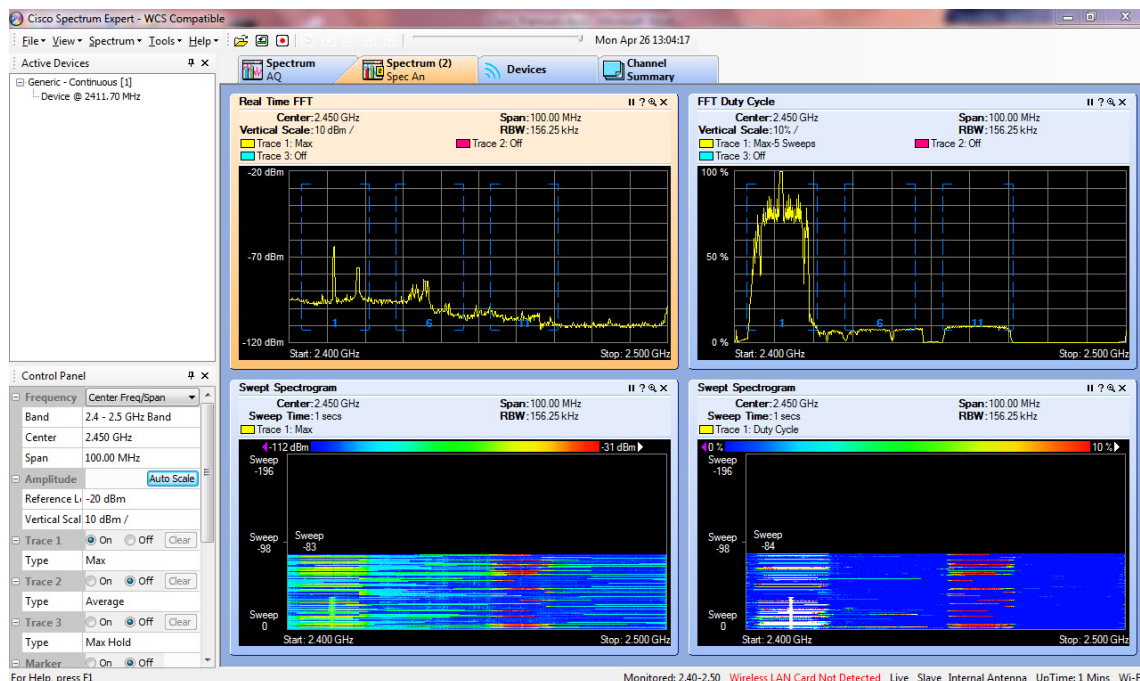
IP Config

When you configure an AP for SE-Connect mode, the AP reboots and becomes a remote spectrum analysis sensor for use with Cisco Spectrum Expert software (remember the 4.x update). This

functionality is just plain slick (have I hidden the fact that I'm drooling?). In WCS, you can launch Spectrum Expert by clicking on the SE icon in the Monitor > AP list.



When you run Cisco Spectrum Expert with a remote sensor, it supports all the same functions as if you had a PCMCIA Spectrum Expert card connected to your laptop. For those users who don't run a WCS, the same functionality—with a different launch method—is supported with CleanAir capable APs and a WLC. The graphic below shows an analog cordless phone on the lower end of the 2.4 GHz band. Of course, I captured this with an SE-Connect CleanAir sensor. Way Cool!



In addition to the new SE-Connect mode, CleanAir also introduces several enhancements to the Monitor mode. This is where the primary, everyday usefulness of CleanAir exists. The CleanAir spectrum analysis functionality sits on the front end of all signal processing when a CleanAir AP is in Monitor

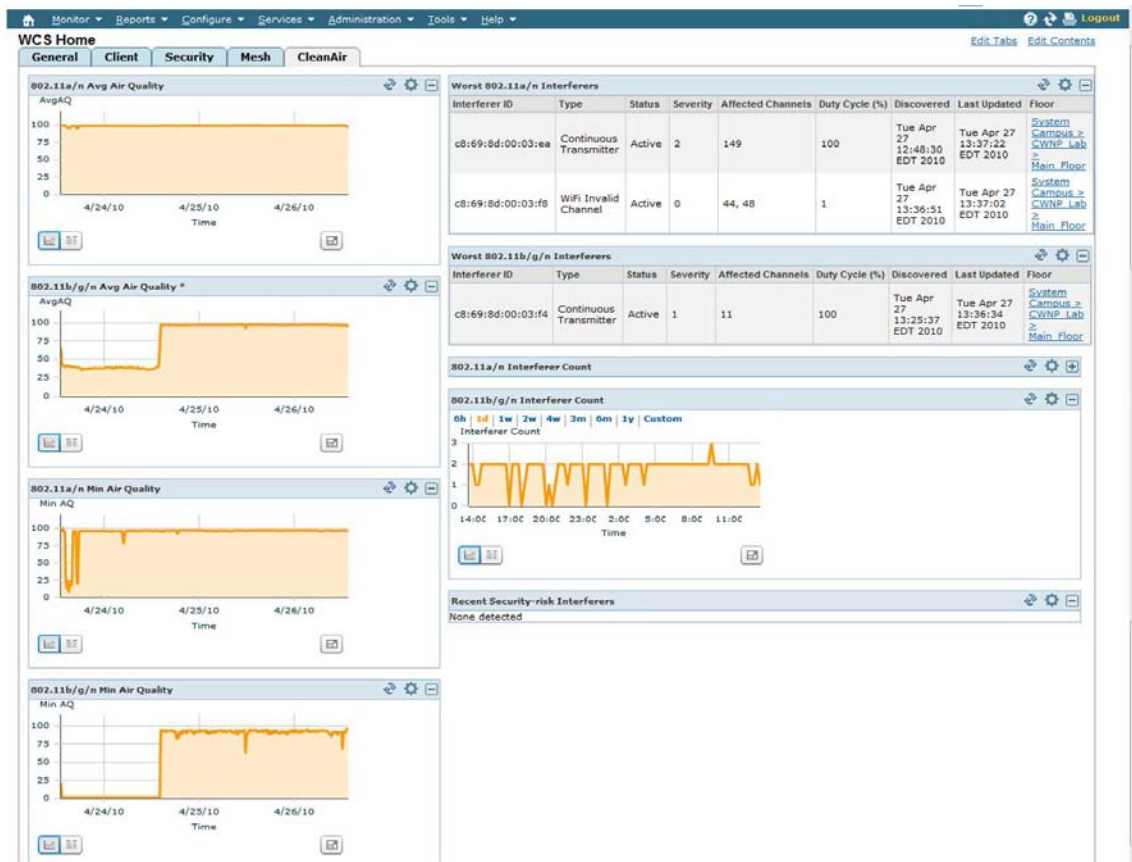
mode. All non-Wi-Fi transmissions are collected and processed by the CleanAir engine. On the other hand, if the radio detects a Wi-Fi transmission (modulated 802.11 signals), signal reception is passed from the spectrum analysis module to the Wi-Fi module for processing. This selection/filtering process allows for detection and classification of signal sources so that the appropriate chip logic can be used to process transmissions. This functionality enables simultaneous support of spectrum analysis (L1 security and performance) and Wi-Fi frame processing (L1 and L2 security and performance), which is a great use of the integration. There's one hiccup with this method that I should note. Specifically, some RF DoS attacks (a spectrum analysis issue) can be performed with Wi-Fi devices using spread spectrum modulation techniques. Nuts about Nets' AirHorn and the Queensland DoS attack with Intersil's Prism NIC are two examples of this type of attack. These modulated Wi-Fi signals would be passed to the Wi-Fi chip module for processing, thus they may not get proper treatment as RF DoS attacks. On the Wi-Fi side, this occurrence should be classified as a security and performance threat if it persistently triggers the CCA ED threshold or cranks up the noise floor beyond useful levels. This issue is a nitpick in the grand scheme of things, especially considering that the spectrum analysis module still picked up my AirHorn DoS attack as an invalid WLAN channel (see graphic). This trigger would allow administrators to investigate further, possibly by launching SE-Connect mode and performing manual analysis.

Worst 802.11a/n Interferers								
Interferer ID	Type	Status	Severity	Affected Channels	Duty Cycle (%)	Discovered	Last Updated	Floor
c8:69:8d:00:03:ea	Continuous Transmitter	Active	2	149	100	Tue Apr 27 12:48:30 EDT 2010	Tue Apr 27 13:37:22 EDT 2010	<a href="#">System Campus &gt; CWNP Lab &gt; Main Floor</a>
c8:69:8d:00:03:f8	WiFi Invalid Channel	Active	0	44, 48	1	Tue Apr 27 13:36:51 EDT 2010	Tue Apr 27 13:37:02 EDT 2010	<a href="#">System Campus &gt; CWNP Lab &gt; Main Floor</a>

This type of scenario highlights an important security aspect addressed by CleanAir. For any standard Wi-Fi radio to properly receive Wi-Fi transmissions, the receiving radio must be configured to receive on a specific frequency. However, with special modifications, rogue Wi-Fi devices could be configured to transmit on invalid Wi-Fi channels where Wi-Fi radios won't normally listen. A traditional Wi-Fi only WIPS without spectrum analysis capabilities would miss these transmissions if the receive radio is not centered on the same frequency as the transmitter, thus highlighting the fact that with spectrum analysis functionality (which processes all RF energy within the monitored frequency range), CleanAir addresses security issues as well as performance issues.

As I think about CleanAir's usefulness for network administrators, I have to come back to some of Cisco's developments in WCS. Specifically, the Home (that's the little house on the top left) menu adds a CleanAir tab that provides a useful launch point and data collection area. As you can see from the screenshot, this screen provides a list of Interferers, as well as Air Quality metrics over time. This Air Quality (AQ) metric is an interesting concept and reflects a granular look at the RF medium. I'll leave it to Cisco to explain this.





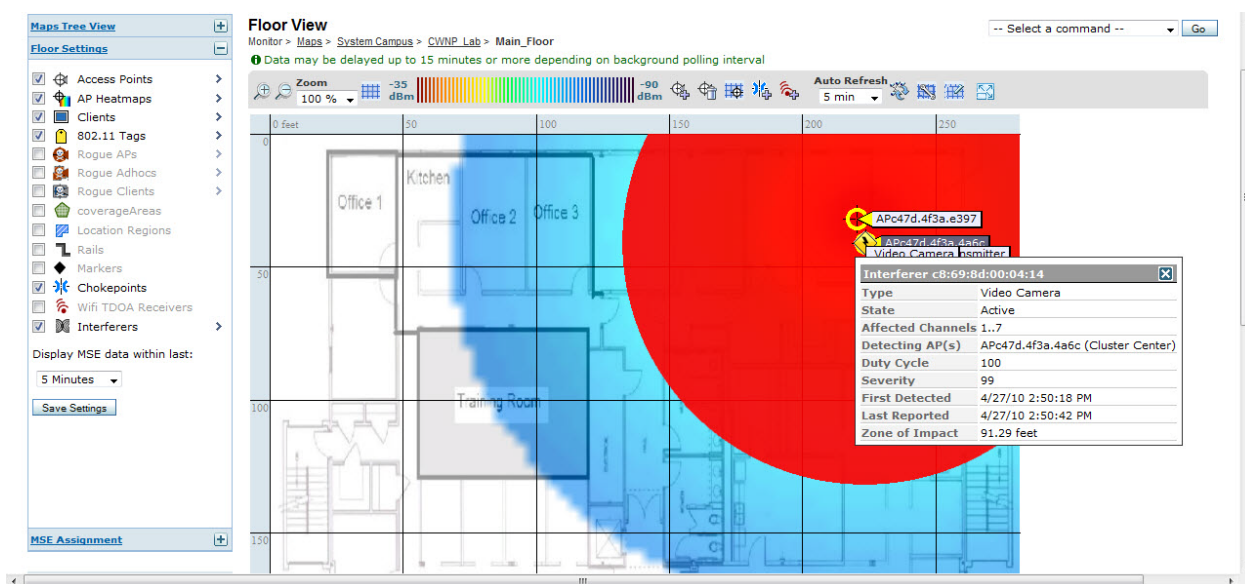
“Today, most standard Wi-Fi chips evaluate the spectrum by tracking all of the packets/energy that can be demodulated on receive—and all of the packets/energy that it is transmitting. Any energy that remains in the spectrum that cannot be demodulated or accounted for by RX/TX activity is lumped into a category called noise. In reality a lot of the “noise” is actually remnants from collisions, or Wi-Fi packets that fall below the receive threshold for reliable demodulation.

“With CleanAir, we take a different approach. We classify all of the energy within the spectrum that is definitely NOT Wi-Fi and account for it. We can also see and understand energy that is 802.11 modulated and classify energy that is coming from Co-channel and Adjacent channel sources. For each classified device, we calculate a severity index, a positive integer between 0 and 100—with 100 being the most severe. Interference severity is then subtracted from the AQ scale (starting at 100—good) to generate the actual AQ for a channel/radio, AP, Floor, Building or campus.” *(From CleanAir Beta guide)*

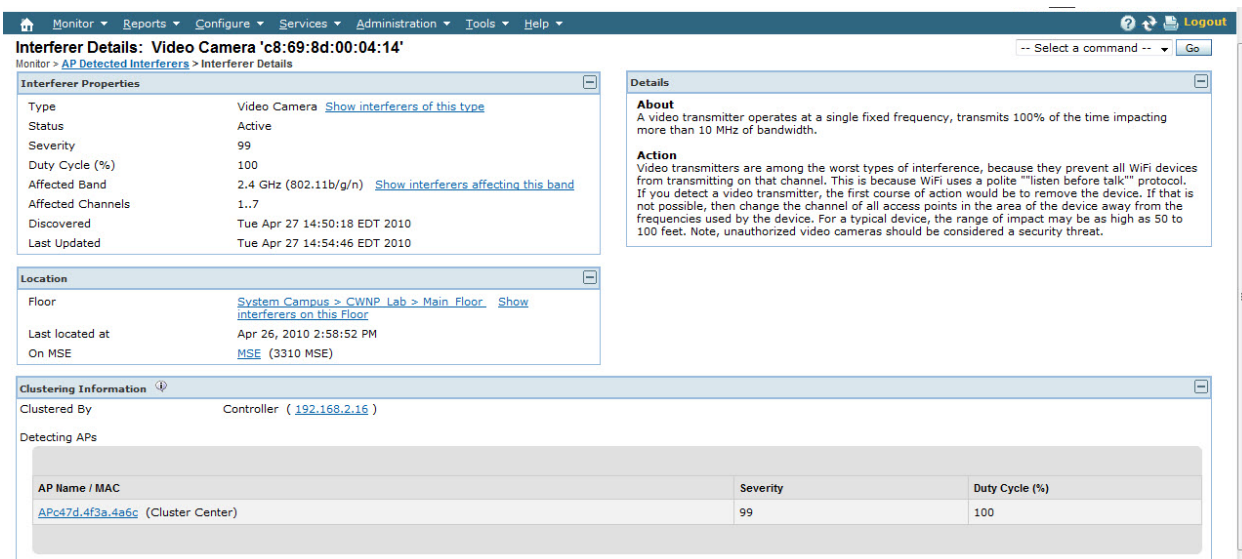
The resolution of the Cognio chipset provides some unique capabilities for Cisco here. Specifically, the quality of the Cognio chipset allows Cisco to proactively respond to interferers that can be positively identified. In other words, there’s a lot of RF traffic in the unlicensed frequency space (especially 2.4 GHz), and it can be difficult to positively classify all of it. So, if CleanAir is to provide reliable and actionable data (and, yes, it does), there is a requirement to ensure positive classification of RF sources before a system response is made. This approach reflects a need for high accuracy, and is the best thing for customers.

They (Cisco) clearly have confidence in the device ID algorithms that they've developed. This confidence allows the CleanAir intelligence to integrate with and inform other features, such as RRM. Case in point, they've added options for RRM's Dynamic Channel Assignment (DCA) functionality, such as Event Driven RRM—allow spectrum-level events to inform RRM decisions—and Avoidance of Persistent RF Interferers. RRM is just one of the many automated uses of spectrum-level visibility within an AP.

Back to my point about administrator usefulness, when you combine CleanAir functionality with a Mobility Services Engine (MSE) and WCS—Cisco recommends this for best use of the features—you get some pretty slick location-based RF information. You may have noticed from the top right corner of the previous screenshot (the CleanAir tab in WCS Home) that Cisco identifies interferers by assigning them to a location with a map link. They're using much of the same location technology used with tracking Wi-Fi tags or client devices (e.g., Fingerprinting and Triangulation). In any case, this location functionality allows for easier isolation of an interferer's location, the interferer's impact on other network devices, and correlation of interference across the network.



On the floor plan, you see the interferer's location (accuracy depends on a number of factors) as well as the interferer's impact with a big red circle. The impact is pretty obvious. As Jim Florwick (Cisco TME) says, "Red is bad." That's easy, even for me. :D If you single click the interferer's location on the map, you get some basic information, such as the type of interferer, affected channels (my wife gets tired of me testing Wi-Fi interference sources near her Wi-Fi network, which is on channel 1), duty cycle, and a severity index (i.e. how bad is the problem). If you double click on the interferer from the map view, you get more information. This is great for inexperienced RF folks, because it spells out the impact in clear language. For example, it provides an "Action" explanation that details the typical impact of this type of device.



The screenshot shows the Cisco CleanAir web interface. The top navigation bar includes links for Monitor, Reports, Configure, Services, Administration, Tools, and Help. The main content area is titled "Interferer Details: Video Camera 'c8:69:8d:00:04:14'". It contains several sections:

- Interferer Properties:** A table showing details about the video camera, including Type (Video Camera), Status (Active), Severity (99), Duty Cycle (%) (100), Affected Band (2.4 GHz (802.11b/g/n)), Affected Channels (1..7), Discovered (Tue Apr 27 14:50:18 EDT 2010), and Last Updated (Tue Apr 27 14:54:46 EDT 2010).
- Location:** A table showing the location of the camera, including Floor (System Campus > CWNP Lab > Main Floor), Last located at (Apr 26, 2010 2:58:52 PM), and On MSE (MSE (3310 MSE)).
- Clustering Information:** A table showing the controller (192.168.2.16) and the detecting APs.
- Details:** A section providing information about video transmitters, including their operating frequency, bandwidth, and the action to be taken (removing the device or changing the channel).

This is already an abnormally long review, but I have one more point, and it relates to Wi-Fi utilization. With a typical protocol analyzer, you can analyze Wi-Fi utilization in terms of Wi-Fi traffic (L2). Wi-Fi utilization is great, and if you know how to analyze the data, it usually gives you a pretty clear sense of the network's performance. However, this type of analysis can't account for utilization of the RF spectrum by non Wi-Fi devices, which may account for a significant portion of your network's problems. I think mobile products will continue to be useful for this type of work, but integrating spectrum analysis in the AP gets us several steps closer to a holistic view of our network's health at the AP. When it comes to troubleshooting, making a network run smoothly is always about finding and fixing the *source* of the problem. We often start with symptoms and diagnose from there. Spectrum visibility is one of the key ingredients to this type of wireless insight.

I'm making a conscious effort to stop myself here and shut up. I believe that integrated spectrum analysis is a trend that will be embraced by other vendors in the near-ish future. At present, Cisco has a significant head start with the integration of one of the best spectrum analysis chipsets in their APs. Given the unique offering, I would have expected a big price premium, but they're turning the "Cisco Premium" upside down with premium features, and palatable prices. Spectrum-level enhancements are incredibly important, and from my perspective, Cisco is doing all the right things with CleanAir by making it accessible and relevant to network administrators. This is a noteworthy advancement for the industry...one that I expect to make a lot of noise (and avoid some noise at the same time). I'm thoroughly impressed!



**About CWNP, Inc.**

CWNP is the recognized industry standard for enterprise Wi-Fi training and certification. CWNP is the only vendor neutral wireless LAN certification program in the industry, covering the full range of technologies underlying all enterprise WLAN products. CWNP offers four levels of enterprise WLAN certification, from novice to expert, and prepares IT professionals to specify, design, and manage wireless LAN infrastructure and applications regardless of the vendor solution utilized. Professionals in more than 130 countries have achieved CWNP certifications, enabling them to make wireless LANs more cost-effective, reliable, and secure. CWNP is a privately-held corporation based in Atlanta, GA. For more information about CWNP, visit [www.cwnp.com](http://www.cwnp.com).

